

IBM Storage DS8000 Safeguarded Copy

Updated for DS8000 Release 9.3.2

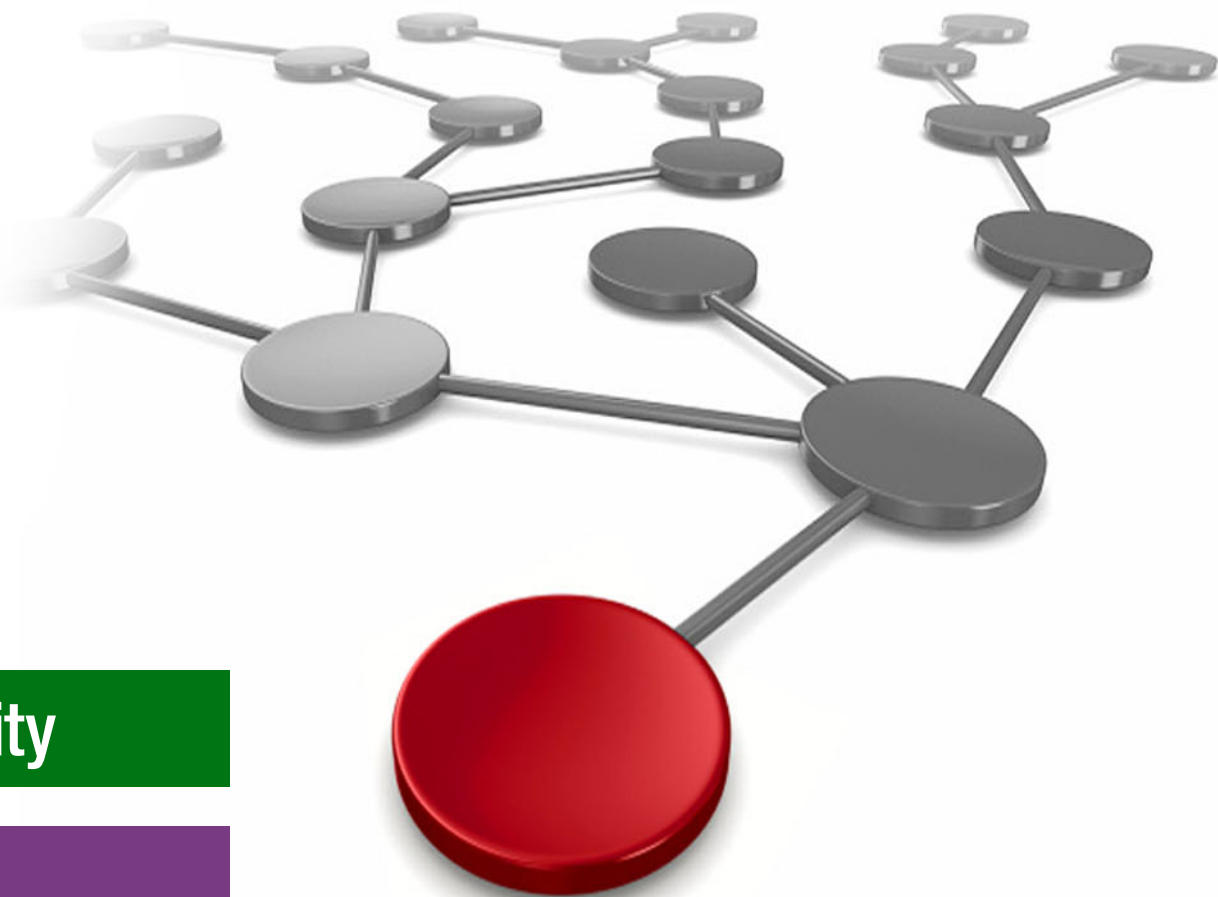
Michael Frankenberg

Eunice Liu

Connie Riggins

Mario Schreuer

Robert Tondini



 **Security**

Storage



IBM Redbooks

**IBM DS8000 Safeguarded Copy: Updated for DS8000
Release 9.3.2**

June 2023

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

Fifth Edition (June 2023)

This edition applies to IBM DS8900F storage systems with IBM DS8000 Licensed Machine Code (LMC) 7.9.3.0 (bundle version 89.30.xx.x), referred to as Release 9.3.

© Copyright International Business Machines Corporation 2018, 2023. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	vii
Trademarks	viii
Preface	ix
Authors	x
Now you can become a published author, too	x
Comments welcome	xi
Stay connected to IBM Redbooks	xi
Chapter 1. Introduction and concepts	1
1.1 The need to protect data	2
1.1.1 What is logical corruption	2
1.1.2 Regulatory requirements	3
1.1.3 Use cases for data protection	4
1.1.4 Requirements for logical corruption protection	5
1.2 IBM DS8000 Logical Corruption Protection capabilities	5
1.2.1 IBM DS8000 Logical Corruption Protection with FlashCopy	6
1.3 IBM DS8000 Safeguarded Copy	7
1.3.1 Safeguarded Copy concept	8
1.3.2 Safeguarded Copy Backup Capacity	9
1.3.3 Safeguarded Copy management software	10
1.3.4 Safeguarded Copy in HADR solutions and isolation methods	11
1.3.5 Creating backups by using Safeguarded Copy	13
1.3.6 Safeguarded Copy recovery	14
1.3.7 Safeguarded Copy restore to production with Global Copy incremental resync. .	17
Chapter 2. Planning and considerations	21
2.1 Information that is required to plan a Safeguarded Copy implementation	22
2.2 HA, DR, and HADR with Safeguarded Copy topologies	23
2.2.1 2-Site HADR and Safeguarded Copy topologies	24
2.2.2 3-site HADR and Safeguarded Copy topologies	30
2.2.3 4-site HADR and Safeguarded Copy topologies	35
2.3 Hardware and software prerequisites	38
2.4 Safeguarded Copy Management software	39
2.4.1 IBM Copy Services Manager	39
2.4.2 IBM GDPS LCP Manager	41
2.5 Safeguarded Copy sizing considerations	42
2.5.1 Safeguarded Copy key operational considerations	43
2.5.2 Safeguarded Copy Backup Capacity	44
2.5.3 Recovery and Safeguarded Copy source volumes	47
2.5.4 Safeguarded Copy capacity sizing methods	48
2.5.5 General Safeguarded Copy sizing considerations	54
2.6 Safeguarded Copy backup priority consideration in an out-of-space situation	55
2.7 Safeguarded Copy performance considerations	56
2.8 Monitoring Safeguarded Copy	57
2.8.1 Using IBM CSM for Safeguarded Copy session monitoring	58
2.8.2 Safeguarded Copy capacity warning messages for z/OS	62
2.8.3 DS8000 DS CLI and Storage Management GUI messages	63
2.8.4 Monitoring Safeguarded Copy capacity and automating Safeguarded Copy capacity	

dynamic expansion	63
2.8.5 Monitoring a DS8000 extent pool	66
2.9 Security considerations	69
2.9.1 More DS8000 security considerations and CSM “dual control”	70
2.10 Safeguarded Copy backup use case considerations	71
2.10.1 Data validation	72
2.10.2 Forensic analysis	73
2.10.3 Surgical recovery	73
2.10.4 Catastrophic recovery	73
2.10.5 Offline backup	75
2.11 Configuration changes considerations	76
2.11.1 Copy set management	76
2.11.2 Dynamic Safeguarded Copy Backup Capacity expansion	80
2.12 Safeguarded Copy considerations	81
Chapter 3. Capacity sizing by using the IBM Copy Services Manager ESESizer functions	83
3.1 Introducing the ESESizer	84
3.2 IBM Copy Services Manager ESESizer session overview and prerequisites	85
3.3 CSM ESESizer session preparation considerations	85
3.4 Preparing and configuring an ESESizer session for querying a DS8000 Write Monitoring Bitmap	87
3.4.1 Preparing CSM to query the DS8000 Write Monitoring Bitmap with the ESESizer session	87
3.4.2 Creating an ESESizer session	90
3.4.3 Configuring the ESESizer session	92
3.4.4 Managing the ESESizer session.	94
3.5 Capacity sizing based on the ESESizer output files	97
3.5.1 ESESizer output files content overview	97
3.5.2 ESESizer session properties settings for using Excel spreadsheets	99
3.5.3 Provided Excel spreadsheets	100
3.5.4 Excel spreadsheet calculations.	105
3.5.5 Excel spreadsheet volume-level Safeguarded Copy Solution Summary	107
3.5.6 Excel spreadsheet box-level Safeguarded Copy calculations	109
3.6 Safeguarded Copy capacity sizing overview and example	110
3.6.1 Safeguarded Copy capacity sizing overview.	110
3.6.2 Capacity sizing example for Safeguarded Copy	112
Chapter 4. Implementation and management.	117
4.1 Implementing a Safeguarded Copy environment	118
4.1.1 Configuring Safeguarded Copy Backup Capacity.	119
4.1.2 Creating a Safeguarded Copy session with IBM Copy Services Manager	125
4.2 Managing a Safeguarded Copy environment	129
4.2.1 Verifying and modifying the Safeguarded Copy session properties	130
4.2.2 Creating a Safeguarded Copy backup	136
4.2.3 Expiring a Safeguarded Copy backup	145
4.2.4 Recovering a Safeguarded Copy backup	148
4.2.5 Expanding Safeguarded Virtual Capacity	150
4.2.6 Other Safeguarded Copy-related Copy Services Manager operations.	152
4.2.7 Other Safeguarded Copy-related DS CLI and DS GUI operations	159
4.3 Restoring a Safeguarded Copy backup to production	160
4.3.1 Restoring a backup to production from H2 in an MM session.	162
4.3.2 Restoring a backup to production from H3 in an MGM session	168
4.3.3 Restoring a backup to production from H3 in cascaded GM sessions	176

4.3.4 Restoring a backup to production from H1 in an MM session.	187
4.3.5 Restoring a backup to production from H1 in a Multi-Target Metro/Global Mirror session	198
4.3.6 Restoring a backup to production for a Metro Mirror session with HyperSwap .	214
4.4 Scheduled tasks examples with Safeguarded Copy topologies	217
4.4.1 Metro Mirror with Safeguarded Copy	219
4.4.2 Global Mirror with Safeguarded Copy	220
4.4.3 Cascaded Global Mirror with Safeguarded Copy	221
4.4.4 Metro/Global Mirror (cascaded) with Safeguarded Copy	222
4.4.5 Multi-Target Metro Mirror-Metro Mirror with Safeguarded Copy	224
4.4.6 Multi-Target Metro Mirror-Global Mirror with Safeguarded Copy	225
Appendix A. Other Safeguarded Copy topologies.	227
Safeguarded Copy topologies	228
Abbreviations and acronyms	231
Related publications	233
IBM Redbooks	233
Other publications	233
Online resources	233
Help from IBM	233

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.

AIX®	Guardium®	Parallel Sysplex®
Db2®	HyperSwap®	QRadar®
DS8000®	IBM®	Redbooks®
Easy Tier®	IBM Cloud®	Redbooks (logo)  ®
FlashCopy®	IBM Spectrum®	Tivoli®
GDPS®	IBM Z®	z/OS®

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.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

Preface

This IBM Redpaper publication explains the IBM Storage DS8000® Safeguarded Copy functions. With Safeguarded Copy, organizations can improve their cyber resiliency by frequently creating protected point-in-time backups of their critical data, with minimum impact and effective resource utilization.

The paper is intended for IT security architects who plan and design an organization's cybersecurity strategy, and the infrastructure technical specialists who implement them.

The content is structured into four major sections:

- ▶ Safeguarded Copy introduction:
 - The need for *logical corruption protection* (LCP) and information about regulatory requirements.
 - The general concepts of LCP, and the use cases for recovery.
 - How Safeguarded Copy works, its design objectives, and new terminology.
 - Backup and recovery processes in general.
- ▶ Safeguarded Copy planning and considerations:
 - Hardware and software prerequisites.
 - Capacity planning and performance considerations.
 - Monitoring, alerting, and security.
 - Integrate Safeguarded Copy in your high availability (HA) and disaster recovery (DR) (HADR) solution.
 - Planning configuration changes.
- ▶ IBM Copy Services Manager (CSM) ESEsizer session.
- ▶ Safeguarded Copy implementation and management:
 - Prepare, set up, and run Safeguarded Copy.
 - Manage your Safeguarded Copy environment:
 - Run, schedule, and expire backups.
 - Recover and use backups.
 - Apply configuration changes.

This edition of the paper applies to DS8000 9.3.2.

IBM Storage rebranding: IBM® has recently rebranded its Storage Portfolio. For more details, see [Evolving the IBM Storage Portfolio Brand Identity and Strategy](#). With this new rebranding, IBM DS8900F became IBM Storage DS8900F. In this document, IBM Storage DS8900F is called IBM DS8900F or DS8900F.

Authors

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

Michael Frankenberg is a Certified IT Specialist in Germany and joined IBM in 1995. With more than 20 years of experience in high-end storage, he works in Technical Sales Support at the EMEA Storage Competence Center. His area of expertise includes performance analysis, establishing HADR solutions, and implementation of storage systems. He supports the introduction of new products and provides advice for IBM Business Partners, Technical Sales, and customers. He holds a degree in Electrical Engineering/Information Technology from University of Applied Sciences Bochum, Germany.

Eunice Liu has been working with IBM Z® platform since 2003. She started working with IBM Z platform as a System Programmer and has been focusing on IBM Z Storage Management in the last 10 years. As an IBM customer, Eunice has experience in various of IBM Z Software and Hardware including DS8000 and implementation of Safeguarded Copy backup.

Connie Riggins is a DS8000 Copy Services (CS) and CSM Subject Matter Expert with the DS8000 Product Engineering group. She started working at IBM in 2015. Before joining IBM, starting in 1991, Connie worked at Amdahl Corp. as a Systems Engineer and later at Softek Storage Solutions as Product Manager of TDMF for IBM z/OS®.

Mario Schreuer is a Senior Mainframe Consultant at IBM Platinum Business Partner SVA (System Vertrieb Alexander GmbH) in Germany. He has more than 15 years of experience on IBM Z and holds a degree in Cologne, Germany. His expertise covers a broad range of IBM products with a focus on z/OS and its subsystems. He was part of several international migration projects and is working with the DS8000 since over ten years.

Robert Tondini is an IBM Consulting IT Specialist in IBM Australia and New Zealand. He has 25 years experience in IBM enterprise storage for mainframe and open systems. He joined IBM in 2000 and since then he has been providing presales and implementation support for high-end disk, tape, and SAN fabric systems with HADR solutions. He co-authored several IBM Redbooks® publications and workshops for DS8000 systems.

Thanks to the authors of the previous editions:

Nick Clayton, Bert Dufrasne, Alexander Warmuth, Rick Pekosh, Mark Wells

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

Randy Blea, Theresa Brown, Craig Gordon, Peter Kimmel, Thomas Luther
IBM

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 ITSO 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:

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:

ibm.com/redbooks

- Send your comments in an email:

redbooks@us.ibm.com

- Mail your comments:

IBM Corporation, International Technical Support Organization
Dept. HYTD Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Look for 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>



Introduction and concepts

In this chapter, we describe what logical corruption is, which dangers it presents, and why many of current infrastructure measurements such as data replication and IBM HyperSwap® might not protect your data sufficiently against it.

Next, we explain the need for logical corruption protection (LCP), general concepts of LCP, and provide information about regulatory requirements.

Then, we focus on the *Safeguarded Copy* solution that the IBM DS8000 (starting with the DS8880) storage system provides to implement LCP. We list the design objectives and describe how Safeguarded Copy fits into the overall data protection solution portfolio of the DS8000.

Next, we describe some considerations about integration into existing high availability (HA) or disaster recovery (DR) solutions, and backup isolation.

Last, we explain some examples that are based on the functions of Safeguarded Copy, introduce some new terms, and describe the backup, recovery, and restore processes of Safeguarded Copy.

This chapter includes the following topics:

- ▶ 1.1, “The need to protect data” on page 2
- ▶ 1.2, “IBM DS8000 Logical Corruption Protection capabilities” on page 5
- ▶ 1.3, “IBM DS8000 Safeguarded Copy” on page 7

1.1 The need to protect data

For many years and with exponential growth, data has become one of the most important assets for most companies across all industries. Organizations are heavily affected if their data is lost or compromised, which makes data now as important as many natural resources. For that reason efficiently protecting data is essential for most businesses.

Over the last decades, most organizations concentrated on developing and implementing high availability and disaster recovery (HADR) solutions to protect their enterprise data against disasters such as hardware and software failures or data center outages. Nowadays companies become increasingly concerned about accidental or intentional logical corruption.

1.1.1 What is logical corruption

In the context of storing data, *logical* means that all hardware components are working as expected, but the data becomes destroyed or corrupted on a content or structural level. This form of corruption can range from deletion, selective manipulation up to encryption.

Logical corruption cannot be prevented with traditional HADR solutions since they are not content aware. In fact, continuous replication solutions such as the DS8000 Metro Mirror (MM) or Global Mirror (GM) that are often used for DR solutions quickly propagate any content level corruption to all copies. That is, because for the storage system, manipulating or encrypting data is just another I/O.

As an example, imagine a ransomware attack that encrypts one of your companies databases. A continuous replication of all I/Os ensures that also the database on the replication target is encrypted. From an infrastructural point of view, everything is fine and operational. However, because your database is now encrypted, you might not be able to access this data anymore on either your primary or DR site.

Therefore, a paradigm shift is needed from a pure availability mind-set to *cyber resilience* (CR). Cyber resilience aims at the ability of an organization to continue to operate with the least amount of disruption, despite cyberattacks and outages. Cyber resilience expands the scope of protection, covering both: cybersecurity and business continuity.

Recent incidents show that cyberattacks are rapidly growing in number and sophistication. Every few months, there are headlines in the news about attacks on enterprise data from ransomware, malware, insider threats, or other destruction of data. One prominent example is the Colonial Pipeline ransomware attack, which took place in May 2021.

This attack targeted the billing infrastructure of the company, leading to a halt of the whole pipeline operation. The Colonial Pipeline carries gasoline, diesel, and jet fuel from Texas to New York. About 45% of all fuel that is consumed on the US East Coast arrives through the pipeline system.¹ The attack resulted in fuel shortages at major airports and filling stations in several states of the US. US President Joe Biden declared a state of emergency 2 days after the ransomware attack. It is reported that the company paid a ransom of about \$5 million in exchange for a decryption tool. Five days after the attack, the pipeline was restarted.

This example is only one of many examples showing that protection against all forms of corruption becomes more important because in addition to hardware or software failures, corruption can also be caused by cyber attacks, inadvertent user errors, and malicious intent.

¹ "Ransomware Attack Shuts Down Massive East Coast Gasoline Pipeline" by Joe Walsh in Forbes, February 6, 2022

For best preparation against this logical corruption, a CR solution should cover the five major points, as shown in Figure 1-1.

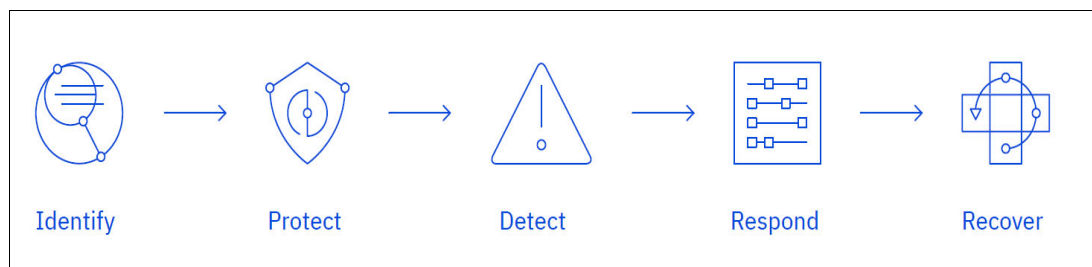


Figure 1-1 IBM Cyber Resilience Lifecycle

- ▶ Identify risks and vulnerabilities.
Pinpoint business-critical applications and their associated risks, analyze the potential business impact of disruption and assess business continuity and DR readiness.
- ▶ Protect your applications and data.
Safeguard business-critical applications and data before they are used by using air-gapped data protection and immutable storage technologies.
- ▶ Detect data corruption and configuration anomalies.
Quickly find changes in system configuration by using automated testing and verification of backed-up data to help trigger rapid response and reduce downtime.
- ▶ Respond to changes in configuration and data.
Address unauthorized changes in configurations and data by using a dashboard that provides real-time visibility into open vulnerabilities and recovery point objective (RPO) and recovery time objective (RTO) deviations.
- ▶ Recover access to critical applications and data.
Rebuild mission-critical business applications, restore data from air-gapped backup and rapidly and reliably recover IT systems from cyberincidents.

An important part of CR is to protect data and the ability to recover from a logical data corruption event. DS8000 Safeguarded Copy provides support to protect and recover data. For more information about the IBM Cyber Resilience Lifecycle, see [Cyber resilience: An important new role for storage](#).

1.1.2 Regulatory requirements

For some industries, such as finance or health care, data protection must conform with drastic regulations.

The US Federal Financial Institutions Examination Council (FFIEC), for example, published a revised *Business Continuity Planning Booklet*, which is part of the FFIEC's *Information Technology Examination Handbook* for the US financial industry.

In Appendix 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.”²
- ▶ “...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.”²

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.”³

In 2019, the EBA wrote in the *Guidelines on ICT and security risk management*:

“... cyberattacks can render common risk management and business continuity arrangements ineffective (for example, DR procedures), and they might in some instances fuel the spread of malware and corrupted data to back up systems.”⁴

For organizations from affected industries, such statements increase the demand to implement solutions that protect against logical corruption. The IT industry is sought after to help their customers to design and implement solutions that meet these requirements.

1.1.3 Use cases for data protection

Because a corruption event might be triggered by a wide range of causes, an LCP solution should cover many different scenarios: from application corruption to user error through inadvertent or malicious destruction of data and to ransomware attacks where data might be encrypted by an attacker.

Typical use cases for protection copies include the following options:

- ▶ Validation

Regular data analysis enables early detection of a problem or reassurance that a specific protection copy is uncorrupted. Performing corruption detection and data validation processes against a copy of data might be more practical than doing these tasks in a live production environment.

- ▶ Forensic analysis

If a data corruption is detected, but systems are still operational, the first step is a forensic analysis. You determine what data is corrupted, when the corruption occurred and which of the available protection copies is the last good one. You also decide whether you can fix the corruption from within the production environment or whether one of the following recovery methods is required.

- ▶ Surgical recovery

You perform surgical recovery to recover only specific parts of the production data from a backup copy. It can be a fast and safe method if only a small portion of the production data is corrupted and if consistency between current production data and the restored parts can be reestablished. A surgical recovery is also needed when the last known good backup copy is too old to restore the complete environment. In this case, you might want to leave most of the production volumes in their present state and copy only replacement data to correct corrupted data.

² FFIEC “Business Continuity Planning Booklet Appendix J”, found at:
https://www.ffiec.gov/press/pdf/ffiec_appendix_j.pdf

³ NAIC “Principles for Effective Cybersecurity: Insurance Regulatory Guidance”, found at:
http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf

⁴ EBA “Guidelines on ICT and security risk management”, found at:
<https://eba.europa.eu/sites/default/documents/files/documents/10180/2522896/32a28233-12f5-49c8-9bb5-f8744ccb4e92/Final%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf>

- Catastrophic recovery

If the corruption is extensive, or if the latest known good protection copy is current enough, the easiest way might be to restore the entire environment to a point in time that is known to be unaffected by the corruption.

- Offline backup

Performing an offline backup of data from a consistent point-in-time copy can be used to build a second line of defense, providing a greater retention period and increased isolation and security.

Note: Because the *offline backup* use case is similar to regular backup methods, it is out of the scope of this book.

1.1.4 Requirements for logical corruption protection

As discussed earlier in this chapter, traditional HADR solutions cannot provide complete protection against content-level destruction of data. Different approaches for data protection are required to provide this kind of protection. The major design requirements for LCP include the following characteristics:

- Granularity: Creation of multiple protection copies to minimize data loss if a corruption incident occurs.
- Isolation: Isolation of the protection copies from the active production data so that it cannot be corrupted by a compromised host system (this situation is also known as an *air-gap*).
- Immutability: Protection of the copies against unauthorized manipulation.

1.2 IBM DS8000 Logical Corruption Protection capabilities

The DS8000 family of data storage systems provides a wide range of data protection capabilities, mostly based on the proven IBM FlashCopy® and Peer-to-Peer Remote Copy (PPRC) technologies. However, these technologies were not designed for today's LCP demands. The Safeguarded Copy function is introduced to fill this gap.

In the next chapter, we are describing how to implement an LCP solution by using the FlashCopy Technology. This implementation also is a good example to explain the basic concepts of LCP.

In the following chapters, we are going to show the advantages of Safeguarded Copy over using FlashCopy for LCP and explain the Safeguarded Copy in more detail.

Note: In Cyber Resilience Lifecycle, the Safeguarded Copy function provides the capability to protect data and recover from protected copies. All other major points, such as identify risks, detect data corruption, validate data, and respond to changes are not part of the DS8000 Safeguarded Copy function.

In addition to the data validation and restore capability, it is important for a Cyber Resiliency solution to detect a cyberattack or insider threat. Therefore, implementing a solution that helps to detect a data corruption, such as IBM Guardium® or IBM QRadar® is also important.

1.2.1 IBM DS8000 Logical Corruption Protection with FlashCopy

The DS8000 family of storage system provided capabilities for LCP, even before the introduction of Safeguarded Copy. In most cases where customers created LCP solutions, the FlashCopy technology was used to provide the protection copies.

Figure 1-2 shows a model configuration that uses FlashCopy that can be used to explain the concepts of DS8000 LCP.

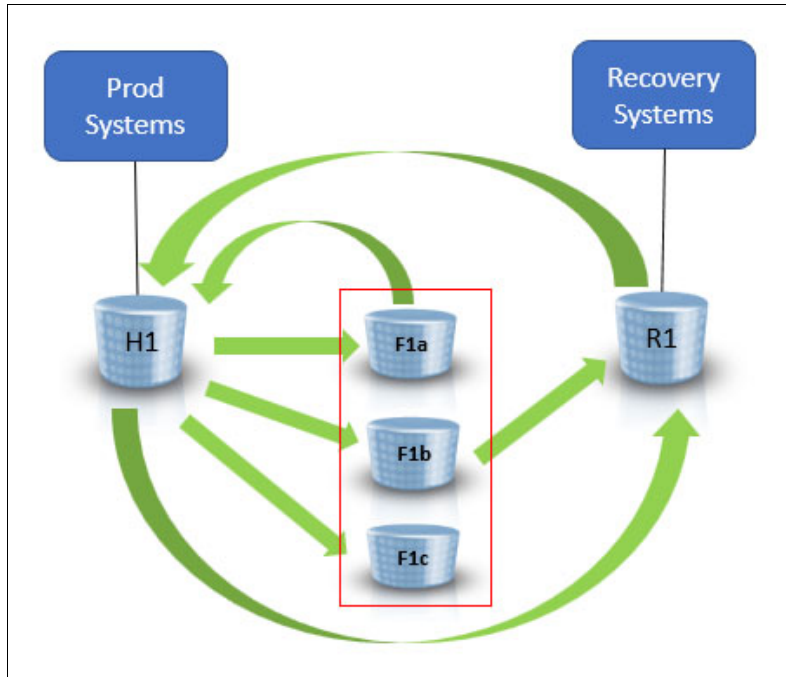


Figure 1-2 Model configuration for DS8000 LCP

The active production data to be protected is on volume H1.

Within a defined time interval, multiple FlashCopy copies (F1a, F1b, and F1c) are created from the source volume H1. These FlashCopy copies provide the recovery points. From these recovery points, the following actions can be performed:

- Recover to recovery volume R1 by creating a new, forward-cascaded, FlashCopy relation.
- Restore to the original volume H1 by using the FlashCopy reverse function.

Important: Theoretically, the FlashCopy targets that provide the recovery point can also be used directly by a host system. However, this use can contradict the goal to protect the security copies from being corrupted.

Restoring from one of the recovery points (F1a, F1b, or F1c) to the original volume H1 provides a fast way to restore the whole volume to a specific time (determined by the time you took a FlashCopy recovery point; namely F1a, F1b, or F1c).

However, before overriding the original volume with the most recent data you might want to perform the following tasks first:

- ▶ Determine which part and how much of your data became corrupted.
- ▶ Obtain which point in time is the latest one that is not corrupted yet.
- ▶ Develop a strategy to merge as much uncorrupted data as possible that is on H1 with the older backup (F1a, F1b, or F1c) that replaces the corrupted part. The main focus is on maintaining data consistency.

For these analytical steps, a recovery volume and an independent recovery system become useful. It allows a differentiated approach to minimize the impact of the recovery (for more information, see 1.1.3, “Use cases for data protection” on page 4):

Validation	Use the recovery volumes to perform regular analysis of the copies to provide early detection of a problem or reassurance that the copy is a good copy before further action.
Forensic analysis	Use the recovery volumes to investigate the problem and determine what the recovery action is.
Surgical recovery	Extract data from the copy on the recovery volumes and logically restore back to the production environment.
Catastrophic recovery	Recover the entire environment to the point in time of a backup.

Tip: Starting with release 4.1, IBM Geographically Dispersed Parallel Sysplex® (IBM GDPS®) provides an integrated LCP function that is based on FlashCopy.

Because FlashCopy was originally designed with other objectives in mind than LCP, it has some characteristics that do not fit ideally for this purpose:

- ▶ It is limited to 12 relations per source volume, which allows for a maximum of 10 targets (point-in-time copies), if a concept (as shown in Figure 1-2 on page 6) is used.
- ▶ FlashCopy targets are regular volumes. Therefore, they can be accessed by hosts and potentially be modified. Also, target volumes use DS8000 device numbers, which are overall limited. For the DS8000, the limit is 65280.
- ▶ FlashCopy relations and targets can be deleted by the DS8000 administrator.
- ▶ Source volumes with multiple targets can suffer from a write performance impact because all targets are maintained individually.

To overcome these limitations and target the requirements for LCP, Safeguarded Copy was introduced with IBM DS8880 8.5 and DS8900F 9.0.

1.3 IBM DS8000 Safeguarded Copy

The Safeguarded Copy was developed to meet the specific needs of LCP. The most important features that distinguish it from the previously introduced method that uses FlashCopy for LCP are:

- ▶ Allow creation of many recovery copies across multiple volumes or storage systems with optimized capacity usage and minimum performance impact (the current limit is 500).
- ▶ Enable any previous recovery point to be made available on a set of recovery volumes while the production environment continues to run.

- ▶ Does not use DS8000 device numbers and host device addresses (UCBs in mainframe environments).
- ▶ Enhanced Security Protection for the Safeguarded Copies to prevent them from being accidentally or deliberately compromised.

Safeguarded Copy does not replace FlashCopy and both technologies remain relevant in LCP scenarios. FlashCopy provides an instantly accessible copy of production volumes and for multiple FlashCopy copies each copy is independent from the others from a data perspective.

In the following chapters the Safeguarded Copy concepts, features and functions are explained in more detail.

1.3.1 Safeguarded Copy concept

Safeguarded Copy provides functions to create multiple recovery points for a volume that you want to protect (which is also referred to as a *Safeguarded Copy source*, or *source* in this publication). These recovery points are called *Safeguarded Copy backups* (also referred to as *backups*).

Unlike with FlashCopy, the recovery data is not stored in separate regular volumes, but in a storage space that is called *Safeguarded Copy Backup Capacity*. The backups are not directly accessible by a host.

The backup data can be used only after its recovery, which can be done only on a separate recovery volume, which provides extra protection to keep the backup volumes from being compromised.

A recovery directly onto the Safeguarded Copy source volume is not possible.

Figure 1-3 on page 9 shows the basic relations within a Safeguarded Copy configuration.

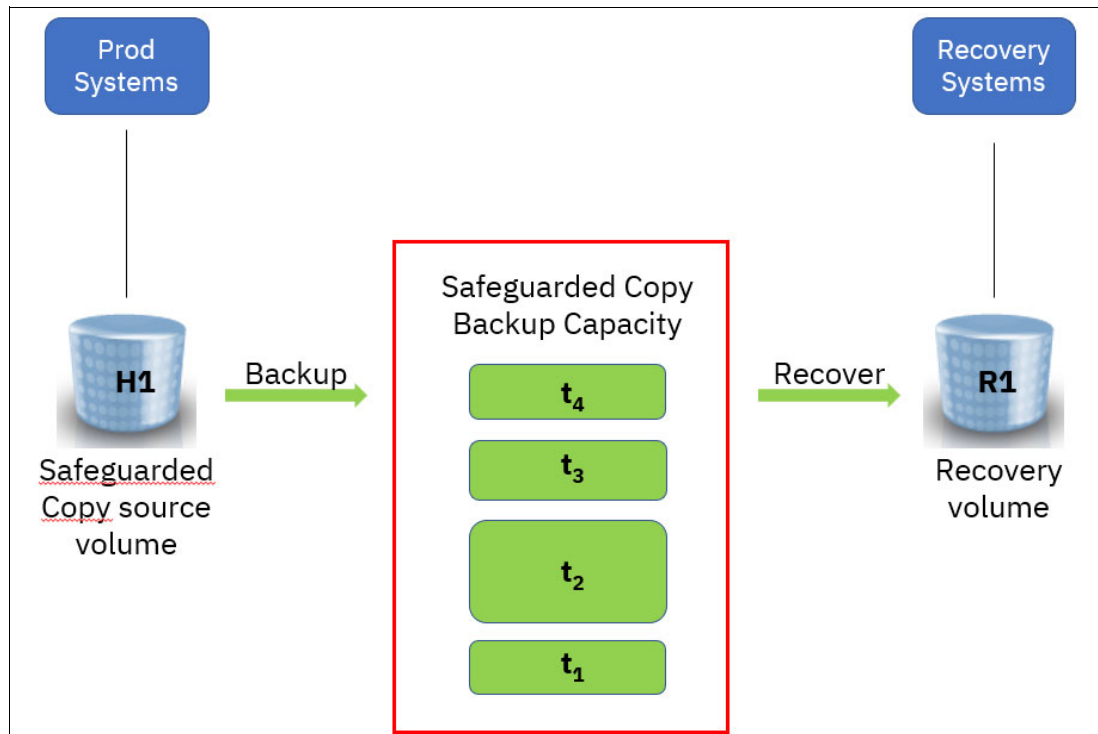


Figure 1-3 Safeguarded Copy basic relationship

When a Point-In-Time copy is recovered to a Recovery volume, you can access this volume by using your Recovery system. This system might not be identical to your production system, depending on your security requirements.

Recovering data from a recovery to a production volume can be done in many ways. Global Copy and Global copy incremental being two of them.

Using the **Restore Backup** action is supported, but has certain prerequisites. For more information, see 4.3, “Restoring a Safeguarded Copy backup to production” on page 160.

Section 1.3.6, “Safeguarded Copy recovery” on page 14 and the following sections describe how the recovery process works.

1.3.2 Safeguarded Copy Backup Capacity

The Safeguarded Copy Backup Capacity is the storage space where the backup data is stored. It is not directly accessible by the host.

The Safeguarded Copy Backup Capacity is always thin-provisioned. For best efficiency, we recommend that you use small extents.

Without any Safeguarded Copy backups, the Safeguarded Copy Backup Capacity is pure virtual capacity, which is also known as *Safeguarded Virtual Capacity*, which is associated with the source volume.

Physical storage space is allocated as you create backups and data that is overwritten in the original volume is saved in this backup. Backup data is saved with track granularity (64 KiB for Fixed Block (FB), approximately 55.3 KiB for Count Key Data (CKD) storage), which leads to a better efficiency than with FlashCopy.

Note: The Safeguarded Copy Backup Capacity is allocated in extents, but data is stored with track granularity. At least one extent is allocated for each Safeguarded Copy backup.

You specify the maximum amount of Safeguarded Virtual Capacity for each volume that you want to back up during the configuration of the Safeguarded Copy function in the Storage Management GUI or DS Command-line Interface (DS CLI) by defining the Backup Capacity Multiplier per volume. When this multiplier is reached, the oldest backups are removed automatically to free up space.

If a Safeguarded Copy backup exists for a volume, you cannot delete its associated Safeguarded Copy Backup Capacity. If a storage pool runs short on physical space, regardless of whether it is for backup or production data, the DS8000 sends notifications according to the pool settings, and might roll off the oldest backup on a volume-level basis.

For more information about capacity management for Safeguarded Copy, see 2.5.2, “Safeguarded Copy Backup Capacity” on page 44.

Extents that are physically allocated as Safeguarded Copy Backup Capacity are *not* monitored by IBM Easy Tier®. After data is written, Safeguarded Copy backup data normally is not accessed at all.

1.3.3 Safeguarded Copy management software

It is a key element of LCP that your backups are protected against unintentional or intentional tampering.

For that reason, there is a strict separation between what the DS8000 administrator and the Safeguarded Copy backup administrator can do regarding Safeguarded Copy backups.

To improve security, it is as best practice to have role and personal separation between the DS8000 administrator who can change the logical configuration and a Safeguarded Copy backup administrator.

The DS8000 administrator can use only the DS8000 management interfaces to prepare the Safeguarded Copy copies. These interfaces cannot be used to create, delete, or recover backups manually.

These tasks can be performed only by an administrator of either an instance of IBM Copy Services Manager (CSM) or IBM GDPS LCP Manager (GDPS LCP). For more information about management software requirements, see 2.4, “Safeguarded Copy Management software” on page 39.

Tip: If GDPS or CSM is already used in your environment for HADR configuration management, it is good practice to use the same solution to manage Safeguarded Copy.

Both management tools (CSM and GDPS LCP) manage the lifecycle of the Safeguarded Copy backups and make management easy and secure. They can perform actions such as create backups, recover backups, restore backups to production volumes, and manage the expiration (removal) of those backups that are no longer required in your safeguarded environment.

In addition, both management tools support restore a backup to production volumes (introduced in DS8900F 9.2) by using a Global Copy incremental resync from recovery to production volumes.

Also, a production environment can consist of hundreds or thousands of volumes across one or more storage systems. One of the most important aspects for LCP is to provide recovery points that are consistent across all volumes that are part of a backup. We call such a recovery point a *Consistency Group* (CG). CSM and GDSP LCP make sure that your backups are consistent.

For more information about various operations that are based on the IBM CSM, see Chapter 4, “Implementation and management” on page 117.

1.3.4 Safeguarded Copy in HADR solutions and isolation methods

This section describes the following topics:

- ▶ Existing HADR solutions
- ▶ Virtual and physical isolation

Existing HADR solutions

You can combine Safeguarded Copy with any supported HADR solution, such as 2-, 3-, or 4-site, with or without IBM HyperSwap. However, consider the following important factors:

- ▶ Consistency: Whenever you want to create a Safeguarded Copy backup, you must ensure that the set of original volumes is consistent. This condition might require more steps that must be performed before creating the backup.
- ▶ Management: You can continue to use your existing management solution for your HADR configuration (although you must use the IBM CSM or the GDPS LCP Manager to manage the Safeguarded Copy configuration and operations). However, it is highly recommended to use the same management solution for the management of your HADR solution and for the Safeguarded Copy management. Using different management solutions makes the handling way more complex and error prone, since there is no coordination between CSM and GDPS. This situation can lead to unpredictable results if, for example, you are using CSM for Safeguarded Copy management, and GDPS/GM for DR management and you do not suspend GM before taking a Safeguarded Copy backup with CSM. In this constellation, you must suspend the GM session first. Because the recommended way to suspend a GM session is to use GDPS and GDPS does not communicate with CSM, this situation is where it gets tricky. You must coordinate these activities between GDPS and CSM and ensure that operations do not become mixed up. Because of this complexity, we emphasize that you use the same management solution for Safeguarded Copy as for HADR.

For more information about and examples of combining HADR topologies with Safeguarded Copy, see 2.2, “HA, DR, and HADR with Safeguarded Copy topologies” on page 23.

Virtual and physical isolation

Just as you have a range of different topologies for HADR, depending on the protection that is required, you also can consider different topologies for IBM Cyber Resilience solutions. The first decision for many organizations is whether they create an environment with physical isolation from production for their protection copies, or whether virtual isolation on existing storage systems is considered sufficient.

For virtual isolation, you create the protection copies on one or more of the storage systems in your existing HADR topology. Figure 1-4 shows synchronous replication being used for HADR with the protection copies being created on one of the production storage systems where each physical storage box is represented by a blue frame.

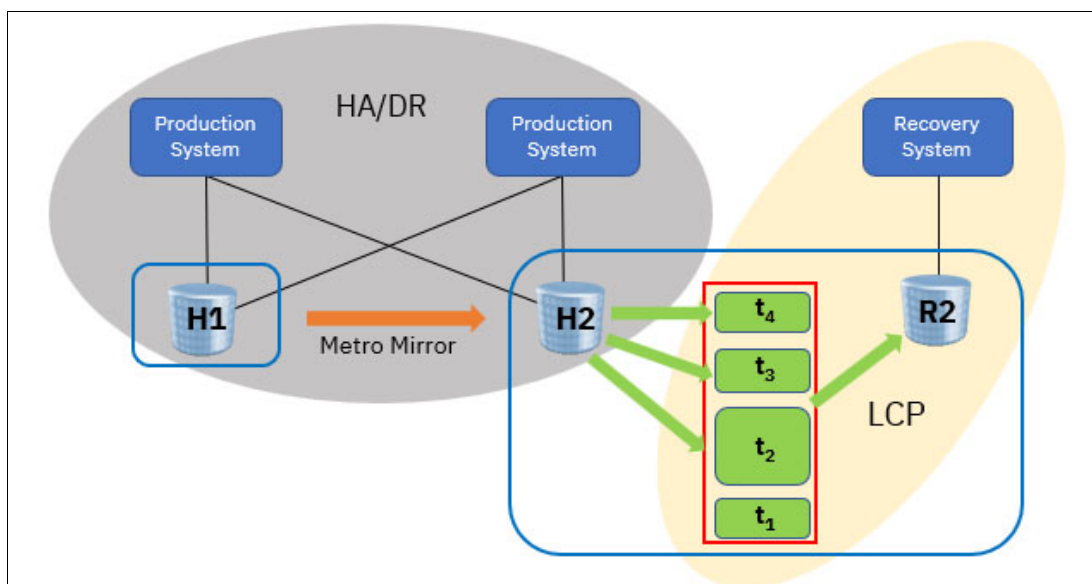


Figure 1-4 Example for Safeguarded Copy with virtual isolation

For physical isolation, you need more storage systems for the protection copies. These storage systems are typically not in the same SAN or IP network as the production environment. The systems feature restricted access, even with different administrators to provide separation of duties. Figure 1-5 shows an example of such an environment, where each blue frame represents one physical storage box.

We use the same HADR configuration as in the previous example. However, the protection copies are placed outside of this configuration. Data is replicated to the isolated storage system by using GM.

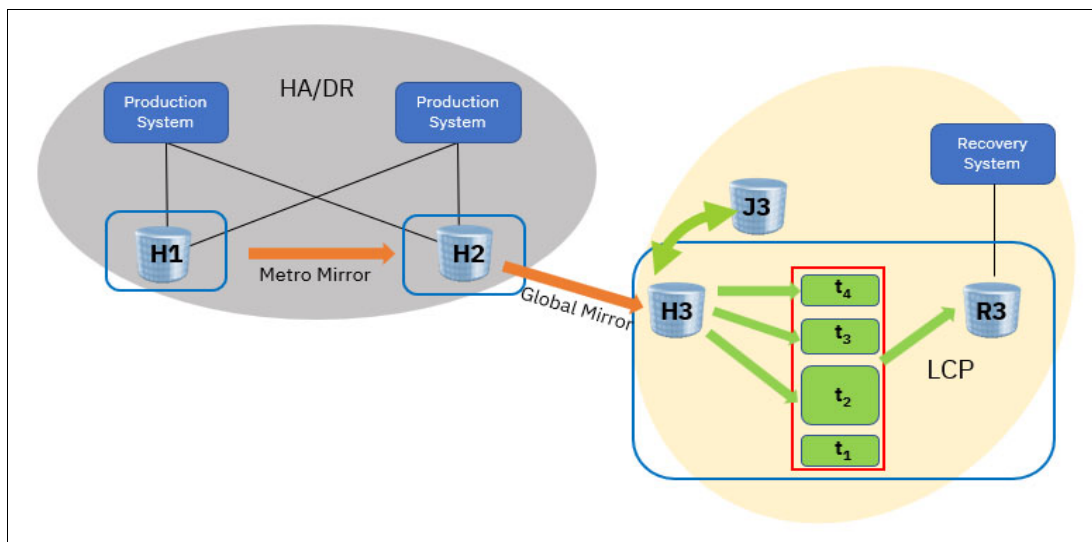


Figure 1-5 Example for Safeguarded Copy with physical isolation

For more information about HADR topologies and virtual / physical isolation, see 2.2, “HA, DR, and HADR with Safeguarded Copy topologies” on page 23.

1.3.5 Creating backups by using Safeguarded Copy

As described in 1.3.3, “Safeguarded Copy management software” on page 10 the tasks of creating, deleting, or recovering is done with CSM or GDPS LCP.

Therefore, you must trigger the creation of backups through one of these software products.

When a Safeguarded Copy backup is started, the DS8000 creates a CG. The DS8000 sets up metadata and bitmaps to track updates to the Safeguarded Copy source volume. After the backup is set up, the DS8000 copies data that will be overwritten by host I/O from the Safeguarded Copy source volume to a *Consistency Group Log* within the Safeguarded Copy Backup Capacity.

Note: Because consistency is created within the storage systems, which are not content-aware, the maximum level that can be achieved is crash consistency, which means that in a recovery, you might have to perform operating system or application recovery.

When the next backup is started, the DS8000 closes the previous one and creates a CG. Therefore, it does not have to maintain each backup individually.

To restore to a certain recovery point, the DS8000 needs all backups that are younger than the one to recover. Figure 1-6 shows the way Safeguarded Copy saves backup data.

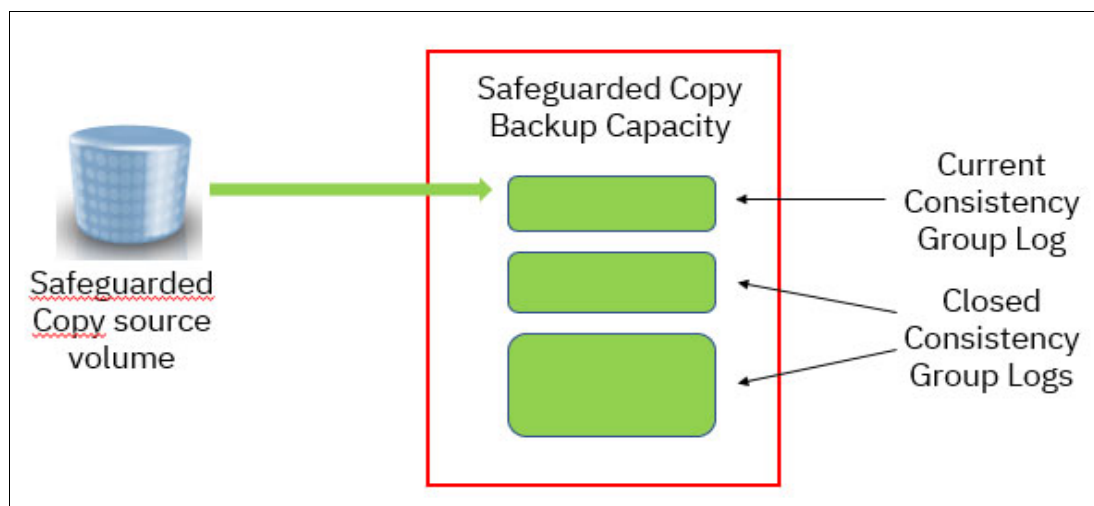


Figure 1-6 Safeguarded Copy backups that use Consistency Group Logs

To minimize the effect of creating a CG, the Safeguarded Copy backup process consists of the following steps:

1. **Reservation:** In this step, the DS8000 prepares to create a Safeguarded Copy backup. It sets up the required bitmaps and prepares the metadata in the Safeguarded Copy Backup Capacity. It also makes sure that all changed data from the previous backup is stored in its Consistency Group Log. After all preparations are done, the CG formation can occur.
2. **Check in:** To create a CG, the DS8000 must stop all updates for all volumes within the CG for a short period. It does this task by presenting an Extended Long Busy (ELB) state. When the data in cache is consistent, the previous Consistency Group Logs of all affected volumes are closed and consistent. From now on, the DS8000 writes further backup data into the Consistency Group Logs of the new backup.
3. **Completion:** The DS8000 lifts the ELB and write operations can continue.

The management software (CSM or GDPS LCP) coordinates and performs these steps automatically and with minimum effect on the host operations.

Note: Expect the effect of the ELB timeout on host writes to be less than when FlashCopy with the CG option is used. The latest enhancements in CSM and the DS8000 reduce the ELB timeout. In z/OS environments, the enhancements in CSM 6.2.11 with the IOS APAR OA59561 also improve the performance and reduce the ELB timeout during the creation of a Safeguarded Copy backup.

1.3.6 Safeguarded Copy recovery

You can recover from any Safeguarded Copy backup to a separate recovery volume. This recovery volume can be accessed from a Recovery System for validation.

However, recovering from a Safeguarded Copy backup directly to a Safeguarded Copy source volume is not possible. To understand the actions that must be taken to restore a corrupted production volume, see 1.3.7, “Safeguarded Copy restore to production with Global Copy incremental resync” on page 17.

The recovery volume must have at least the same capacity as the Safeguarded Copy source volume. It can be thin-provisioned. The recovery can be performed with background copy or without background copy. Typically, you specify **nocopy** if you need the recovered data only for a limited period and **copy** if you intend to use it for a longer period. You can start a Safeguarded Copy recovery exclusively through CSM or GDPS LCP.

We use the following example (see Figure 1-7 on page 15) to explain how the recovery process works.

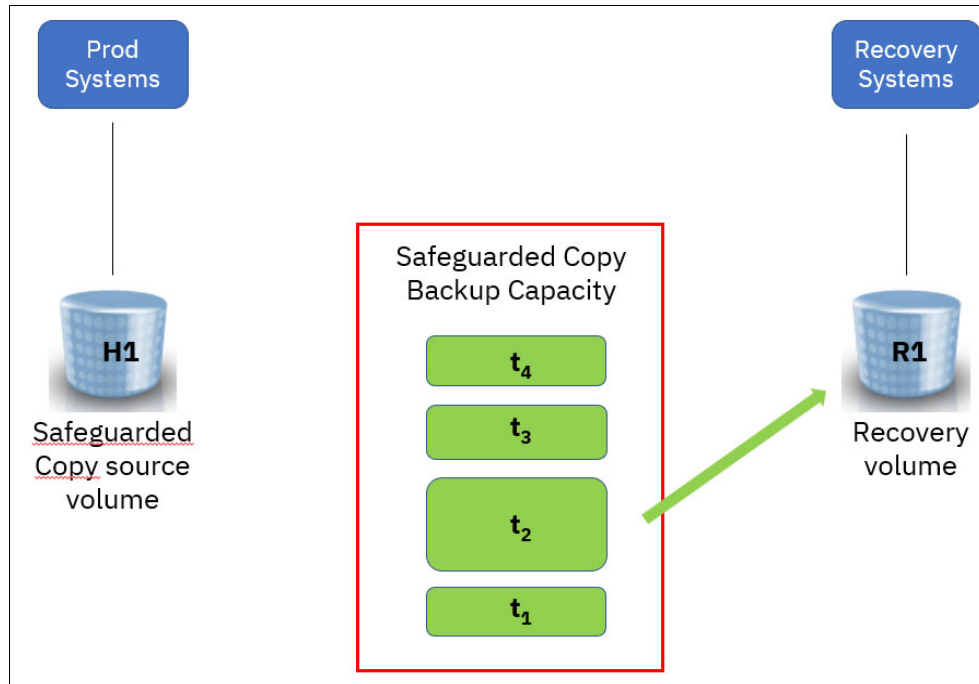


Figure 1-7 Example to explain Safeguarded Copy recovery

You have a Safeguarded Copy configuration with the Safeguarded Copy source volume H1, the Recovery volume R1, and four Safeguarded Copy backups (t_1 - t_4 , with t_4 being the most recent one) representing four recovery points. You want to recover to point in time t_2 with the **nocopy** option.

The recovery consists of two steps and is shown in Figure 1-8:

1. The DS8000 establishes a FlashCopy from H1 to R1, which makes R1 identical to H1.
2. The DS8000 then creates a recovery bitmap that indicates all data that was changed since t_2 and must be referenced from the Consistency Group Logs t_4 , t_3 , and t_2 , rather than from H1.

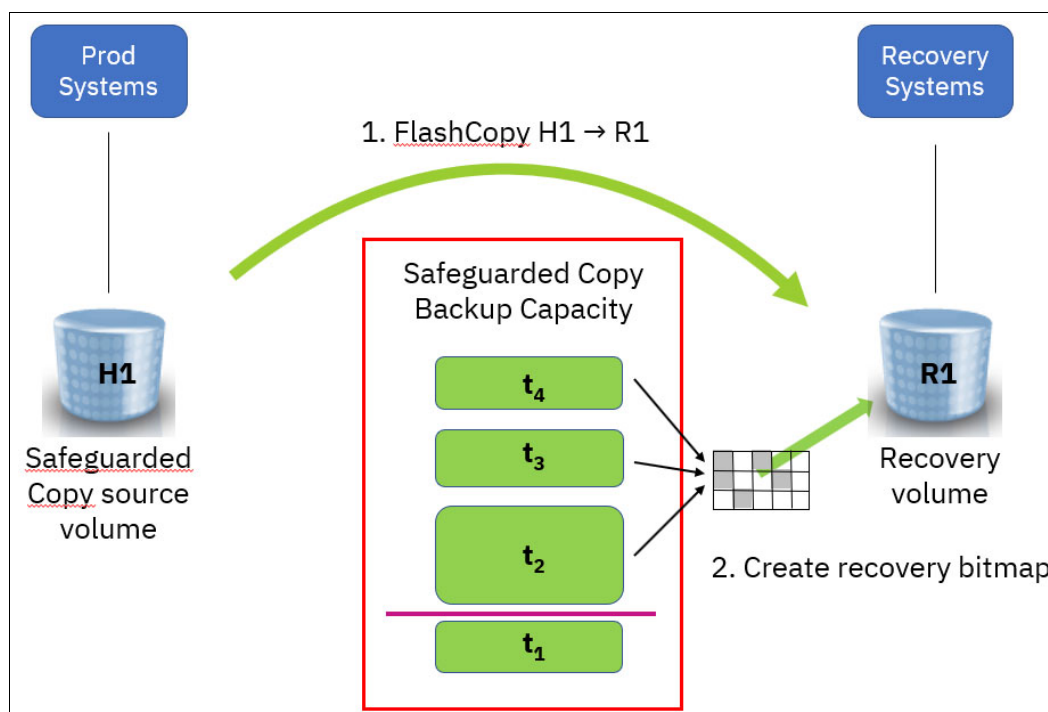


Figure 1-8 Safeguarded Copy recovery data flow

From this point, you can do read/write access to R1. If the recovery system reads data from R1, the DS8000 examines the recovery bitmap, and decides whether it must fetch the requested data from H1 or from one of the Consistency Group Logs. If the same track shows up in more than one backup, it must use the “oldest” instance (the one closest to recovery point t_2).

If the recovery system writes to R1, we distinguish two cases:

- Full track write: the DS8000 can write directly to R1 without considering existing data.
- Partial track write: the DS8000 must fetch existing data first (according to the rules) and can then apply the update.

If you perform the recovery with background copy, the DS8000 copies all data from H1 and the CGs to R1 in the background, following the same rules. You can access R1 at any time while the background copy is still running.

Note: You can continue to create backups, even while a recovery is active and in use.

If you want to restore data to the original volume H1, you first must recover the data to the recovery volume R1. After the recovered data is validated from the recovery system, you have two choices:

- ▶ **Selective restore:** Make the production volume H1 available to the recovery system, or make the recovery volume R1 available to the production system. Then, you can use standard operating system or application methods to copy the data that you need from the recovery volume R1 to the production volume H1.
- ▶ **Full volume restore:** You can use Global Copy to replicate the data from the recovery volume R1 to the production volume H1. The production volume H1 can be on the same or a different DS8000 as the recovery volume. For more information about how to perform a faster incremental resync by using Global Copy rather than a Global Copy full copy, see 1.3.7, “Safeguarded Copy restore to production with Global Copy incremental resync” on page 17.

1.3.7 Safeguarded Copy restore to production with Global Copy incremental resync

In 1.3.6, “Safeguarded Copy recovery” on page 14, we explained how to recover a volume from the Safeguarded Copy source and the Safeguarded Copy backup to a recovery volume. Then, we explained what choices you can use to bring parts or the whole recovery volume back to your production data.

In this section, we want to show the benefits of using Global Copy incremental resync to restore a recovered backup on to productions volumes in an MM environment with virtual isolation.

The Global Copy incremental resync feature is helpful in a catastrophic event that causes a corruption of a larger amount of data.

As a prerequisite for this function, the Safeguarded Copy source volumes must be on a DS8900F system with microcode release 9.2 or later. Also, the management software (CSM Rel. 6.3.0 or later or GDPS 4.4 SPE or later) must be implemented to support the function. The incremental resynchronization is supported only if all volumes in a PPRC relationship are defined in a Safeguarded Copy session. Restore to production with incremental resync is not supported, if only a subset of the PPRC volumes in a relationship is protected with Safeguarded Copy.

Note: The incremental resync function to restore a Safeguarded Copy backup to the production environment is not supported if the Safeguarded Copy source volumes are in the simplex state, that is, the volumes are not in a PPRC relationship.

Using Global Copy incremental resync between the recovery volume and the production volume for restoring the data can reduce dramatically the time that it takes to restart a production environment that is based on a Safeguarded Copy backup. With this function, no Global Copy full copy is required; therefore, fewer data tracks must be copied in a recovery from a logical corruption. This function performs an incremental resync from the DS8000 that hosts the Safeguarded Copy source volume to another DS8000 system, potentially at a remote site.

Note: This feature does not support an incremental resync from the recovery volume (R1) directly to the Safeguarded Copy source volume.

The entire restore to production process is managed by CSM Rel. 6.3.0 or later or GDPS 4.4 SPE or later.

We use a virtually isolated MM environment as an example to explain the required steps (see Figure 1-9).

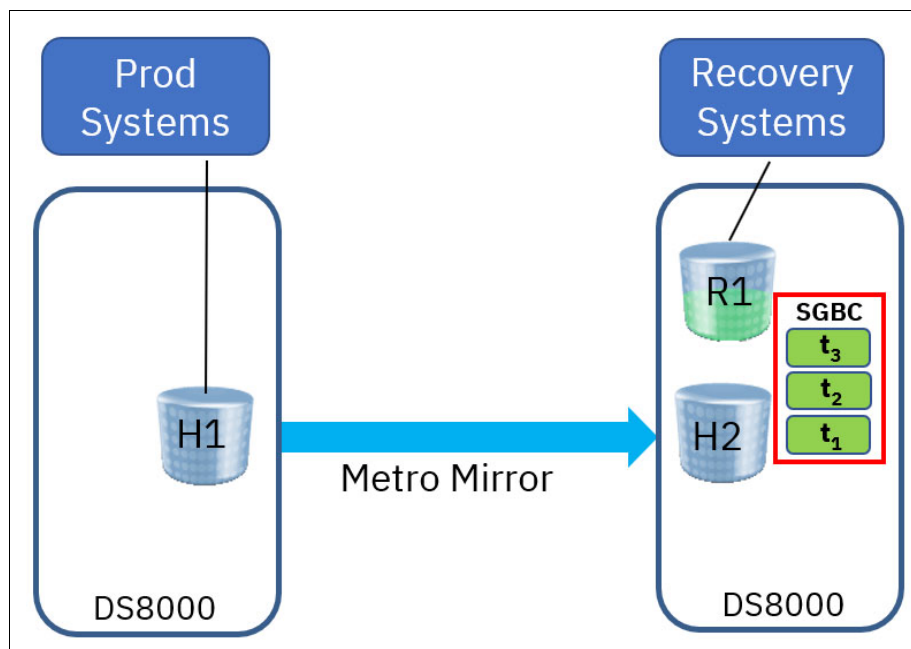


Figure 1-9 Virtual isolation example for Restore to production description

Incremental resync also supports other virtually and physically isolated topologies. For more information about virtual and physical isolation, see Chapter 2, “Planning and considerations” on page 21.

For incremental resync to production, the DS8000 creates and maintains out-of-sync (OOS) bitmaps that track changes between the recovery volumes (R1) and the production volumes (H1).

Compared to a regular Safeguarded Copy recovery action that is done for recurrent data validation purpose, the restore to production function requires some preparation.

To prepare for an incremental Global Copy restore to production of a validated Safeguarded Copy backup, complete the following steps:

1. Stop the production applications and shut down the production system.
2. Suspend the replication relationships.
3. Verify that the recovery volumes are not in another replication relationship.

In our example, after completion of these steps, the MM is suspended and the OOS bitmaps are prepared on H1 and H2 volumes, as shown in Figure 1-10 on page 19.

Note: The second OOS bitmap on H2 that is shown in the Figure 1-10 on page 19 allows a Multi-Target (MT) relationship.

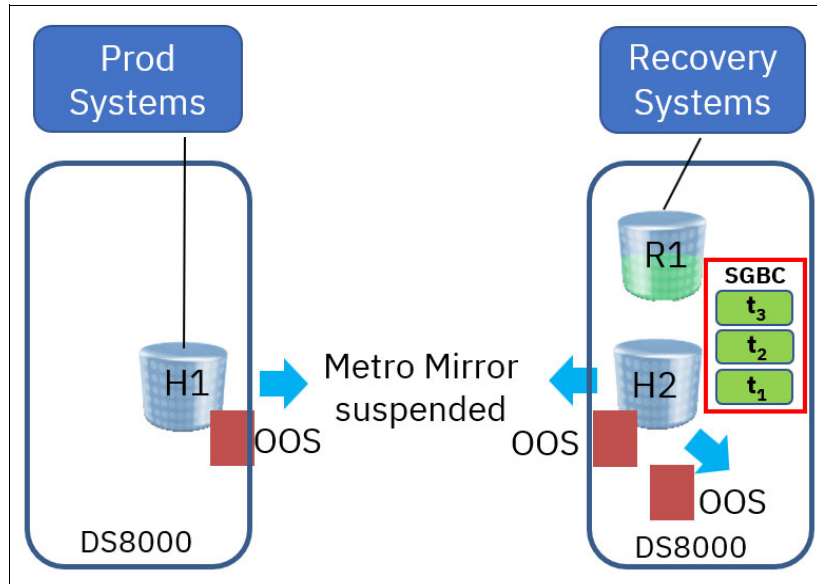


Figure 1-10 Example Metro Mirror environment after preparation steps are done

Now, by using your management solution (CSM or GDPS LCP), you can issue a **Recover Backup** command for a specific Safeguarded Copy backup (for example, t_2).

Then, a relationship is created between H2 and R1, including the data from the selected Safeguarded Copy backup (for example, t_3 and t_2).

If you are sure that you want to restore this specific Safeguarded Copy backup from R1 to H1, you can issue a **Restore Backup** action with your management solution (for example, CSM). This process prepares the OOS bitmap in the DS8000 for all R1 volumes.

The bitmap preparation on the R1 volumes can take some time because the Safeguarded Copy logs (tx) are scanned for the updated tracks. After that task is completed, a Global Copy relationship between R1 and H1 is established, and a failback command is issued to merge the bitmaps of H1. Next, R1 starts copying the changed data from R1 to H1 (see Figure 1-11).

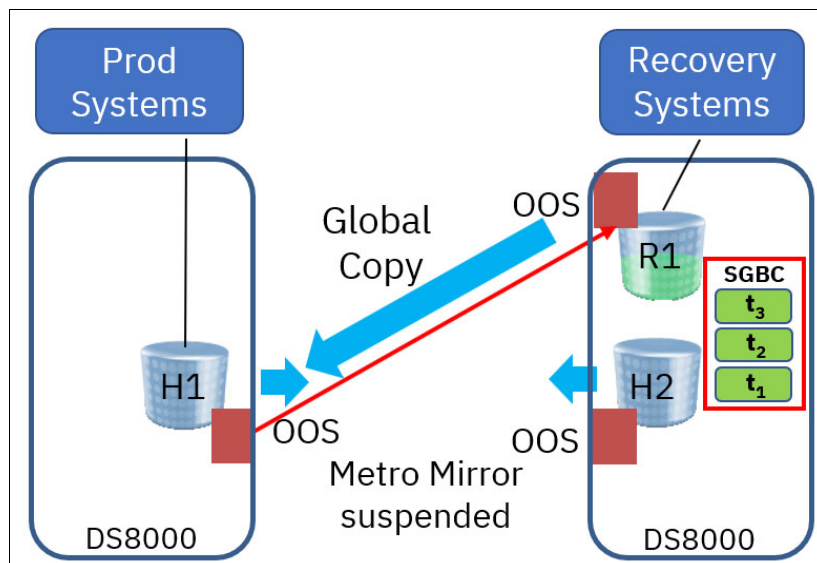


Figure 1-11 Metro Mirror environment example: Copying changed data to H1

After the changed data is copied from R1 to H1, the management software ends the R1 - H1 relationship. Now, you can do validation testing to verify that the data on H1 is okay.

After you verify that the data on H1 is correct, and you are sure that you do not want to fall back to H2, you can manually resynchronize the MM H1 to H2 relationship. That action copies all changes from H1 to H2 and stores them into the current open Safeguarded Copy backup on H2.

Note: Considering that at least all tracks that are restored from R1 to H1 must be resynchronized from H1 to H2 and are stored in your current open Safeguarded Copy backup, that process might use significant extra capacity.

Depending on your requirements, you might want to stop creating Safeguarded Copy backups and disable the CSM Scheduled tasks before you resync the H1 to H2 relationship. These steps can save physical capacity on the DS8000 that hosts the Safeguarded Copy Source volumes.

This entire process ends in a restored full duplex MM relationship that contains the data from the selected Safeguarded Copy backup (see Figure 1-12).

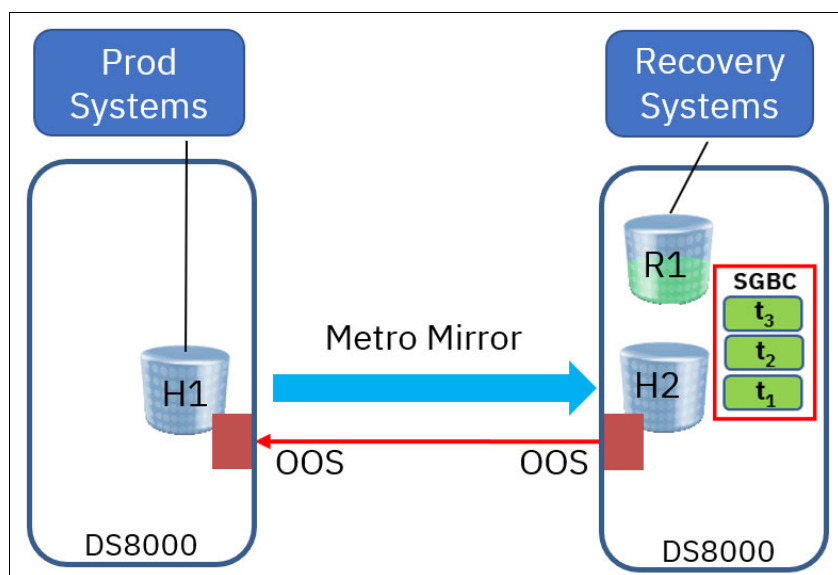


Figure 1-12 Restore to production example after resync of H1 -H2 relationship

For a detailed description on how to perform this task with CSM, see 4.3, “Restoring a Safeguarded Copy backup to production” on page 160.

For more information about which configuration is tested and other planning considerations for this feature, see 2.10.4, “Catastrophic recovery” on page 73.



Planning and considerations

This chapter includes planning guidelines and describes important considerations for implementing and making the most of Safeguarded Copy.

This chapter includes the following topics:

- ▶ 2.1, “Information that is required to plan a Safeguarded Copy implementation” on page 22
- ▶ 2.2, “HA, DR, and HADR with Safeguarded Copy topologies” on page 23
- ▶ 2.3, “Hardware and software prerequisites” on page 38
- ▶ 2.4, “Safeguarded Copy Management software” on page 39
- ▶ 2.5, “Safeguarded Copy sizing considerations” on page 42
- ▶ 2.6, “Safeguarded Copy backup priority consideration in an out-of-space situation” on page 55
- ▶ 2.7, “Safeguarded Copy performance considerations” on page 56
- ▶ 2.8, “Monitoring Safeguarded Copy” on page 57
- ▶ 2.9, “Security considerations” on page 69
- ▶ 2.10, “Safeguarded Copy backup use case considerations” on page 71
- ▶ 2.11, “Configuration changes considerations” on page 76
- ▶ 2.12, “Safeguarded Copy considerations” on page 81

2.1 Information that is required to plan a Safeguarded Copy implementation

Implementing a Safeguarded Copy solution requires meeting well-defined business requirements and planning considerations similar to implementing a high availability (HA) and disaster recovery (DR) (HADR) solution, such as for Metro Mirror (MM), Global Mirror (GM), and Metro/Global Mirror (MGM). Typically, Safeguarded Copy is coupled to an HADR solution to deliver logical corruption protection (LCP). Whether building out an entirely new solution or adding to an existing HADR solution, consider the following questions for any Safeguarded Copy implementation:

- ▶ What is the potential problem or exposure that you must solve?
 - For example, protect against inadvertent deletion, malicious destruction, selective manipulation, or ransomware attack?
 - Do you need to meet external regulatory requirements or satisfy internal auditors?
 - Which data do you need to protect? The entire environment or a subset?
- ▶ How current must the protected data be to offer business value if it is recovered? (The answers to the next two questions determine the number of Safeguarded Copy backups to keep.)
 - How frequently do you need to take Safeguarded Copy backups? For example, take one every 10 or 30 minutes or every 1, 2, 3, 4, 6, 12, or 24 hours?
 - How long do you need to keep the Safeguarded Copy backups? For example, keep them for 1 day, 2 days, 4 days, 1 week, or a month?
- ▶ What is the current or planned HADR solution and how is it managed; for example, by using IBM Copy Services Manager (CSM) or IBM Geographically Dispersed Parallel Sysplex (IBM GDPS): Whichever replication management is used for HADR also is used to manage Safeguarded Copy.
- ▶ Where should Safeguarded Copy be implemented? For example, at the production data center, the DR data center, both, or at another site.
 - Do you require virtual or physical isolation? That is, what type of “air-gap” is required?
 - Because of the FlashCopy restrictions for Safeguarded Copy Source volumes, the use of FlashCopy might decide where you can implement Safeguarded Copy. Therefore, verify how FlashCopy is in use in the current HADR solution.
 - The current or planned HADR solution and type of isolation determines the topology; for example, 2-site, 3-site, 4-site, or even 5-site.
- ▶ How do you intend to use Safeguarded Copy? The best practice *“Practice what you recover; recover what you practice”* applies to LCP and HADR solutions.
 - Section 1.1.3, “Use cases for data protection” on page 4 describes the five uses cases. Consider the following points if you must plan and prepare for the first four cases: Validation, Forensic Analysis, Surgical Recovery, and Catastrophic Recovery:
 - Determine how to perform Validation and Forensic Analysis for logical corruption detection.
 - Decide on the server that you will use for Validation and Forensic Analysis.
 - Plan and prepare for Surgical Recovery and Catastrophic Recovery.

- If you intend to use offline backups (for Catastrophic Recovery), you also must plan for that usage (offline backups are described here):
 - How frequently are the offline backups performed?
 - Where do you store the backups?
 - How long do you retain the backups?
 - Does the storage media need to be immutable; for example, IBM TS7700 VTS Write-Once, Read-Many (WORM), or IBM Cloud® Object Storage?

