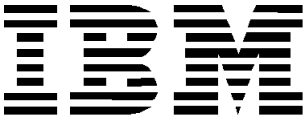
IBM® Storage

Cyber Resiliency Solution using IBM Spectrum Virtualize



Contents

About this document

This document is intended to facilitate the solution for Safeguarded Copy for cyber resiliency and logical air gap solution for IBM FlashSystem and SAN Volume Controller. The document showcases the configuration and end-to-end architecture for configuring the logical air-gap solution for cyber resiliency by using the Safeguarded Copy feature in IBM FlashSystem and IBM SAN Volume Control storage.

The information in this document is distributed on an “as is” basis without any warranty that is either expressed or implied. Support assistance for the use of this material is limited to situations where IBM FlashSystem or IBM SAN Volume Controller storage devices are supported and entitled and where the issues are specific to a blueprint implementation.

Executive Summary

In today's world, data security is of utmost importance. The data can be compromised by human error, system glitches, or malicious acts. Data breaches are among the gravest and most expensive threats to businesses today.

The traditional business continuity solutions that most organizations developed and implemented high availability (HA) and disaster recovery (DR) solutions to protect their data are not sufficient enough to protect against the cyberattacks. According to the 2020 Cost of Data Breach Report[1] (a recent Ponemon Institute study), the average cost worldwide of a data breach in the preceding 12 months was $4 million US, an adjusted-average total cost. Organizations that are affected by a breach also run the risk of having their normal business operations disrupted and valuable data, customers, and reputation lost within their industry.

Cyber resilience solutions are developed and aim for organizations to continue to operate with the least amount of disruption, despite cyberattacks and outages. Cyber resilience expands the scope of protection, covering cybersecurity and business continuity.

A significant part of cyber resilience is the ability to recover from a logical data corruption event. Because this unrelenting tide of data breaches is driving increased interest in providing secure authentication across hybrid cloud environments, IBM Spectrum Virtualize offers the powerful data security functions of IBM Safeguarded Copy.

The new Safeguarded Copy solution that is available with IBM Spectrum Virtualize 8.4.2 software is the latest protection mechanism for data on IBM FlashSystem family and SAN Volume Controller storage systems. Safeguarded Copy, as with IBM DS8000® Safeguarded Copy solution, helps secure data to prevent it from being compromised accidentally or deliberately. It also allows for fast recovery from protected backups if a cyberattack occurs.

It provides secure, point-in-time copies or snapshots of active production data that cannot be altered or deleted (known as *immutable copies*). They also can later be used for identification, repair, or replacement of data that was compromised by a cyber or internal attack or corrupted by system failures or human error.

The safeguarded backups or copies of data are protected with more user role security restrictions (separation of duties) that are designed to keep your data safe.

The Safeguarded Copy solution on IBM FlashSystem family and IBM SAN Volume Controller storage systems integrates with IBM Copy Services Manager software, starting with Copy Services Manager version 6.3.0.1, by using its automated, built-in copy and retention scheduling, testing, and ease of recovery capabilities.

[1] https://www.ibm.com/security/data-breach

Scope

This blueprint guide provides:

- A solutions architecture and related solution configuration workflows, with the following essential software and hardware components:
  - IBM FlashSystem Array
  - IBM Copy Services Manager

  Note: Safeguarded Copy uses FlashCopy® snapshot technology. For systems that do not have FlashCopy with IBM® Spectrum Virtualize software, they must acquire the FlashCopy license as an Add-On because it is required for SGC.

- Detailed technical configuration steps for building the cyber resiliency solutions

This technical report does not:

- Provide performance analysis from a user perspective
- Replace any official manuals and documents that are issued by IBM

Prerequisites

This technical paper assumes that the reader has a basic knowledge of IBM FlashSystem Array concepts.

Getting started: Cyber Resiliency Solution using Safeguarded Copy with IBM FlashSystem Arrays

This section describes the essential building material for creating the logical air-gap, cyber resiliency solution that uses the Safeguarded Copy feature that is available in IBM FlashSystem.

IBM FlashSystem family

The IBM FlashSystem family simplifies storage for hybrid cloud environments. With a unified set of software, tools, and APIs, the IBM FlashSystem addresses the entire range of storage needs, all from one data platform that extends enterprise functions across the storage ecosystem.

With IBM Spectrum Virtualize software, the IBM FlashSystem family is an industry-leading storage solution that includes technologies that complement and enhance virtual environments to achieve a simpler, more scalable and cost-efficient IT infrastructure. To further drive your IT transformation, IBM Spectrum Virtualize for Public Cloud offers multiple ways to create hybrid cloud solutions between on-premises private clouds and the public cloud. It enables real-time storage-based data replication and disaster recovery, and data migration between local storage and AWS. This feature enables storage administration at a cloud service provider’s site in the same way as on-premises, regardless of the type of storage.

For more information about IBM FlashSystem family, see this web page.

IBM FlashSystem storage solutions include the following features:

- NVMe-accelerated flash arrays with control enclosures that are end-to-end NVMe-enabled. They include the flexibility to choose and mix between IBM FlashCore® Modules, industry-standard NVMe drives, and Storage Class Memory (SCM). The systems offer industry-leading performance and scalability with support for bare-metal, virtual, and containerized environments.
- Built with IBM Spectrum Virtualize, with a full range of industry-leading data services, such as dynamic tiering, IBM FlashCopy management, data mobility, and high-performance data encryption, among many other data management features.
- Hybrid cloud ready, with support for private, hybrid, or public cloud deployments. The solutions include ready-to-use, proven, validated “cloud blueprints” with support for cloud API automation and secondary data orchestration software.
- Cost-efficient, with innovative data reduction pool (DRP) technology that includes deduplication and hardware-accelerated compression technology, and SCSI UNMAP support and all the thin provisioning, copy management, and efficiency you expect from IBM Spectrum Virtualize based storage.
- Hybrid storage enabled, with multiple expansion enclosure options that are based on 12 Gbps SAS that supports solid-state drives (SSD) and hard disk drives (HDD).
- Ready for new generation applications, supporting Red Hat OpenShift, Container Storage Interface (CSI), Ansible automation, and Kubernetes along with traditional VMware and bare metal environments.
- IBM Cloud® Satellite™ helps you deploy consistently across all on-premises, edge computing, and public cloud environments from any cloud vendor. The result is greater developer productivity and development velocity. IBM FlashSystem® family is the perfect storage choice for IBM Cloud Satellite™ because of its simplicity, high performance, and low latency.
- IBM Copy Services Manager coordinates and automates Safeguarded Copy function across multiple systems

Architecture for Cyber Resiliency solution using Safeguarded Copy: Lab setup

The architecture that was deployed in lab to showcase Safeguarded Copy setup for a cyber resiliency solution using MS-SQL database is shown in Figure 1 on page 5.

