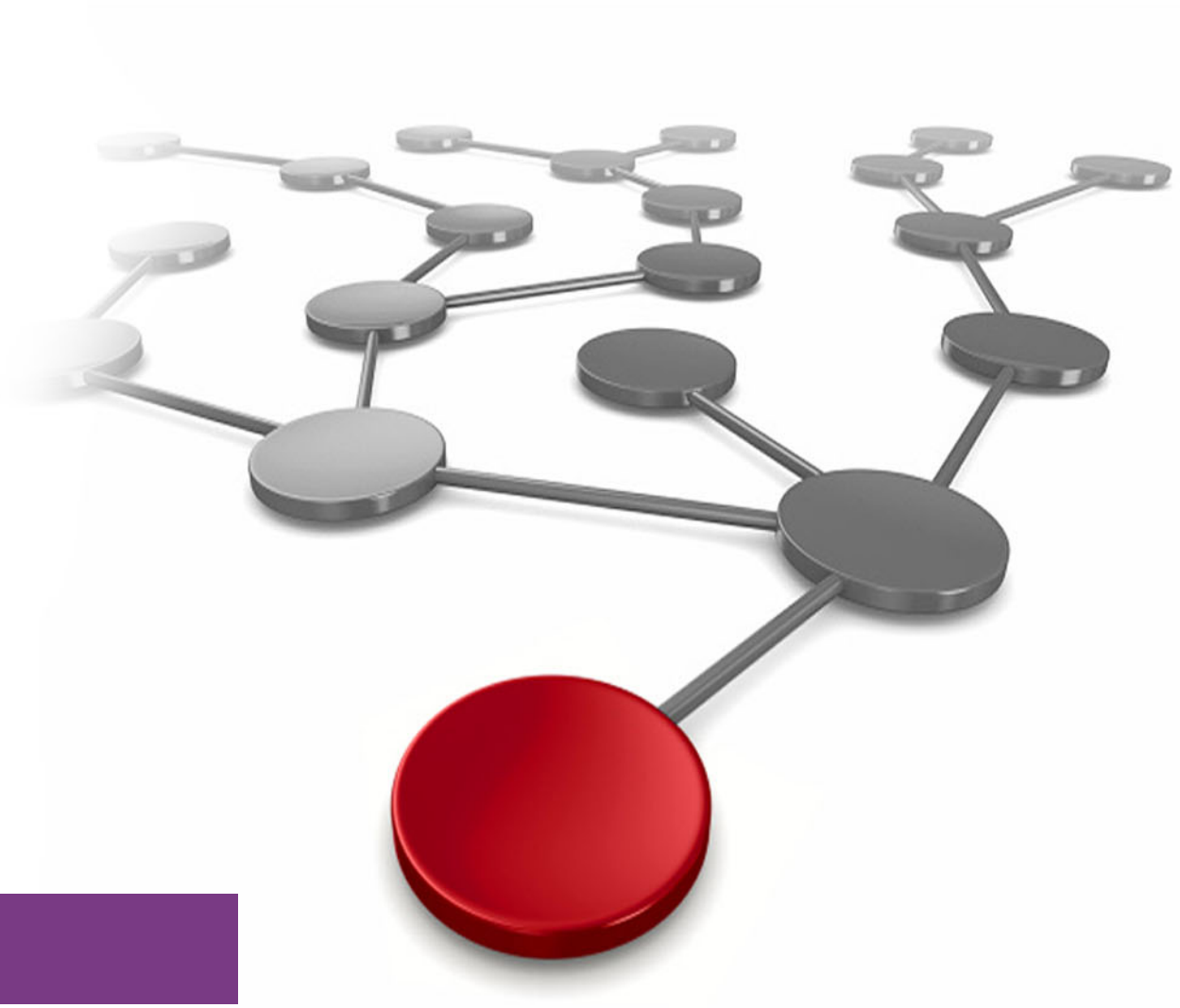
Redbooks
ibm.com/redbooks

IBM FlashSystem Safeguarded Copy Implementation Guide

Andrew Greenfield
Jackson Shea
Hemanand Gadgil
Vasfi Gucer



Storage

IBM

Redpaper

IBM Redbooks

IBM FlashSystem Safeguarded Copy Implementation Guide

March 2022

REDP-5654-00

Note: Before using this information and the product it supports, read the information in “Notices” on page v.

First Edition (March 2022)

This edition applies to Safeguarded Copy function that is available with IBM Spectrum Virtualize Version 8.4.2

Contents

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

FlashCopy®	IBM Security™	Redbooks®
HyperSwap®	IBM Spectrum®	Redbooks (logo)  ®
IBM®	Passport Advantage®	Storwize®
IBM FlashSystem®	QRadar®	XIV®

The following terms are trademarks of other companies:

ITIL is a Registered Trade Mark of AXELOS Limited.

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

Safeguarded Copy function that is available with IBM® Spectrum Virtualize software Version 8.4.2 supports the ability to create cyber-resilient point-in-time copies of volumes that cannot be changed or deleted through user errors, malicious actions, or ransomware attacks. The system integrates with IBM Copy Services Manager to provide automated backup copies and data recovery.

This IBM Redpaper publication introduces the features and functions of Safeguarded Copy function by using several examples.

This document is aimed at pre-sales and post-sales technical support and storage administrators.

Authors

This paper was produced by a team of specialists from around the world.

Andrew Greenfield is an IBM Global XIV® and Flash Solution Engineer who is based in Phoenix, Arizona. He holds numerous technical certifications from Cisco, Microsoft, and IBM. Andrew brings over 24 years of data center experience inside the Fortune 100 to the team. He graduated magna cum laude, honors, from the University of Michigan, Ann Arbor. Andrew has also written for and contributed to several IBM Redbooks® publication.

Jackson Shea is a consultant on the North America IBM Systems Lab Services team. He has been with IBM for 10 years. Before that, he worked for The Regence Group, a BlueCross BlueShield consortium for Oregon, Washington, Idaho and Utah. The Regence Group was a long-time IBM client where Jackson managed IBM, EMC, and Hitachi storage systems on McData, Brocade and Cisco Storage Area Networks (SANs) in three data centers. With IBM, he has focused on implementations of Spectrum Virtualize, particularly SAN Volume Controller Enhanced Stretch Cluster, and has been deeply involved with the development of Spectrum Virtualize for public cloud. He is also knowledgeable in areas of data encryption, storage management automation, and SAN management and extension technologies.

Hemanand Gadgil is an IBM Storage Solutions Architect who works with various independent software vendors (ISVs) partners for storage solutions designs in Pune, India. He received his Bachelor of Engineering degree in Electronics from the University of Pune, India. His current interests are cloud, hybrid multicloud, disaster recovery (DR), and business continuity solutions. Hemanand joined IBM in 2015 as a Storage Solutions Architect. His skills include various storage technologies, data center migration, and infrastructure and data center consulting.

Vasfi Gucer is a project leader with the IBM Systems WW Client Experience Center. He has more than 25 years of experience in the areas of systems management, networking hardware, and software. He writes extensively and teaches IBM classes worldwide about IBM products. His focus has been primarily on storage and cloud computing for the last 8 years. Vasfi is also an IBM Certified Senior IT Specialist, Project Management Professional (PMP), IT Infrastructure Library (ITIL) V2 Manager, and ITIL V3 Expert.

Thanks to the following people for their contributions to this project:

Kristopher Keller, Mary J. Connell, Oiza Dorgu Yves Santos
IBM USA

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an IBM Redbooks residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks
- Send your comments in an email to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, IBM Redbooks
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

1

Spectrum Virtualize Safeguarded Copy introduction and concepts

The Spectrum Virtualize Safeguarded Copy technology, concepts, and use cases are described in this chapter. First, the business driver for this function is established, especially the need for *logical corruption protection* (LCP) and information is provided about regulatory requirements.

Next, the general concepts and components of LCP, as implemented in Spectrum Virtualize Safeguarded Copy, are described. This involves a discussion of the general process of LCP and a specific focus on how Copy Services Manager is used to implement the policies for the Spectrum Virtualize snapshots that are housed in Safeguarded child pools.

Lastly, all the information is presented in sample use cases.

This chapter includes the following topics:

1.1 The business need for Safeguarded Copy

Safeguarded Copy on Spectrum Virtualize supports the ability to create cyber-resilient point-in-time copies of volumes that cannot be changed or deleted through user errors, malicious actions, or ransomware attacks. The system integrates with IBM Copy Services Manager to provide automated backup copies and data recovery.

The business needs of Safeguarded Copy are as follows:

- "Ransomware and cyberattacks"
- "Regulatory requirements"
- "Data protection methods"

1.1.1 Ransomware and cyberattacks

The recent high profile ransomware attacks of 2021 (Accenture, Kaseya, and Colonial Pipeline) brought to the forefront the personal, financial, and social impacts of ransomware attacks. In the 2020, several high profile attacks were launched against health care facilities, likely targeted during the height of the COVID-19 pandemic.

1.1.2 Regulatory requirements

However, even before the recent string of cyberattacks, Health Insurance Portability and Accountability Act (HIPAA) in the USA and General Data Protection Regulation (GDPR) in the EU compelled organizations to use technologies to ensure that certain data is encrypted, but also preserved for a set time in a non-modifiable state.

More specific examples of cybersecurity guidelines are found in the *US Federal Financial Institutions Examination Council* (FFIEC) revised publication, *Business Continuity Planning Booklet,* which is part of the FFIEC's *Information Technology Examination Handbook* for the US financial industry.

In Appendix J, colloquially referred to as App-J, the FFIEC provides the following guidelines:

- "The financial institution should take steps to ensure that replicated backup data cannot be destroyed or corrupted in an attack on production data."[1]
- "...air-gapped data backup architecture limits exposure to a cyberattack and allows for restoration of data to a point in time before the attack began."[1]

Similar statements are made by the US *National Association of Insurance Commissioners* (NAIC) and from the *European Banking Authority* (EBA).

The NAIC states:

> *... It is vital for state insurance regulators to provide effective cyber-security guidance regarding the protection of the insurance sector's data security and infrastructure.*[2]

[1] https://www.ffiec.gov/press/pdf/ffiec_appendix_j.pdf
[2] http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf

1.1.3 Data protection methods

The new Safeguarded child-pool capability on the Spectrum Virtualize family of products (FlashSystems, SAN Volume Controller, and Spectrum Virtualize for Public Cloud) and is introduced in version 8.4.2.0.

High Availability (HA) configurations mitigate against physical component failure and provide small *Recovery Point Objective* (RPO) and *Recover Time Objective* (RTO). Continuous protection and operation occur in the event of a component failure. Spectrum Virtualize HA configurations such as HyperSwap® and Stretch Cluster provide such protection.

Disaster Recovery (DR) is designed to have a slightly higher RPO and RTO. Therefore, DR is in a position to provide an *airgap* to protect against corruption to the data that would be replicated immediately in a Spectrum Virtualize HA configuration like HyperSwap or Stretch Cluster. However, since DR solutions at the storage layer are only replicating data, any logical corruption would eventually get replicated to the DR site as well.

One way to provide adequate protection against logical data corruption is to take periodic snapshots of the data and to have that data stored in a non-modifiable state that is inaccessible to administrators, servers, and applications. These *Safeguarded* copies can then serve as recovery points from which the data could be restored to a pre-corruption state, whether that corruption occurred as a result of an errant batch job, a disgruntled employee, or a ransomware attack.

1.2 The components and concepts of Safeguarded Copy

The key components of Spectrum Virtualize Safeguarded Copy are as follows:

- “Volume groups”
- “Safeguarded child pools”
- “Safeguarded policies”
- “Copy Services Manager integration”

1.2.1 Volume groups

Safeguarded Copy on Spectrum Virtualize is implemented through the introduction of a new way of working with point in time copies, or the FlashCopy® function. The new method uses v*olume groups,* which are similar to *consistency groups*. However, in addition to ensuring that a group of volumes is preserved at the same point in time, the volume group also enables the simplification of restoration or recovery to that point in time. It does this through the association of a group of volumes with a snapshot policy that determines frequency and retention duration.

1.2.2 Safeguarded child pools

Introduced in IBM Spectrum® Virtualize Version 7.3, c*hild pools* allow the creation of a logical pool or managed disk group (`mdiskgrp`) within a parent pool or `mdiskgrp`. This child pool is assigned capacity out of the parent pool and can be assigned administrative ownership to a specific user or group-of-users distinct from the parent pool.

Note: In the Spectrum Virtualize implementation of immutable copy, the Safeguarded Copies of a volume *must* reside in a child pool of the pool or `mdiskgrp` that contains the source volume. Otherwise, upon attempting to associate a *Safeguarded policy* with the volume group, an error will occur.

1.2.3 Safeguarded policies

The Spectrum Virtualize Safeguarded Copy function includes policies that drive the frequency and retention of copies taken. A policy is then applied to a volume group so that volumes in that volume group have immutable copies taken and retained in accordance with the policy. Three default policies are included (see Figure 1-1).

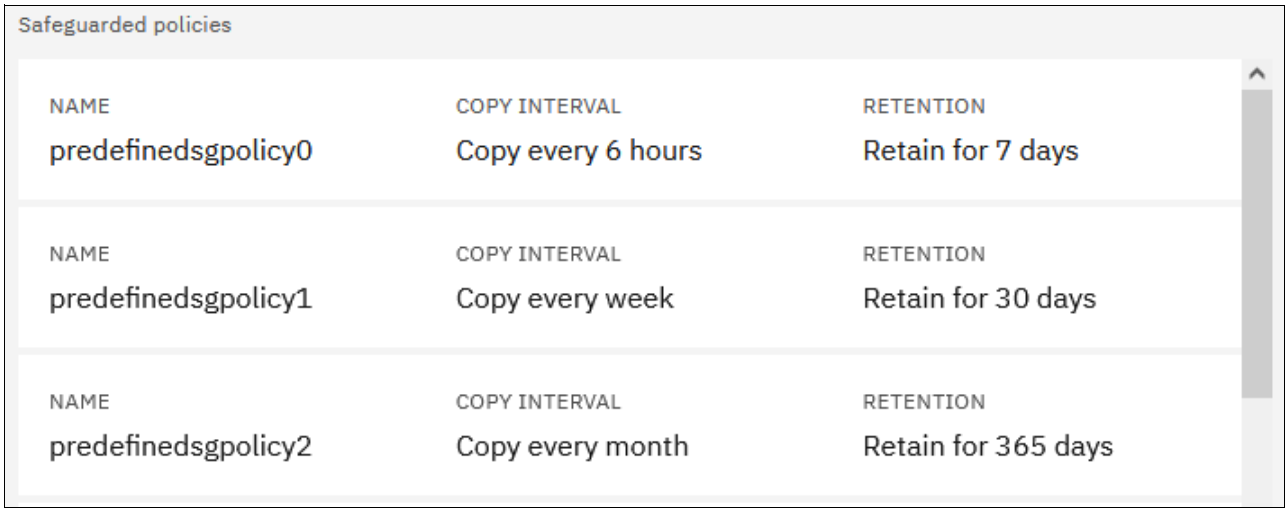


Figure 1-1 Default Safeguarded policies

To create additional policies, use the **`mksafeguardedpolicy`** CLI command:

```
mksafeguardedpolicy -name 4hr14keep -backupunit hours -backupinterval 4
-backupstarttime 2109161500 -retentiondays 14
```

The start time format is `YYMMDDHHMM`, and `backupunit` options are: minute, hour, day, week, or month.