More issues must be considered, such as hardware and software prerequisites and capacity and performance sizing. We cover these topics in this chapter.

2.2 HA, DR, and HADR with Safeguarded Copy topologies

This section describes how Safeguarded Copy integrates with various DS8000 HA, DR, and HADR solutions. It provides several examples of 2-, 3-, and 4-site solutions with virtual and physical isolation.

Safeguarded Copy can be implemented when it meets business requirements for LCP. It can be configured at any site, and it is most often implemented at the DR site or an external site for better physical isolation.

The examples that are included in this section describe both implementations with virtual or physical isolation. More sophisticated solutions are possible, such as two Safeguarded Copy implementations: one in the production data center, the other in the DR data center.

CSM or GDPS LCP is required to manage Safeguarded Copy and both can manage various implementations. Whichever is used to manage the HADR solution is used to manage Safeguarded Copy. The figures that are used in this publication use CSM session names and CSM volume identifiers. For some of the topologies that are described next, you might need to implement more than one CSM session.

Note: GDPS offers various 2-, 3-, and 4-site HADR solutions in which GDPS LCP can be used to manage Safeguarded Copy.

The solutions are described in the following sections:

- ▶ 2-Site HADR solutions with Safeguarded Copy:
 - Metro Mirror - Safeguarded Copy Virtually Isolated
 - Metro Mirror - Safeguarded Copy Physically Isolated
 - Global Mirror - Safeguarded Copy Virtually Isolated
 - Global Mirror - Safeguarded Copy Physically Isolated
- ▶ 3-Site HADR solutions with Safeguarded Copy:
 - Multi-Target Metro Mirror - Safeguarded Copy Virtually Isolated
 - Multi-Target Metro/Global Mirror - Safeguarded Copy Virtually Isolated
 - Multi-Target Metro/Global Mirror - Safeguarded Copy Physically Isolated
- ▶ 4-Site HADR solutions with Safeguarded Copy:
 - 4-Site Metro/Global Mirror - Safeguarded Copy Virtually Isolated
 - 4-Site Metro/Global Mirror - Safeguarded Copy Physically Isolated

Note: GDPS 3-site and 4-site solutions can include GM or z/OS GM (“XRC”) for asynchronous replication. For more information, see *IBM GDPS: An Introduction to Concepts and Capabilities*, SG24-6374.

Important: The IBM DS8900F family is the last platform to support z/OS GM. No new z/OS GM functions are to be provided with IBM DS8900F. For more information, see [IBM Announcement Letter 920-001](#).

The 3-Site MGM solutions can be implemented in 2 or 3 physical sites and 4-site MGM solutions in 2, 3, or 4 physical sites. However, maintaining data centers is expensive, and adding distance between MM pairs also adds latency (to any synchronous replication technique) because of the laws of physics and the speed of light.

The greater the distance, the greater the added latency. For these reasons, 3-Site MGM and 4-site MGM solutions are often installed in two data centers. This configuration is common in the US and Canada.

The following terms are used in the figures in this publication:

- ▶ Hx: Host volumes, which are defined to production host systems, where x = site indicator
- ▶ SGBC: Safeguarded Copy Backup Capacity (the immutable storage capacity)
- ▶ Rx: Recovery volumes, which are defined to recovery host systems, where x = site indicator
- ▶ Jx: GM journal volumes, where x = site indicator
- ▶ LCP: Logical corruption protection
- ▶ Site X: Used in physical isolation examples to designate the DR data center or other external site
- ▶ MT MGM: Multi-Target Metro/Global Mirror

2.2.1 2-Site HADR and Safeguarded Copy topologies

In this section, the following 2-Site HADR solutions with Safeguarded Copy are described:

- ▶ Metro Mirror - Safeguarded Copy Virtually Isolated
- ▶ Metro Mirror - Safeguarded Copy Physically Isolated
- ▶ Global Mirror - Safeguarded Copy Virtually Isolated
- ▶ Global Mirror - Safeguarded Copy Physically Isolated

For more information about how you can combine Safeguarded Copy with CSM sessions with Practice Volumes, see Appendix A, “Other Safeguarded Copy topologies” on page 227.

Metro Mirror - Safeguarded Copy Virtually Isolated

In some geographies, MM is implemented across two local data centers and used as an HADR solution. In this solution (see Figure 2-1 on page 25), Safeguarded Copy is implemented with virtual isolation. H2 represents the Safeguarded Copy source volumes and R2 the Safeguarded Copy recovery volumes.

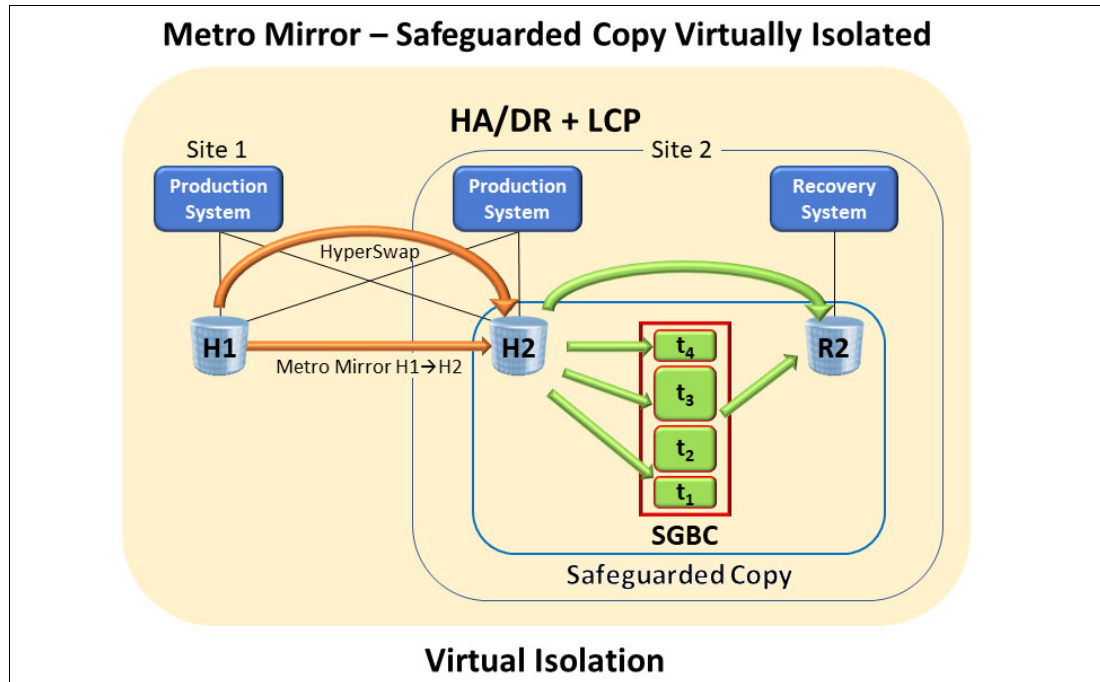


Figure 2-1 Metro Mirror - Safeguarded Copy Virtually Isolated

Safeguarded Copy backup consistency is performed during the “Check In” phase, which is described in 1.3.2, “Safeguarded Copy Backup Capacity” on page 9. It requires a short pause to write I/Os through an Extended Long Busy (ELB). Until that check-in process completes, write I/Os are paused. H1→H2 remains in a full duplex state, which means HyperSwap is available.

For some businesses, that temporary pause might not meet response time or service-level agreement (SLA) requirements. The Metro Mirror - Safeguarded Copy Physically Isolated solution eliminates the need to pause host write I/O to enable Consistency Groups (CGs) to complete.

Note: Consider the following points:

- ▶ GDPS LCP topology name is MM2SITE with Virtual Isolation.
- ▶ In an MM environment, do not create a CSM Safeguarded Copy session or GDPS LCP management profile that contains Safeguarded Copy source volumes from both MM primaries and secondaries. This configuration is unsupported, although it is not prevented by CSM. It might cause an extended impact to host writes during Safeguarded Copy Consistency Group (CG) creation.

For information about implementing this type of Safeguarded environment, see Chapter 4, “Implementation and management” on page 117.

Metro Mirror - Safeguarded Copy Physically Isolated

In some geographies, MM is implemented across two local data centers and used as both an HADR solution. In the solution that is shown in Figure 2-2, Safeguarded Copy is implemented with physical isolation. It can be implemented at Site 1, Site 2, the DR data center that is shown in Figure 2-2, or an external site that is designated by Site X.

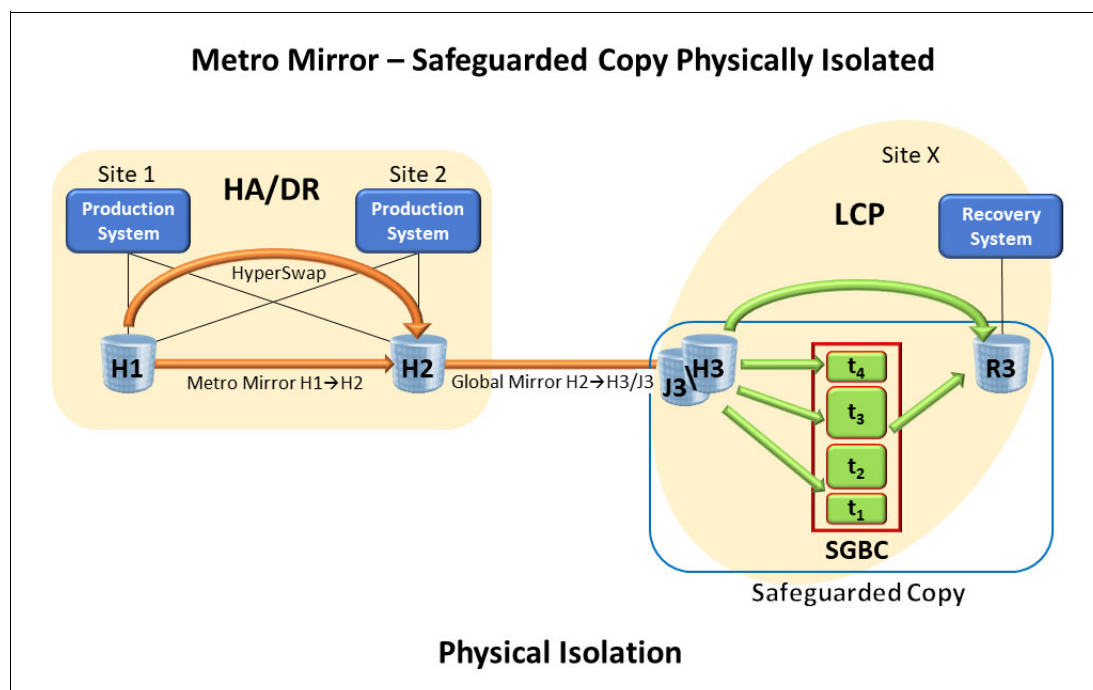


Figure 2-2 Metro Mirror - Safeguarded Copy Physically Isolated

This solution enables MM H1→H2 with HyperSwap to continue to run and provide HA while Safeguarded Copy backups complete. It is possible to enable H1 to be the Safeguarded Copy source volumes when running MM H2→H1 after a HyperSwap; that is, run MGM H2→H1→H3/J3.

H3 represents the Safeguarded Copy source volumes and R3 the Safeguarded Copy recovery volumes. GM is implemented solely to enable consistency for Safeguarded Copy backups to complete. Functionally, it is cascaded MGM H1→H2→H3/J3, but the GM component is not used for DR.

In such topologies where the Safeguarded Copy source volume is a GM target volume, you must ensure that the Safeguarded Copy source volumes are in a consistent state before creating the Safeguarded Copy backup.

Safeguarded Copy backup consistency is achieved by momentarily suspending GM H2→H3/J3 by using pause with consistency. The suspension occurs on a CG boundary that ensures that H3 is consistent; then, the Safeguarded Copy backup can be created.

Although that backup process completes, MM H1→H2 continues to run, and the GM is in suspended state. After the Safeguarded Copy backup is successfully created, resuming the GM H2→H3/J3 is done immediately to minimize the recovery point objective (RPO). To coordinate these tasks to create a consistent Safeguarded Copy backup, use self-written scripts or batch jobs, or the CSM Scheduler if CSM is used.

For more information about implementing this type of environment, see 4.4.1, "Metro Mirror with Safeguarded Copy" on page 219.

Note: The GDPS LCP topology name is MM2SITE with Physical Isolation. For more information about GDPS, see *IBM GDPS: An Introduction to Concepts and Capabilities*, SG24-6374.

Global Mirror - Safeguarded Copy Virtually Isolated

GM is a DR solution. Unlike GM with Practice, it does not include an extra set of volumes for DR test and recovery. For more information about topologies with practice volumes, see Appendix A, “Other Safeguarded Copy topologies” on page 227.

GM replicates H1→H2/J2. The H2 volumes are used for DR test and recovery if a disaster occurs. GM is suspended during a DR test.

In Figure 2-3, the Global Mirror - Safeguarded Copy Virtually Isolated Safeguarded Copy is implemented on the GM target DS8000 that is labeled “H2.” H2 is also used to represent the Safeguarded Copy source volumes: “SGBC” represents the Safeguarded Copy Backup Capacity, and “R2” represents the Safeguarded Copy recovery volumes.

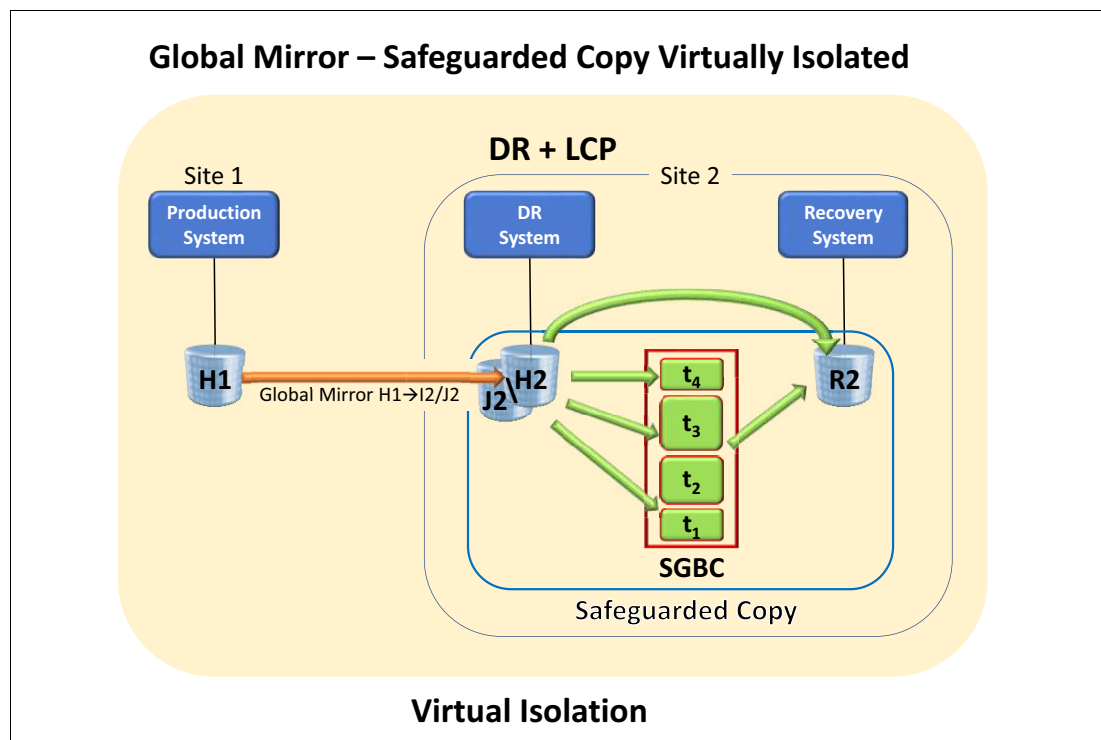


Figure 2-3 Global Mirror - Safeguarded Copy Virtually Isolated

In topologies where the Safeguarded Copy source volumes are GM target volumes, you must ensure that the Safeguarded Copy source volumes are in a consistent state before creating the Safeguarded Copy backup.

Safeguarded Copy backup consistency is achieved by momentarily suspending GM H1→H2/J2; that is, pause with consistency. The suspension occurs on a CG boundary that ensures that H2 is consistent; then, the Safeguarded Copy backup can be created. While the backup is taking place, the GM is in suspended state.

After the Safeguarded Copy backup is successfully created, resuming the GM H1→H2/J2 is done immediately to minimize the RPO. To coordinate these tasks and create a consistent Safeguarded Copy backup, use self-written scripts or batch jobs or the CSM Scheduler if CSM is used. For more information, see 4.4.2, “Global Mirror with Safeguarded Copy” on page 220.

Note: The GDPS LCP topology name is GM2SITE with Virtual Isolation. For more information about GDPS, see *IBM GDPS: An Introduction to Concepts and Capabilities*, SG24-6374.

Global Mirror - Safeguarded Copy Physically Isolated

GM is a DR solution. Unlike GM with Practice, it does not include an extra set of volumes for DR test and recovery. For more information about topologies with practice volumes, see Appendix A, “Other Safeguarded Copy topologies” on page 227.

GM replicates H1→H2/J2. The H2 volumes are used for DR test and recovery if a disaster occurs. GM is suspended during a DR test.

In Figure 2-4, Safeguarded Copy is implemented on a physically isolated DS8000 that is labeled “H3.” H3 also is used to represent the Safeguarded Copy source volumes, “SGBC” represents the Safeguarded Copy Backup Capacity, and “R3” represents the Safeguarded Copy recovery volumes.

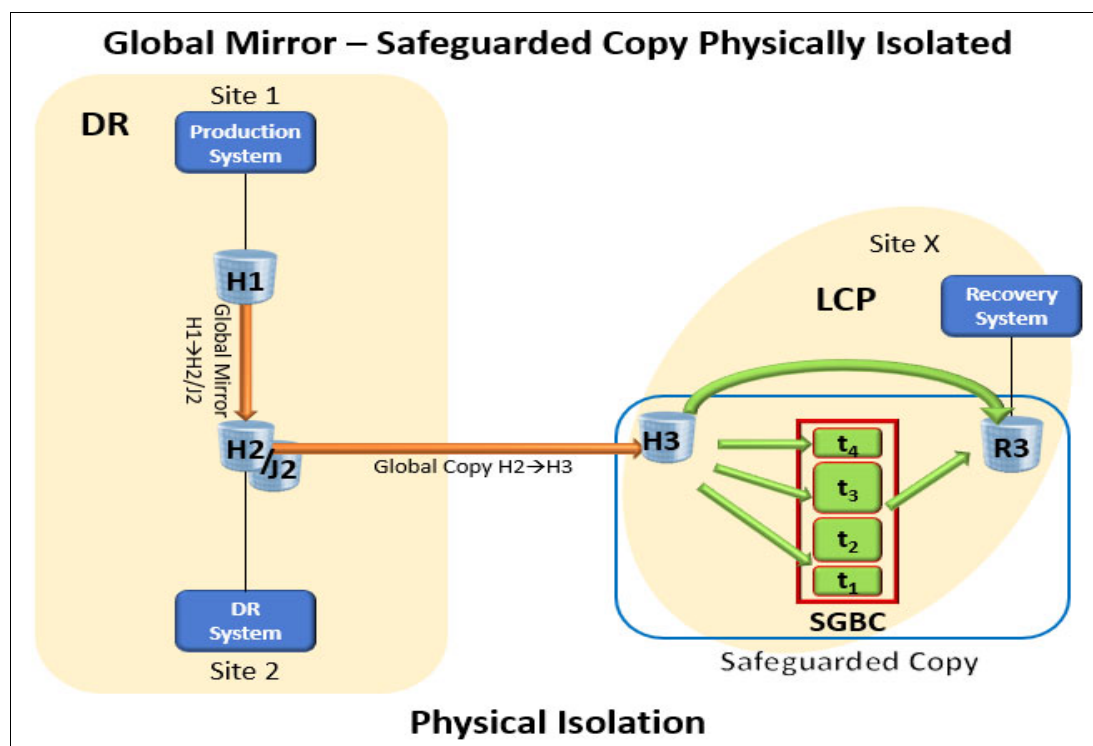


Figure 2-4 Global Mirror - Safeguarded Copy Physically Isolated

In such topologies where the Safeguarded Copy source volumes are a Global Copy target volume, you must ensure that the Safeguarded Copy source volumes are in a consistent state before creating the Safeguarded Copy backup.

Safeguarded Copy Source volume consistency is achieved by suspending GM H1→H2/J2, by using the pause with consistency function, and waiting until the out-of-sync (OOS) tracks are zero between H2→H3, which ensures that H3 is consistent.

Then, the Safeguarded Copy backup can be created. Although that backup process completes, the GM is in suspended state.

After the Safeguarded Copy backup is successfully created, resume the GM H1→H2/J2 immediately to minimize the RPO. To coordinate these tasks or actions and create a consistent Safeguarded Copy backup, use self-written scripts, batch jobs, or the CSM Scheduler if CSM is used. For more information about implementing this type of environment, see 4.4.2, “Global Mirror with Safeguarded Copy” on page 220.

Note: The GDPS LCP topology name is MM2SITE with Physical Isolation. For more information about GDPS, see *IBM GDPS: An Introduction to Concepts and Capabilities*, SG24-6374.

Cascaded Global Mirror - Safeguarded Copy Physically Isolated

As shown in Figure 2-5, Safeguarded Copy is implemented on a physically isolated DS8000 that is labeled “H3.” H3 is also used to represent the Safeguarded Copy source volumes, “SGBC” represents the Safeguarded Copy Backup Capacity, and “R3” represents the Safeguarded Copy recovery volumes.

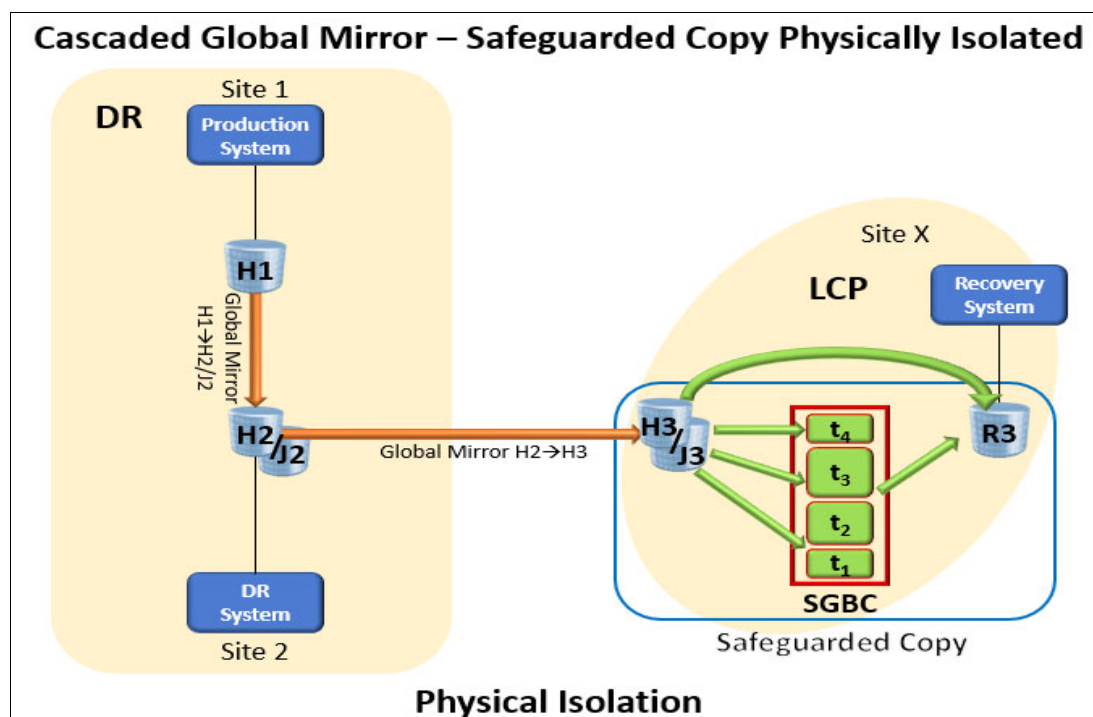


Figure 2-5 Cascaded Global Mirror - Safeguarded Copy Physically Isolated: another approach

Unlike the former physical isolated topology, the Safeguarded Copy source volumes are GM target volumes, which implement a cascaded GM. This topology can be considered where backups are taken frequently and to minimize the time between the pause and resume of GM. An example of this situation is when the backup frequency is less than 1 hour, such as every 10 - 30 minutes. However, this topology requires extra capacity for the second set of GM Journal volumes “J3”.

Note: This topology requires DS8880 microcode 8.5 SP7, and DS8900F 9.0 SP4 or 9.1 SP1 or later. The management software must be CSM 6.2.10 or later, or GDPS 4.2 with APAR PH31059 or later.

Safeguarded Copy source volume consistency is achieved by first suspending the cascaded GM H2→H3/J3; then, suspend the Production GM H1→H2/J2, which creates a CG on the cascaded GM. Then, wait until both GMs are in suspended state.

Important: It is a good idea to check the RPO on the H1→H2/J2 before starting this process to ensure a fast Safeguarded backup.

Now, the GM H1→H2/J2 can be resumed to minimize the RPO, and then the Safeguarded Copy backup can be created. After the backup is created, the cascaded GM H2→H3/J3 can be resumed. To coordinate these tasks and create a consistent Safeguarded Copy backup, use self-written scripts, batch jobs, or the CSM Scheduler if CSM is used. For more information about how to implement this environment, see 4.4.3, “Cascaded Global Mirror with Safeguarded Copy” on page 221.

Note: Consider the following points:

- ▶ The GDPS LCP topology name is GM2SITE with Physical Isolation.
- ▶ If your planned topology contains a GM with Practice replication and you want to perform Safeguarded Copy on the GM secondary, you must use the intermediate (Ix) volume (Global Copy secondary) as the Safeguarded Copy source volume.

The advantage of the use of a GM with Practice replication is that the extra set of volumes enables you to perform DR testing while the GM continues to run. For more information about GM with practice volumes, see Appendix A, “Other Safeguarded Copy topologies” on page 227.

2.2.2 3-site HADR and Safeguarded Copy topologies

In this section, the following 3-Site HADR solutions with Safeguarded Copy solutions are described:

- ▶ Multi-Target Metro Mirror - Safeguarded Copy Virtually Isolated
- ▶ Multi-Target Metro/Global Mirror - Safeguarded Copy Virtually Isolated
- ▶ Multi-Target Metro/Global Mirror - Safeguarded Copy Physically Isolated

IBM DS8000 3-site HADR solutions are based on MGM, which is an integration of MM with HyperSwap providing HA and GM. This integration provides DR that is implemented often at an out-of-region data center.

Two variations of MGM (that is, without DR practice volumes) and MGM with Practice (that is, with DR practice volumes) are available. Only the topologies without the DR practice volumes are described in this section with Safeguarded Copy implemented virtually or physically isolated.

The figures that are shown use CSM session names and volume identifiers (H1, H2, H3, J3, H4, R4, and so on). GDPS also offers 3-site MGM solutions with Safeguarded Copy.

For more information about implementing these topologies, see 4.4, “Scheduled tasks examples with Safeguarded Copy topologies” on page 217.

Multi-Target Metro Mirror - Safeguarded Copy Virtually Isolated

Multi-Target Metro Mirror - Safeguarded Copy can be used as an HADR solution if the DS8000s are implemented across two or three data centers. In the solution that is shown in Figure 2-6, a pair of MM solutions is represented by MM H1→H2 and MM H1→H3, with Incremental Resync enabled between H2 and H3. This solution enables MM to be readily established H2→H3 if H1 becomes unavailable.

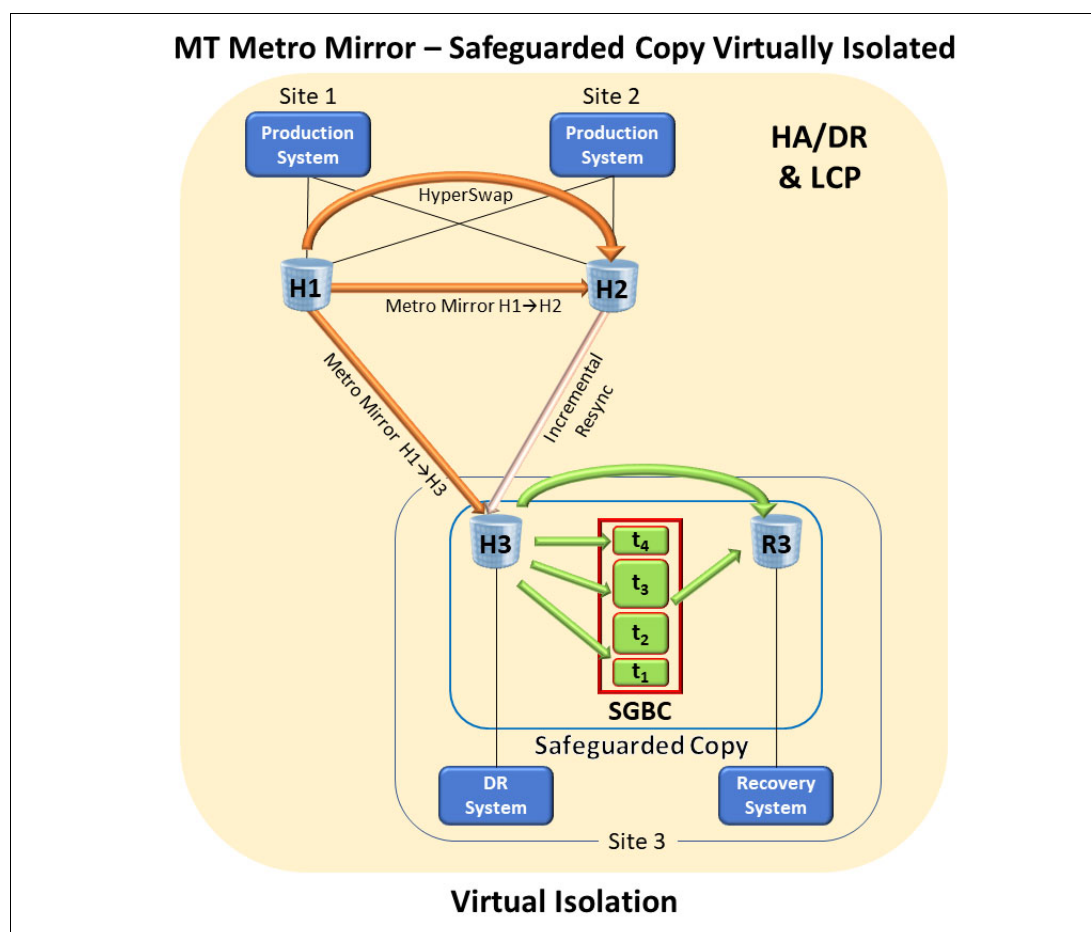


Figure 2-6 Multi-Target Metro Mirror - Safeguarded Copy Virtually Isolated

Safeguarded Copy is implemented with virtual isolation on H3. H3 represents the Safeguarded Copy source volumes and R3 the Safeguarded Copy recovery volumes. Safeguarded Copy backup consistency is created during the Safeguarded Copy “Check In” process. It requires a short pause to write I/Os through an ELB. Until that check-in process completes, write I/Os are paused.

Both MM relationships remain in full duplex state, which means HyperSwap is available. For some businesses, that temporary pause might not meet response time or SLA requirements. In that case, a topology that provides physical isolation is required.

Attention: Consider the following points:

- In an MM environment, do not create a CSM Safeguarded Copy session or GDPS LCP management profile that contains Safeguarded Copy source volumes from both MM primaries and secondaries. This configuration is unsupported, although it is technically possible, and it might affect host writes during Safeguarded Copy CG creation.
- The GDPS LCP topology name is MM3SITE with Virtual Isolation. An MM 3-site physical isolation topology also is available, but it is not described here.

Multi-Target Metro/Global Mirror - Safeguarded Copy Virtually Isolated

In Figure 2-7, Safeguarded Copy is implemented on the GM target DS8000 H3. H3 also is used to represent the Safeguarded Copy source volumes; “SGBC” represents the Safeguarded Copy Backup Capacity; and “R3” represents the Safeguarded Copy recovery volumes.

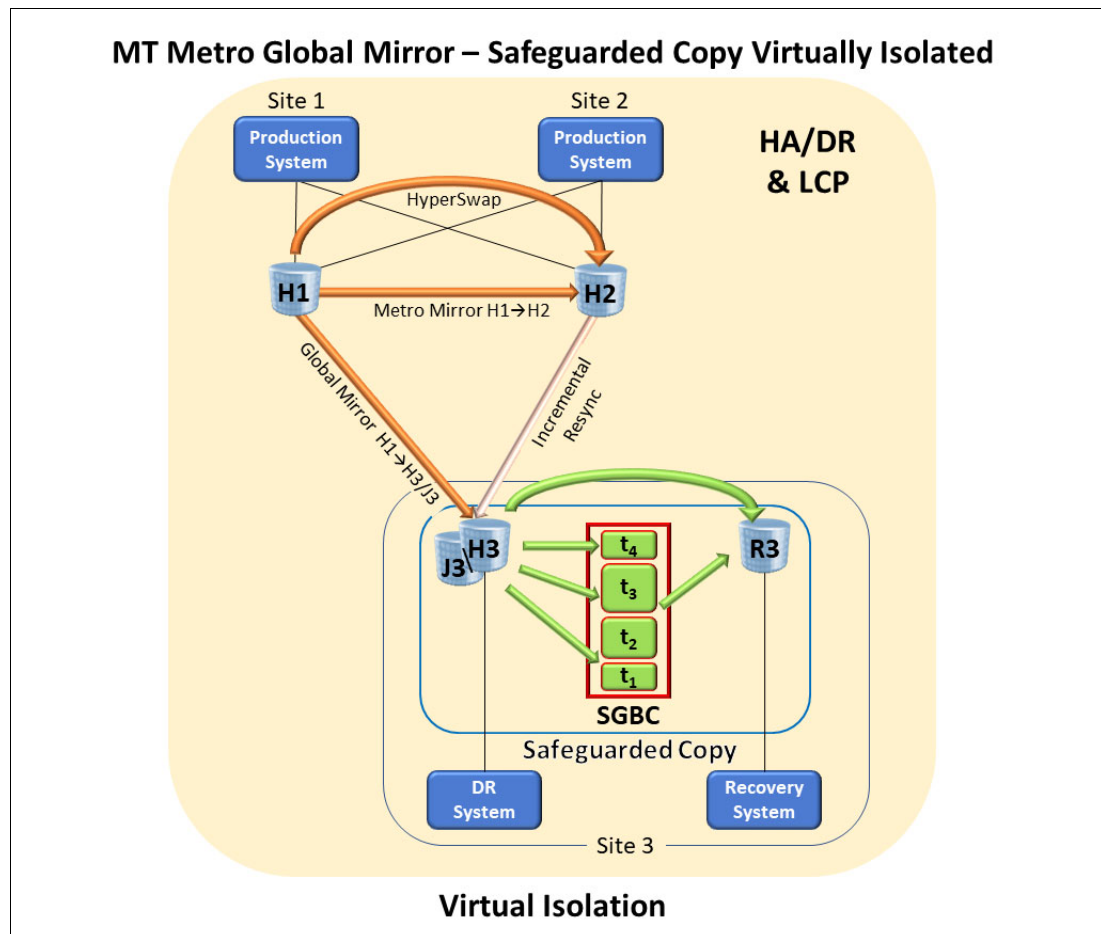


Figure 2-7 Multi-Target Metro/Global Mirror - Safeguarded Copy Virtually Isolated

Again, in topologies where the Safeguarded Copy source volumes are GM target volumes, you must ensure that the Safeguarded Copy source volumes are in a consistent state before creating the Safeguarded Copy backup.

Safeguarded Copy backup consistency is achieved by momentarily suspending GM H1→H3/J3; that is, pause with consistency. The suspension occurs on a CG boundary that ensures that the H3 is consistent; then, the Safeguarded Copy backup can be created.

Although that backup process completes, MM H1→H2 continues to run, and the GM H1→H3/J3 is in suspended state.

After the Safeguarded Copy backup is successfully created, resuming the GM H1→H3/J3 is done immediately to minimize the RPO. To coordinate these tasks and create a consistent Safeguarded Copy backup, use self-written scripts, batch jobs, or the CSM Scheduler if CSM is used.

Note: The GDPS LCP topology name is MGM3SITE with Virtual Isolation. For more information about GDPS, see *IBM GDPS: An Introduction to Concepts and Capabilities*, SG24-6374.

Multi-Target Metro/Global Mirror - Safeguarded Copy Physically Isolated

As shown in Figure 2-8 shows, site X represents the data center where Safeguarded Copy is implemented. Site X can be the DR data center or for better physical isolation, a different site that is local or remote to the DR data center. “H4” represents the Safeguarded Copy DS8000. H4 is also used to represent the Safeguarded Copy source volumes; “SGBC” represents the Safeguarded Copy Backup Capacity; and “R4” represents the Safeguarded Copy recovery volumes.

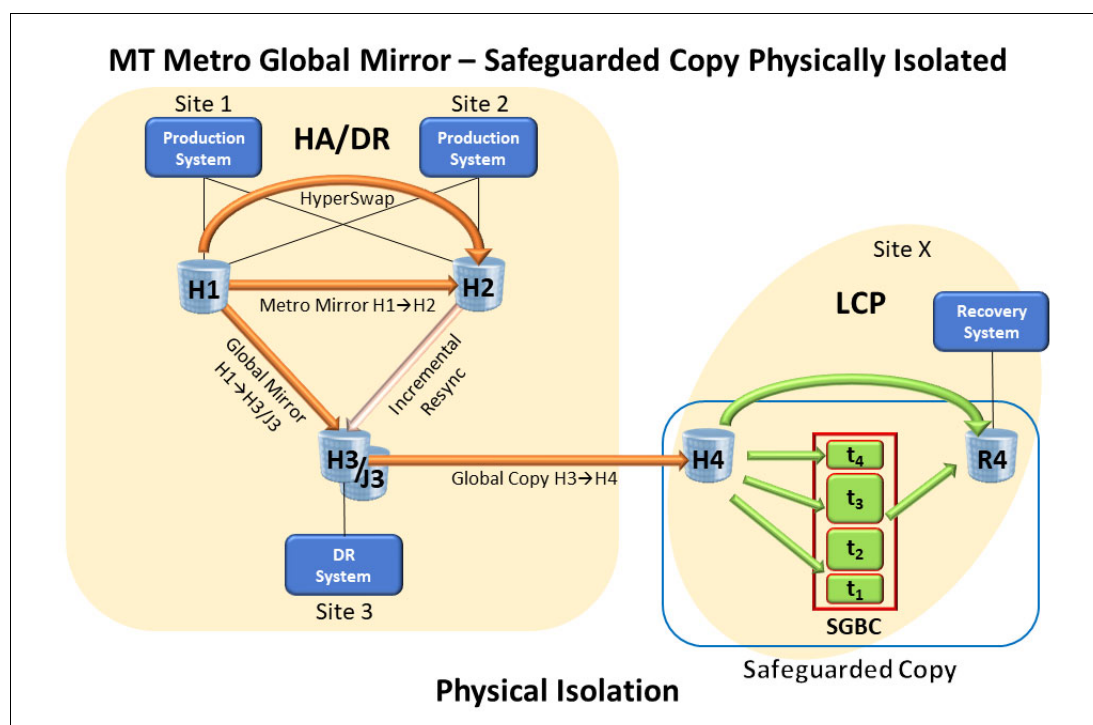


Figure 2-8 Multi-Target Metro/Global Mirror - Safeguarded Copy Physically Isolated

This type of topology where Global Copy is cascaded off GM is good for those environments that can tolerate a high RPO and do not require a high frequency of Safeguarded Copy backups. For customers who need a low RPO and high frequency of Safeguarded Copy backups, see “Cascaded Global Mirror - Safeguarded Copy Physically Isolated” on page 29.

In a topology where the Safeguarded Copy source volumes are Global Copy target volumes, you must ensure that the Safeguarded Copy source volumes are in a consistent state before creating the Safeguarded Copy backup.

Safeguarded Copy source volume consistency is achieved by suspending GM H1→H3/J3; that is, pause with consistency, and wait until the OOS tracks are zero between the Global Copy H3→H4. This process ensures that H4 is consistent; then, the Safeguarded Copy backup can be created. Although that backup process completes the MM, the H1→H2 relationship is in the full duplex state, and GM H1→H3/J3 is in the suspended state.

After the Safeguarded Copy backup is successfully created, resuming the GM H1→H3/J3 is done immediately to minimize the RPO. Again, to coordinate these tasks and create a consistent Safeguarded Copy backup, use self-written scripts, batch jobs, or the CSM Scheduler if CSM is used.

Note: The GDPS LCP topology name is MGM3SITE with Physical Isolation. For more information about GDPS, see *IBM GDPS: An Introduction to Concepts and Capabilities*, SG24-6374.

Cascaded Metro/Global Mirror - Safeguarded Copy Physically Isolated

Figure 2-9 shows a variation of the solution that also is shown in Figure 2-8 on page 33. Cascaded MGM means that MGM is replicating serially (H1→H2→H3/J3). Safeguarded Copy backup consistency is achieved in the same manner as shown in Figure 2-8 on page 33, except that the GM is running H2→H3/J3 instead of H1→H3/J3.

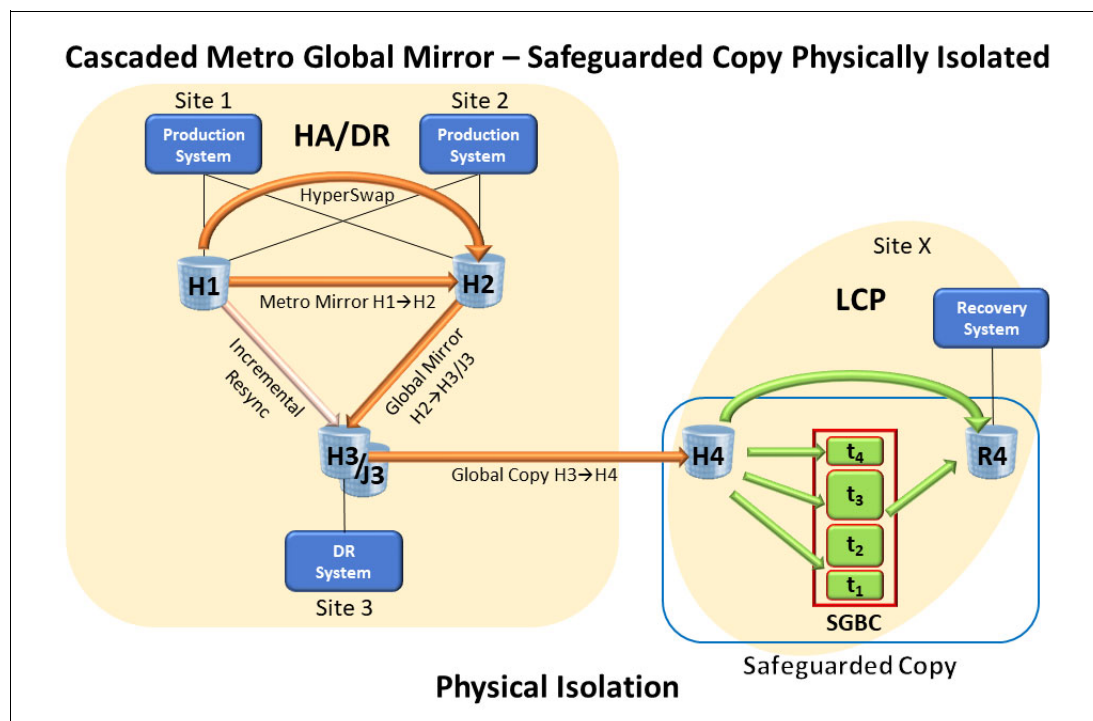


Figure 2-9 Cascaded Metro/Global Mirror - Safeguarded Copy Physically Isolated

Note: The GDPS LCP topology name is MGM3SITE with Physical Isolation. For more information about GDPS, see *IBM GDPS: An Introduction to Concepts and Capabilities*, SG24-6374.

This type of topology where Global Copy is cascaded off GM works well for environments that can tolerate a high RPO and do not require a high frequency of Safeguarded Copy backups. For customers who need a low RPO and high frequency of Safeguarded Copy backups, see “Cascaded Global Mirror - Safeguarded Copy Physically Isolated” on page 29.

For more information about the implementation of this topology, see Chapter 4, “Implementation and management” on page 117.

Note: If your planned topology contains a GM with Practice replication, and you want to perform Safeguarded Copy on the GM secondary, you must use the lx volume (Global Copy secondary) as the Safeguarded Copy source volume.

The advantage of the use of a GM with Practice replication is that the extra set of volumes enables you to perform DR testing while the GM continues to run. For more information about GM with practice volumes, see Appendix A, “Other Safeguarded Copy topologies” on page 227.

2.2.3 4-site HADR and Safeguarded Copy topologies

In this section, the following 4-Site HADR solutions with Safeguarded Copy solutions are described:

- ▶ 4-Site Metro/Global Mirror - Safeguarded Copy Virtually Isolated
- ▶ 4-Site Metro/Global Mirror - Safeguarded Copy Physically Isolated

IBM DS8000 4-site HADR solutions were developed as an extension of MGM functions. US financial market regulators changed business continuity requirements for some financial market businesses that were deemed “too big to fail.” Those businesses had to demonstrate that they can effectively run their production IT operations in a secondary site.

The ability to successfully perform a DR test was no longer sufficient evidence of recoverability. Therefore, customers began “site swapping” where production is smoothly quiesced in one data center and production is brought up rapidly in another. They reversed GM (run in the return direction) without the need to perform an initial copy. All that was required to run in reverse was GM Journal volumes on GM primary DS8000s.

However, those customers wanted HA when running production in the return direction. When production is running in the DR data center, they also wanted HA there (MM with HyperSwap).

The DS8000 has long had the ability to reverse MM, GM, and Global Copy. It also can cascade replication from one DS8000 to another. The 4-site MGM combines MGM (running in MT or Cascaded MGM) with Global Copy from the third DS8000 to the fourth. The purpose is to rapidly enable MM with HyperSwap after a site swap. That cascaded Global Copy primes the secondary DS8000s at the DR site.

CSM and GDPS support automated 4-site MGM failover and failback. Also, both support Safeguarded Copy on 4-site solutions. Figure 2-10 on page 36 and Figure 2-11 on page 37 show CSM-based implementations that use CSM session names and volume identifiers. GDPS also offers 4-site MGM solutions with Safeguarded Copy.

For more information about implementing these topologies, see Chapter 4.3 Safeguarded Copy topologies - Scheduled tasks examples.

4-Site Metro/Global Mirror - Safeguarded Copy Virtually Isolated

A solution that is built for site swapping is shown in Figure 2-10. That is, to provide HADR functions whether running production out of the primary data centers or the DR data centers.

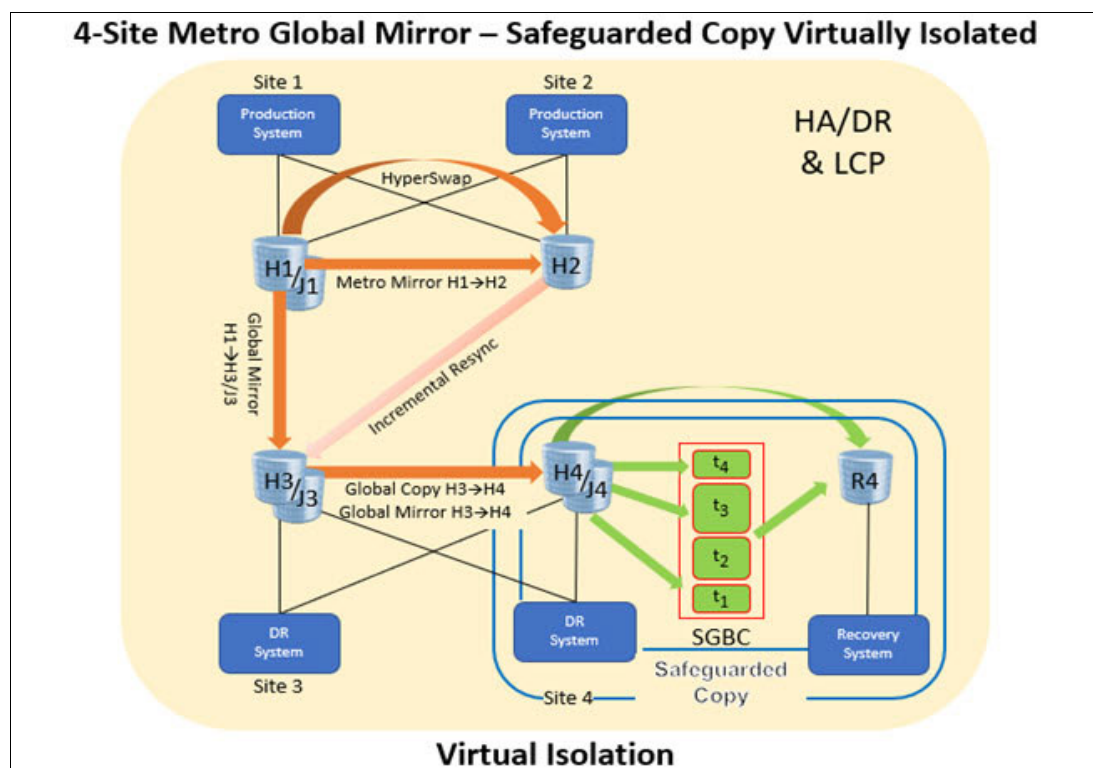


Figure 2-10 4-Site Metro/Global Mirror - Safeguarded Copy Virtually Isolated

MT MGM replicates MM H1→H2 with HyperSwap for HA, GM H1→H3/J3 for DR, and cascaded Global Copy H3→H4 to enable conversion from Global Copy to MM H3→H4 after a site swap. Safeguarded Copy is implemented on the DS8000 that is labeled H4. H4 also is used to represent the Safeguarded Copy source volumes; “SGBC” represents the Safeguarded Copy Backup Capacity; and “R4” represents the Safeguarded Copy recovery volumes.

In a topology where the Safeguarded Copy source volumes are Global Copy target volumes, you must ensure that the Safeguarded Copy source volumes are in a consistent state before creating the Safeguarded Copy backup.

Safeguarded Copy source volume consistency is achieved by suspending GM H1→H3/J3; that is, pause with consistency, and wait until the OOS tracks are zero between the Global Copy H3→H4, which ensures that H4 is consistent; then, the Safeguarded Copy backup can be created.

Although that backup process completes, the MM H1→H2 relationship is in a full duplex state, and the GM H1→H3/J3 is in a suspended state. After the Safeguarded Copy backup is successfully created, resuming the GM H1→H3/J3 is done immediately to minimize the RPO. Again, to coordinate these tasks and create a consistent Safeguarded Copy backup, use self-written scripts, batch jobs, or the CSM Scheduler if CSM is used.

The primary DS8000 H1 also has GM Journal volumes J1. Those volumes are used for the site swap when production is reversed running in the DR data center, which is effectively MM H3→H4, GM H3→H1/J1, and Global Copy H1→H2.

The difference between this implementation and the implementation that is described in “4-Site Metro/Global Mirror - Safeguarded Copy Physically Isolated” is where Safeguarded Copy runs. In 4-site MGM - Safeguarded Copy Physically Isolated, Safeguarded Copy is maintained on a fifth DS8000 that is labeled H5 (see Figure 2-11). It is at the DR site or at Site X for even better physical isolation.

Note: The GDPS LCP topology name is MGM4SITE with Virtual Isolation. For more information about GDPS, see *IBM GDPS: An Introduction to Concepts and Capabilities*, SG24-6374.

4-Site Metro/Global Mirror - Safeguarded Copy Physically Isolated

The 4-site MGM - Safeguarded Copy Physically Isolated solution (see Figure 2-11) is also built for site swapping. This solution is nearly identical to 4-Site Metro/Global Mirror - Safeguarded Copy Logically Isolated, except that it features two serial cascaded Global Copies; that is, Global Copy H3→H4 and Global Copy H4→H5. Safeguarded Copy is implemented on the DS8000 labeled “H5.” H5 also is used to represent the Safeguarded Copy source volumes; “SGBC” represents the Safeguarded Copy Backup Capacity; and “R5” represents the Safeguarded Copy recovery volumes.

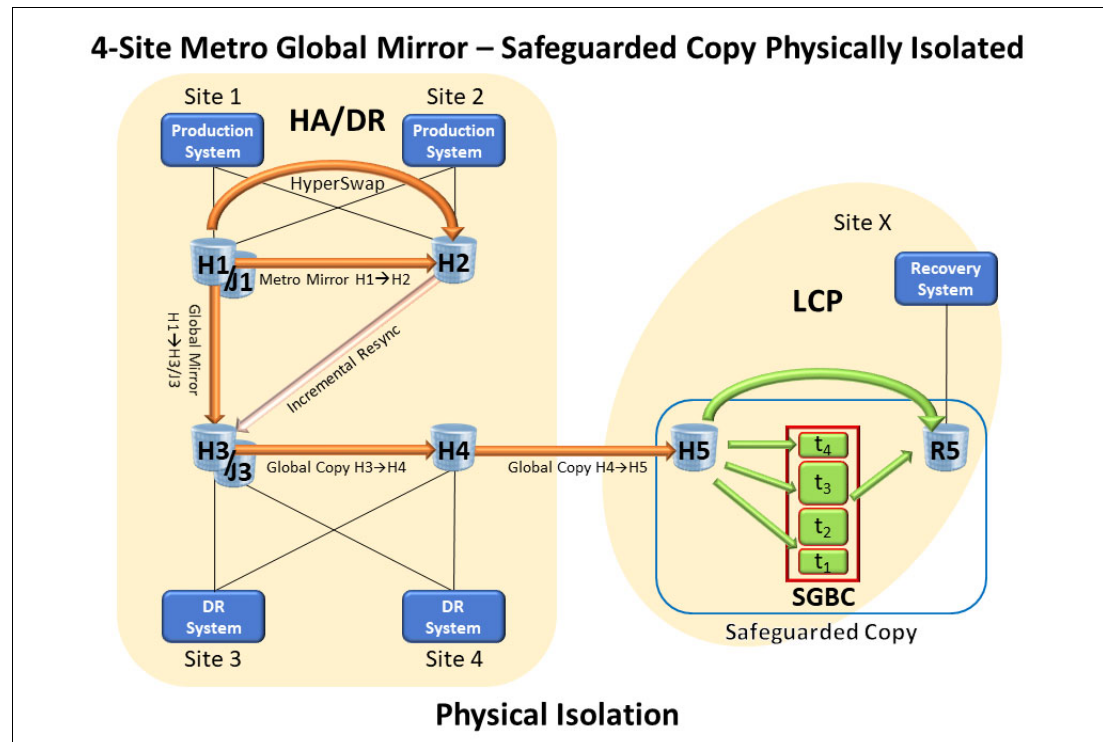


Figure 2-11 4-Site Metro/Global Mirror - Safeguarded Copy Physically Isolated

In a topology where the Safeguarded Copy source volumes are Global Copy target volumes, you must ensure that the Safeguarded Copy source volumes are in a consistent state before creating the Safeguarded Copy backup.

Safeguarded Copy Source volume consistency is achieved by suspending GM H1→H3/J3; that is, pause with consistency, and wait until the OOS tracks are zero between the Global Copy H3→H4 and H4→H5, which ensures that H5 is consistent; then, the Safeguarded Copy backup can be created.

While the backup process is taking place, the MM H1→H2 is in a full duplex state, and the GM H1→H3/J3 is in a suspended state. After the Safeguarded Copy backup is successfully created, resuming the GM H1→H3/J3 is done immediately to minimize the RPO. Again, to coordinate these tasks and create a consistent Safeguarded Copy backup, use self-written scripts, batch jobs, or the CSM Scheduler if CSM is used.

The primary DS8000 H1 also includes GM Journal volumes J1. After a planned site swap, replication is effectively running MM H3→H4, GM H3→H1/J1, and Global Copy H1→H2. With the correct implementation, Safeguarded Copy can be continued during a site swap with a cascaded Global Copy H2→H5.

Note: The GDPS LCP topology name is MGM4SITE with Physical Isolation. For more information about GDPS, see *IBM GDPS: An Introduction to Concepts and Capabilities*, SG24-6374.

2.3 Hardware and software prerequisites

The Safeguarded Copy function is integrated in the IBM DS8000 microcode and supported on DS8880 storage system models with microcode release 8.5 or later and on all DS8900F storage system models. The DS Command-line Interface (DS CLI) level 7.8.5 or later is required to set up and configure Safeguarded Copy.

To check your current DS8000 microcode level, run the **lsserver -l** DS CLI command, as shown in Example 2-1.

Example 2-1 DS8000 microcode level verification

```
dscli> lsserver -l
Date/Time: July 15, 2021 1:25:06 AM CEST IBM DSCLI Version: 7.9.20.431 DS: -
ID Image ID Image Name      Power Control SFI State  LIC Version OS Version Bundle Version
=====
00 1          SF75LLB70ESS01          0 online 7.9.20.431 7.2.5.105 89.20.131.0
01 1          SF75LLB70ESS11          0 online 7.9.20.431 7.2.5.105 89.20.131.0
```

Note: In Example 2-1, the Bundle Version column shows the DS8000 9.2 and the LIC Version column shows DS CLI 7.9.20.

To start using Safeguarded Copy, you must have a Copy Services (CS) license that is installed on the DS8000 system. The CS license bundle is based on usable capacity and usage. For example, if you must protect 50 TB of your production data with Safeguarded Copy, 50 TB of DS8000 CS license is required. For more information about DS8000 CS license, see [Licensed functions](#).

Also, to manage Safeguarded Copy, CSM 6.2.3.1 or later or GDPS 4.2 with APAR PH17926 or later is required. For information about CSM and GDPS LCP, see 2.4, “Safeguarded Copy Management software” on page 39.

Note: Use the most current version of CSM (6.3.3.0) to take advantage of the most recent updates.

In addition to these hardware and software requirements, more physical storage capacity is required for the following components:

- ▶ The changed data that is stored in the Safeguarded Copy Backup Capacity over the retention period
- ▶ The small Safeguarded Copy overhead for each CG
- ▶ Recovery volumes
- ▶ Production volumes (in case of physical isolation)

2.4 Safeguarded Copy Management software

As described in 1.3.3, “Safeguarded Copy management software” on page 10, the DS8000 management interfaces DS CLI or DS GUI or the z/OS interfaces cannot be used to manage Safeguarded Copy. The DS8000 management interfaces are used to prepare for the Safeguarded Copy function by defining the backup capacity multiplier per volume (see 4.1.1, “Configuring Safeguarded Copy Backup Capacity” on page 119) and modify or delete the Safeguarded Virtual Capacity for volumes.

Note: You cannot manage Safeguarded Copy with the DS8000 management interfaces.

A second interface to manage Safeguarded Copy is required. This interface can be a fully licensed IBM CSM 6.2.3 or later instance or IBM GDPS Logical Corruption Protection Manager V4.2 with APAR PH17926 or later.

Tip: If GDPS or CSM is used in your environment, it is best practice to use the same product for managing Safeguarded Copy.

2.4.1 IBM Copy Services Manager

IBM CSM 6.2.3 or later supports Safeguarded Copy. A Safeguarded Copy session type is available, which is used to create, delete, recover, and restore Safeguarded Copy backups. Within CSM, you can specify the required properties, such as the Safeguarded Copy retention period, and you can automate the backup frequency.

If you use CSM to manage your HADR solution, you can use CSM Scheduled tasks to automate and coordinate Safeguarded Copy so that you create consistent backups. For example, consistent backups are required if you want to implement Safeguarded Copy on a GM target system. For more information about implementing Safeguarded Copy with CSM, see Chapter 4, “Implementation and management” on page 117.

CSM can be installed on z/OS or open systems platforms (IBM AIX®, UNIX, Windows, and so on). With DS8880 or later systems, it is also included on each Hardware Management Console (HMC). An activation license key is required before you can start using CSM on the HMC. In addition to the activation key, you need a CSM license.

The CSM software is licensed per TiB usable source disk capacity that is converted into Resource Value Units (RVUs). CSM licensing for Safeguarded Copy is based on the capacity that is protected by Safeguarded Copy on each DS8000 storage system. For more information about the CSM license, see [5725-Z54 IBM Copy Services Manager 6.3](#).

To interact with a CSM server, you need a web browser that is certified by IBM CSM. For the list of supported web browsers, see [Supported Platforms and Browsers for IBM Copy Services Manager 6.3.x](#).

In mainframe environments, you should implement CSM 6.2.11 or later together with [IOS APAR OA59561](#) to improve the performance and minimize the application impact during the creation of Safeguarded Copy backups. For more information, see *Best Practices for DS8000 and z/OS HyperSwap with Copy Services Manager*, SG24-8431.

With the CSM 6.2.11 or later, you can associate the Safeguarded Copy session to a z/OS sysplex, and then, the necessary commands to perform a backup are passed down to the IOS component on z/OS. To use this enhancement, the minimum required DS8000 microcode levels are DS8880 8.5 SP7 or DS8900F 9.1 SP1.

If CSM is not running on z/OS, an IP connection between the CSM running on a distributed server platform and the z/OS LPAR is required. On the z/OS LPAR, the HyperSwap Management Address Space also must be active.

Copy Services Manager server memory sizing considerations

The CSM server can be run by way of the DS8000 HMC, z/OS, or on Distributed Systems. The CSM server includes a default Java heap size for standard operations. Replication sessions and Safeguarded Copy sessions also allocate part of that heap size. Correct sizing of the Java heap size is essential to ensure optimal operation of the CSM server.

The default heap size for distributed systems and z/OS is 1280 MB. If CSM on the HMC is used, the default heap size depends on the amount of memory in the HMC.

Table 2-1 lists the HMC memory sizes and the CSM default Java heap size.

Table 2-1 HMC memory size and CSM default Java heap size

HMC memory size	CSM default Java heap size
8 GB	1024 MB
16 GB	4 GB
32 GB	4 GB

To determine the memory size of the installed HMC, the DS CLI `lshmc -l` command can be used, as shown in Example 2-2. (For brevity, not all fields from this command are listed.)

Example 2-2 DS CLI `lshmc -l` command output

```
dscli> lshmc -l
Date/Time: July 17, 2021 2:10:25 AM CEST IBM DSCLI Version 7.9.20.431 DS: -
Name          State Role      Release      Memory Disk
=====
ds8k-r9-02     Online Secondary(2) R9.2 bundle 89.20.131.0 16GB 250GB
ds8k-r9-01     Online Primary(1)   R9.2 bundle 89.20.131.0 16GB 250GB
```

Note: If a distributed server is used, allowance for the operating system or Hypervisor must be considered.

You can increase the CSM Java heap size on a Distributed server or an z/OS server, depending on the calculated memory size. For more information about CSM memory requirements, see this IBM Documentation [web page](#).

For more information about IBM CSM, see this IBM Documentation [web page](#).

2.4.2 IBM GDPS LCP Manager

Starting with release 4.1, GDPS provides an integrated LCP function that is based on the FlashCopy function. GDPS 4.2 with APAR PH17926 also supports the Safeguarded Copy function in the GDPS LCP Manager.

At a high level, the GDPS LCP Manager captures multiple, secure point-in-time copies of critical production data with the Safeguarded Copy or FlashCopy function, and to restore the data back into production, if necessary.

The LCP Manager also recovers a specific point-in-time copy to another set of devices that can be used to start one or more isolated recovery systems to analyze the scope of a particular logical corruption event.

More security and protection are provided for the LCP protection copies than for copies that are taken with more traditional methods by minimizing host access to these volumes and by providing specific roles and rules for their management.

The GDPS LCP Manager is a separate product that is available for GDPS Metro and GDPS Global. GDPS LCP Manager is a separately priced feature of GDPS.

Safeguarded Copy is supported in the following supported LCP topologies in GDPS 4.4 and later:

- ▶ Metro Mirror 2-site and 3-site with Virtual Isolation
- ▶ Metro Mirror 2-site and 3-site with Physical Isolation
- ▶ Global Mirror 2-site (Global Mirror Secondary) with Virtual Isolation
- ▶ Global Mirror 2-site (Global Mirror Secondary) with Physical Isolation
- ▶ Metro/Global Mirror 3-site and 4-site with Virtual Isolation
- ▶ Metro/Global Mirror 3-site and 4-site with Physical Isolation
- ▶ Metro Global - XRC 3-site and 4-site with Virtual Isolation

In a z/OS MGM context, GDPS LCP also supports Safeguarded Copy on the MM 2-site with virtual isolation.

For more information about IBM GDPS LCP Manager, see *IBM GDPS: An Introduction to Concepts and Capabilities*, SG24-6374.

2.5 Safeguarded Copy sizing considerations

Adequately sizing the DS8000 for capacity and performance is crucial to successfully implement and effectively use Safeguarded Copy functions.

Estimate the physical and virtual capacity of the following components (see Figure 2-12):

- ▶ Safeguarded Copy Backup Capacity.
- ▶ Recovery volume.
- ▶ A Safeguarded Copy source volume, if a physical isolation approach is planned.

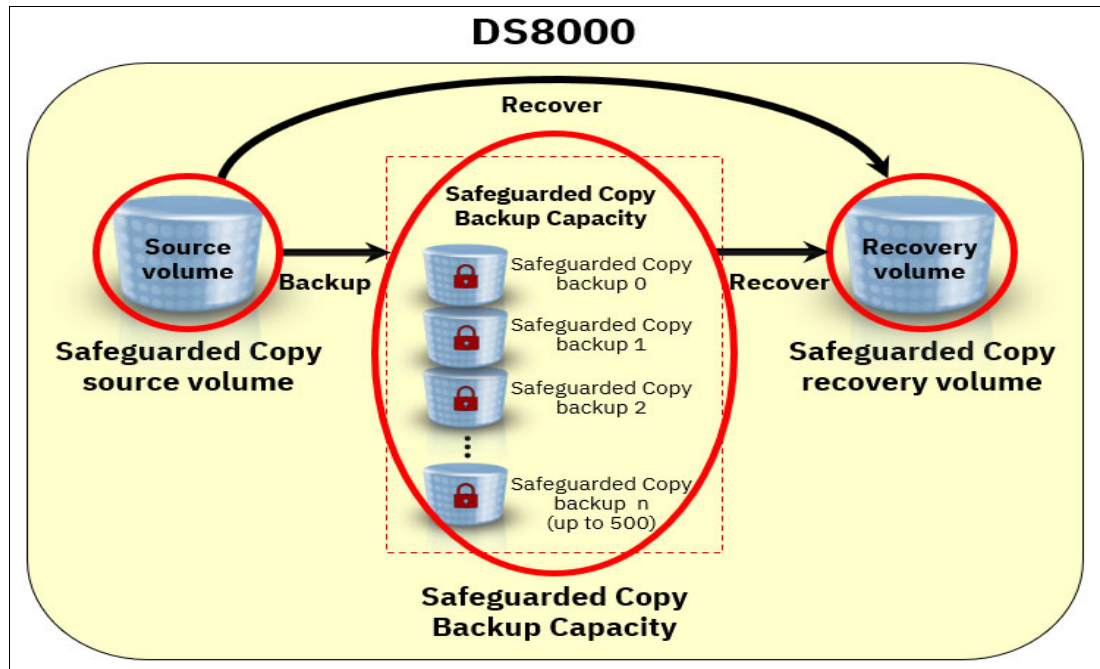


Figure 2-12 Components of Safeguarded Copy that must be sized

Physical capacity estimation is required to determine how much capacity is required to implement Safeguarded Copy; that is to store all changed data in the Safeguarded Copy Backup Capacity and recovery actions. The estimation also ensures that the physical limitation of the DS8000 is not exceeded.

Also, the DS8000 virtual capacity limit is based on the DS8000 cache size; therefore to determine whether that limit is exceeded, the virtual capacity for all volumes within the DS8000 must be estimated. For each Safeguarded Copy source volume, you must calculate the required Safeguarded Copy Virtual Capacity to estimate the Backup Capacity Multiplier.

Important: The total virtual capacity (provisioned capacity) of a DS8000 storage system (including the Safeguarded Copy Virtual Capacity) must not exceed the following limits:

- ▶ 1024 TB (Fixed Block (FB)) or 913 TB (Count Key Data (CKD)) for systems with system memory lesser or equal to 512 GB
- ▶ 3968 TB - 4096 TB (FB) or 3538 TB - 3652 TB (CKD) for systems with system memory greater or equal to 1 TB

Configurable capacity varies between limits based on the number and size of logical volumes. Conservatively plan for configurations targeting the low end of the range.

2.5.1 Safeguarded Copy key operational considerations

Two key operational considerations must be considered when planning and implementing Safeguarded Copy:

- ▶ Frequency of Safeguarded Copy backups
- ▶ Retention period of Safeguarded Copy backups

During the implementation of a Safeguarded Copy solution, consider how often you create Safeguarded Copy backups and how long you keep them. This information might depend on regulatory or business requirements.

In addition, consider how often you must validate your data.

A higher backup frequency and a high regular frequency of data validation means that you are losing less data if a logical corruption occurs and are more quickly detecting a logical corruption during the data validation is possible.

The Safeguarded Copy backup frequency, backup retention period of your backups, and data change rate are key factors that influence how much capacity you need to store the backups. Also, you need capacity for the recovery volumes on which you are performing the data validation.

Frequency of Safeguarded Copy backups

With a high frequency of Safeguarded Copy backups, you reduce the RPO. A low RPO is wanted, but might require more capacity to store the changed data in your DS8000 system.

It might be that some business requirements call for a specific frequency; therefore, consider the backup frequency based on the requirements for your environment.

The Safeguarded Copy backups require consistent data. When backups are taken in an MM environment, you must freeze all write I/O to the volumes that are being backed up. A higher backup frequency results in such freezes, which can affect production.

However, if the Safeguarded Copy backups are taken on a GM DR DS8000 storage system or on the isolated third- or fourth-site DS8000, such freeze actions do not affect production. This configuration allows much more frequent backups.

Experience shows that a backup frequency of 4 - 6 hours is common practice. The DS8000 currently supports a maximum frequency of one backup every 10 minutes (although that frequency rate is requested by that few customers). In Figure 2-13, you see an overview of common backup frequencies and how often customers implemented them.

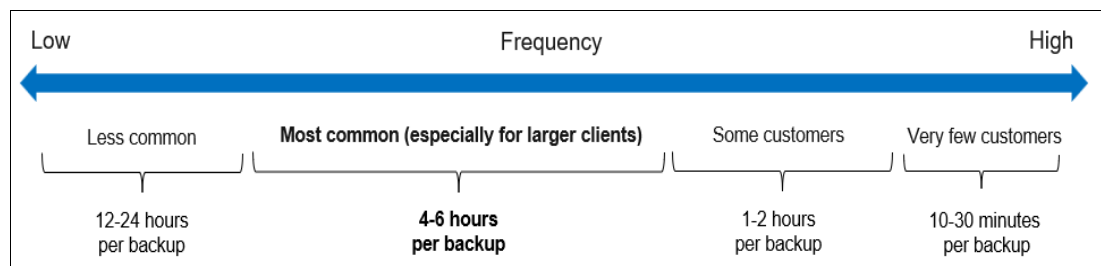


Figure 2-13 Backup frequencies that are used by customers

Retention period of Safeguarded Copy backups

Along with the backup frequency, you must decide how long you want to keep the Safeguarded Copy backups. The longer the retention period, the more capacity that is required to store the changes in the DS8000. Consider the following aspects before you define the retention period for your environment:

- ▶ Do you have regulatory or business requirements that define how long you need to keep the backups?
- ▶ Would it be helpful to restore a backup that is 14 days old? Is such a restoration acceptable for your business?
- ▶ How long would it take to detect that a logical corruption occurred?

Apart from these general aspects, other aspects might be specific to your situation. Today, the most common retention period is 2 - 5 days. Some customers want long retention periods. For those customers, it might make sense to copy regularly validated data from the DS8000 to WORM tape to increase the retention period and reduces the amount of capacity that is required in the DS8000 system.