In this sample configuration, an IBM FlashSystem 9100 is used.

The lab configuration shows the following steps:

1. Create a Safeguarded Pool on an IBM FlashSystem 9100 array.
2. Set up a volume group and Safeguarded Copy policies.
3. Install and configure the IBM Copy Services Manager.
4. Take a Safeguarded Copy backup of the production volume that is running MS-SQL database.
5. Restore/Recover data from the immutable Safeguarded Copy snapshots.

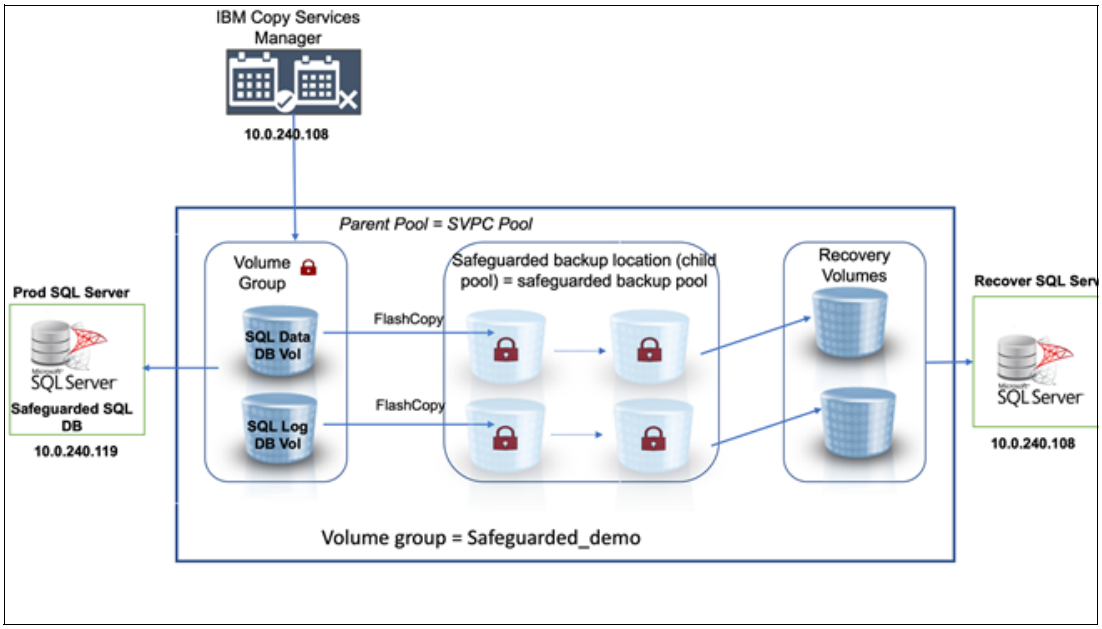


Figure 1 Safeguarded Copy lab setup architecture

Configuring a Safeguarded Pool on IBM FlashSystem

To configure the Safeguarded Copy functions, the first step is to create a safeguarded backup location. The safeguarded backup location is established with the help of FlashSystem child pools.

A safeguarded backup location is a child pool in each parent pool where the source volume is located. The safeguarded backup location stores Safeguarded backup copies.

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 Safeguarded backup location can contain multiple versions of volume data that is backed up, based on different copy intervals and retention to cover various recovery point objectives.

To create a Safeguarded backup location, complete the following steps:

1. In the management GUI, select **Pools** → **Pools**.
2. Right-click a parent pool and select **Create Child Pool**.
3. On the Create Child Pool page (see Figure 2 on page 6), enter a name for the child pool.

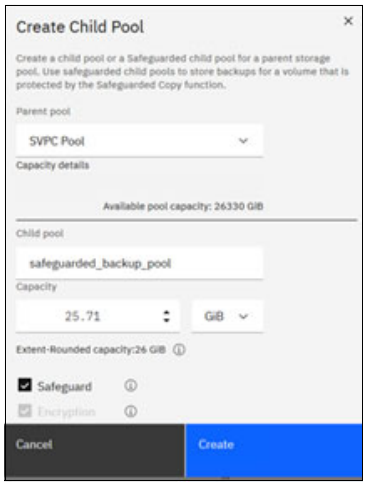


Figure 2 Create safeguarded backup location: Child pool

4. 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 data reduction pool, the child pool shares capacity with the parent pool.
5. Select **Safeguard** to indicate that the child pool is used as the Safeguarded backup location for immutable backup copies of source volumes.
6. Click **Create**. Child pools that are used as Safeguarded backup locations are marked with a shield icon on the Pools page (see Figure 3).

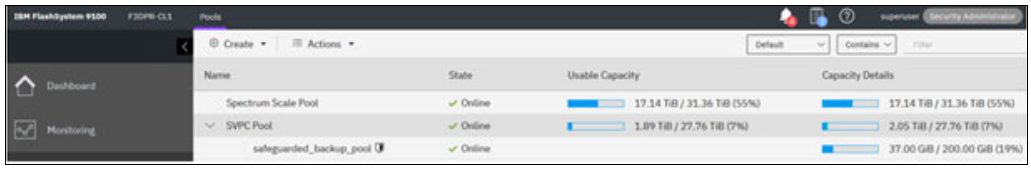


Figure 3 Child Pool as a safeguarded backup location

In this lab setup, the child pool `safeguarded_backup_pool` is configured in the parent SVPC Pool, as shown in Figure 3.