1.2.4 Copy Services Manager integration

In the first iteration of the Spectrum Virtualize Safeguarded Copy function, IBM Copy Services Manager is used to interpret and implement the policy set for a *volume group* by creating the necessary components within the copy services orchestration tool, starting with a session with the naming convention of {*volume_group*}_{*Spectrum Virtualize System*}. Within the session, there are copy sets for each of the protected volumes. In addition, a scheduled task is set up to execute copies on the frequency that is specified in the safeguarded policy.

1.2.5 Putting it all together

To create Safeguarded Copies on Spectrum Virtualize, complete the following steps:

1. Identify volumes to be copied.

2. Create Safeguarded child pool in the parent pool of those volumes.
3. Create a volume group for those volumes.
4. Create or select a predefined Safeguarded policy and associate the policy with the volume group.
5. IBM Copy Services Manager periodically scans managed Spectrum Virtualize storage systems for the existence of volume groups with an associated Safeguarded policy.
6. IBM Copy Services Manager periodically creates Safeguarded copies in accordance with the backup interval value that is specified in the Safeguarded policy.
7. Spectrum Virtualize then deletes the IBM Copy Services Manager-orchestrated *Safeguarded Copy* volumes in accordance with the retention value that is specified in the Safeguarded policy.
8. After copies are made of the volumes in the volume group, they can be used to *restore* or *recover* the data.

Note: In the IBM Copy Services Manager-mediated Safeguarded Copy function for Spectrum Virtualize, the two modes of data retrieval are as follows:

- **Recovery**: This method of data retrieval creates new volumes from the parent pool that contains the Safeguarded child pool and copies the data from the Safeguarded Copy (where retained copies of changed blocks are stored) and the source volumes (for unchanged blocks since the time of the Safeguarded FlashCopy).
- **Restoration:** This method of data retrieval copies the data back to the original source volume in the same way as described for *recovery*. The only difference is that the target of the retrieval is the original volume and not a new one. This should be used only when it is determined that the Safeguarded Copy from which the retrieval is occurring is the correct one.

1.3 Overall strategy considerations for Safeguarded Copy

While this document focuses on the components and use of Spectrum Virtualize Safeguarded Copy, it is important to place the solution in a larger context to illustrate how this new capability might fit into an overall cyber resiliency strategy. Some other components to consider are as follows:

- “Disaster recovery replication”
- “Backup infrastructure architecture”
- “Storage Management Hardening”
- “Monitoring”
- “Validation”
- “Automation”

1.3.1 Disaster recovery replication

One of the key components of a sound cyber resiliency solution is the notion of an air-gap that insulates the *safeguarded* or immutable copy from access or tampering. Spectrum Virtualize accomplishes this by making the immutable copies unmappable. Since the volumes cannot be mounted by a host system, they have significant protection against tampering.

For further isolation, if the environment has replication in place, the choice might be made to take the Safeguarded Copy at the DR or replication target site. This has the added benefits of physical and network isolation and also removes any additional load on the primary volumes that is incurred by maintaining the point-in-time copies.

1.3.2 Backup infrastructure architecture

Another consideration and possible integration point for Safeguarded Copy is a traditional backup infrastructure like IBM Spectrum Protect (https://www.ibm.com/products/data-protection-and-recovery). Because IBM Spectrum Protect can have a longer retention period than what you might want to implement by using online Safeguarded Copy in IBM Spectrum Virtualize (due to performance and capacity considerations), it is useful to balance the two complementary capabilities in a holistic data protection strategy.

Moreover, many environments use traditional FlashCopies with the “backup” setting (incremental FlashCopies with copy rate greater than zero) to decouple the heavy read-I/O from the primary volume. It might be advantageous to create the *Safeguarded copies* against these “backup” FlashCopies instead of the primary volume.

Another benefit of using these “backup” FlashCopies is that the *Safeguarded copies* would then be stored in a *Safeguarded child pool* whose parent is the pool in which the “backup” FlashCopies are created rather than the primary volume. This further insulates I/Os against the primary volume.

1.3.3 Storage Management Hardening

In the overall solution workflow and lifecycle description, Spectrum Virtualize performs the deletion of *Safeguarded copies*. Manual deletions are also allowed by users with *Security Administrator* role. To mitigate this potential exposure to tampering, it is now possible to lock out the default Security Administrator user, which is *superuser*. However, there are specific maintenance functions that can be performed only by the *superuser* account, such as service assistant commands (**satask** or **sainfo** command line interface (CLI) commands or by accessing the service assistant tool graphical user interface (GUI)). Therefore, there are specific steps regarding the restriction of *security administrator* functions, especially the *superuser* account. These steps are detailed Chapter 3, “Safeguarded Copy implementation and management” on page 17.

1.3.4 Monitoring

A key component of any cyber resiliency solution is intrusion detection. While this is mainly implemented in the network or application layer, there are also tools associated with storage that can provide early warning and direct integration into Spectrum Virtualize. One such tool is *Storage Insights* (https://www.ibm.com/products/analytics-driven-data-management), which has traditionally been used to provide performance and capacity reporting capabilities to storage environments. The Storage Insights tool provides additional support enhancement benefits such as reducing the amount of time needed to create tickets and uploading logs to support.

Because these tools already have the capability to monitor the storage environment, they are perfectly positioned to detect sudden changes in storage consumption and decreased compressibility, which would be indicative of an application-level encryption-based ransomware attack.

Another IBM monitoring tool that is capable of correlating events that might be indicative of an intrusion is *IBM Security™ QRadar® XCD* (https://www.ibm.com/security/security-intelligence/qradar). Both these tools, when incorporated into an overall cyber resiliency solution, can provide valuable alerting that might greatly reduce recovery time.

1.3.5 Validation

Another important part of a complete cyber resiliency solution is the ability to validate the created copies. This can be accomplished through a range of methods.

Typically, if the volumes are part of a filesystem, you can map the recovery volume to a validation host that will verify that it is operating as expected.

Further validation at the application level might be desired beyond simply mounting the filesystem at the operating system level. Other strategies involve checkpoint files that might be used. Regardless of the method used, and other than cyber resiliency, periodic validation of backups is a sound IT practice.

1.3.6 Automation

The last consideration for a full range, end-to-end cyber resiliency solution is automation. As implied by end-to-end, this starts with the provisioning of a new set of volumes for an application that meets requirements for Safeguarded Copy protection. The automation is incorporated into the provisioning process so that either the primary volume, or backup FlashCopy or replication target volume is placed into an appropriate volume group with the appropriate policy for the frequency and retention of Safeguarded copies.

There is also automation for periodic recovery and validation of the Safeguarded copies. Another area for automation is the monitoring of suspicious activity, which might then trigger the initiation of access lockdown.

If the primary volumes are corrupt and require restoration, there should be automation for the selection of the most recent valid Safeguarded Copy of the data and the retrieval of that data back to the original volumes.

2

Safeguarded Copy planning considerations

This chapter discusses the following considerations for the implementation of Spectrum Virtualize Safeguarded Copy and several IBM resources that can assist with the planning process.

This chapter includes the following topics:

The IBM resources that might be of assistance with some or all of these considerations are:

2.1 Planning considerations

The planning considerations that are listed in this section are generally interdependent, although the level of interdependence varies from environment to environment. For instance, security regarding access restriction, network isolation, and process integration are driven by regulatory and business requirements. The interdependencies also tend to iterate and nest. Examples of these are access restriction and network isolation. These considerations pervade all aspects of IT infrastructure. Therefore, the discussion of the considerations is not meant to be approached in a linear fashion but continually balanced.

2.1.1 Regulatory requirements

Two examples of regulatory requirements for the US and Europe are listed in the introduction chapter. These are not comprehensive, considering that they apply only to two geopolitical regions of the world. Furthermore, each industry has specific guidance that extends into specifics regarding data protection and privacy. The common ones are health care and finance.

Rather than detail additional specifics from the regulatory guidance and requirements, it is sufficient to know that they are frequently the driving force behind implementation decisions and business requirements.

2.1.2 Business requirements

Regulatory requirements often drive implementation decisions. By extension, financial cost, integration with existing processes, and many other considerations need to be balanced in concert. However, the common themes of those decisions revolve around the following concepts:

- **Recovery Point Objective (RPO)**: Common terminology for discussing the amount of data or transaction loss that can be tolerated by the business measured in time (seconds, minutes, hours). This determines the frequency of backups that need to be taken and also considers replicated environments and how aggressively the replicated data needs to be in sync with the primary site.
- **Recovery Time Objective (RTO)**: Common terminology for discussing the amount of time that is needed to get back to business after a disrupting event occurs. This is measured in time (seconds, minutes, hours, and possibly days). This consideration drives several factors. The main ones are speed of the backup storage media, application consistency, and the number and duration of sequential steps involved in the restoration of business functionality. How many steps does it take to get back to business and how long do those steps take? Keep in mind that while this is heavily influenced by technology, it is as important to consider the established business processes and staffing considerations.
- **Network isolation or airgap**: This requirement surfaces as a desire to “vault” protected backup assets in an isolated environment that is difficult or impossible to access through means by which normal application use or administrative operations are conducted. In the case of Safeguarded Copy for Spectrum Virtualize, this might be satisfied by the fact that the immutable copies cannot be mounted by a host and cannot be deleted by a user other than superuser and the expiration date on the volume cannot be changed. However, some businesses might require the Safeguarded copies to be taken on a separate storage device that is receiving replicated data from the primary volumes.

2.1.3 Copy Services Manager

The Spectrum Virtualize Safeguarded Copy function introduced in 8.4.2.0 requires *Copy Services Manager* 6.3.0 or higher to orchestrate and automate many aspects of the solution such as:

- Scheduled execution of the backups.
- Visualization of the backup time points for a given set of volumes in a volume group.
- Perform recovery and restoration.
- Manage remote copy replication.

Refer to the IBM Documentation on IBM Copy Services Manager 6.3.1 (https://www.ibm.com/docs/en/csm/6.3.1) for supported platforms and recommended sizing.

2.1.4 Process integration

Safeguarded Copy is one feature in a full-spectrum enterprise data-protection landscape. Many environments will also use some, and possibly all of the following:

- Backup software such as Spectrum Protect, which might write to tape or virtual tape
- Standard point-in-time copies (non-Safeguarded), snapshots, or full copies
- Remote copy replication

Therefore, Safeguarded Copy should not be implemented in a vacuum but rather together with the other existing processes. This might help to determine or change frequency requirements from what was initially determined.

If full-copy FlashCopies are already being taken to insulate the primary volumes from heavy reads during backups, then those volumes might be better candidates for the Safeguarded Copy source volume, assuming this meets the RPO and RTO requirements.

Finally, if the data is replicated to a secondary site, the replicated volume might be a better place to serve as the source for Safeguarded Copies. The replicate volume would also provide a physical air-gap from the primary volume. However, this affects the RTO because recovery to the primary site requires replication back from the secondary site before the application can be brought online unless compute and network resources are available for the application to be brought up at the replication target site.

These are examples of scenarios that might affect how Safeguarded Copy is implemented in a larger context and should be part of the planning process.

2.1.5 Capacity

Safeguarded Copy uses the Spectrum Virtualize point-in-time copy functionality, called *FlashCopy*. FlashCopy is designed so that Spectrum Virtualize attempts to consume as little space as possible by using *Copy on Write* (CoW) with traditional volumes and *Redirect on Write* for deduplicated volumes in a Data Reduction Pool (DRP). For more information on these topics, see *Implementing the IBM FlashSystem® with IBM Spectrum Virtualize Version 8.4.2,* SG24-8506.

The greatest capacity savings are achieved by using deduplicated volumes in a DRP, but using deduplicated volumes must be balanced against the additional overhead of metadata management. With non-deduplicated volumes that are using *Copy on Write* (CoW), further

efficiency is engineered by using a linked list for referencing data so it needs to be written only once (to the most recent FlashCopy relative to when a region of data is changed). All older FlashCopies dependent on that block are linked through pointers.

Even with those efficiencies it is still necessary to consume space to preserve a series of points in time. Therefore, considerations for the amount of space consumed by Safeguarded Copies factor in the following items:

- ***Policy parameters of frequency and retention***: Copies-per-data times retention-in-days gives the total number of FlashCopies
- ***Change rate of data***: This can be estimated by reviewing the write-activity of the volume. The most accurate estimation of the change rate is to create a FlashCopy and then keep it for a reasonable period to capture sudden increases, like monthly batch jobs or database loads. Then, divide the size of the FlashCopy by the number of days it was kept to get the average daily change rate.

The above calculation provides a general idea of space consumption under normal conditions. It is a fairly straightforward calculation of `(A ÷ B) x C`, where:

- A = number of FlashCopies per day
- B = average daily change rate
- C = retention in number of days

However, a more accurate capacity-planning picture also accounts for the impacts of an actual ransomware attack by factoring in:

- ***Loss of compression***: The most popular form of ransomware attack encrypts the data with a key for which the victim must pay to unlock their data. Since encrypted data (done at the Operating System through a nefarious application instead of at the storage level) defeats compression, a comprehensive capacity plan accounts for this increase in capacity.
- ***Recovery Volume Space:*** It is highly recommended, if not required, that an implementation of Safeguarded Copy include a periodic recovery validation. The recovery volumes are full-copy clones of the original volumes from the point-in-time of the chosen backup.

  It is unlikely that all protected volumes will need to be recovered at the same time. Therefore, IBM strongly recommends that all production volumes be periodically validated. However, a sub-section of all protected volumes can be validated as a minimum starting point.

  Volumes can be validated by using various tools as outlined in the Cyber Vault blueprint at:

  `https://www.ibm.com/downloads/cas/ODKXBLR9`

While the calculation is fairly straightforward, it is recommended that the resources discussed in section 2.2, “IBM resources” on page 15 be considered, especially to assist with capacity planning.

2.1.6 Security and access control

A key element of protection from external and internal threats is isolation of capabilities to limit the ability for either a hacker or disgruntled storage administrator to destroy data.

In addressing this requirement, the Spectrum Virtualize Safeguarded Copy implementation is designed so that there is a division of capabilities and the truly destructive functions are allowed only by the *superuser* account. This account can be disabled on the Spectrum Virtualize device. The *superuser* account can be enabled only through a *Security Admin* level

account or, in highly sensitive environments, require IBM support to re-enable the *superuser* account. For details on the procedure of disabling the superuser account, see Chapter 3, “Safeguarded Copy implementation and management” on page 17

Normal Administrator

A normal Administrator level account can complete the following tasks:

- Create and delete empty volume groups.
- Create and delete unattached Safeguarded policies.
- Assign volumes to a volume group.
- Attach a Safeguarded policy to a volume group.
- Remove a policy or change policy for a volume group. This does not affect retention of existing Safeguarded copies.