Figure 2-14 shows retention periods that were requested by customers, including an indication of how often these periods are implemented.

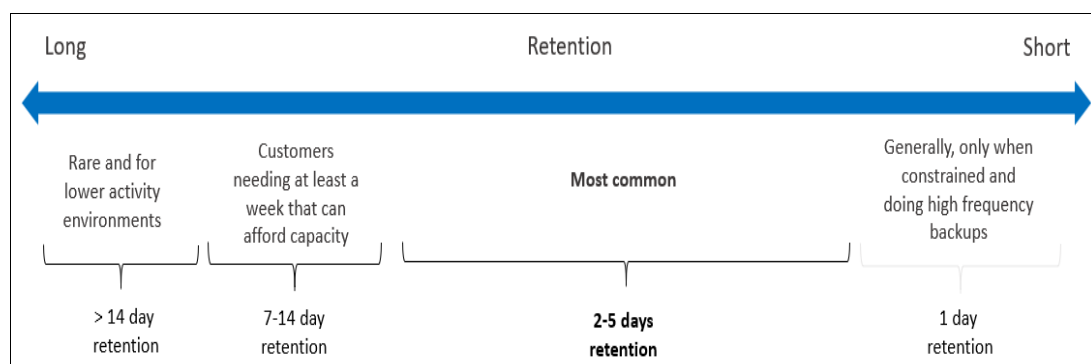


Figure 2-14 Safeguarded Copy Backup retention periods

You do not need to select one of the retention periods that is shown in Figure 2-14. You can define the retention period based on your own requirements.

Make sure that you use a Safeguarded Capacity sizing that reflects your requirements in terms of retention period and backup frequency. By doing so, you make sure that you know the capacity requirements before you implement Safeguarded Copy.

2.5.2 Safeguarded Copy Backup Capacity

The Safeguarded Copy Backup Capacity can be defined in storage pools with large or small extents. However, a best practice is to use small extents that give the best results regarding space efficiency and performance. At least one new extent must be allocated with every backup version (even if the source volumes were not changed). Therefore, it is more advantageous to use small extents with Safeguarded Copy because you can significantly reduce total space requirements.

Note: The best practice is to use small extents and thin-provisioned volumes.

Although the Safeguarded Copy Backup Capacity cannot be directly accessed or even “seen” by the host system, it requires physical storage capacity and other storage system resources. After you create a backup version, physical capacity is used from the storage pool where the Safeguarded Copy Backup Capacity is available. Because physical capacity is a finite resource, there is the possibility of running out of space; therefore, the space must be monitored.

On a DS8000, the physical capacity is shared between its host volumes and the Safeguarded Copy Backup Capacity. One option to mitigate this situation is to migrate the Safeguarded Copy Backup Capacity to another storage pool with more space, if possible. Alternatively, capacity can be added to the storage pool when you receive capacity threshold alerts.

Note: A best practice is to share physical capacity between all resources (host volumes, FlashCopy target volumes, and the Safeguarded Copy Backup Capacity) in the same storage pool.

To determine the amount of Safeguarded Copy Backup Capacity that is required for Safeguarded Copy backups, you must determine the data change rate for specific intervals in accordance with your backup management policy requirements (backup frequency and retention periods).

Again, both the required Safeguarded Copy Backup Capacity and the Safeguarded Virtual Capacity depend on the data change rate and following backup management policies:

- ▶ Frequency of backups to be taken
- ▶ Retention period for the backups

Safeguarded Virtual Capacity and Backup Capacity Multiplier

When sizing the Safeguarded Copy Backup Capacity, you also must determine the Safeguarded Copy Virtual Capacity for each source volume that is protected by Safeguarded Copy. Unlike the Safeguarded Copy Backup Capacity, the Safeguarded Virtual Capacity cannot be shared between volumes in a storage pool.

To store the Safeguarded Copy backup for a source volume, you must assign Safeguarded Virtual Capacity to this volume. This process is done by assigning a Backup Capacity Multiplier for each Safeguarded Copy source volume by using the DS CLI or Storage Management GUI.

The capacity that is required depends on the size of the source volume, backup retention period, change rate of the source volume’s data, and backup frequency. Safeguarded Virtual Capacity is specific to each host source volume rather than a total value for the entire Safeguarded Copy configuration. Running out of Safeguarded Virtual Capacity does not cause write inhibit to the production volume. However, the oldest backup is automatically expired (deleted).

To calculate the Backup Capacity Multiplier for each Safeguarded Copy source volume, divide the estimated Safeguarded Virtual Capacity in GiB for that volume by the volume size in GiB.

If only a few backups are taken and enough physical and virtual capacity is available in your DS8000 storage system, it might be practical to assume that you are using 100% of the virtual capacity for each volume in each backup. In that case, if the volume was 100 GiB and the objective was to maintain six backups, 600 GiB (or a multiplier of 6) can be used for the virtual capacity.

Important: The total virtual capacity of a DS8000 storage system (including the Safeguarded Copy Virtual Capacity) must not exceed the following limits:

- ▶ 1024 TB (FB) or 913 TB (CKD) for systems with system memory lesser or equal to 512 GB
- ▶ 3968 TB - 4096 TB (FB) or 3538 TB - 3652 TB (CKD) for systems with system memory greater or equal to 1 TB

Configurable capacity varies between the limits that are based on the number and size of logical volumes.

When planning for Safeguard Virtual Capacity with large systems and many backups, having the same Backup Capacity Multiplier for each host volume might not be possible because of the virtual capacity limitation. Therefore, you must analyze the data change rate for each production volume; identify volumes with high, medium, and low data change rates; and assign Backup Capacity Multiplier per each host volume.

In this way, your Safeguarded Virtual Capacity is used more efficiently, but more importantly, you can keep the total virtual capacity below the maximum limit per DS8000 system. Because this process results in different values for each host volume in the configuration, grouping the volumes and using a common maximum value (Backup Capacity Multiplier) for each group simplifies the configuration process.

Figure 2-15 shows the step that is used to define Safeguarded Copy by using DS8000 GUI (see 4.1.1, “Configuring Safeguarded Copy Backup Capacity” on page 119). In this step, you must specify a Backup Capacity Multiplier, which means virtual capacity reservation for this specific host volume and the backup location.

Configure Safeguarded Capacity [X]

ckd_ats_0018_0018

Configure the safeguarded capacity for the volumes by entering the location to store safeguarded backups in and the capacity multiplier for the safeguarded virtual capacity.

Backup location:

CKD_0 [v]

Backup capacity multiplier(*):

6

6.00 Mod1

Pool usable capacity 11.67 KMod1

System provisioned capacity 70.86 TiB

[?] Need Help [Configure] [Cancel]

Figure 2-15 Define Backup Capacity Multiplier for Safeguarded Copy

To determine the correct Backup Capacity Multiplier, complete the following steps:

1. Decide the number and retention period of the backups that are maintained by your Safeguarded schedule.

For example, if your Safeguarded schedule creates two backups per day and holds each backup for up to three days, the system must maintain six backups per volume.

2. Determine the change rate of the data that you want to back up by using one of methods that are described in 2.5.4, “Safeguarded Copy capacity sizing methods” on page 48.
3. Determine the Backup Capacity Multiplier by dividing the data change rate in GiB that is required for Safeguarded Copy backups by the volume size in GiB.

For example, if the source volume size is 500 GiB, and the data change rate is 1000 GiB, the Backup Capacity Multiplier is 2 (1000 GiB/500GiB).

Note: Consider the following points:

- ▶ The smallest Backup Capacity Multiplier that you can select is 1.5.
- ▶ You can specify a different storage location (storage pool) for the Safeguarded Copy Backup Capacity than the pool you are using. However, both must have the same DS8000 server affinity.
- ▶ For systems that can support up to 4 PB of virtual capacity when small extents are used, do not allocate more than 2 PB because Easy Tier cannot monitor the capacity beyond 2 PB. The extra 2 PB of virtual capacity still can be used for Safeguarded Copy Backup Capacity because this backup capacity is not monitored by Easy Tier.

In addition to the Safeguarded Copy Capacity sizing, it is equally important to plan capacity for the recovery volumes, which are a part of the entire Safeguarded Copy logical data protection solution.

2.5.3 Recovery and Safeguarded Copy source volumes

In this section, we describe the recovery and Safeguarded Copy source volumes.

Recovery volumes

The recovery volumes are host-attached to the recovery environment for data corruption analysis (validation and forensics) and production recovery. These volumes can be defined as fully provisioned volumes or thin-provisioned (that is, Extent Space Efficient (ESE)). How you use the recovery volumes depends on your requirements.

Although you can consider using the recovery volumes for longer, you can plan 100% of the source volume capacity as physical capacity. The best practice is to configure the recovery volumes as thin-provisioned volumes. This configuration gives you more flexibility by using the physical capacity for other purpose if you do not need the capacity for a recovery action.

The required capacity for recovery volumes depends on how long you intend to keep the recovery volumes copy relationship active, and how much the Safeguarded Copy source volumes change while the relationship exists.

Note: Defining the recovery volume as thin-provisioned is a best practice even though you want to provide 100% of the source volumes as the physical capacity for the recovery volumes. This capacity is not used until a recovery action is required; therefore, the free capacity is available for Safeguarded Copy backups or other purposes for the remaining time.

If dedicated capacity exists for your data cloning or DR test purposes, these recovery volumes can be used only for forensic analysis and for a relatively short duration. Therefore, ESE volumes are more suitable.

If you decide to use ESE recovery volumes, you must plan capacity for these volumes. Capacity sizing for ESE recovery volumes depends on how long you might need to keep this recovery volume copy relationship, and how much the Safeguarded Copy source volumes change while the relationship exists.

In addition, other options must be considered when sizing ESE recovery volumes. The following options are available when establishing the relationship during the recovery process between Safeguarded Copy source (H1) volume and recovery volume (R1):

- ▶ No-copy (default)
- ▶ Background copy

In a no-copy relationship, a copy on-demand is done whenever a write to a source track occurs for the first time after the relationship is established. This option is ideal when the relationship H1-R1 is needed for a relatively short period only (which it is in most cases that are used for forensic analysis, that is, hours rather than days).

Alternatively, with the **Background copy** action, only the data from source volume (H1) is copied and not the empty space; therefore, only H1 used extents are copied to recovery volumes (R1). In this case, you must provision for recovery volumes at least with the same used capacity of your production volumes.

Tip: If capacity is allocated for FlashCopy target volumes that are used for DR tests, data mining, or regular backups, this capacity can be shared with the Safeguarded Copy environment. Therefore, your FlashCopy target volumes for DR test also can be used for recovery volumes in a Safeguarded Copy relationship.

The required virtual capacity for the thin-provisioned recovery volumes is as large as the provisioned Safeguarded Copy source volume.

Safeguarded Copy source volume

If you plan to implement Safeguarded Copy in a physically isolated environment, you must consider the required physical capacity for the Safeguarded Copy source volume. The required physical capacity is the same as the safeguarded production volume capacity. The same is true for the required virtual capacity.

Defining the Safeguarded Copy source volumes as thin-provisioned (ESE volumes) also is preferable. In this configuration, the space that the source volumes are not using can be used for Safeguarded Copy backups or recovery volumes, which provide extra headroom for backups and the recovery volumes.

2.5.4 Safeguarded Copy capacity sizing methods

This section describes different Safeguarded Copy capacity sizing methods.

The required Safeguarded Copy Backup Capacity depends on the data change rate and following backup management policies:

- ▶ Frequency of backups to be taken (that is, how often they are taken)
- ▶ Retention period for the backups (that is, how long they are kept)

To determine the amount of physical and virtual capacity that is required for Safeguarded Copy backups, you must determine the data change rate for specific intervals in accordance with your backup management policy requirements (frequency and retention periods).

For example, if you were creating a backup every 6 hours and retaining it for 48 hours, you must understand the total data change rate over a 48-hour retention period.

The capacity sizing for ESE recovery volumes depends on how long you intend to keep the recovery volume copy relationship active, and how much the Safeguarded Copy source volumes change while the relationship exists.

The sizing for the Safeguarded Copy Capacity (physical and virtual) and recovery volumes can be done by using any of the methods that are described next.

All of these methods determine the data change or destage rate in tracks. This absolute number is then used for converting to GiB (or TiB) capacity (see Example 2-4 on page 54).

To calculate the required capacity that is based on the data change rate or destage rate, use a sliding sum approach to estimate the peak capacity. Therefore, add up the data change rate or destage rate in GiB (or TiB) per interval for as many intervals as the length of the retention period. Use this approach for each involved DS8000 to calculate the required physical capacity for the Safeguarded Copy backups.

You also must do the same for each Safeguarded Copy source volume to estimate the Backup Capacity Multiplier if you cannot use the simple approach by using the number of backups in a retention period as the Backup Capacity Multiplier for each volume.

You can use one of the following approaches to determine the data change rates for your workload:

- ▶ Analyzing the DS8000 Write Monitoring (WM) Bitmap (preferred method)
- ▶ Analyzing performance data such as RMF data in z/OS or IBM Storage Insights
- ▶ DS8000 CS queries
- ▶ DS8000 DS CLI `showckdvo1` or `showfbvo1` commands: destage rate

Analyzing the DS8000 Write Monitoring Bitmap

The purpose of the Write Monitoring Bitmap is to provide an effective way to determine usable space requirements for ESE FlashCopy and Safeguarded Copy without affecting host write I/O or disk replication performance.

The Write Monitoring Bitmap enables a DS8000 to track the amount and locality of its changed data over definable time intervals and across a set period in a production environment. That level of detail can readily be used to determine how much physical storage is allocated over time.

The Write Monitoring Bitmap was implemented on the DS8880 in microcode release 8.5.4 and on DS8900F 9.1. The Write Monitoring Bitmap tracks all writes for each volume, but has no other function. The bitmap can be started, stopped, reset, and queried.

The bitmap is started with all bits set to zero and acts as a Change Recording bitmap with the first update to a track setting the bit to one. The reset sets all bits back to zero.

The query provides the entire bitmap, which can then be parsed to understand the changed tracks, small extents, and large extents. With that information, you can use the Write Monitoring Bitmap for Safeguarded Copy and ESE FlashCopy sizing.

Write Monitoring Bitmap queries provide an accurate figure that is based on the workload during the period that is measured.

At the time of writing, these commands are made available through IBM CSM only. Although the ESESizer session was introduced in CSM 6.2.11, use IBM CSM 6.3.3.0 or later to query the Write Monitoring Bitmap.

The ESESizer session issues commands against a DS8000, but the ESESizer session does not need an active license and can be the CSM on an HMC.

For Safeguarded Copy sizing, the following process is used when the sizing tool is run:

1. Start Write Monitoring Bitmap on the identified volumes:
 - a. Loop for several iterations.
 - b. Sleep for a defined interval.
 - c. Query the bitmap and store the results in a CSM session database.
 - d. Reset the bitmap.
2. Stop the Write Monitoring Bitmap.

The ESESizer session generates two CSV files that can be exported and managed by using Excel. For each monitored DS8000 per interval, the storage system (box) level CSV file includes the currently allocated extents, changed tracks, changed small extents, and change large extents.

The volume-level CSV file includes the same values but separately for each volume. With that information, you can precisely calculate the required physical and virtual capacity and determine the Backup Capacity Multiplier per volume. Querying data for one or more Safeguarded Copy retention periods provides an accurate figure that is based on the current workload.

If you do not reset the Write Monitoring Bitmap during the query, you also can estimate the size of the ESE recovery volume by using the tool. Run the query if you planned to work with the recovery volume for testing purposes.

Figure 2-16 shows the prerequisites for the use of the CSM ESESizer session type to query the Write Monitoring Bitmap.

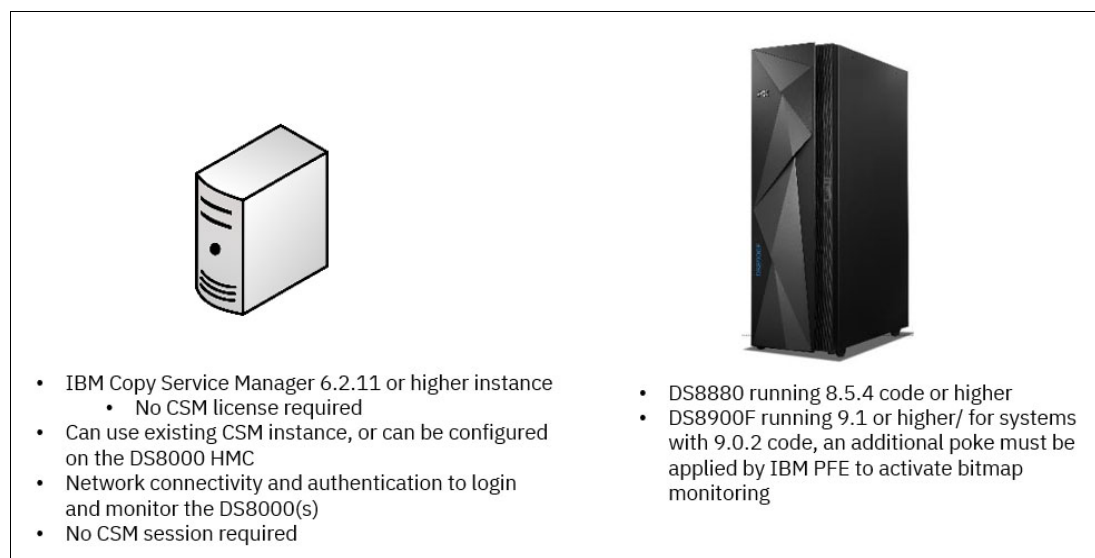


Figure 2-16 Prerequisites for query Write Monitoring Bitmap with the ESESizer session type

Note: Although the ESESizer session was introduced in CSM 6.2.11, use IBM CSM 6.3.3.0 or later to query the Write Monitoring Bitmap.

For more information about how to use the DS8000 Write Monitoring Bitmap with the ESESizer session to query changed tracks or extents, see Chapter 3, “Capacity sizing by using the IBM Copy Services Manager ESESizer functions” on page 83.

Tip: Use the Write Monitoring Bitmap sizing method if a DS8880 or a DS8900F with suitable microcode level is available for monitoring. This method provides the most accurate sizing for the Safeguarded Copy Backup Capacity.

Analyzing performance data

Performance data can be used to provide an estimate of the capacity for the Safeguarded Copy backups. This method might overestimate the Safeguarded Capacity because it does not account for tracks that are destaged multiple times within one Safeguarded Copy backup period. Therefore, it tends to be most accurate for configurations where a shorter period exists between backups.

You can use the following performance analysis tools to gather the required information:

- IBM RMF data for mainframe systems

From RMF, use the R745DCTD field (Cache to DASD XFRs) from the Cache Activity - SMF record type 74-5 report and estimate required GiB peak with a sliding sum per interval, by multiplying “GiB destaged / interval” with “number of intervals in retention period”.

R745DCTD means tracks destaged per second during SMF interval.

To calculate the GiB / interval, use the following formula:

$$\text{GiB destaged / interval} = \text{R745DCTD} * 56664 / 1024^3$$

For more information about the 74-5 record, see [Cache Activity - SMF record type 74-5](#).

- IBM Spectrum® Control or Storage Insights performance reports for open systems and mainframe

From IBM Spectrum Control or Storage Insights, use the cache-to-disk transfer rate metric for your DS8000 storage system and estimate required GiB peak with a sliding sum per interval by multiplying “GiB destaged / interval” by “number of intervals in retention period”.

The Cache-to-Disk Transfer Rate (ops/s) means tracks destaged per second.

To calculate the GiB / interval, use the following formula:

$$\text{GiB destaged / interval} = \text{“Cache-to-Disk Transfer Rate (ops/s)”} * \text{“interval in sec”} * \text{“track size”} / 1024^3$$

- FB: track size = 65536 bytes
- CKD: track size = 56664 bytes

For more information, see [Performance metrics for storage system controllers on DS8000 Storage Systems](#).

Note: Consider the following points:

- ▶ For the z/OS environment, use the RMF performance data method if no IBM disk storage system or older DS8000 disk systems are installed.
- ▶ The performance data method leads to an over-estimation if the period between backups is long because it does not consider rewrites of the same track within the same Safeguarded Copy backup.

DS8000 Copy Services queries

Another approach to determine capacity requirements for Safeguarded Copy is by using DS8000 CS queries. It is possible to use a query of a suspended MGM relationship. Alternatively (if you cannot afford to suspend your disk replication because of the strict RPO requirements), use a FlashCopy with the **NOCOPY** parameter relationship to calculate the capacity that is required for the Safeguarded Copy backups.

A CS query command provides an accurate figure that is based on the workload during the period that is measured. However, it includes the requirement to have a CS relationship or to set up such a relationship specifically for the sizing exercise. The CS relationship must be re-created or reset for each period to understand the capacity use at different times, although this effort might be less practical for situations with a smaller period between backups.

The following CS interfaces can be used to query MM, GM, or FlashCopy relationships:

▶ DS8000 DS CLI

On systems that use FlashCopy, MM, GM, or Multi-Target Peer-to-Peer Remote Copy (PPRC), you can use the DS CLI to determine the capacity that is required.

For FlashCopy, start FlashCopy **NOCOPY** and run the **1sflash -1** command to receive a count of the tracks that changed since the FlashCopy relationship was established (look for Out-Of-Sync Tracks).

For MM, GM, or Multi-Target PPRC, run the **1spprc -1** command to receive a count of the tracks that were changed since the relationship was suspended (look for Out-Of-Sync Tracks).

For more information and a full description of the **1sflash** and **1spprc** commands and other disk replication commands, see *IBM DS8000 Series Version 8 Release 5 Command-Line Interface User's Guide*, SC27-8526, and *IBM DS8000 Series Release 9 Command-Line Interface User's Guide*, SC27-9562.

▶ TSO: mainframe users only

On systems that use FlashCopy, MM, GM, or Multi-Target PPRC, you can run TSO commands to determine the capacity that is required.

For FlashCopy, start FlashCopy with the **NOCOPY** command and run the **FCQUERY** command to receive a count of the tracks that changed since the FlashCopy relationship was established.

For MM, GM, or Multi-Target PPRC, run the **CQUERY** command to receive a count of the tracks that were changed since the relationship was suspended.

For more information about the TSO **FCQUERY** FlashCopy command, see [FlashCopy query \(FCQUERY\) command](#).

For more information about the TSO **CQUERY** PPRC command, see [CQUERY - querying status](#).

► IBM CSM and GDPS

CSM and GDPS disk management replication interfaces also can be used to find OOS tracks.

In CSM, whether you use Metro or GM or a Multi-Target PPRC session, select the session and suspend it. From the session overview window, in the Participating Role Pairs table, you can monitor the tracks that were changed since the relationship was suspended under the Progress columns. Mouse cursor the xx% remaining and you can see the number of remaining tracks to be copied. Alternatively, you can use the CSM FlashCopy session (with **NOCOPY**).

Similarly, with GDPS managed disk replication, you can run a Flash command if your GDPS configuration defined FlashCopy volumes. Otherwise, suspend your session and monitor Out-Of-Sync Tracks with the query command options from ISPF windows.

Note: This method might require interventions in the customer environment. Therefore, it is likely not the best approach to gather the required data change rate, although it provides accurate data.

DS8000 DS CLI showckdvol or showfbvol commands: Destage rate

The DS CLI **showckdvol** or **showfbvol** commands can also be used to determine the changed data rate for individual volumes you want to protect with Safeguarded Copy. However, this method might over-estimate the Safeguarded Copy Backup Capacity because it does not account for tracks that are destaged multiple times within one backup period. Therefore, it tends to be most accurate for configurations where a shorter period exists between backups.

Use the **metrics** parameter (see Example 2-3) and look for **cachetrans** data. **Cachetrans** indicates the Cache to DASD Transfer Operation Count, and it is a count of destaged tracks.

Example 2-3 DS CLI showckdvol command

```
dscli> showckdvol -metrics 0B00
Date/Time: July 19, 2021 12:40:16 AM CEST IBM DSCLI Version: 7.9.20.431 DS:
IBM.2107-75xxxxx
ID                                0B00
Date                              07/19/2021 00:40:17 CEST
...
cachetrans                      713992
...
```

The same output with the **cachetrans** metric is available by using the **showfbvol** command for FB data.

To obtain a clear history of the destage rate on your system, query the **cachetrans** metric periodically (for example, every 30 minutes) and gather approximately one week's worth of destage data. To ensure that the virtual capacity accommodates your backups, use the number of destaged tracks from a peak period that matches the period of your Safeguard schedule.

For example, if your Safeguard Copy retention period is 72 hours, you might find 15,000,000 destaged tracks within a peak 72-hour period.

Summary

Each of these sizing methods provides several changed tracks for each host volume in the configuration over the total retention time for the backups. The number of changed tracks can be converted to actual usable capacity measured in binary; for example, in GiB. In Example 2-4, you can see how the required capacity is calculated for the specific backup retention period, interval, and total destaged tracks for the retention period. This example shows the conversion method for CKD and FB.

Example 2-4 Converting total number of tracks into GiB capacity

Backup retention period = 48 hours

Backup interval = 2 hours

Total number of destaged tracks in 48 hours = 15,000,000

DS8000 is configured with small extents:

CKD small extent size = 21 cylinders = 315 tracks = 0.016613 GiB

FB small extent size = 256 tracks = 0.015626 GiB

Convert the number of destaged tracks to extents:

CKD extents: $15,000,000 / 315 = 47,619$ extents

FB extents: $15,000,000 / 256 = 58,594$ extents

Convert extents to GiB

CKD capacity in GiB: $47,619 \text{ extents} * 0.016613 \text{ GiB} = 791 \text{ GiB}$

FB capacity in GiB: $58,594 \text{ extents} * 0.015626 \text{ GiB} = 916 \text{ GiB}$

Important: Make sure that you analyze representative peak intervals and periods. Analyze different days, weeks, and end-of-month workloads to capture the highest activity period.

2.5.5 General Safeguarded Copy sizing considerations

Capacity planning is important for Safeguarded Copy. Extrapolate data out of the DS8000 Write Monitoring Bitmap, your performance reports, or DS8000 CS to determine day-to-day data change rates during normal operation.

Also, be aware of different scenarios that might cause a total data loss. The scale and severity of logical data corruption must be considered when planning for capacity. For example, if all host volumes are accidentally formatted, the Safeguarded Copy Backup Capacity uses extents up to the total capacity of Safeguarded Copy source volumes.

Similarly, malicious intent to destroy a large amount of data in a short period can cause a similar effect. After only a few backup intervals, you might experience a high data rate change because repeated overwrite of source data volumes. You also might use more than 100% of the total Safeguarded Copy Backup Capacity that is allocated to your source volumes before you realize you are under attack.

2.6 Safeguarded Copy backup priority consideration in an out-of-space situation

As mentioned in 2.5.2, “Safeguarded Copy Backup Capacity” on page 44, it is important to size properly the Safeguarded Copy physical and virtual capacity to avoid an out-of-space situation (either the physical capacity in a storage pool or the Safeguarded Copy virtual capacity of a volume).

With DS8880 and DS8900 running microcode earlier than Rel.9.3.2, the host workload or replication workload has a higher priority than Safeguarded Copy backups if an out-of-space situation occurs. Therefore, if a write I/O against a Safeguarded Copy source volume causes a space threshold to be reached, the DS8000 microcode deletes the oldest backup of this volume to allow the write I/O to complete. If the space that is constrained still exists, the DS8000 deletes older backups until only the last (current active) backup exists. If only one backup exists, the Safeguarded Copy Source volume becomes write-inhibited.

As stated before, an out-of-space situation can occur because of physical space constraints in a storage pool or because of a small defined Backup Capacity Multiplier (Safeguarded Copy virtual capacity) for a volume. With DS8880 and DS8900 running microcode earlier than Rel.9.3.2, the default space thresholds for Safeguarded Copy are as follows:

- ▶ 90% usage of a storage pool (extentpool)
- ▶ 98% usage of defined volume Safeguarded Copy virtual capacity

If one of these conditions is reached, the DS8000 starts to roll off the oldest backup of the volume that causes this condition.

Starting with DS8900 microcode Rel.9.3.2, clients can decide whether Safeguarded Copy should have a higher priority than a host workload or a replication workload if an out-of-space situation occurs. Clients can decide how many backups should be kept if a space threshold is reached. Therefore, a new control switch was introduced that can be set 0 - 500.

- ▶ The default setting is 1, where the behavior is like former DS8000 microcode releases, as described above.
- ▶ A setting of 0 terminates Safeguarded Copy processing. No more data is stored in the backup, and you cannot recover a backup.
- ▶ A setting of 500 means that a DS8000 cannot roll off a backup in an out-of-space situation.

Note: If a setting of 500 is used, your management software still manages the backup retention period. To change this default behavior through this control switch, contact IBM DS8000 support.

In DS8000 microcode Rel.9.3.2, the default space thresholds for Safeguarded Copy are as follows:

- ▶ 98% usage of a storage pool (extentpool)
- ▶ 98% usage of defined volume Safeguarded Copy virtual capacity (same as before)

With this new control switch, you have more flexibility regarding Safeguarded Copy backup priority, which helps to fulfill different client requirements. Which value should be selected depends on a client's business requirements.

2.7 Safeguarded Copy performance considerations

Small extents are preferred for more efficient capacity usage and better performance because volume metadata is stripped across many physical flash drives. Moreover, when sequential writes are performed to allocated storage, small extents can use many more flash drives in parallel than large extents.

With large extents, the first 1 GiB (FB) or 1,113 cylinders (CKD) of writes are performed to a single eight drive array; the next large extent is written to the next array and continuing in that same manner for subsequent writes. However, because small extents are much more granular (smaller in size for both FB and CKD), subsequent writes to the next array occur far more often; for example, FB small extents are 64 times more granular than its large extents, and CKD small extents are 53 times more granular than large extents.

Therefore, with small extents, subsequent writes to the next array for FB occur after 16 MiB are written; and for CKD, it is after 21 cylinders are written. As a result, more flash drives are active for the write stream for small extents than for large extents. This issue is true for fully provisioned and thin-provisioned volumes for FB and CKD writes.

The DS8880 can be configured as an all flash array, that is, as a 'hybrid' with both flash drives and hard disk drives (HDDs), or with all HDDs. Because the Safeguarded Copy Backup Capacity uses thin provisioning and recovery volumes also can be thin-provisioned, consider adding flash drives to a DS8000 with HDDs and reviewing the flash configuration on a hybrid.

Volume metadata is stored on the flash drives (when present) to ensure the best metadata performance. A best practice for hybrid DS8880 systems that use thin-provisioned volumes and small extents is to spread the flash drives across three High-Performance Flash Enclosure (HPFE) pairs to ensure that global metadata is also spread across three PCI device adapter pairs. That layout ensures good metadata performance.

Regardless of the technology that is used, creating data consistency across many volumes has some effect (small and negligible) on application I/Os. The same is true with DS8000 CS, such as MM or FlashCopy with CGs and similar services.

Safeguarded Copy was designed to create CGs with minimum performance effect. As with FlashCopy CGs, Safeguarded Copy uses the ELB state logic to pause some work in progress at the time of capture, which puts all dependent writes in a point-in-time consistent state.

With DS8880 8.5 SP7, DS8900F R9.1 SP1 and later performance improvements are implemented for creating backups, especially for environments with a higher amount of volume on a single DS8000 system. These enhancements reduce the effect of creating backups and provide the capability to create more often backups in virtual isolated environments.

With the latest DS8900F 9.3, a Safeguarded Copy performance enhancement is implemented to reduce back-end utilization by using destage grouping to copy data to the Safeguarded Copy Backup Capacity. Also, a reduction in reservation time is introduced by improving the reservation scan algorithm during backup creation.

In addition to these performance enhancements, with CSM 6.2.11 or later, customers can associate the session with a z/OS sysplex in the properties for a Safeguarded Copy session. When a sysplex is associated, the necessary commands are passed down to the IOS component on z/OS to perform the Safeguarded Copy backup, which dramatically improves performance and minimizes the impact on applications.

It is a best practice that any customer who wants to safeguard production volumes in a mainframe environment use this function. For more information about the prerequisites, see 2.4.1, “IBM Copy Services Manager” on page 39. For more information about how to implement the function, see 4.2.1, “Verifying and modifying the Safeguarded Copy session properties” on page 130.

When the performance sizing is done for the DS8000 systems that create the Safeguarded Copy backups, consider the Safeguarded Copy workload as one FlashCopy **nocopy** (copy on write) relationship for all Safeguarded Copy source volumes. Add this extra workload to your performance model and check whether the DS8000 system can handle the added workload for all peak intervals, especially for the write throughput peak interval.

FlashCopy onto Safeguarded Copy source volumes

FlashCopy onto a Safeguarded Copy source volume is supported starting from DS8900F 9.3. Both full-volume FlashCopy and data set FlashCopy are supported onto a Safeguarded Copy source volume. However, you must plan for Safeguarded Copy Backup Capacity when performing full-volume FlashCopy onto a Safeguarded Copy source. A full-volume FlashCopy implies that many tracks in the Safeguarded Copy source volume are changed; hence, Safeguarded Copy Backup Capacity is needed for these updates.

The main use case for supporting FlashCopy onto Safeguarded Copy is to support data-set-level FlashCopy in environments where Safeguarded Copy is running on an MM primary or secondary. FlashCopy onto Safeguarded Copy source volume is useful if a small set of volumes, for example, the volumes containing IBM Db2® Image Copy backups, must be restored from the Safeguarded Copy backup.

If many volumes are copied by full-volume FlashCopy onto a Safeguarded Copy source, it might cause the Safeguarded Copy Backup Capacity to be exhausted. If the FlashCopy is established just before the next Safeguarded Copy backup is created, it might cause the backup to time out because there is not enough time to copy all the data during the Safeguarded Copy reservation phase.

Important: A new Safeguarded Copy backup must be created with the new microcode Rel. 9.3 before establishing a FlashCopy onto Safeguarded Copy source volumes. The new DS8900F microcode Rel. 9.3 is using a different bitmap layout for Safeguarded Copy that must be active before establishing the FlashCopy onto Safeguarded Copy source volumes.

2.8 Monitoring Safeguarded Copy

The Safeguarded Copy environment can be monitored and controlled from IBM CSM or from the GDPS LCP Manager. In this section, we focus on CSM.

Note: For more information about how to monitor the Safeguarded Copy environment with GDPS LCP Manager, see the GDPS manuals.

The health of CSM Safeguarded Copy sessions is reflected from their status and state through color-coded symbols and diagrams. CSM receives alerts directly from DS8000 concerning various conditions that are occurring in the Safeguarded Copy environment. Based on those conditions, they might change the session status and state. All messages are logged in the CSM console log, and alert notifications can be sent by way of email or SNMP.

In addition to CSM, various DS8000 DS CLI and Storage Management GUI messages are generated during the Safeguarded Copy creation or regular backup operations. These messages are related to volumes that are participating in a Safeguarded Copy relationship, and they are displayed in the DS CLI or DS8000 event log when those volumes are created or modified. Critical alerts, such as running out of space, are sent to hosts (for example, z/OS SYSLOG, Open Systems Syslog servers, or SNMP listener).

For z/OS environments, there are more messages that are available to monitor the Safeguarded Copy capacity and the physical capacity of the DS8000 storage pools to avoid out-of-capacity situations.

Note: A new message generation enhancement was introduced in DS8000 microcode Rel.9.3.2. By using it, an LPAR that is controlled by GDPS may receive out-of-space messages that are generated by a managed DS8000 if at least one device per DS8000 cluster is online. This approach minimizes the need for logical paths and volumes to be defined to a system like an LPAR that is controlled by GDPS. It also limits any extra message presentation to only systems that need the message.

To use this enhancement, you must use GDPS 4.5 with APAR PH50146, and SDM APAR OA63501 for z/OS 2.4 or 2.5 and DS8900 microcode Rel.9.3.2.

2.8.1 Using IBM CSM for Safeguarded Copy session monitoring

IBM CSM is a central place to look for all events and messages, and to check the status and state of your Safeguarded Copy session.

To check the status of your Safeguarded Copy session, select the **Sessions** link from the main top menu selection in your CSM, as shown in Figure 2-17.

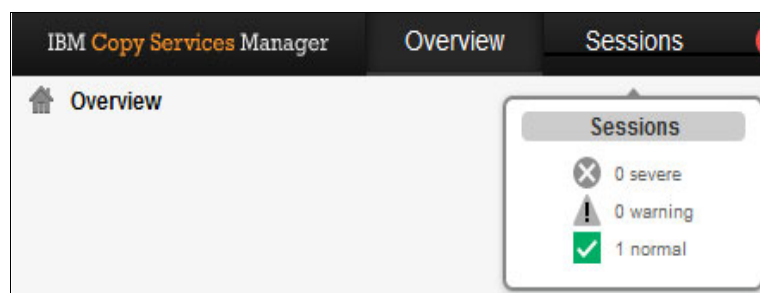


Figure 2-17 CSM Sessions link

When you click the Safeguarded Copy session hyperlink, more information is presented about the session, as shown in Figure 2-18 on page 59.

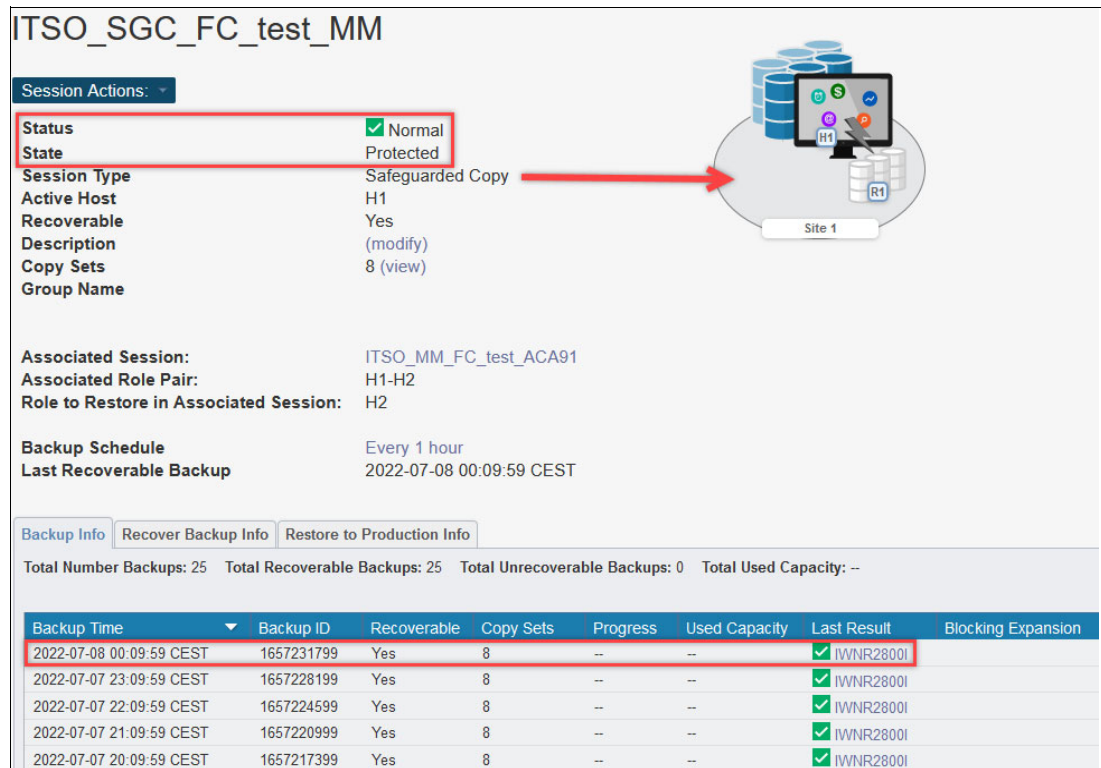


Figure 2-18 CSM Safeguarded Copy session details

The session Status and State are displayed in the left side of the window. Each CSM session type has its own unique icon or diagram representation. For a Safeguarded Copy session, two sets of volumes are defined: H1 Safeguarded Copy source volumes (darker blue volumes) and R1 Recovery volumes (as shown in Figure 2-19).

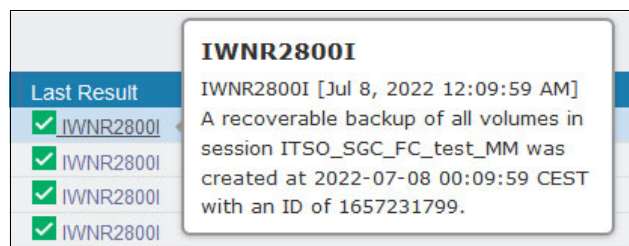


Figure 2-19 Safeguarded Copy session message details

Light blue disk cylinders represent Safeguarded Copy Backup Capacity. A FlashCopy relationship between H1 and R1 also is shown. In our example, this FlashCopy is inactive because the FlashCopy arrow is gray (for more information about FlashCopy symbols, see “Monitoring session icons and symbols” on page 60).

Each message is a hyperlink. You can get more information by hovering the mouse over the specific message or by clicking it (see Figure 2-19).

Alternatively, all messages can be displayed in the CSM Console, which can be accessed from the CSM main top menu, as shown in Figure 2-20.

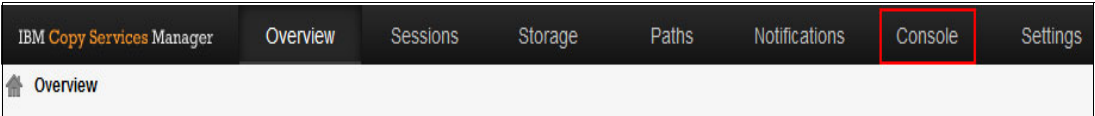


Figure 2-20 CSM Console link

In the CSM Console, you find your CSM session messages and their related details, for example, the timestamp, who ran a specific action, and a description. In our example that is shown in Figure 2-21, a backup command was issued by the CSM server because it was started by a predefined CSM Scheduled task.

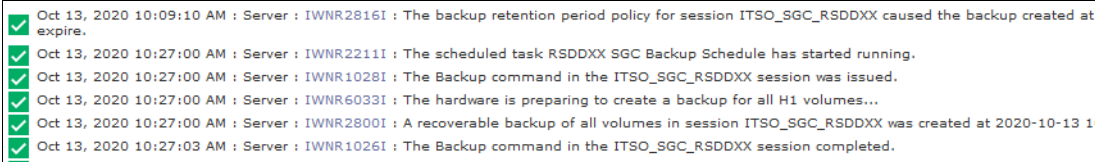


Figure 2-21 CSM Console log abstract

The following most common messages are found in the console during normal Safeguarded Copy operation:



- ▶ IWNR1028I: Command issued
 - ▶ IWNR1026I: Command completed
 - ▶ IWNR2211I: Scheduler Task started
 - ▶ IWNR2800I: A recoverable backup of all volumes in session xxx was created
 - ▶ IWNR2816I: One or more Backup versions expired
- Note:** Messages IWNR2211I, IWNR1028I, and IWNR1026I are *not* specific for the Safeguarded Copy session type.

Monitoring session icons and symbols

The CSM GUI uses icons to represent the status of the Safeguarded Copy session or severity of each message. The Table 2-2 lists the session status icons and the message severity.





Table 2-2 CSM session Status and Message Severity symbols

Icon	Status/Message severity	Description
	Normal	A consistent copy of the data exists or is being maintained. The Safeguarded Copy session is in Normal Status when the State is Protected or Target Available. This icon also is used to represent Safeguarded-related messages without any errors or warnings.
	Warning	Safeguarded Copy is in Warning status, which means that your session might be in an unrecoverable state. This issue can exist when you run the Backup command for the first time, or if you add copy sets to a session and new backups were not taken. When a subsequent backup is performed, the session turns in Normal status.

Icon	Status/Message severity	Description
	Severe	One or more errors exist that you must address immediately. A possible cause might be that a backup failed because of a lack of space in the storage pool. The Safeguarded Copy session also turns to Severe status if you add copy sets while the session is in Target Available state. Therefore, the newly added volumes are not yet recoverable. After two new backups, the newly added copy sets are recoverable, and the session changes to the <i>Warning</i> status.
	Inactive	This symbol indicates that the session is defined, but with no activity on the hardware.

To understand H1-R1 FlashCopy relationship activity, different symbols are used that indicate whether the FlashCopy is active, inactive, or with errors, as listed in Table 2-3.

Table 2-3 CSM FlashCopy symbols

Symbol	Description
	Active FlashCopy operation. You see this icon whenever you use the Recover Backup or Initiate Background Copy actions.
	Active FlashCopy operation with one or more pairs in error. For example, FlashCopy is not established because the volume is targeted to some other FlashCopy relationship. Review the CSM console to learn more details and potential reasons for these errors.
	Inactive FlashCopy operation.
	Inactive FlashCopy operation with one or more pairs in error. Check the CSM console to learn more details and potential reasons for these errors.

CSM alert notifications

CSM can deliver the following types of alerts:

- ▶ Email alerts
- ▶ SNMP notifications

CSM sends email alerts if any session changes its status or state, but also for other events, such as configuration change and any CSM communication failures (to defined storage systems).

The same is true for SNMP alerts, which are sent with associated object IDs (OIDs) to your defined SNMP listener.

For more information about how to set up CSM email and SNMP alert notifications, see the following resources:

- ▶ *IBM Copy Services Manager, Version 6 Release 3 User's Guide*, SC27-8542
- ▶ [IBM Documentation](#)

2.8.2 Safeguarded Copy capacity warning messages for z/OS

The most challenging task when planning for Safeguarded Copy is sizing the overall required capacity for backups and recovery volumes storage pools. No matter how careful you are with Safeguarded Copy Backup Capacity sizing, you might still exhaust your storage pools.

Therefore, capacity alert notifications that are sent to your host can help you rectify that problem if you take prompt action. For example, you can expire the oldest backup versions to release some space, dynamically expand the Safeguarded Virtual Capacity, migrate Safeguarded Copy backups in a new storage pool with more space, or add capacity to the storage pool, if possible.

The host receives messages when the physical space has exceeded a threshold or is exhausted for a storage pool. Moreover, some storage pool statistics also are provided. These messages and statistics can help monitor and analyze your Safeguarded Copy environment, which help you with better capacity planning for future growth.

A new important information message that was introduced with APAR OA55440 for Safeguarded Copy is IEC817I. This message indicates per volume that a space constraint threshold was reached for a Safeguarded Copy Backup Capacity.

In addition to the IEC817I, it is important to monitor the IEA499E message that is related to storage pool capacity, for example, threshold capacity warnings for the storage pool with your production and Safeguarded Copy Backup Capacity allocations. For more information about these messages, see *z/OS MVS System Messages, Vol 7 (IEB-IEE)*, SA38-0674.

As shown in Example 2-5, messages IEC817I and IEA499E are captured in z/OS SYSLOG.

Example 2-5 IEC817I and IEA499E messages

17.52.14 SYSTEM1	IEC817I 0F43,IN0F40,0111,3008,002107.951.IBM.75.0000000TN141,BACKUP
VOLUME CAPACITY WARNING: AT 15% CAPACITY	
REMAINING	
17.54.13 SYSTEM1	IEC817I 0F43,IN0F40,0111,3008,002107.951.IBM.75.0000000TN141,BACKUP
VOLUME CAPACITY	
EXHAUSTED	
17.57.04 SYSTEM1	IEC817I 0F43,IN0F40,0112,3008,002107.951.IBM.75.0000000TN141,BACKUP
VOLUME CAPACITY RELIEVED	
18.03.52 SYSTEM1	*IEA499E 0F43,IN0F40,0112,3008,002107.951.IBM.75.0000000TN141,EXTENT
POOL CAPACITY WARNING: AT 15% CAPACITY	
REMAINING	
18.06.28 SYSTEM1	*IEA499E 0F43,IN0F40,0112,3008,002107.951.IBM.75.0000000TN141,EXTENT
POOL CAPACITY EXHAUSTED	

A new message is generated whenever the specific capacity threshold is reached (in our example, at 15% capacity remaining and when the backup or storage pool capacity is exhausted).

Note: The following hardware and software is required to resolve message IEC817I:

- ▶ Install z/OS APAR OA55440. For more information, see [APAR OA55440](#).
- ▶ DS8000 microcode level 8.5 SP11 or R9.2 SP2 or R9.3

2.8.3 DS8000 DS CLI and Storage Management GUI messages

DS CLI and Storage Management GUI messages are grouped in the following categories:

- ▶ Informational
- ▶ Warning
- ▶ Error

The following informational messages are logged in the DS8000 event log:

- ▶ Safeguarded capacity for volume <volName> created
- ▶ Safeguarded capacity for volume <volName> expanded
- ▶ Safeguarded capacity for volume <volName> deleted
- ▶ Safeguarded capacity for volume <volName> migrating to pool <newPool>
- ▶ Safeguarded capacity for volume <volName> finished migrating or redistributing capacity
- ▶ Safeguarded backups for volume <volName> scheduled
- ▶ Safeguarded backups for volume <volName> unscheduled

The following warning message is logged in the DS8000 event log:

Safeguarded capacity for volume <volName> is <percentFull>% full

The following error messages are logged in the DS8000 event log:

- ▶ Safeguarded backup for volume <volName> rolled off because of insufficient Safeguarded virtual capacity
- ▶ Safeguarded backup for volume <volName> rolled off because of insufficient pool capacity

Note: These messages are displayed only in the DS8000 Event Log at microcode levels R9.2 or R8.5 SP9 and later.

2.8.4 Monitoring Safeguarded Copy capacity and automating Safeguarded Copy capacity dynamic expansion

In addition to the event log and z/OS messages, you might want to monitor the used Safeguarded Copy capacity per volume and the storage pool capacity.

Thus, automation can be put in place to perform an action when high utilization is detected. One way for Safeguarded Copy Virtual Capacity is to monitor the occurrence of message IEC817I. When the IEC817I message occurs, a job can be triggered to run a DS CLI command to expand the Safeguarded Copy capacity dynamically. Another way of doing that task is to run scripts or jobs to run the DS CLI command or the z/OS IDCAMS **LISTDATA** command to list all Safeguarded Copy capacity regularly and check whether the used capacity is above a certain threshold. If the used Safeguarded Copy capacity is above the threshold, run the DS CLI command to dynamically expand the Safeguarded Copy Virtual Capacity for particular volumes.

Example 2-6 shows an example DS CLI command to display the Safeguarded Copy Virtual Capacity per volume.

Example 2-6 DS CLI command example for listing Safeguarded Copy Virtual Capacity

```
dsccli> lsckdvol -sgc DDOC-DDOF
NameIDextpool cap (cyl) safeguardedcap (cyl) safeguardedloc usedsafeguardedcap (cyl)
safeguarded sgcrecovered safeguardedcapstate
=====
=====
```

```
ckd_p9_DD0C DD0C P930051 45077P910500YesNoNormal
ckd_p9_DD0D DD0D P930051 45077P910500YesNoNormal
ckd_p9_DD0E DD0E P930051 45077P910500YesNoNormal
ckd_p9_DD0F DD0F P930051 45077P910500YesNoNormal
```

Example 2-7 shows examples of an **LISTDATA** command to list used Safeguarded Copy Virtual Capacity.

Example 2-7 LISTDATA commands example for listing Safeguarded Copy Virtual Capacity

LISTDATA VOLSPACE SSYS FILE(SEFLC1)

Note: Safeguarded Copy source volume must be online.

SSYS and ALL works as a parameter.

(specify DD statement, for example,

SEFLC1 DD UNIT=3390,VOL=SER=SGA100,DISP=SHR)

DEVICE	VOLSER	CAPUSED	CAP	POOL	ID	SAM	EXTENT
A000	SGA100	1029	10017	0000	ESE		
	SGCB	21	30051	0000	ESE		
A001	SGA101	1029	10017	0000	ESE		
	SGCB	0	40068	0000	ESE		
TOTAL NUMBER OF STANDARD (FP) VOLUMES:							0
TOTAL NUMBER OF EXTENT SPACE EFFICIENT VOLUMES:							2
TOTAL NUMBER OF VOLUMES WITH Safeguarded Copy Backup Capacity:							2

LISTDATA VOLSPACE VOLUME(SGA10A) UNIT(3390) SUBSYSTEM

Note: Safeguarded Copy source volume must be online.

SSYS and ALL works as a parameter.

DEVICE	VOLSER	CAPUSED	CAP	POOL	ID	SAM	EXTENT
A008	SGA108	3003	30051	0000	ESE		
	SGCB	63	90153	0000	ESE		
A009	SGA109	1029	30051	0000	ESE		
	SGCB	63	90153	0000	ESE		
A00A	SGA10A	7980	30051	0000	ESE		
	SGCB	6027	90153	0000	ESE		
A00B	SGA10B	1029	30051	0000	ESE		
	SGCB	63	90153	0000	ESE		
TOTAL NUMBER OF STANDARD (FP) VOLUMES:							0
TOTAL NUMBER OF EXTENT SPACE EFFICIENT VOLUMES:							4
TOTAL NUMBER OF VOLUMES WITH Safeguarded Copy Backup Capacity:							4

LISTDATA VOLSPACE DEV UNITNUMBER(A000)

Note: Safeguarded Copy source volume must be offline.

SSYS and ALL are not working with the VOLSPACE / UNITNUMBER parameter.

DEVICE	VOLSER	CAPUSED	CAP	POOL	ID	SAM	EXTENT
A000		1029	10017	0000	ESE		
	SGCB	21	30051	0000	ESE		
TOTAL NUMBER OF STANDARD (FP) VOLUMES:							0
TOTAL NUMBER OF EXTENT SPACE EFFICIENT VOLUMES:							1
TOTAL NUMBER OF VOLUMES WITH Safeguarded Copy Backup Capacity:							1

GDPS Logical Corruption Protection Safeguarded Copy Statistics

For customers that use GDPS LCP Manager, virtual capacity usage information can be listed on the GDPS Logical Corruption Protection Safeguarded Copy Statistics panel. Virtual capacity usage information is displayed for the Safeguarded Copy source volume, as shown in Figure 2-22. Virtual Used% shows the percentage of virtual capacity that is used currently by the Safeguarded Copy source volume.

Management Profile: SGC1XHOUR Latest Seqno: 62B345C6
 Consistency Group: G8A2B UTC TimeStamp: 2022/06/22.16:39:34
 Replication Site: 1 Oldest Seqno: 62B2FB8C
 Volumes Protected: 38 UTC TimeStamp: 2022/06/22.11:22:52
 Detected Captures: 3

Actions: Q uery P ools

UCB	Volser	SafeGuarded Source	Pool ID Src Bkp CapI Cyls	Virtual CapM Used%	Oldest Seqno	Flags PBRP..
0190A	PX8LC1	00KYR91.33.0A	001 005 0003 003339	0001 002.516	62B2FB8C	FYNN..
0190B	PX8LC2	00KYR91.33.0B	001 005 0003 003339	0001 002.516	62B2FB8C	FYNN..
0190C	PX8NV1	00KYR91.33.0C	001 005 0003 003339	0001 001.887	62B2FB8C	FYNN..
0190D	PX8NV2	00KYR91.33.0D	001 005 0003 003339	0001 003.774	62B2FB8C	FYNN..
0190E	CD8ALG	00KYR91.33.0E	001 005 0003 003339	0001 006.226	62B2FB8C	FYNN..
0190F	PX8LG2	00KYR91.33.0F	001 005 0003 003339	0001 001.887	62B2FB8C	FYNN..
01910	PX8GD0	00KYR91.33.10	001 005 0003 003339	0001 002.516	62B2FB8C	FYNN..
01911	PX8W00	00KYR91.33.11	001 005 0003 003339	0001 002.516	62B2FB8C	FYNN..
01912	PX8W01	00KYR91.33.12	001 005 0003 003339	0002 001.258	62B2FB8C	FYNN..
01913	PX8SP0	00KYR91.33.13	001 005 0003 003339	0001 005.031	62B2FB8C	FYNN..

Command/Filter ==> Row 11 of 38
 F1=Help F3=Return F4=Monitor F5=Refresh F6=Roll F7=Up F8=Down

Figure 2-22 GDPS Logical Corruption Protection Safeguarded Copy Statistics panel

This panel provides a range of filtering and SORT capabilities. Filtering can be used to reduce the list to display only the volumes exceeding the warning threshold. For example, all volumes with Virtual Used% above 85% can be displayed by using the filter command **FILTER USED(85,GT)**. Figure 2-23 shows an example of a filtered display.

Management Profile: SGC1XHOUR Latest Seqno: 62B345C6
 Consistency Group: G8A2B UTC TimeStamp: 2022/06/22.16:39:34
 Replication Site: 1 Oldest Seqno: 62B2FB8C
 Volumes Protected: 38 UTC TimeStamp: 2022/06/22.11:22:52
 Detected Captures: 3

Actions: Q uery P ools

UCB	Volser	SafeGuarded Source	Pool ID Src Bkp CapI Cyls	Virtual CapM Used%	Oldest Seqno	Flags PBRP..
0190E	CD8ALG	00KYR91.33.0E	001 005 0003 003339	0001 006.226	62B2FB8C	FYNN..

Command/Filter ==> Row 1 of 1
 F1=Help F3=Return F4=Monitor F6=Roll F7=Up F8=Down

Figure 2-23 GDPS Logical Corruption Protection Safeguarded Copy Statistics panel with a filter applied

2.8.5 Monitoring a DS8000 extent pool

For monitoring used capacity in a DS8000 storage pool, you can use a DS CLI command, the IDCAMS **LISTDATA** command in z/OS environments, or the DS8000 Storage Pool Capacity Report in GDPS. In z/OS environments, DS CLI or **LISTDATA** commands can be used for creating scripts to run a space release by using the DFSMSdss **SPACEREL** command against volumes in the particular DS8000 storage pool when high utilization is detected.

DS CLI command example

To query the used capacity in the extent pool, run the DS CLI command **showextpool**, as shown in Example 2-8.

Example 2-8 DS CLI command example for listing extent pool utilization

```
dsccli> showextpool p0
Name                CKD
ID                  P0
stgtype             ckd
totlstor (2^30B)    10278
availstor (2^30B)   8884
resvdstor (2^30B)    1
rankgrp             0
numranks            1
numvoIs             1266
status              below
%allocated          13
%available           86
configured           618257
allowed             618204
available            534403
allocated            83801
reserved            53
configuredCap(MiB/cyl) 12983397
allowedCap(MiB/cyl)  12982284
availableCap(MiB/cyl) 11222463
allocatedCap(MiB/cyl) 1759821
reservedCap(MiB/cyl) 1113
%limit              100
%threshold           15
virextstatus         full
%virallocated        0
%viravailable        0
virconfigured        0
virallowed           0
viravailable         0
virallocated         0
virreserved          0
%virextlimit         -
%virextthreshold     -
keygrp               1
opratio              1.85
opratiolimit         -
%allocated(ese)      6
%allocated(rep)      0
%allocated(std)      6
%allocated(over)     1
%virallocated(ese)   -
%virallocated(tse)   -
%virallocated(init)  -
```

%migrating(in)	0
%migrating(out)	0
numtiers	1
etmanaged	yes
etmigpauseremain	-
etmonpauseremain	-
etmonitorreset	unknown
extsize	21cyl
%allocated(over)	0
%virallocated(ese)	-
%virallocated(tse)	-
%virallocated(init)	-
%migrating(in)	0
%migrating(out)	0
numtiers	2
etmanaged	yes
etmigpauseremain	-
etmonpauseremain	-
etmonitorreset	unknown
extsize	21cyl

z/OS IDCAMS LISTDATA command example

In z/OS environments, to query the extent pool size and number of allocated pools in cylinders, run the IDCAMS **LISTDATA EXTENTPOOLCONFIG** command, as shown in Example 2-9.

Example 2-9 LISTDATA command example for listing the extent pool allocated capacity

```
LISTDATA EXTENTPOOLCONFIG EXTENTPOOLID(8) VER1 UNITNUMBER(DC00)
```

```
.....EXTENT POOL ID 0008 SUMMARY.....
REPOSITORY FULL WARNING PERCENTAGE:          0
EXT POOL FULL WARNING PERCENTAGE:             45
EXTENT POOL STATUS
    FIXED BLOCK EXT POOL:                      NO
    REPOSITORY CONFIGURED:                     NO
    EXTENT POOL AT WARNING PERCENTAGE:         NO
    SGC BACKUP VOLUMES CONFIGURED:             YES
    ...EXTENT POOL 0008 DETAILED REPORT VERSION 1...
EXTENT POOL REPOSITORY STATUS
    REPOSITORY AT WARNING PERCENTAGE:          NO
    REPOSITORY FULL:                          NO
    SIZE                                       ALLOCATED
EXTENT POOL      10301907                    2921373
REPOSITORY        0                          0
```

GDPS DS8000 Storage Pool Capacity report

For customers that use GDPS LCP Manager with APAR PH37133 for the Logical Corruption Protection feature of GDPS, DS8000 Storage Pool Capacity reports can be generated by using the GDPS user interface. The reports can be based on either the copy sets that are associated with a Management Profile or the copy sets that are associated with a CG within a specified replication site. The report displays capacity and usage information by GiB or GB Capacity, or Extents, as shown in Figure 2-24 and in Figure 2-25.

Consistency Group: G8A2B
Replication Site: 1

Actions: Details

Storage System	Pool Type	Extent Size	Usable Capacity	Provisioned Capacity	Available Capacity	%Used
00KYR91	0 CKD	21cyls	60,650.20	49,885.22	12,824.08	78.86
00KYR91	1 CKD	21cyls	60,650.20	59,511.06	4,791.74	92.10
00KYR91	5 CKD	21cyls	4,279.48	34,398.56	3,505.68	18.08

Capacity=GiB

Command =====>
F1=Help F3=Return F5=Refresh F6=Roll F7=Up F8=Down F9=Toggle

Figure 2-24 Storage Pool Capacity Report displayed by GiB

Consistency Group: G8A2B
Replication Site: 1

Actions: Details

Storage System	Pool Type	Extent Size	Usable Capacity	Provisioned Capacity	Available Capacity	%Used
00KYR91	0 CKD	21cyls	3,648,500	3,000,917	771,451	78.86
00KYR91	1 CKD	21cyls	3,648,500	3,579,973	288,254	92.10
00KYR91	5 CKD	21cyls	257,438	2,069,295	210,889	18.08

Toggling to Extents based capacity reporting
Capacity=Extents

Command =====>
F1=Help F3=Return F5=Refresh F6=Roll F7=Up F8=Down F9=Toggle

Figure 2-25 Storage Pool Capacity Report displayed by Extents

In the GDPS DS8000 Storage Pool Capacity Report panel, a detail report can be requested for a specific storage pool in the list. The detail report displays the detailed capacity information in more detail, as shown in Figure 2-26.

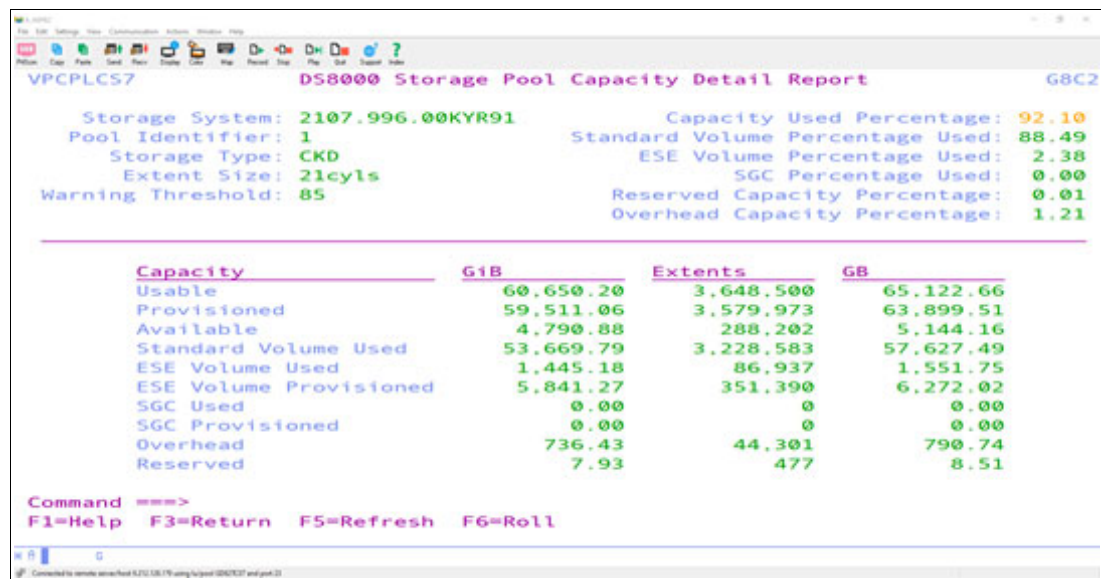


Figure 2-26 Storage Pool Capacity Detail Report

2.9 Security considerations

One of the main objectives for Safeguarded Copy is to quickly enable recovery after data is (accidentally or deliberately) compromised. For example, someone might accidentally delete backup versions or source volumes that are Safeguarded Copy protected.

With Safeguarded Copy, storage administrators can ensure that data is kept safe, secure, and recoverable in a way that is transparent and easy to manage. One aspect of security is addressed with different user roles and authority levels that are used to manage the source volumes, backup capacity, and recovery volumes involved in a Safeguarded Copy relationship.

At least the following interfaces are required to create, enable, and manage Safeguarded Copy:

- ▶ The DS8000 DS CLI or Storage Management GUI to create the Safeguarded Copy Backup Capacity
- ▶ The GDPS LCP manager or IBM CSM to enable and alter the session

Therefore, access to one or the other interface can be limited and restricted to specific storage administrators. Moreover, each administrator who is responsible for backups can have restricted access to a specific CSM Safeguarded Copy session and therefore access to a limited range of volumes that are defined in the DS8000 system and managed by CSM.

Another security feature is the protection of the source volumes that are in the Safeguarded Copy relationship. These source volumes cannot be deleted from the DS8000 Storage Management GUI or DS CLI, even by running the **force** command while they are in a Safeguarded Copy relationship. Safeguarded Copy source volumes can be deleted only if they are no longer in a Safeguarded Copy relationship; for example, if the volumes are removed from a CSM session (by removing the Safeguarded Copy hardware relationship) or removed from the GDPS LCP management profile.

2.9.1 More DS8000 security considerations and CSM “dual control”

A Safeguarded Copy implementation is enabled through coordinated configuration activities on the DS8000 to logically configure the Safeguard Copy Backup Capacity and the Safeguarded Copy management application (that is, CSM or GDPS LCP) to set up and run Safeguarded Copy. The DS8900F and CSM offer enhanced user management to further limit changes to a defined set of actions by a single user or dual control, which requires two authorized users to confirm a specific task (or action) to be completed.

The DS8900F provides a storage administrator with the ability to create custom user roles with a fully customizable set of permissions to complete only authorized actions (see Figure 2-27). Those permissions help ensure that the authorization level of each user matches their job role so that the security of the system is more robust against internal attacks or mistakes.

Permission	Allowed	
> Array and Pools	<input checked="" type="checkbox"/>	
> IBM Z Volumes and LSSs	<input checked="" type="checkbox"/>	
Configure IBM Z volumes and LSSs	<input checked="" type="checkbox"/>	
Manage IBM Z volumes, LSSs, and aliases	<input checked="" type="checkbox"/>	
Delete/Reinitialize IBM Z volumes	<input type="checkbox"/>	
> Open System Volumes	<input checked="" type="checkbox"/>	
> IBM i Volumes and LSSs	<input checked="" type="checkbox"/>	
> Local and Remote Access Management	<input type="checkbox"/>	

Figure 2-27 DS8000 Create Custom User role

Changes to user roles and permissions are dynamic and can be completed on demand by an authorized user. Logical configuration changes to a DS8000 often are infrequent and limited to a new implementation or as part of upgrading an implementation.

Therefore, you might want to consider granting configuration change authorization to users only during a “change window” rather than having it at all the time. Also, to create a separation in configuration change authorizations, you can assign create or add privileges to one user and delete privileges from another user.

For an added level of security, starting with version 6.2.5, CSM introduced dual control functions that require two users with the proper authority to perform specific tasks (or actions). Dual control is enabled through two users with Administrator or User Administrator authority (see Figure 2-28). This feature prevents malicious actions by a disgruntled storage administrator and an inadvertent action by a well-intended user.

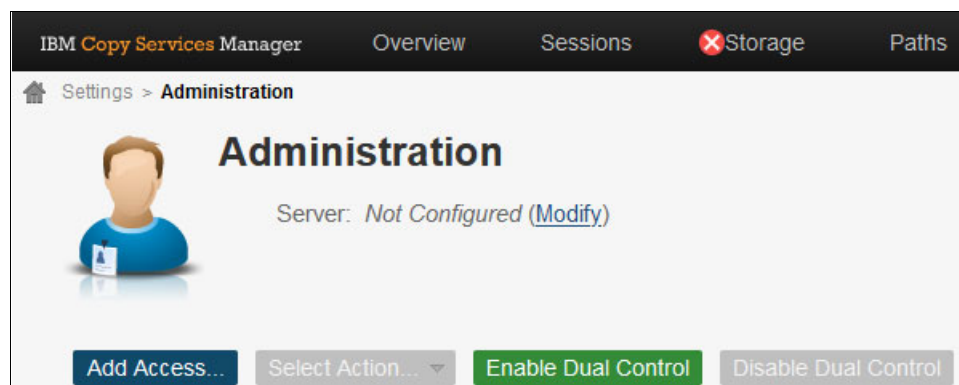


Figure 2-28 CSM Enable Dual Control window

Dual control for a specific task (or action) requires two users with authorization for that task (or action) for the CSM session to confirm that the task (or action) should be taken. After dual control is implemented, changes to any FlashCopy (Point-in-Time Copy or PtC), MM (HA), GM (DR), or Safeguarded Copy (LCP) session requires confirmation from two authorized users. Because PtC, HA, DR, and LCP solutions are implemented to provide availability and recoverability (that is, protect the business), dual control is a best practice.

For more information about how to implement dual control, which actions it covers, and how to prevent a potential lockout, see [IBM Documentation](#).

Important: Care should be taken to ensure that the same person does not have access to two user IDs with sufficient authority to effectively self-confirm changes to any replication environment, whether it be PtC, HA, DR, or LCP.

2.10 Safeguarded Copy backup use case considerations

The DS8000 Safeguarded Copy function does not provide any integrated data validation or forensic analysis function. It is crucial to plan and validate those tasks and actions to establish a complete cyber resiliency solution. As described in 1.1.3, “Use cases for data protection” on page 4, typical use cases for Safeguarded Copy function include data validation, forensic analysis, surgical recovery, catastrophic recovery, and offline backup.

The user must plan for data analysis and validation and restoration of the protected copies to the production environment based on the environment, the selected topology in which Safeguarded Copy is implemented, and on business requirements.

In general, you must understand which parts and how much of your data became corrupted and determine which backup is the last backup that was taken before the corruption event.

Various methods are available to accomplish these tasks. General guidance about typical use cases is provided in this section. For more information about planning and the setup of the IBM Z Cyber Vault solution, see *Getting Started with IBM Z Cyber Vault*, SG24-8511.

Note: In addition to the data validation and restore capability, it is important to detect a cyberattack or insider threat. Therefore, implementing a solution or software that helps to detect a data corruption, such as IBM Z Cyber Vault, IBM Guardium, or IBM QRadar, also is important.

2.10.1 Data validation

For data validation, it is good practice to establish a stand-alone environment that is dedicated specifically to that function so that you can perform proactive and reactive data validation. It is essential to practice the data validation process to ensure that it works if a real-world logical corruption event occurs.

For data validation, a best practice is to establish new servers, or in a z/OS environment, new LPARs that are outside of the production sysplex and not connected to the outside world. This configuration allows you to recover a Safeguarded Copy backup to restart or perform an IPL of the systems in an isolated environment.

If you are planning to automate the data validation process within a separated environment, you might need to store some data that is produced during the data validation process, for example, the validation results. Therefore, it is a best practice to create extra persistent volumes for storing this data.

If you know that a catastrophic corruption event occurred, your first step in the data validation process is to perform an IPL of or restart your systems from the most recent unaffected Safeguarded Copy backup.