Setting up volume groups and a Safeguarded Policy

Volume groups are the way SGC 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 that are configured as part of the Safeguarded Copy function.

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.

To create a volume group, 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. 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.

4. Click **Create Volume Group**.

The volume group is created with the name `safeguarded_demo`, as shown in Figure 4.

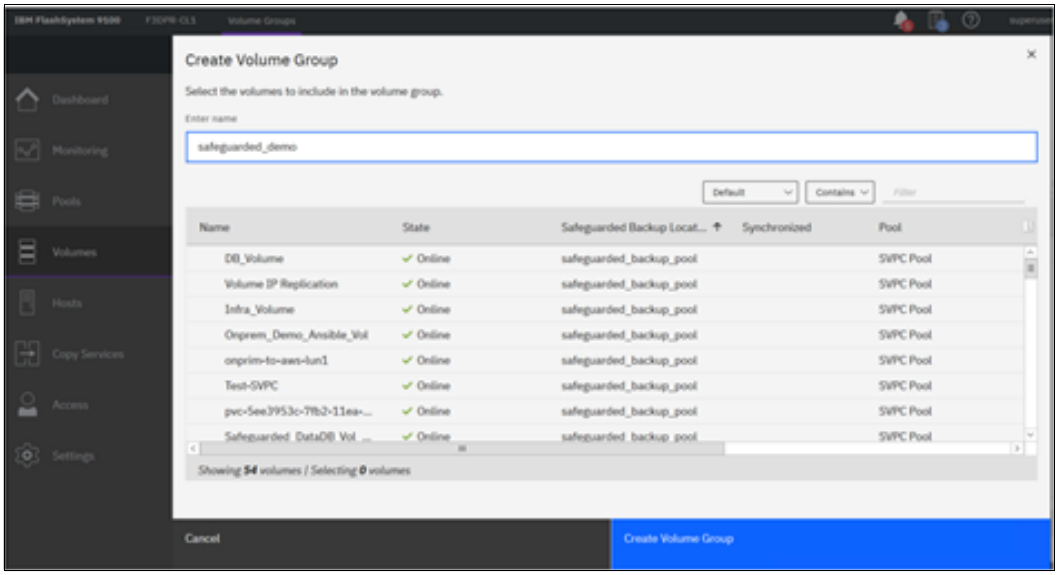


Figure 4 Creating volume group and adding volume to the group

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

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

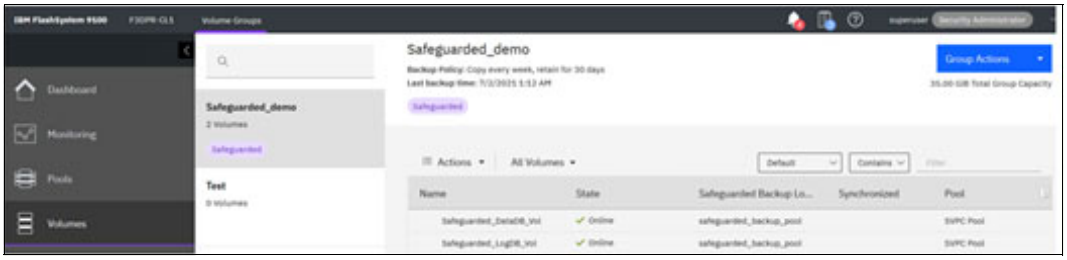


Figure 5 Volume addition to the volume group

Safeguarded backup policy

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

As of this writing, the management GUI does not support creating user-defined Safeguarded backup policies. However, you can use the CLI **`mksafeguardedpolicy`** command to create user-defined policies. Three predefined policies are in the system, as shown in Figure 6.

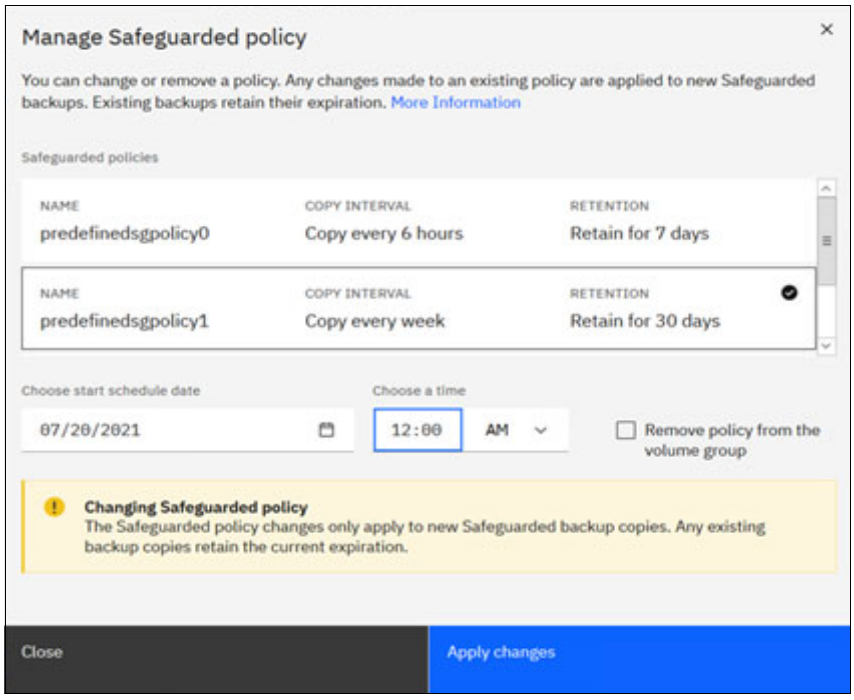


Figure 6 Predefined backup policies

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 that you want to assign a predefined policy to and then, select **Group Actions** → **Assign Safeguarded policy**.
3. Select one of the following predefined Safeguarded backup policies (see Figure 6).

   In this example, `predefinedsgpolicy1` is selected.

   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 starts 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 to start creating Safeguarded backups that use the policy.
5. Click **Assign**.

After the Safeguarded backup policy is assigned to the volume group, the status of the volume group displays as Safeguarded scheduled, as shown in Figure 7.