Normal Administrator used by IBM Copy Services Manager

A normal Administrator level account is also used by IBM Copy Services Manager to complete the following tasks:

- Periodically poll Spectrum Virtualize for changes to volume groups and policies.
- Create Safeguarded Copy backups (create FlashCopy consistency groups, maps, and start maps).
- Perform recoveries (create new volumes, create FlashCopy consistency groups, maps and start maps, map volumes).
- Perform restorations (activate reverse maps to copy data from a Safeguarded Copy backup to the original source volumes).
- Manage remote copy replication.

Security Administrator

A Security Administrator level user is needed to complete the following tasks:

- Disable and enable the superuser account.
- Delete Safeguarded Copy backups before the end of their retention period.

2.1.7 Monitoring

Related to security and access control is the cornerstone of environment monitoring to detect anomalous behavior that requires remediation. This behavior might be nefarious activity or might be misconfiguration or unforeseen consequences of normal processes. Well-designed monitoring and auditing also helps to offset more restrictive measures that might otherwise render an environment unmanageable.

An example is storage administrator’s ability to change the Safeguarded policy for a volume group. Legitimate reasons for this exist, such as a status change for an application and its associated volumes. However, these reasons should be well-documented and verified in a change-control process. To protect against an unauthorized or accidental change in frequency or retention of Safeguarded copies, you should use a monitoring and reconciliation process to detect when the level of protection of a set of volumes that are associated with an application deviates from the expected policy.

2.1.8 Network

As with any solution that involves multiple components, network communication between components is always a consideration, particularly about a security-oriented application. Sufficient access must exist between the various control planes and the components that are controlled. In this case most of the control is being performed by IBM Copy Services Manager, which might be controlling multiple Spectrum Virtualize systems. There could also be remote replication involved that is also controlled by IBM Copy Services Manager, which adds to the network access complexity.

Another consideration regarding networking is potential attack vectors. Therefore, it is a great benefit in the case of implementing Safeguarded Copy to isolate, to the greatest extent possible and practical, the storage (and compute) management networks from normal data traffic.

2.1.9 Architectural limitations

The information in this section from the published configuration limits for Spectrum Virtualize 8.4.2 (https://www.ibm.com/support/pages/node/6463481). The relevant architectural limits in Spectrum Virtualize for Safeguarded Copy are highlighted in Table 2-1:

Table 2-1 Architectural limitations

Item	Limit
Safeguarded volume groups per system	256
FlashCopy mappings per graph (backups per source)	256
Safeguarded volumes per volume group	512
Safeguarded policies per system	32 (3 predefined and 29 custom)
Basic Volumes (VDisks) per system	15,864
FlashCopy consistency groups per system	500

The following restrictions apply for Safeguarded Copy:

- Mirrored volumes cannot be safeguarded. Stretched cluster is not supported.
- Mirroring of existing Safeguarded source volumes is supported for migration purposes only.
- HyperSwap volumes are supported. However, recovery requires that they be converted to regular volumes before use.
- Predefined schedules are designed to avoid running out of FlashCopy maps in a single graph and keep within the supported volumes count. It is possible to create policies (using the command line interface (CLI) only) that can potentially breach those limits. Therefore, be careful when you create these policies.
- The graphical user interface (GUI) does not support creating user-defined policies but displays user-defined policies that are created using the CLI.
- The source volume cannot be in an ownership group.
- The source volume cannot be used with Transparent Cloud Tiering (TCT).

Another FlashCopy based consideration is the 2GB bitmap memory per I/O group (FlashSystem enclosure). The formula for bitmap consumption is:

```
For every 2TB of source volume virtual capacity, 1MB FlashCopy bitmap memory is
consumed. For example, a FlashCopy mapping for a 20TB volume (even if it is thin
provisioned and compressed and only consumes 2GB of actual capacity) will consume
10MB of bitmap memory for EVERY FlashCopy map for which this 20TB volume is the
source. So, if there are one hundred FlashCopies of this volume, that amounts to
1GB, or half the bitmap memory available to the I/O group.
```

2.2 IBM resources

Programs, tools, and consultants exist that are specifically designed to assist with the planning to increase the success of deploying Spectrum Virtualize Safeguarded Copy. Contact your IBM sales team or business partner to use the specific appropriate resources.

The following items are discussed in this section:

- “Cyber Resiliency Assessment Tool” on page 15
- “Cyber Vault Storage Assessment” on page 15
- “IBM Storage Modeller” on page 16

2.2.1 Cyber Resiliency Assessment Tool

Quoting from the *Assess your risk and architect steps to protect your business* online brochure:

“Based on the NIST Security Framework, the Storage Cyber Resiliency Assessment Tool (CRAT) provides a bridge mechanism to evaluate the current data protection state of your organization, identify gaps, strengths, weaknesses, and provides recommendations to build an effective cyber resiliency plan.”[1]

For additional details and contact information, see:
https://www.ibm.com/downloads/cas/W7VJLDPE

2.2.2 Cyber Vault Storage Assessment

Cyber Vault Storage Assessment (CVSA) is similar to the CRAT, but more customized to each client. CVSA is designed and delivered by Lab Services consultants who are trained in delivering *Storage Infrastructure Optimization* assessments.

This workshop approach organically gathers requirements, assessments existing processes and identifies integration points, and an implementation roadmap. This approach utilizes the Storage Modeller tool to balance business objects for frequency and retention with the amount of storage capacity that is needed to meet those objectives.

For additional details and contact information, see the IBM Lab Services page:
(https://www.ibm.com/it-infrastructure/services/lab-services)

[1] https://www.ibm.com/downloads/cas/W7VJLDPE

2.2.3 IBM Storage Modeller

Capacity Magic and *Disk Magic* from IntelliMagic was developed as a replacement for the storage pre-sales tools. *Storage Modeller* was updated to provide capacity estimation for the inclusion of Safeguarded Copy in a storage solution. It factors in the capacity planning considerations discussed in section “Capacity” on page 11. This tool is available only to IBM staff and business partners. Contact your IBM storage sales representative or business partner to arrange access to this tool directly or through the CVSA, which is led by IBM Lab Services.

3

Safeguarded Copy implementation and management

This chapter provides information about how to implement a Safeguarded Copy environment by using the IBM FlashSystem Storage Management graphical user interface (GUI) or FlashSystem command line interface (CLI), and how to manage Safeguarded Copy with IBM Copy Services Manager.

The following topics are also described:

- The Storage Management GUI options
- The FlashSystem CLI commands that are required to configure Safeguarded Copy
- A demonstration of creating a Safeguarded Copy session by using IBM Copy Services Manager

The second part of the chapter describes the management of a Safeguarded Copy environment with an IBM Copy Services Manager Safeguarded Copy session. This includes ongoing operations, such as expiring backups, recovering a backup, or expanding Safeguarded Virtual Capacity.

Important: The detailed configuration steps covered in this chapter apply to the first (pre volume group snapshot) version of Safeguarded Copy (Safeguarded Copy V1, code levels 8.4.2 through 8.5.1). For code 8.5.2 onwards, Safeguarded volume group snapshots are configured at the volume group level and do not need a dedicated child pool.

You can refer to IBM Redpaper *Data Resiliency Designs: A Deep Dive into IBM Storage Safeguarded Snapshots*, REDP-5737 for more information.

This chapter includes the following topics:

- 3.4, “Safeguarded backup policy” on page 24
- 3.5, “IBM Copy Services Manager” on page 27

3.1 Implementing a Safeguarded Copy environment

Before you begin to configure a Safeguarded Copy environment, it is important that you completed the planning phase, which includes the following tasks:

- Sizing the Safeguarded Copy Backup capacity
- Verifying the prerequisites
- Deciding which topology to implement
- Defining the backup frequency
- Specifying the retention period

For more information about planning, see Chapter 1, “Spectrum Virtualize Safeguarded Copy introduction and concepts” on page 1.

The Safeguarded Copy configuration consists of a two-step approach:

1. You configure the Safeguarded Copy Backup Capacity for all of the relevant volumes by using the Storage Management GUI or the FlashSystem CLI.
2. You configure a Safeguarded Copy Session with IBM Copy Services Manager, which allows you to manage the Safeguarded Copy environment.

Figure 3-1 shows the configuration that we use as an example to set up a Safeguarded Copy environment.

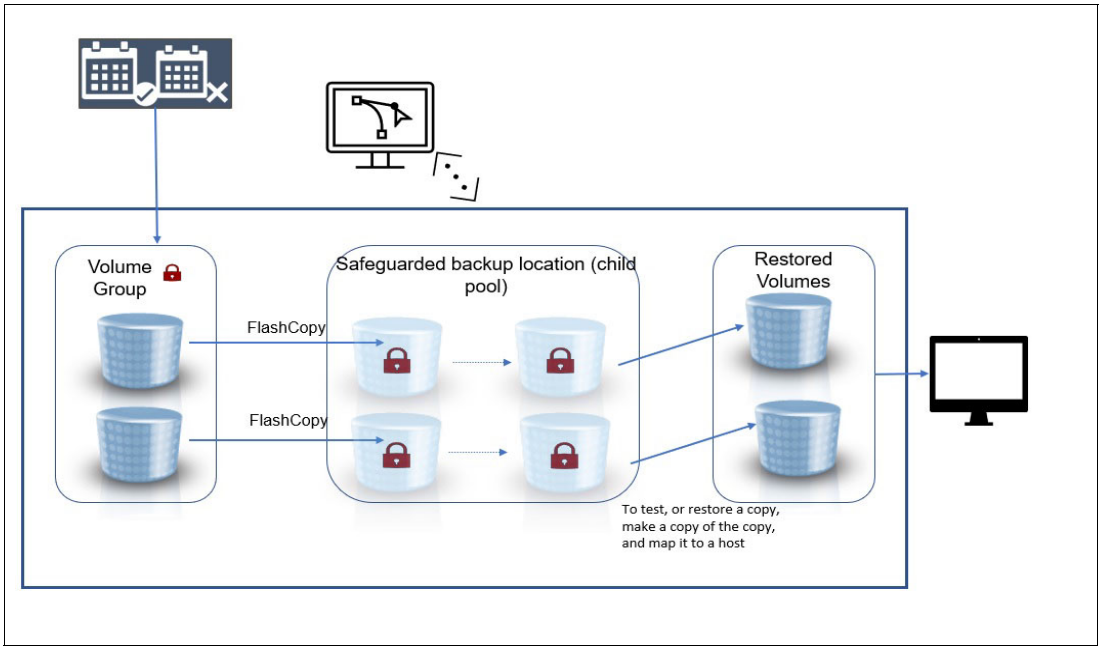


Figure 3-1 Safeguarded Copy environment

The Safeguarded Copy environment requires a set of Safeguarded Copy source volumes and an equal number of recovery volumes. The recovery volumes are necessary to recover data from a Safeguarded Copy backup. For more information about this requirement, see Chapter 2, “Safeguarded Copy planning considerations” on page 9.

Note: The following terms are used in the examples in this document:

- *Source volume* refers to the volume where the Safeguarded Copy relationship is defined. This volume can a Metro Mirror or Global Mirror Secondary.
- P*roduction volume* refers to the volume that is active to the host.

3.2 Configuring the Safeguarded Copy Backup capacity

A Safeguarded backup location is a child-pool of a parent-pool. A parent-pool cannot be designated as Safeguarded. A *regular* child-pool must be designated as *safeguarded* on creation and this designation cannot be changed.

The properties and restriction of the Safeguarded pool are as follows:

- A maximum of one Safeguarded backup location (child-pool) per parent-pool.
- A Safeguarded backup location (child-pool) cannot be deleted if:
  - The Safeguarded backup location (child-pool) contains all Safeguarded backups (except by the Security Admin).
  - The Safeguarded backup location (child-pool) is associated to a Safeguarded source. This restriction also applies to the Security Admin.
- A Safeguarded backup location can have its quota increased but not reduced (except by the Security Admin). Quotaless data reduction pool (DRP) child-pools are supported as a Safeguarded backup location.

3.2.1 Configuring a Safeguarded backup location (pool)

A Safeguarded backup location is a *child-pool.* The new **-safeguarded** parameter is added to the **mkmdiskgrp** command. Therefore, this parameter will be allowed only for child-pools, and also requires the -**parentmdiskgrp** parameter to be set.

A Safeguarded Copy backup location can be created by using both the CLI and the GUI, as follows:

- Using the CLI:

```
mkdiskgrp -parentmdiskgrp safeguarded_backup_pool -size 100 - unit gb -safeguarded
```

- Using the GUI:

1. In the management GUI, select **Pools** → **Pools**. Right-click a parent-pool and select **Create Child Pool**. On the Create Child Pool page, enter a name of the child pool.
2. If the parent pool is a standard pool, enter the amount of capacity that is dedicated to the child pool. If the parent pool is a DRP, the child pool shares capacity with the parent pool. See Figure 3-2.

.

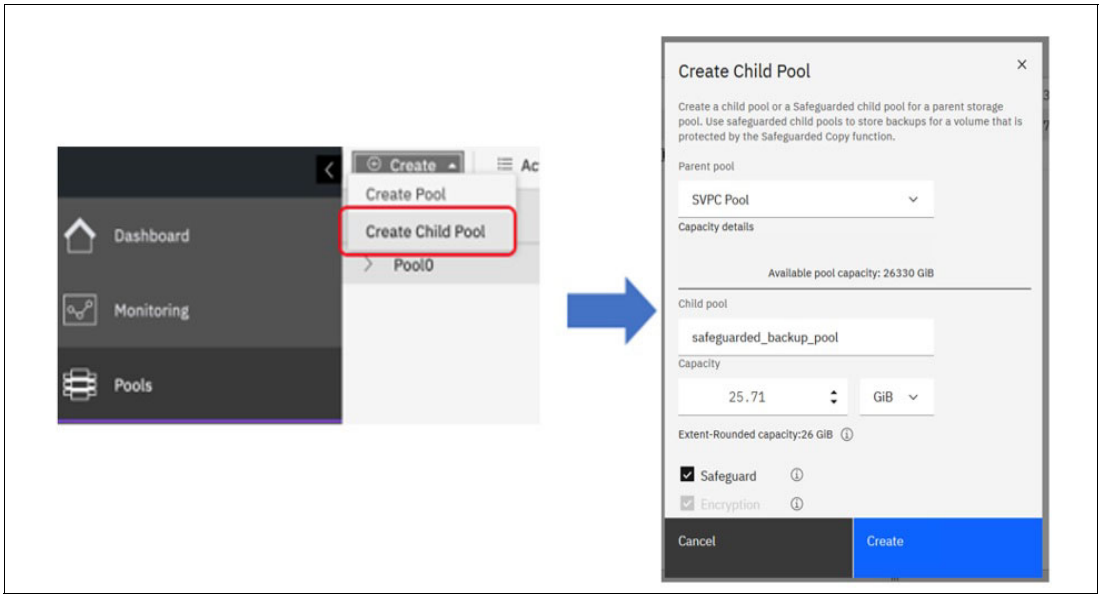


Figure 3-2 Create child pool

3. Select **Safeguard** to indicate that the child pool is used as the Safeguarded backup location for immutable backup copies of source volumes.
4. Click **Create**. Child pools that are used as Safeguarded backup locations are marked with a shield icon on the Pools page as shown in Figure 3-3.