If the IPL is successful, then you can perform some basic infrastructure function tests. In a z/OS environment, these tests include checking the Sysplex structure, data sharing, Logger, and JES2.

The next step is to continue with a data structure validation and check the database structures. For that process, z/OS provides several tools, such as Db2 Utility Suite or IMS High Performance Pointer Checker, to speed up the validation processing.

Now, you might want to begin some forensic analysis by using some of the available middleware tools. The following software products for an z/OS environment can support the analysis:

- ▶ IBM Tivoli® Advanced Catalog Management for z/OS
- ▶ IBM Advanced Audit for DFSMSHsm
- ▶ zSecure
- ▶ Db2 Recovery Expert
- ▶ Db2 Object Recovery
- ▶ MS Recovery Expert

The final and most complicated step is to use customer-facing applications to validate the data content, if required.

If you know that only a limited set of the data was corrupted, only the necessary volumes might be recoverable from a Safeguarded Copy backup. Then, you can begin the process of forensic analysis, which is followed by a surgical recovery of the valid data.

Based on your findings in the data validation process, you must decide on the best process to restore the valid data to your production systems.

2.10.2 Forensic analysis

When data corruption is detected, whether it is by software detecting a data error or regular data validation on the Safeguarded Copy backup, it is important that the investigation is done to determine what data was corrupted, when the data was corrupted, and how the data got corrupted.

During the forensic analysis process, you investigate problems and check which recovery actions must be done. To successfully do so, you must have a system that resembles the production environment at the time of the corruption. Multiple versions of data might have to be restored to discover the corruption and identify a valid copy of data. Therefore, you might need extra sets of recovery volumes, so planning of extra storage is needed.

For small-scale data corruption, it might be possible that the corruption can be fixed within the production environment. When it is determined that the corrupted data must be restored from backup, the scale of data corruption and consistency of data determines whether the data recovery from a Safeguarded Copy backup can be a surgical recovery or a catastrophic recovery.

2.10.3 Surgical recovery

If during the forensic analysis, you discover that you must recover only portions of the data, you can do a selective restore, which is also known as a *surgical recovery*. For a surgical recovery, you potentially need some extra volumes that might be accessible from your data validation and your production environment. Those volumes, also known as *staging volumes*, are volumes that are used to store a validated version of recovered data sets to restore them to production. You can use standard operating system or application methods to copy the data that you need from the recovery volumes or staging volumes to the production volumes if the recovery / staging volumes are in one of the production DS8000s (that is, a virtual isolation topology).

Note: It is not possible to use a cascaded FlashCopy from the recovery volume to another volume if the Safeguarded Copy recovery action is done with the **nocopy** option. If FlashCopy will be used to copy data from a Safeguarded Copy recovery volume, the Safeguarded Copy recovery action must be done with the **copy** option, and the FlashCopy relationship from the Safeguarded Copy recovery volume to another volume can be established only after the Safeguarded Copy backup is fully copied to the recovery volume.

An important consideration of using surgical recovery is data consistency. Ensure that there is consistency between the specific part of data that is recovered from backup and the current production data.

2.10.4 Catastrophic recovery

Implementing the Safeguarded Copy function makes sense only if a validated process is in place to restore the required Safeguarded Copy backup to your production environment. Depending on the amount of data that was affected by the logical corruption event and the implemented production environment topology, the process to restore the data might differ.

If you must perform a catastrophic recovery because the data corruption is extensive, a full restore of a Safeguarded Copy backup is required. For that full restore, you must establish an infrastructure that allows you to restore the data in a short period. This task requires enough DS8000 resources and adequate bandwidth in the SAN infrastructure between the recovery volumes and the production volumes.

A best practice is to use Global Copy to replicate the data from the recovery volumes to the production volumes if a full restore is required (see the blue arrow in Figure 2-29).

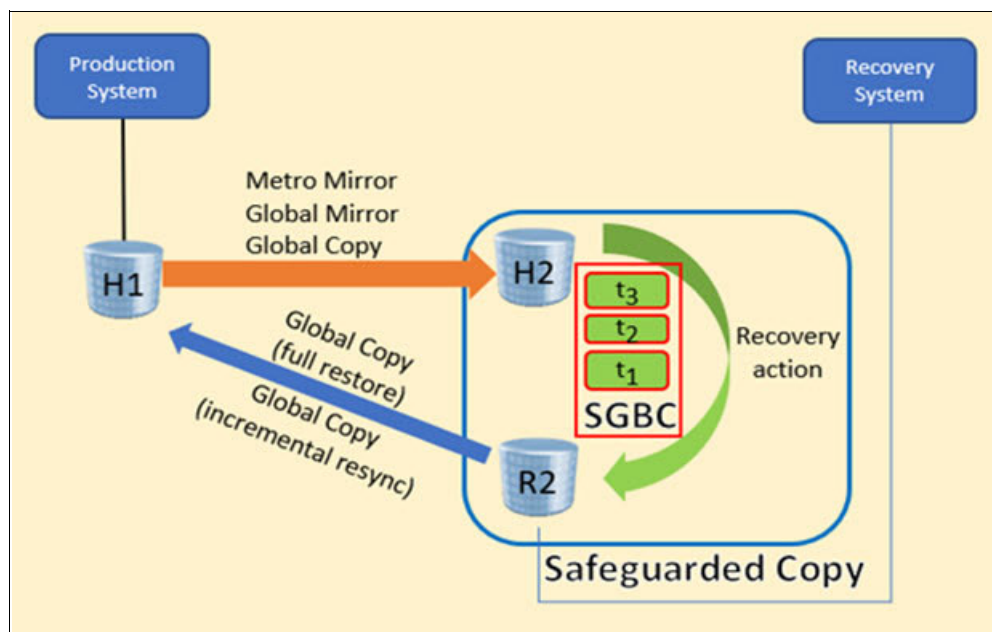


Figure 2-29 Common Safeguarded Copy backup restore infrastructure

Figure 2-29 shows a configuration that must be established when a full restore of a Safeguarded Copy backup is required. To restore, you suspend the H1 → H2 relationship and then establish a Global Copy from R2 to H1. You can prepare this Global Copy relationship so that it is ready and can be easily established if a catastrophic event occurs.

Note: Global Copy full copy is required if the Safeguarded Copy source is on a DS8880 R8.5 or a DS8900F R9.1 and earlier.

For DS8900F R9.2 and above, Global Copy incremental resync and full copy are available.

Note: It is not possible to use a cascaded FlashCopy from the recovery volume to another volume if the Safeguarded Copy recovery action is done with the **nocopy** option. If FlashCopy will be used to copy data from a Safeguarded Copy recovery volume, the Safeguarded Copy recovery action must be done with the **copy** option, and the FlashCopy relationship from the Safeguarded Copy recovery volume to another volume can be established only after the Safeguarded Copy backup is fully copied to the recovery volume.

With CSM 6.3.0 and DS8900F 9.2, now you can use Safeguarded Copy backups to restore data to production by using incremental resync Global Copy. This capability enables you to restore only the data that changed since the last Safeguarded Copy backup and supports both logically and physically isolated topologies. The Safeguarded Copy source volumes must be in a CS replication topology (MM, GM, or GC) or any combination of them.

The following topologies are tested:

- ▶ MM with Safeguarded Copy on the secondary
- ▶ GM with Safeguarded Copy on the secondary
- ▶ MT MM/MM with Safeguarded Copy on the MM secondary
- ▶ MT MM/GM with Safeguarded Copy on the MM secondary
- ▶ MT MM/GM with Safeguarded Copy on the GM secondary
- ▶ MGM (cascaded that uses incremental resync) with Safeguarded Copy on the tertiary
- ▶ 4-site MT MM/GM - cascaded GC off GM with Safeguarded on the GM secondary
- ▶ Cascaded GM

With CSM 6.3.1 and DS8900F 9.2.1, an enhancement was introduced to allow restore to production if the primary volume (H1) is the Safeguarded Copy source volume by using incremental resync Global Copy. The following CSM session types are supported for an incremental restore for H1 volumes:

- ▶ MM
- ▶ GM
- ▶ GM either direction
- ▶ MT MM-GM
- ▶ MT MM-GM in cascaded mode
- ▶ MT MM-MM
- ▶ MM - GM with Site 4 Replication
- ▶ MM - MM with Site 4 Replication

Note: Restore to production from H1 as the Safeguarded Copy source volume is not supported for cascaded three site sessions (MGM session) because there is no way to restore to the H2 volume and failback H2 to H1.

Also, a restore against a site that contains PRACTICE volumes is not supported.

Note: Consider the following points:

- ▶ For GDPS LCP Manager, the required steps to restore a validated Safeguarded Copy backup to production can be different.
- ▶ Thorough analysis and validation of the recovered backup data should be performed before continuing to restoring more data.
- ▶ During the restore process, all data that is changed on the recovery volume during data validation or analysis is withdrawn and the original backup is restored.
- ▶ In a 2-site CS replication environment (MM or GM), you must shut down the production applications before running the **Restore Backup** command.

For more information about the implementation of this function, see Chapter 4, “Implementation and management” on page 117.

2.10.5 Offline backup

An offline backup to tape can be used to create a second layer of defense and provide a longer retention period and increased isolation and security by providing a media brake and air-gap. Using WORM tape technologies provide a secure copy on either virtual or physical tape devices.

For a fast dump to tape process, you should consider establishing FlashCopy nocopy from your source volumes to the recovery volumes in parallel to the Safeguarded Copy backup creation. This action provides better throughput performance for the dump to tape process compared to recovering a Safeguarded Copy backup onto the recovery volumes and then starting the dump to tape process.

When using a Safeguarded Copy backup as a point-in-time offline backup copy, consider your business requirements to determine the following items:

- ▶ How often a backup is required to be taken.
- ▶ Retention period for the backup copy.
- ▶ The extent of isolation that is needed for the Safeguarded Copy backup.

2.11 Configuration changes considerations

You can modify or change the Safeguarded Copy environment by using the CSM interface and DS8000 DS CLI or GUI.

DS8000 DS CLI or GUI is used for the following tasks:

- ▶ Create Safeguarded Copy Backup Capacity for new volumes that you want to protect.
- ▶ Create recovery volumes.
- ▶ Migrate Safeguarded Copy Backup Capacity from one pool to another one.
- ▶ Dynamically expand the Safeguarded Virtual Capacity.
- ▶ Delete the Safeguarded Copy backup.

All the previous DS CLI or GUI changes do not affect an active Safeguarded Copy session. Migration of Safeguarded Copy Backup Capacity is concurrent. You cannot delete Safeguarded Copy Backup Capacity if an active Safeguarded Copy session is available for the associated volume. Therefore, the main changes that can affect the Safeguarded copy status and state are done by using the CSM interface.

The following changes can be made by using CSM:

- ▶ Add or remove copy sets into an active Safeguarded Copy session.
- ▶ Modify session properties dynamically.

For more information, see Chapter 4, “Implementation and management” on page 117.

2.11.1 Copy set management

This section describes copy set management and Safeguarded Copy session behavior.

Adding copy sets

If you add volumes to your production environment (for example, because you need more capacity), you add those new volumes to the Safeguarded Copy configuration. From this point, your Safeguarded Copy CGs are larger than before. However, the existing backups still consist of fewer volumes than the ones that you create after the configuration change. If you must recover to an older backup, the content of the newly added volumes is invalid.

By adding new Safeguarded Copy source volumes, you also change the hardware configuration of your production environment so that the newly added volumes are recognized and can be used. If you must recover your Safeguarded Copy environment to a point-in-time where the new volumes contain invalid data, you must reverse the hardware configuration changes in such a way that these volumes are not accessed anymore.

Note: If you add volumes to an IBM z/OS environment, you make these new volumes known to the systems by adding them to the Input/Output Definition File (IODF). If you must recover to a backup that does not contain the new volumes, a possible way to avoid these volumes being accessed is to undo the IODF changes.

Adding copy sets into an active Safeguarded Copy session can change the session status to Warning or Severe. The status depends on the state of the session when the copy sets are added.

If the session status is Normal and the state is Protected while copy sets are added, the Safeguarded session status changes to Warning, but still with the Protected state. At least one recoverable backup version is available for this session, but it does not include all the copy sets in the session. This issue causes the session to be not fully recoverable.

The session status changes back to Normal after one new backup is created. If the next scheduled backup is hours away, you might want to perform a manual backup after adding copy sets. As shown in Figure 2-30, after adding one copy set, nine copy sets are among the recent backup versions.

Backup Info Recover Backup Info Restore to Production Info								
Total Number Backups: 26 Total Recoverable Backups: 26 Total Unrecoverable Backups: 0 Total Used Capacity: --								
Backup Time	Backup ID	Recoverable	Copy Sets	Progress	Used Capacity	Last Result	Blocking Expansion	
2022-07-08 04:15:53 CEST	1657246553	Yes	9	--	--	✓ IWNR2800I		
2022-07-08 03:37:09 CEST	1657244229	Yes	9	--	--	✓ IWNR2800I		
2022-07-08 03:32:41 CEST	1657243961	Yes	9	--	--	✓ IWNR2800I		
2022-07-08 03:09:59 CEST	1657242599	Yes	8	--	--	✓ IWNR2800I		
2022-07-08 02:09:59 CEST	1657238999	Yes	8	--	--	✓ IWNR2800I		
2022-07-08 01:09:59 CEST	1657235399	Yes	8	--	--	✓ IWNR2800I		

Figure 2-30 CSM Backup Info table

Now, with nine copy sets in this example, if you try to recover any older backup version with fewer than nine copy sets, the session changes to the Warning status. Warning message IWNR1045W with corresponding children messages IWNR2037W are logged in the CSM log, which indicates that a newly added volume does not exist in the recovered backup.

If you attempt to add copy sets while the session state is Target Available, the session changes to the Severe status, as shown in Figure 2-31.



Figure 2-31 CSM Safeguarded Copy in the Severe status

After you create one backup, the session changes from the Severe status back to Warning and Target Available state. Another method is to sever the recovery volume relationship by issuing a **Terminate H1>R1** action.

Removing copy sets considerations

Removing copy sets from a Safeguarded Copy Session is more critical than adding them. Carefully consider such an action because you can remove volumes containing data that potentially might be required as part of a recovery option. Therefore, you must ensure that no relevant data exists on these copy sets or volumes, or you might lose your LCP.

Important: It is a best practice to wait with the removal of the volumes until all Safeguarded Copy backups that rely on them are expired.

When copy sets are removed from a session that is in a Normal status and a Protected state, the session status and state do not change. If a session is in a Warning or Severe status and you remove copy sets that caused the non-normal status, then the status returns to Normal.

When removing copy sets from the Safeguarded Copy session, the following options are available:

- ▶ Remove the hardware relationships.
- ▶ Keep the base hardware relationships on the storage system.

By removing the hardware relationships, you terminate the backup process and delete all previous backups for these volumes. If you keep the hardware relationships, the previous Safeguarded Copy backups still exist on the DS8000. However, new backups for the session are not created for these volumes.

Volumes with Safeguarded Copy backups can be assimilated into Safeguarded Copy sessions. This process is done by adding copy sets that contain those volumes as H1 volumes. CSM matches the timestamps and sequence numbers of the backups of the added volumes and adapts the recovery points.

Restoring to production copy set considerations

If you are planning to use the restore to production function that was introduced with DS8000 9.2, consider the following points:

- ▶ Adding or removing copy sets (Safeguarded Copy restore to production)

Configuration changes must be performed in both CSM sessions, that is, the replication session and the Safeguarded Copy session. CSM marks both sessions as in a Warning state if mismatches are found after the Safeguarded Copy session is associated to the replication session.

Removal of Safeguarded Copy copy sets deletes all Safeguarded Copy backups of the removed volume (unless the option to keep the base hardware relationship is used).

The volumes also are removed from previous backup sets of the session.

Adding Safeguarded Copy copy sets provides a complete backup only for *future* Safeguarded Copy backups.

Previous backup sets do *not* contain the added volumes unless CSM found backups on the hardware and assimilates them into the previous backup sets.

- ▶ Recovering a previous backup set to the recovery volumes

The added volumes that are not contained in the recovered backup cannot establish a recovery FlashCopy relationship. As a result, the session is in Target Available state and Warning status.

The new recovery volumes cannot create the internal OOS bitmap for incremental failback.

Unrecovered H1-R1 pairs are shown as in a Defined state rather than Target Available in the Recover Backup Info tab.

- ▶ Restoring a partially recovered backup is not supported

The restore to production solution is designed to restore all production volumes to a previous Point-in-Time copy. If newer production volumes cannot be restored, a data consistency issue might occur between the restored and unrestored production volumes.

CSM remains in a Restoring state if not all pairs in the session can be prepared for the incremental Global Copy Failback.

Use the **Terminate H1-R1** command to return to a Protected state.

- ▶ Restoring an older, partial Safeguarded Copy backup

To restore an older, partial backup, complete the following steps:

- a. In the Safeguarded Copy session, remove the added copy sets that are not contained in the recovered backup to be restored. For more information, see “Recovering a previous backup set to the recovery volumes”.

Keep the existing hardware relationship upon removal to maintain newer backups of the removed volumes so that they can be used at a later point, if needed.

- b. Restore the remaining volumes back to production volumes by using the **Restore Backup** command.

Important: Because a mismatch exists between the Safeguarded Copy restored volumes and the primary volumes of the associated replication session, the data of the restored volumes might be inconsistent with the volume data that is not included in the restored backup.

The Safeguarded Copy session can now complete the restore operation, clean up the recovery relationships, and transition the session into a Protected state again.

- c. When you are ready to use the restored data for production, you can add the removed copy sets back into the Safeguarded Copy session again.

CSM discovers backups for the added volumes and assimilates them into the previous backup sets. Use **Refresh States** if backups are not refreshed with added volumes that are contained the Safeguarded Copy backups.

The volume mismatch warning in both sessions should disappear, and future Safeguarded Copy backups contain all production volumes.

Increasing the retention period or backup frequency

Because of SLAs or other reasons, you might need to expand the retention period or increase the frequency of the Safeguarded Copy backups. Both operations might require more physical capacity and change the Safeguarded Virtual Capacity per volume.

Note: Consider the following points:

- ▶ It is a best practice to estimate the required Safeguarded Copy Backup Capacity before you expand the retention period or increase the backup frequency.
- ▶ Starting with DS8880 8.5 SP7 and DS8900F 9.1, it is possible to dynamically expand the Safeguarded Virtual Capacity of volumes, even though they are in an active Safeguarded Copy relationship.

2.11.2 Dynamic Safeguarded Copy Backup Capacity expansion

Safeguarded Copy Backup Capacity dynamic expansion is the ability to expand the defined space that maintains the immutable copies of a Safeguarded Copy implementation without affecting its Safeguarded Copy backups.

Use cases include the need to increase the Safeguarded Copy Backup Capacity to meet current retention policies because of increased workload or anticipated workload growth, and Safeguarded Copy requirements that changed because of internal drivers, such as new business requirements or external factors, such as expanded requirements from industry regulators. In the latter case, the frequency of backups changed to become more frequent, the retention period increased, or both frequency and retention increased.

For example, a customer might start with Safeguarded Copy backups taken every hour and maintained them for 2 days (that is, a rolling 48 hours, which means 48 backups). Then, they decide that they must extend that retention to 4 days (that is, a rolling 96 hours, which means 96 backups). All that is required is the correct amount of free space and a suitable microcode level on the DS8000.

For more information about how to dynamically expand Safeguarded Virtual Capacity, see 4.2.5, “Expanding Safeguarded Virtual Capacity” on page 150.

DS8900F systems require microcode release 9.1 or later. For DS8900F systems, Safeguarded Copy dynamic expansion can be effected by using the Storage Management GUI or the DS CLI. DS8880 systems require microcode 8.5.7 or later. For DS8880 systems, Safeguarded Copy dynamic expansion can be effected through the DS CLI only.

2.12 Safeguarded Copy considerations


Consider the following points when planning for Safeguarded Copy implementation:

- ▶ Safeguarded Copy operates on the volume level. The data set or file levels are not supported.
- ▶ The DS8000 maintains a maximum number of 500 backups per volume. If you attempt to create more, the oldest backups are automatically expired.
- ▶ The CSM Scheduler allows a minimum of 5 minutes between backups. If you intend to schedule the interval for less than 10 minutes (through the CSM Scheduler or your own custom scripts), IBM requires that you submit an RPQ for approval and support. Backups can be created manually. Consider this issue carefully to avoid a potential effect on the production performance.
- ▶ The maximum Safeguarded Copy Backup Capacity for a volume is 16 TiB.
- ▶ Starting with microcode release 9.3 on the DS8900F, you can create a FlashCopy copy onto a Safeguarded Copy. Before 9.3, a Safeguarded Copy source could not be a FlashCopy target. z/OS DFSMS APAR OA62836 is needed for new sense data that is available.
- ▶ Starting with microcode release 9.3 on the DS8900F, Remote Pair FlashCopy (RPFC) is supported.
- ▶ The source and recovery volumes must be managed by the same DS8000 internal server. Therefore, they both must be in an even or odd logical subsystem (LSS).
- ▶ Starting with release 8.5.7 on the DS8880 and release 9.1 on the DS8900F, you can expand the Safeguarded Copy Backup Capacity for source volumes that are in an active Safeguarded Copy relationship.
- ▶ DS8000 Dynamic Volume Expansion (DVE) is not supported for Safeguarded Copy source volumes.
- ▶ During a Safeguarded Copy recovery action with the no-copy option, a cascaded FlashCopy from the Recovery volume to another volume is not possible.

Note: Consider the following points:

- ▶ Beginning with DS8900F 9.1, you can release space for a volume that is in a Safeguarded Copy relationship.
- ▶ During a Safeguarded Copy recovery action (with the **NOCOPY** option), a cascaded FlashCopy from the recovery volume to another volume is *not* supported.

Important: A new Safeguarded Copy backup must be created with the new microcode Rel. 9.3 before establishing a FlashCopy onto Safeguarded Copy source volumes. The new DS8900F microcode Rel. 9.3 is using a different bitmap layout for Safeguarded Copy that must be active before establishing the FlashCopy onto Safeguarded Copy source volumes.



Capacity sizing by using the IBM Copy Services Manager ESESizer functions

IBM Copy Services Manager (CSM) 6.2.11 introduced the ESESizer session type, which supports capacity calculations for DS8000 Extent Space Efficient (ESE) FlashCopy and Safeguarded Copy. The session queries the DS8000 Write Monitoring (WM) Bitmap that was implemented with DS8880 8.5.4 and DS8900F 9.1 to track all writes to each volume. It also provides two output files that simplify capacity calculations.

For more information about the DS8000 Write Monitoring Bitmap, see “Analyzing the DS8000 Write Monitoring Bitmap” on page 49.

This chapter describes how to configure the ESESizer session for querying the Write Monitoring Bitmap. It also describes how to perform the capacity sizing based on the ESESizer output files with the separately delivered Excel spreadsheets.

This chapter includes the following topics:

- ▶ 3.1, “Introducing the ESESizer” on page 84
- ▶ 3.2, “IBM Copy Services Manager ESESizer session overview and prerequisites” on page 85
- ▶ 3.3, “CSM ESESizer session preparation considerations” on page 85
- ▶ 3.4, “Preparing and configuring an ESESizer session for querying a DS8000 Write Monitoring Bitmap” on page 87
- ▶ 3.5, “Capacity sizing based on the ESESizer output files” on page 97
- ▶ 3.6, “Safeguarded Copy capacity sizing overview and example” on page 110

3.1 Introducing the ESESizer

When customers want to implement DS8000 Safeguarded Copy or ESE FlashCopy, they are interested in how much storage capacity is required to make sure that they are not running out-of-space because not enough physical storage capacity is available in the storage systems.

To simplify the sizing effort, DS8000 development implemented the Write Monitoring Bitmap in the DS8880 and DS8900F systems. To query the Write Monitoring Bitmap, IBM introduced in CSM 6.2.11 or later a session type that is called *ESESizer*. The combination of both functions dramatically reduces the sizing effort.

This chapter describes how to configure the ESESizer session for querying the Write Monitoring Bitmap. It also describes how to perform the capacity sizing based on the ESESizer output files with the separately delivered Excel spreadsheets. You can download the Excel spreadsheets from this [IBM Support web page](#).

The Excel spreadsheets provide an easy way to make a capacity sizing for ESE FlashCopy and Safeguarded Copy. After using the spreadsheet, you know the required physical capacity for the monitored volume range, and you get also the information about the required virtual capacity and the backup capacity multiplier for each volume for Safeguarded Copy. With that information, you can prepare your environment for Safeguarded Copy or ESE FlashCopy.

The Excel spreadsheets support the ESESizer session configuration and capacity sizing that is based on the ESESizer session output CSV files.

If you need support for a Safeguarded Copy capacity sizing, contact your IBM representative.

At the [IBM Support web page](#), a .zip file is available that contains the following files:

- ▶ A spreadsheet to create IBM CSM copy sets files that can be imported in to the session based on the DS Command-line Interface (DS CLI) commands **1sckdvol** and **1sfbvol**:
DS8000 Import dscli volume list to prepare CSM ESEsizer session copysets.xlsb
- ▶ A spreadsheet for ESE FlashCopy and Safeguarded Copy capacity calculation for Fixed Block (FB) or Count Key Data (CKD) Volumes:
CSM ESEsizer CSV Output Files calculation.xlsb

After running the provided Excel spreadsheet, you know the required physical capacity for the monitored environment. For Safeguarded Copy, you also get information about the required virtual capacity and volume backup capacity multiplier for each volume that is used to prepare the Safeguarded Copy function in the DS8000.

3.2 IBM Copy Services Manager ESESizer session overview and prerequisites

Querying the Write Monitoring Bitmap requires a CSM instance to issue the commands against a DS8000. However, this process does not require an active CSM license and the CSM instance can run on a DS8000 Hardware Management Console (HMC), where it is installed per default since DS8880 8.1.

The ESESizer session is available for the storage types DS8880 and DS8900F only. The session requires only one set of volumes. These volumes should be the production, FlashCopy source, or Safeguarded Copy source volumes for which the capacity sizing is wanted.

The ESESizer session queries the Write Monitoring Bitmap and provides output files on storage system (“box”) and on volume-level. These output files contain the allocated extents, and changed tracks, small extents, and large extents. That level of detail can be used to calculate how much capacity is allocated over time for both functions ESE FlashCopy and Safeguarded Copy.

The ESESizer session can start, stop, and reset the Write Monitoring Bitmap. With the available session properties, you can define the volume query interval and the bitmap reset interval. The correct setting of those parameters for your purpose is important to query the data correctly so that the capacity sizing is accurate.

The following prerequisites must be met to use the ESESizer session:

- ▶ IBM CSM 6.3.0.0 or later (No active CSM license is required.)
- ▶ DS8880 8.5 SP4 or later or DS8900F 9.1 or later

Note: Although the ESESizer session was introduced with CSM 6.2.11, it is a best practice to use CSM 6.3.3.0 or later for the ESESizer session.

3.3 CSM ESESizer session preparation considerations

Before preparing your ESESizer session, consider that querying the Write Monitoring Bitmap means that the entire bitmap of each volume is read during the query process. This situation can lead to a higher CSM server resource requirement compared to other CSM session types.

Note: We recommend that you do not run the ESESizer session on a CSM server that is running other sessions.

Therefore, consider the following points:

- ▶ Querying a large environment with large volumes or with a larger number of volumes can take some time. If you must run the ESESizer for larger capacity (greater 200 TB) and short retention period (equal or less 30 minutes), consider splitting the queries over multiple CSM servers.
- ▶ Querying larger environments requires a larger amount of server memory for the CSM Java heap. The CSM server that is running on an HMC might not have a large enough Java heap size that is configured for CSM, which can cause memory constraints. For more information, see Table 3-1.

Table 3-1 Recommended CSM Java heap size for a ESESizer session

CSM Java heap size	Queried DS8000 capacity
4 GB	<= 20 TiB
8 GB	<= 60 TiB
16 GB	> 60 TiB

Hint: In larger environments that require more than 4 GB Java heap size, you might split the queries over multiple CSM servers.

- ▶ To avoid overusing a CSM server, consider the use of a separate CSM server that is not running production replication sessions.
- ▶ If more than one storage system must be queried in a larger environment, use different ESESizer sessions on different CSM servers.
- ▶ Use the latest available CSM server version for running the ESESizer session.
- ▶ Use different sessions for FB and CKD volumes because the track and extent sizes are different for these volumes. The output files do not indicate whether a volume is an FB or CKD volume.
- ▶ Set the session properties as required for the different copy service functions, Safeguarded Copy, and ESE FlashCopy. For more information, see 3.4.3, “Configuring the ESESizer session” on page 92.
- ▶ Use the session to query data for a longer period or a multiple of the planned lifetime of the FlashCopy targets or Safeguarded Copy backups. For example, if the planned Safeguarded Copy retention period is 24 hours, gather the data for at least a week to catch the data change rate peaks. For example, if an IBM Db2 reorg occurs during the monitoring period, the change rate will be included into the report.
- ▶ The ESESizer calculator processes the maximum change rate for each volume during the monitoring period, which might result in a higher than expected capacity requirement due to SMS group configuration and application design. For example, an SMS storage group has 50 volumes that are tiered for different applications. One application has a heavy write workload that uses only 10 volumes (such as a full backup). Other applications employ incremental backups with low or moderate write activity. Based on the SMS group configuration, it is possible that a different set of 10 volumes can be used during the monitoring period, thus skewing the numbers.
- ▶ Do not use the same volume in two active ESESizer sessions at the same time.

3.4 Preparing and configuring an ESESizer session for querying a DS8000 Write Monitoring Bitmap

The only purpose for the ESESizer session is to query the DS8000 Write Monitoring Bitmap for a set of volumes and provide output files at the box- and volume-level for capacity calculations for Safeguarded Copy or ESE FlashCopy.

An active ESESizer session stores the Write Monitoring Bitmap results for 14 days by default in CSM. You can modify this period through the Server Properties file. For more information, see “Data retention in an ESESizer session” on page 96.

In this section, we describe how to prepare, create, configure, and manage the ESESizer session.

3.4.1 Preparing CSM to query the DS8000 Write Monitoring Bitmap with the ESESizer session

To use the ESESizer session, you must update the CSM and DS8000 to the supported levels. You also must add IP connections from your CSM server to all DS8000 storage systems that contain volumes for which sizing is wanted.

Therefore, before you continue with the preparation, check whether the DS8000 microcode and CSM version match the prerequisites. The installed CSM version information is available at the bottom of the login window (see Figure 3-1).



Figure 3-1 CSM 6.3.3.0 login window

For the DS8000, check the microcode level in the DSGUI main window or use the DS CLI `1sserver -1` command. The “Bundle Version” must be for the DS8880 “88.54.xx.xx” or later or for the DS8900F “89.10.xx.xx” or later.

For a DS8000 microcode update, contact your IBM Support representative.

When you use CSM for capacity sizing only, you are likely using CSM for the first time, and you might use the CSM server that is included with the DS8000 HMC.

You also can install CSM on another server platform. For more information about supported links, see the following resources:

- ▶ [This IBM Support web page](#)
- ▶ 3.3, “CSM ESESizer session preparation considerations” on page 85

If you must update CSM, download the required version by using this IBM Fix Central [web page](#).

Note: We recommend that you do not run the ESESizer session on a CSM server that is running other sessions.

For CSM preinstalled on the DS8000 HMC, a Linux-x86_64 version is required.

An upgrade of the CSM version on an HMC can be performed only by way of a stand-alone DS CLI by using the following command:

```
installsoftware -type csm -loc software_package -certloc certificate_file
```

After the upgrade completes successfully, log in to the CSM server.

To access the CSM server on the DS8000 HMC, use:

`http://xxx.xxx.xxx.xxx/CSM/`

xxx.xxx.xxx.xxx represents your DS8000 IP address or Domain Name System (DNS) name.

The following default CSM username and password information is used:

- ▶ Username: csmadmin
- ▶ Password: passw0rd

Note: If this login is the first login, the password must be changed.

To establish the IP communication between the CSM server and the storage systems, select the CSM main window in the Storage tab and then, **Storage Systems** (see Figure 3-2).

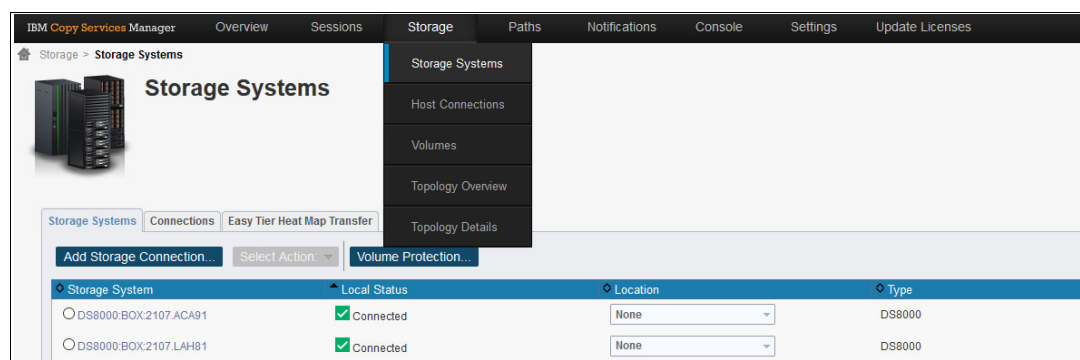


Figure 3-2 CSM Storage Systems window

On the Storage System window, click **Add Storage Connection** if your wanted DS8000 is not displayed. A new window opens in which you can add storage systems. Follow the **Add Storage Wizard** window by choosing the DS8000 type. Then, enter the IP addresses of the DS8000 HMCs and a DS CLI user ID and password (see Figure 3-3 on page 89). The DS CLI user ID must include at least a Copy Services (CS) user role.

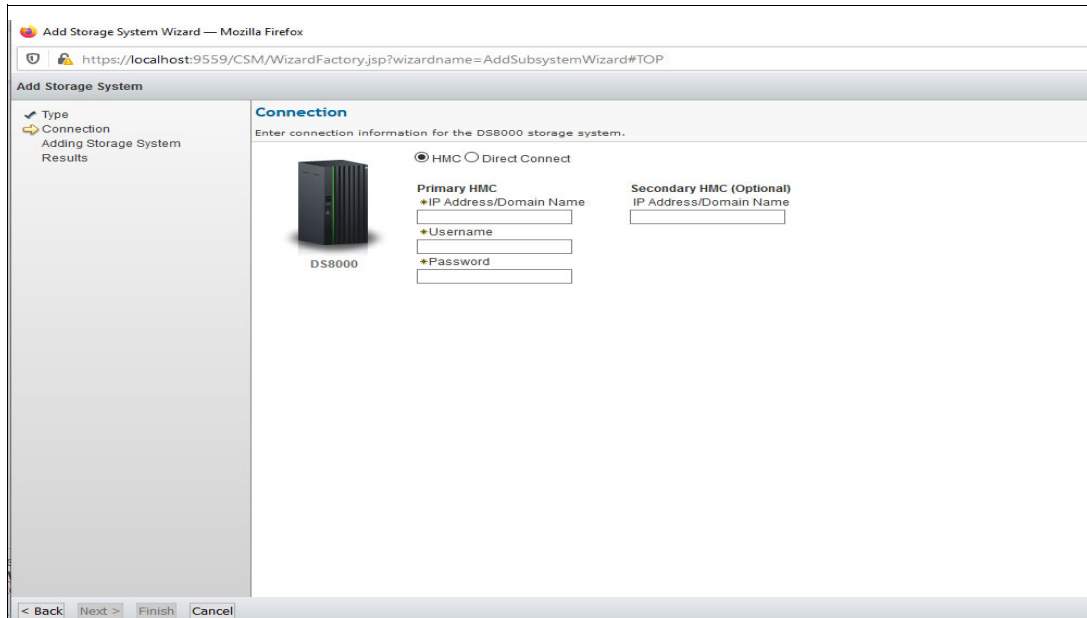


Figure 3-3 Add Storage System Wizard

Then, click **Next**. After the result is shown, click **Finish**. If the IP communication is working correctly, you see the newly added storage in the list, and the Local Status is connected.

The CSM is now prepared for the ESESizer session.

Preparing a CSM copy set for an ESESizer session

For simplifying the session creation, you can prepare in advance the CSM copy sets that must be imported during establishing the session. Therefore, you can use the provided Excel spreadsheet that is named DS8000 Import dscli volume list to prepare CSM ESESizer session copysets.xlsb.

The spreadsheet can import a file that contains outputs from the DS CLI commands **lsckdvol** or **lsfbvol** to produce an output file that can be used during the CSM add copy set procedure. To use the spreadsheet, the following criteria must be met:

- ▶ The output contains only data from one DS8000 system
- ▶ The output does not include the DS CLI command
- ▶ No header is included in the output
- ▶ The data and values in the output are comma-separated

The DS CLI commands that are show in Example 3-1 are for CKD and FB volumes.

Note: All information that is italicized in Example 3-1 must be modified for the customer environment.

Example 3-1 DS CLI command examples for CKD and FB volumes

DSCLI command for CKD volumes:

```
dscli> -cfg xxxx.profile lsckdvol -l -hdr off -fmt delim -delim , -voltype
base xxxx-zzzz > X:\DSS_image_ID.csv
dscli> -hmc1 xx.xx.xx.xx -user username -passwd password lsckdvol -l -hdr
off -fmt delim -delim , -voltype base xxxx-zzzz > X:\DSS_image_ID.csv
```

DSCLI command for FB volumes:

```
dscli> -cfg xxxx.profile lsfbvol -l -hdr off -fmt delim -delim , xxxx-zzzz  
> X:\DSS_image_ID.csv  
dscli> -hmc1 xx.xx.xx.xx -user username -passwd password lsfbvol -l -hdr off -fmt  
delim -delim , xxxx-zzzz > X:\DSS_image_ID.csv
```

After you create the DS CLI volume list, open the Excel spreadsheet and click **Import DSCLI lsfbvol -l / Isckdvol -l output file**. A window opens in which you must enter the last five characters of the DS8000 storage image ID. For example, if the ID is IBM.2107-75ACA91, use ACA91 as the input. Entering the number correctly is important to use the produced CSV file in CSM during the add copy set procedure.

The spreadsheet macro produces a CSV output file in the same directory from where you selected the DS CLI output. The file name Volume_list_image ID_date and time.csv. Use the file later to import the copy sets in your ESESizer session.

Repeat this procedure for all involved DS8000 systems.

3.4.2 Creating an ESESizer session

To create an ESESizer session, at least one set of volumes is required. The set includes the production, Safeguarded Copy source, or FlashCopy source volumes. For our example, we use devices 0100 - 0107, which are the production volumes in our environment.

Note: If you want to use the provided Excel spreadsheet for the capacity sizing, use separate sessions for FB and CKD volumes. Otherwise, the calculations will be incorrect.

To create an ESESizer session, complete the following steps:

1. Log in to your CSM server.
2. Click the **Sessions** tab. In this tab, click **Create Session**.

A new window opens (see Figure 3-4).

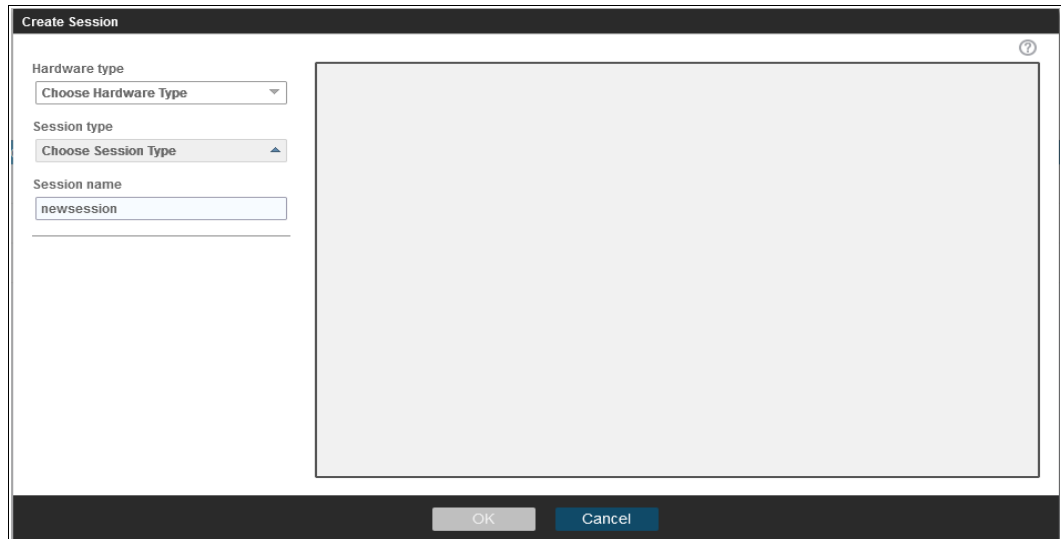


Figure 3-4 Create Session

3. From the **Hardware type** menu, select **DS8000, DS6000, ESS 800**:
 - a. Select the new session type **ESESizer** from the **Session type** menu.
 - b. Enter a Session name and select the **Site 1 location** from the menu (these options are the only options for a ESESizer session).
 - c. Click **OK** to create the session (in our example, the session name is ESESizer_XXXX1_NOV2020).
4. A window opens in which you can add copy sets for this session. Click **Launch Add Copy Sets Wizard**.
5. In the **Add Copy Sets** wizard, select the volumes that are required to create the copy sets for your ESESizer session, as shown in Figure 3-5.

The volumes can be selected from the menu or by importing a CSV file.

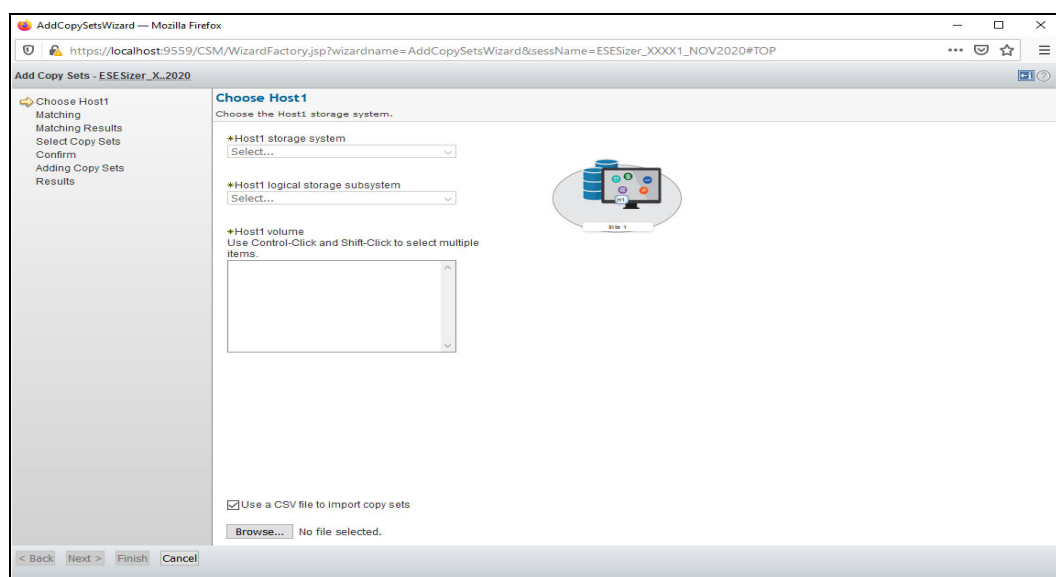


Figure 3-5 Add Copy Sets wizard

6. In our example, we used the CSV file that we prepared with the provided Excel spreadsheet (see “Preparing a CSM copy set for an ESESizer session” on page 89) to import the copy sets:
 - Host1 (H1) are the volumes for which a sizing is wanted (in our example, 0100 - 0107).
 - Here, an abstract of the CSV to import the copy sets for a ESESizer session:


```
H1
DS8000:2107.XXXX1:VOL:0100
DS8000:2107.XXXX1:VOL:0101
...
DS8000:2107.XXXX1:VOL:0107
```
- a. The **Add Copy Sets** wizard verifies that the copy sets match and might display an error or warning message. Verify the messages and, if everything is okay, click **Next** twice.

In our example, we receive a warning message because volumes 0100 - 0107 are in another CSM session. They are the Metro Mirror (MM) primary volumes of our high availability and disaster recovery (HADR) solution. Therefore, this warning message can be ignored.

Note: Ensure that volumes are not used in two active ESESizer sessions at the same time.

- b. Confirm that you want to add the copy sets by clicking **Next**. A progress bar is displayed during this process and you receive the results.

Now, the CSM ESESizer session is established and is in Inactive status because no monitoring is started yet (see Figure 3-6).

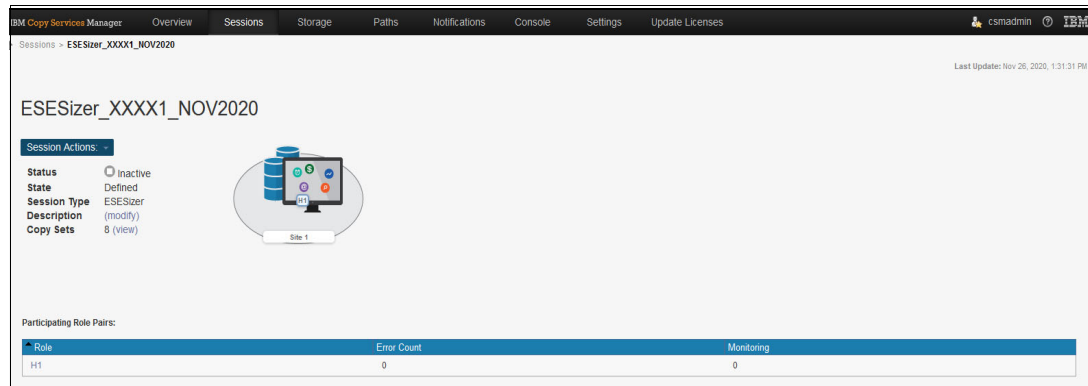


Figure 3-6 Inactive ESESizer session

Before you start the monitoring, verify and modify the properties for your ESESizer session to ensure that it meets your requirements. The next section describes the session properties.

3.4.3 Configuring the ESESizer session

You must decide for what CS function you want to use the monitoring before you start the session: Safeguarded Copy or ESE FlashCopy. You modify the session properties based on that decision.

To modify the properties before you start monitoring, open your session, and select **Session Actions** → **View/Modify** → **Properties** (see Figure 3-7).

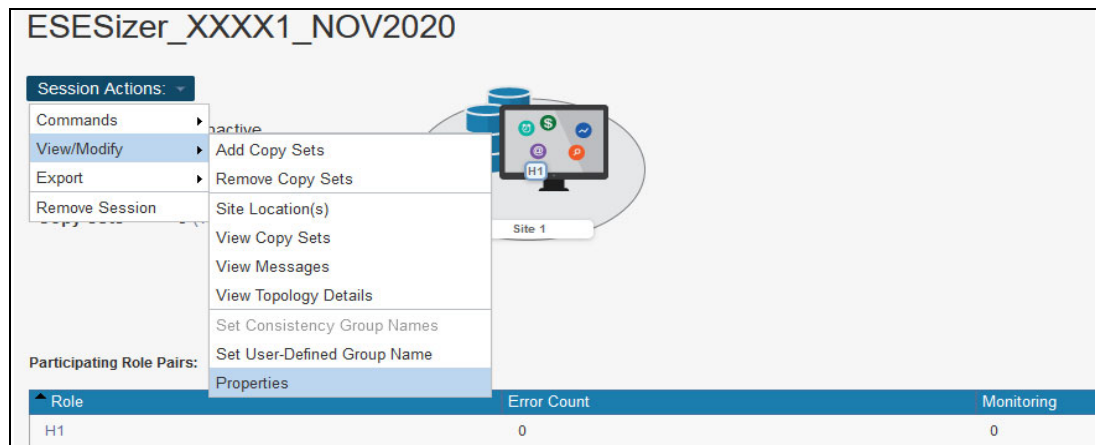


Figure 3-7 Selecting the session properties

This session type has two different properties, as shown in Figure 3-8:

- ▶ Volume query interval (secs)

With this parameter, you specify the interval length between two queries in seconds. Because the default value is 1800 seconds, you must adjust the value so that it fits to your requirements.

- ▶ Monitor reset interval (secs)

This parameter defines when the Write Monitoring Bitmap is reset after the last bitmap query. The default value is 0 seconds, which means that the Write Monitoring Bitmap for the monitored volumes is not automatically reset.

In addition, you can add a description; for example, describe for what purpose you are using this session.

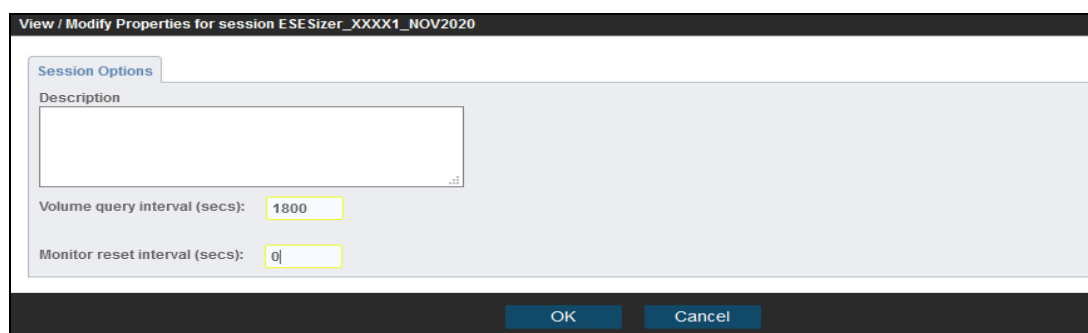


Figure 3-8 Session properties

The respective parameters must be modified to perform an accurate sizing with the provided Excel spreadsheets. For more information about how to set the parameter for ESE FlashCopy or Safeguarded Copy capacity sizing, see 3.5, “Capacity sizing based on the ESESizer output files” on page 97.

Consider the following examples:

- ▶ For ESE FlashCopy sizing, you might query the data every 2 or 4 hours and never reset the Write Monitoring Bitmap during the time the session is active. Then, allow the session to run if you plan to use the ESE FlashCopy targets (for example, 24 hours). That process requires setting the following parameters:

Volume query interval (secs): 7200 / 14400 seconds

Monitor reset interval (secs): 0 seconds

Then, the output files are downloaded after 24 hours.

- ▶ For Safeguarded Copy, you must specify the volume query interval if the time between the two backups should be 1 hour (for example) and reset the Write Monitoring Bitmap immediately after the query is complete. Then, allow the session to run if the Safeguarded Copy retention period is 48 hours, for example. The parameters must be set as shown in the following example:

Volume query interval (secs): 3600 seconds

Monitor reset interval (secs): 1 second

The output files are downloaded after 48 hours or a multiple of the retention period.

For more information about capacity sizing, see 3.5, “Capacity sizing based on the ESESizer output files” on page 97, and 3.6, “Safeguarded Copy capacity sizing overview and example” on page 110.

3.4.4 Managing the ESESizer session

After you configure your session, you can activate the session so that it queries the Write Monitoring Bitmap. Within the session, you can start, stop, and reset the monitor under the **Session Actions** → **Commands** menu (see Figure 3-9).

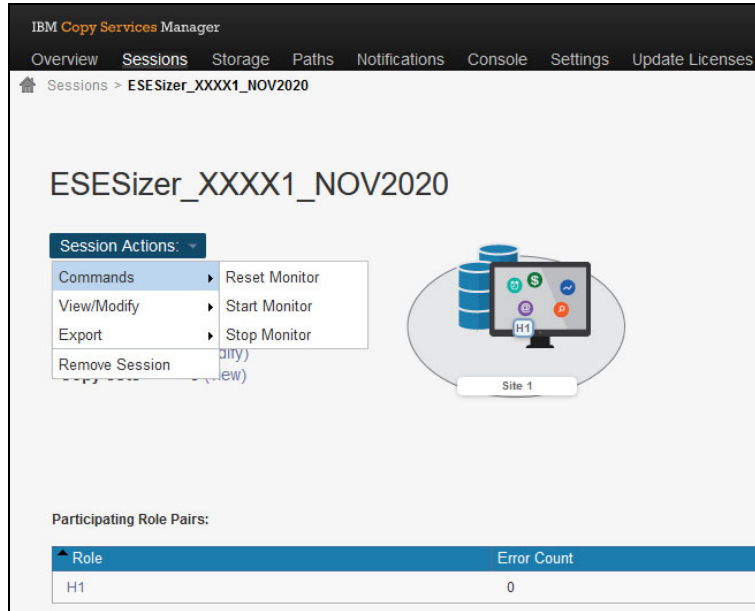


Figure 3-9 Session Action Commands

You can also use the CSM Scheduled Tasks function or the CSM command-line interface (CSMCLI) to manage the session.

Start Monitor and Export data

When you click **Start Monitor**, a window opens. After you click **Yes**, the Write Monitoring Bitmap is started for all volumes in the session by setting all bits to zero. Then, the Write Monitoring Bitmap tracks all write I/Os for each volume. The session is now in Normal status with the state as Running.

Then, the CSM session database stores the query results. During the start process, the CSM session database also is reset. Therefore, you see only query results since the Start Monitor command was issued. The results can be exported at the box and volume level at any time after the first volume query interval completes.

Select **Session Actions** → **Export** and select the file that you want to download for further analysis (see Figure 3-10 on page 95).

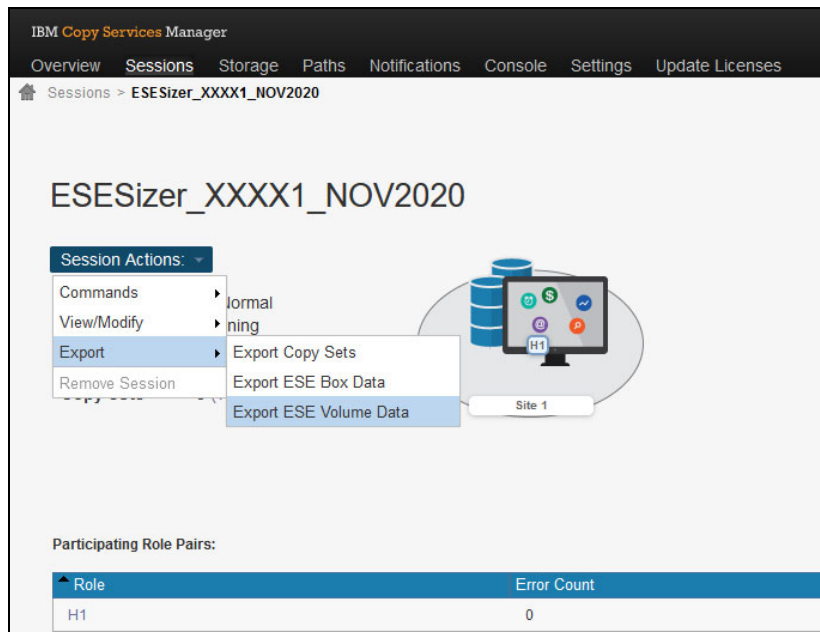


Figure 3-10 Export ESE Box / Volume Data

A window opens that you use to download a CSV file (see Figure 3-11).

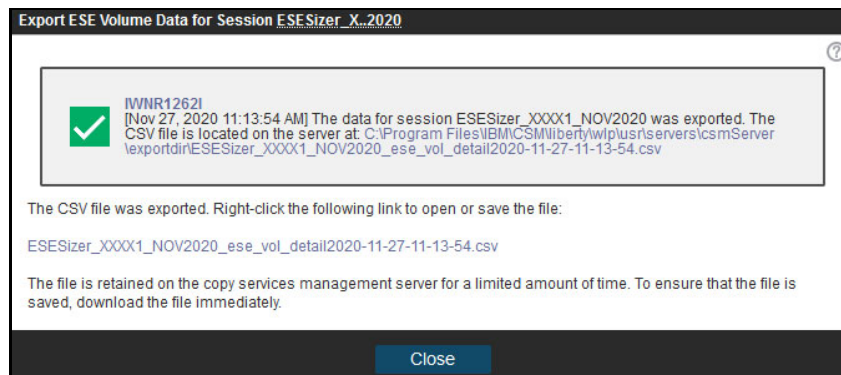


Figure 3-11 Export Volume Data

You see an error message if no data exists because the first query interval is not over. Click the listed file to save it to your workstation. For more information about the content of the file, see 3.5, “Capacity sizing based on the ESESizer output files” on page 97.

Note: Before you import the output file into the Excel spreadsheet, check that the output file contains each interval data from all monitored volumes. Also, ensure that the time difference between the intervals match the specified volume query interval length.

Stop Monitor

After you gather the data that is based on your requirements for the wanted time, you can stop the monitoring by clicking **Stop Monitor** under **Session Actions** → **Commands**.

A message appears that indicates that the WM stopped for all volumes in the session. Although the monitoring is stopped and the session is in an Inactive status, you can download the query results from the former data gathering period until **Start Monitor** is clicked again for this session (see Figure 3-12).

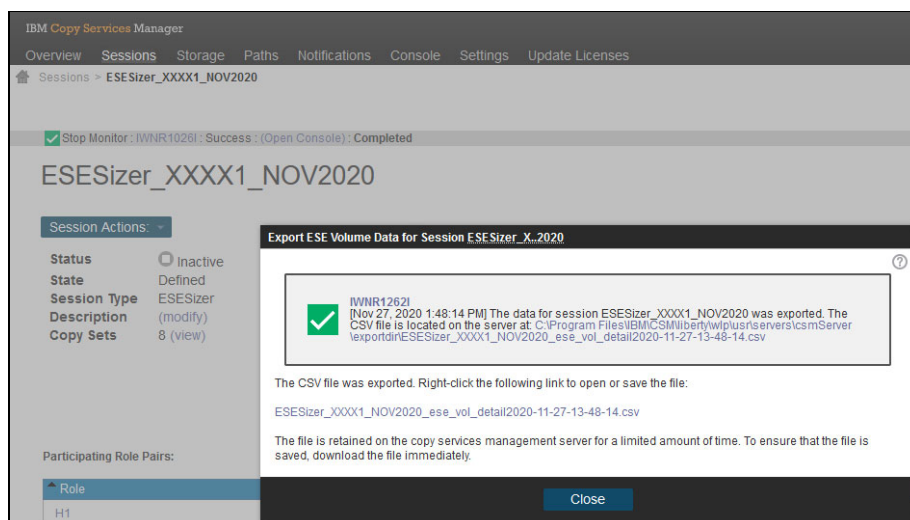


Figure 3-12 Downloading the query results after the monitor is stopped

Reset Monitor

If you must reset the Write Monitoring Bitmap during the monitoring period, you can use the **Reset Monitor** in the session. This command resets the Write Monitoring Bitmap for all volumes in the session and continues the monitoring. The reset command fails if no monitoring is active.

If a regular reset of Write Monitoring Bitmap is required, use **Monitor reset interval** in the session properties instead of **Reset Monitor**. For example, setting the parameter to 1 resets the bitmap immediately after the end of each query interval, which is required to use the provided Excel spreadsheet for a Safeguarded Copy capacity sizing.

You also can use the **CSM Scheduled Tasks** function to automate the reset of the bitmap, for example, resetting the bitmap every 12 hours if you want to size the ESE FlashCopy capacity that is required for a FlashCopy relationship that must be withdrawn after 12 hours.

Data retention in an ESESizer session

An active ESESizer session stores the Write Monitoring Bitmap results for 14 days by default in the CSM session database. If you must query the data for a longer or shorter period, you can specify ESESizer data retention by setting the CSM properties through the following parameters: one for the box, and another one for the volume-level data.

```
db.esevolumedetails.retention.days=28
db.eseboxdetails.retention.days=28
```

These settings extend the data retention period to 28 days for the box and volume levels. To implement the parameter, select **Settings tab** → **Server Properties**. Then, click **Edit** and enter the parameter in the file. To activate the changes, click **Save**.

3.5 Capacity sizing based on the ESESizer output files

In this section, we explain the content of the ESESizer output files and how to set the ESESizer session parameters correctly for both CS functions. These parameters are set so that you can use the provided Excel spreadsheets to support your capacity sizing. In addition, we describe which calculations are done in the spreadsheets. Finally, we demonstrate the use of the spreadsheets.

3.5.1 ESESizer output files content overview

The queries provide the entire Write Monitoring Bitmap, which then can be parsed to understand the changed tracks, small extents, or large extents (see Table 3-2).

Table 3-2 CSV file format and content

Query time	Query interval (secs)	Box name	Small extents	Large extents	Allocated small extents	Allocated large extents	Changed tracks
2020-11-17 T13:43:18	1800	2107.LAH81	11448	216	192	4	59604

In this section, we explain the content of both ESESizer output files that you can export by using the export option in the session. You can save a box-level and a volume-level CSV file to your workstation.

The CSV file name starts with the CSM session name, includes `ese_box_` or `ese_vol_`, and ends with the date and time. Do not change the name because the separately delivered Excel spreadsheets expect `box` or `vol` in the file name.

The box-level file features the following format:

```
#Generated at: 18-11-20 12:40
#Session Name: ESESizer_XXXX1_NOV2020
```

In addition to the information about when the box-level file was generated and the session name, the columns that are listed in Table 3-3 are included.

Table 3-3 Columns that are listed in Metro Mirror

ESESizer Session output file: Export ESE Box Data	Description
Query Time	Time of query
Query Interval (secs)	Interval length in seconds
Box Name	Image ID/Name of the monitored DS8000
Small Extents	Sum of the volume capacity for the box measured in small extents
Large Extents	Sum of the volume capacity for the box measured in large extents
Allocated Small Extents	Are the small extents that have bits set in the monitored bitmap
Allocated Large Extents	Are the large extents that have bits set in the monitored bitmap
Changed Tracks	Sum of bits set in the monitored bitmap

In the box-level file, all values are summarized for each DS8000 system per interval.

The volume-level CSV file provides information for each volume that is monitored in the ESESizer session and contains the information that is listed in Table 3-4.

Table 3-4 Volume-level CSV file content

Query time	Query interval (secs)	Box name	Volume number	Volume name	Small extents	Large extents	Allocated small extents	Allocated large extents	Changed tracks
2020-11-17T13:43:18	1800	2107.L AH81	106	SGA106	1431	27	0	0	0
2020-11-17T13:43:18	1800	2107.L AH81	107	SGA107	1431	27	0	0	0
2020-11-17T13:43:18	1800	2107.L AH81	101	SGA101	1431	27	0	0	0
2020-11-17T13:43:18	1800	2107.L AH81	103	SGA103	1431	27	0	0	0
2020-11-17T13:43:18	1800	2107.L AH81	105	SGA105	1431	27	0	0	0
2020-11-17T13:43:18	1800	2107.L AH81	100	SGA100	1431	27	0	0	0
2020-11-17T13:43:18	1800	2107.L AH81	104	SGA104	1431	27	96	2	29802
2020-11-17T13:43:18	1800	2107.L AH81	102	SGA102	1431	27	96	2	29802

The information that is included in each column of the CSV file is explained in Table 3-5.

Table 3-5 Included columns

ESESizer Session output file: Export ESE Volume Data	Description
Query Time	Time of Query.
Query Interval (secs)	Interval length in seconds.
Box Name	Image ID / Name of the monitored DS8000.
Volume Number	DS8000 Volume-ID.
Volume Name	DS8000 volume name or for CKD volumes the z/OS volser.
Small Extents	Sum of the volume capacity for the volume measured in small extents.
Large Extents	Sum of the volume capacity for the volume measured in large extents.

ESESizer Session output file: Export ESE Volume Data	Description
Allocated Small Extents	The number of small extents that have bits that are set in the monitored bitmap.
Allocated Large Extents	The number of large extents that have bits that are set in the monitored bitmap.
Changed Tracks	Sum of bits that are set in the monitored bitmap.

Again, the ESESizer output files do not distinguish between FB or CKD volumes. Therefore, you must take care that only FB or CKD volumes are in the same session for calculating the capacity in GiB correctly because the extent and track size is different between FB and CKD volumes.

The different values for CKD and FB are shown in Table 3-6.

Table 3-6 Size differences between CKD and FB volumes

Format	Small extent size	Large extent size	Track size in bytes	Number of tracks per small extent	Number of tracks per large extent
CKD	21 Cyl	1113 Cyl	56664	315	16695
FB	16 MiB	1024 MiB	65536	256	16384

Based on this data, capacity sizing is possible. For Safeguarded Copy, you must use the Changed Tracks values, and for FlashCopy, use the small or large extent numbers for the capacity sizing. You can decide whether you use your own method to perform the calculation based on the output files or you use the separately provided Excel spreadsheets. For more information, see this IBM Support [web page](#).

3.5.2 ESESizer session properties settings for using Excel spreadsheets

In 3.4.3, “Configuring the ESESizer session” on page 92, we described the two session parameters and how to modify them to support your capacity sizing. To use the separately delivered Excel spreadsheet, you must modify the parameters as described next, or your sizing will be incorrect.

The following parameter settings are used for Safeguarded Copy:

1. Specify the Volume query interval for the time between two backups. For example, if the planned Safeguarded Copy backup frequency is to create a backup every hour, set the Volume query interval (secs) to 3600.
2. Reset the Write Monitoring Bitmap immediately after each query interval is complete. Set the Monitor reset interval (secs) to 1 (do *not* use a different value).

Allow the session to run at least as long as your Safeguarded Copy retention period is planned. The data can be queried for any retention period (such as an entire week) or a more. To use the provided Excel spreadsheets, import data that contains at least two more backup intervals as the number of required Safeguarded Copies during the retention period. Then, download the outputs files by way of the export function in the session.

For Safeguarded Copy capacity sizing, the volume-level CSV file is more important.

The following parameter settings are used for ESE FlashCopy:

1. Specify the Volume query interval so that you can see how the capacity is growing over time until you withdraw the FlashCopy relationship. The use of an interval of 1, 2, or 4 hours likely is a good approach. For larger environments, it is a best practice to use a less frequent query (for example, 4 hours).

For example, if you plan that your ESE FlashCopy relationships exist for 24 hours, set the Volume query interval (secs) to 7200.

2. If resets of the Write Monitoring Bitmap are required, create a CSM Scheduled Task to reset the Write Monitoring Bitmap instead of using the Monitor reset interval (secs) parameter. Set the Monitor reset interval (secs) to 0.

For example, if you plan that your ESE FlashCopy relationships exist for 24 hours, create a Scheduled Tasks with CSM by selecting **Settings tab** → **Scheduled Tasks** → **Create Task** and follow the wizard prompts.

Allow the session to run at least as long as your FlashCopy relationship should exist. It can be queried multiple times during a week. Then, download the outputs files by using the session export function. For ESE FlashCopy capacity sizing, the box-level CSV file is (in most cases) more important.

3.5.3 Provided Excel spreadsheets

As described in 3.5.1, “ESESizer output files content overview” on page 97, the ESESizer output files do not distinguish between FB or CKD volumes because the extent and track sizes are different for FB and CKD volumes.

After you open one of the capacity calculation spreadsheets that is called CSM ESESizer CSV Output Files calculation.xlsb, you see the Excel worksheet that is shown in Figure 3-13.

COPYRIGHT IBM CORP. 2021. All Rights Reserved

Specify volume type before import:

Start Volume level data import and calculation:

Click the button and select all ESESizer session volume output files

For Safeguarded Copy enter:

Required Safeguarded Copies:

Note: CSM will expire the first Backup some time after the retention period ends, so we are adding one extra Safeguarded Copy to your input, to be on the save side.

For Safeguarded Copy, import data that contain at least two more intervals as the number of required Safeguarded Copies you have entered!

For Safeguarded Copy, please set the ESESizer session "Volume query interval" parameter as long as the time between two backups and set the "Monitor reset interval" to 1. Otherwise the calculations in this spreadsheet will be wrong!

The volume data will be imported into a new sheet and calculations for required GiB and percentage of allocated small / large extents and changed tracks are done.

Volume data legend:

Small Extents	Volume capacity measured in small extents
Large Extents	Volume capacity measured in large extents
Allocated Small Extents	Small extents which have bits set in the monitored bitmap
Allocated Large Extents	Large extents which have bits set in the monitored bitmap
Changed tracks	Sum of bits set in the monitored bitmap

Start Box level data import and calculation:

Click the button and select all ESESizer session box output files

For Safeguarded Copy enter:

Number of involved DS8000:

Required Safeguarded Copies:

Number of involved volumes:

CSM will expire the first Backup some time after the retention period ends, so we are adding one extra Safeguarded Copy to your input, to be on the save side.

For Safeguarded Copy, import data that contain at least two more intervals as the number of required Safeguarded Copies you have entered!

For Safeguarded Copy, please set the ESESizer session "Volume query interval" parameter as long as the time between two backups and set the "Monitor reset interval" to 1. Otherwise the calculations in this spreadsheet will be wrong!

The box data will be imported into a new sheet and calculations for required GiB and percentage of allocated small / large extents and changed tracks are done.

Box data legend:

Small Extents	Monitored DS8000 capacity measured in small extents
Large Extents	Monitored DS8000 capacity measured in large extents
Allocated Small Extents	Small extents which have bits set in the monitored bitmap
Allocated Large Extents	Large extents which have bits set in the monitored bitmap
Changed tracks	Sum of bits set in the monitored bitmap

Figure 3-13 Capacity sizing spreadsheet input worksheet

Here, you can import the ESESizer session output files for the box or volume level. Before you to select the files, you must specify the volume type (CKD or FB), and you must decide whether you want to perform a FlashCopy capacity sizing. A window opens in which **No** is preselected because the spreadsheets are mostly used for Safeguarded Copy capacity sizing (see Figure 3-14).

If you want to perform a FlashCopy sizing, select **Yes**, and you can directly import the ESESizer output files later. The spreadsheet performs all of the calculations and creates a pivot chart worksheet. For more information about the values you can visualize in the pivot chart, see 3.5.4, “Excel spreadsheet calculations” on page 105.

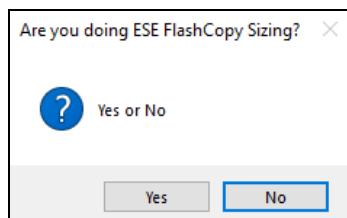


Figure 3-14 Selection: ESE FlashCopy sizing wanted YES or NO

If you select **No**, you must provide more information for the Safeguarded Copy sizing, depending on whether you import the volume or box-level CSV files (see “Safeguarded Copy import volume-level CSV file” on page 101, and “Safeguarded Copy import box-level CSV file” on page 103).

Safeguarded Copy import volume-level CSV file

For Safeguarded Copy capacity sizing that is based on the volume-level output file, you must enter the number of Safeguarded Copy backups that are planned for the retention period (see Figure 3-15) before you can import the volume-level CSV file.

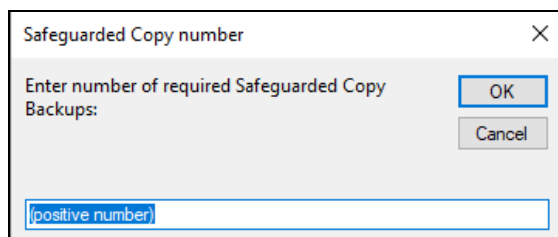


Figure 3-15 Entering the number of planned Safeguarded Copy backups during the retention period

After you enter the number of required Safeguarded Copy, a new window opens in which you can import CSV files that include vol in the file name (see Figure 3-16).

Note: Before you import the output file into the Excel spreadsheet, check that the output files contain each interval data from all monitored volumes. Also, ensure that the time difference between the intervals match with the specified volume query interval length.

A good indicator that data for all monitored volumes exists is to check whether the box-level CSV-file contains data for each interval.