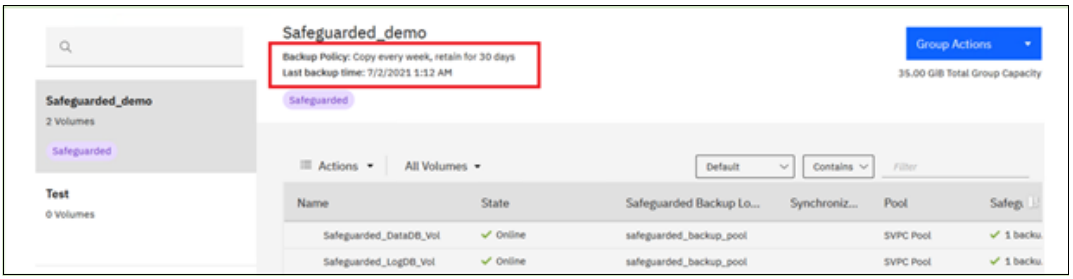


Figure 7 Backup policy schedule

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 any parent pool with a Safeguarded backup location.

Installing and configuring IBM's Copy Services Manager

This section provides information about installing and configuring IBM Copy Services Manager.

IBM's Copy Services Manager is excellent at many replication automations and is essential for SGC.

IBM Copy Services Manager automates the process of creating Safeguarded backup copies according to the schedule that is defined in a Safeguarded backup policy. IBM Copy Services Manager supports testing, restoring, and recovering operations with Safeguarded backup copies.

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

- IBM Copy Services Manager is included in all versions of IBM Spectrum® Control, Virtual Storage Center (VSC), and Spectrum Storage Suite. However, if you do not have an IBM Copy Services Manager license, purchase the IBM Copy Manager for IBM Spectrum Virtualize, which includes IBM Copy Services Manager version 6.3.0.1 or later. This license option is available through iERP/AAS, IBM Passport Advantage®, or your IBM Sales team.
- If you have a license for IBM Copy Services Manager, download IBM Copy Services Manager version 6.3.0.1 or later at this web page.

- 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 this web page.

Creating an Administrator user for IBM Copy Services Manager

Before you can establish the IBM FlashSystem as a connection endpoint in IBM Copy Services Manager, you must configure a user with an Administrator role on the IBM FlashSystem array or IBM SAN Volume Controller.

For auditing, it is recommended that you create an 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.

The IBM Copy Services Manager uses this role to create FlashCopy mappings between the source volumes and the Safeguarded backup copies on the IBM FlashSystem. To create an Administrator user on IBM FlashSystem for IBM Copy Services Manager, complete the following steps:

1. In the management GUI, select **Access** → **Users by Groups** → **Create User Group**.
2. On the Create User Group page, enter a name of 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**.
6. To connect to the management GUI with this user, enter and confirm a password.
7. Click **Create**.

In this example, the `csmuser` user is created, which is used for IBM Copy Services Manager, as shown in Figure 8.

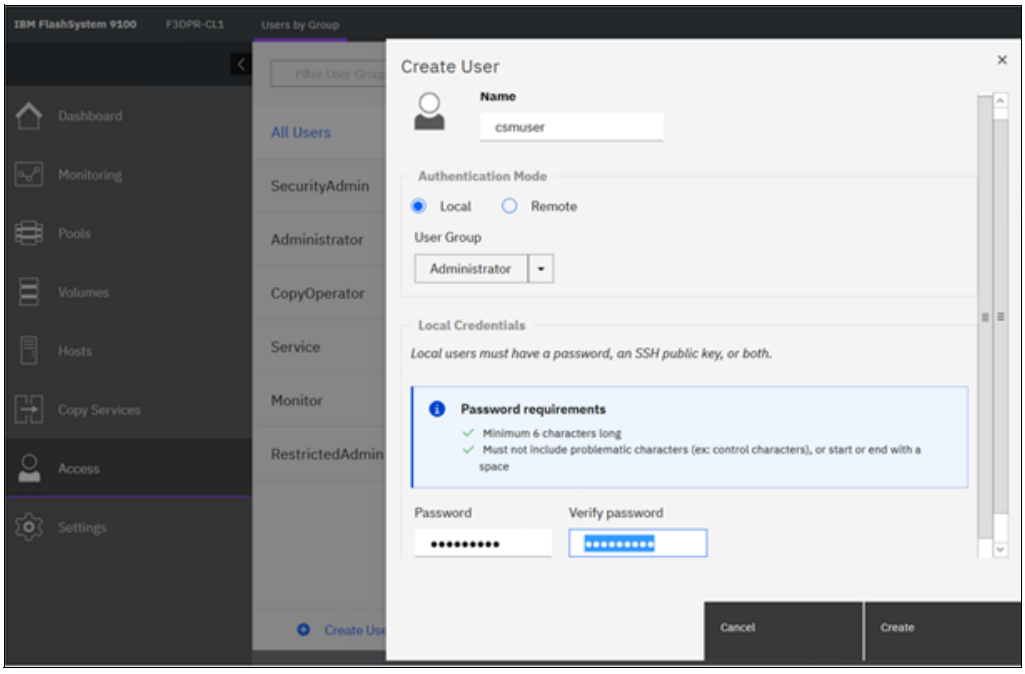


Figure 8 Creating an administrator user

Creating a connection to the FlashSystem inside of IBM Copy Services Manager

To use Safeguarded Copy function, you must create a connection to the system in the IBM Copy Services Manager interface. Complete the following steps:

1. Log in to IBM Copy Services Manager at: `https:// <IP/hostname> :9559/CSM`.

   Where the IP address or host name is the IBM Copy Services Manager instance that is 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 IBM Storwize® Family
5. On the Connections page, enter the following information for your system:
   - Cluster IP/Domain Name: The management IP address or domain name for your system.
   - Username: The username for the Administrator user for the system.
   - Password: The password that is associated with the Administrator user for the system.
6. Click **Finish**.
7. On the Storage Systems page, verify that Local Status for the connection is `Connected`, as shown in Figure 9.