   In this example, `safeguarded_backup_pool` is configured in the parent “SVPC Pool”, as shown in Figure 3-3.

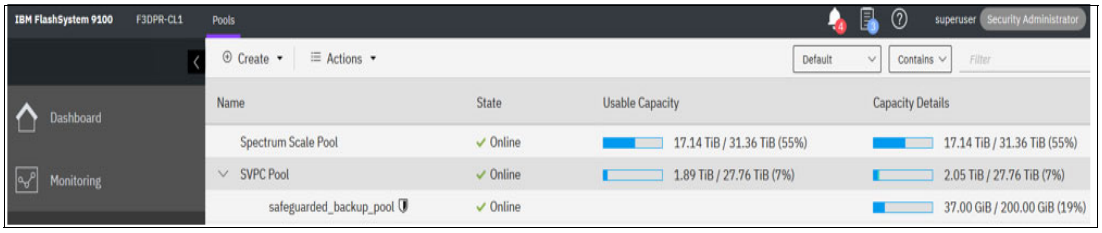


Figure 3-3 safeguarded_backup_pool

A Safeguarded pool can be created through the CLI, by using the following command:

```
mkmdiskgrp -parentmdiskgrp SVPC Pool -size 100 -unit gb -safeguarded
```

3.3 Setting up volume groups and a Safeguarded policy

Volume groups are the way Safeguarded Copy manages a group of related volumes. A *volume group* is a set of related volumes that can be managed and configured collectively. Volume groups manage source volumes (referred to as Safeguarded source) that are configured as part of the Safeguarded Copy function.

Not all volumes in a Safeguarded volume group must belong to the same parent pool. However, all volumes in the Safeguarded volume group must have a Safeguarded backup location. This condition must also be met when a volume is added to a Safeguarded volume group. Otherwise, adding the volume will fail.

Additional restrictions exist for to specify which volumes can be Safeguarded source volumes. If these restrictions are not met, a volume group might be prevented from becoming Safeguarded or a volume might be prevented from being added to a Safeguarded volume group.

A vdisk volume can be designated as *Safeguarded source volume* only if its volume group is associated with a Safeguarded policy. A Safeguarded source is automatically associated with a Safeguarded backup location, which is a child pool in the Safeguarded source's parent pool. For a mirrored Safeguarded source, each volume copy is associated with a Safeguarded backup location.

Safeguarded-source volumes include the following limitations:

- Cannot be in a Safeguarded backup location
- Cannot be mirrored volumes
- Cannot be in an ownership group
- Cannot be a change volume that is used in either HyperSwap or Global Mirror relationships
- Cannot be used as cloud backups with the transparent cloud-tiering function

3.3.1 Volume group creation

Volume groups create a set of source volumes that can span different pools and are copied collectively to a Safeguarded backup location by using the Safeguarded Copy policies. Before you create a volume group, determine of which source volumes you want to create Safeguarded backup copies.

A volume group becomes *Safeguarded* when it is associated with a Safeguarded policy.

The volume group object itself does not guarantee that consistent FlashCopy operations will be performed. The Spectrum Virtualize Administrator user, or more commonly External Copy Management software, must create FlashCopy consistency groups and operate on the mappings such that they are backed up consistently.

Note that a volume group can be considered Safeguarded, but not have any volumes in it nor any Safeguarded backups created yet.

Creating a volume group using the GUI

To create a volume group using the GUI, complete the following steps:

1. In the management GUI, select **Volumes** → **Volumes Groups**.
2. Click **Create Volume Group**.
3. On the Create Volume Group page, enter a name for the volume group.
4. From the list of volumes, select of the volumes that you want in the volume group.

> **Note:** If you select volumes in a parent pool that do not contain a child pool to use as the Safeguarded backup location, select **Navigate to Pools**. For each parent pool with source volumes, you must configure a child pool as the Safeguarded backup location.

5. Click **Create Volume Group**.

The volume group is created with the name `safeguarded_demo`, as shown in Figure 3-4 on page 23.

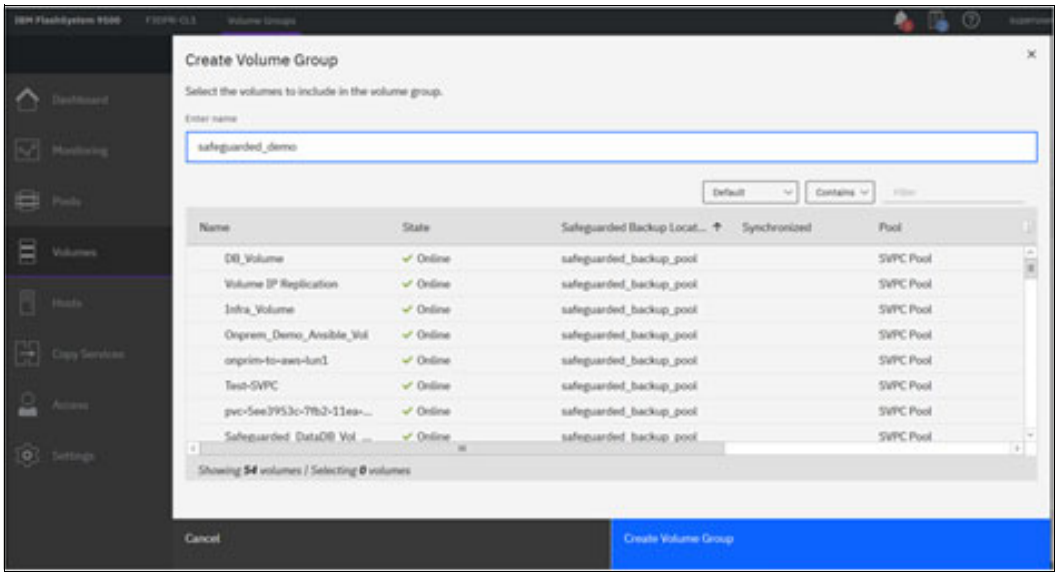


Figure 3-4 Creating volume group and adding volume to the group

After the volume group is created, you can add source volumes to the same volume group. In this example, two source volumes are added to the volume group, which are presented to the Windows production server, as shown in Figure 3-5.

- `Safeguarded_DataDB_vol`, which includes SQL database data tables
- `Safeguarded_LogDB_vol`, which includes the database log files

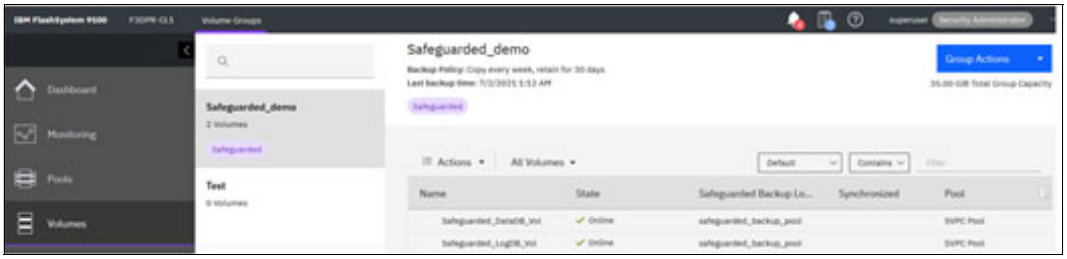


Figure 3-5 Volume addition to the volume group

Creating a volume group using the CLI

To create and configure a new volume group and assign volumes to that group, complete these steps:

1. To create the new volume group, enter the following command:

   ```
   mkvolumegroup -name volumegroup_name -safeguardedpolicy safeguarded_policy_id | safeguarded_policy_name
   ```

   where:

   - `volumegroup_name` specifies a volume group name
   - `safeguarded_policy_id | safeguarded_policy_name` specifies the ID or name of one of the predefined policies, 0, 1 or 2

This command creates the volume group and assigns the policy to the volume group.

2. Create new volumes or change existing volumes and assign them to the volume group that you created in Step 1.

If you are assigning a new volume to the volume group, enter the following command:

`mkvolume -pool <pool_name_or_id> -volumegroup <volumegroup_name_or_id> -size <disk_size>`

where:

- `<pool_name_or_id>` is the name or identifier of the parent pool that contains the Safeguarded backup location
- `<volumegroup_name_or_id>` is the name or identifier of the volume group
- `<disk_size>` indicates the capacity that is provisioned for the volume from the parent pool

3. If you are assigning existing volumes to the volume group, enter the following command:

   `chvdisk -volumegroup <volumegroup_name_or_id> <name_or_id>,`

   where:

   - `<volumegroup_name_or_id>` is the name or identifier of the volume group
   - `<name_or_id>` of the volume

3.4 Safeguarded backup policy

A Safeguarded backup policy controls the creation, retention, and expiration of Safeguarded backup copies of source volumes. The management GUI supports the display of predefined and user-defined Safeguarded backup policies.

IBM Copy Services Manager uses a Safeguarded policy to automatically configure FlashCopy mapping and consistency groups to create backup copies. When Safeguarded backups are created, IBM Copy Services Manager uses the retention time for the Safeguarded backups based on the settings in the Safeguarded policy. After copies expire, the IBM Spectrum Virtualize software deletes the expired copies from the Safeguarded backup location.

As of this writing, the management GUI does not support the creation of user-defined Safeguarded backup policies. However, you can use the CLI **`mksafeguardedpolicy`** command to create user-defined policies. The system contains three predefined policies, as shown in Figure 3-6 on page 25.

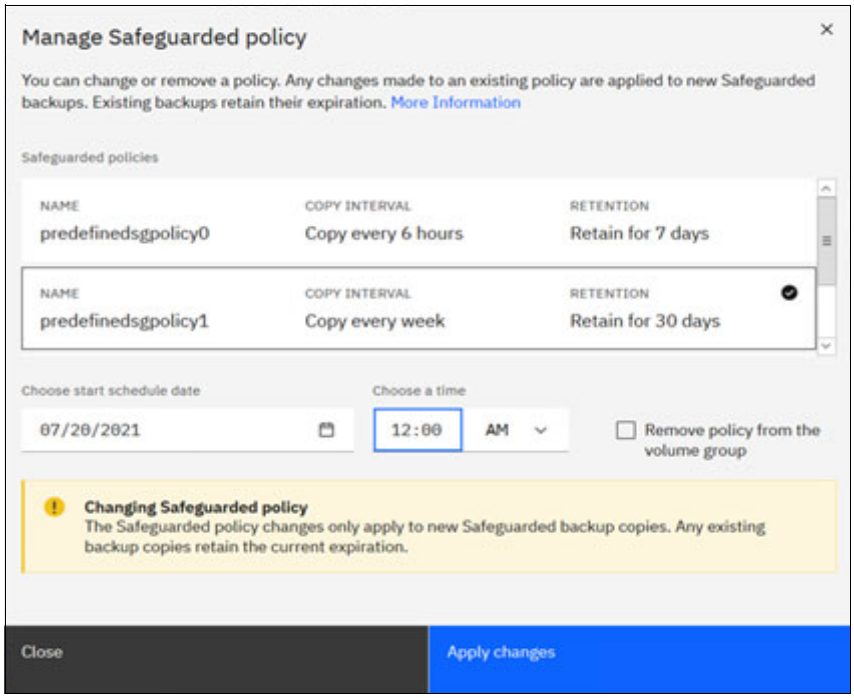


Figure 3-6 Predefined backup policies

3.4.1 To assign Safeguarded policy to a volume group using the GUI

To assign a Safeguarded backup policy to a volume group, complete the following steps:

1. In the management GUI, select **Volumes** → **Volumes Groups**.
2. Select the volume group to which you want to assign a predefined policy and select **Group Actions** → **Assign Safeguarded policy**.
3. Select one of the following predefined Safeguarded policies:
   - **Predefinedsgpolicy0**

     Select this policy for the most frequent copies and retention. For this policy, Safeguarded backup copies are created daily and retained for a week. Use this policy for volume data that requires the highest recovery point objective (RPO). For example, volume data that is frequently updated and critical to your business can benefit from frequent copies and retention. Customer accounts, orders, or proprietary information are examples of data that might need more frequent backups. For more information, refer to your organization's business continuity plan.
   - **Predefinedsgpolicy1**

     Select this policy for less frequent copies and medium retention. For this policy, Safeguarded backups are created weekly and retained for a month. Use this policy for application data that is updated frequently and requires a high RPO, but might not contain business-critical data.
   - **Predefinedsgpolicy2**

     Select this policy for less frequent copies and longer retention. For this policy, Safeguarded backup copies are created monthly and retained for a year. Use this policy for older data that is not updated frequently but still requires retention, such past customer accounts or employee records.

In this example, `predefinedsgpolicy1` is selected. See Figure 3-6.

For the selected policy, Safeguarded backup copies are created weekly and retained for a month.

> **Note:** These predefined policies cannot be changed or deleted. However, you can use the CLI **`mksafeguardedpolicy`** command to create user-defined Safeguarded backup policies. For user-defined policies, the policy IDs start after the first three predefined policy IDs. The system supports a maximum of 32 Safeguarded backup policies with three predefined policies and 29 user-defined policies. If you create user-defined Safeguarded backup policies in the CLI, you can view and select these policies within the management GUI.

At this time, neither interface supports changes to the factory predefined Safeguarded backup policies.

4. Select a date and time when you want IBM Copy Services Manager to start creating Safeguarded backups that use the policy. IBM Copy Services Manager queries the system every five minutes to process existing Safeguarded policies. The start time that is defined in the Safeguarded policy must factor in the possible five-minute delay.

   When IBM Copy Services Manager detects a new Safeguarded policy for a volume group, it creates the session and scheduled task to create and manage the Safeguarded backups. IBM Copy Services Manager starts Safeguarded backup copies based on the start time and the copy interval that is defined in the Safeguarded backup policy. If the start time occurs before IBM Copy Services Manager detects the policy, the Safeguarded backup is initiated based on the copy interval set in the Safeguarded policy and not at the start time.

5. Click **Assign**.

   After the Safeguarded backup policy is assigned to the volume group, the status of the volume group displays as Safeguarded scheduled. See Figure 3-7.

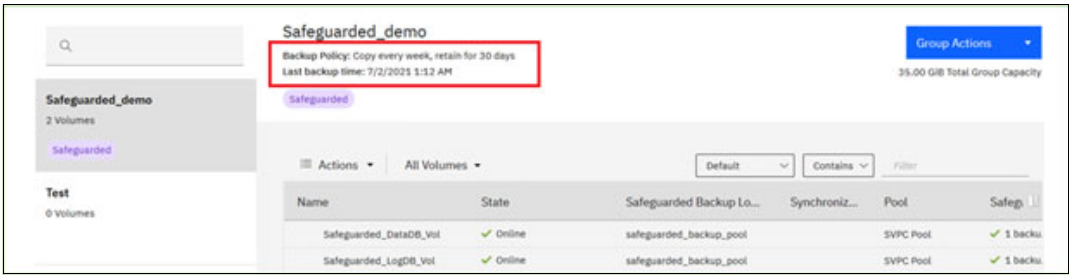


Figure 3-7 Backup policy schedule

This status indicates that the policy is assigned, but the Safeguarded backup copies are not started. When Safeguarded backup copies are stored on the Safeguarded backup location, the status of volume group displays as Safeguarded.