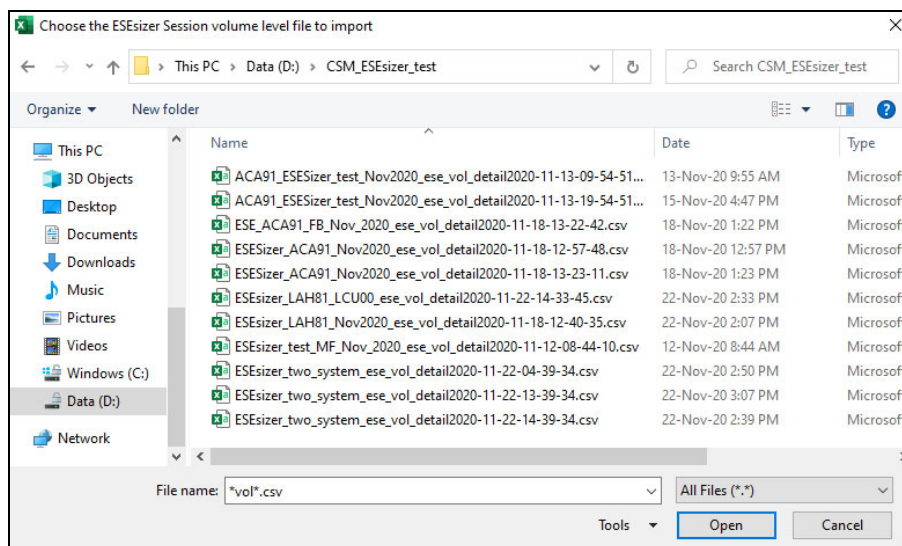


Figure 3-16 Importing a volume-level ESESizer output CSV file

Then, the Excel macro performs the calculations based on the imported data and your inputs.

After the import and calculations are complete, the message that is shown in Figure 3-17 is displayed.

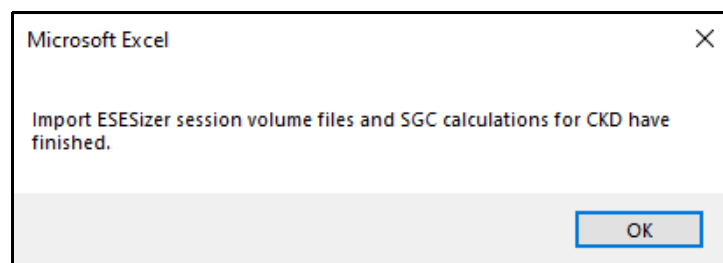


Figure 3-17 Import and calculations have finished

Click **OK** to display the calculation results in a separately created file that is in the same directory from where you imported the ESESizer output files. The file name is either `SGC_CKD_Volume_date_time.xlsb` or `SGC_FB_Volume_date_time.xlsb`, depending on which volume type you specified (CKD or FB).

Note: The calculation can take several minutes, depending on the number of volumes and intervals.

The Solution Summary worksheet in the new files shows the results that are based on your input and the imported ESESizer session volume-level CSV file (see Figure 3-18).

Safeguarded Copy CKD Summary:								
Don't forget to size the Recovery Volume capacity!								
SGC overhead (one extent per volume per SGC backup) in GiB:				583.83 GiB				
SUM of Volume Capacity in GiB:				SUM of Required SGC Backup Capacity in GiB:	Overall SGC Backup Capacity in % of Volume Capacity:	Required Safeguarded Copies:	SUM of Required SGC Virtual Capacity based on adjusted Volume Backup capacity multiplier in GiB:	
64,392.85 GiB				12,758.58 GiB	20.72 %	7	99,178.32 GiB	
Overall required Safeguarded Copy Backup capacity in GiB:				13,342.41 GiB				
Volume Number	LSS	Volume Name	Box Name	Average Volume Size in GiB	Max required Volume SGC capacity in GiB	Max Volume Backup capacity multiplier	Adjusted Volume Backup capacity multiplier	Required SGC Virtual Capacity based on adjusted Volume Backup capacity multiplier in GiB
7100	71	UT87C0	2107.XXXX1	0.881036259	0	0	1.5	1.32155438
7101	71	MV3J01	2107.XXXX1	2.643108778	0.008285277	0.003134671	1.5	3.96466316
7102	71	8387C2	2107.XXXX1	2.643108778	0	0	1.5	3.96466316
7103	71	G3BA1F	2107.XXXX1	7.929326333	6.753555872	0.851718745	1.5	11.893989
7104	71	G3DF0D	2107.XXXX1	7.929326333	6.168836989	0.777977438	1.5	11.893989
7105	71	G3BA0A	2107.XXXX1	7.929326333	10.00207034	1.261402283	2	15.8586526
7106	71	SM3002	2107.XXXX1	7.929326333	9.095333889	1.147050015	2	15.8586526
7107	71	G3SY02	2107.XXXX1	7.929326333	20.3613047	2.567847992	3	23.78797
7108	71	G3SY01	2107.XXXX1	7.929326333	16.97077954	2.1402549	3	23.78797
7109	71	MV3T02	2107.XXXX1	7.929326333	17.90939055	2.258627001	3	23.78797

Figure 3-18 Volume-level Solution Summary example

In addition to the information that is shown in Figure 3-18, the Solution Summary worksheet contains also an overview about which Volume Backup capacity multiplier is required for how many volumes. Therefore, move the worksheet to the right, as shown in Figure 3-19.

Number of Volumes:	1728
Adjusted Volume Backup capacity multiplier:	Number of Volumes with same Backup capacity multiplier:
1.5	1658
2	30
3	16
4	7
5	17
6	0
7	0
8	0

Figure 3-19 Volumes per multiplier

For more information about calculations that done on this worksheet and the meaning of the values that are displayed see 3.5.5, “Excel spreadsheet volume-level Safeguarded Copy Solution Summary” on page 107.

Safeguarded Copy import box-level CSV file

For a Safeguarded Copy capacity sizing that is based on box-level output files, complete the following steps:

1. Enter the number of involved DS8000 systems (see Figure 3-20).

Box number

Enter number of involved DS8000 systems:

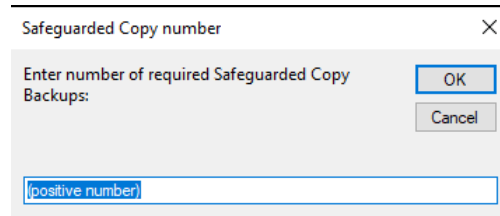
OK

Cancel

positive number

Figure 3-20 Entering the number of involved DS8000 systems

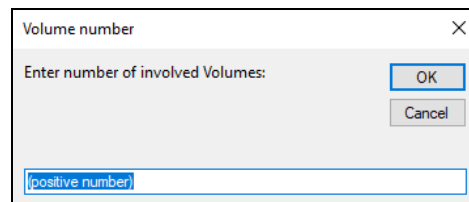
2. Enter the number of planned Safeguarded Copy backups (see Figure 3-21).



A dialog box titled "Safeguarded Copy number" with a close button (X) in the top right corner. It contains the text "Enter number of required Safeguarded Copy Backups:" followed by "OK" and "Cancel" buttons. Below the text is a text input field containing the placeholder text "[positive number]".

Figure 3-21 Entering the required Safeguarded Copy backups

3. Finally, before you can import the box-level CSV file, enter the number of involved volumes (see Figure 3-22).



A dialog box titled "Volume number" with a close button (X) in the top right corner. It contains the text "Enter number of involved Volumes:" followed by "OK" and "Cancel" buttons. Below the text is a text input field containing the placeholder text "[positive number]".

Figure 3-22 Entering the number of involved volumes

The number of involved volumes is used to calculate the Safeguarded Copy overhead for each backup.

4. After you enter the number of involved volumes, a window opens in which you can import CSV files that include box in the file name (see Figure 3-23).

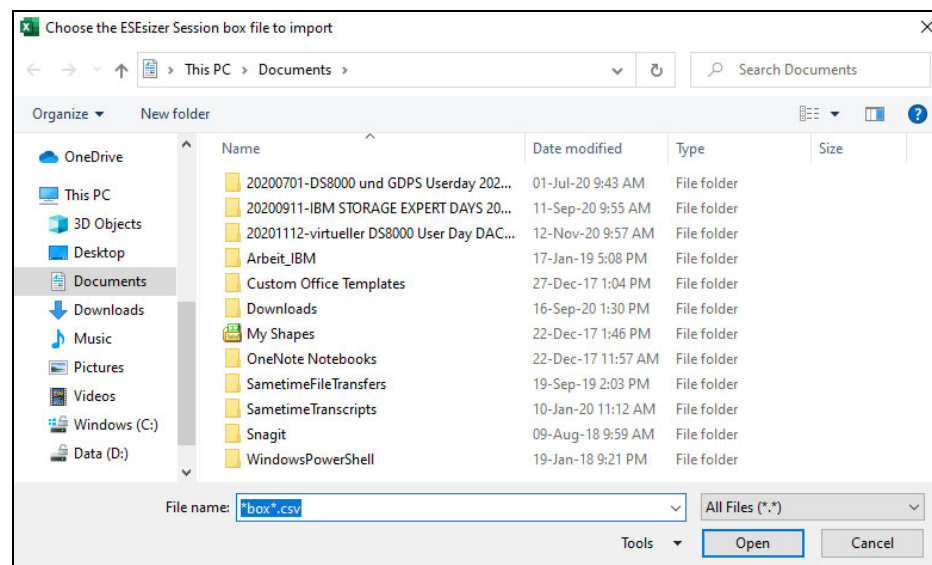


Figure 3-23 Importing a box-level CSV file

Note: Before you import the output file into the Excel spreadsheet, check that the output files contain data for each interval from all monitored volumes. And make sure that the time difference between the intervals matches with the specified volume query interval length.

A good indicator that data for all monitored volumes exists is to check whether the box-level CSV-file contains data for each interval.

5. The Excel macro performs the calculation that is based on the imported data and your inputs. After the import and calculations are completed, a message is displayed that indicates that data imports and calculations finished. Click **OK** to display the calculation results in a separately created file in the directory from where you imported the ESESizer session output files. The file name is either SGC_CKD_BOX_date_time.xlsb or SGC_FB_BOX_date_time.xlsb, depending on which spreadsheet you used (the one for CKD volumes or the one for FB volumes).
6. The new Excel file shows the results that are based on your input and the imported ESESizer session box-level CSV file (see Figure 3-24).

Sum of Required SGCBC in GiB	CKD Box Calculatic	Required Safeguarded Copies	49	Involved Volumes	1851
Data points	2107.XXXXX1	Safeguarded Copy Backup Capacity Sliding SUM: System 1			
2021-09-05T05:45:52	65.0068 GiB	3,944.0275 GiB			
2021-09-05T06:45:52	88.5821 GiB	3,879.0207 GiB			
2021-09-05T07:45:52	110.6157 GiB	3,790.4386 GiB			
2021-09-05T08:45:52	57.4460 GiB	3,679.8230 GiB			
2021-09-05T09:45:52	68.2401 GiB	3,622.3769 GiB			
2021-09-05T10:45:52	126.4656 GiB	3,554.1368 GiB			
2021-09-05T11:45:52	96.4110 GiB	3,427.6712 GiB			
2021-09-05T12:45:52	46.0558 GiB	3,331.2602 GiB			
2021-09-05T13:45:52	43.3384 GiB	3,285.2044 GiB			
2021-09-05T14:45:52	85.2015 GiB	3,241.8660 GiB			
2021-09-05T15:45:52	82.7740 GiB	3,156.6646 GiB			
2021-09-05T16:45:52	66.9640 GiB	3,073.8906 GiB			
2021-09-05T17:45:52	63.0025 GiB	3,006.9266 GiB			
2021-09-05T18:45:52	154.8165 GiB	2,943.9241 GiB			
2021-09-05T19:45:52	164.4995 GiB	2,789.1076 GiB			
2021-09-05T20:45:52	87.0807 GiB	2,624.6082 GiB			
2021-09-05T21:45:52	64.2991 GiB	2,537.5274 GiB			
2021-09-05T22:45:52	50.0701 GiB	2,473.2284 GiB			
2021-09-05T23:45:52	48.9263 GiB	2,423.1582 GiB			
2021-09-06T00:45:52	586.3401 GiB	2,374.2319 GiB			
2021-09-06T01:45:52	663.2404 GiB	1,787.8919 GiB			
2021-09-06T02:45:52	601.3673 GiB	1,124.6515 GiB			
2021-09-06T03:45:52	159.3520 GiB	523.2841 GiB			
2021-09-06T04:45:52	125.3199 GiB	363.9321 GiB			
2021-09-06T05:45:52	40.0576 GiB	238.6122 GiB			
2021-09-06T06:45:52	94.8116 GiB	198.5546 GiB			
2021-09-06T07:45:52	103.7430 GiB	103.7430 GiB			
Max required physical Safeguarded Copy Backup Capacity in GiB:		14,785.20 GiB			
As a buffer, please add 20 % of max. required physical Safeguarded Copy Backup Capacity:		2,953.04 GiB			
Consider also the Safeguarded Copy overhead (one extent per volume per Safeguarded Copy backup) in GiB:		1,507.72 GiB			
Overall required physical Safeguarded Copy Backup Capacity in GiB:		19,225.95 GiB			
Overall Safeguarded Copy Backup Capacity in % of Volume Capacity:		31.94 %			
In addition, please size the required physical capacity for the recovery volumes (it depends on the use case)					
Box Name	2107.XXXXX1	Average Box capacity in GiB	60,202.99 GiB		

Figure 3-24 Box-level summary worksheet

For more information about the calculations and the meaning of the values that are displayed, see 3.5.6, “Excel spreadsheet box-level Safeguarded Copy calculations” on page 109.

3.5.4 Excel spreadsheet calculations

To support the capacity calculations, the spreadsheet macros perform some other calculations and add them as new columns. Those added columns and the related calculations are independent from the type of capacity sizing (FlashCopy or Safeguarded Copy) that is done.

The added columns are included as a worksheet that is called Volume_info or Box_info, depending on what data you imported (volume or box-level).

In addition to the columns that are imported directly from the ESESizer volume-level output file (see 3.5.1, “ESESizer output files content overview” on page 97), the Volume_info worksheet shows the columns that are listed in Table 3-7.

Table 3-7 Columns that are listed in the Volume_info worksheet

Provided excel spreadsheet: Volume_info	Calculation description	Comment
LSS	The first 2 digits from the Volume ID	Logical subsystem (LSS) number, which can be used as another filter option.
Required SGCBC in GiB	“Changed tracks” * track size / 1024 ³	Required physical Safeguarded Copy Backup Capacity
SGCBC: percentage of volume size:	“Required SGCBC in GiB”/“Small Extents” * number of tracks per small extent * track size / 1024 ³) * 100	Percentage of volume size in GiB
Required ESE-FC cap. in GiB:	“Allocated Small Extents” * number of tracks per extent * track size / 1024 ³	Required physical capacity for ESE FlashCopy
ESE-FC: percentage of volume size:	“Required ESE-FC cap. in GiB” / (“Small Extents” * number of tracks per small extent * track size / 1024 ³) * 100	Percentage of volume size in GiB
Volume size in GiB:	“Small Extents” * number of tracks per small extent * track size / 1024 ³	None
Backup capacity multiplier:	“Required SGCBC in GiB”/Volume size in GiB”	Safeguarded Copy required volume backup capacity multiplier
Required SGC Virtual Capacity:	“Volume size in GiB” * “Backup capacity multiplier”	None

All calculations are done for each volume and interval.

In addition to the columns that are imported directly from the ESESizer box-level output file (see 3.5.1, “ESESizer output files content overview” on page 97), the Box_info worksheet shows the columns that are listed in Table 3-8.

Table 3-8 Columns that are listed in the Box_info worksheet

Provided excel spreadsheet: Box_info	Calculation description	Comment
Required SGCBC in GiB	“Changed tracks” * track size / 1024 ³	Required physical Safeguarded Copy Backup Capacity
SGCBC: percentage of DS8000 capacity	“Required SGCBC in GiB”/ (“Small Extents” * number of tracks per small extent * track size / 1024 ³) * 100	Percentage of DS8000 capacity
Required ESE-FC cap. with small extents in GiB	“Allocated Small Extents” * number of tracks per small extent * track size / 1024 ³	Required physical capacity for ESE FlashCopy with small extents in GiB

Provided excel spreadsheet: Box_info	Calculation description	Comment
ESE-FC with small extents: percentage of DS8000 capacity	"Required ESE-FC cap. with small extents in GiB" / ("Small Extents" * number of tracks per small extent * track size / 1024 ³) * 100	Percentage of monitored volume capacity
Required ESE-FC cap. with large extents in GiB	"Overall required physical Safeguarded Copy Backup Capacity" / "Average Box capacity" * 100	Required physical capacity for ESE FlashCopy with large extents in GiB
ESE-FC with large extents: percentage of DS8000 capacity	"Required ESE-FC cap. with large extents in GiB" / ("Large Extents" * number of tracks per large extent * track size / 1024 ³) * 100	Percentage of monitored volume capacity
Box capacity in GiB	"Small Extents" * number of tracks per small extent * track size / 1024 ³	Monitored volume capacity

All calculations are done for each DS8000 system and interval.

Table 3-9 provides the track and extent values for CKD and FB volumes.

Table 3-9 Track and extent values for CKD and FB volumes

Format	Small extent size	Large extent size	Track size in bytes	Number of tracks per small extent	Number of tracks per large extent
CKD	21 Cyl	1113 Cyl	56664	315	16695
FB	16 MiB	1024 MiB	65536	256	16384

Some of these calculated values are used for the Safeguarded Copy capacity sizing, and others are required for ESE FlashCopy sizing only.

For more information about a sizing example and the results of the calculation for Safeguarded Copy, see 3.6, "Safeguarded Copy capacity sizing overview and example" on page 110.

3.5.5 Excel spreadsheet volume-level Safeguarded Copy Solution Summary

The Excel spreadsheet volume-level output file for Safeguarded Copy includes two worksheets:

- ▶ Volume_info (see 3.5.4, "Excel spreadsheet calculations" on page 105)
- ▶ Solution Summary

The Solution Summary worksheet provides much information that is helpful for sizing. You find values that provide overall capacity estimation, such as the required overall physical Safeguarded Copy Backup Capacity or the overall required Safeguarded Virtual Capacity. You also get information for each volume, such as the Backup Capacity Multiplier. Important for your sizing is that you must accurately enter the number of required Safeguarded Copy backups during the retention period.

Table 3-10 lists the values that are included in the worksheet and how they are calculated.

Table 3-10 Overall values

Solution Summary worksheet: Overall values	Calculation description	Comment
Safeguarded Copy overhead (one extent per volume per Safeguarded Copy backup) in GiB	Number of volumes * (number of required Safeguarded Copies +1) * small extent size in GiB plus 3% of the SGCBC.	Overhead calculation because each backup requires one extent, although no data is changed.
SUM of required Safeguarded Copy Backup Capacity in GiB	SUM of column "Max required Volume SGC capacity in GiB"	None.
Overall required Safeguarded Copy Backup Capacity in GiB	Overhead + "SUM of Required Safeguarded Copy Backup Capacity"	None.
SUM of Volume Capacity in GiB	SUM of column "Average Volume Size"	None.
Overall Safeguarded Copy Backup Capacity in % of Volume Capacity	"Overall required Safeguarded Copy Backup Capacity" / "SUM of Volume Capacity" * 100	None.
SUM of Required Safeguarded Virtual Capacity based on adjusted Volume Backup capacity multiplier in GiB	SUM of column "Required SGC Virtual Capacity based on adjusted Volume Backup capacity multiplier"	Might not display correctly if a volume Backup capacity multiplier is "Too Large".
Required Safeguarded Copies	Entered number of Safeguarded Copy backups + 1	You add another backup because the oldest backup is deleted sometime after the retention period is over and the new backup was created.

Table 3-11 lists the individual values that are included in the worksheet and how they are calculated.

Table 3-11 Individual values

Solution Summary worksheet: individual values per volume	Calculation description	Comment
Average Volume Size in GiB	Calculated based on: "Small Extents" * number of tracks per small extent * track size / 1024 ³	None.
Max required Volume SGC capacity in GiB	Calculate sum in sliding window based on entered number of Safeguarded Copy backups + 1, then find max values per volume.	Another interval or backup is added because the oldest backup is deleted after a new one is created.
Max Volume Backup capacity multiplier	"Max required Volume SGC capacity in GiB" / "Average Volume Size"	None.

Solution Summary worksheet: individual values per volume	Calculation description	Comment
Adjusted Volume Backup capacity multiplier	If values < 1 use 1.5 as multiplier, if values > Required Safeguarded Copies +1 round to full integer, else use Required Safeguarded Copies + 1 as multiplier	None.
Required SGC Virtual Capacity based on adjusted Volume Backup capacity multiplier in GiB	"Adjusted Volume Backup capacity multiplier" * "Average Volume Size in GiB"	If the value is larger than 16 TiB (FB) or 14.6 TiB (CKD), set "Too Large".

Table 3-12 lists the backup capacity values that are included in the worksheet and how they are calculated.

Table 3-12 Backup capacity values

Solution Summary worksheet: Backup capacity multiplier table	Calculation description	Comment
Number of Volumes	Count Volume number column	None.
Adjusted Volume Backup capacity multiplier	None	Shows number of required Safeguarded Copies + 1.
Number of Volumes with same Backup capacity multiplier	Count volume number with same multiplier	None.

3.5.6 Excel spreadsheet box-level Safeguarded Copy calculations

The Excel spreadsheet box-level output file for Safeguarded Copy includes two worksheets: Box_info (see 3.5.4, "Excel spreadsheet calculations" on page 105) and a summary worksheet that contains the information that is listed in Table 3-13.

Table 3-13 Summary worksheet information

Box-level summary worksheet	Calculation description	Comment
Required physical Safeguarded Copy Backup Capacity in GiB	Max of Column "Safeguarded Copy Backup Capacity Sliding SUM: System X"	Calculated per system.
20% of maximum required physical Safeguarded Copy Backup Capacity	"Required physical Safeguarded Copy Backup Capacity" * 0.2	As a buffer, add 20% because volumes might have different peak intervals. Calculated per system.
Safeguarded Copy overhead (one extent per volume per Safeguarded Copy backup) in GiB	Number of volumes * number of required Safeguarded Copies * small extent size in GiB	Overhead calculation because each backup requires one extent, although no data is changed. If there are multiple storage systems, use an average volume number per system.

Box-level summary worksheet	Calculation description	Comment
Overall required physical Safeguarded Copy Backup Capacity in GiB	“Required physical Safeguarded Copy Backup Capacity” + “20% of maximum required physical Safeguarded Copy Backup Capacity” + “Safeguarded Copy overhead”	Calculated per system.
Overall Safeguarded Copy Backup Capacity in % of Volume Capacity	“Overall required physical Safeguarded Copy Backup Capacity” / “Average Box capacity” * 100	Calculated per system.
Safeguarded Copy Backup Capacity Sliding SUM: System X	Calculate sum in sliding window based on entered number of Safeguarded Copy backups + 1	One other interval / backup is added because the oldest backup is deleted after a new one is created.
Required Safeguarded Copies	Entered number of required Safeguarded Copy backups + 1	One other interval / backup is added because the oldest backup is deleted after a new one is created.
Involved Volumes	Entered number of involved volumes	If multiple storage systems are involved, use an average volume number per system.
Average Box capacity in GiB	Box capacity calculated	Displayed per involved system.

During Safeguarded Copy capacity calculations, the box-level files are used to determine the required physical Safeguarded Copy Backup Capacity. If an ESESizer session includes only a single storage system, the volume-level files are enough to estimate all required capacity information.

3.6 Safeguarded Copy capacity sizing overview and example

In this section, we show a sizing example by using the provided Excel spreadsheets. We also provide a brief overview of the Safeguarded Copy capacity sizing. For more information, see 2.5, “Safeguarded Copy sizing considerations” on page 42.

3.6.1 Safeguarded Copy capacity sizing overview

You must estimate the physical and virtual capacity of the following components (see Figure 3-25 on page 111):

- ▶ Safeguarded Copy Backup Capacity
- ▶ Recovery volume
- ▶ Safeguarded Copy source volume if a physical isolation approach is planned.

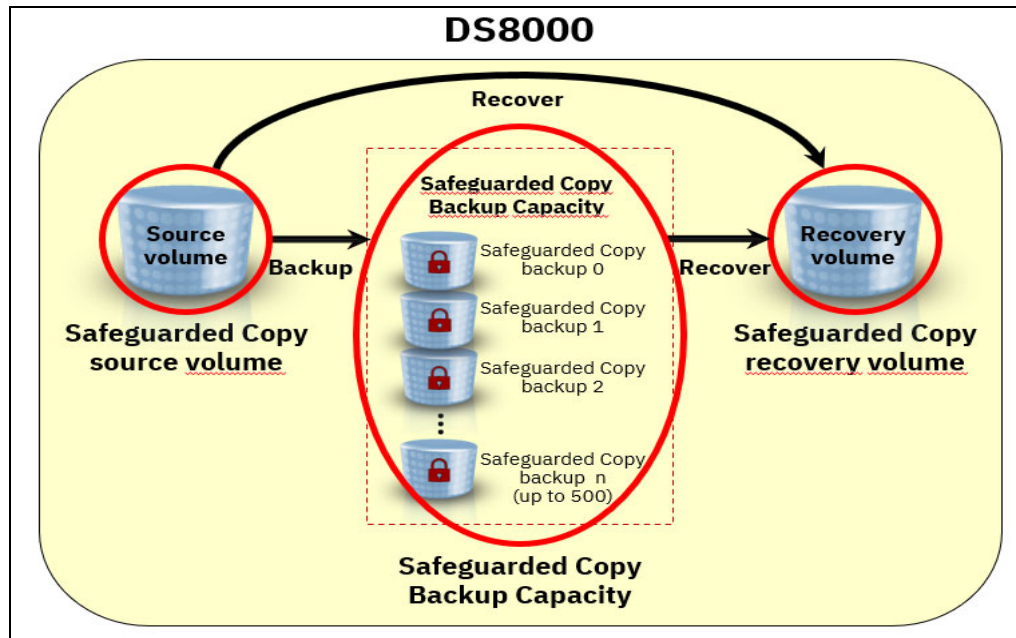


Figure 3-25 Components of Safeguarded Copy that must be sized

Physical capacity estimation is required to determine how much capacity is required to implement Safeguarded Copy, for example, to store all changed data in the Safeguarded Copy Backup Capacity and during recovery actions. The estimation also ensures that the physical limitation of the DS8000 is not exceeded.

Also, the DS8000 virtual capacity limit is based on the DS8000's cache size (see Table 3-14). Therefore, to determine whether that limit will be exceeded, the virtual capacity for all volumes within the DS8000 must be estimated. For each Safeguarded Copy source volume, you also must calculate the required Safeguarded Copy Virtual Capacity to estimate the Backup Capacity Multiplier.

Table 3-14 DS8000 capacity limits

System memory	Maximum number of physical extents	Maximum number of volume extents	Maximum physical size small extents (FB/CKD)	Maximum virtual size small extents (FB/CKD)
<= 512 GB	32 Million	64 Million	512 TiB (FB)	1024 TiB (FB)
<= 512 GB	32 Million	64 Million	551 TiB (CKD)	913 TiB (CKD)
> 512 GB	128 Million	256 Million	2048 TiB (FB)	3968 - 4096 TiB (FB)
> 512 GB	128 Million	256 Million	2205 TiB (CKD)	3538 - 3652 TiB (CKD)

Note: Configurable capacity varies between the limits based on the number and size of logical volumes.

IBM DS8880 and DS8900F configuration limits for large extents is 8 PiB of capacity for FB and 7.4 PiB for CKD.

The required Safeguarded Copy Backup Capacity and Safeguarded Virtual Capacity depend on the data change rate and the following backup management policies:

- ▶ Frequency of backups that will be taken.
- ▶ Retention period for the backups.

The required physical capacity for recovery volumes depends on how long you intend to keep the recovery volume copy relationship active and how much the Safeguarded Copy source volumes change while the relationship exists. Use the FlashCopy capacity sizing approach to estimate the required physical capacity with the Excel spreadsheets.

The following process is used to size a Safeguarded Copy solution:

1. Understand the wanted topology (virtual or physical isolation).
2. Determine the requirements for backup retention and frequency.
3. Understand how the recovery volumes are used in different scenarios.
4. Size the Safeguarded Copy recovery volume and source volume physical and virtual capacity.
5. Size the Safeguarded Copy physical and virtual capacity.
6. Model the performance of the new or upgraded storage systems.

An accurate capacity sizing is crucial because it is a best practice to use thin-provisioned volumes, and the DS8000 capacity limits should not be reached.

Although this section focuses on the capacity sizing, do not forget to complete a performance modeling of the new or upgraded DS8000 systems. Consider the following points:

- ▶ Hybrid DS8880 performance
Three High-Performance Flash Enclosure (HPFE) enclosure pairs are required in a hybrid configurations so that the global metadata is on flash drives. At least 10% of the volume capacity must be on flash storage to ensure that all volume metadata is on flash storage.
- ▶ Overall DS8000 system performance sizing
The system must handle peak write workload of production volumes and the backup workload, which is essentially 2 or 3 times the write workload of Safeguarded volumes (depending on the solution; that is, MM or Global Mirror (GM)). Ensure that the utilization of resources (such as arrays and device interfaces) is at or below 30%, based on the production workload alone.

3.6.2 Capacity sizing example for Safeguarded Copy

Understanding the topology (virtually or physically isolated), determining the requirements for backup frequency, and learning how the recovery volumes are used is important for capacity sizing.

In our example, assume that the client uses a z/OS MM HADR solution and decides that the Safeguarded Copy function will be implemented on a new physically separate DS8900F system. The production data that must be safeguarded is replicated with GM to the new storage system.

The new possible environment is shown in Figure 3-26.

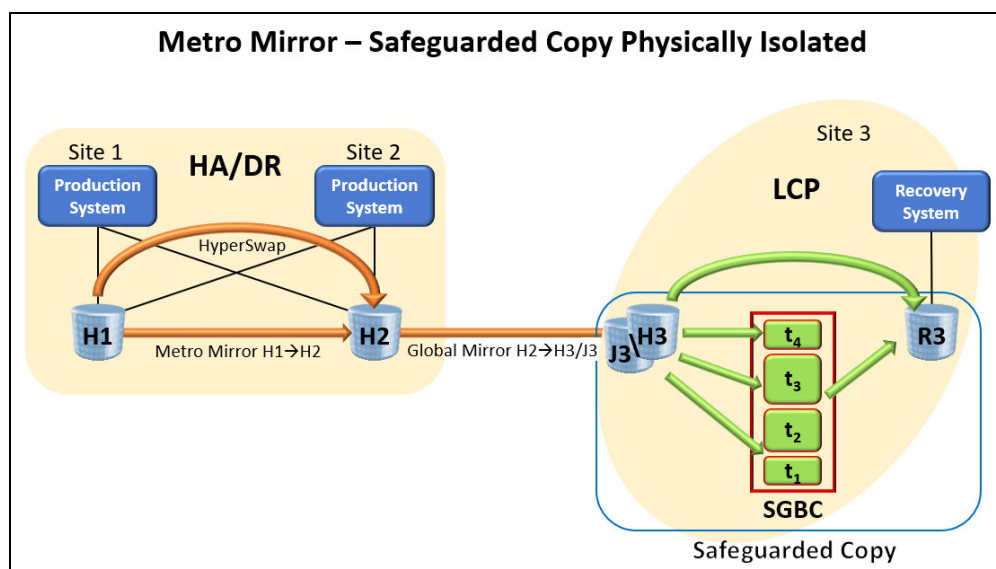


Figure 3-26 Planned new topology for Safeguarded Copy

The entire production environment must be safeguarded and the planned retention period is 24 hours with a backup frequency of every 4 hours.

The client believes that the recovery volume relationship will be active no longer than 24 hours.

With this information, you can plan the configuration of CSM ESESizer session.

You can use the provided Excel spreadsheet that is called DS8000 Import dscli volume list to prepare CSM ESESizer session copysets.xlsb to prepare the CSM copy sets for your ESESizer session.

After the session is created and all copy sets are added, set the session properties, depending on the specific information as shown in the following parameter settings for Safeguarded Copy capacity sizing example:

1. Set the **Volume query interval (secs)** to 14400 (4 * 3600 seconds).
2. Set the **Monitor reset interval (secs)** to 1 (Reset bitmap immediately after each query interval). Do *not* use a different value.

Allow the session to run at least for the planned retention period (in our example, 24 hours); or better, run it for a week. To use the provided Excel spreadsheets, import data that contains at least two more backup intervals as the number of Safeguarded Copy backups during the retention period; then, export the ESE Volume Data from the session.

Import the ESESizer session volume-level output file into the separate provided Excel spreadsheet that is called CSM ESESizer CSV Output Files calculation.xlsb and follow the steps that are described in 3.5.3, "Provided Excel spreadsheets" on page 100. The Excel spreadsheets can be downloaded from this IBM Support [web page](#).

Note: Before you import the output file into the Excel spreadsheet, check that the output files contain data for each interval from all monitored volumes. Also, ensure that the time difference between the intervals match with the specified volume query interval length.

In our example, we use the results that are shown in Figure 3-27 and Figure 3-29 on page 116.

Safeguarded Copy Solution Summary:									
				Don't forget to size the Recovery Volume capacity!			Required safeguarded Copies:		
				Safeguarded Copy overhead (one extent per volume per Safeguarded Copy backup) in GiB:	201.08			7	
				SUM of Volume Capacity in GiB:	SUM of Required Safeguarded Copy Backup Capacity in GiB:				SUM of Required Safeguarded Virtual Capacity based on adjusted Volume Backup capacity multiplier in GiB:
				64392.85	12758.58	Overall Safeguarded Copy Backup Capacity in % of Volume Capacity:			99178.32
				Overall required Safeguarded Copy Backup capacity in GiB:	12959.66	20.13			
Volume Number	Volume Name	Box Name	Average Volume Size in GiB	Max required Volume SGC capacity in GiB	Max Volume Backup capacity multiplier	Adjusted Volume Backup capacity multiplier	Required SGC Virtual Capacity based on adjusted Volume Backup capacity multiplier in GiB		
7100	UT87C0	2107.XXXX1	0.881036259	0	0	1.5	1.321554389		
7101	MV3J01	2107.XXXX1	2.643108778	0.008285277	0.003134671	1.5	3.964663167		
7102	8387C2	2107.XXXX1	2.643108778	0	0	1.5	3.964663167		
7103	G3BA1F	2107.XXXX1	7.929326333	6.753555872	0.851718745	1.5	11.8939895		
7104	G3DF0D	2107.XXXX1	7.929326333	6.168836989	0.777977438	1.5	11.8939895		
7105	G3BA0A	2107.XXXX1	7.929326333	10.00207034	1.261402283	2	15.85865267		
7106	SM3002	2107.XXXX1	7.929326333	9.095333889	1.147050015	2	15.85865267		
7107	G3S002	2107.XXXX1	7.929326333	20.3613047	2.567847992	3	23.787979		
7108	G3S001	2107.XXXX1	7.929326333	16.97077954	2.1402549	3	23.787979		
7109	MV3T02	2107.XXXX1	7.929326333	17.90939055	2.258627001	3	23.787979		
710A	G3MQ15	2107.XXXX1	7.929326333	18.68066009	2.355894979	3	23.787979		
710B	G3S003	2107.XXXX1	7.929326333	13.82897099	1.744028485	2	15.85865267		
710C	G3S000	2107.XXXX1	7.929326333	16.33946257	2.060636917	3	23.787979		

Figure 3-27 Used Solution Summary worksheet for our example

The Solution Summary worksheet provides information about the required overall physical Safeguarded Copy Backup Capacity, the required overall Safeguarded Virtual Capacity, and the Backup Capacity Multiplier per volumes.

Although this view is a volume-level view, the Solution Summary worksheet provides the following information:

- ▶ Safeguarded Copy Source Volume Capacity: ~64.4 TiB
- ▶ Overall required physical Safeguarded Copy Backup Capacity: ~13.0 TiB
- ▶ Overall required Safeguarded Virtual Capacity based on the calculated multiplier: ~99.2 TiB
- ▶ Backup Capacity Multiplier per volume to prepare Safeguarded Copy in the DS8000

With this information, you know also the virtual capacity that is required:

- ▶ Safeguarded Copy source volume: ~64.4 TiB
- ▶ Recovery volume: ~64.4 TiB

The missing part in our example is sizing the recovery volume physical capacity. Therefore, run the ESEsizer session again, but with slightly different session properties, as shown in the following parameter settings for a recover volume capacity sizing example:

1. Set the **Volume query interval (secs)** to 14400 (4 * 3600 seconds to see how the capacity is growing over time).
2. Set the **Monitor reset interval (secs)** to 0 (no bitmap reset after each query interval).

Allow the session run for 24 hours, which is the planned period to have the recovery volume relationship active. It can run longer and use CSM Scheduled Tasks to reset the bitmap automatically every 24 hours. Then, export the ESE box data from the session.

Import the ESESizer session box-level output file into the provided Excel spreadsheet and click **Yes** in the spreadsheet when the window opens (see Figure 3-28).

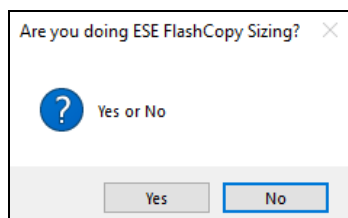


Figure 3-28 Selection: ESE FlashCopy sizing wanted YES or NO

Then, the spreadsheet provides a pivot chart in which you can select **Required ESE-FC cap. with small extents in GiB** to display the required recovery volume capacity over the monitored period.

In our example, the physical capacity that is required for the recovery volumes is ~19.5 TiB.

Now, all Safeguarded Copy-related capacities are calculated based on the monitored DS8000 Write Monitoring Bitmap.

In addition to those capacities, you must consider the physical and virtual capacity that is required to establish the GM solution. Therefore, the GM journal volumes (FlashCopy targets) also must be sized. In our example, we use the capacity sizing results of the recovery volumes:

- ▶ FlashCopy targets physical capacity: ~19.5 TiB
- ▶ FlashCopy targets virtual capacity: ~64.4 TiB

Based on these results, the new storage system requires 116.6 TiB physical capacity and 292.4 TiB virtual capacity to implement the physically isolated Safeguarded Copy solution that is shown in Figure 3-26 on page 113.

With this information, you have a good starting point for further discussions with your customer.

You might need to adjust the Safeguarded Copy Backup Capacity, depending on which scenarios or use cases (for example, a ransomware attack) the Safeguarded Copy solution must protect. That adjustment depends on customer requirements or the service-level agreement (SLA).

Also, discuss the Backup Capacity Multiplier per volume with the customer. It is a best practice to group volumes and use the same multiplier for those grouped volumes.

For an initial impression of what is the highest required multiplier and how many volumes include the same multiplier, the **Solution Summary** worksheet includes the table that is shown in Figure 3-29.

Number of Volumes:	1728
Adjusted Volume Backup capacity multiplier:	Number of Volumes with same Backup capacity multiplier:
1.5	1658
2	30
3	16
4	7
5	17
6	0
7	0
8	0

Figure 3-29 Number of volumes with the same multiplier table

Volumes can be grouped by using the following approaches:

- ▶ Volume name or z/OS volser.
- ▶ Volume size.
- ▶ Operating systems instances (perhaps the best way), such as AIX volume groups or z/OS storage groups. You need more information from your customer for this option, such as which volumes belong to which z/OS storage group.

After you receive this information, check what is the highest volume Backup Capacity Multiplier in the group of volumes that belongs to that z/OS storage group and use the highest multiplier for all volumes in this group.


When you complete the process of grouping the volume and assigning the multiplier, calculate again the overall required virtual capacity so that you ensure to not reach the limits that are described in 3.6.1, “Safeguarded Copy capacity sizing overview” on page 110, or 2.5, “Safeguarded Copy sizing considerations” on page 42.

Note: With the DS8880 8.5 SP7 and DS8900F 9.1 or later, you can dynamically increase the volume backup capacity multiplier, although they are part of an active Safeguarded Copy relationship.

Performance modeling of the new or upgraded DS8000 systems is important. For more information about Safeguarded Copy performance considerations, see 2.7, “Safeguarded Copy performance considerations” on page 56.

If you need support for a Safeguarded Copy capacity sizing, contact your IBM representative.

Note: For large DS8000 environments, we recommend that you contact IBM to support you during the setup of the monitoring environment. Depending on your region, contact the IBM Advanced Technology Group or the IBM EMEA Storage Competence Center.



Implementation and management

This chapter provides information about how to implement a Safeguarded Copy environment by using the IBM DS8000 Storage Management GUI or DS CLI, and how to manage Safeguarded Copy with IBM Copy Services Manager (CSM).

We also show the Storage Management GUI options and the DS CLI commands that are required to configure Safeguarded Copy. Furthermore, we demonstrate how to create a Safeguarded Copy session by using CSM.

In the second part of the chapter, we describe the management of a Safeguarded Copy environment with a CSM Safeguarded Copy session, including ongoing operations, such as expiring backups, recovering a backup, or expanding Safeguarded Virtual Capacity, and how to restore a backup to a production volume.

This chapter also includes some Safeguarded Copy scheduled tasks examples for various 3-Site and 4-Site copy topologies.

This chapter covers the following topics:

- ▶ 4.1, “Implementing a Safeguarded Copy environment” on page 118
- ▶ 4.2, “Managing a Safeguarded Copy environment” on page 129
- ▶ 4.3, “Restoring a Safeguarded Copy backup to production” on page 160
- ▶ 4.4, “Scheduled tasks examples with Safeguarded Copy topologies” on page 217

4.1 Implementing a Safeguarded Copy environment

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

- ▶ Sizing Safeguarded Copy Backup Capacity
- ▶ Verifying the prerequisites
- ▶ Deciding what topology to implement
- ▶ Defining the backup frequency
- ▶ Specifying the retention period

For more information about planning, see Chapter 2, “Planning and considerations” on page 21.

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

1. The Safeguarded Copy Backup Capacity is configured for all the relevant volumes by using the Storage Management GUI or the DS CLI.
2. A Safeguarded Copy Session is configured with the CSM, with which the Safeguarded Copy environment can be managed.

Figure 4-1 shows the configuration that we use as an example to set up a Safeguarded Copy environment in a Metro Mirror (MM) (high availability (HA)) environment.

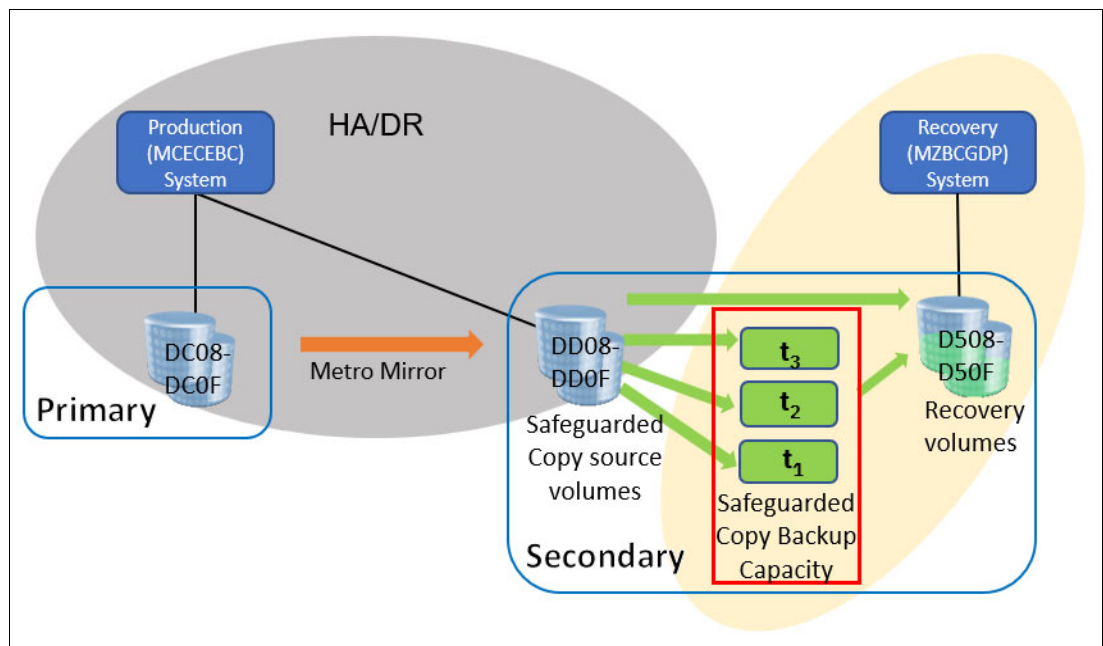


Figure 4-1 Safeguarded Copy environment example with Metro Mirror

This example shows an MM solution with Safeguarded Copy that is used at the secondary site. The MM secondaries are the Safeguarded Copy source volumes. This Safeguarded Copy is an example of virtual isolation. The Safeguarded Copy production volumes are part of the high availability and disaster recovery (HADR) solution (in this case, the MM primaries).

Figure 4-2 shows a Global Mirror (GM) solution with Safeguarded Copy that is used at the secondary site. The GM secondaries are the Safeguarded Copy source volumes. This Safeguarded Copy is an example of physical isolation. The Safeguarded Copy production volumes are part of the HADR solution (in this case, the MM primaries).

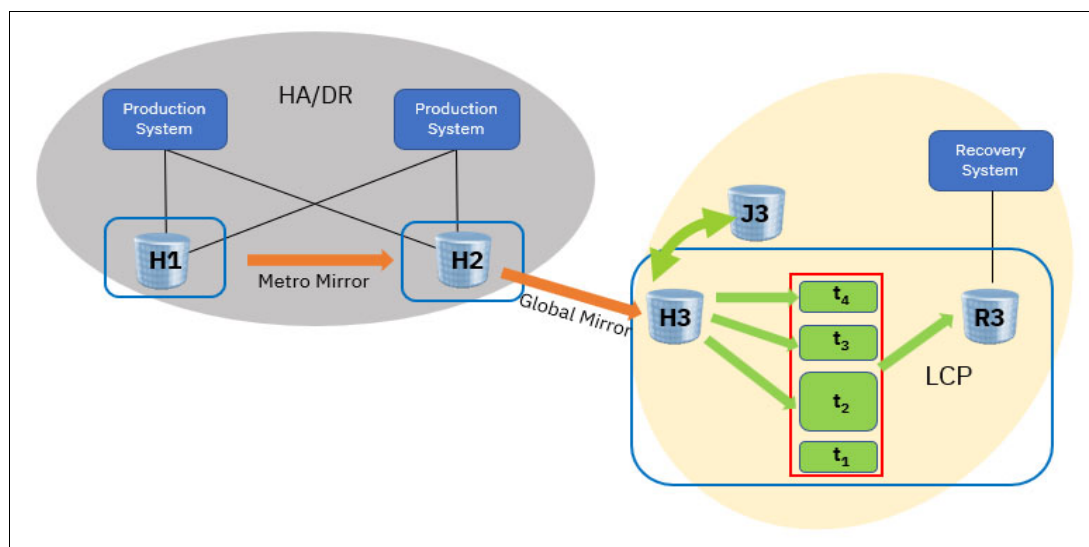


Figure 4-2 Safeguarded Copy environment example with Global Mirror

The Safeguarded Copy environment requires a set of Safeguarded Copy source volumes and an equal number of recovery volumes, which often are created as Extent Space Efficient (ESE) volumes. These recovery volumes are necessary to recover data from a Safeguarded Copy backup. For more information about this requirement, see 2.5.3, “Recovery and Safeguarded Copy source volumes” on page 47.

Note: Throughout the following examples, the term *source volume* refers to the volume where the Safeguarded Copy relationship is defined. This volume can be an MM or GM primary or secondary. The term *production volume* refers to the volume that is active to the host.

4.1.1 Configuring Safeguarded Copy Backup Capacity

Safeguarded Copy Backup Capacity is assigned and dedicated to a source volume. The Safeguarded Copy source volume can be a production MM or GM primary and also secondary volume. The allocation of Safeguarded Copy Backup Capacity is like an ESE or thin-provisioned volume. When defining this capacity, only space for the metadata is allocated. Physical extents are allocated only after the first Safeguarded Copy backup (Consistency Group (CG)) is established and changes to the production volumes occurred.

The required Safeguarded Copy Backup Capacity for each source volume depends on the number of changed tracks during the retention period of the Safeguarded Copy backup, and on the number of backups that you are planning to keep. For more information about capacity planning, see 2.5, “Safeguarded Copy sizing considerations” on page 42.

Note: The assigned Backup Capacity must be at least as large as the production volume. At least 1.5 times the capacity of the production volume must be assigned to allow a full copy of the production volume.

The maximum Safeguarded Copy Backup Capacity is 16 TiB per source Fixed Block (FB) volume and 14.6 TiB for a Count Key Data (CKD) volume.

You cannot expand the Backup Capacity of a volume after you initially set it unless you are on DS8880 8.5.SP7 or DS8900F 9.1 or later.

To optimize capacity allocation, it is preferable to use small extents for storage pools that contain Safeguarded Copy Backup Capacity.

With DS8880 8.5 and later, you can configure Safeguarded Copy Backup Capacity by using the Storage Management GUI or the DS CLI. These options are described next.

Storage Management GUI

To create Safeguarded Copy Backup Capacity with the Storage Management GUI, complete the following steps:

1. After you log in to the GUI, select the **Volume** icon.

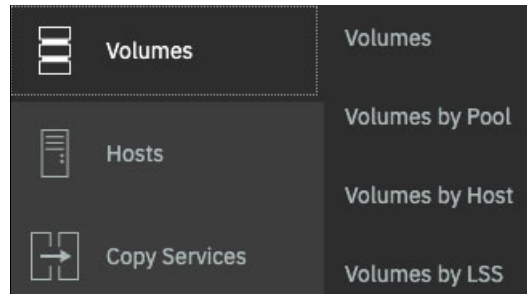


Figure 4-3 Volume menu

2. In the **Volumes** sub-menu, choose the volume list that you prefer to find the required volumes.

3. Right-click a volume or a selected range of volumes and click the **Actions** tab. Then, select **Safeguarded** → **Configure Capacity**, as shown in Figure 4-4.

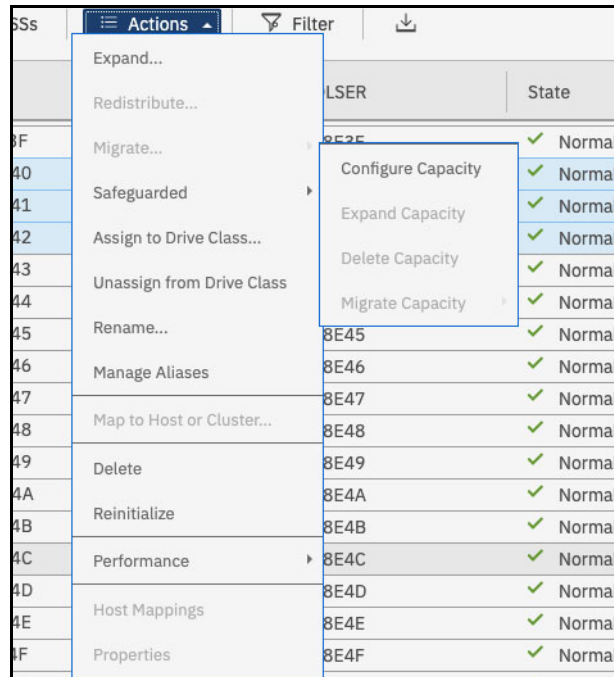


Figure 4-4 Safeguarded tab in the Volume menu

4. Specify the backup location (named storage pool) and the Backup Capacity Multiplier, and then select **Configure** (see Figure 4-5).

Configure Safeguarded Capacity

Volumes

Configure the safeguarded capacity for the volumes by entering the location to store safeguarded backups in and the capacity multiplier for the safeguarded virtual capacity.

Backup location:

Backup capacity multiplier(*):

4.50 Mod1

Pool usable capacity

8.10 KMod1

System provisioned capacity

98.60 TiB

Need Help

Figure 4-5 Configure Safeguarded Copy

As you can see, you can select multiple volumes and create the backup capacity for them in one step. From the backup location menu, you can select eligible extent pools.

Note: The backup location (storage pool) must include the same DS8000 server affinity as its source volume.

All volumes that are selected in a range must include the same Backup Capacity Multiplier.

The highest Backup Capacity Multiplier for a 2 TiB FB source volume is 8, and for a 1 TiB CKD EAV volume, it is 16.

The minimum Backup Capacity Multiplier number is 1.5.

To assign a backup capacity in GiB (for FB volumes) or in cylinders (for CKD), you must use the suitable DS CLI command with the **-cap** and **-type** parameters.

5. You can follow the task progress by expanding the More details section. Click **Close** after the task is 100% completed (see Figure 4-6).

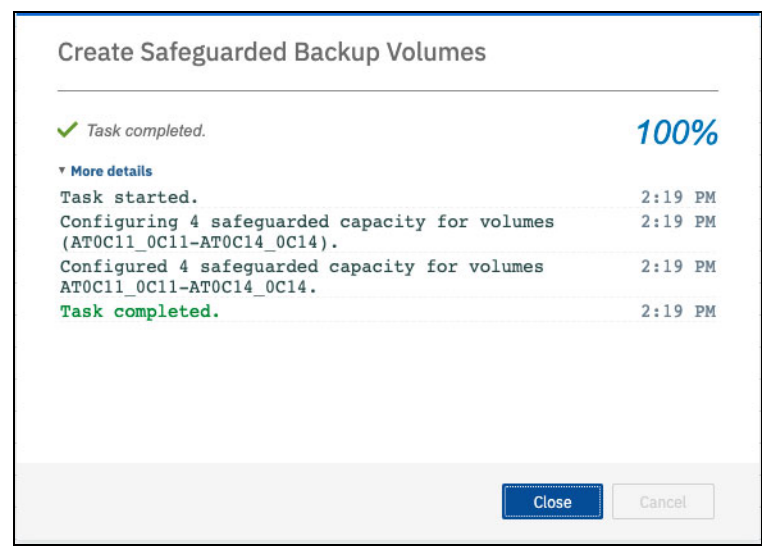


Figure 4-6 Create Safeguarded Backup Volumes task progress

After Safeguarded Copy Backup Capacity is created, you can modify the Volume table view filter (as indicated by the arrow in Figure 4-7) and select **Safeguarded**, **Safeguarded Location**, **Safeguarded Virtual Capacity**, and **Safeguarded Recovered**.

Name	Safeguarded	Safeguarded Location	Safeguarded Virtual Capacity	Safeguarded Recovered	↑	!!!
ATOC10_OC10						
ATOC11_OC11		CKD_z/OS_2	1.5 Mod1			
ATOC12_OC12		CKD_z/OS_2	1.5 Mod1			
ATOC13_OC13		CKD_z/OS_2	1.5 Mod1			
ATOC14_OC14		CKD_z/OS_2	1.5 Mod1			

Figure 4-7 Displaying Safeguarded Copy information per volume

As shown in Figure 4-7 on page 122, the backup location (Safeguarded Location) and backup capacity size (Safeguarded Virtual Capacity) for the selected volumes are displayed. At this stage, Safeguarded and Safeguarded Recovered indicators are empty; that is, no Safeguarded Copy backup was created yet and no Recovery action is ongoing for these volumes.

If you make a mistake and want to move the backup capacity to a different location, you can migrate it to another storage pool. If no Safeguarded Copy active CSM session exists, you can delete Safeguarded Copy Backup Capacity. Also, if you run out of backup space, you can dynamically expand it. All these options are available from the Safeguarded menu, as shown in Figure 4-8.

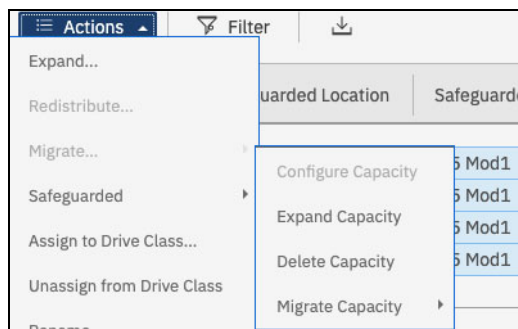


Figure 4-8 Other Safeguarded Copy Backup Capacity operations in the Storage Management GUI

For more information about these options, see 4.2.7, “Other Safeguarded Copy-related DS CLI and DS GUI operations” on page 159.

Note: The Expand Capacity option in the GUI is supported for DS8900 R9.x only. To expand the backup capacity for DS8880 R8.5, you must use the DS CLI, as shown in Example 4-1.

DS CLI

The DS CLI commands `manageckdvol` and `managefbvol` of DS8880 8.5 and later provide a new parameter that is called `-action mksafeguardedcap`. In combination with the new `-cap` or `-multiplier` parameters, this parameter enables you to configure a backup capacity.

Note: With DS8900 R9.x, and with DS8880 R8.5.x, the minimum multiplier number is 1.5.

A multiplier value of 1.5 means that the backup capacity has 50% more space than the Safeguarded Copy source volume. Therefore, a multiplier value of 2 assigns twice the capacity of the source volume, and so on. Alternatively, you can assign a backup capacity in GB (for FB volumes) and cylinders (for CKD volumes) with the `-cap` and `-type` parameters that are used in `manageckdvol` and `managefbvol` commands.

We use the `-multiplier` parameter in our example because it is easier to use.

In our example, we select the source volume range DD0C - DD0F to create the backup capacity with the DS CLI, as shown in Example 4-1.

Example 4-1 Creating Safeguarded Copy Backup Capacity with the DS CLI

```
dsccli> manageckdvol -multiplier 1.5 -action mksafeguardedcap -extpool p9 DD0C-DD0F
CMUC00570I manageckdvol: Backup capacity for CKD volume DD0C is successfully created.
CMUC00570I manageckdvol: Backup capacity for CKD volume DD0D is successfully created.
CMUC00570I manageckdvol: Backup capacity for CKD volume DD0E is successfully created.
CMUC00570I manageckdvol: Backup capacity for CKD volume DD0F is successfully created.
```

With the DS CLI commands **lsckdvol -1**, **lsfbvol-1**, **showckdvol**, or **showfbvol**, you can list the assigned backup capacity, the location of the backup capacity, how much capacity is used, and if Safeguarded Copy protection exists, as shown in Example 4-2.

Example 4-2 DS CLI showckdvol example for one volume

```
dsccli> showckdvol DD0C
Name                ckd_p9_DD0C
ID                  DD0C
accstate            Online
datastate           Normal
configstate         Normal
deviceMTM           3390-9
volser              RSDCOC
....
....
....
safeguardedcap (cyl) 45077
safeguardedloc       P0
usedsafeguardedcap (cyl) 0
safeguarded          No
sgcrecovered         No
safeguardedcapstate  Normal
```

An effective way to get an overview of the Safeguarded Copy status per volume is to use the DS CLI command **lsckdvol -sgc**, **lsfbvol-sgc**, as shown in Example 4-3:

Example 4-3 DS CLI lsckdvol -sgc for a volume range

```
dsccli> lsckdvol -sgc DD0C-DD0F
Date/Time: July 2, 2022 4:33:40 AM CEST IBM DSCLI Version: 7.9.30.154 DS: IBM.2107-75LAH81
Name      ID  extpool cap (cyl) safeguardedcap (cyl) safeguardedloc usedsafeguardedcap (cyl) safeguarded sgcrecovered safeguardedcapst
=====
ckd_p9_DD0C 0006 P9      30051 45007          P9          0              No          No          Normal
ckd_p9_DD0D 0007 P9      30051 45007          P9          0              No          No          Normal
ckd_p9_DD0E 0008 P9      30051 45077          P9          0              No          No          Normal
ckd_p9_DD0F 0009 P9      30051 45077          P9          0              No          No          Normal
```

The DS CLI list command output in Example 4-3 provides information about the configured Safeguarded Copy Backup Capacity and the used Safeguarded Copy Backup Capacity per volume. Moreover, the backup has never been created and recovered for these volumes (“safeguarded” = No and “sgcrecovered” = No). In addition, you see that the state of the Safeguarded Copy Backup Capacity is Normal.

If you make a mistake and want to move the backup capacity to a different location, you can migrate it to another storage pool. If no Safeguarded Copy active CSM session exists, you can delete the Safeguarded Copy Backup Capacity. Also, if you run out of backup space, you can dynamically expand it. All these Safeguarded Copy actions can be run by using the DS CLI `manageckdvol` or `managefbvol` commands and the following **-action** parameters:

- ▶ **migsafeguardedcap**: Migrate backup capacity to a different extent pool.
- ▶ **rmsafeguardedcap**: Delete backup capacity.
- ▶ **expandsafeguardedcap**: Dynamically expand backup space.

For more information about the DS CLI commands, see this IBM DS8900 documentation [web page](#).

The Safeguarded Copy Backup Capacity is now configured.

4.1.2 Creating a Safeguarded Copy session with IBM Copy Services Manager

After you create the backup capacity for each of the involved source volumes, you can establish a Safeguarded Copy session with the IBM CSM.

Note: The Safeguarded Copy function requires a fully licensed IBM CSM. CSM 6.3.3.0 or later is required for the latest Safeguarded Copy functions enhancement that is described in this publication.

It is a best practice to implement CSM Standby Server for redundancy when you manage a CSM Safeguarded Copy session.

Creating a Safeguarded Copy session with CSM requires two sets of volumes: a set of source volumes and an equivalent set of recovery volumes. The CSM session requires a one-to-one relationship between source volumes and recovery volumes.

The recovery volumes that are used in this example are thin-provisioned, ESE volumes with the same virtual capacity as the source volumes.

In our example, devices DC08-DC0F are the production volumes, DD08 - DD0F are the source volumes (H1), and devices D508 - D50F are recovery volumes (R1), as shown in Figure 4-1 on page 118.

To create a Safeguarded Copy session, complete the following steps:

1. Log in to your CSM server and click the **Sessions** tab.
2. In the Sessions window, click **Create Session**, and a new window opens. From the **Hardware type** menu, select **DS8000**, **DS6000**, or **ESS 800**, and from the **Session type** menu, select **Safeguarded Copy**.

Provide a Session name (ITS0_SGC_RSDDXX in our example in Figure 4-9) and select the DS8000 system in the **Site 1 location** menu.

Click **OK** to continue (see Figure 4-9).

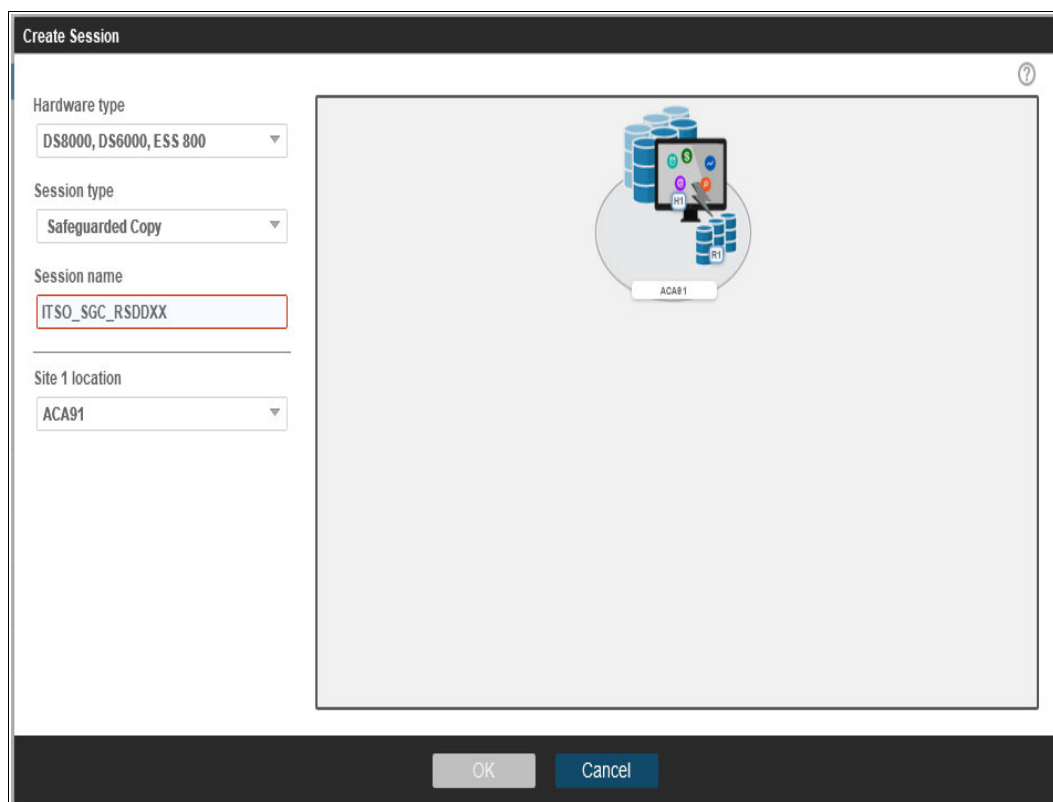


Figure 4-9 Creating a CSM session

3. A window opens in which you can add copy sets for this session. Click **Launch Add Copy Sets Wizard**.

4. In the **Add Copy Sets** wizard, select the volumes that are required to create the copy sets for your Safeguarded Copy session, as shown in Figure 4-10. The volume list can be selected from the drop-down menu or imported from a CSV file.

Add Copy Sets - ITSO_SGC_RSDCXX

Choose Host1

Choose the Host1 storage system.

*Host1 storage system
DS8000:BOX:2107.ACA91

*Host1 logical storage subsystem
DS8000:2107.ACA91:LSS:DD

*Host1 volume
DS8000:2107.ACA91:VOL:DD08 (RSDC08)

Volume Details
 User Name: RSDC08
 Full Name: DS8000:2107.ACA91:VOL:DD08
 Type: 3390
 Capacity: 10017 Cyls
 Protected: No
 Space Efficient: ESE
 z/OS Connection: No

☒ Use a CSV file to import copy sets

Browse... No file selected.

< Back Next > Finish Cancel

Figure 4-10 Add Copy Sets wizard for a Safeguarded Copy session

5. In our example, we use a CSV file to import the copy sets:
 - Host1 (H1) are the source volumes (in our example, DD08 - DD0F).
 - Recover1 (R1) are the recovery volumes (in our example, D508 - D50F).

Example 4-4 shows an abstract for the CSV file that is used and the required formatting.

Example 4-4 Abstract of the CSV to import the copy sets for a Safeguarded Copy Session

H1	R1
DS8000:2107.ACA91:VOL:DD08	DS8000:2107.ACA91:VOL:D508
DS8000:2107.ACA91:VOL:DD09	DS8000:2107.ACA91:VOL:D509

- The **Add Copy Sets** wizard verifies that the copy sets are matching, and might display an error or warning message. Verify the messages and, if everything is okay, click **Next** twice.
In our example, we receive a warning message because the source volumes DD08 - DD0F are in another CSM session. They are the MM secondary volumes of our HADR solution. Therefore, this warning message can be ignored because this situation does not cause any issue or conflict in DS8000 Copy Services (CS) functions.
- Confirm that you want to add the copy sets by clicking **Next**. A progress bar is displayed during this process and the Results are then displayed, as shown in Figure 4-11.



Figure 4-11 Add Copy Sets results

Now, the CSM Safeguarded Copy session is established and is in an Inactive status because no backup was created yet (see Figure 4-12).

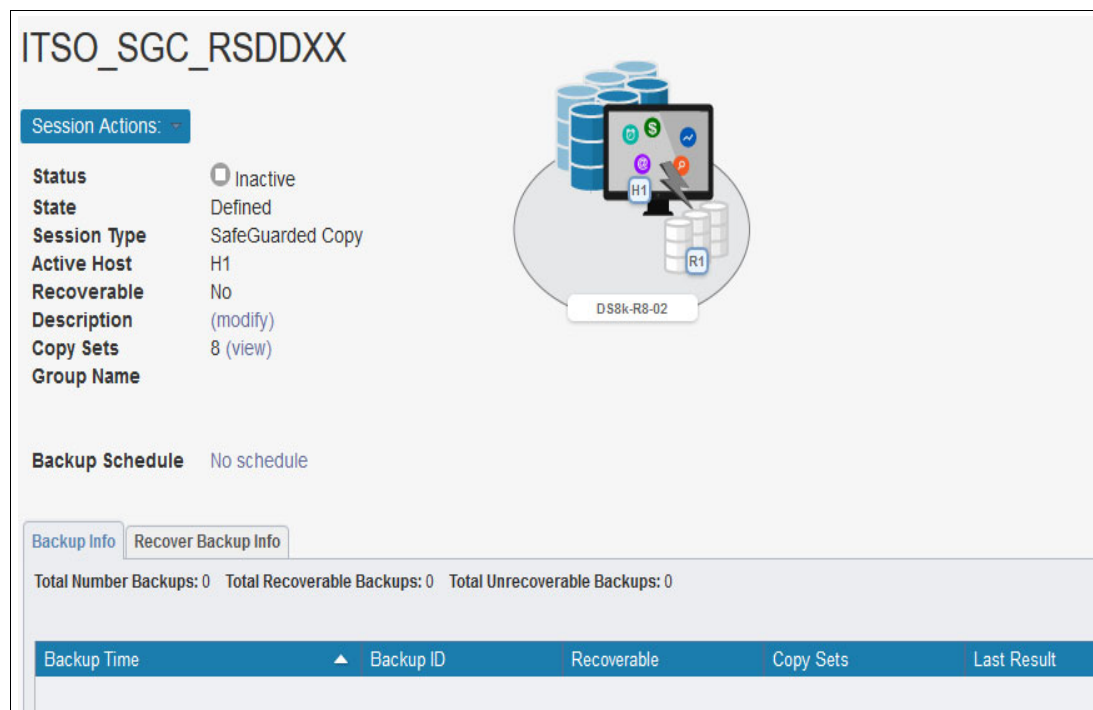


Figure 4-12 CSM Safeguarded Copy Session after creation

Before you create the first backup, verify and modify the properties of your Safeguarded Copy session to ensure that it meets your requirements. For more information, see 4.2.1, “Verifying and modifying the Safeguarded Copy session properties” on page 130.

The next section describes the session properties, how you can establish a backup (CG), the expiration of a backup, and the recovery operation.

4.2 Managing a Safeguarded Copy environment

In 4.1, “Implementing a Safeguarded Copy environment” on page 118, we explained what is required to prepare your Safeguarded Copy environment and how you create a CSM Safeguarded Copy session after you complete the planning phase.

In this section, we describe the management of your Safeguarded Copy environment with IBM CSM V6.2.3 and later, and what you can modify with the Storage Management GUI or DS CLI regarding Safeguarded Copy.

You can manage a Safeguarded Copy environment with CSM or IBM Geographically Dispersed Parallel Sysplex (IBM GDPS) Logical Corruption Protection Manager 4.2 2 with APAR PH17926 and later. This publication focuses on a CSM implementation. For more information about GDPS implementations, see *IBM GDPS: An Introduction to Concepts and Capabilities*, SG24-6374.

Within a CSM Safeguarded Copy session, you can create, expire, and recover a Safeguarded Copy backup.

Depending on your environment setup, you might need to coordinate the Safeguarded Copy session activity within your environment.

For example, if you have a GM environment and your Safeguarded Copy source volumes are GM secondaries, you must complete the following steps to take a point-in-time consistent backup:

1. Pause your GM with consistency (Suspend GM session).
2. Wait until GM is paused (Suspended GM session State).
3. Establish a Safeguarded Copy backup (Backup Safeguarded Copy session).
4. Resume your GM session (Start GM session).

Unlike this example with GM session, the examples that we use in the following sections of this chapter are based on the environment that is shown in Figure 4-1 on page 118 and do not require any coordination between the CSM MM and Safeguarded Copy sessions.

However, you can associate a Safeguarded Copy session and its source volumes to the respective CSM session in which these Safeguarded Copy source volumes are defined as primary or secondary volumes. Whenever you add volumes (copy sets) in the CSM replication session, both associated sessions change to the Warning status because of the volumes mismatch. For more information about this process, see “Safeguarded Copy session associations” on page 157.

CSM features a GUI and a command-line interface (the CSMCLI). In our examples, we focus on the CSM GUI. For more information about CSM and the CSMCLI, see this IBM Documentation [web page](#).

4.2.1 Verifying and modifying the Safeguarded Copy session properties

Before you create the first backup, verify and if necessary modify the properties of the Safeguarded Copy session so that it meets your requirements. To view or change these options, open your session and select **Session Actions** → **View/Modify** → **Properties**.