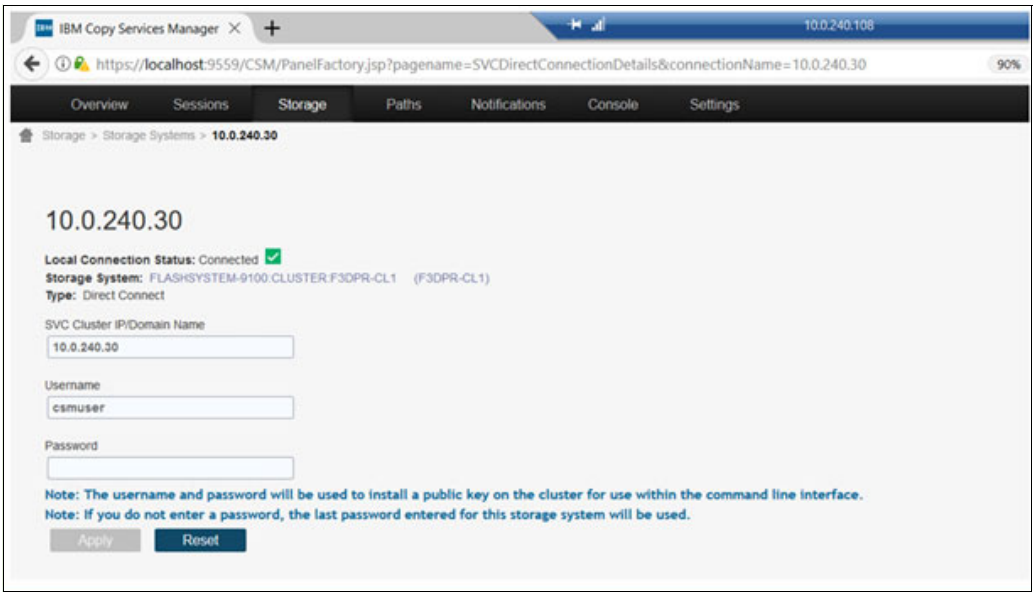


Figure 9 Creating connection to IBM FlashSystem in IBM Copy Services Manager

After a connection is established, IBM Copy Services Manager automatically detects volume groups with Safeguarded backup policies and schedules the backup copies. IBM Copy Services Manager queries the system every 5 minutes to process Safeguarded backup policies.

The start time that is defined in the Safeguarded backup policy must factor in the possible 5-minute delay. When IBM Copy Services Manager detects a new Safeguarded backup policy for a volume group, it creates the session and scheduled task to create and manage the Safeguarded backup copies.

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 (see Figure 10), the volume group `Safeguarded_demo` that was created on IBM FlashSystem is automatically visible as a session in IBM Copy Services Manager, as shown in Figure 10.

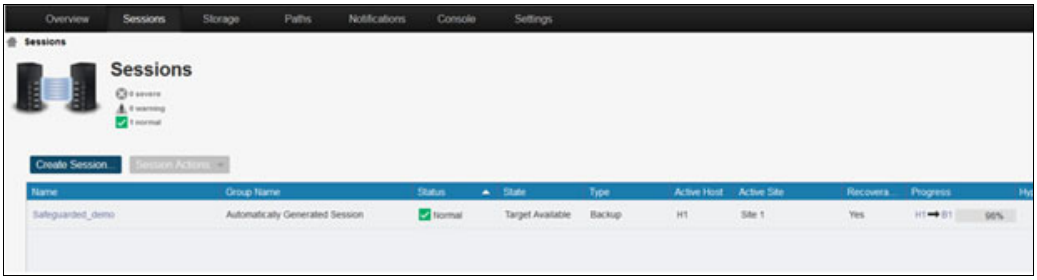


Figure 10 Safeguarded Copy session automatically visible in IBM Copy Services Manager

This session includes the two volumes that are part of the volume group that was defined earlier (see Figure 11).

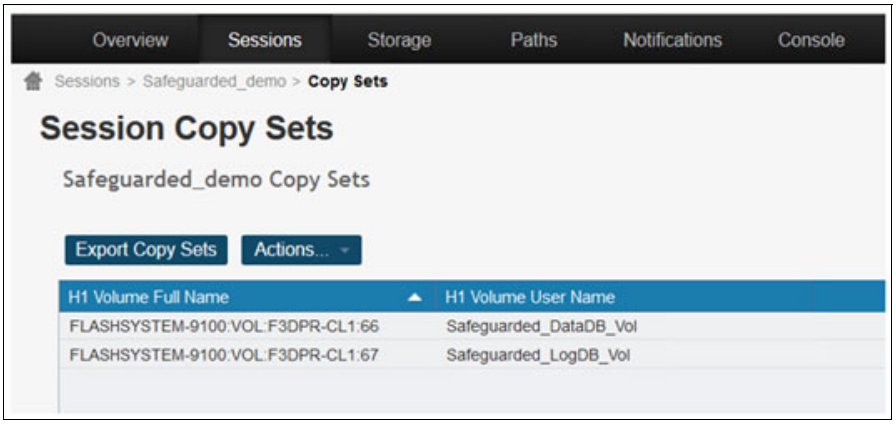


Figure 11 Volume information of the session

The IBM Copy Services Manager session details (as shown in Figure 12) shows more information about the safeguarded policy that is set on the volumes for the backup and retention.