After Safeguarded backup copies are added to the Safeguarded backup location, users with the Administrator role or lower cannot delete a parent pool with a Safeguarded backup location.

3.4.2 To assign Safeguarded policy to a volume group using the CLI

To assign a Safeguarded policy to a volume group, complete these steps:

1. To create a new Safeguarded policy that can later be associated with volume groups, enter the following command.

```
mksafeguardedpolicy -name
safeguarded_policy_name -backupunit minute | hour | day | week | month
-backupinterval interval_value -backupstarttime start_time -retentiondays
num_days
```

where:

- The `safeguarded_policy_name` indicates the name for the Safeguarded backup policy and it is optional.
- The `minute | hour | day | week | month` specifies the unit of time of the backup interval.
- The `interval_value` indicates the unit of time of `backup_interval`.
- The `start_time` indicates the time when the Safeguarded backups are started.
- The `num_days` indicates the number of days to keep the Safeguarded backups.

2. To change the volume group properties and assigns a Safeguarded policy to the volume group, enter the following command.

```
chvolumegroup -safeguardedpolicy xxxx
```

3.5 IBM Copy Services Manager

You can configure the Safeguarded Copy function by using the management GUI or the CLI. The Safeguarded Copy function supports the ability to create cyber-resilient point-in-time copies of volumes that cannot be changed or deleted through user errors, malicious actions, or ransomware attacks. The system integrates with IBM Copy Services Manager to provide automated backup copies and data recovery.

Before you configure the Safeguarded Copy function on your system, ensure that you meet the prerequisites as described in “IBM Copy Services Manager requirements” on page 27.

3.5.1 IBM Copy Services Manager requirements

Ensure that the following requirements are met for IBM Copy Services Manager:

- If you do not have an existing IBM Copy Services Manager license, purchase the IBM Copy Services Manager for IBM Spectrum Virtualize license, which includes IBM Copy Services Manager version 6.3.0.1. This license option is available through iERP/AAS, Passport Advantage®, or your IBM Sales team.
- If you currently have an existing license for IBM Copy Services Manager, download IBM Copy Services Manager version 6.3.0.1 at: https://www.ibm.com/support/pages/latest-downloads-ibm-copy-services-manager

Note: If you are using an existing license, ensure that the licensed capacity is adequate for use of the Safeguarded Copy function. If you need more capacity for Safeguarded Copy function, contact you IBM sales representative to update your licensed capacity for IBM Copy Services Manager.

After you download IBM Copy Services Manager, complete the instructions for your installation. IBM Copy Services Manager supports several installation options on different environments. For more information, see: https://www.ibm.com/docs/en/csm/6.3.0?topic=overview-installing-copy-services-manager.

During installation, license files can be imported for IBM Copy Services Manager. If the license was not imported during the installation, you need to apply the license to the installation. For more information, see: https://www.ibm.com/docs/en/csm/6.2.11?topic=icsm-applying-license-files-after-installation-migration-updating-licenses.

IBM Copy Services Manager uses a Safeguarded policy to configure FlashCopy mapping and consistency groups automatically to create backup copies. When Safeguarded backups are created, IBM Copy Services Manager uses the retention time for the Safeguarded backups based on the settings in the Safeguarded policy. After copies expire, the IBM Spectrum Virtualize software deletes the expired copies from the Safeguarded backup location.

After the IBM Copy Services Manager is installed and before you can establish the system as a connection endpoint in IBM Copy Services Manager, you must configure a user with the Administrator role on the IBM Spectrum Virtualize system. For auditing, it is recommended that you create a new Administrator user to configure the Safeguarded Copy function. Users with this role are limited in how they can manage and interact with Safeguarded Copy operations. IBM Copy Services Manager uses this role to create FlashCopy mappings between the source volumes and the Safeguarded backups on the system.

3.5.2 Creating an Administrator user for IBM Copy Services Manager

This section describes how to create an Administrator user for IBM Copy Services Manager using both the GUI and CLI.

Using the management GUI

To create new Administrator user for IBM Copy Services Manager, complete these steps:

1. In the management GUI, select **Access** → **Users by Groups** → **Create User Group**.
2. On the Create User Group page, enter a name for the user group, and select Administrator for the role.
3. Click **Create**.
4. In the list of user groups, select the user group that you created and select **Create Users**.
5. On the Create Users page, enter the name of the user, and select **Local**. See Figure 3-8 on page 29
6. To connect to the management GUI with this user, enter and confirm a password.
7. Click **Create.**

   After you create the Administrator user, create a connection to the system in IBM Copy Services Manager, as described in step 1 on page 29 to step 10 on page 30.

.

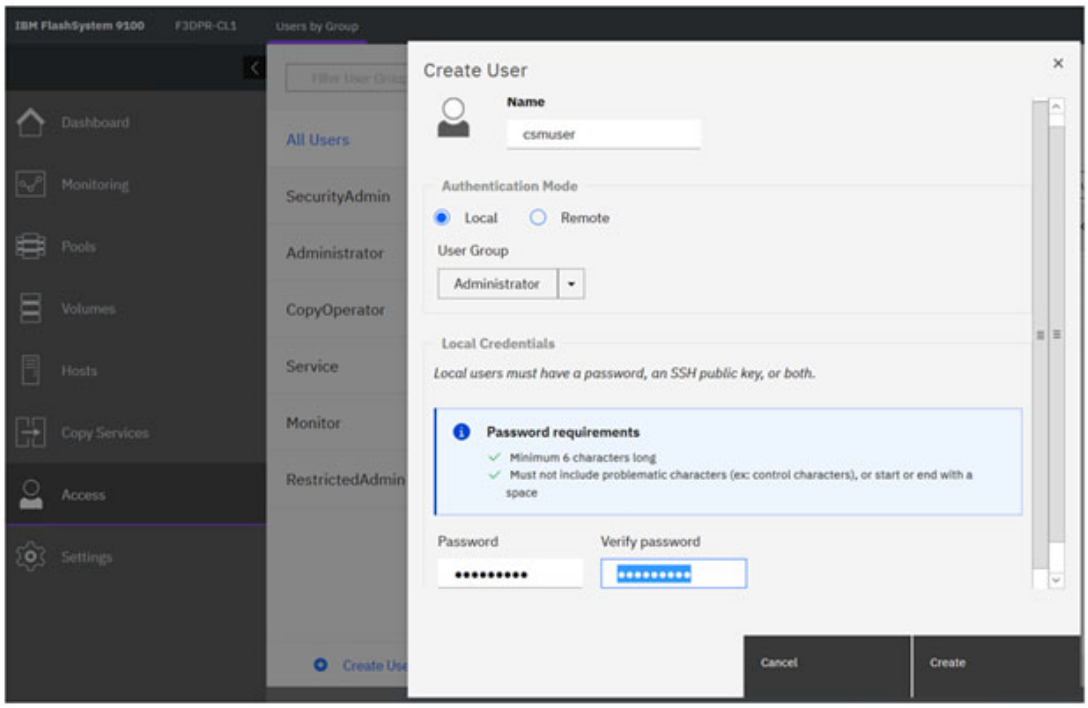


Figure 3-8 Creating an Administrator user

To create a connection to the system in IBM Copy Services Manager, complete these steps:

1. Log in to IBM Copy Services Manager at `https://<IP address or domain name>:9559/CSM` where `<IP address or domain name>` is the IP address or domain name of IBM Copy Services Manager instance in your network.
2. Select **Storage** → **Storage Systems**.
3. On the Storage Systems page, select **Add Storage Connection**.
4. Click one of the following options based on your product:
   - FlashSystem Spectrum Virtualize
   - SAN Volume Controller
   - Storwize® Family
5. On the Connections page, enter the following information for your system:
   - Cluster IP / Domain Name

     Enter the management IP address or domain name for your system.
   - Username

     Enter the username for the Administrator user for the system.
   - Password

     Enter the password that is associated with the Administrator user for the system.
6. Click **Next**.
7. Click **Finish**.
8. On the Storage Systems page, verify that Local Status for the connection is *Connected*, as shown in Figure 3-9 on page 30.

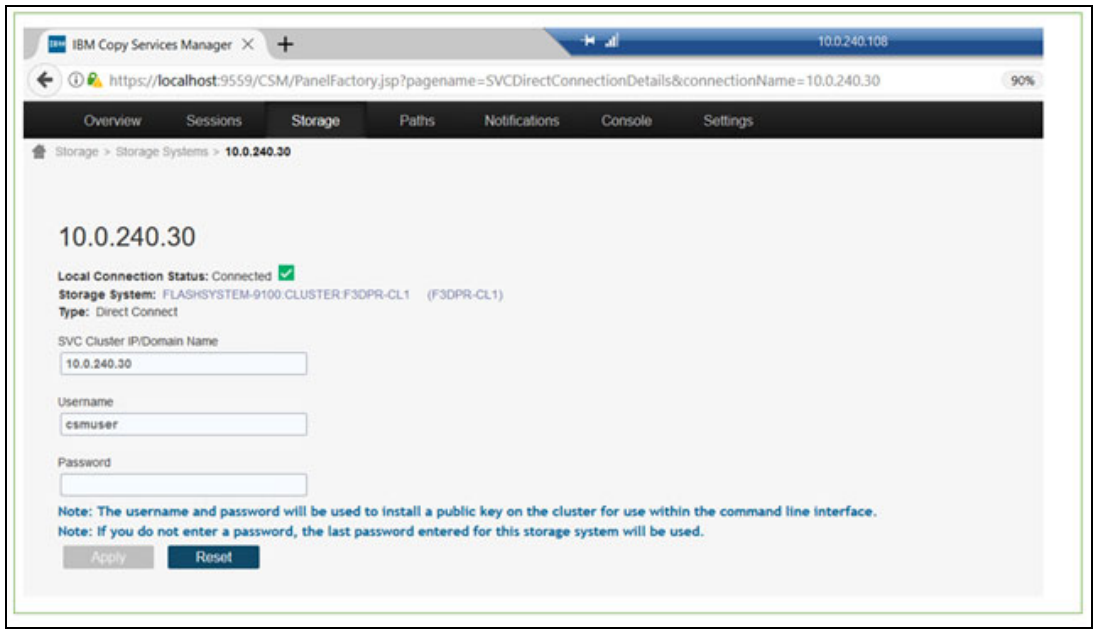


Figure 3-9 Create a connection to the system in the IBM Copy Services Manager interface

After a connection is established, IBM Copy Services Manager automatically detects volume groups with Safeguarded policies and then schedules the backup copies.

IBM Copy Services Manager queries the system every 5 minutes to process the existing Safeguarded policies. The start time that is defined in the Safeguarded policy must factor in the possible 5-minute delay. When IBM Copy Services Manager detects a new Safeguarded policy for a volume group, it creates the session and scheduled task to create and manage the Safeguarded backups.

9. To view Safeguarded backups in IBM Copy Services Manager interface, select **Sessions**.

   The session name is based on the name of the volume group.

10. To view Safeguarded backup copies in IBM Copy Services Manager interface, select **Sessions**.

    The session name is based on the name of the volume group. In our lab example, the `Safeguarded_demo` volume group that was created on IBM FlashSystem is automatically visible as a session in IBM Copy Services Manager. See Figure 3-10.

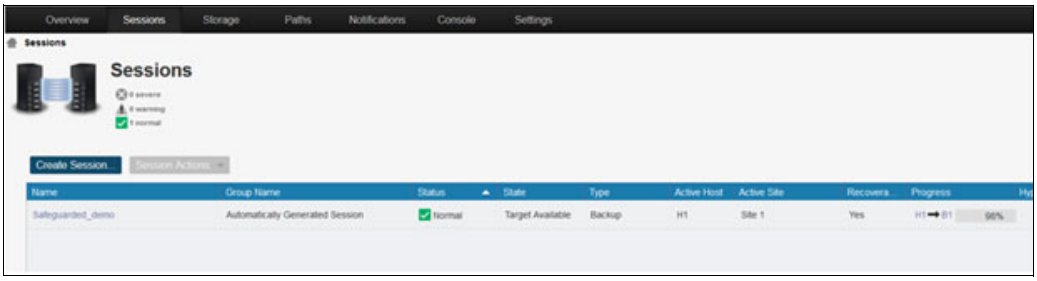


Figure 3-10 Safeguarded Copy session automatically visible in IBM Copy Services Manager

This session includes the two volumes that are part of the volume group that was defined earlier. See Figure 3-11.

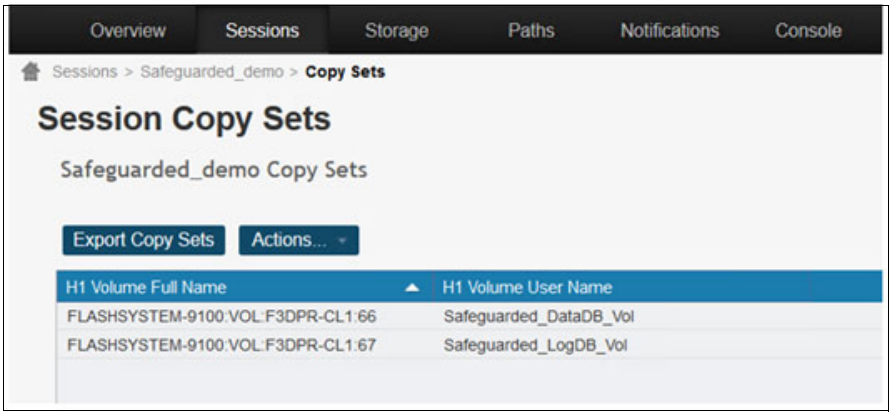


Figure 3-11 Volume information of the session

The IBM Copy Services Manager session details show more information about the Safeguarded policy that is set on the volumes for the backup and retention. See Figure 3-12.