You can modify the following properties:

- ▶ Session Options (see Figure 4-15 on page 132):
 - Enter a detailed session description.
 - z/OS Management.
- ▶ Backup Options (see Figure 4-13):
 - Select **Expire Backup On Auto Roll** (default is cleared).
 - Minimum Timeframe Per Backup (Minutes; default is 30).
 - Retention Period Since Last Recoverable Backup (Days and Hours).
- ▶ H1-R1 Options (see Figure 4-14 on page 131):
 - Select **FlashCopy: No Copy** (default is selected).
 - Select **Persistent** (default is cleared).

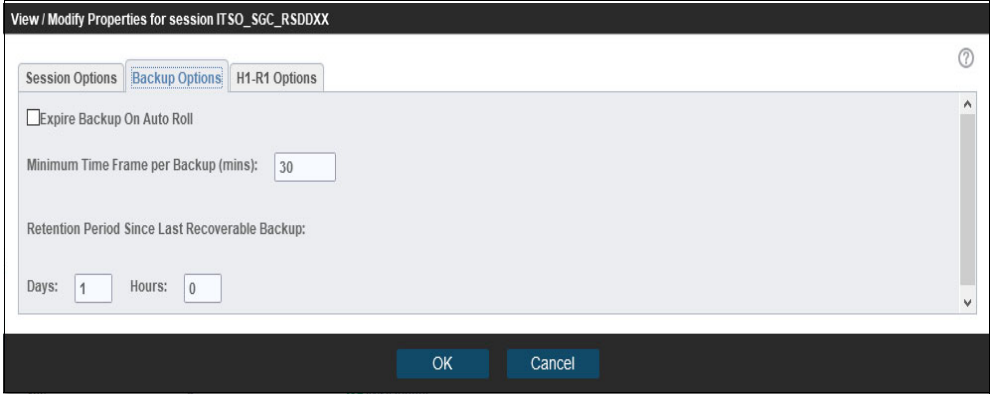


Figure 4-13 Safeguarded Copy Backup Options properties

The key session properties are on the Backup Options and H1-R1 Options tabs.

You can change these parameters, even if the session is in an Active status.

As shown in Figure 4-13, you do not change the H1-R1 options; instead, you modify only the *Backup option Retention Period Since Last Recoverable Backup* value so that the backups expire automatically after one day.

When the *Expire Backup On Auto Roll* option is selected, the session automatically expires a backup when the session determines that one or more of the volumes auto-rolled the backup. Set the *Expire Backup on Auto Roll* option to free up space whenever one or more volumes do not have enough backup capacity to form new backups.

This feature can help avoid out-of-space conditions. However, when a backup is automatically expired, it is no longer available for recovery across any of the volumes that contained that backup.

By default, this option is *not* selected; therefore, you must select it to enable this feature. When this option is not set, the backup is not automatically expired so that if one or more volumes did not auto roll the backup, those volumes can still be recovered to that backup.

To allow recovery to those volumes, you must remove any volumes that indicate that they auto rolled that backup from the session.

Note: With the introduction of the Expire Backup on Auto Roll option in CSM 6.2.7, if the backup is in a recovery relationship and the hardware rolls off a volume, CSM does not expire it if the option is selected.

With Minimum Timeframe per Backup, you specify how frequently you can create a Safeguarded Copy backup. This option makes it difficult for a malicious user to create backup after backup, in a short period, until all good backups are rolled off automatically.

The default value is 30 minutes. For example, if the default value is configured and you attempt to create a backup 15 minutes after the last backup was created, the backup request fails and you receive a failure message.

Note: Although Safeguarded copies are important, a high frequency of backups might affect the performance of your production environment. Therefore, it is a best practice *not* to use a period of less than 10 minutes. For more information about performance considerations, see 2.7, “Safeguarded Copy performance considerations” on page 56.

Retention Period Since Last Recoverable Backup defines how long a backup exists before CSM automatically expires the backup. The default values of 0 days and 0 hours mean that backups do not automatically expire. The minimum Retention Period is 1 hour. CSM does not roll off all older Safeguarded Copy backups, so at least the last recoverable backup remains.

Note: You should set a retention period that fulfills your service-level agreements (SLAs).

If you forgot to specify a retention period, CSM expires the oldest backup when the limit of 500 Safeguarded Copy backups is reached. Many backups can require much more capacity.

Therefore, it is a best practice to specify a retention period that fulfills your requirements and fits the available capacity of your DS8000 system.

Within the H1-R1 Options tab, you can define whether a FlashCopy is with or without background copy and if the relationship is persistent if you perform a CSM recovery action for a specific backup. The default is *No Copy*, Non-Persistent, as shown in Figure 4-14.

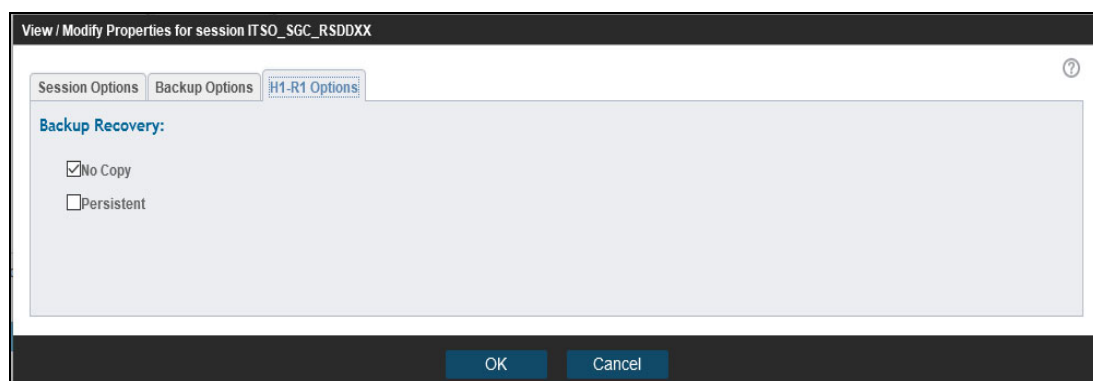


Figure 4-14 CSM Safeguarded Copy Session H1R1 options

The *Persistent* option is used to keep the recovery relationship established on the hardware after all tracks are copied to the target volume.

In addition to these properties, you can enable the z/OS Management function in the Session Options tab, which is available with CSM version 6.2.11 or later for mainframe environments, as shown in Figure 4-15.

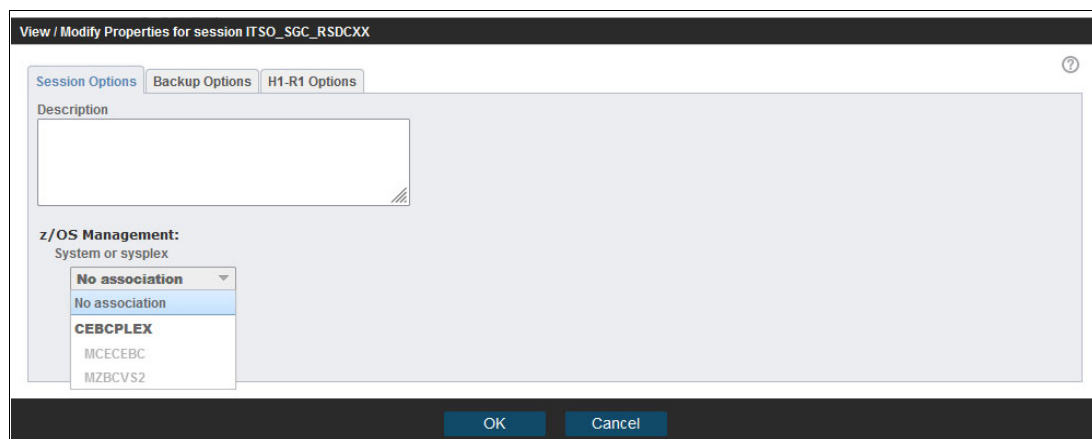


Figure 4-15 CSM Safeguarded Copy Session Options

Note: Consider the following points:

- ▶ The z/OS Management section is visible only if z/OS Connections are defined in the CSM server. Otherwise, this option is not displayed in the Session Options window.
- ▶ z/OS IOS APAR OA59561 must be applied to the z/OS system that is associated with the Safeguarded Copy or FlashCopy sessions. If the APAR is not applied, the **backup** or **flash** commands result in an error.

By associating the session to a z/OS sysplex, the necessary commands to perform a Safeguarded Copy backup are passed down to the IOS component on z/OS. This configuration dramatically improves the performance and minimizes application impact.

To use this feature, all volumes in the session must be attached to the z/OS system (defined in an Input/Output Definition File (IODF) or Hardware Configuration Definition (HCD)) that is associated to the session. If the volumes are not attached, the Safeguarded Copy backup fails. Then, sysplex association must be removed so that the backup can be run the traditional way.

It is a best practice for customers taking Safeguarded Copy backups in a production mainframe environment to create a z/OS connection and associate the respective Safeguarded Copy session to it.

We provide more information about how to create a z/OS connection next.

Creating z/OS connection

This section includes only a high-level process summary about how to create z/OS Connection in the CSM GUI. For more information about this process, see *Best Practices for DS8000 and z/OS HyperSwap with Copy Services Manager*, SG24-8431.

The following prerequisites must be met before you can define the z/OS Connection in the CSM GUI:

- The HyperSwap Management address spaces HSIB and HSIBAPI are started in a z/OS LPAR.

Note: The z/OS HyperSwap HA configuration does not need to be enabled if the z/OS connection is used for Safeguarded Copy only.

- HSIB uses the SOCKPORT parameter to define the port that is used to establish the CSM z/OS IP connection. After a connection is established, HSIB starts a HyperSwap Socket Server address space for each connection (IEESYSAS program) to manage the communication.
- z/OS LPAR also runs the PAGENT address space with a loaded Application Transparent Transport Layer Security (AT-TLS) policy. This policy describes the certificates that are used to encrypt and decrypt traffic over the HSIB socket port.

This policy and certificates are required if you need the traffic over z/OS Connection to be encrypted.

After these prerequisites are met, complete the following steps:

1. From the CSM GUI, select **Storage** → **z/OS Connections** and then, click **Add Host Connection** as shown in Figure 4-16.

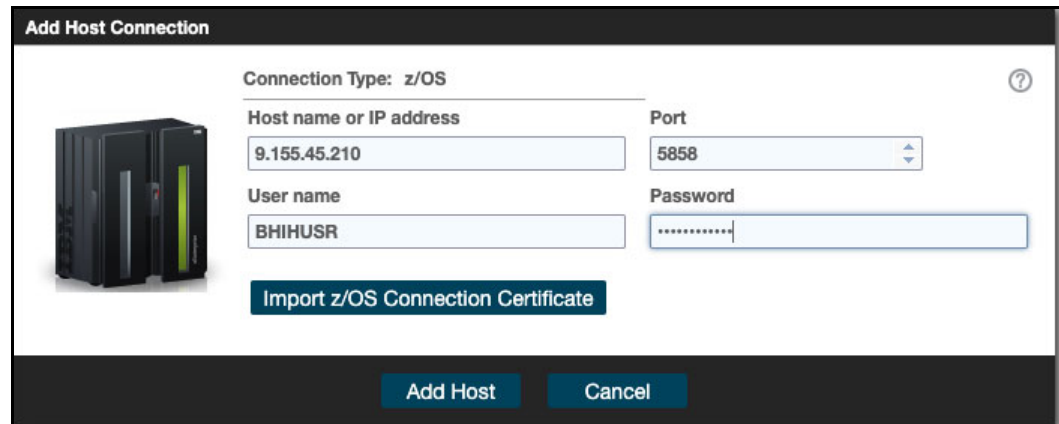


Figure 4-16 Add Host Connection option

2. In the **Add Host Connection** window, enter the IP address or hostname of the LPAR you want this CSM server to be connected to, along with the username and its password that were created in this LPAR. The default port is 5858; however, you can change it if this port number is taken.
3. Click **Import z/OS Connection Certificate** to import the z/OS certificate that was exported from your LPAR. A file selection dialog opens and you can browse for the certificate file on your local system.

After you select and confirm the file, the selected certificate file is shown next to the Import button in the Add Host Connection dialog.

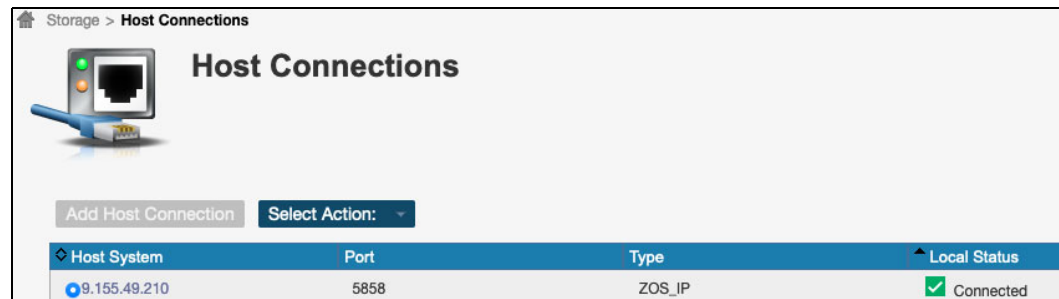
4. Click **Add Host** (see Figure 4-17). The z/OS IP host connection definition is created and the GUI transferred the certificate to the CSM server and imports it into its keystore repository.



The 'Add Host Connection' dialog box is shown. It has a title bar 'Add Host Connection'. On the left is an icon of a server rack. The main area contains the following fields: 'Connection Type: z/OS' (dropdown), 'Host name or IP address' (text box with '9.155.45.210'), 'Port' (dropdown with '5858'), 'User name' (text box with 'BHIHUSR'), and 'Password' (password box with dots). Below these fields is a button 'Import z/OS Connection Certificate'. At the bottom are two buttons: 'Add Host' and 'Cancel'.

Figure 4-17 Add Host Connection and Import z/OS Connection Certificate

If the z/OS IP host connection was configured correctly on the z/OS LPAR and the CSM server, CSM can connect to the LPAR that serves the defined IP address. The newly created z/OS connection is listed in the **Storage** → **Host Connections** window, as shown in Figure 4-18.



The 'Host Connections' window is shown. It has a title bar 'Storage > Host Connections'. On the left is an icon of a network card. The main area has a heading 'Host Connections'. Below the heading are two buttons: 'Add Host Connection' and 'Select Action:'. Below these buttons is a table with the following data:

Host System	Port	Type	Local Status
9.155.49.210	5858	ZOS_IP	Connected

Figure 4-18 z/OS Host Connections table view

- Establish a Storage z/OS direct connection from the CSM GUI by selecting **Storage** → **Storage Systems** and then, click **Add Storage Connection**, as shown in Figure 4-19.

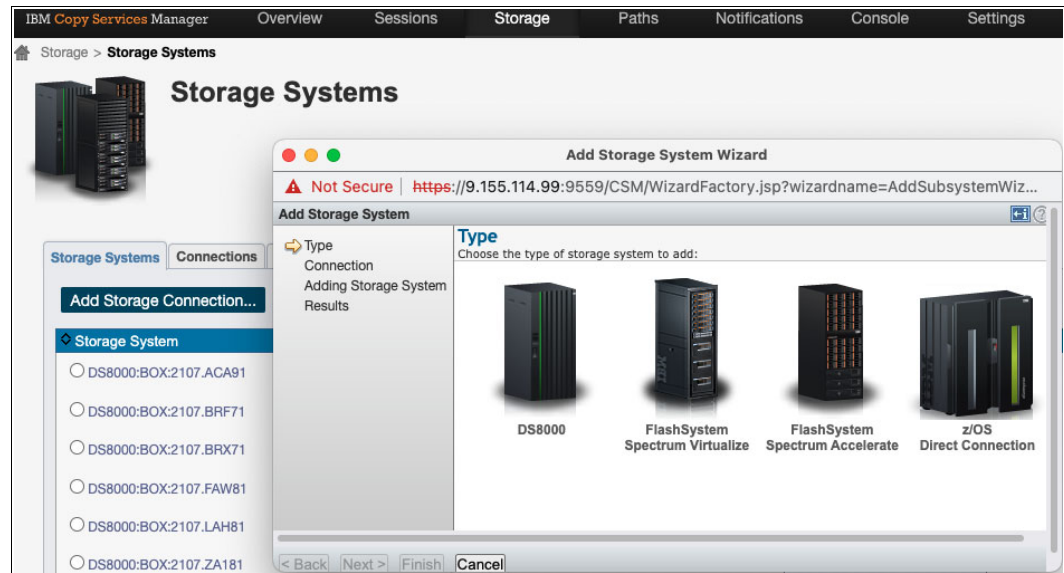


Figure 4-19 Adding Storage z/OS Direct Connections

- In the **Add Storage Connection** wizard, select **z/OS Direct Connections**. In the next window, you can select all storage systems that can communicate with a z/OS LPAR, as shown in Figure 4-20.

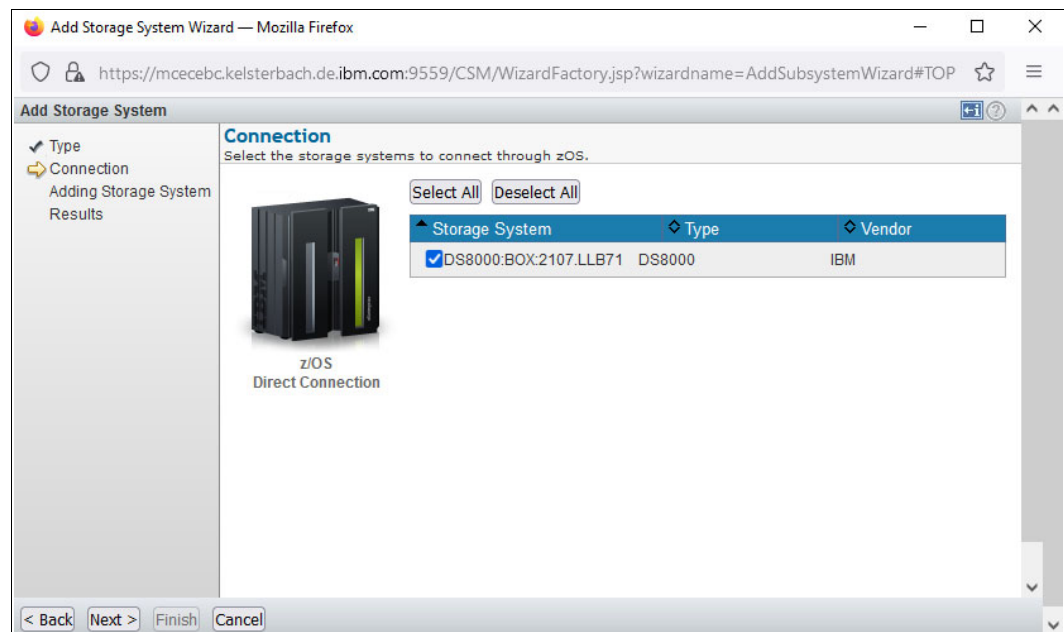


Figure 4-20 Selecting storage systems

7. Selected **Next** and then, **Finish** in the wizard. The new z/OS Direct Connections are displayed for each storage system, as shown in Figure 4-21.

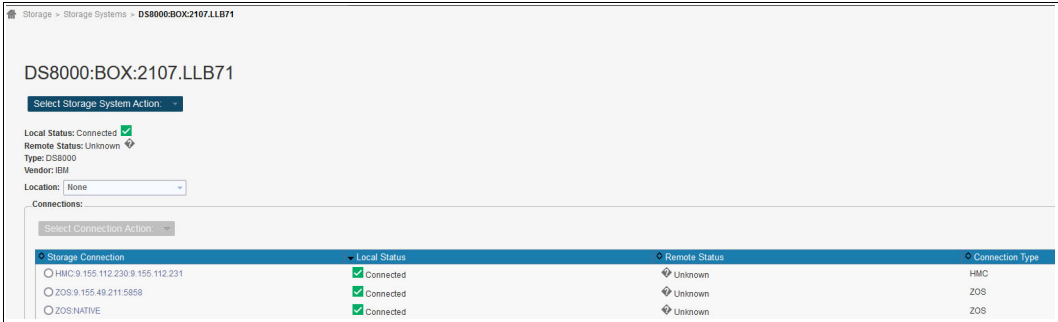


Figure 4-21 Storage System connection view

If the CSM server is running on z/OS, you also see a z/OS native connection for each storage system.

4.2.2 Creating a Safeguarded Copy backup

With CSM, you can create a backup manually, by using a script, or by using the CSM Scheduler.

Before you create a backup, ensure that you coordinate this action with your environment or other CSM sessions, and take the actions that might be required to create a consistent backup. Manual backups can be used for initial Safeguarded Copy testing to build a recovery environment for testing, or if a Safeguarded Copy backup is required between the scheduled backups. The best practice is to use the CSM Scheduler to create regular backups.

How frequently you create backups and how long you specify the retention period of a backup depends on your requirements or any SLAs you need to fulfill. More frequent backups or a longer retention period might require more physical capacity in the DS8000.

For more information, see Chapter 2, “Planning and considerations” on page 21.

Creating a manual backup with CSM

To create a manual backup, open your session and select **Session Actions** → **Commands** → **Backup**. If this backup is the first backup, only the Backup and Refresh States options are available; otherwise, you see all other available options for a Safeguarded Copy session, as shown in Figure 4-22.

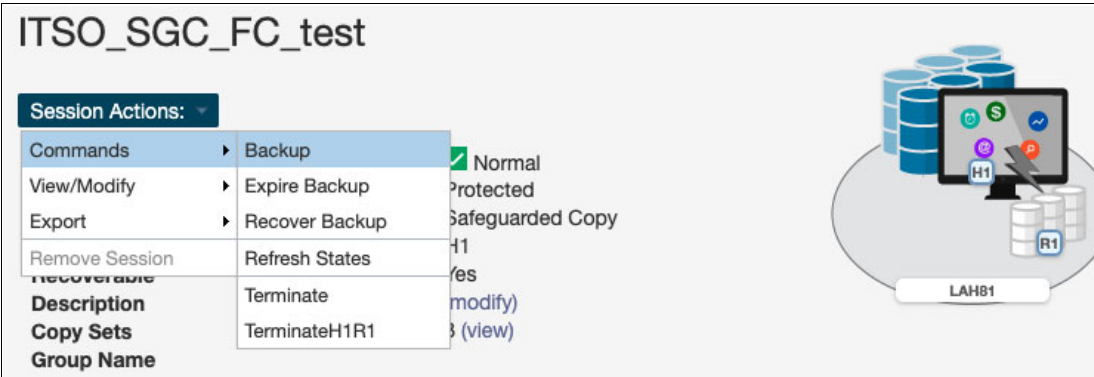


Figure 4-22 Safeguarded Copy Session Actions

After the first backup is created, the session state is Protected and the status is Normal, as shown in Figure 4-23.

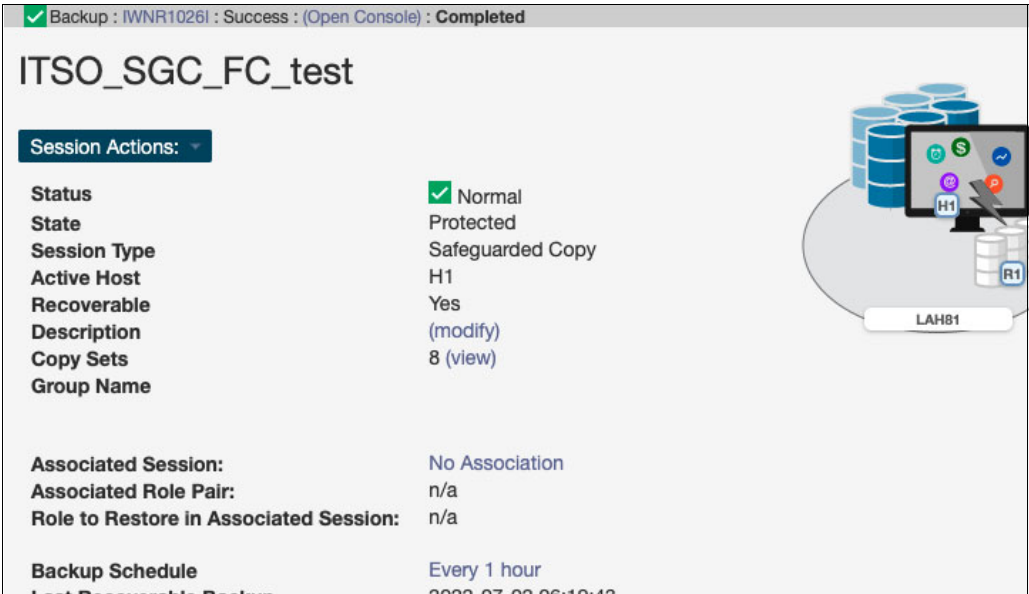


Figure 4-23 Safeguarded Copy Session after the first backup

The IWNR1026I message indicates that the backup command was successfully completed.

Note: If you try to create a backup more often than the value of *Minimum Timeframe per backup* allows (in our example, the value is set to 30 minutes), you receive the following error message:

IWNR2802E: A backup command is not allowed now for session ITSO_SGC_RSDDXX due to the current backup frequency value in the session options.

Creating periodical Safeguarded Copy backups with CSM Scheduler

In almost all cases, a Safeguarded Copy backup is a periodical task; therefore, the CSM Scheduler or the use of a script that uses CSMCLI commands is more practical than performing manual backups. To schedule regular backups with the CSM Scheduler, complete the following steps:

1. When you define your CSM session, you can schedule backups periodically by clicking **No schedule** in your CSM session (see Figure 4-12 on page 128), or by selecting **Scheduled Task** under the **Settings** tab to open the Scheduled tasks window. Click **Create Task** to continue, as shown in Figure 4-24.

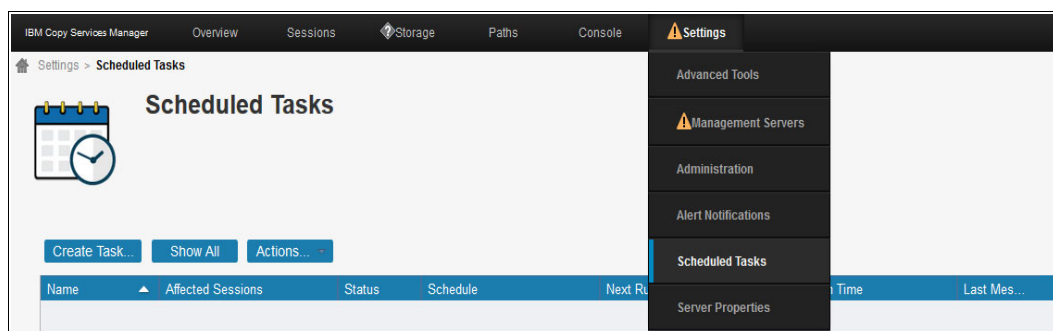


Figure 4-24 Creating a Scheduled Task

2. After you click **Create Task**, a new window opens. In this window, you must enter a Task Name and a meaningful description. In addition, you can select **Create a PE package if error occurs running the task**. With that option selected, you can easily provide CSM log data that IBM support often asks for problem root cause analysis (see Figure 4-25).

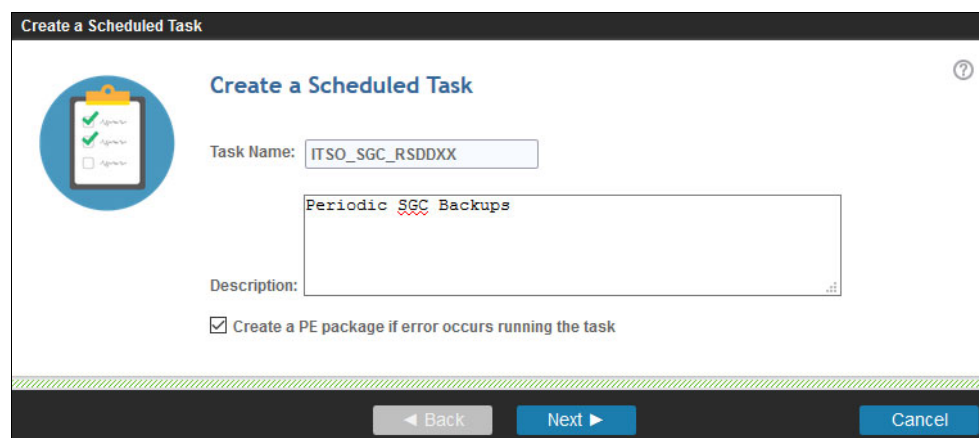
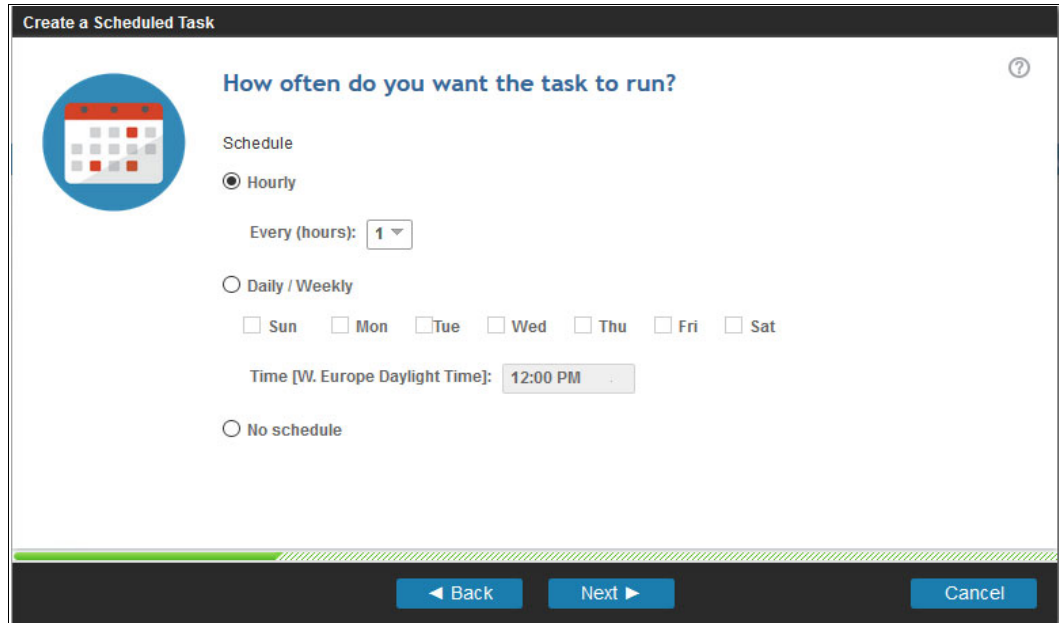


Figure 4-25 Scheduled Task Name and Description

3. Click **Next** and you can define how often you want the task to run. In addition to *Hourly*, you can select *Daily/Weekly* on a specific time (see Figure 4-26 on page 139). In our example, we want a backup every hour; therefore, we choose 1 hour.

Note: Starting with CSM 6.2.10.1, the smallest timeframe you can select is 5 minutes. On earlier releases, 30 minutes is the smallest timeframe that you can select. DS8000 supports only schedules that are 10 minutes or longer for a Safeguarded Copy related scheduled task.



Create a Scheduled Task

How often do you want the task to run?

Schedule

☒ Hourly

Every (hours):

☐ Daily / Weekly

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

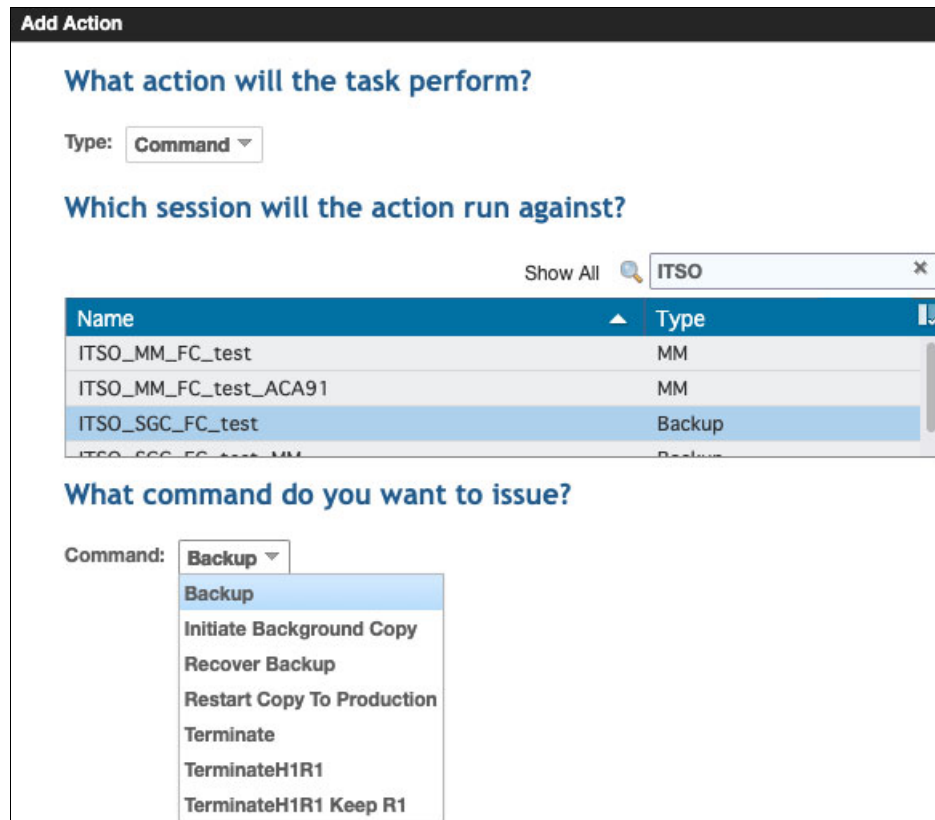
Time [W. Europe Daylight Time]:

☐ No schedule

Figure 4-26 Scheduled Task: Defining how often the task should run

- Click **Next** to define what action that you want to perform by clicking **Add Action**. Now, you can select the session and the suitable command for this session.

In our case, we select the Safeguarded Copy session `ITSO_SGC_FC_test` (use the Show All search window to find the session), select **Backup**, and click **OK** (see Figure 4-27).



Add Action

What action will the task perform?

Type:

Which session will the action run against?

Show All

Name	Type
ITSO_MM_FC_test	MM
ITSO_MM_FC_test_ACA91	MM
ITSO_SGC_FC_test	Backup
ITSO_SGC_FC_test_MM	Backup

What command do you want to issue?

Command:

- Backup
- Initiate Background Copy
- Recover Backup
- Restart Copy To Production
- Terminate
- TerminateH1R1
- TerminateH1R1 Keep R1

Figure 4-27 Scheduled Task Add Action

5. You are returned to the “What action would you like to perform?” window (see Figure 4-28). Here, you can add actions to this task when they are required; for example, if coordination with other sessions is required. Alternatively, you may run another task if this task is successful or if it fails. From the menu for “Run the following task if successful” and “Run the following task on failure”, there is a list of all tasks that are defined in this CSM server.

In our example, we add only one action and continue with the next step by clicking **Next**.

The screenshot shows a web interface titled "Create a Scheduled Task". The main heading is "What action would you like to perform?". On the left is a blue circular icon with a white running figure. To the right of the heading are five buttons: "Add Action" (highlighted in dark blue), "Modify Action", "Remove Action", "Up", and "Down". Below these buttons is a table with the following data:

Step #	Action type	Session	Action
1	Command	ITSO_SGC_FC_test	Issue 'Backup' to 'ITSO_SGC_FC_test'

Below the table are two dropdown menus. The first is labeled "Run the following task if successful" and the second is labeled "Run the following task on failure". Both dropdowns currently show "Do not run a Task". At the bottom of the window are three buttons: "Back", "Next" (highlighted in dark blue), and "Cancel".

Figure 4-28 Schedule Task: What action would you like to perform

6. The Scheduled Task Summary window opens. After you verify that this task is correctly configured, click **Finish** to create the task, as shown in Figure 4-29 on page 141. If something is incorrect, click **Back** to make changes for this scheduled task. The new task is *not* enabled automatically.

Scheduled Task Summary

Task Name: test

Description:

Collect PE package if error occurs running the task: No

Scheduled: Every 2.0 hours

Run the following task if successful Do not run a Task

Run the following task on failure Do not run a Task

List of Actions:

Step #	Action type	Session	Action
1	Command	ITSO_SGC_FC...	Issue 'Backup' to 'ITSO_SGC_FC_test' se

Back

Finish

Cancel

Figure 4-29 Scheduled Task Summary

7. You are returned to the Scheduled Tasks window. Here, you can complete the following actions after you select a specific task, as shown in Figure 4-30:
 - Modify Task: Change the setting for a specific task.
 - Remove Task: Delete a task.
 - Run Task: Run a Task once; for example, to test the task.
 - Enable **Task** → **Now** or At a specific time.
The task runs as it is defined in the schedule until it is unavailable.
 - Disable Task: Disable an enabled task.

Create Task...

Actions...

Name	ns	Status	Schedule
ITSO_FC_SGC_Tes	test	Disabled	Every 1 hour

Modify Task

Remove Task

Run Task

Enable Task

Disable Task

Select All

Deselect All

Clear Filter

Figure 4-30 Scheduled Task main window: Selecting an action for a specific task

8. The newly created scheduled task is *not* enabled automatically. To do so, select your task, and click **Enable Task** under **Actions**. There are two options to enable the scheduled task:
- **Now**: The scheduled task is enabled and the next run is based on the schedule. You also can run the task as soon as it is enabled. Select the task and from the **Action** menu, and then select **Run Task** → **Now** command.
 - **At specified time**: The task is enabled and it runs at the specified time.

Select **Yes** in the Confirmation window to complete this step.

Regardless of which option you choose, a confirmation message appears that indicates that the task is enabled successfully. The task status changes to Enabled, as shown in Figure 4-31.

Note: When an Hourly schedule is selected, the schedule is based on the time that the task was enabled. The task does not run immediately with **Now**; instead, it runs only after the scheduled hourly time elapses. However, you also can run the task when it is enabled. Select the task, and from the **Action** menu, select **Run Task** → **Now**.

Create Task...		Actions...	
Name	Affected Sessions	Status	Schedule
ITSO_FC_SGC_Test	ITSO_SGC_FC_test	Enabled	Every 1 hour

Figure 4-31 Scheduled Task main window: task enabled

The task schedule is now complete, and CSM creates a backup every hour.

When you open your Safeguarded Copy session, the **Backup Info** tab shows more detailed information for each individual backup version, such as backup timestamp and ID; whether the backup is recoverable; the copy progress of the last backup version; and used capacity for each backup version (Figure 4-32 on page 143).

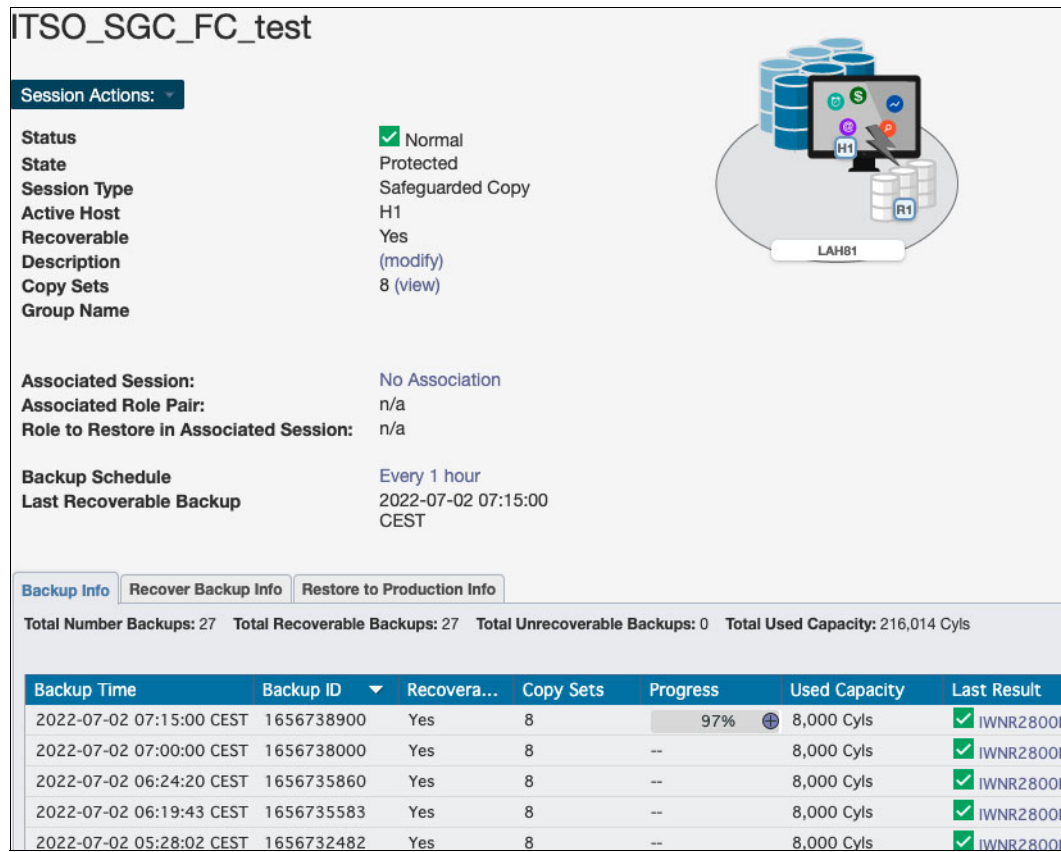


Figure 4-32 Safeguarded Copy Active Session overview

Note: If the Used Capacity or Progress columns show --, it means that either the DS8000 model or microcode does not support this query statistics or the capacity has not been used because the Safeguarded Copy source volume has not been changed.

You must be using DS8900 R9.3 or later and CSM 6.3.3.0 and later to get these statistics.

Used Capacity indicates the number of tracks that had to be hardened in the backup capacity before a new backup was created. The value displays in cylinders if all volumes are CKD or in TiB or GiB if all volumes are FB or there is a mix of the two formats.

This data is not meant to be used for capacity management. This value might not represent the total capacity that is used in a volume's backup capacity because there is some metadata that is stored in the backup capacity too. However, the value can help you determine whether there is a large fluctuation in the number of writes between backups at a certain time, which might lead to a need for more backup capacity.

For the last backup that is taken on a Safeguarded Copy session, as new writes occur to the source volume, those tracks must be written to the backup capacity to safeguard that data so that it can be restored if needed. If there are too many writes pending, they can affect the next backup, and the cache scans might not complete.

The Progress column shows, for the last backup, the number of tracks that are left to copy. This value might go up and down depending on the I/O that is being written to the source volume. The progress does not prevent a new backup from being taken, but if a backup or scheduled backup fail because the cache scans did not complete, this value might help indicate the cause.

To find out more about the progress of the last backup, hover your cursor over the + sign next to the percentage in the Progress column. A new information window opens. In our example in Figure 4-33, 120,008 tracks out of 3,606,120 were updated in the Safeguarded Copy source volume. 97% of tracks of the source volumes have not yet been updated. The Progress% number drops as the new updates occur on the source volumes.

Progress	Used Capacity	Last Result
97%	3	
	8	
	8,000 Cyls	✓ IWNR2800I

Backup ID 1656741600

Total source tracks: 3606120

Tracks to be copied: 120008

Figure 4-33 Progress of the last backup

Both Used Capacity and Progress (Tracks to be Copied) can be displayed on the volume level. To get the progress level per volume, you must select the last backup version, and the new window shows details for each volume in this backup (Figure 4-34).

View Backup

Backup Time2022-07-03 01:00:00 CEST

Number of copy sets8

Last Result

IWNR2800I

RecoverableYes

Filter...

H1	Last Result	Tracks to be Copied	Used Capacity	Expansion
DS8000:2107.LAH81:VOL:0108	<div><div></div><div>IWNR2819I</div></div>	3842	17 Cyls	
DS8000:2107.LAH81:VOL:0109	<div><div></div><div>IWNR2819I</div></div>	3834	18 Cyls	
DS8000:2107.LAH81:VOL:010A	<div><div></div><div>IWNR2819I</div></div>	3820	18 Cyls	
DS8000:2107.LAH81:VOL:010B	<div><div></div><div>IWNR2819I</div></div>	3825	19 Cyls	
DS8000:2107.LAH81:VOL:010C	<div><div></div><div>IWNR2819I</div></div>	3818	19 Cyls	
DS8000:2107.LAH81:VOL:010D	<div><div></div><div>IWNR2819I</div></div>	3810	19 Cyls	
DS8000:2107.LAH81:VOL:010E	<div><div></div><div>IWNR2819I</div></div>	3886	14 Cyls	
DS8000:2107.LAH81:VOL:010F	<div><div></div><div>IWNR2819I</div></div>	3986	8 Cyls	

OK

Figure 4-34 Used Capacity and Progress per volume

Note: With DS8880 8.5 and later and CSM 6.2.3 and later, you cannot create more than 500 Safeguarded Copy backups per production volume.

4.2.3 Expiring a Safeguarded Copy backup

The decision of when a backup expires is essential because a longer retention period potentially requires more capacity in the DS8000 system.

You can manually or automatically expire a backup with CSM, as described in the following section.

Automatically expiring a backup with CSM

The easiest way to expire a backup automatically is to specify the retention period in your Safeguarded Copy session.

You can click **Retention Period Since Last Recoverable Backup** in the properties window of your session to a value that meets your requirements.

In our example session, we set the retention period to 1 day. If you want to modify this parameter, in your CSM session select **Session Actions** → **View/Modify** → **Properties** and then, open the **Backup Options** tab.

Here, you can modify the *Retention Period Since Last Recoverable Backup* parameter, as shown in Figure 4-35.

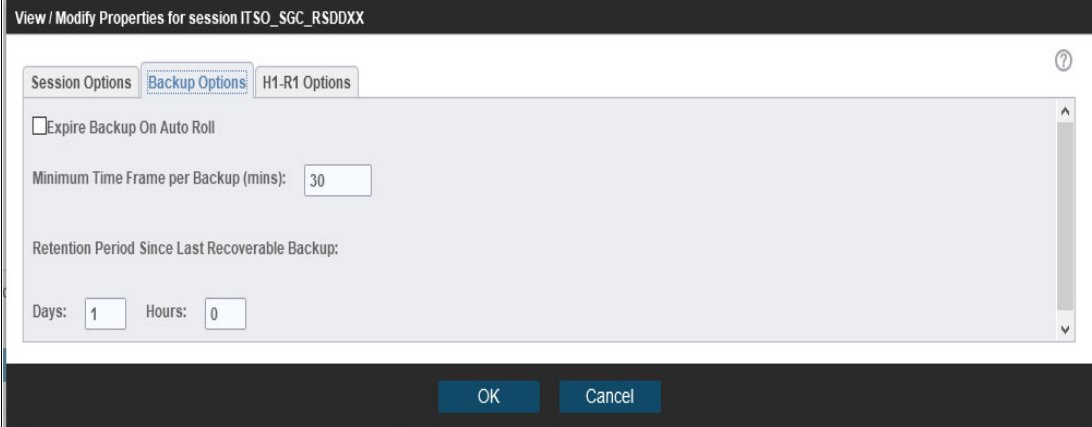


Figure 4-35 Example of Safeguarded Copy Backup Options properties

When you specified this parameter in your session, CSM periodically checks whether a backup is rolled-off because of the specified retention policy.

If you set a retention period, CSM automatically rolls-off all backups that are older than the last recoverable backup plus the retention period.

For each group of rolled-off backups, you can find a message in the CSM Console log. An example of the message for our session ITS0_SGC_RSDDXX is shown in Example 4-5.

Example 4-5 Console Message example for a rolled-off backup

IWNR2816I : The backup retention period policy for session ITS0_SGC_RSDDXX caused the backup created at 'backup_time' and all earlier backups to expire.

Also, CSM rolls off the oldest Safeguarded Copy backups when a backup is taken and the maximum number of supported Safeguarded Copy backups is reached.

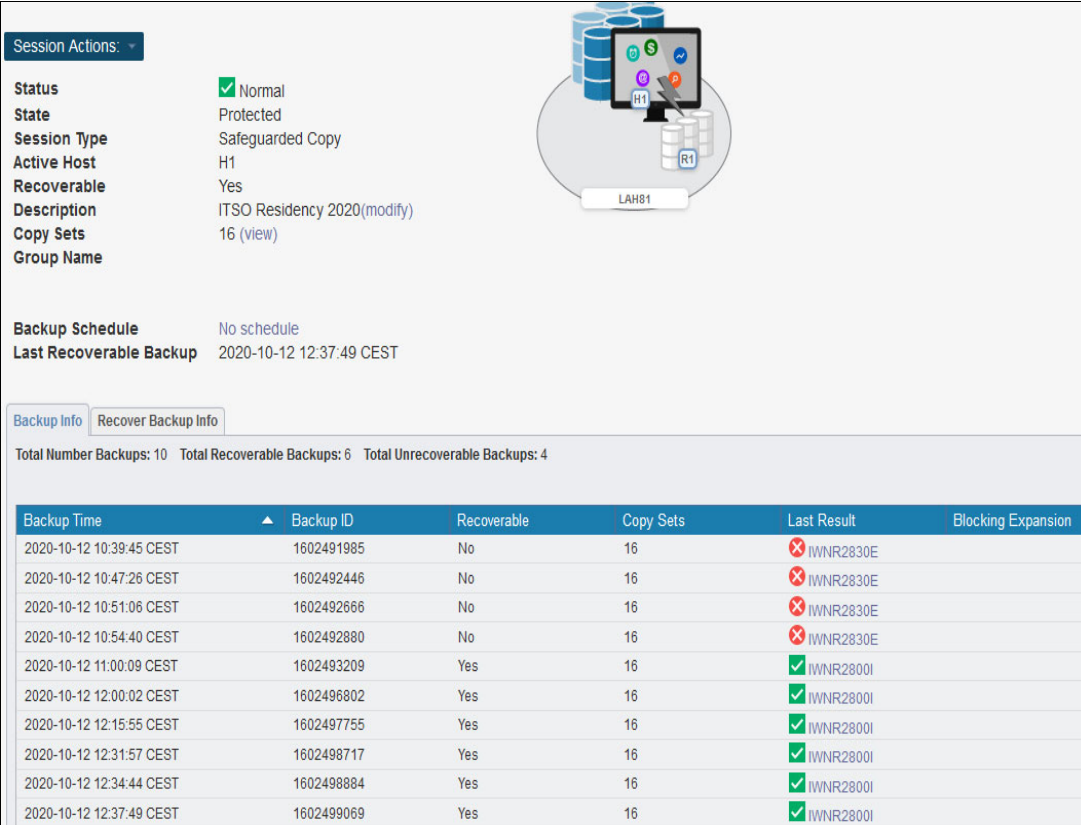
Manually expiring a backup with CSM

Under some circumstances, a backup must be expired manually with CSM; for example, if you run out of space in a DS8000 storage pool.

Note: When **Expire Backup On Auto Roll (Backup Options** in session properties) is selected, the CSM Safeguarded Copy session automatically expires a backup when the session determines that one or more of the volumes auto-rolled the backup. By default, this option is *not* selected; therefore, you must select it to enable this feature.

If such a scenario occurs, you might need to adjust your Safeguarded Copy environment by changing your retention period or backup schedule, or increasing your Safeguarded Copy Backup Capacity to meet your SLAs (for more information, see 2.6, “Safeguarded Copy backup priority consideration in an out-of-space situation” on page 55).

Figure 4-36 shows the list of all backups, including expired backups, which are no longer recoverable.



The screenshot displays the IBM DS8000 Safeguarded Copy interface. At the top, there's a 'Session Actions' dropdown and a status summary. The status is 'Normal', 'Protected', 'Safeguarded Copy', 'H1', 'Yes', 'ITSO Residency 2020(modify)', '16 (view)', and 'Group Name'. Below this, the 'Backup Schedule' is 'No schedule' and the 'Last Recoverable Backup' is '2020-10-12 12:37:49 CEST'. A diagram shows a server icon labeled 'LAH81' connected to a storage pool icon.

Below the session information, there are tabs for 'Backup Info' and 'Recover Backup Info'. The 'Backup Info' tab is active, showing a summary: 'Total Number Backups: 10', 'Total Recoverable Backups: 6', and 'Total Unrecoverable Backups: 4'.

Backup Time	Backup ID	Recoverable	Copy Sets	Last Result	Blocking Expansion
2020-10-12 10:39:45 CEST	1602491985	No	16	✗ IWNR2830E	
2020-10-12 10:47:26 CEST	1602492446	No	16	✗ IWNR2830E	
2020-10-12 10:51:06 CEST	1602492666	No	16	✗ IWNR2830E	
2020-10-12 10:54:40 CEST	1602492880	No	16	✗ IWNR2830E	
2020-10-12 11:00:09 CEST	1602493209	Yes	16	✓ IWNR2800I	
2020-10-12 12:00:02 CEST	1602496802	Yes	16	✓ IWNR2800I	
2020-10-12 12:15:55 CEST	1602497755	Yes	16	✓ IWNR2800I	
2020-10-12 12:31:57 CEST	1602498717	Yes	16	✓ IWNR2800I	
2020-10-12 12:34:44 CEST	1602498884	Yes	16	✓ IWNR2800I	
2020-10-12 12:37:49 CEST	1602499069	Yes	16	✓ IWNR2800I	

Figure 4-36 Unrecoverable backups after a storage pool full condition

To manually expire a backup, complete the following steps:

1. In your CSM session, select **Session Actions** → **Commands** → **Expire Backup**. A new window opens. In this window, select the backup that you want to expire, as shown in Figure 4-37.

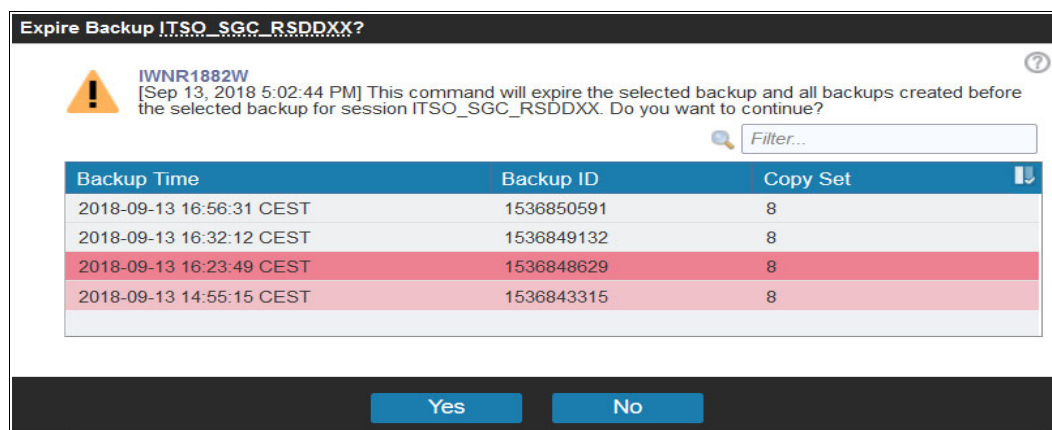


Figure 4-37 Manually expiring a backup

2. Carefully review the warning message IWNR1882W and decide which backup you want to expire. When you select a specific backup, this backup and all backups that were created before the selected backup expire.
3. Mark the backup that you want to expire and click **Yes** to continue. A new window displays. Click **Yes** to confirm your selection (see Figure 4-38).

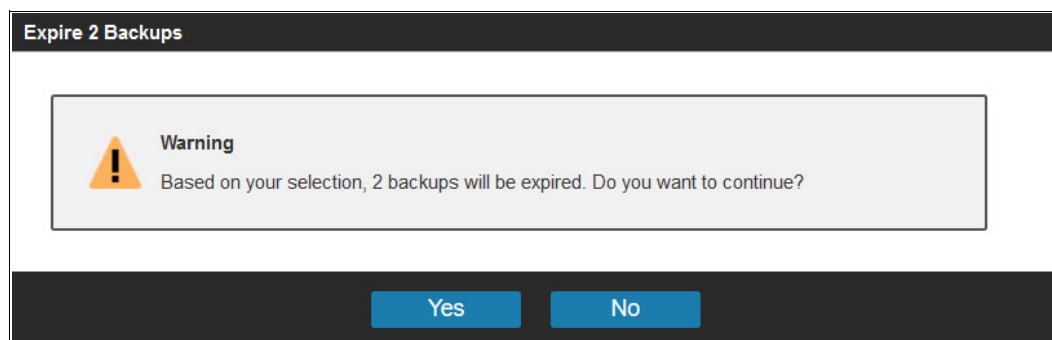


Figure 4-38 Expiring a backup confirmation window

After you expired the backups, the space of those backups is released back into the DS8000 storage pools.

Note: If the backup capacity runs out of space for a specific volume, the DS8000 expires the oldest backup of this volume to free up some extents. Therefore, this backup is no longer available for recovery (for more information, see 2.6, "Safeguarded Copy backup priority consideration in an out-of-space situation" on page 55).

4.2.4 Recovering a Safeguarded Copy backup

The key element of Safeguarded Copy is a fast data recovery if a logical corruption occurs, and regularly validating backup data without disrupting production workloads. The CSM Safeguarded Copy session provides this capability by using a recovery volume.

When you perform a Safeguarded Copy recovery action in CSM for a selected backup, CSM establishes a FlashCopy relationship between the Safeguarded Copy source volumes (H1) and the recovery volumes (R1), and merges the safeguarded data from the time of the selected Safeguarded Copy backup. After that process is complete, the R1 volumes contain the data from the timestamp of the recovered backup. After you issue the recovery action, you can access the recovery volume from an attached host to verify the data of the selected backup.

Note: Even during a recover action, users can continue to create Safeguarded Copy backups with CSM by clicking **Backup** or by creating a scheduled task.

To start a recovery, complete the following steps:

1. In your CSM Safeguarded Copy session, select **Sessions Action** → **Commands** → **Recover Backup**. A new window opens, in which you must select the backup that you want to recover from, as shown in Figure 4-39. In this window, only recoverable backups are listed.

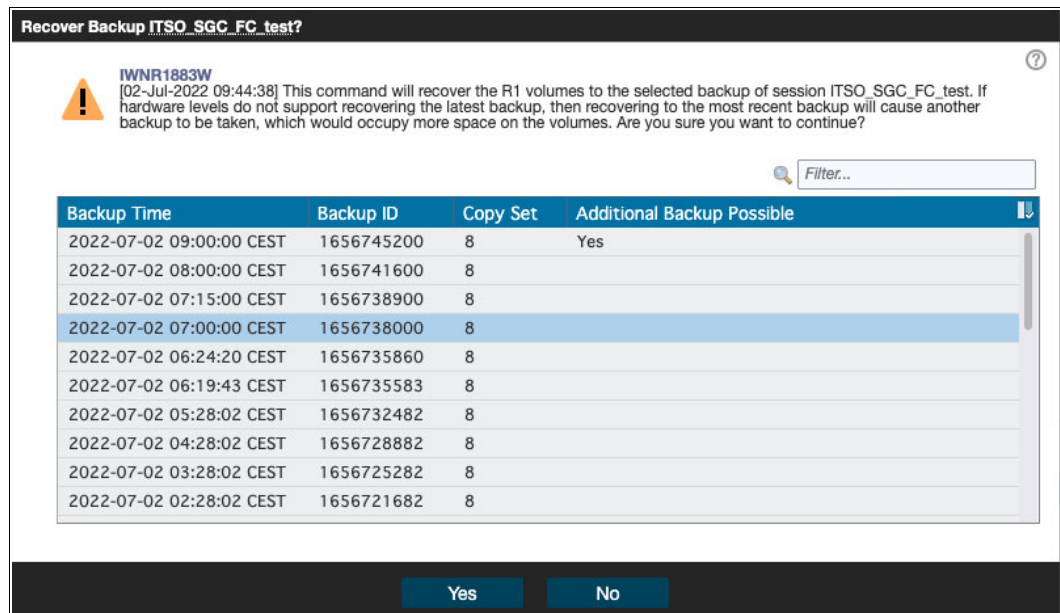


Figure 4-39 Safeguarded Copy session: Recover action

2. Mark the backup that you want to recover and click **Yes**.

Important: No confirmation window opens. A warning window displays if you select a backup that does not contain all of the volumes that are in the session.

3. If **Recover Backup** runs successfully, the session state changes from Protected to Target Available, the Last Recovered To display the selected backup time, and message IWNR1026I (at the top of the window) confirms successful command completion. More information about the recovered backup is found in the **Recover Backup Info** tab, as shown in Figure 4-40.

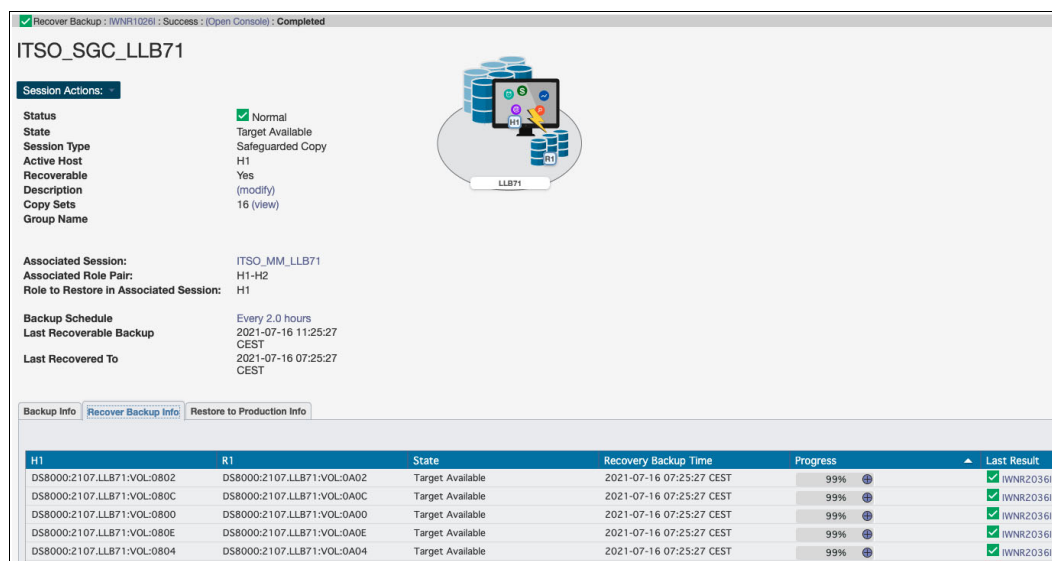


Figure 4-40 Safeguarded Copy Session Overview after a Recover action

The Last Recovered To information is available from CSM 6.3.0 and higher.

4. In the Recover Backup Info window, you can see for each copy set H1 - R1 that the Recovery Backup Time and the Progress bar show the background copy process if you started it.

After a successful **Recover Backup**, the following new Safeguarded Copy session actions are available in the **Session Actions** → **Commands** menu:

- **Initiate Background Copy**
- **Restore Backup**

If you need an independent recovery volume (for example, you need to analyze data for a longer period), you can click **Initiate Background Copy** in a CSM session to create a full copy. You also must have 100% of your recovery (R1) volume size as physical capacity available in your DS8000 system.

When you determine during your analysis that the data on the recovery volumes is unusable or from the incorrect period and you must recover another backup, you can again use **Recover Backup** in your CSM session for a different backup time.

The analysis of the backup data occurs on the recovery volumes. After you find the correct backup that is required to fix your logical corruption problem, you can restore the entire backup to your production volumes by clicking **Restore Backup** if the Safeguarded Copy was taken on DS8900 R9.2 and higher. This process is described in 4.3, “Restoring a Safeguarded Copy backup to production” on page 160.

After you complete all required actions on recovery volumes and you no longer need this data, click **TerminateH1R1** to remove the recovery relationship between the Safeguarded source volumes (H1) and the recovery volumes (R1), and release the space on the recovery volumes.

4.2.5 Expanding Safeguarded Virtual Capacity

Managing Safeguarded Virtual Capacity is critical to maintaining the recovery environment. Changes in the environment and in the backup and recovery requirements can affect the physical capacity that is needed to meet those demands.

Starting with microcode releases R8.5 SP7 and R9.1, the virtual capacity that is provisioned for a volume that is protected by Safeguarded Copy can be dynamically increased to allow for extra or more frequent backups by increasing the Backup Capacity Multiplier. This function allows the customer to expand the Safeguarded Copy Backup Capacity and provides queries to determine when they must expand their Safeguarded Copy Backup Capacity.

Note: Increasing Safeguarded Virtual Capacity can create a demand for more flash arrays to support the near term physical capacity requirements.

Expanding Safeguarded Virtual Capacity

The process to dynamically increase the current Backup Capacity Multiplier value for a volume or a range of volumes depends on the DS8000 platform that you are using. For DS8880 R8.5 SP7 or later, use the DS CLI interface to expand the volumes. For DS8900F R9.1 or later, use the Storage Management GUI or the DS CLI to expand the volumes.

Note: The Backup Capacity multiplier for any volume can be increased only from its current value. It cannot be decreased.

DS CLI

To expand a volume or range of volumes, use the **manageckdvol -action expandsafeguardedcap** command. For example, to increase the capacity multiplier to 3 for the volumes in the range 0010 - 0017, enter the command that is shown in Example 4-6.

Example 4-6 A dscli command to expand Safeguarded Virtual Capacity

```
dscli> manageckdvol -action expandsafeguardedcap -multiplier 3 0010-0017
Date/Time: October 8, 2020 6:29:30 PM CEST IBM DSCLI Version: 7.9.10.275 DS:
IBM.2107-75LAH81
CMUC00431I manageckdvol: The expandsafeguardedcap action for CKD volume 0010 has completed.
CMUC00431I manageckdvol: The expandsafeguardedcap action for CKD volume 0011 has completed.
CMUC00431I manageckdvol: The expandsafeguardedcap action for CKD volume 0012 has completed.
CMUC00431I manageckdvol: The expandsafeguardedcap action for CKD volume 0013 has completed.
CMUC00431I manageckdvol: The expandsafeguardedcap action for CKD volume 0014 has completed.
CMUC00431I manageckdvol: The expandsafeguardedcap action for CKD volume 0015 has completed.
CMUC00431I manageckdvol: The expandsafeguardedcap action for CKD volume 0016 has completed.
CMUC00431I manageckdvol: The expandsafeguardedcap action for CKD volume 0017 has completed.
```

Storage Management GUI

To increase a volume or a range of volumes with the Storage Management GUI, complete the following steps:

1. Select the suitable volume range on the DS8000, as shown in Figure 4-41.

<div> ⊕ Create CKD LSSs ⋮ Actions ▾ 🔍 Filter 📄 </div>							
Name	VOLSER	State	Capacity	↑	Safeguarded	Safeguarded Location	Safeguarded Virtual Capacity
ckd_ats_0010_0010	SGA110	✓ Normal	1.0 Mod1		✓	CKD_0	1.0 Mod1
ckd_ats_0011_0011	SGA111	✓ Normal	1.0 Mod1		✓	CKD_0	1.0 Mod1
ckd_ats_0012_0012	SGA112	✓ Normal	1.0 Mod1		✓	CKD_0	1.0 Mod1
ckd_ats_0013_0013	SGA113	✓ Normal	1.0 Mod1		✓	CKD_0	1.0 Mod1
ckd_ats_0014_0014	SGA114	✓ Normal	1.0 Mod1		✓	CKD_0	1.0 Mod1
ckd_ats_0015_0015	SGA115	✓ Normal	1.0 Mod1		✓	CKD_0	1.0 Mod1
ckd_ats_0016_0016	SGA116	✓ Normal	1.0 Mod1		✓	CKD_0	1.0 Mod1
ckd_ats_0017_0017	SGA117	✓ Normal	1.0 Mod1		✓	CKD_0	1.0 Mod1

Figure 4-41 Selecting the volume range for expansion

2. Select **Actions** → **Safeguarded** → **Expand Capacity** to open the Expand Safeguarded Virtual Capacity window (see Figure 4-42).

Expand Safeguarded Virtual Capacity

CKD

8 Volumes

Expand the safeguarded virtual capacity for the volumes by entering a new backup capacity multiplier value that reflects the requirements of your Safeguarded Copy policy.

Backup location:

CKD_0

Backup capacity multiplier(*):

3

24.00 Mod1

Pool usable capacity

11.67 KMod1

System provisioned capacity

70.86 TiB

?

Need Help

Expand

Cancel

Figure 4-42 Expand Safeguarded Virtual Capacity

3. You can now increase the multiplier value to the required number (3 in our example) and click **Expand** to continue. The message that is shown in Figure 4-43 appears. Click **Yes** to continue.

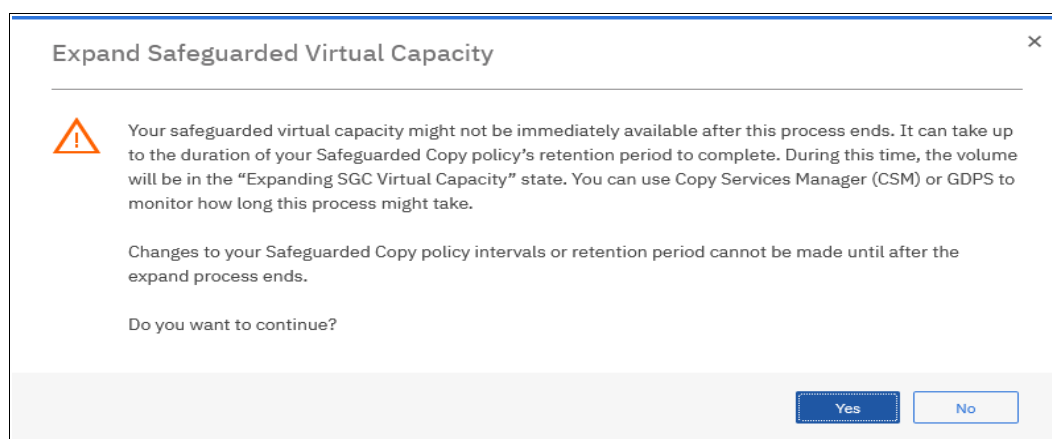


Figure 4-43 Expand Safeguarded Virtual Capacity message window

As indicated in this message, the progress of the expansion is monitored in the suitable CSM session or GDPS Logical Corruption Protection Manager. Also, the expansion can take some time until the retention period is over.

Figure 4-44 shows an example of the DS8000 Storage Management GUI status for the affected volumes during this process.

<div> <div>Create CKD LSSs</div> <div> <div>Actions</div> <div>Filter</div> <div></div> </div> </div> <div>1 LSS sel</div>						
Name	VOLSER	State	Capacity	Safeguarded	Safeguarded Location	Safeguarded Virtual Capacity
ckd_ats_000D_000D	SGA10D	✓ Normal	27.0 Mod1	✓	CKD_0	81.0 Mod1
ckd_ats_000E_000E	SGA10E	✓ Normal	27.0 Mod1	✓	CKD_0	81.0 Mod1
ckd_ats_000F_000F	SGA10F	✓ Normal	27.0 Mod1	✓	CKD_0	81.0 Mod1
ckd_ats_0010_0010	SGA110	✓ Safeguarded backup capacity expanding	1.0 Mod1	✓	CKD_0	3.0 Mod1
ckd_ats_0011_0011	SGA111	✓ Safeguarded backup capacity expanding	1.0 Mod1	✓	CKD_0	3.0 Mod1
ckd_ats_0012_0012	SGA112	✓ Safeguarded backup capacity expanding	1.0 Mod1	✓	CKD_0	3.0 Mod1
ckd_ats_0013_0013	SGA113	✓ Safeguarded backup capacity expanding	1.0 Mod1	✓	CKD_0	3.0 Mod1
ckd_ats_0014_0014	SGA114	✓ Safeguarded backup capacity expanding	1.0 Mod1	✓	CKD_0	3.0 Mod1
ckd_ats_0015_0015	SGA115	✓ Safeguarded backup capacity expanding	1.0 Mod1	✓	CKD_0	3.0 Mod1
ckd_ats_0016_0016	SGA116	✓ Safeguarded backup capacity expanding	1.0 Mod1	✓	CKD_0	3.0 Mod1
ckd_ats_0017_0017	SGA117	✓ Safeguarded backup capacity expanding	1.0 Mod1	✓	CKD_0	3.0 Mod1

Figure 4-44 Safeguarded Virtual Capacity Expansion Status on a DS8000

After the process completes, you return to the Preferred Volumes view on the DS8900F to validate that the expansion completed successfully.