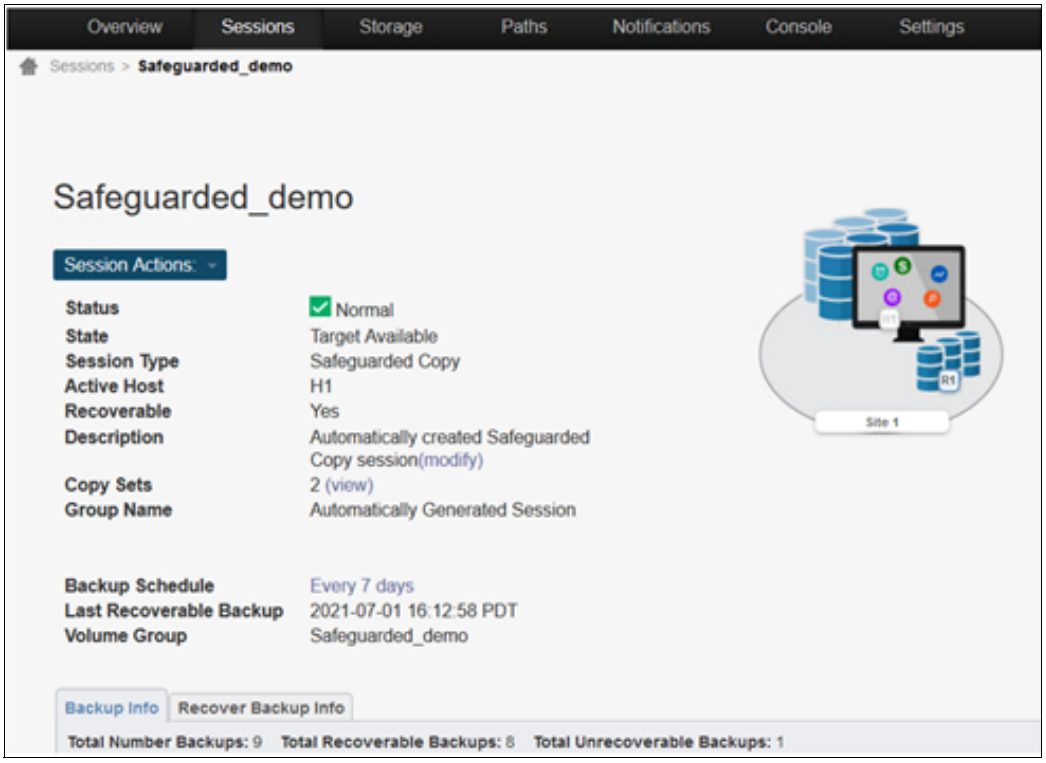


Figure 12 Policy information about the safeguarded volume group

Safeguarded Copy Backup of a production volume running an MS-SQL database

For this lab environment, we defined the Safeguarded Copy to back up two volumes running the MS-SQL database, where one volume contains the data tables of SQL database that is named `Safeguarded_DataDB_Vol` and second volume includes the logs table of the SQL database that is named `Safeguarded_LogDB_Vol`.

The Safeguarded Copy backup is a crash consistent IBM FlashCopy. To create full application consistency, an administrator must quiesce the database or make the database read-only before taking the backup.

In this example, an MS-SQL database that is named `Safeguarded_Copy_DB` is running (see Figure 13) on the lab production Windows server (10.0.240.119). The entire lab is defined earlier, as shown in Figure 1 on page 5.

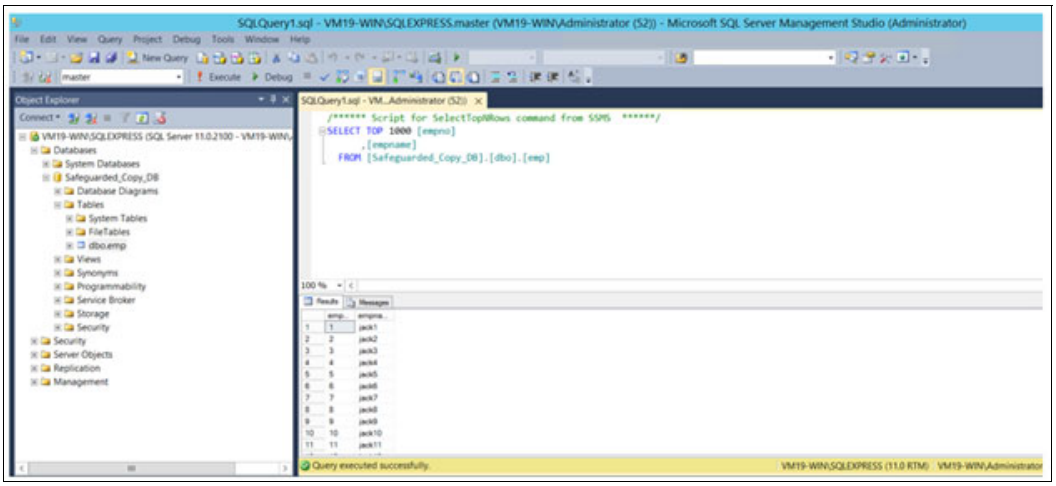


Figure 13 SQL Database running at production server

The safeguarded backup copy was created earlier by using IBM Copy Services Manager with the schedule and policy that is assigned to that volume group, as shown in Figure 14.

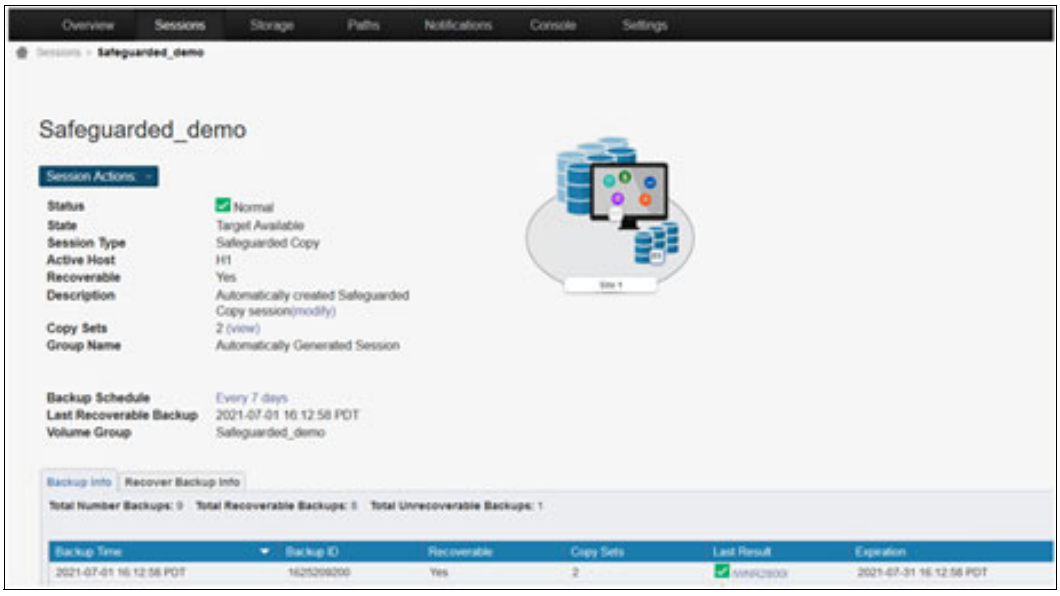


Figure 14 Safeguarded backup completed as per the backup policy assigned

SGC creates the backup immutable snapshot volumes in the safeguarded backup location (also known as a *child pool*) as in Figure 15.