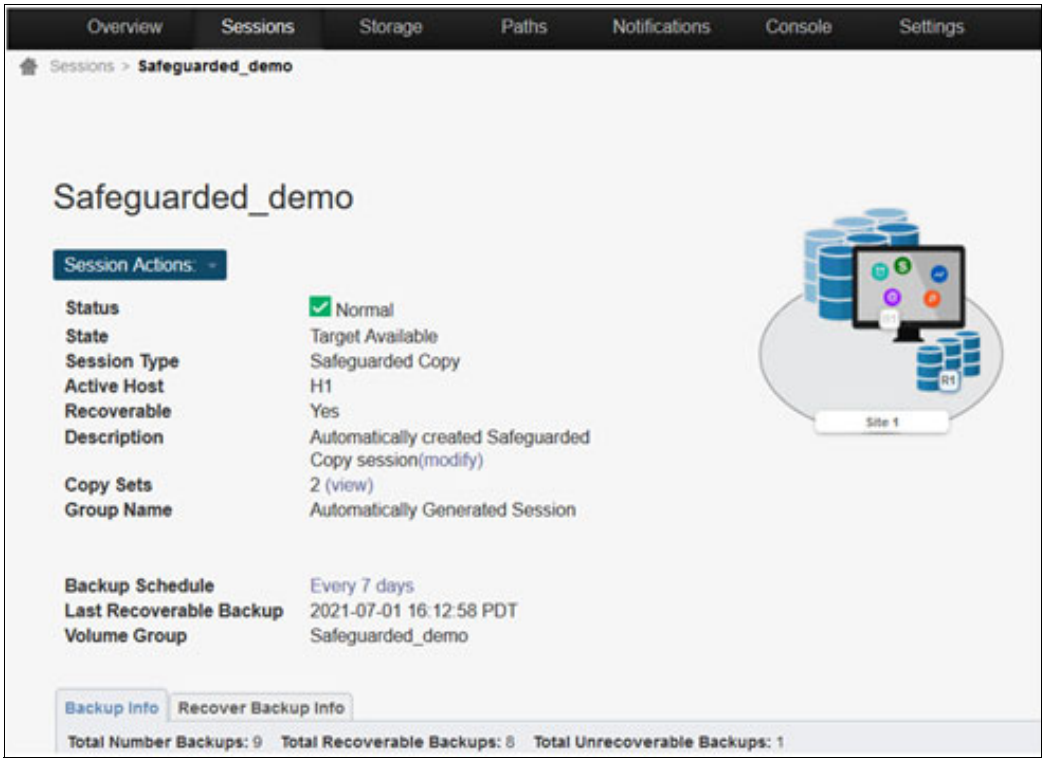


Figure 3-12 Policy information about the Safeguarded volume group

4

Recovery and restoration of Safeguarded Copies

This chapter provides information about how to recover and restore from the Safeguarded Copy environment by using the IBM FlashSystem Storage Management graphical user interface (GUI) or FlashSystem command line interface (CLI), and how do the same using with IBM Copy Services Manager.

It is critical to note that using either the recovery or the restoration features of SGC, does not change the immutable source snapshots on the original FlashSystem. Equally critical is the important difference in terminology:

- *Recovery* uses the Safeguarded Copy to make a new volume in the original FlashSystem pool. It also allows for mapping and testing through other hosts that are defined on that FlashSystem array. This is the safest way to preserve the existing volume for analysis.
- *Restore Backup to Production* immediately overwrites the current existing (live-mapped) source volume from the immutable Safeguarded Copy snapshot.

This chapter includes the following topics:

4.1 Recovery of Safeguarded volumes to a new host

Important: Ensure that you regularly test your configuration to ensure that Safeguarded backups can be recovered and restored, if necessary.

If a cyberattack occurs, a Safeguarded source volume can be compromised for an indefinite amount of time until the breach is detected. In this situation, the most recent Safeguarded backups are no longer valid and healthy for restoring data back to the production volume. A regular test of a sample of critical volumes is instrumental in rapidly identifying healthy versions of Safeguarded backups that can be used to restore the compromised data.

IBM Copy Services Manager provides automation for both recovery and testing with the *Recover Backup* action. The Recover Backup action creates recovered versions of Safeguarded backup copies that you can map to a test alternative host and verify that the applications run properly. This command is shown in the Copy Service Manager Session Details window. See Figure 4-1.

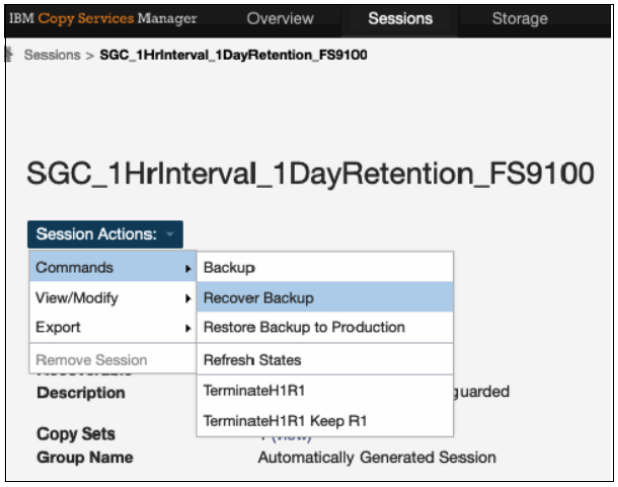


Figure 4-1 Session Actions using Recover Backup

4.1.1 Recover or test Safeguarded backup copies

This section describes the steps for the process of recovering or testing Safeguarded backup copies. These steps are detailed in “Recover or test Safeguarded backup copies” on page 35:

1. Log in to `https://<IP/host>:9559/CSM`

   where: `<IP/host>` is the IP address or hostname of the IBM Copy Services Manager instance.

2. On the Sessions Overview page, select **Sessions**.
3. On the Sessions page, select the volume group that contains the Safeguarded backup copies that you want to recover.
4. Select **Session Actions** → **Command** → **Recover Backup**.
5. Select which generation of the backup that you want to recover.

When the recovery is complete, the new volumes are created in the parent pool where the source volume is a member. These newly-recovered volumes can now be mapped to a host to check for data integrity and consistency.

6. Use the Recovered Backup page to verify the original source volume (H1 column) and the recovered volume (R1 column) and the currently mapped hosts.

   Each recovery volume is named with the original source volume name and appended with the timestamp of when the backup was created. You can use the management GUI on the system to view and filter these recovery volumes.

   In the management GUI, select **Volumes** → **Volumes** and filter the volume list on the timestamp to show all the recovery volumes.

7. To test the recovered version (R1 volume) of the Safeguarded backup, assign the recovered volume to an alternative host or host cluster that you use for testing.
8. Select **Assign R1 to host**.
9. On the Map volume to host page, select the host or host cluster to assign to the recovered version of the Safeguarded backup. Click **Yes**.
10. Validate that host application runs as expected to the recovered Safeguarded backup.
11. After you complete testing, continue as follows:
    - To delete the recovery relationship and recovery volume, select **Session Actions** → **Command** → **Terminate H1R1**.
    - To delete the relationship between the source volume (H1) and recovered volume, but keep the recovered volume (R1), select **Terminate H1 Keep R1**.

4.1.2 Recover or test Safeguarded backup copies

To recover or test Safeguarded backup copies, complete these steps:

1. Log in to `https://<IP/host>:9559/CSM`

   where: `IP/host` is the IP address or hostname of the IBM Copy Services Manager instance.

   Ensure that your role is admin or higher to perform these actions. See Figure 4-2.

Figure 4-2 Copy Services Manager main screen

2. From the top menu bar on the Overview page, select **Sessions**. See Figure 4-3.

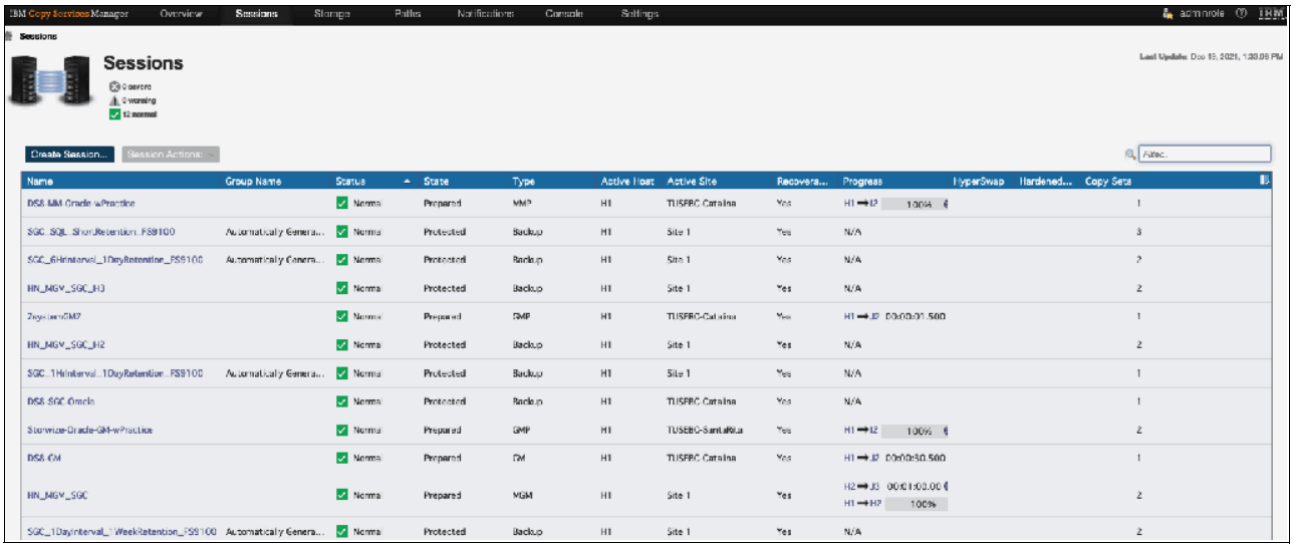


Figure 4-3 Sessions page of IBM Copy Service Manager

3.From the Sessions overview page, select the volume group that contains the Safeguarded backup copies that you want to recover. See Figure 4.

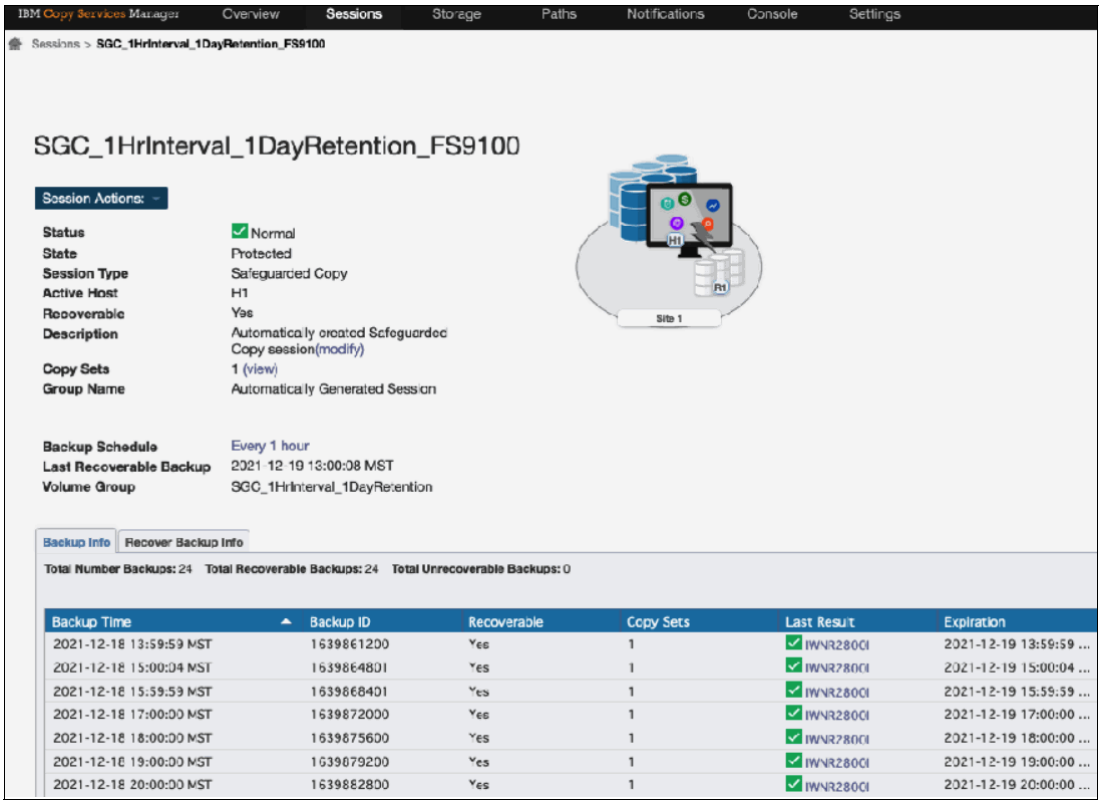


Figure 4 Volume group to recover

4.Select **Session Actions** → **Commands** → **Recover Backup**.

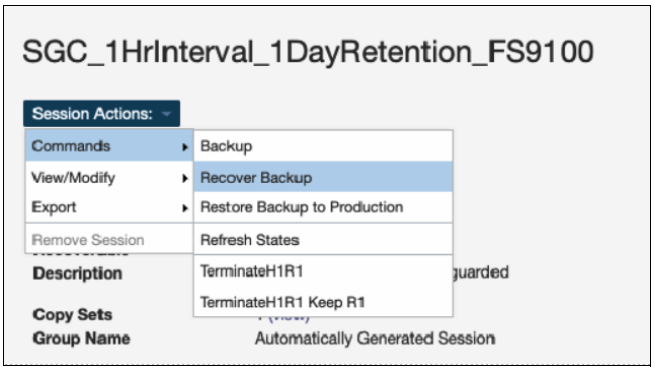


Figure 4-5 Session Actions menu: selecting Recover Backup

3. Select the generation of the backup that you want to recover. A snapshot is then recovered to a new volume; the existing volume is not overwritten. See Figure 4-6.

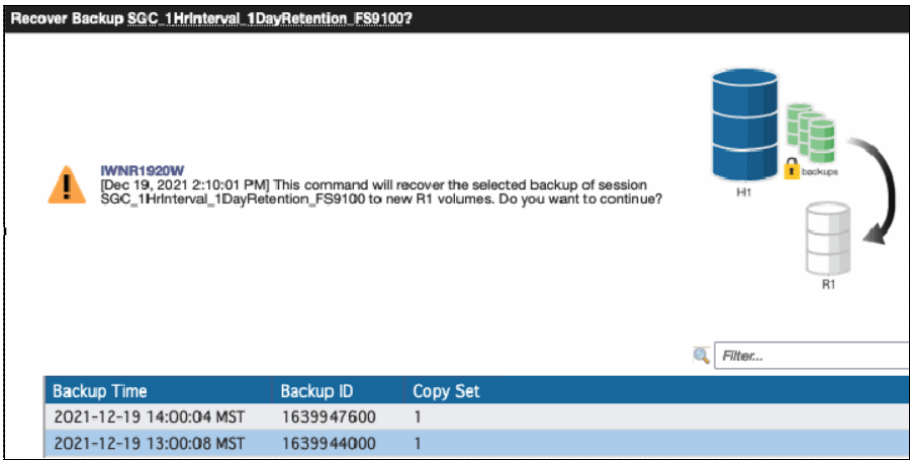


Figure 4-6 Select the specific Safeguarded snapshot to recover to a new host

When the recovery has completed, the new volumes are created in the parent pool where the source volume is a member. The newly-recovered volumes can now be mapped to a host to check for data integrity and consistency.

The steps are shown below in a series of screenshots from both IBM Copy Services Manager and the FlashSystem array.

a. In Figure 4-7, the user can see that the job has completed.

Figure 4-7 Recover Backup Volume ready for Host Mapping

b. In Figure 4-8, the user can click the **Recover Backup Info** sub-tab to see the overview of the recovery.

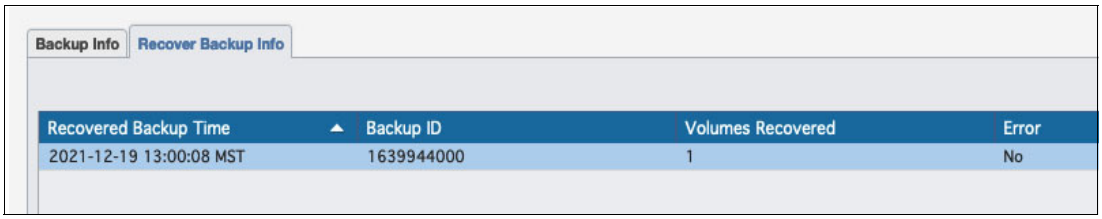


Figure 4-8 Overview of Recovery

c. For more details, the user can click the highlighted line to view more details of the Recovery including the name of the volume that is restored to the same pool as the source volume. See Figure 4-9.