4.2.6 Other Safeguarded Copy-related Copy Services Manager operations

In addition to the creation, expiration, recovery, and restore backup functions of a Safeguarded Copy session, other operations are available, such as:

- ▶ Adding copy sets
- ▶ Removing copy sets

Adding copy sets

During the lifetime of a CSM session, it is normal that you add copy sets; for example, if capacity is added to a system and new volumes must be protected.

To add copy sets in a CSM Safeguarded Copy session, complete the following steps:

1. Open your session by clicking the session name in the Sessions window.
2. Click **Session Actions**, select **View/Modify**, and then select **Add Copy Sets**.
3. The Add Copy Sets wizard opens. Here, you must specify the H1 and the R1 volumes or import a CSV file as you might do when you create the session (see Figure 4-10 on page 127).

In an active Safeguarded Copy session, the status changes to Warning after you add copy sets, and you notice that now more copy sets are in the session as in the recoverable backups, as shown in Figure 4-45.

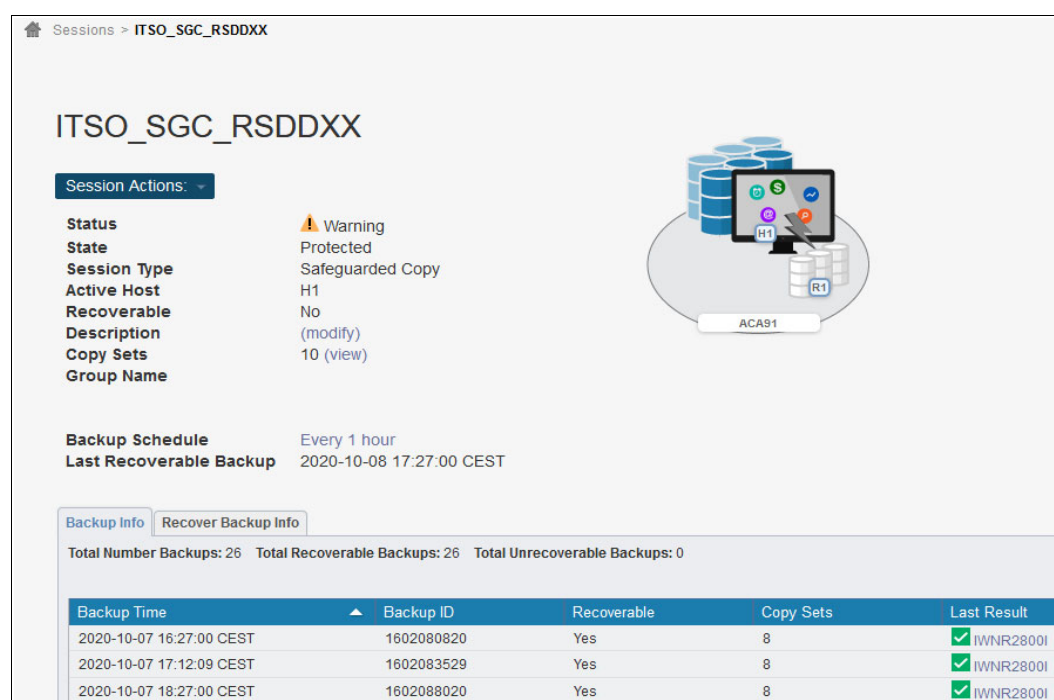


Figure 4-45 Session overview after a new copy set was added

The status changes back to Normal after you created two backups that include the new copy sets.

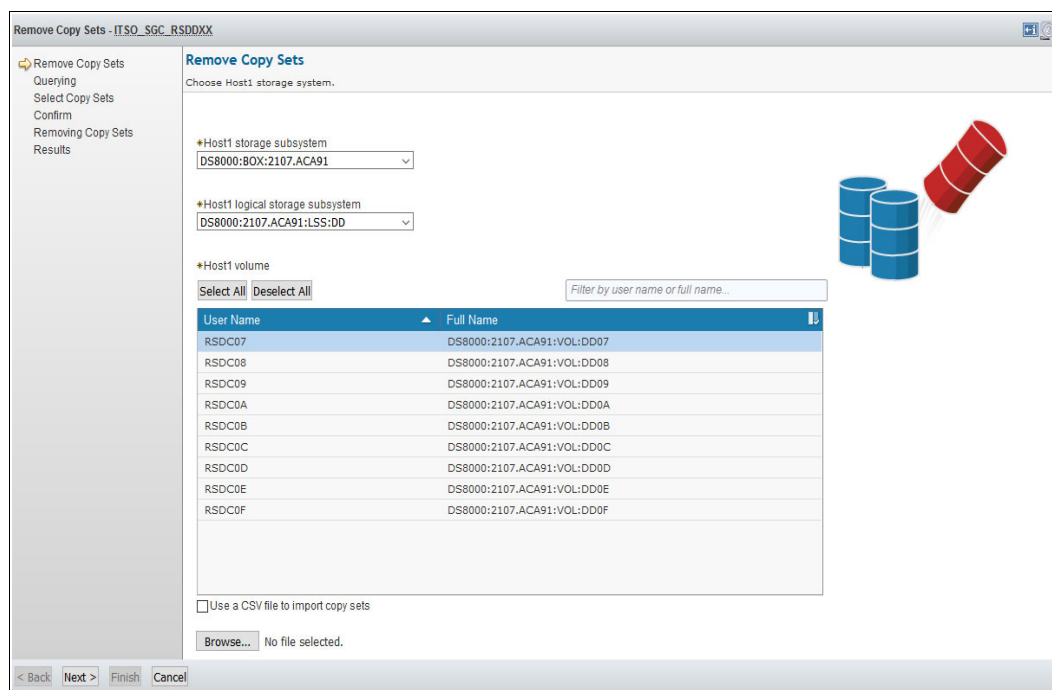
Removing copy sets

Under some circumstances, it might be necessary to remove copy sets from a Safeguarded Copy session. Removing copy sets is a more critical action than adding them. Carefully consider how to do so because you might remove volumes that contain data that is required in a recovery action.

You also must take care that no relevant data exists on the source (H1) volumes of those copy sets. Otherwise, you might lose your logical corruption protection (LCP).

To remove copy sets in a CSM Safeguarded Copy session, complete the following steps:

1. Open your session by clicking the session name in the Sessions window.
2. Click **Session Actions**, select **View/Modify**, and then select **Remove Copy Sets**.
3. The Remove Copy Sets wizard opens. Here, select the H1 volumes that you want to remove, as shown in Figure 4-46.



Remove Copy Sets - ITSO_SGC_RSDDXX

Remove Copy Sets

Choose Host1 storage system.

*Host1 storage subsystem
DS8000:BOX:2107.ACA91

*Host1 logical storage subsystem
DS8000:2107.ACA91:LSS:DD

*Host1 volume

Select All Deselect All

Filter by user name or full name...

User Name	Full Name
RSDC07	DS8000:2107.ACA91:VOL:DD07
RSDC08	DS8000:2107.ACA91:VOL:DD08
RSDC09	DS8000:2107.ACA91:VOL:DD09
RSDC0A	DS8000:2107.ACA91:VOL:DD0A
RSDC0B	DS8000:2107.ACA91:VOL:DD0B
RSDC0C	DS8000:2107.ACA91:VOL:DD0C
RSDC0D	DS8000:2107.ACA91:VOL:DD0D
RSDC0E	DS8000:2107.ACA91:VOL:DD0E
RSDC0F	DS8000:2107.ACA91:VOL:DD0F

☐ Use a CSV file to import copy sets

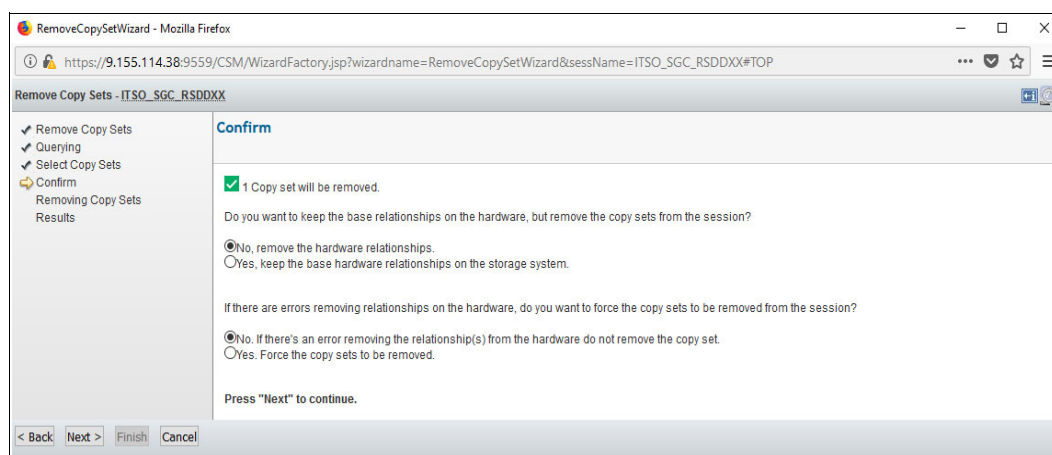
Browse... No file selected.

< Back Next > Finish Cancel

Figure 4-46 CSM Remove Copy Sets wizard

4. Click **Next** twice. In the Confirm window, you can decide whether you want to keep the hardware relationship on the storage system or not, as shown in Figure 4-47.

After the copy sets are removed, the session stays in the Normal status and the Protected state. Only the number of copy sets that are included in the available backups is reduced by the number of removed copy sets.



RemoveCopySetWizard - Mozilla Firefox

https://9.155.114.38:9559/CSM/WizardFactory.jsp?wizardname=RemoveCopySetWizard&sessName=ITSO_SGC_RSDDXX#TOP

Remove Copy Sets - ITSO_SGC_RSDDXX

Remove Copy Sets

Confirm

1 Copy set will be removed.

Do you want to keep the base relationships on the hardware, but remove the copy sets from the session?

☒ No, remove the hardware relationships.
☐ Yes, keep the base hardware relationships on the storage system.

If there are errors removing relationships on the hardware, do you want to force the copy sets to be removed from the session?

☒ No. If there's an error removing the relationship(s) from the hardware do not remove the copy set.
☐ Yes. Force the copy sets to be removed.

Press "Next" to continue.

< Back Next > Finish Cancel

Figure 4-47 CSM removes a copy set: Confirm window

Note: If you do not keep the hardware relationship during the copy set removal process, you must take care that no relevant data exists on those volumes for a full retention period before you remove the copy sets so that you can ensure that no relevant data exists on any of the formerly created backups.

5. If you select to keep the hardware relationships for the copy sets that you remove, the DS8000 maintains the backups for the H1 volumes of the removed copy sets. New backups for the session do not contain these volumes.

Such copy sets can be assimilated back into the session. To do so, add the copy sets to the session again and click **Refresh State**. CSM checks the timestamps and backup IDs of the backups and adapts the recoverable backups. Consider the following points:

- Backups that were made before the copy sets were removed contain all copy sets.
- Backups that were made after the copy sets were removed contain fewer copy sets.

Other use cases for keeping the hardware relationship include the following examples:

- Add the copy sets to a separate session to treat them separately; for example, to perform a recovery action for those volumes only.
- Assimilate volumes with Safeguarded Copy backups in to another session. This method is used to replace the recovery volumes of a session with different volumes.

6. After adding these volumes to a session, trigger the assimilation by selecting **Session Actions** → **Refresh States**.

Note: Be careful if you have volumes in more than one Safeguarded Copy session. If you terminate one of these sessions, you lose the Safeguarded Copy backups for the volumes in that session.

Displaying the volumes of a Safeguarded Copy backup

If you want to know which volumes are included in a specific Safeguarded Copy backup, click **Backup Time** in your Safeguarded Copy backup Info. A window opens that shows all volumes in this backup (see Figure 4-48).

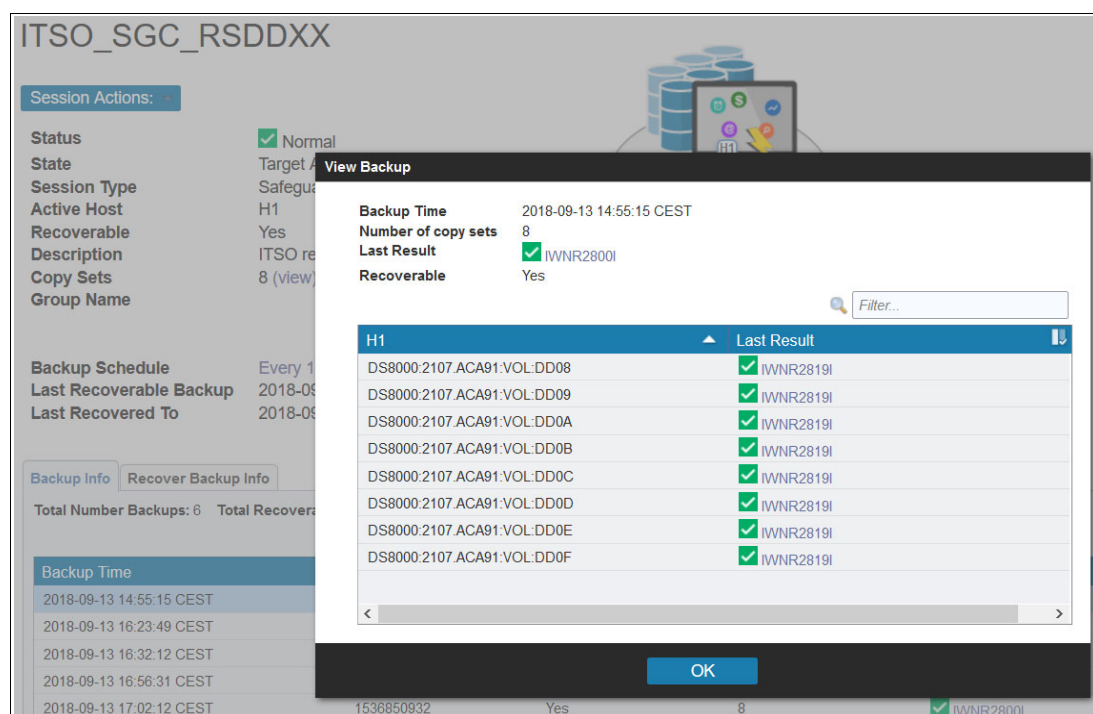


Figure 4-48 Displaying volumes that are included in a backup

Terminating a Safeguarded Copy session

If you no longer need data protection for a specific CSM Safeguarded Copy session, you can terminate your session by completing the following steps:

1. Open your session by clicking the session name in the Sessions window.
2. Click the **Session Actions** and select **Terminate**.
3. A warning message opens. Click **Yes** to confirm your action, as shown in Figure 4-49.

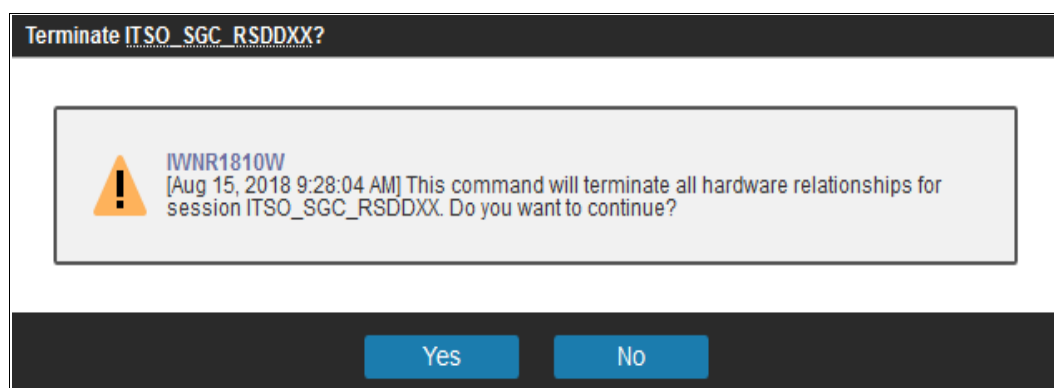


Figure 4-49 CSM Terminate session

The session status changes to *Inactive* and the DS8000 releases the Backup Capacity of the Safeguarded Copy source volumes. Your backups are now deleted.

Safeguarded Copy session associations

Usually, volumes that are protected with Safeguarded Copy are in other CS relationships, such as MM, GM, or in any other combination of both, which provides a 2-, 3-, or even a 4-site HADR solution.

Adding and removing copy sets must be done in all associated sessions to maintain data protection and HADR integrity. For example, when adding volumes (copy sets) in an MM session, you also must add the associated volumes in a Safeguarded Copy session. It can be challenging in a large CSM environment with many sessions to remember all the necessary changes.

With CSM 6.2.12 and later, a Safeguarded Copy session can be associated with another session. The following common use cases are available when Safeguarded Copy session association is used:

- Restore a backup to a production volume.

A Safeguarded Copy session must be associated to another replication session with its volumes being protected by this Safeguarded Copy session. For more information about how to restore a backup to a production volume, including how to create a session association, see 4.3, “Restoring a Safeguarded Copy backup to production” on page 160.

- To be alerted when volumes or copy sets are added to an associated session.

When a Safeguarded Copy session is associated to another session, every time a new copy set is added to the associated session, both sessions change to the Warning state, and the message alerts are logged to the CSM console.

To set up session associations, follow steps 1 on page 162 and 2 on page 162 in 4.3.1, “Restoring a backup to production from H2 in an MM session” on page 162.

In our example, we removed one copy set from the ITSO_MM_LL70 MM session, which is associated with the ITSO_SGC_LL70 Safeguarded Copy session. When the copy set is removed, both sessions changed to the Warning status, as shown in Figure 4-50 for our MM session and in Figure 4-51 for our Safeguarded Copy session.

The same IWN6047W message is logged in the CSM console.

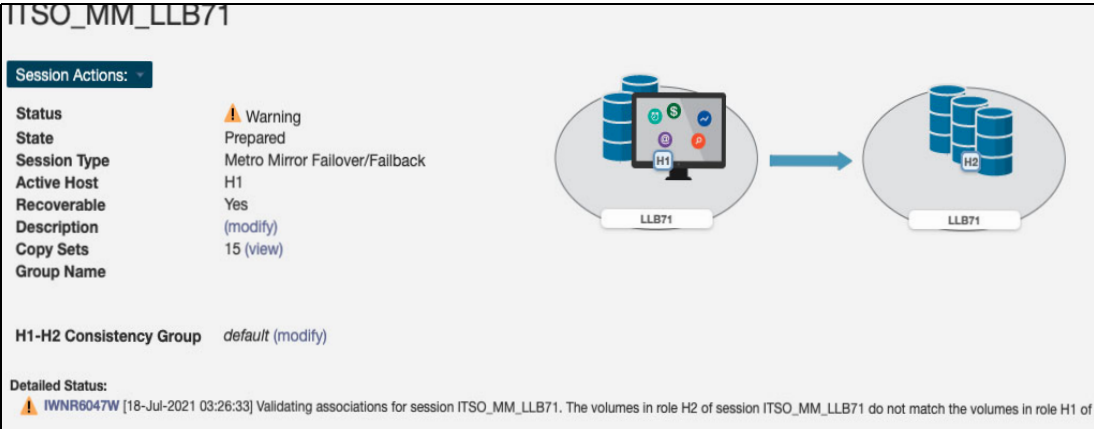


Figure 4-50 IWN6047W warning message for validation association for an MM session

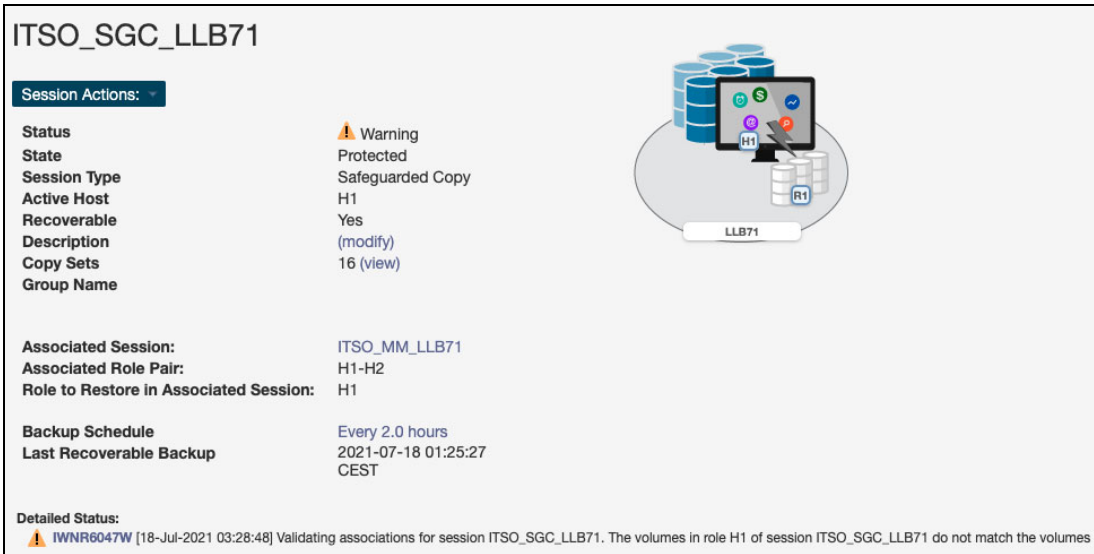


Figure 4-51 IWN6047W warning message for a validation association Safeguarded Copy session

Both sessions return to the Normal status when all volumes in the associated roles match in both sessions.

4.2.7 Other Safeguarded Copy-related DS CLI and DS GUI operations

By using the DS CLI or the DS GUI, you can migrate or delete the backup capacity of a production volume.

Migrating backup capacity

If a storage pool out-of-space issue occurs, you might want to migrate the backup capacity to another storage pool.

Complete the following steps by using the Storage Management GUI:

1. Open the Volumes window.
2. Select a specific volume or a range of volumes, and then select **Actions** → **Safeguarded**.
3. Select **Migrate Capacity**, and then click **Start**.
4. A new window opens in which you can select the new pool from the menu. Click **Migrate** to start the migration of the backup capacity.

Alternatively, you can run the DS CLI `manageckdvol` or `managefbvol` command with the parameter `-action migsafeguardcap`. In our example, we migrate the Backup Capacity for one production volume (DD0A) from storage pool p9 to storage pool p17, as shown in Example 4-7.

Example 4-7 DS CLI migrate backup capacity

Before the migration:

```
dsccli> lsckdvol -l DD0A
Name      ID      accstate  datastate  configstate  deviceMTM  volser  datatype  voltype  orgbvols  extpool  sam  cap (cyl)  cap (10^9B)  cap (2^30B)
reqcap (cyl) eam      pergrp  resgrp  safeguardedcap (cyl) safeguardedloc
=====
ckd_p9_DD0A DD0A Online   Normal    Normal    3390-9   RSDCOA 3390   CKD Base -    P9     ESE     10017      8.5      7.9
10017 managed PGO      RGO      10017                P9
```

```
dsccli> manageckdvol -action migsafeguardedcap -extpool p17 DD0A-DD0F
CMUC00431I manageckdvol: The migsafeguardedcap action for CKD volume DD0A has completed.
```

After the migration:

```
dsccli> lsckdvol -l DD0A-DD0F
Name      ID      accstate  datastate  configstate  deviceMTM  volser  datatype  voltype  orgbvols  extpool  sam  cap (cyl)  cap (10^9B)  cap (2^30B)
reqcap (cyl) eam      pergrp  resgrp  safeguardedcap (cyl) safeguardedloc
=====
ckd_p9_DD0A DD0A Online   Normal    Normal    3390-9   RSDCOA 3390   CKD Base -    P9     ESE     10017      8.5      7.9
10017 managed PGO      RGO      10017                P17
```

In our example, we run the `lsckdvol -l` command to show the volume status before and after the migration. You see that for this volume, the Safeguarded Copy backup location changed from storage pool p9 to p17. If required, you can pause, resume, or cancel an ongoing migration by using the DS CLI or Storage Management GUI.

Deleting backup capacity

If the volumes do not need to be protected, such as when the volumes are no longer used in a production environment, you can delete the backup capacity if no Safeguarded Copy backups exist for those volumes.

Another example is if you must decrease the Safeguarded Virtual Capacity because the retention period is reduced or the virtual capacity limit of the DS8000 system was reached.

By using the Storage Management GUI or the DS CLI, you can delete the backup capacity of a production volume only if it is *not* safeguarded.

To delete a backup capacity with the Storage Management GUI, complete the following steps:

1. Open the Volumes window.
2. Select a specific volume or a range of volumes, and then select **Actions** → **Safeguarded**.
3. Select **Delete Capacity** and confirm by clicking **Yes** after you read the warning message.

With the command-line interface (CLI), you again run the `manageckdvol` or `managefbvol` command to delete the backup capacity, now with the parameter `-action rmsafeguardedcap`. In our example, two volumes exist: one is safeguarded (DD08), and the other (DD07) is not (see Example 4-8).

Example 4-8 DS CLI deleting backup capacity

Volume status before deletion:

```
dsccli> lsckdvol -l DD07-DD08
```

Name	ID	accstate	datastate	configstate	deviceMTM	volser	datatype	voltype	orgbvols	extpool	sam	cap (cyl)	cap (10^9B)	cap (2^30B)
reqcap (cyl)	eam	perfgrp	resgrp	safeguardedcap (cyl)	safeguardedloc									
ckd_p9_DD07	DD07	Online	Normal	Normal	3390-9	RSDC07	3390	CKD Base -	P9	ESE	10017	8.5	7.9	
10017 managed	PG0	RG0	10017		P17		0		no					
ckd_p9_DD08	DD08	Online	Normal	Normal	3390-9	RSDC08	3390	CKD Base -	P9	ESE	10017	8.5	7.9	
10017 managed	PG0	RG0	10017		P17									

Try to delete Backup Capacity for a volume that is safeguarded:

```
dsccli> manageckdvol -action rmsafeguardedcap DD08
```

CMUC00569W manageckdvol: Are you sure you want to delete the backup capacity for CKD volume DD08? [y/n]: y

CMUN02947E manageckdvol: DD08: The Delete logical volume task cannot be initiated because the Allow Host Pre-check Control Switch is set to true and the volume that you have specified is in a Copy Services relationship.

Try to delete Backup Capacity for a volume that is not safeguarded:

```
dsccli> manageckdvol -action rmsafeguardedcap DD07
```

CMUC00569W manageckdvol: Are you sure you want to delete the backup capacity for CKD volume DD07? [y/n]: y

CMUC00571I manageckdvol: Backup capacity for CKD volume DD07 is successfully deleted.

Volume status after successfully deletion of the Backup Capacity for volume DD07:

```
dsccli> lsckdvol -l DD07-DD08
```

Name	ID	accstate	datastate	configstate	deviceMTM	volser	datatype	voltype	orgbvols	extpool	sam	cap (cyl)	cap (10^9B)	cap (2^30B)
reqcap (cyl)	eam	perfgrp	resgrp	safeguardedcap (cyl)	safeguardedloc									
ckd_p9_DD07	DD07	Online	Normal	Normal	3390-9	RSDC07	3390	CKD Base -	P9	ESE	10017	8.5	7.9	
10017 managed	PG0	RG0	-		-									
ckd_p9_DD08	DD08	Online	Normal	Normal	3390-9	RSDC08	3390	CKD Base -	P9	ESE	10017	8.5	7.9	
10017 managed	PG0	RG0	10017		P17									

The safeguarded state must be No; otherwise, you cannot delete the backup capacity. You must expire all backups in your CSM Safeguarded Copy session before you can delete the Safeguarded Copy Backup Capacity.

4.3 Restoring a Safeguarded Copy backup to production

In a catastrophic cyberattack against production data, restoring recovered backup data (after validation) to the production volumes is possible by clicking **Restore Backup**. This command is supported if the Safeguarded Copy source volume is in a replication relationship, such as MM, GM, GC, or a combination of these items. Clicking **Restore Backup** restores the recovered backup directly to the production volumes by copying only incremental changes.

Note: Restore Backup is supported on DS8900 R9.2 and later and with CSM 6.3.0 and later.

The production volumes, where the backup is restored to, can be on any DS8880 and DS8900 microcode release.

If Safeguarded Copy runs on any DS8880 supported microcode release, you must use a separate Global Copy session from recovery volumes to production volume with full copy.

To start the process of restoring a backup to a production volume, the Safeguarded Copy session must feature an association to a CSM replication session to where you want to restore Safeguarded Copy backup data.

Moreover, the associated MM or GM session must be suspended before you click **Restore Backup**.

Important: Consider the following points:

- ▶ Make sure you validate carefully your recovered backup data before you click **Restore Backup**.
Furthermore, in a two site DR scenario (with MM or GM replication), you must shut down your production applications before you click **Restore Backup**.
- ▶ Restore backup to production volumes process is identical for all Safeguarded Copy topologies with exception to restoring backup to cascaded volumes in any cascaded CS topology, such as Metro/Global Mirror (MGM) or the cascaded GM. Another step is required when restoring backup to cascaded volumes being part of any 3-Site or 4-Site topology. For more information about restore backup to cascaded volumes, see “Restoring a backup to production from H3 in cascaded GM sessions” on page 176.
- ▶ Disable Safeguarded Copy scheduled task for the session to which you are about to initiate a restore to avoid extra Safeguarded Copy backups.

In the following sections, we provide examples how to restore Safeguarded Copy backup to a production volume:

- ▶ 4.3.1, “Restoring a backup to production from H2 in an MM session” on page 162
- ▶ 4.3.2, “Restoring a backup to production from H3 in an MGM session” on page 168
- ▶ 4.3.3, “Restoring a backup to production from H3 in cascaded GM sessions” on page 176
- ▶ 4.3.4, “Restoring a backup to production from H1 in an MM session” on page 187
- ▶ 4.3.5, “Restoring a backup to production from H1 in a Multi-Target Metro/Global Mirror session” on page 198

Restore backup to a production volume was tested in different Safeguarded Copy topologies. For more information about tested topologies, see 2.10.4, “Catastrophic recovery” on page 73.

4.3.1 Restoring a backup to production from H2 in an MM session

The steps that are described in this section are applicable for restoring a Safeguarded Copy backup from the secondary volume (H2) to the production volume (H1) in an MM topology / session.

In this example, we use the following sessions:

- ▶ ITS0_MM_LL71 production MM session:
 - H1 primary volumes
 - H2 Secondary volumes
- ▶ ITS0_SGC_LL71 Safeguarded Copy session:
 - H1 Safeguarded Copy source volume, but also H2 MM secondary volumes that are defined in ITS0_MM_LL71
 - R1 Recovery volumes

Complete the following steps:

1. Create a Safeguarded copy session association with MM session by selecting **View/Modify** → **Session Associations** → **Add/Update Association**, as shown in Figure 4-52.

Note: The association of the Safeguarded Copy session with the corresponding replication session can be done anytime before starting the restore to production process. However, the best practice is to create the association during the process of configuring the Safeguarded Copy session.

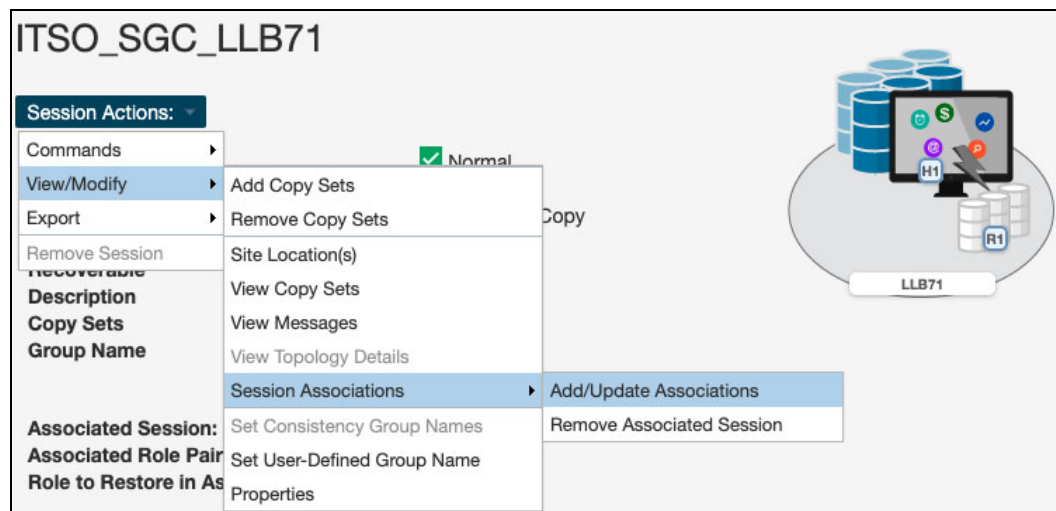


Figure 4-52 Creating a Safeguarded Copy session association

2. In Figure 4-53 on page 163, select the session that you want to associate to this Safeguarded copy session. Also, specify the session volumes role pair and specific volume role.

Use the filter to narrow the list of sessions. In our example, we associated the MM session ITS0_MM_LL7 and selected the **H1-H2** Role Pair.

Note: H1-H2 is the only available Role Pair option for two site (MM or GM) topology. In 3- or 4-site topologies, more Role Pair options are available.

- Choose which of the previously selected role pair volumes will be defined as Safeguarded Copy source volumes. Because the Safeguarded Copy in our example is taken from the MM secondary volume, the answer to “Which role in the selected role pair is the H1 volume in the Safeguarded Copy session?” is H2.

The role selection in our example for the last question “Which role in the selected role pair do you want to restore from a Safeguarded backup?” is H1 because you cannot Restore Backup to the Safeguarded Copy source volume (see Figure 4-53).

Associate a session to this Safeguarded Copy session

By Associating a session to this Safeguarded Copy session, the server will validate that the H1 volumes in this session are always the same as the associated session.

Which session should be associated to this Safeguarded Copy session?

Show All

Name	Type
ITSO_MM_ACA91_LLB71	MM
ITSO_MM_LLB71	MM

Which role pair in the session selected above should be associated to the session?

Role Pair:

Which role in the selected role pair is the H1 volume in the Safeguarded Copy session?

Role:

Which role in the selected role pair do you want to restore from a Safeguarded backup?

Role:

OK Cancel

Figure 4-53 Associate a session to this Safeguarded Copy session

- Start backup recovery to the recovery volumes. From the Safeguarded Copy **Session Actions** menu, select **Commands**, and then click **Recover Backup**, as shown in Figure 4-54.

ITSO_SGC_LLB71

Session Actions:

- Commands
 - Backup
 - Expire Backup
 - Recover Backup
 - Refresh States
 - Terminate
 - TerminateH1R1
- View/Modify
- Export
- Remove Session
- Recover Backup
- Description
- Copy Sets
- Group Name

LLB71

Figure 4-54 Recover Backup

- The new window includes a list of all available backup versions. Select the required backup and click **Yes** to start the backup recovery to the recovery volumes (see Figure 4-55).

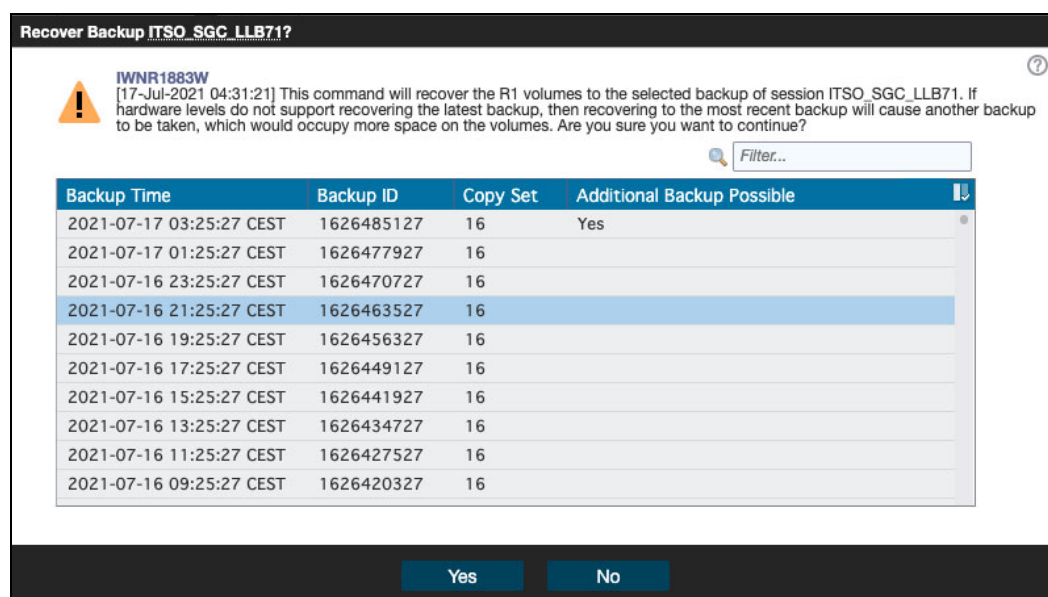


Figure 4-55 Selecting the required backup version

- Wait for the IWN1026I message, which indicates that **Recover Backup** completed successfully (see Figure 4-56).

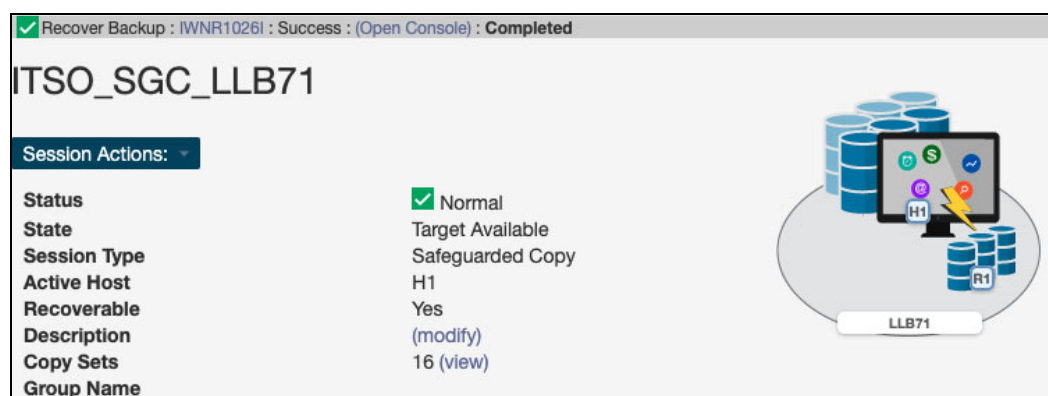


Figure 4-56 Recover Backup completed

At this stage, you can start validating data from the recovery system. If the data in this backup version is still corrupted, you can end the H1-R1 relationship (click **Terminate H1-R1**) and recover another backup version (starting at step 3 on page 163).

Important: Before proceeding to the next step, continue validating backup versions until you find the version that is not corrupted. Ensure that your production applications are not running (no I/Os to production volumes) before you click **Restore Backup**, as described in the next steps.

Also, all changes that are made during the validation process on recovery volumes are lost and not restored to production volumes.

- In the CSM Sessions window, select the associated replication session. In our example that is shown in Figure 4-57, we used the ITS0_MM_LL71 MM session.

Select **Session Actions** → **Commands** → **Suspend**.

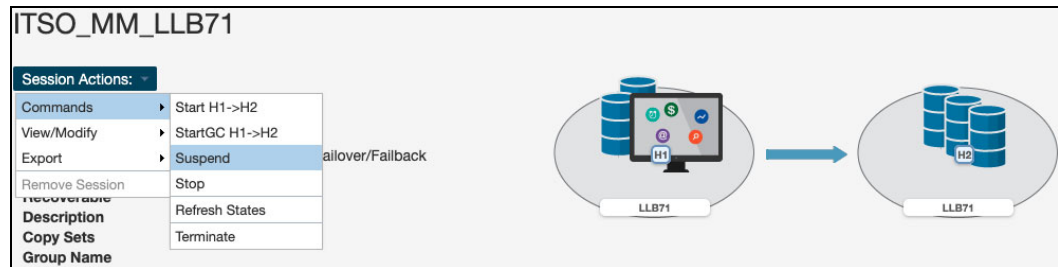


Figure 4-57 Suspending the associated session

- Click **Yes** to continue (see Figure 4-58).

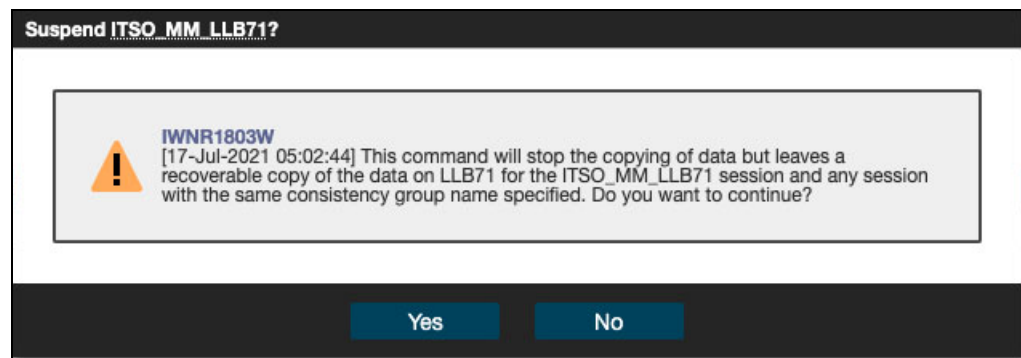


Figure 4-58 Confirming the Suspend command

- Return to the Safeguarded Copy session. In our example, the session is ITS0_SGC_LL71. Select **Session Actions** → **Restore Backup** (see Figure 4-59).

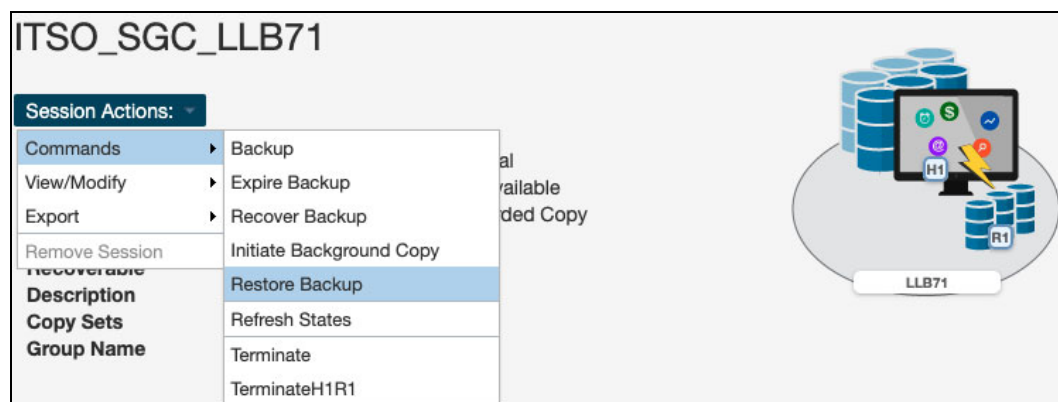


Figure 4-59 Safeguarded Copy Restore Backup command

10. A confirmation window opens. Click **Yes** to continue (see Figure 4-60).

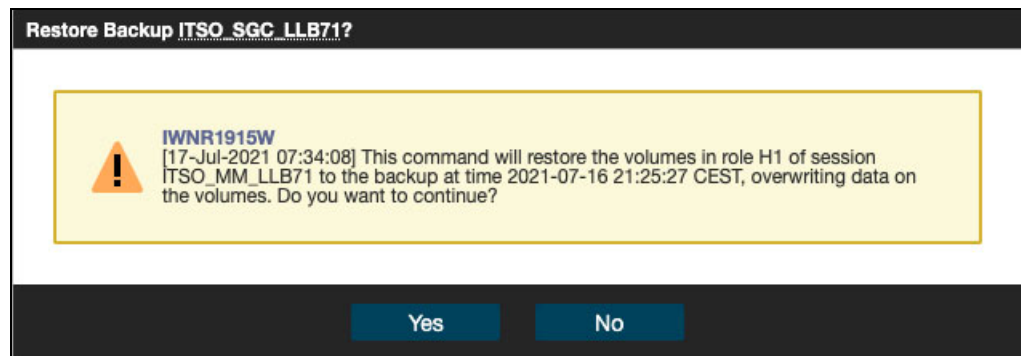


Figure 4-60 Confirming Restore Backup

11. The Safeguarded Copy session State changes to Restoring. In the Detailed Status section, you can monitor the restore progress, as shown in Figure 4-61.

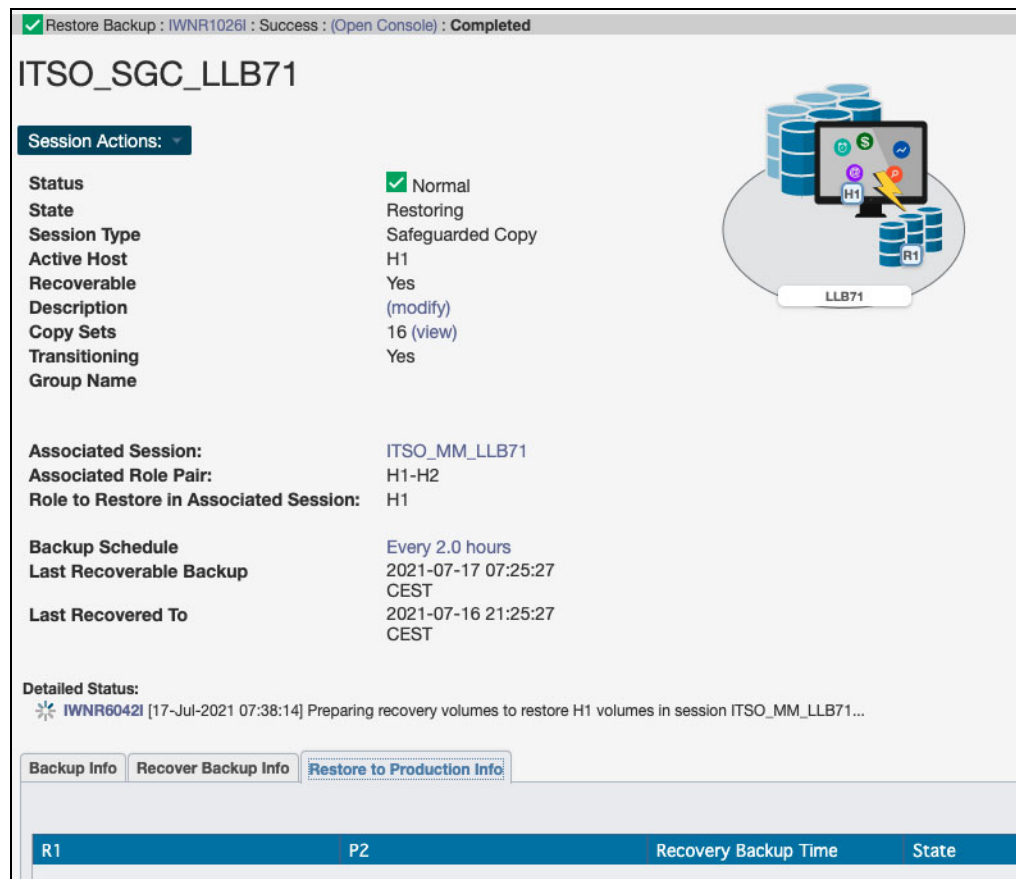


Figure 4-61 Restore Backup completed

The backup data is now being replicated from the recovery volumes R1 to the production MM primary volumes H1. This process is done with Global Copy incremental resync, so only changed tracks for this backup version are sent to the production volumes.

After the backup is restored to the production volumes, the Safeguarded Copy session changes to Protected state.

As you can see in Figure 4-62, the H1-R1 relationship was automatically removed.

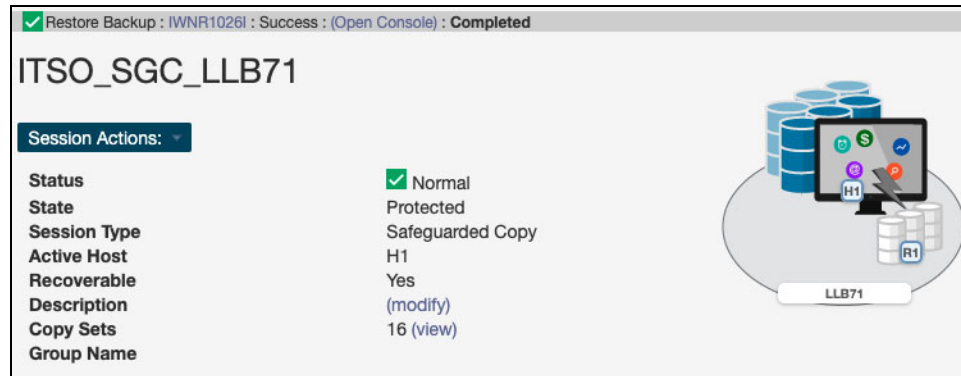


Figure 4-62 Restore Backup to production volumes completed

12. After the restore to production of MM primary volumes is completed, the ITSO_MM_LLB71 MM session (which was in Suspended state before the **Restore Backup** action) changes to the Target Available state (see Figure 4-63).

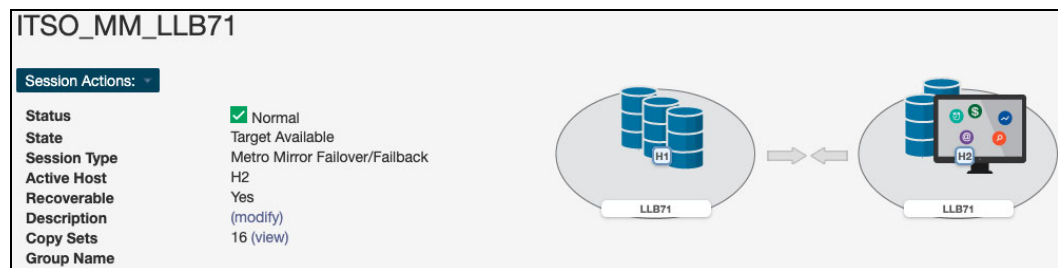


Figure 4-63 Target Available State for the Metro Mirror session

13. Click **Start H1-H2** to restore HADR protection. This command starts an incremental resync unless all backup data was changed.

Note: Before you click **Start H1-H2**, consider the following extra steps:

1. Perform an IPL from the H1 volumes and validate the environment another time before clicking **Start H1-H2**.
2. All tracks that were restored from R1 to H1 will be resynchronized from H1 to H2 and will be stored in your open Safeguarded Copy backup. This process might use significant extra capacity. Depending on your requirements, you might expire all Safeguarded Copy copies and stop Safeguarded Copy before you click **Start H1-H2**.

4.3.2 Restoring a backup to production from H3 in an MGM session

The steps that are described in this section are applicable for restoring a Safeguarded Copy backup from the tertiary volume (H3) to the production volume (H1) in an MGM topology or session.

In this example, we use the following sessions:

- ▶ ITS0_MGM_ACA91_LAH81 - production MGM session:
 - H1 primary MM volumes: Production volumes.
 - H2 Secondary MM volumes are cascaded; therefore, they are also primary GM volumes.
 - H3 GM secondary volumes are also the H1 volumes in the Safeguarded Copy Session.
- ▶ ITS0_SGC_H3_LAH81 - Safeguarded Copy session:
 - H1 Safeguarded Copy source volume, but also H3 GM Secondary volumes that are defined in the ITS0_MGM_ACA91.
 - R1 Recovery volumes.

Before we show each step in detail, here is a summary of the required steps to restore a backup to production from tertiary volumes in an MGM session:

1. Associate the Safeguarded Copy session with the MGM session to be restored.
2. If you established a Scheduled Task for the session that you want to initiate a restore, you might disable this task to avoid extra Safeguarded Copy backups.
3. Click **Recover Backup** and select the required backup.
4. Perform data analysis on the recovery system.
5. Stop production applications (if not already done).
6. Suspend the associated MGM session (the whole session).
7. Start H1-H3 in an MGM session.
8. Suspend the associated MGM session.
9. Click **Restore Backup** from the Safeguarded Copy session.
10. Click **Start H1>H2>H3** from the MGM session.

To restore the R1 volumes to the H1 production MM primary volumes, complete the following steps:

1. Create a Safeguarded Copy session association by selecting **View/Modify** → **Session Associations** → **Add/Update Association**, as shown in Figure 4-64 on page 169.

Note: The association of the Safeguarded Copy session with the corresponding replication session can be done anytime before starting the restore to production process. However, a best practice is to create the association during the process of configuring the Safeguarded Copy session.

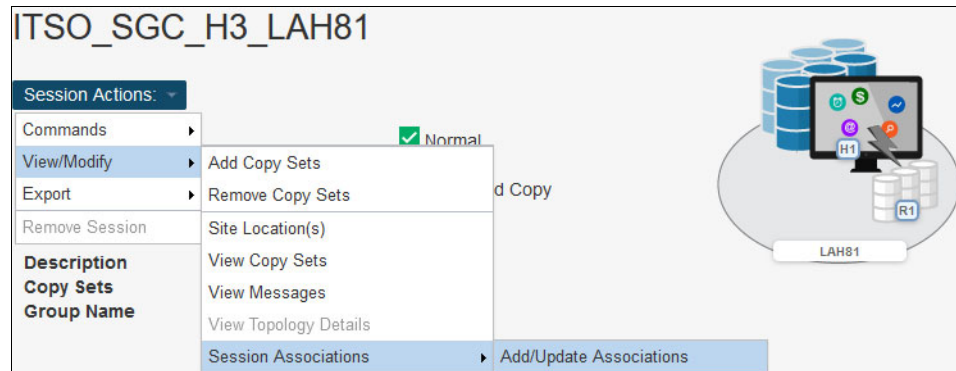


Figure 4-64 Creating a Safeguarded Copy Session association

- In Figure 4-65, select the session that you want to associate to this Safeguarded Copy session. You also must specify the session volumes role pair and specific volume role.

Use the filter to narrow down the list of sessions. In our example, we associated the MGM session ITSO_MGM_ACA91 and selected the H1-H3 Role Pair.

Then, you must choose which of the previously selected role pair volumes will be the Safeguarded Copy source volume. In our example, the Safeguarded Copy is taken from the cascaded GM secondary volume, the answer to “Which role in the selected role pair is the H1 volume in the Safeguarded Copy session?” is H3.

The role selection for the last question “Which role in the selected role pair do you want to restore from a Safeguarded backup?” is in our example H1 because you cannot restore a backup to the Safeguarded Copy source volume.

Associate a session to this Safeguarded Copy session

By Associating a session to this Safeguarded Copy session, the server will validate that the H1 volumes in this session are always the same as the associated session.

Which session should be associated to this Safeguarded Copy session?

Show All

Name	Type
ITSO_MGM_ACA91	MGM
ITSO_MM_LAH81_H1	MM
ITSO_MT_MM_GM_LAH81_ACA91	MT-MM-GM

Which role pair in the session selected above should be associated to the session?

Role Pair:

Which role in the selected role pair is the H1 volume in the Safeguarded Copy session?

Role:

Which role in the selected role pair do you want to restore from a Safeguarded backup?

Role:

OK
Cancel

Figure 4-65 Associate a session to this Safeguarded Copy session

- Before you start backup recovery to the recovery volumes, you might disable the Scheduled Task to avoid creating extra Safeguarded Copy backups. From the Safeguarded Copy **Session Actions** menu, select **Commands**, and then click **Recover Backup**, as shown in Figure 4-66.

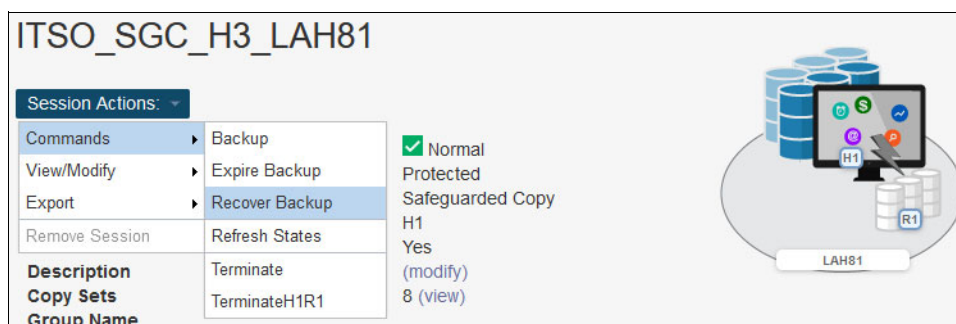


Figure 4-66 Recover Backup

- A new window opens that includes a list of all available backup versions. Select the required backup and click **Yes** to start the backup recovery to the recovery volumes (see Figure 4-67).

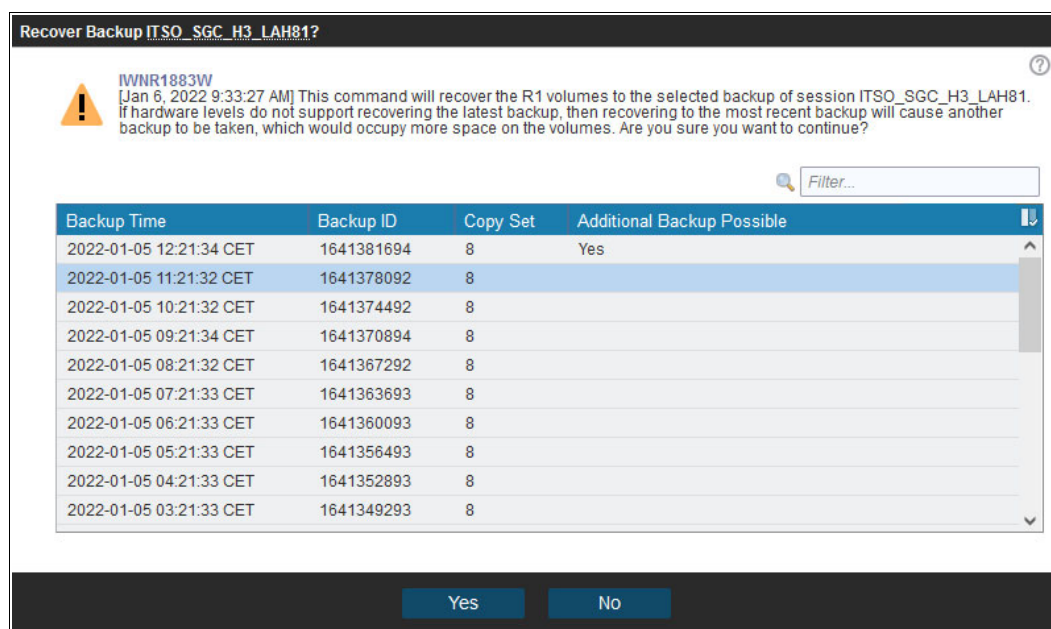


Figure 4-67 Selecting the required backup time and ID

- Wait for the IWN1026I message, which indicates that Recover Backup completed successfully, and check that the correct backup time is displayed beside Last Recovered To Backup, as shown in Figure 4-68 on page 171. The session State should be Target Available.

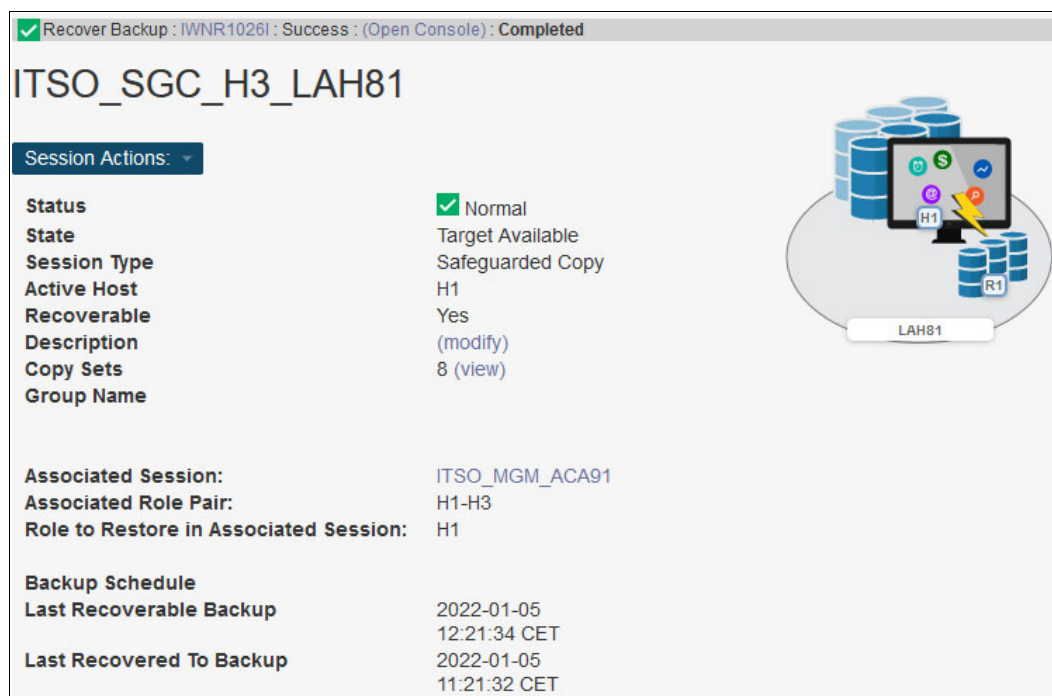


Figure 4-68 Recover Backup completed

At this stage, you can start validating data from the recovery system. If the data in this backup version is still corrupted, you can end the H1-R1 relationship (click **TerminateH1R1**) and recover another backup version (starting at step 3 on page 170).

Important: Before proceeding to step , continue validating backup versions until you find the version that is not corrupted. Ensure that your production applications are not running (no I/Os to production volumes) before you click **Restore Backup**, as described in the next steps.

Also, all changes that are made during the validation process on recovery volumes are lost and therefore are not restored to production volumes.

In the next steps, you prepare the associated replication (MGM) session so that an incremental Global Copy sync process is done during the restore. Multiple steps are required for an MGM session type to build bitmap relationships between H1 - H3 that are required for an incremental resync.

- In the CSM Sessions window, select the associated replication session. In our example that is shown in Figure 4-69, we used the ITSO_MGM_ACA91 MGM session. Select **Session Actions** → **Commands** → **Suspend**.

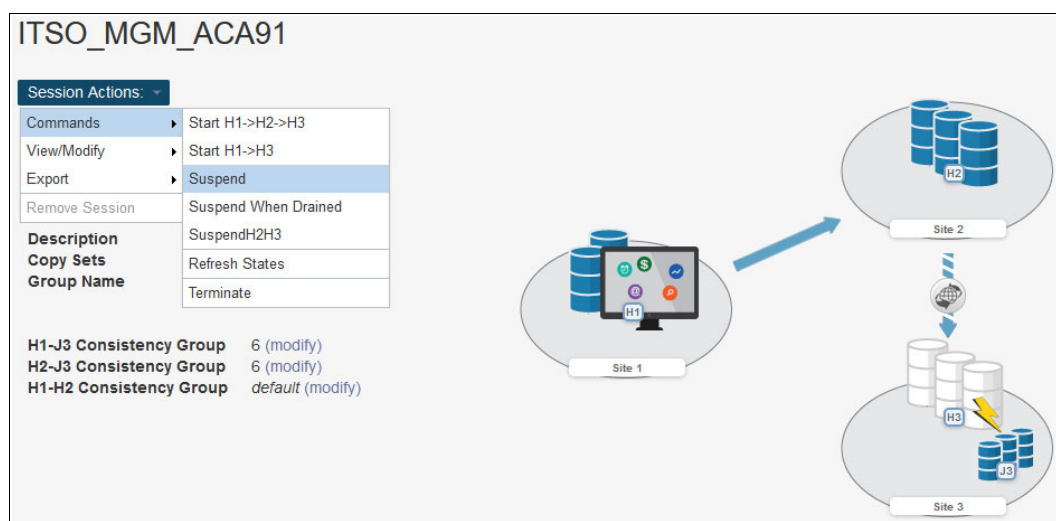


Figure 4-69 Suspending the associated replication session

- Wait until the MGM session is suspended, as shown in Figure 4-70.

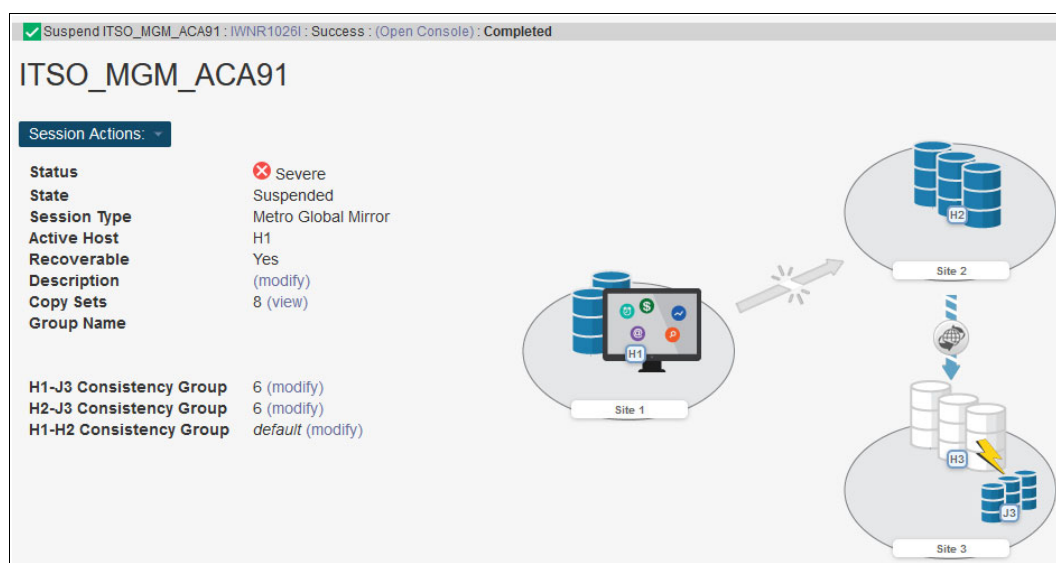


Figure 4-70 Suspending the MGM session

- Select **Session Actions** → **Commands** → **Start H1->H3** for the MGM session and confirm the action by clicking **Yes**, as shown in Figure 4-71 on page 173 to establish a relationship between H1-H3, where H3 is the Safeguarded Copy source volumes.

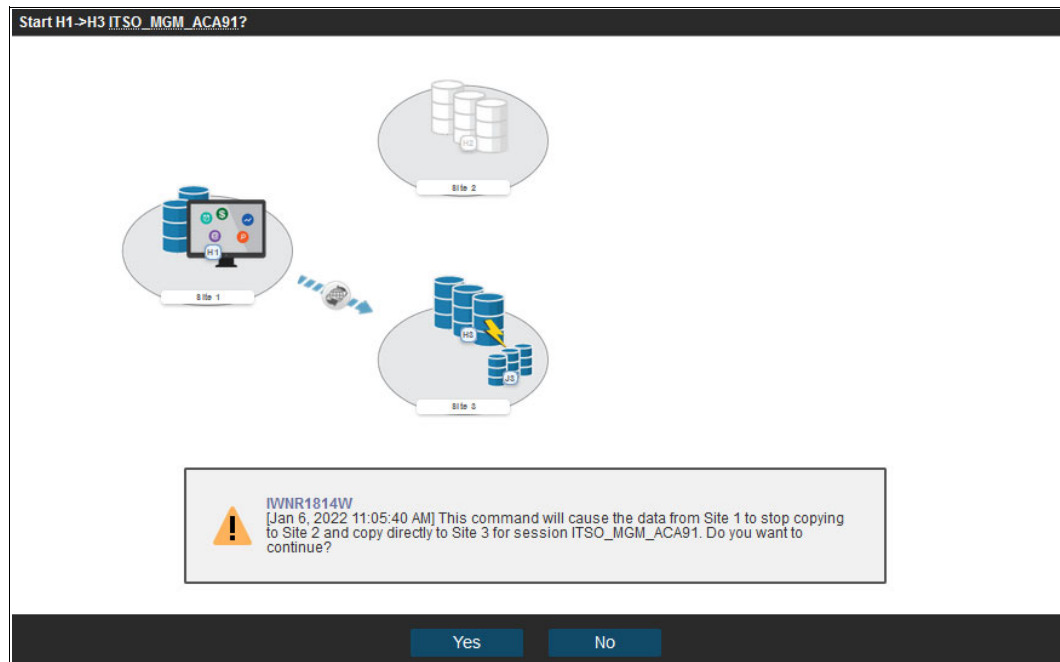


Figure 4-71 Confirming Start H1>H3 in the MGM session

9. After the MGM session is back in the Prepared state with a H1- H3 relationship, select **Session Actions** → **Commands** → **Suspend** for the MGM session, as shown in Figure 4-72.

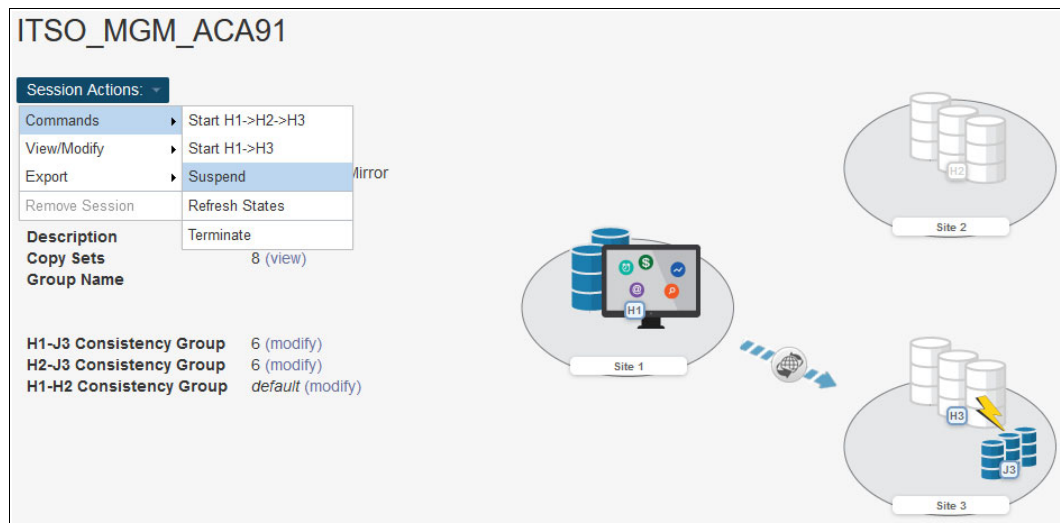


Figure 4-72 Second suspension of the MGM session

When the session is in the Suspended state, continue with the next step.

10. Return to the Safeguarded Copy session. In our example, the session is ITSO_SGC_H3_LAH81. Select **Session Actions** → **Restore Backup** (see Figure 4-73).