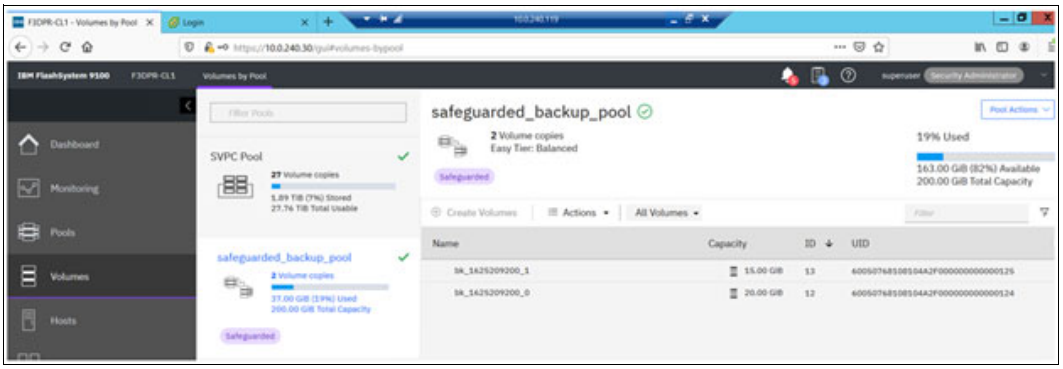


Figure 15 Immutable backup copies created

These immutable volumes are in the safeguarded backup location, which cannot be deleted, modified, or assigned to a host for reads or writes.

Restore/Recover of data by using immutable Safeguarded Copy backups

IBM Copy Services Manager provides automation for testing with the Recover Backup action. The Recover Backup action creates recovered versions of Safeguarded backup copies that you can map to test host and verify that applications run properly.

To test Safeguarded backup copies, complete the following steps:

1. Log in to `https://<IP/hostname>:9559/CSM`, where *<IP or Hostname>* is the IP address or host name of 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 recover.
4. Select **Session Actions** → **Command** → **Recover Backup**.
5. Select which generation of the backup you want to recover; in this example, we are restoring the latest backup, as shown in Figure 16.

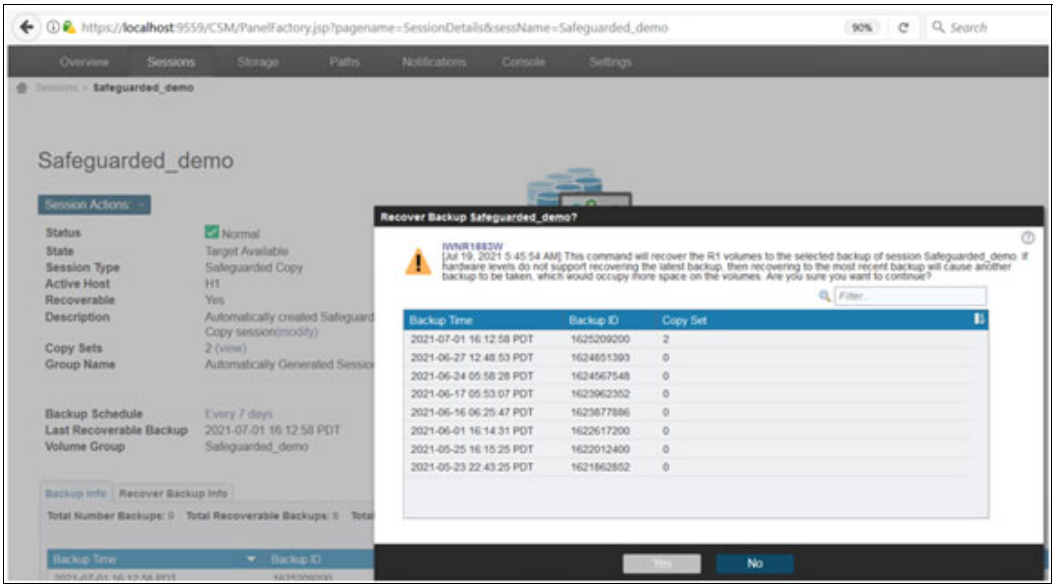


Figure 16 Recover of latest backup copy

After the recovery completes, the immutable snapshots are used to create volumes in the parent pool where the source volume originally is present (see Figure 17).

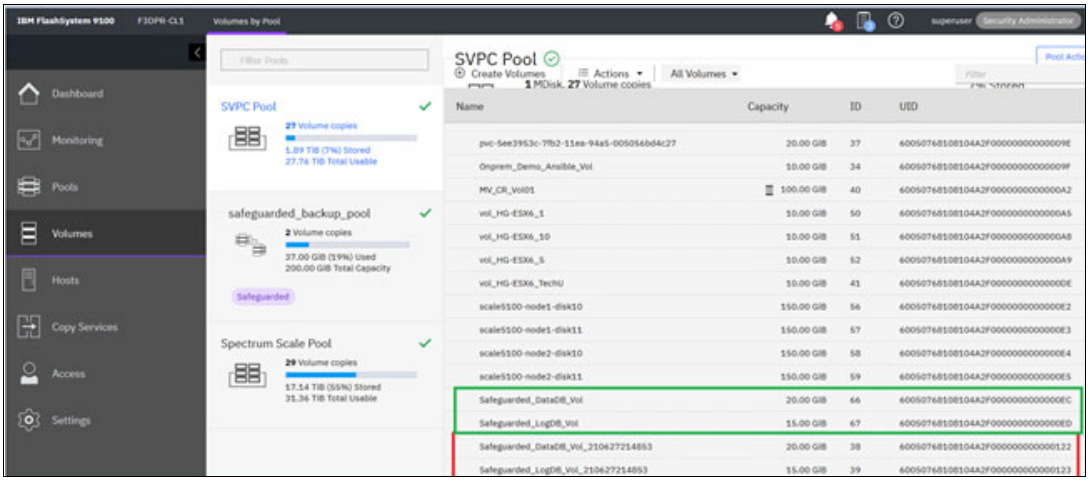


Figure 17 Recovered volume information

For reference, the volumes that are outlined in green in Figure 17 are the production volumes. The volumes that are outlined in red in Figure 17 are the restored volumes from the safeguarded backup copies.