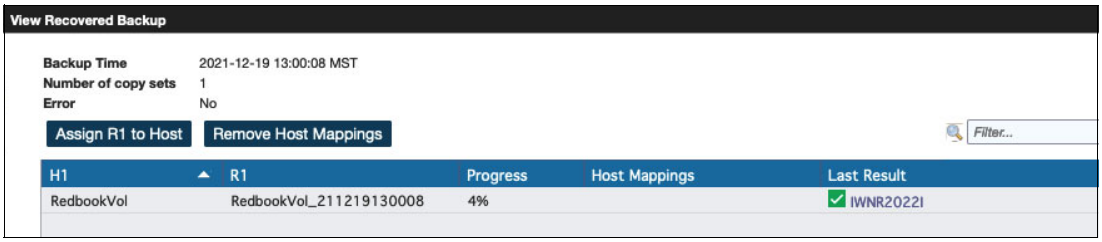


Figure 4-9 Recovery detail information confirming the restore with specific name of volume

d. As a further validation, by going to the FlashSystem the user can navigate to the pool that contains the source volume and see the newly restored volume, which matches the name from IBM Copy Services Manager. See Figure 4-10

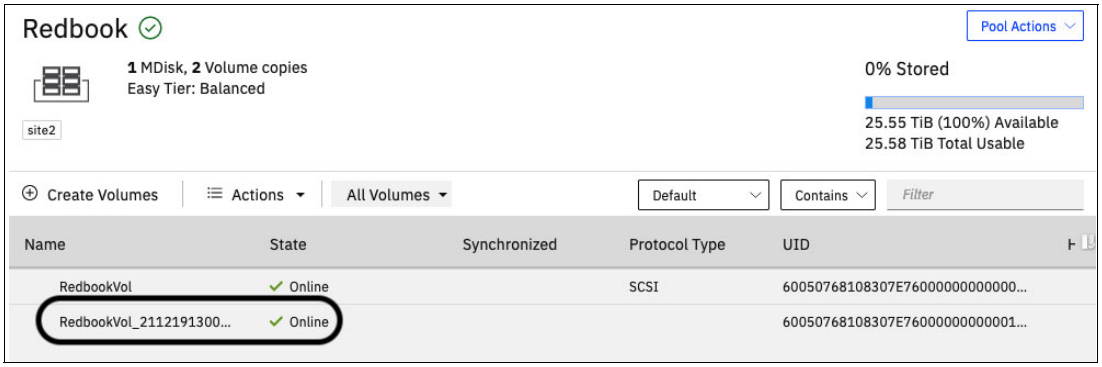


Figure 4-10 Newly created restore volume shown inside FlashArray, same pool as source

4. Using the above series of screenshots, you can verify the original source volume (H1 column) and the recovered volume (R1 column). The new recovery volume is not currently mapped to any host.

   Each recovery volume is named with the original source volume name and appended with the timestamp when the backup was created. You can use the management GUI on the system to view and filter these recovery volumes. In the management GUI, select **Volumes** → **Volumes** and filter the volume list on the timestamp to show all the recovery volumes.

5. To test the recovered version (R1 volume) of the Safeguarded backup, assign the recovered volume to an alternative host or host cluster that you use for testing.

   a. Select **Assign R1 to host**.

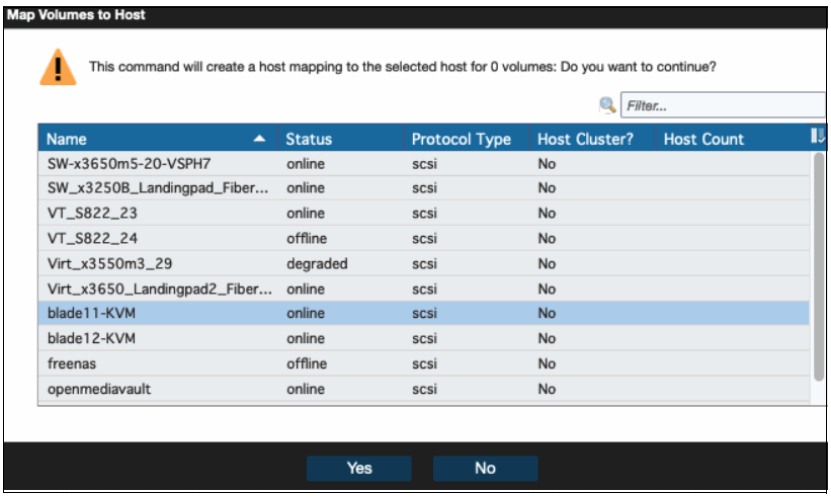


Figure 4-11 Ready to map recovered backup to a new host

6. Proceed to map the host, and validate that the application runs as expected to the recovered Safeguarded backup.
7. After you complete testing, the **`Terminate H1R1`** command can be used to delete the recovery relationship and recovery volume.

   Select **Session Actions** → **Command** → **Terminate H1R1**.
8. You can also select **`Terminate H1 Keep R1`** to delete the relationship between the source volume (H1) and recovered volume, but keep the recovered volume (R1). Figure 4-12 shows the **Session Actions** submenu.

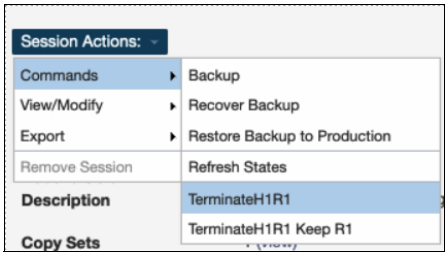


Figure 4-12 Terminate H1R1 commands to help clean up any tests

4.2 Restoring from a Safeguarded Copy: Overwrite source volume to original host

If your production data is compromised by a cyber-attack, you can restore data back to the source volumes with a Safeguarded backup copy. The IBM Copy Services Manager automates and simplifies the process of testing and restoring compromised data from a Safeguarded backup copy.

Before you can restore data to the source volume with a Safeguarded backup copy, ensure that you fully test the Safeguarded backup copies that are associated with the compromised source volume. Multiple versions of Safeguarded backup copies can exist, and some versions can include malware or damaged data. The restore operation is similar to the recovery steps described in “Recovery of Safeguarded volumes to a new host” on page 34. Both recovery

and restore use the immutable volume data from the selected version of the Safeguarded backup copy from which you are restoring.

4.2.1 Overview of the steps to restore Safeguarded backup copies to production

The following sections contain an overview of the steps that are required to restore Safeguarded backup copies to production.

4.2.2 Prerequisites for HyperSwap volumes

If the Safeguarded source volume is *also* a HyperSwap volume, you must complete prerequisite tasks before you can use IBM Copy Services Manager to restore the HyperSwap source volume. The procedures depend on which HyperSwap site the Safeguarded Copy function is configured.

A best practice is to configure Safeguarded Copy function on the master site in the HyperSwap configuration. Configuring Safeguarded Copy function on the master site of a HyperSwap configuration simplifies the restore process to the same source volumes.

Similarly, you can create Safeguarded backup on the auxiliary site and not the master site, but this use case has more considerations and steps. Use the following instructions before you restore a HyperSwap source volume:

Master site contains Safeguarded backups; auxiliary site does not

In this use case, the master site in the HyperSwap system contains the HyperSwap source volumes with Safeguarded backups. Complete these CLI steps before you restore the Safeguarded backup to the HyperSwap master volume:

1. Verify the HyperSwap volume copies on the HyperSwap system when Secure Shell (SSH) is connected into the FlashArray as admin. Enter the following command using the CLI through SSH to perform the verification:

   ```
   lsvdisk
   ```

   In the results that display, determine both the master site copy of the HyperSwap volume and the auxiliary site copy of the HyperSwap volume.

   Use the results in the function field to determine whether the volume copy is on the auxiliary site in the HyperSwap relationship. The value `aux` indicates the volume copy at the auxiliary site.

   – Determine the pool name or ID that is used by the volume copy on the auxiliary site.

   – Determine the ID of the volume copy on the auxiliary site.

   – Determine the name or the ID of the volume on which the copies are based.

2. To filter the results, use the following command:

   ```
   lsvdisk -delim : -filtervalue function=aux
   ```

   Figure 4-13 shows the resulting list of auxiliary HyperSwap volumes.

Figure 4-13 List of Aux HyperSwap volumes

3. To remove the volume copy that was identified in above step, enter the following command:

   `svctask rmvolumecopy -copy <copy_id> -pool <pool_id_or_name> -removefcmaps <name_id>`

   where:

   – `<copy_id>` is the copy identifier for the copy on the auxiliary site.
   – `<pool_id_or_name>` is the name or identifier of the pool.
   – `<name_id>` is the name or ID of the volume that is associated with the copy.

   This command removes the volume copy at the auxiliary site, its associated FlashCopy mappings, and the change volumes that are created when HyperSwap volume is created. This action makes the volume copy at the master site an independent volume that can be recovered with IBM Copy Services Manager.

Auxiliary site contains Safeguarded backups; master site does not

In this use case, the Auxiliary site in the HyperSwap system contains the HyperSwap source volumes with Safeguarded backups. Complete these steps before you restore the Safeguarded backup to the HyperSwap auxiliary volume:

1. To verify the HyperSwap volume copies on the HyperSwap FlashSystem when SSH is connected into the FlashArray as administrator, enter the following command:

   `lsvdisk`

2. From the results that display, determine both the master site copy of the HyperSwap volume and the auxiliary site copy of the HyperSwap volume.

   Gather the following information, and use it to determine whether the volume copy is on the master site in the HyperSwap relationship. The value master indicates the volume copy at the master site.

   – Determine the pool name or ID that is used by the volume copy on the master site.
   – Determine the ID of the volume copy on the master site.
   – Determine the name or the ID of the volume on which the copies are based.

3. Use the following command to help filter the results:

   `lsvdisk -delim : -filtervalue function=master`

   The result will look similar to the list in Figure 4-14.

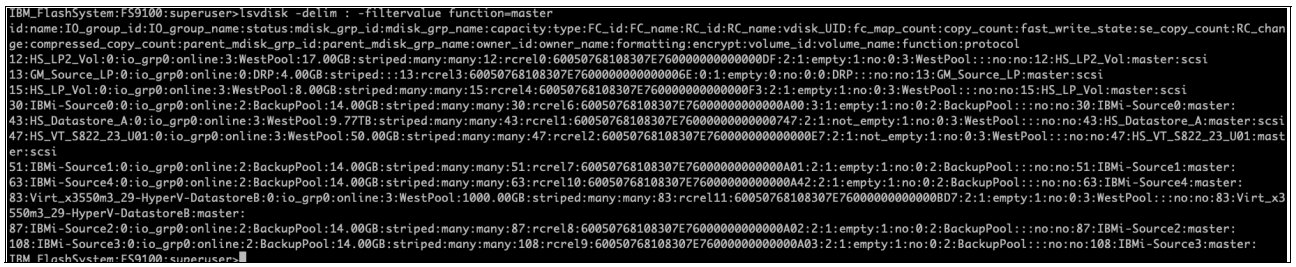


Figure 4-14 Example of CLI command to list Master HyperSwap volumes

4. To remove the volume copy that was identified in above step, enter the following command:

   ```
   svctask rmvolumecopy -copy <copy_id> -pool <pool_id_or_name> -removefcmaps <name_id>
   ```

   where:

   – <copy_id> is the copy identifier for the copy on the master site.
   – <pool_id_or_name> is the name or identifier of the pool.
   – <name_id> indicates is name or ID of the volume that is associated with the copy.

   This command removes the volume copy at the master site, its associated FlashCopy mappings, and change volumes that were created when HyperSwap volume was created. This action makes the volume copy at the auxiliary site an independent volume that can be recovered with IBM Copy Services Manager.

Dual HyperSwapped sites: Restoring the backup to the master site

If both sites of a HyperSwap contain Safeguarded backups, but you want to restore to the master site only, complete the following steps:

1. To verify the HyperSwap volume copies on the HyperSwap FlashSystem **when SSH is connected into the FlashArray as administrator**, enter the following command:

   ```
   lsvdisk
   ```

2. Use the following command to help filter the results:

   ```
   lsvdisk -delim : -filtervalue function=master
   ```

   The result will look similar to the list in Figure 4-15.

Figure 4-15 List of Aux HyperSwap volumes

3. To remove the volume copy that was identified in above step, enter the following command:

   ```
   svctask rmvolumecopy -copy <copy_id> -pool <pool_id_or_name> -removefcmaps <name_id>
   ```

   where:

   – <copy_id> is the copy identifier for the copy on the auxiliary site.
   – <pool_id_or_name> is the name or identifier of the pool.
   – <name_id> indicates is name or ID of the volume that is associated with the copy.

   This command removes the volume copy at the auxiliary site, its associated FlashCopy mappings, and change volumes that were created when HyperSwap volume was created. This action makes the volume copy at the master site an independent volume that can be recovered with IBM Copy Services Manager.

4.2.3 Overview of Copy Services Manager steps for Safeguarded Restore

The following steps are an overview of the IBM Copy Services Manager process for Safeguarded Restore:

1. Log in to the IBM Copy Services Manager instance `https://<IP/Host>:9559/CSM`

where: `<IP/host>` is the IP address or hostname of the IBM Copy Services Manager instance.

2. On the Sessions Overview page, select **Sessions**.
3. On the Sessions page, select the volume group that contains Safeguarded backup copies that you want to restore.
4. Select **Session Actions** → **Command** → **Restore Backup to Production**.
5. On the Restore Backup page, select the version of the Safeguarded backup snapshot that you want to restore. This backup overwrites the existing production volume.

   Safeguarded backup copies are displayed by their backup time from the most recent to the oldest version. In a restore, Safeguarded backup copies completely replace the source volumes on the original host that is currently defined in volume group.
6. Click **Yes**.

4.2.4 Detailed GUI steps to restore Safeguarded backup copies to production

The following are the detailed GUI steps to restore Safeguarded backup copies to production

1. Log in to the IBM Copy Services Manager instance `https://<IP/Host>:9559/CSM`

   where: `<IP/host>` is the IP address or hostname of the IBM Copy Services Manager instance.

   Ensure that your role is admin or higher to perform these actions.

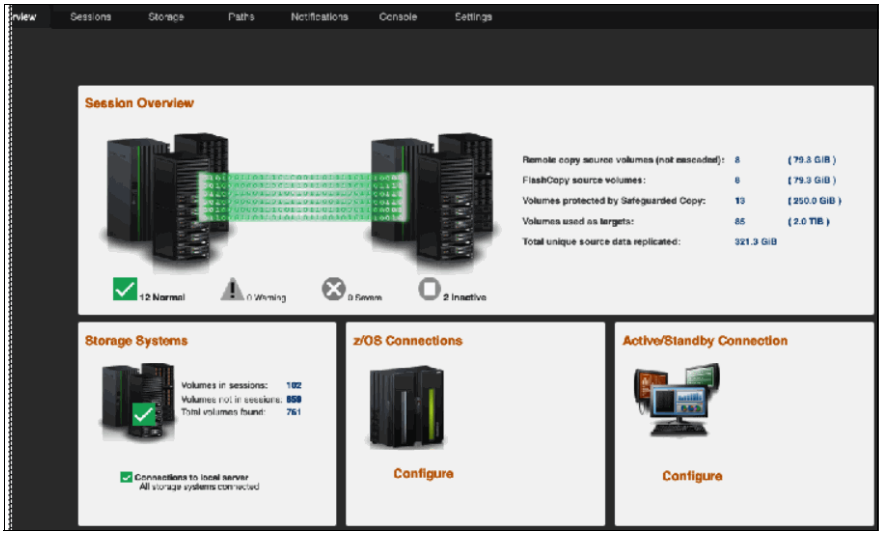


Figure 4-16 Copy Services Manager main screen

2. On the Overview page, select **Sessions**. See Figure 4-17.

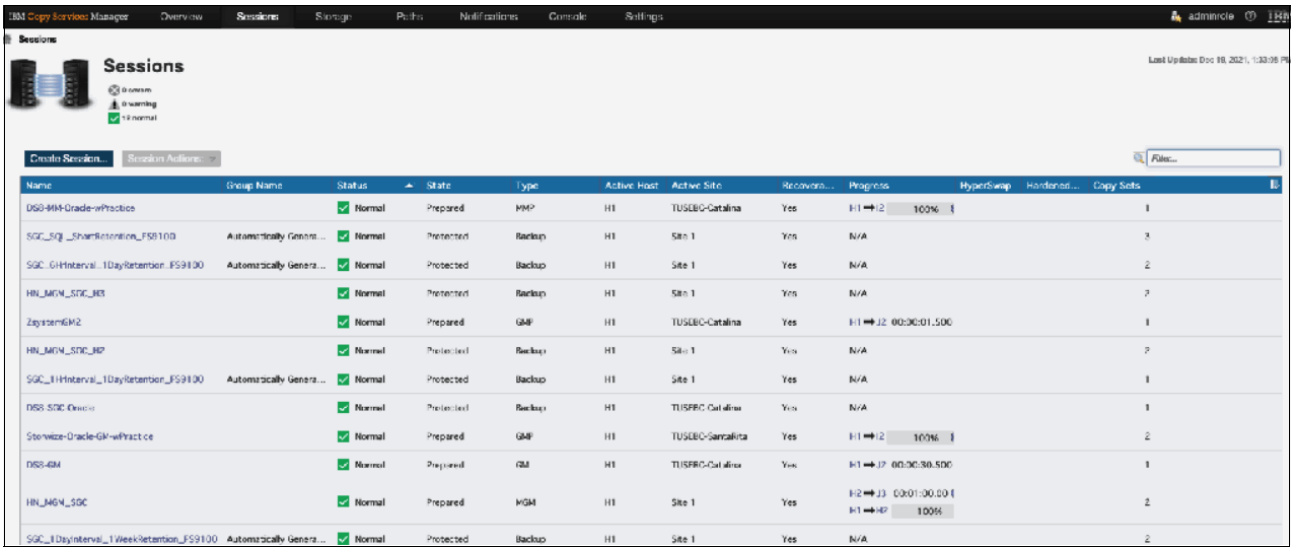


Figure 4-17 Sessions page of IBM Copy Service Manager

3.From the Sessions overview page, select the volume group that contains the volumes you want to restore and overwrite to production. See Figure 4-18.

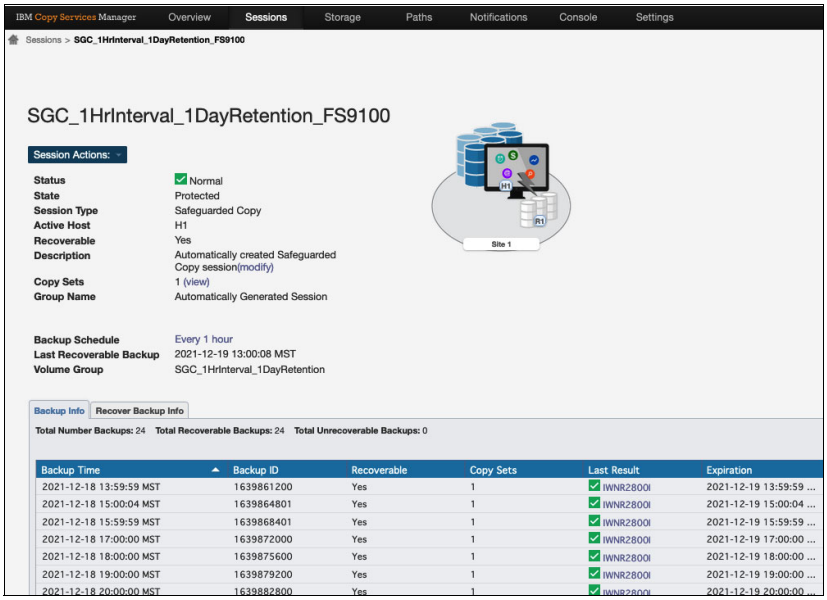


Figure 4-18 List of volume groups to recover

4.Select **Session Actions** → **Commands** → **Recover Backup to Production**.

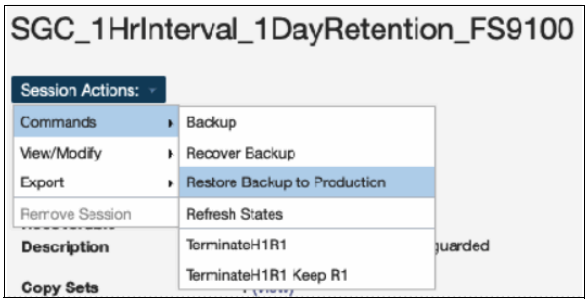


Figure 4-19 Key command difference to restore backup to production

3. Select the generation of the backup that you want to recover. See Figure 4-20.

   The snapshot is restored and it overwrites the existing mapped volumes. To ensure data integrity, the graphic and information will be emphasized on the pop-up window.

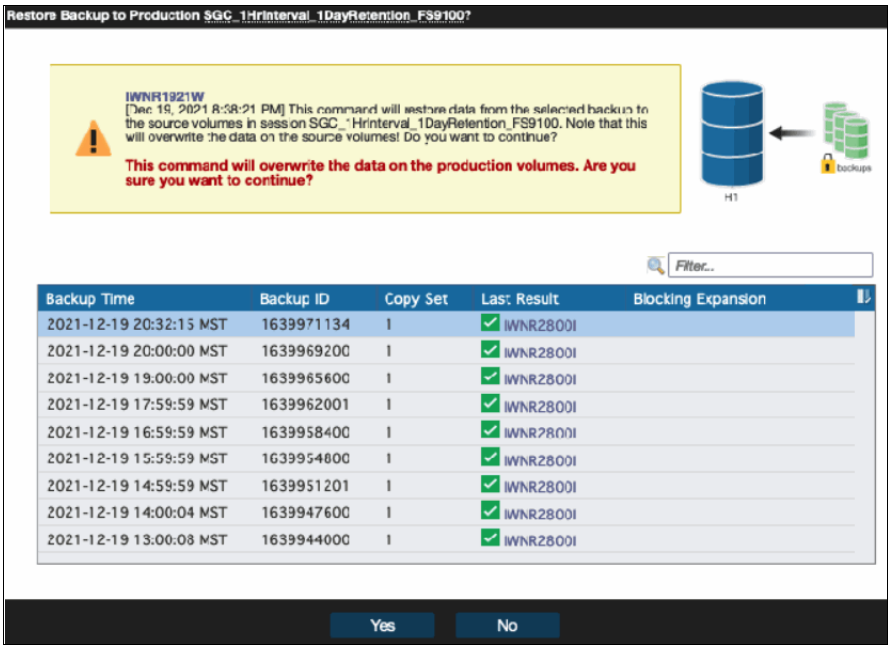


Figure 4-20 Select the specific Safeguarded Snapshot to restore to existing host

When the restore is complete, the immediate results are displayed in the main window and in the event log on IBM Copy Services Manager. See Figure 4-21.

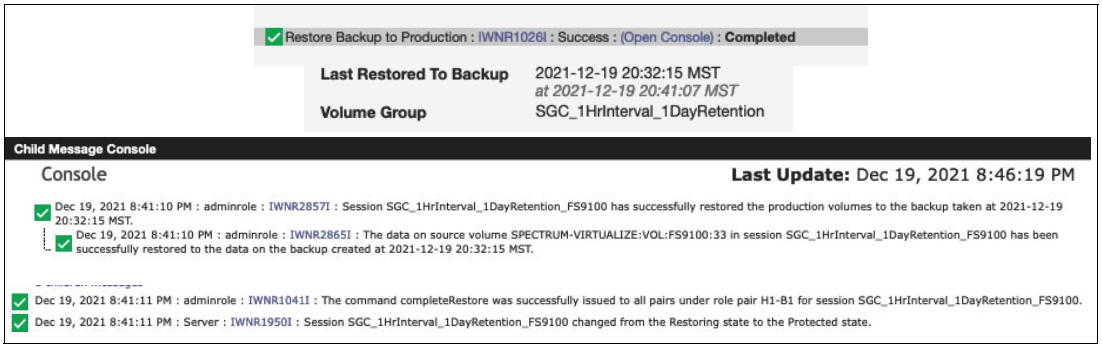


Figure 4-21 Recover Backup to production confirmations

Note: Unlike Restore, when you use Recover Backup to Production the volume immediately overwrites the existing mapped volume. Therefore, there it is not necessary to manually map the volume.

4. Restart your existing mapped hosts to ensure they pick up the restored changes to the volumes.
5. If you restored a HyperSwap source volume, you must return the recovered source volume to a HyperSwap volume.

   Enter the following command to create a copy of the restored volume on the other site:

   ```
   addvolumecopy -pool <storage_pool_id or storage_pool_name> <volume_name or volume_id>
   ```

4.3 IBM Copy Services Manager CLI commands

The Restore steps can also be accomplished by using the CLI through SSH.

Attention: A detailed manual of all IBM Copy Services Manager CLI commands and their syntax can be found at the following location:

A detailed manual of all commands and their syntax can be found at the following location:

https://www.ibm.com/support/pages/ibm-copy-services-manager-command-line-interface-users-guide

1. To access the IBM Copy Services Manager CLI, you must SSH into the IBM Copy Services Manager host and then run the CLI shell. An example is shown in Figure 4-22 for Linux, where the default directory is `/opt/IBM/CSM/CLI`.

```
[root@csm CLI]# ls
cliTrace.log  csmcli-auth.properties  csmcli.bat  csmcli.sh
[root@csm CLI]# ./csmcli.sh
Please enter a username for logging onto the server
csmadmin
Please enter a password for logging onto the server
>
IBM Copy Services Manager Command Line Interface (CLI)
 Copyright 2007, 2015 IBM Corporation
 CLI Client Version: 6.3.1.0, Build: a20211109-1034
 Authentication file: csmcli-auth.properties

Connected to:
 Server: csm     Port: 9560   UseREST: false
 Server Version: 6.3.1.0, Build: a20211109-1034
```

Figure 4-22 Using SSH to access host and launch CSMCLI shell

2. To show the all the IBM Copy Services Manager sessions and their status, use the **lssess** command.

```
csmcli> lssess
Name                 Status State     Copy Type        Group
==========================================================================================
BFS_SGC_VG_MACBETH Normal Protected Safeguarded Copy Automatically Generated Session
csmcli>
```

Figure 4-23 Listing of IBM Copy Services Manager sessions

3. To show the details of a session inside IBM Copy Services Manager, use the **showsess** command with the specific name of that session:

   `showsess <session name>`

```
CMMCI9022E Missing required parameter: session_name.
Usage: showsess [ { -help|-h|-? } ] session_name | -
Tip: Enter "help showsess" for more information.
csmcli>
csmcli>
csmcli>
csmcli> showsess BFS_SGC_VG_MACBETH
Name              BFS_SGC_VG_MACBETH
Group             Automatically Generated Session
Type              Safeguarded Copy
State             Protected
Status            Normal
Locations         Site1
Copy Sets         4
Copying           Yes
Recoverable       Yes
Active Host       H1
Error Count       0
Description       Automatically created Safeguarded Copy session
Transitioning     No
Consistency Group -
Volume Group      BFS_SGC_VG
Detailed Status

 IWNR1500I [Dec 25, 2021 7:12:14 PM] Session information about session BFS_SGC_VG_MACBETH was successfully obtained.
csmcli>
```

Figure 4-24 Listing of a specific IBM Copy Services Manager Session

4. To see the available actions for a given specific session, use the **lssessactions** command:

   `lssessactions <name of session>`

```
csmcli> lssessactions BFS_SGC_VG_MACBETH
Action                       Description
=============================================================================================================
backup                       Backup the session
recover_backup               Recover the session to a selected backup
restore_backup_to_production No description available.
terminateh1r1                Terminate the relationships between host1 and recovery1
terminateh1r1_keep_r1        Terminate the relationships between host1 and recovery1 and persist recovery1 volumes
csmcli>
```

Figure 4-25 Listing of session available commands

5. To take one of those actions on a particular session inside IBM Copy Services Manager, use the **cmdsess** command:

   `cmdsess -action <action> -retentiondays <number of days to keep> <name of session>`

```
csmcli> cmdsess -action backup -retentiondays 1 BFS_SGC_VG_MACBETH
IWNR1881W [Dec 25, 2021 7:25:51 PM] This command will create a backup of session BFS_SGC_VG_MACBETH. Do you want to continue? [y/n]:y
 IWNR1026I [Dec 25, 2021 7:26:01 PM] The Backup command in the BFS_SGC_VG_MACBETH session completed.
csmcli>
```

Figure 4-26 Taking an additional Safeguarded backup

6. To list all the Safeguarded volumes with recovery relationships, enter the following command:

   `lsrecoveredbackupscommand`

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this paper.

IBM Redbooks

The following IBM Redbooks publications provide additional information about the topic in this document. Note that some publications referenced in this list might be available in softcopy only.

- *Implementing the IBM FlashSystem with IBM Spectrum Virtualize Version 8.4.2,* SG24-8506

You can search for, view, download or order these documents and other Redbooks, Redpapers, Web Docs, draft and additional materials, at: **ibm.com**/redbooks

Other publications

These publications are also relevant as further information sources:

- https://www.ffiec.gov/press/pdf/ffiec_appendix_j.pdf
- http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf

Online resources

These websites are also relevant as further information sources:

- IBM Security QRadar XCD:

  https://www.ibm.com/security/security-intelligence/qradar
- IBM Storage Insights:

  https://www.ibm.com/products/analytics-driven-data-management
- IBM Spectrum Protect:

  https://www.ibm.com/products/data-protection-and-recovery

Help from IBM

- IBM Support and Downloads

  ibm.com/support
- IBM Global Services

  ibm.com/support

REDP-5654-00

ISBN 0738460303

Printed in U.S.A.