These newly recovered volumes can now be mapped to a host to check for data integrity and consistency.

In this example, these restored volumes are mapped to a different Windows host (10.0.240.108), as shown in Figure 1 on page 5, and imported into the SQL database to validate the SQL database. The import is shown in Figure 18.

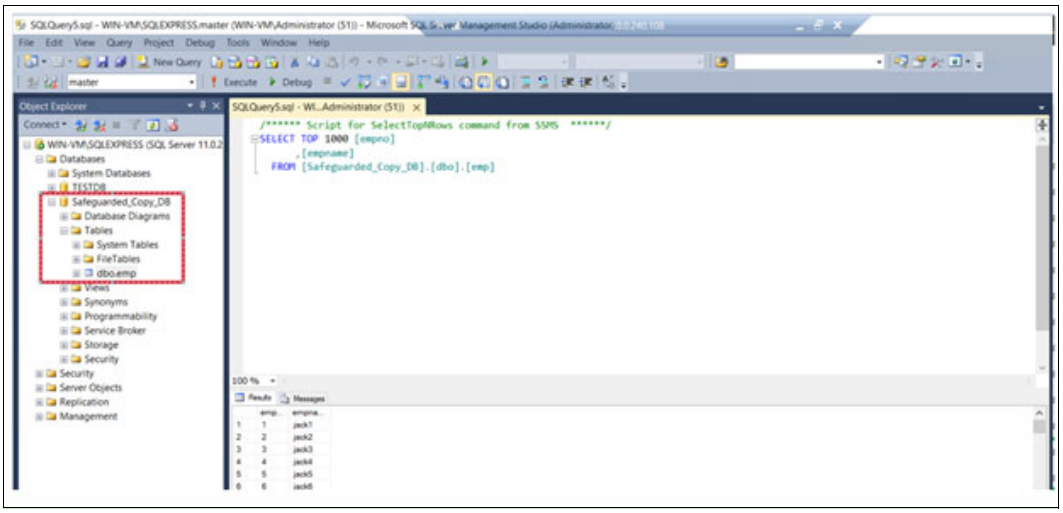


Figure 18 Recovered database on the restore server from recovered volumes

Restoring from a Safeguarded backup copy

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

Before you can restore data to the source volume by using 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 process. Both processes use the immutable volume data from the selected version of the Safeguarded backup copy from which you are restoring.

To recover Safeguarded backup copies, complete the following steps:

1. Log in to `https://<IP or Hostname>:9559/CSM` where `<IP or Hostname>` is the IP address or domain name of 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 restore.
4. Select **Session Actions** → **Command** → **Restore Backup**.
5. On the Restore Backup page, select the version of the Safeguarded backup copy that you want to restore.

   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**.

Summary

In this paper, we explored how easy it is to enable Safeguarded Copy on IBM FlashSystem arrays and IBM SAN Volume Controller to protect your most critical data. After a cyber attack occurs, a business must recover data as fast as possible because time is money.

The issue is that no single solution is correct for all your needs.

But, IBM makes fast recoveries easy to obtain.

The use of IBM's Safeguarded Copy for Spectrum Virtualize makes it easy to obtain the fastest recovery possible for your high frequency, short-term snapshots by using immutable data copies in your primary storage (see Figure 19).

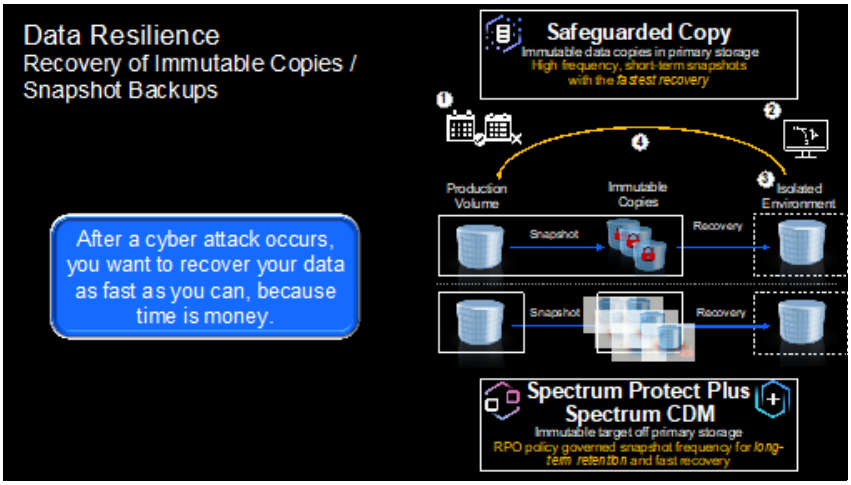


Figure 19 Data resilience: Recovery of immutable copies or Snapshot back ups

Customers use policy governed, agentless snapshots that use Service Level Agreements options to create snapshot copies of production data based on time interval or number of copies. If an event occurs and they suddenly find themselves recovering from an attack, they use the iterative process to choose the correct recovery copy.

Acknowledgment

The author thanks the following people for their support on this project:

Oiza Dorgu
Yves Santos
Brian Sherman
Andrew J Greenfield
Jackson Shea
Falk Schneider
IBM

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.

DS8000®
FlashCopy®
IBM®
IBM Cloud®
IBM Cloud Satellite™
IBM FlashCore®
IBM FlashSystem®
IBM Spectrum®
Passport Advantage®
Redbooks (logo) ®
Satellite™
Storwize®

The following terms are trademarks of other companies:

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

Ansible, OpenShift, Red Hat, are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

VMware, and the VMware logo are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

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

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

August 2021

Please recycle

ISBN 0738459925

REDP-5657-00