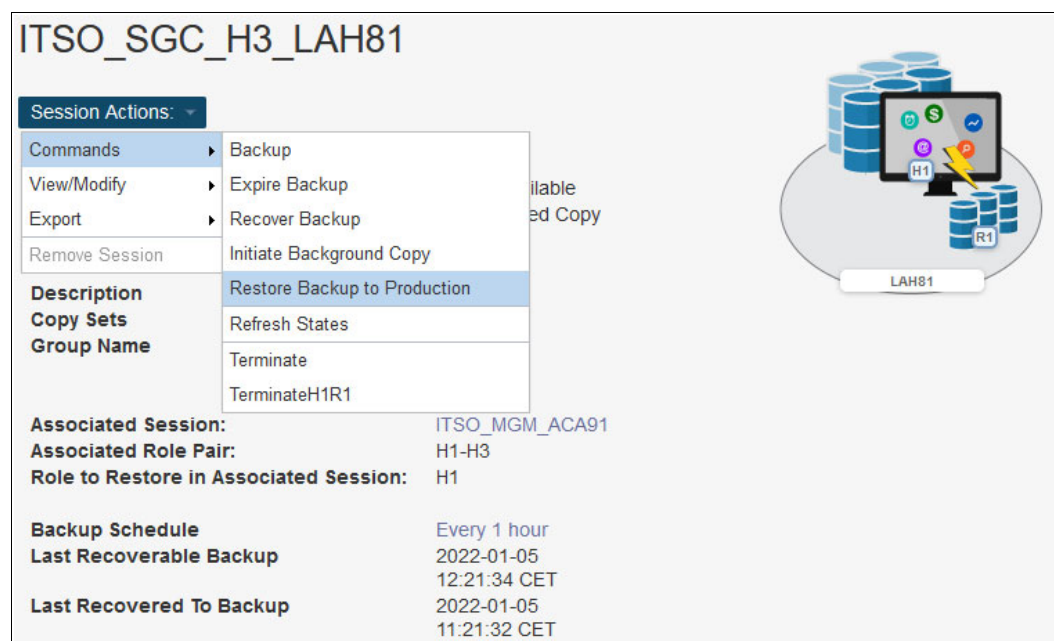


Figure 4-73 Restore Backup to Production

11. A confirmation window opens. Click **Yes** to continue (see Figure 4-74).

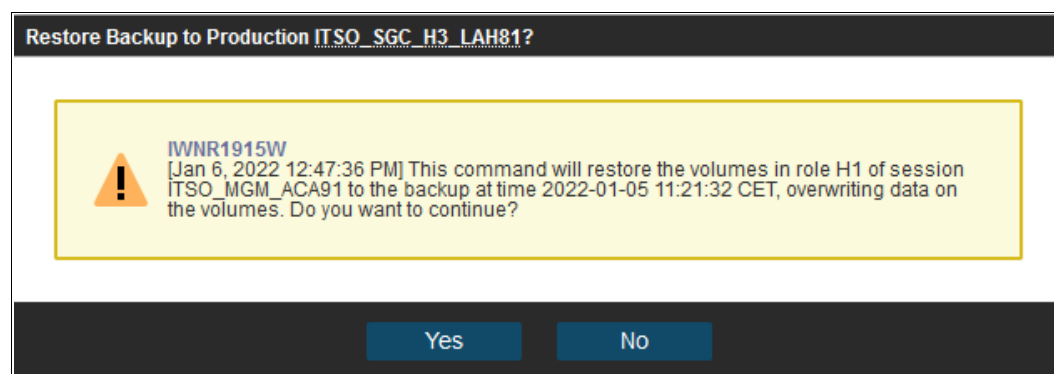


Figure 4-74 Confirming Restore Backup

12. The Safeguarded Copy session state changes to Restoring In the Detailed Status section. You can monitor the restore progress, as shown in Figure 4-75 on page 175.

As you can see in Figure 4-76, the H1-R1 relationship was automatically removed.

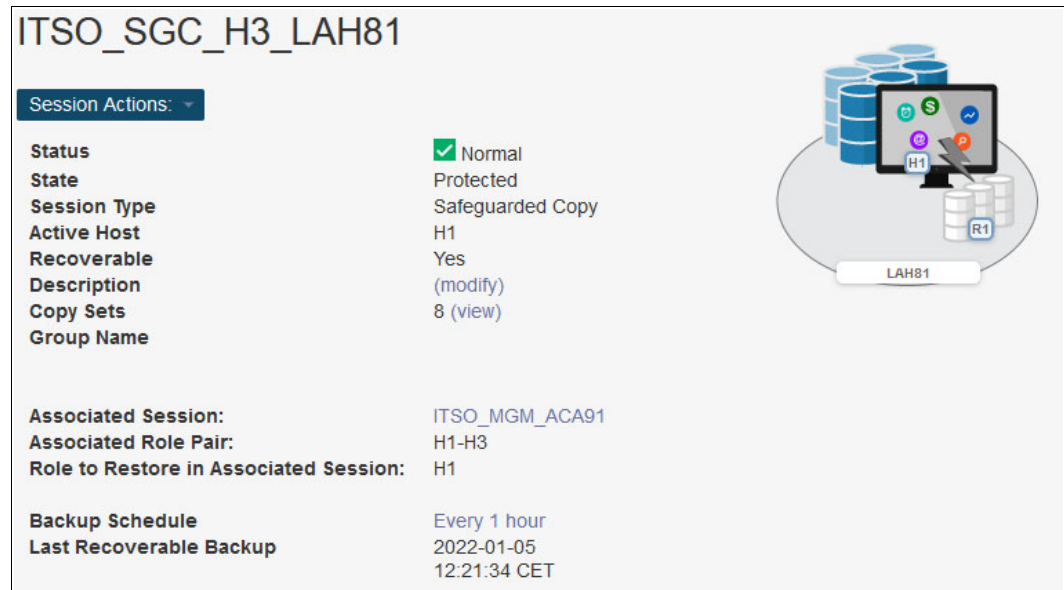


Figure 4-76 Safeguarded Copy session state after Backup Restore completed

13. After the restore process is completed, the MGM session is still in the Suspended state.

Click **Start H1-H2-H3** to restore HADR protection in the MGM session. This action starts an incremental resync unless all backup data was changed.

Note: Before you click **Start H1-H2-H3**, consider the following extra steps:

1. Perform an IPL from the H1 volumes and validate the environment before clicking **Start H1-H2-H3**.
2. Considering that at least all tracks that were restored from R1 to H1 will be resynchronized from H1 to H2 to H3 and stored in your open Safeguarded Copy backup, that process might use significant extra capacity. Depending on your requirements, you might expire all Safeguarded Copy copies and stop Safeguarded Copy before you click **Start H1-H2-H3**.

4.3.3 Restoring a backup to production from H3 in cascaded GM sessions

The steps that are described in this section are applicable for restoring a Safeguarded Copy backup to a cascaded volume in any cascaded CS topology, such as MGM, cascaded GM, or in any 4-Site topology with cascaded GM.

As an example, we explain the procedure to restore a Safeguarded Copy backup to cascaded production volumes in a cascaded GM topology. This example is typical for a Safeguarded Copy physical isolation and in particular for customers who need high frequency backups (see 2.5.1, “Safeguarded Copy key operational considerations” on page 43).

In our example, which is shown in Figure 4-77 on page 177, we use the following sessions:

- ▶ ITSO_GM_ACA90_LAH81 - production GM session:
 - H1 GM primary volumes: Production volumes.
 - H2 GM secondary volumes are cascaded; therefore, they are also primary GM volumes that are defined in ITSO_CASCADE_LAH81_LLB71.

- ▶ ITSO_CASCADE_LAH81_LL71 - cascaded GM session:
 - H2 GM primary volumes are cascaded volumes; therefore, they are also secondary GM volumes that are defined in ITSO_GM_ACA90_LAGH81.
 - H3 GM secondary volumes.
- ▶ ITSO_CASCADE_SGC_LAH81_LL71 - Safeguarded Copy session:
 - H3 Safeguarded Copy source volume, but also GM secondary volumes that are defined in ITSO_CASCADE_LAH81_LL71.
 - R3 Recovery volumes.

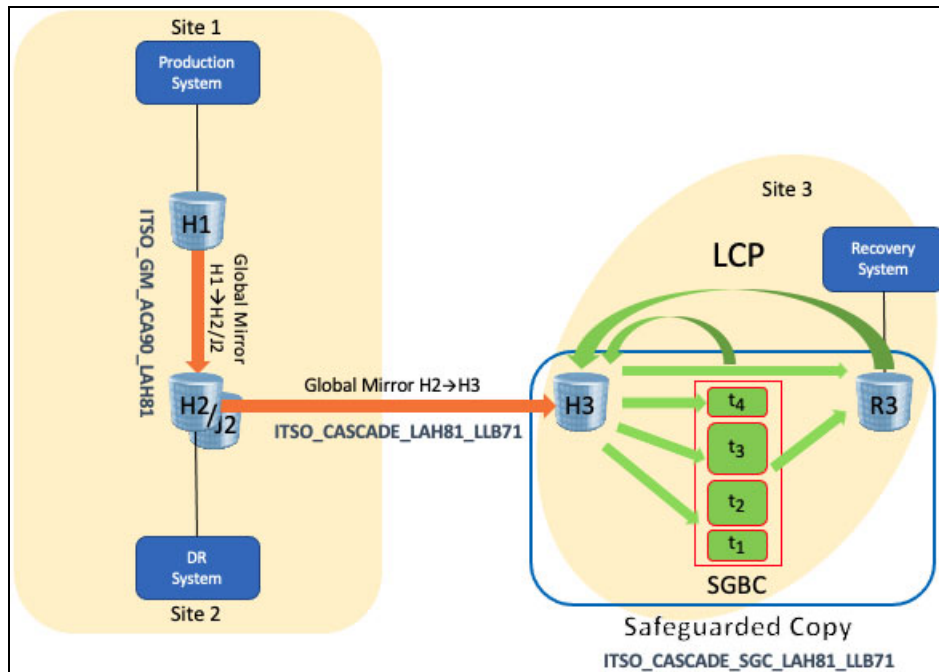


Figure 4-77 Safeguarded Copy with cascaded Global Mirror topology

To restore the R1 volumes to the H1 production GM primary volumes, complete the following steps:

1. Create a Safeguarded copy session association by selecting **View/Modify** → **Session Associations** → **Add/Update Association**, as shown in Figure 4-78.

Note: The association of the Safeguarded Copy session with the corresponding replication session can be done anytime before starting the restore to production process. However, the best practice is to create the association during configuration of the Safeguarded Copy session.

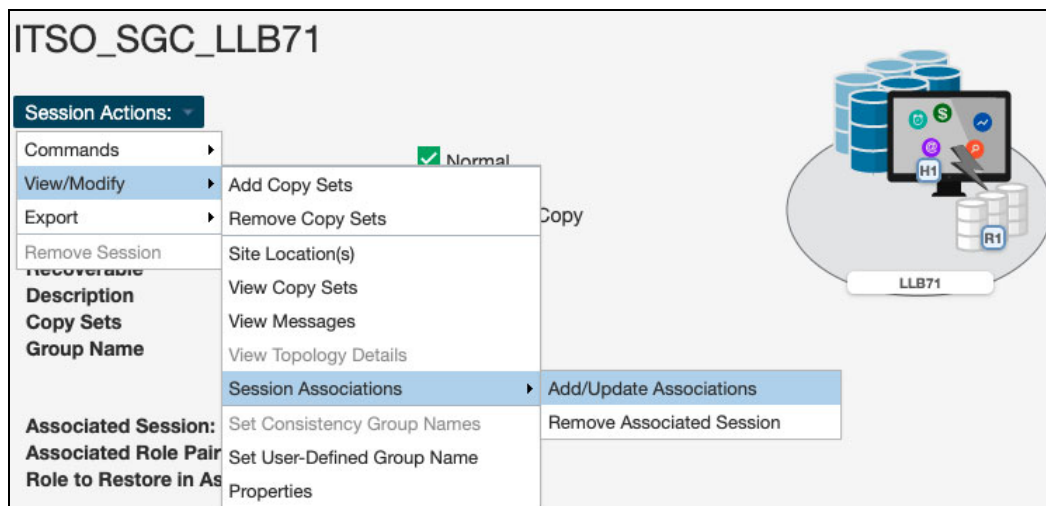


Figure 4-78 Creating a Safeguarded Copy session association

2. In the next window (see Figure 4-79 on page 179), you must select the session that you want to associate to this Safeguarded copy session. You also must specify the session volumes role pair and specific volume role.

Use the filter to narrow down the list of sessions. In our example, we associated the cascaded GM session ITSO_CASCADE_LAH81_LLB71 and selected the **H1-H2** Role Pair.

Then, you must choose which of the previously selected role pair volumes are to be the Safeguarded Copy source volume. In our example, the Safeguarded Copy is taken from the cascaded GM secondary volume, the answer to “Which role in the selected role pair is the H1 volume in the Safeguarded Copy session?” is H2.

The role selection for the last question “Which role in the selected role pair do you want to restore from a Safeguarded backup?” is in our example H1 because you cannot restore backup to the Safeguarded Copy source volume.

Associate a session to this Safeguarded Copy session

By Associating a session to this Safeguarded Copy session, the server will validate that the H1 volumes in this session are always the same as the associated session.

Which session should be associated to this Safeguarded Copy session?

Show All

Name	Type
ITSO_CASCADE_GM_LAH81_LLB71	GM

Which role pair in the session selected above should be associated to the session?

Role Pair:

Which role in the selected role pair is the H1 volume in the Safeguarded Copy session?

Role:

Which role in the selected role pair do you want to restore from a Safeguarded backup?

Role:

OK Cancel

Figure 4-79 Associate a session to this Safeguarded Copy session

- To recover a Safeguarded Copy backup to recovery volumes, from the Safeguarded Copy **Session Actions** menu, select **Commands** → **Recover Backup**, as shown in Figure 4-80.

ITSO_CASCADE_SGC_LAH81_LLB71

Session Actions:

Commands	Backup	Normal
View/Modify	Expire Backup	Protected
Export	Recover Backup	Safeguarded Copy
Remove Session	Refresh States	H1
Recoverable	Terminate	yes
Description	TerminateH1R1	modify
Copy Sets		6 (view)

Figure 4-80 Recover Backup

4. A new window opens that includes a list of all available backup versions. Select the required backup and click **Yes** to start the backup recovery to the recovery volumes (see Figure 4-81).

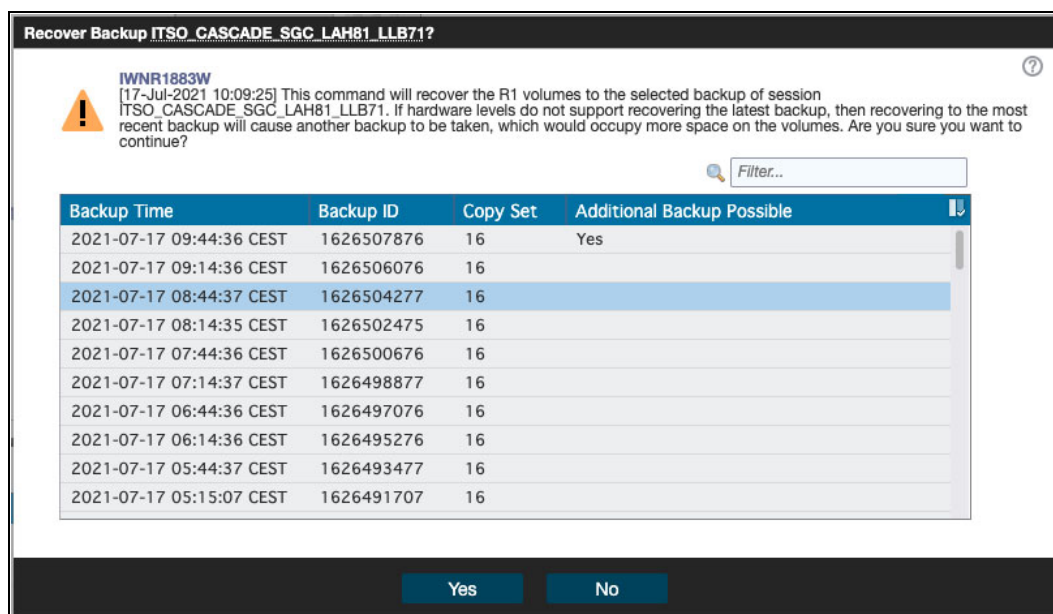


Figure 4-81 Selecting the required backup version

5. Wait for the IWN1026I message, which indicates that the Recover Backup action completed successfully (see Figure 4-82).

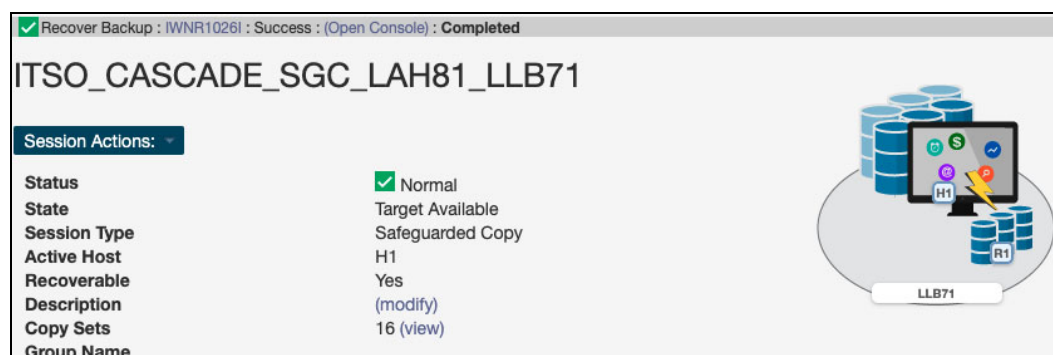


Figure 4-82 Recover Backup completed

At this stage, you can start validating data from the recovery system. If the data in this backup version is still corrupted, you must end the H1-R1 relationship (click **TerminateH1R1**) and recover another backup version (from step 3 on page 179).

Important: Before proceeding to the next step, continue validating backup versions until you find the one that is not corrupted.

Make sure that your production applications are not running (no I/Os to production volumes) before you click **Restore Backup** in the next step.

Also, all changes that are made during the validation process on recovery volumes are lost and not restored to production volumes.

- In the CSM Sessions window, select the associated replication session. In our example (see Figure 4-57 on page 165), it is ITSO_CASCADE_GM_LAH81_LLB71 cascaded GM session. From Session Actions, select **Commands** → **Suspend**.

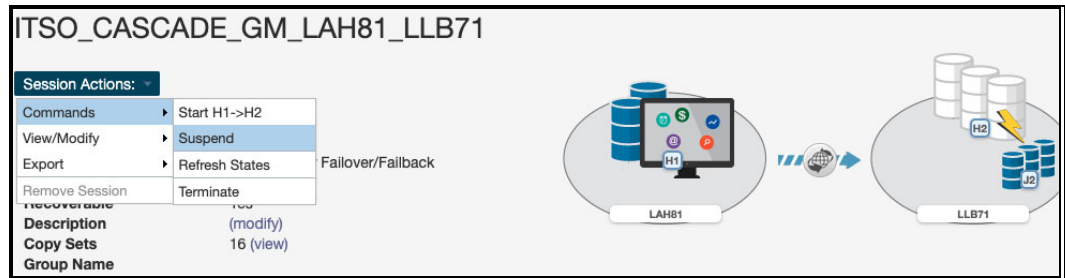


Figure 4-83 Suspending the associated cascaded GM session

After you confirm the Suspend action, the session changes to the Suspending state, but it is not suspended until the production GM session also is suspended.

- Go to the production GM session. In our example (shown in Figure 4-84), it is the ITSO_GM_ACA90_LAH81 cascaded GM session.

Select **Session Actions** → **Commands** → **Suspend**.

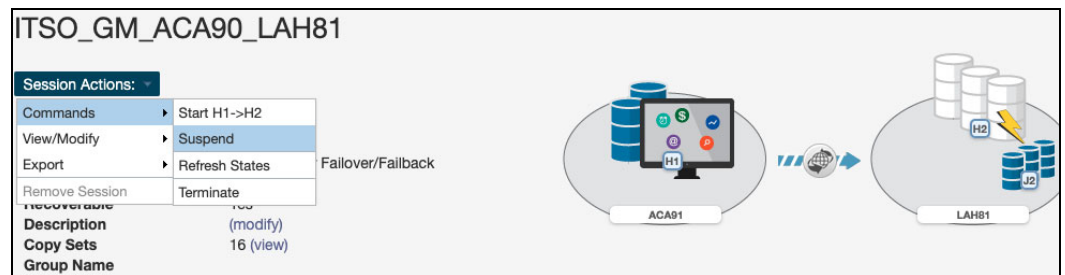


Figure 4-84 Suspending the production GM session

When the production GM session ITSO_GM_ACA90_LAH81 is suspended, the cascaded GM session ITSO_CASCADE_GM_LAH81_LLB71 also is suspended, and the CG is formed for the cascaded GM session.

- Before you can click **Restore Backup** for the cascaded GM secondary volume, you first must click **Recover** from the production GM session, which in our example is ITSO_GM_ACA90_LAH81 (see Figure 4-85).

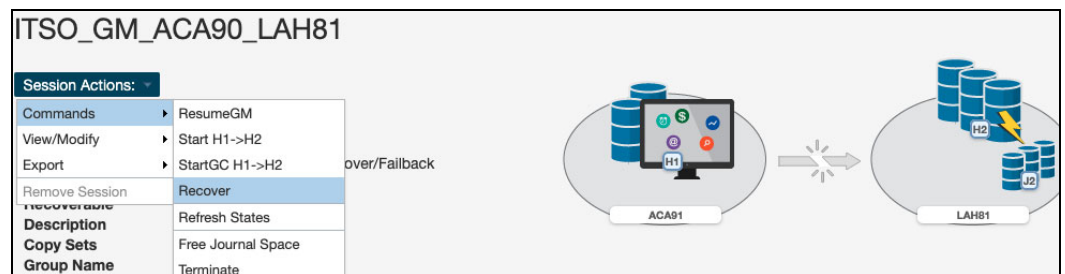


Figure 4-85 Recovering the production GM session

Attention: Failing to recover the production GM session causes **Restore Backup** to fail because the cascaded volume to which the backup is restored to must be in primary suspended state for both production and cascaded GM sessions.

9. Click **Yes** to continue (see Figure 4-86).

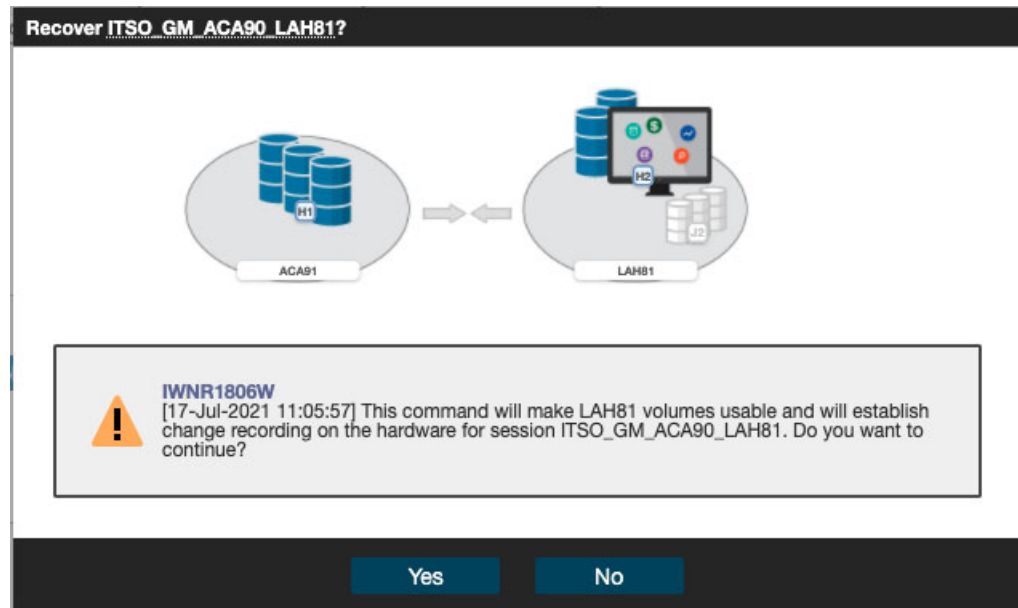


Figure 4-86 Confirming the recovery of the production GM session

The IWNR1026I message is displayed, which confirms that the recovery completed successfully, as shown in Figure 4-87.

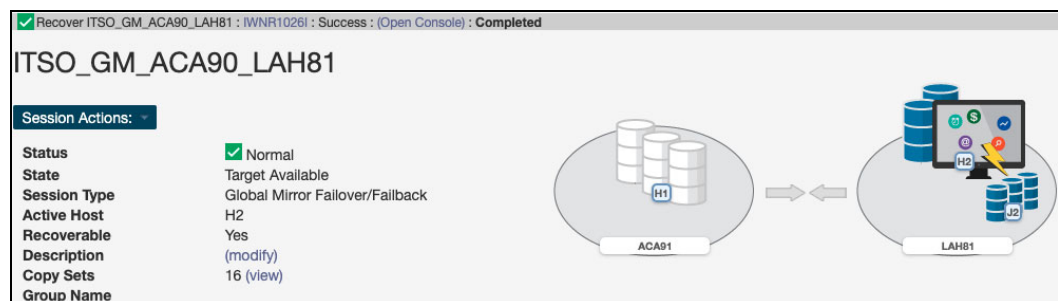


Figure 4-87 Recovery completed

10. Return to the Safeguarded Copy session. In our example, this session is the ITSO_CASCADE_SGC_LLB71 session. Select **Session Actions** → **Commands** → **Restore Backup** (see Figure 4-88).

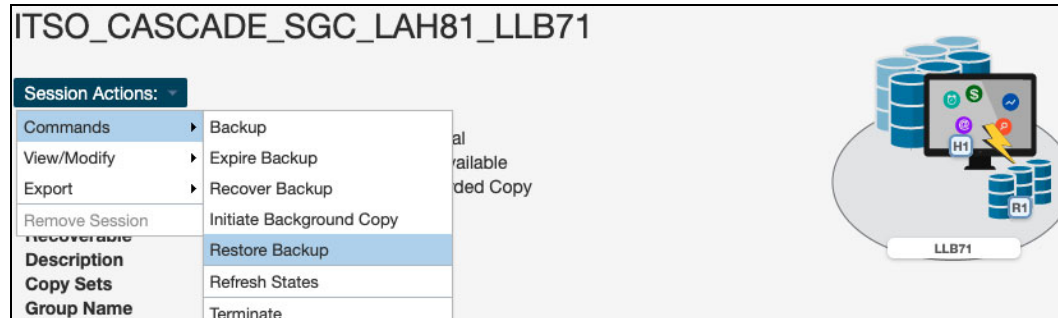


Figure 4-88 Safeguarded Copy Restore Backup

A confirmation window opens. Click **Yes** to continue (see Figure 4-89).

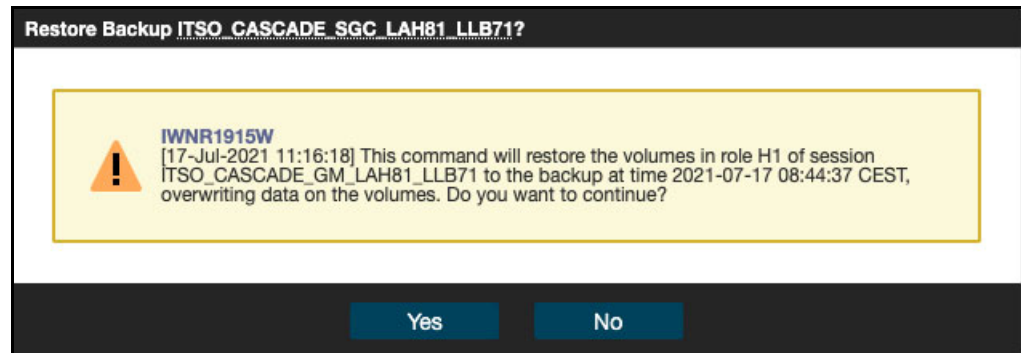


Figure 4-89 Confirming Restore Backup

11. The Safeguarded Copy session changed to the Restoring state. In the **Restore to Production Info** tab, you can monitor the restore progress, as shown in Figure 4-90.

Restore Backup : IWNR1026I : Success : (Open Console) : Completed

ITSO_CASCADE_SGC_LAH81_LLB71

Session Actions:

Status	Normal
State	Restoring
Session Type	Safeguarded Copy
Active Host	H1
Recoverable	Yes
Description	(modify)
Copy Sets	16 (view)
Transitioning	Yes
Group Name	

Associated Session: ITSO_CASCADE_GM_LAH81_LLB71
Associated Role Pair: H1-H2
Role to Restore in Associated Session: H1

Backup Schedule Every 30 mins
Last Recoverable Backup 2021-07-17 10:14:36 CEST
Last Recovered To 2021-07-17 08:44:37 CEST

Detailed Status:
 ✨ IWNR6042I [17-Jul-2021 12:12:41] Preparing recovery volumes to restore H1 volumes in session ITSO_CASCADE_GM_LAH81_LLB71...

Backup Info **Recover Backup Info** **Restore to Production Info**

R1	P2	Recovery Backup Time	State	Progress
----	----	----------------------	-------	----------

Figure 4-90 Restore Backup completed

The backup data replicates from recovery R1 volumes to the cascaded H1 GM primary volumes. This process is done with Global Copy incremental resync, that is, only changed tracks for this backup version are sent to the cascaded GM primary volumes.

After the restore backup process is completed, the Safeguarded Copy session changes to the Protected state. As you can see in Figure 4-91, the H1-R1 relationship was automatically removed.

Restore Backup : IWNR1026I : Success : (Open Console) : Completed

ITSO_CASCADE_SGC_LAH81_LLB71

Session Actions:

Status	Normal
State	Protected
Session Type	Safeguarded Copy
Active Host	H1
Recoverable	Yes
Description	(modify)
Copy Sets	16 (view)
Group Name	

Associated Session: ITSO_CASCADE_GM_LAH81_LLB71
Associated Role Pair: H1-H2
Role to Restore in Associated Session: H1

Backup Schedule Every 30 mins
Last Recoverable Backup 2021-07-17 10:14:36 CEST
Last Recovered To 2021-07-17 08:44:37 CEST

Detailed Status:
 ✨ IWNR6042I [17-Jul-2021 12:12:41] Preparing recovery volumes to restore H1 volumes in session ITSO_CASCADE_GM_LAH81_LLB71...

Backup Info **Recover Backup Info** **Restore to Production Info**

R1	P2	Recovery Backup Time	State	Progress
----	----	----------------------	-------	----------

Figure 4-91 Restore Backup to production volumes completed

12. After the restore process to the cascaded GM primary volumes is completed, go to the production GM session (in our example, it is the ITSO_GM_ACA90_LAH71 GM session), which is in the Target Available state (see Figure 4-92 on page 185).

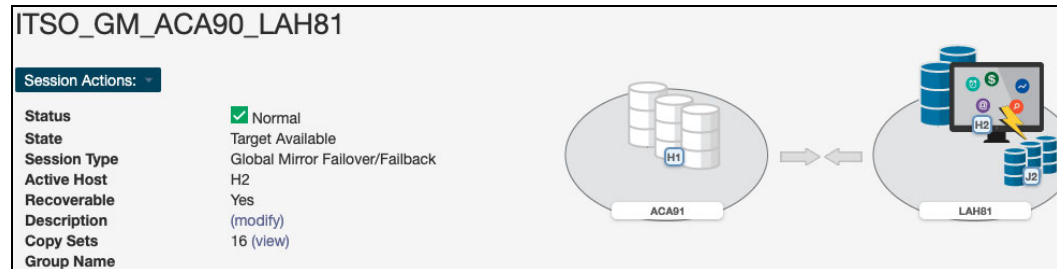


Figure 4-92 Target Available State for a production GM session

The H2 volume in this session is a cascaded volume that also is defined as H1 volume in our cascaded GM session on which you restored the Safeguarded Copy backup. To copy data from the H2 volume to the production H1 GM volume, you must first enable copy direction from H2 to H1.

Select **Commands** → **Enable Copy to Site 1**, as shown in Figure 4-93.

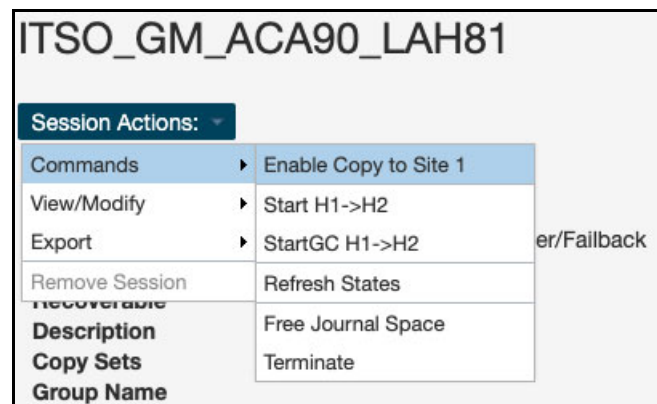


Figure 4-93 Enable Copy to Site 1 for the production GM session

Then, select **Commands** → **Start H2-H1** (see Figure 4-94).

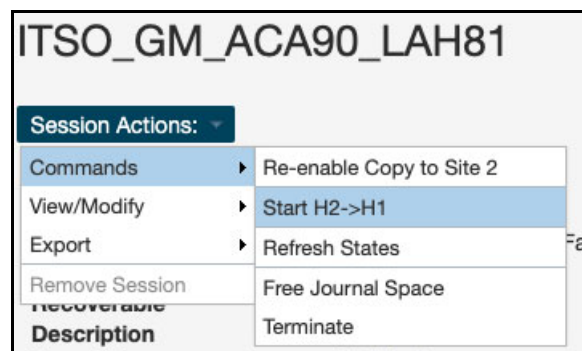


Figure 4-94 Selecting Start H2-H1 for the production GM session

Note: In our example, the production GM is not defined as GM Either Direction (with GM Journal volumes at both sites). **Start H2-H1** uses Global Copy replication. Therefore, the session stays in Warning status.

Wait for the resync from H2 to H1 to complete and reach 100% copy Progress and 0 remaining tracks, as shown in Figure 4-95.

If your production GM session is defined as Either Direction, wait for the session to change to Normal status and Prepared state before you continue with next steps.


Role Pairs Info		Global Mirror Info			
Participating Role Pairs:					
Role Pair	Error Count	Recoverable	Copying	Progress	Copy Type
H1 ← H2	0	0	16	100% 	GC
Non-Participating Role Pairs:					
Role Pair	Error Count	Recoverable	Copying		
				<div>Role Pair H1-H2 IWN6013I [17-Jul-2021 11:50:57] 100% of the data on H2 has been copied to H1. Total: 320,544 Cyls (4,808,160 tracks) Remaining: 0 (0 tracks)</div>	

Figure 4-95 Global Copy progress

13. From the production GM session, fail over to the original production H1 GM volumes with the following sequence:

- Suspend**
- Recover**
- Enable Copy to Site 2**
- Start H1-H2**

14. At this stage, you can also start the cascaded GM session and completely restore the Safeguarded Copy topology with cascaded GM.

From the cascaded GM, click **Start H1-H2**. The session might stay in the Warning state until the production GM session is suspended. If so, go to the next step.

Note: Before you click **Start H1-H2**, consider the following steps:

- ▶ Perform an IPL from the H1 volumes and validate the environment another time before clicking **Start H1-H2**.
- ▶ Because at least all tracks that were restored from R1 to H1 are resynchronized from H1 to H2 and are stored in your current open Safeguarded Copy backup, that process might use significant extra capacity. Depending on your requirements, you might expire all Safeguarded Copies and stop Safeguarded Copy before you click **Start H1-H2**.

15. From the production GM session, click the following menu items:

- Suspend**
- Resume GM**

At this stage, both production and cascaded GM sessions are in the Normal status and the Prepared state. You also can check whether the Safeguarded Copy session that is associated to the cascaded GM session is still active.

Now that the Safeguarded Copy topology with cascaded GM is restored as it was originally, you can start your production applications from the production H1 GM primary volumes.

4.3.4 Restoring a backup to production from H1 in an MM session

The steps that are described in this section are applicable for restoring a Safeguarded Copy backup from the primary H1 volumes to the secondary H2 volumes and replicating it to the primary (H1) volumes in an MM topology / session.

In this example, we use the following sessions:

- ▶ ITS0_MM_LAH81_H1 - production MM session:
 - H1 primary volumes
 - H2 Secondary volumes
- ▶ ITS0_SGC_H1_LAH81 - Safeguarded Copy session:
 - H1 Safeguarded Copy source volume, but also H1 MM primary volumes that re defined in ITS0_MM_LAH81_H1
 - R1 Recovery volumes

Before we show each step in detail, here is a summary with the required steps to restore a backup to production from H1 volumes in an MM session:

1. Associate the Safeguarded Copy session with the MM session that will be restored.
2. If you established a Safeguarded Copy Scheduled Task for the session on which you want to initiate a restore, you might disable this task to avoid extra Safeguarded Copy backups.
3. Click **Recover Backup** from the Safeguarded Copy session, and then select the required backup.
4. Perform data analysis on the recovery system.
5. Stop production applications (if not already done).
6. Suspend the associated MM session.
7. Click **Restore to production** from the Safeguarded Copy session.
8. Click **Start H2>H1** from the MM session.
9. Fail over or fail back the MM session to start the production workload from the H1 volumes.

To restore the R1 volumes to the H1 production MM primary volumes, complete the following steps:

1. Create a Safeguarded Copy session association with the MM session by selecting **View/Modify** → **Session Associations** → **Add/Update Association**, as shown in Figure 4-96.

Note: The association of the Safeguarded Copy session with the corresponding replication session can be done anytime before starting the restore to production process. However, a best practice is to create the association during the process of configuring the Safeguarded Copy session.

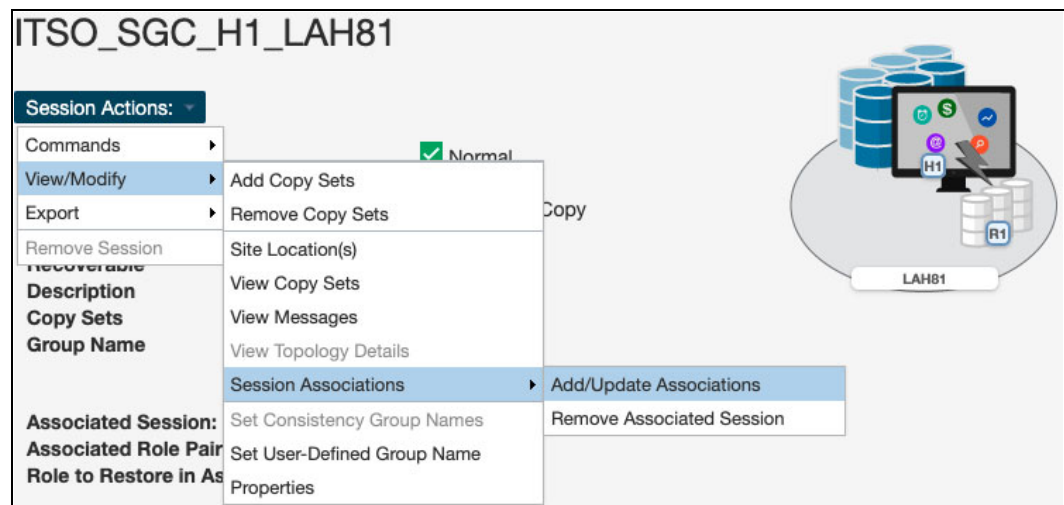


Figure 4-96 Creating a Safeguarded Copy session association

2. In Figure 4-97 on page 189, select the session that you want to associate to this Safeguarded Copy session. Also, specify the session volumes role pair and specific volume role.

Use the filter to narrow the list of sessions. In our example, we associated the MM session ITSO_MM_LAH81_H1 and selected the **H1-H2** Role Pair.

Note: H1-H2 is the only available Role Pair option for a 2-site (MM or GM) topology. In 3- or 4-site topologies, more Role Pair options are available.

Associate a session to this Safeguarded Copy session

By Associating a session to this Safeguarded Copy session, the server will validate that the H1 volumes in this session are always the same as the associated session.

Which session should be associated to this Safeguarded Copy session?

Show All

Name	Type
ITSO_MGM_ACA91	MGM
ITSO_MM_LAH81_H1	MM
ITSO_MT_MM_GM_LAH81_ACA...	MT-MM-GM

Which role pair in the session selected above should be associated to the session?

Role Pair:

Which role in the selected role pair is the H1 volume in the Safeguarded Copy session?

Role:

Which role in the selected role pair do you want to restore from a Safeguarded backup?

Role:

OK Cancel

Figure 4-97 Associate a session to this Safeguarded Copy session

- Choose which of the previously selected role pair volumes will be the Safeguarded Copy source volumes. Because the Safeguarded Copy in our example is taken from the MM primary volumes, the answer to “Which role in the selected role pair is the H1 volume in the Safeguarded Copy session?” is H1.

The role selection for the last question “Which role in the selected role pair do you want to restore from a Safeguarded backup?” is in our example H2 because you cannot restore the backup to the Safeguarded Copy source volume (see Figure 4-97).

- Start the backup recovery to the recovery volumes. From the Safeguarded Copy **Session Actions** menu, select **Commands** and then click **Recover Backup**, as shown in Figure 4-98.

ITSO_SGC_H1_LAH81

Session Actions:

- Commands
 - Backup
 - Expire Backup
 - Recover Backup
- View/Modify
- Export
- Remove Session
- Refresh States
- Terminate
- TerminateH1R1

Description

Copy Sets

Normal
Protected
Safeguarded Copy
H1
yes
(modify)
(view)

Figure 4-98 Recover Backup

- The new window includes a list of all available backup versions. Select the required backup and click **Yes** to start the backup recovery to the recovery volumes (see Figure 4-99).

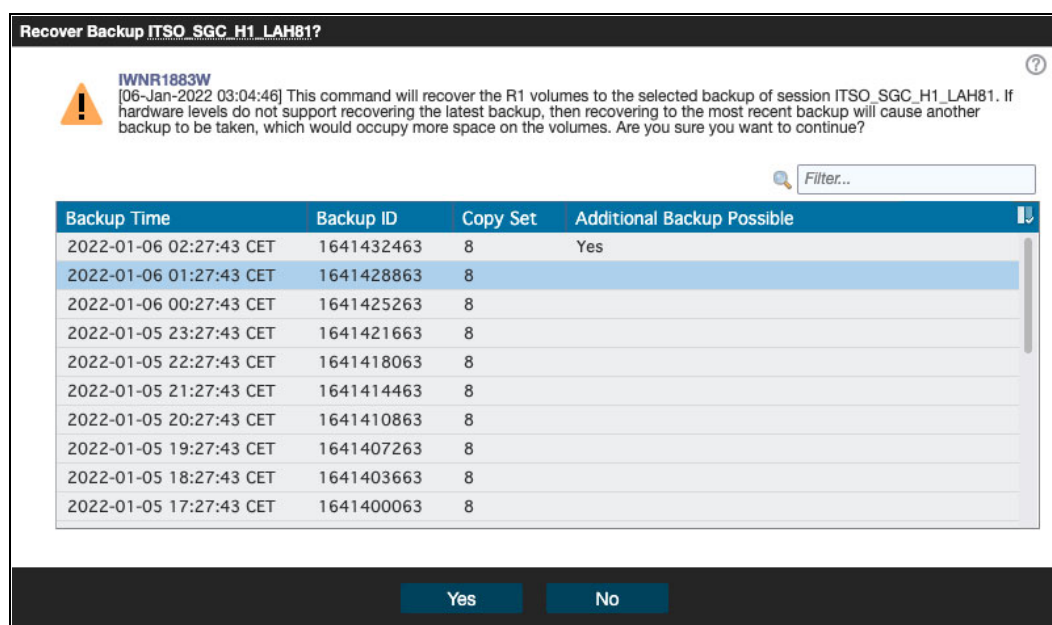


Figure 4-99 Selecting the required backup version

- Wait for the IWN1026I message, which indicates that Recover Backup completed successfully (see Figure 4-100).

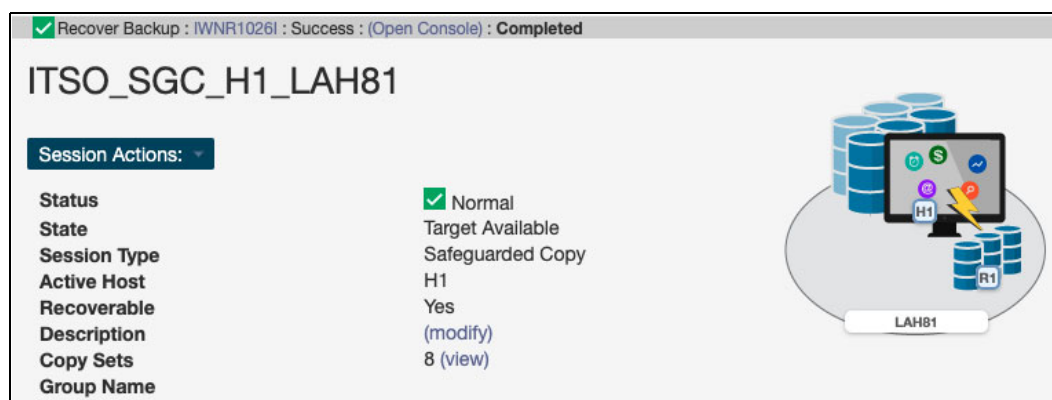


Figure 4-100 Recover Backup completed

At this stage, you can start validating data from the recovery system. If the data in this backup version is still corrupted, you can end the H1-R1 relationship (click **TerminateH1R1**) and recover another backup version (starting at step 4 on page 189).

Important: Before proceeding to the next step, continue validating backup versions until you find the version that is not corrupted. Ensure that your production applications are not running (no I/Os to production volumes) before you use **Restore Backup**, as described in the next steps.

Also, all changes that are made during the validation process on recovery volumes are lost and not restored to production volumes.

- In the CSM Sessions window, select the associated replication session. In our example, which is shown in Figure 4-101, we use the ITSO_MM_LAH81_H1 MM session. Select **Session Actions** → **Commands** → **Suspend**.

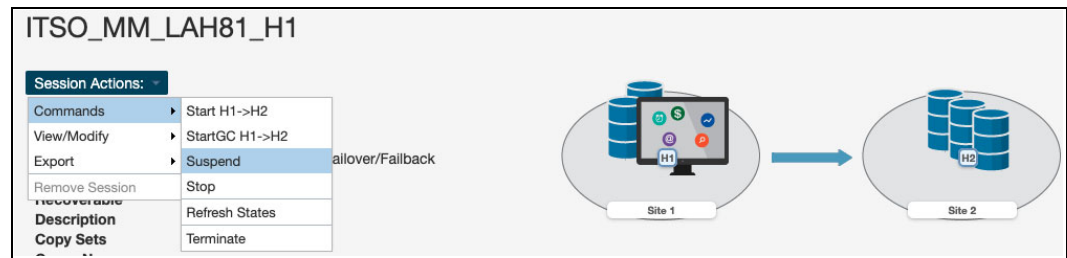


Figure 4-101 Suspending the associated session

- Click **Yes** to continue (see Figure 4-102).

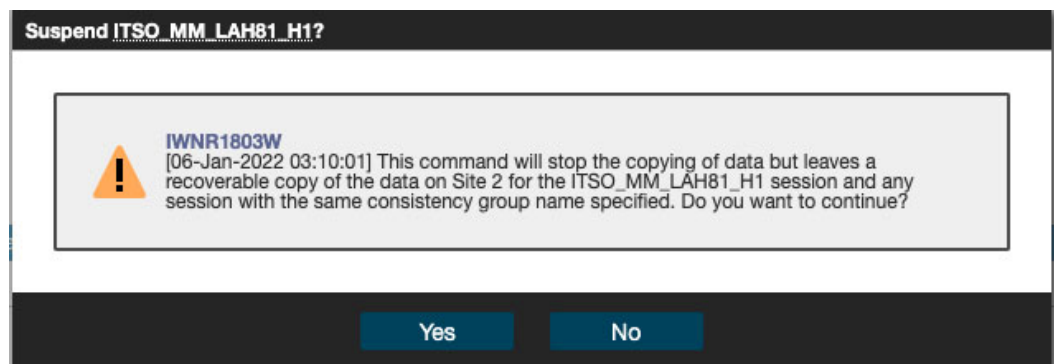


Figure 4-102 Confirming the suspension

- Return to the Safeguarded Copy session. In our example, the session is ITSO_SGC_H1_LAH81. Select **Session Actions** → **Restore Backup to Production** (see Figure 4-103).

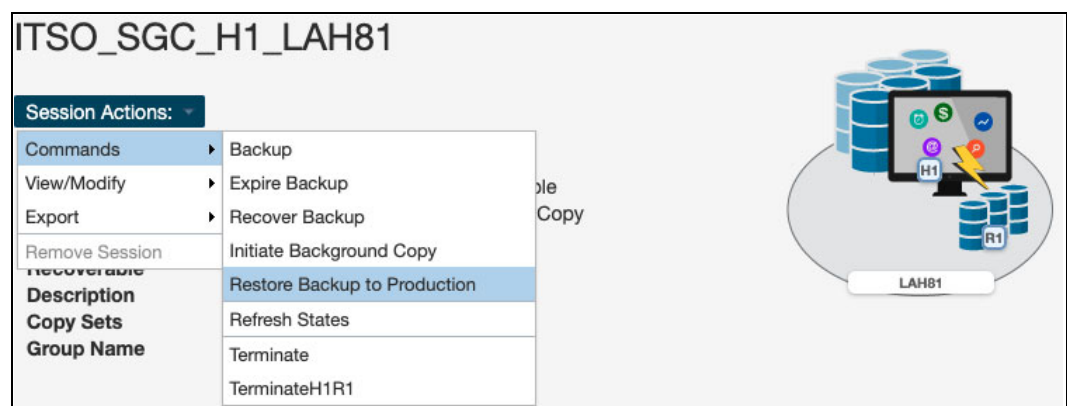


Figure 4-103 Safeguarded Copy Restore Backup

10.A confirmation window opens. Click **Yes** to continue (see Figure 4-104).

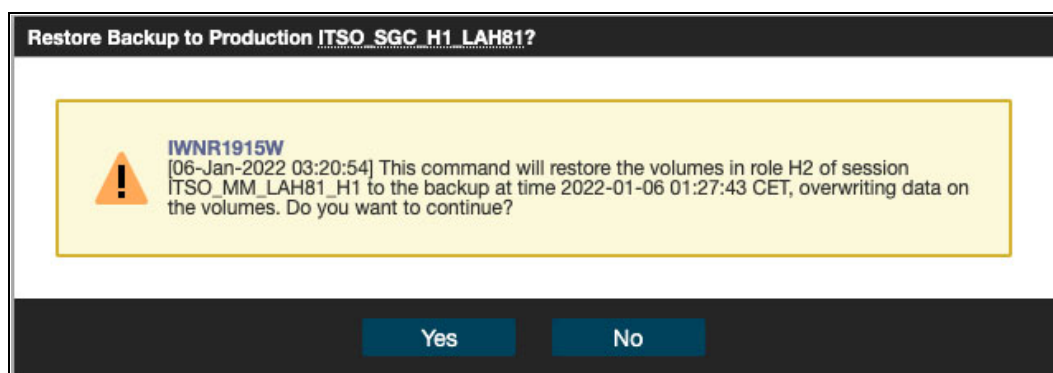


Figure 4-104 Confirming Restore Backup

11.The Safeguarded Copy session state changes to Restoring, as shown in Figure 4-105. In the Detailed Status section, you can monitor the restore progress.

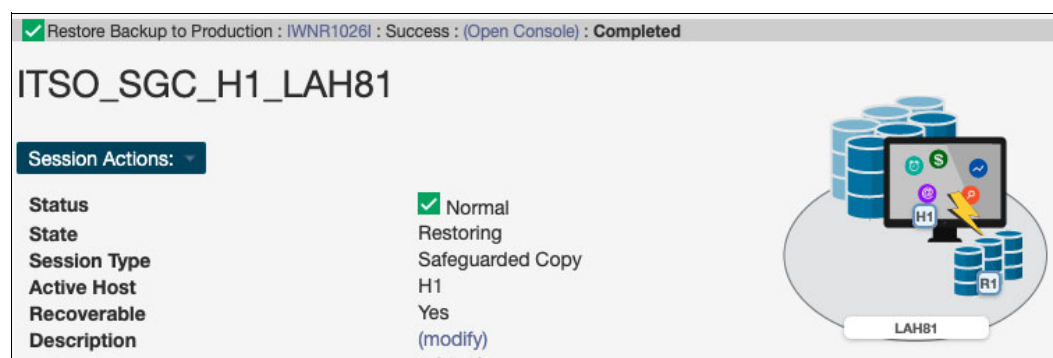


Figure 4-105 Restoring Backup

The backup data is now being replicated from the recovery volumes R1 to the production MM secondary volumes H2. This process is done with Global Copy incremental resync so that only changed tracks for this backup version are sent to the production H2 volumes.

After the backup is restored to the production volumes, the Safeguarded Copy session changes to the Protected state.

As you can see in Figure 4-106, the H1-R1 relationship was automatically removed.

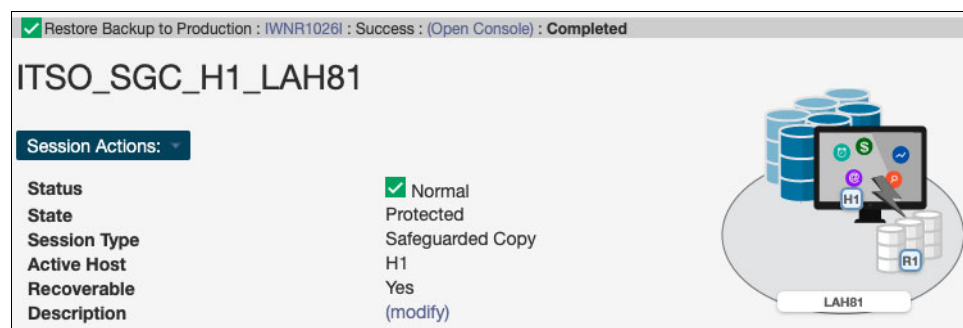


Figure 4-106 Restore Backup to production volumes completed

12. After the restore to production of MM primary volumes is completed, the ITSO_MM_LAH81_H1 MM session (which was in the Suspended state before **Restore Backup**) changes to the Target Available state (see Figure 4-107).

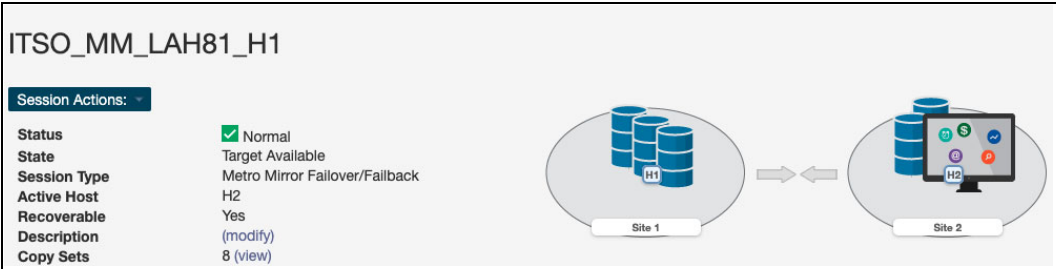


Figure 4-107 Target Available State for the Metro Mirror session

13. Now that the Safeguarded Copy is restored successfully to the H2 MM secondary volumes and before you start replication from H2 to H1, shut down all systems and applications on the primary H1 volumes.

To use **Start H2-H1**, from **Session Actions** → **Commands**, select **Enable Copy to Site 1**, as shown in Figure 4-108.

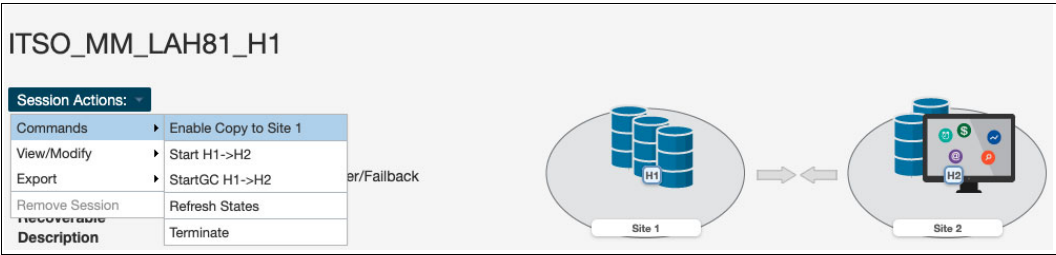


Figure 4-108 Enable Copy to Site 1

14. The window that is shown in Figure 4-109 is a confirmation to enable **Start H2-H1**.

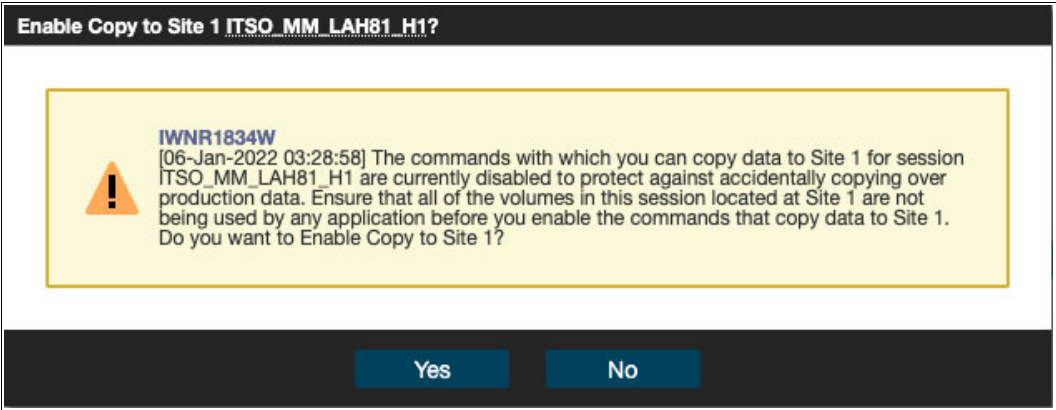


Figure 4-109 Enabling Start H2-H1

15. Click **Start H2-H1** (Figure 4-110) to start replicating the restored Safeguarded Copy data from the H2 volumes. This action starts an incremental resync.

Note: Before you click **Start H2-H1**, consider the following extra steps:

- ▶ Perform an IPL from the H2 volumes and validate the environment another time before clicking **Start H2-H1**.
- ▶ Considering that at least all tracks that were restored from R1 to H2 will be resynchronized from H2 to H1 and stored in your open Safeguarded Copy backup, that process might use significant extra capacity. Depending on your requirements, you might expire all Safeguarded Copies and stop Safeguarded Copy before you click **Start H2-H1**.

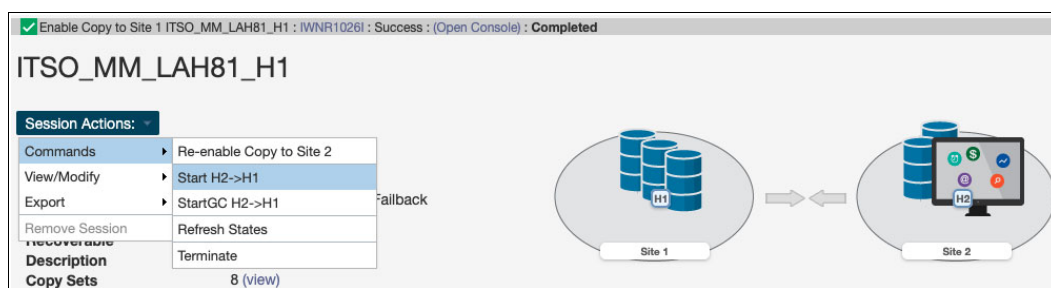


Figure 4-110 Start H2-H1

16. After the resynchronization between the H2 and H1 volumes is completed, the session status is Normal and the state is Prepared, as shown in Figure 4-111.

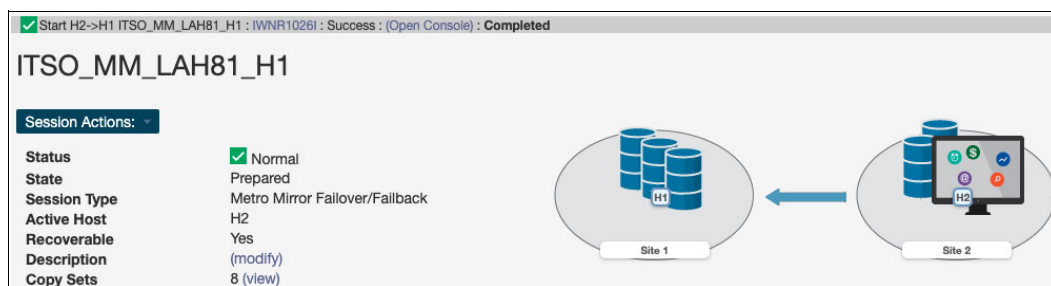


Figure 4-111 Metro Mirror session in Normal status and Prepared state

17. The next few steps are required to fail over the MM session and start production applications from the H1 volumes. From the **Session Actions** menu, select **Commands** → **Suspend** (Figure 4-112).

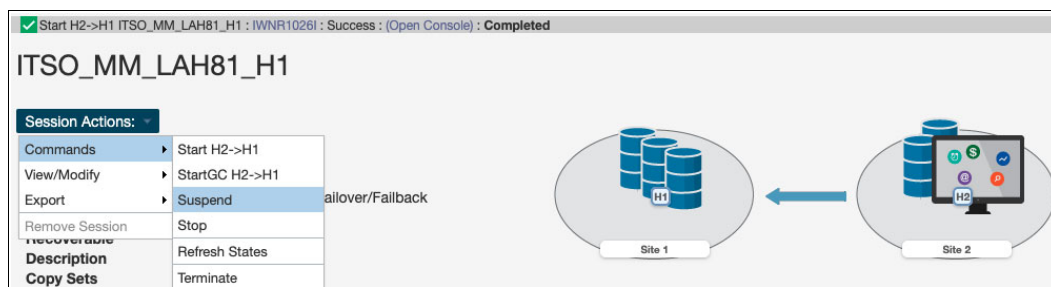


Figure 4-112 Suspending the Metro Mirror session

18. Confirm the **Suspend** action (Figure 4-113).

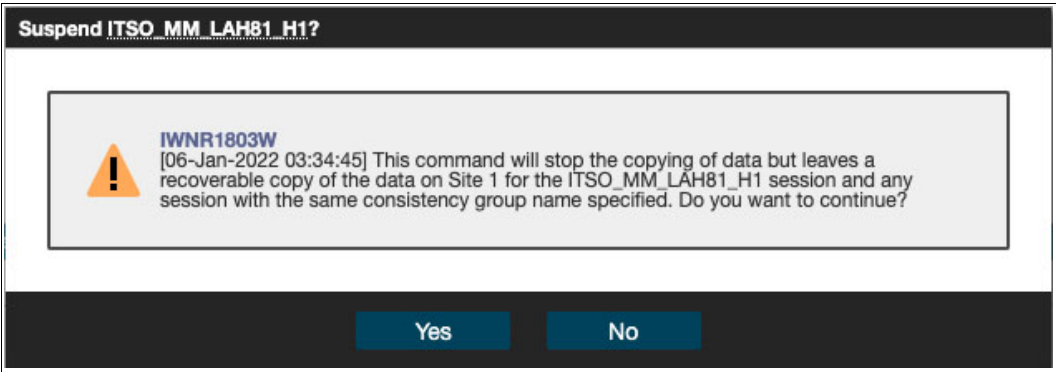


Figure 4-113 Confirming the Suspend action for the Metro Mirror session

19. The session status is Severe and its state is Suspended, as shown in Figure 4-114.

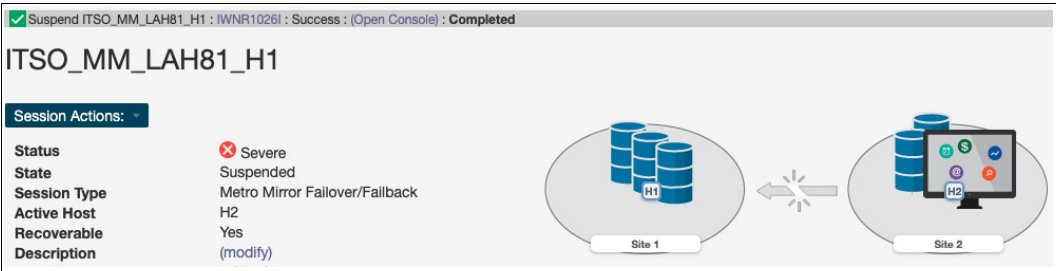


Figure 4-114 Metro Mirror session in the Severe status and Suspended state

20. From the **Session Actions** menu, select **Command** → **Recover** (see Figure 4-115).

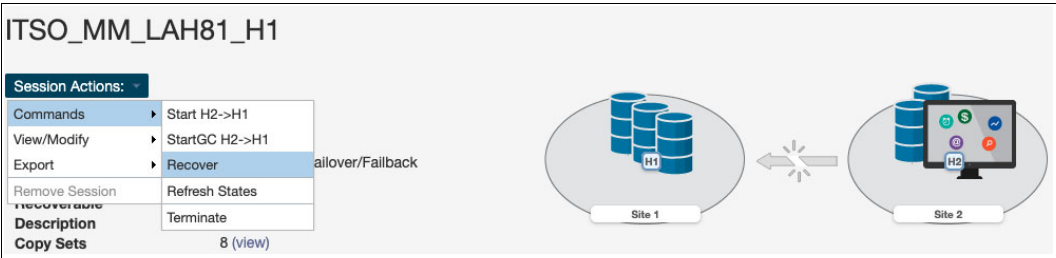


Figure 4-115 Recovering the MM session

21. Confirm the **Recover** action (see Figure 4-116).

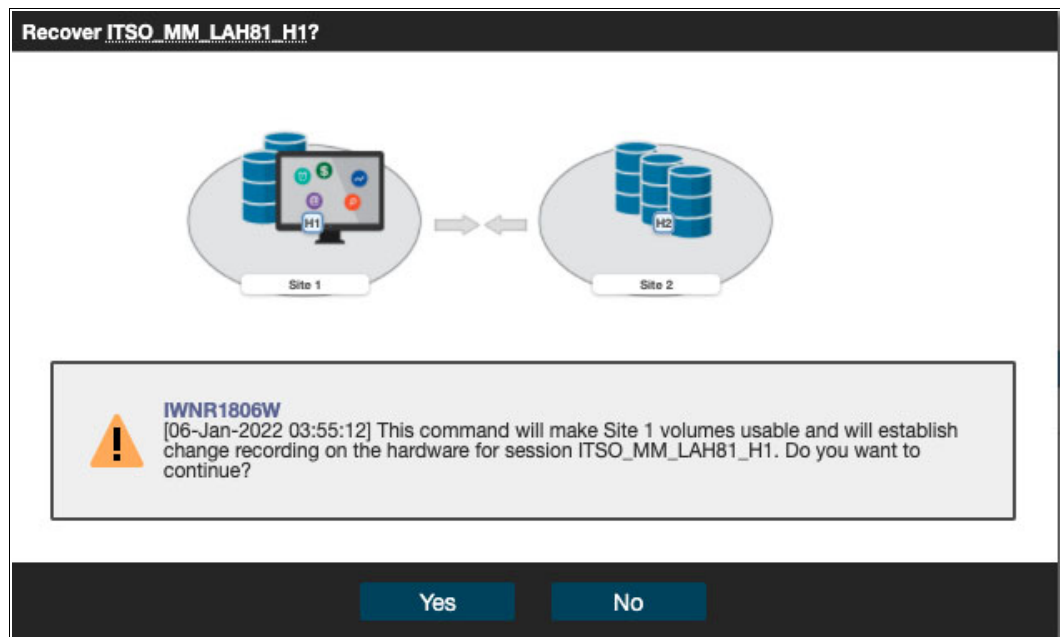


Figure 4-116 Confirming the Recover action

22. After the **Recover** action is completed, the MM session status changes to Normal, and its state is Target Available (see Figure 4-117).

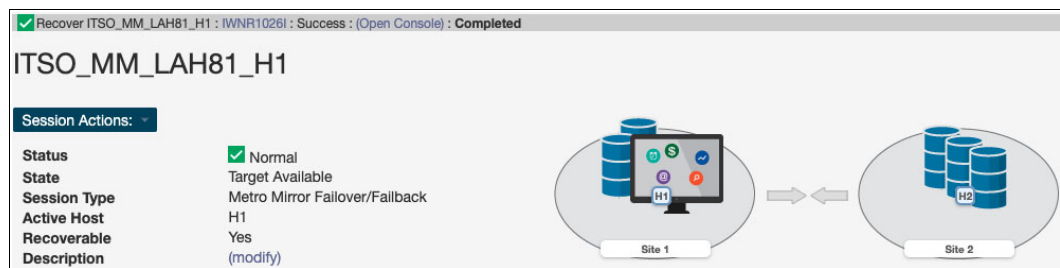


Figure 4-117 MM session in the Target Available state

23. To complete the failover and start production from the H1 volumes, from the **Session Actions** menu, select **Command** → **Enable Copy to Site 2** (as shown in Figure 4-118). This action is required to use **Start H1-H2**.

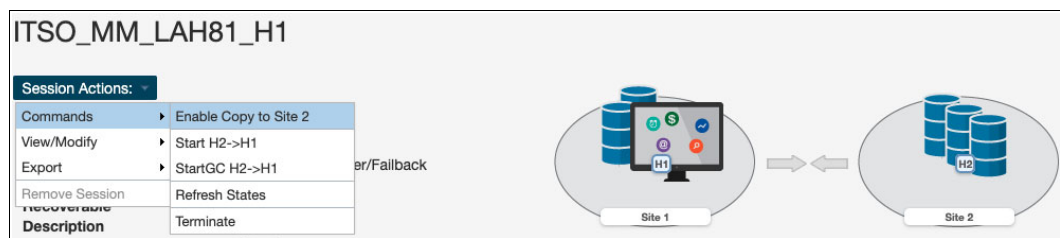


Figure 4-118 Enable Copy to Site 2

24. Click **Yes** to confirm **Start H1-H2** enablement (see Figure 4-119 on page 197).

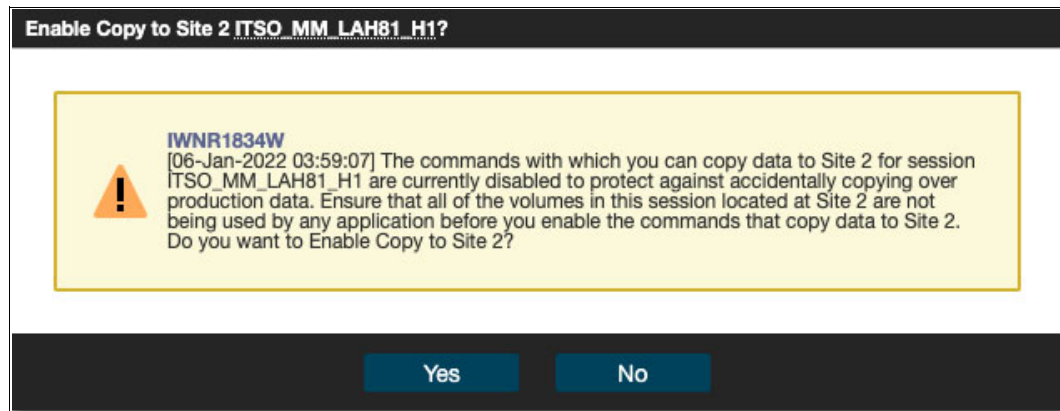


Figure 4-119 Confirming Start H1-H2 enablement

25. Start replication by going to the **Session Actions** menu and selecting **Command** → **Start H1-H2** (see Figure 4-120).

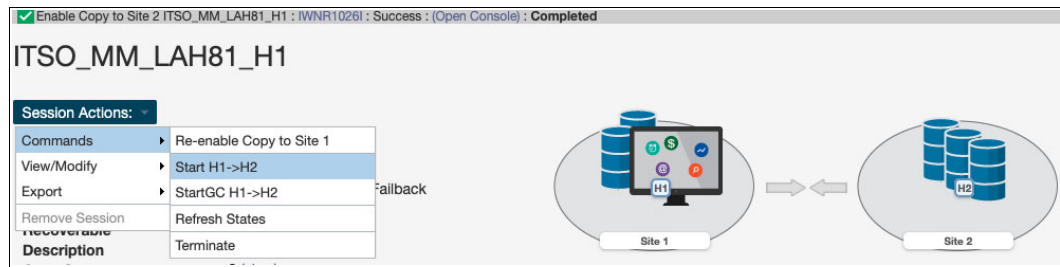


Figure 4-120 Start H1-H2

26. Click **Yes** to start replication from the H1 to H2 volumes (see Figure 4-121).

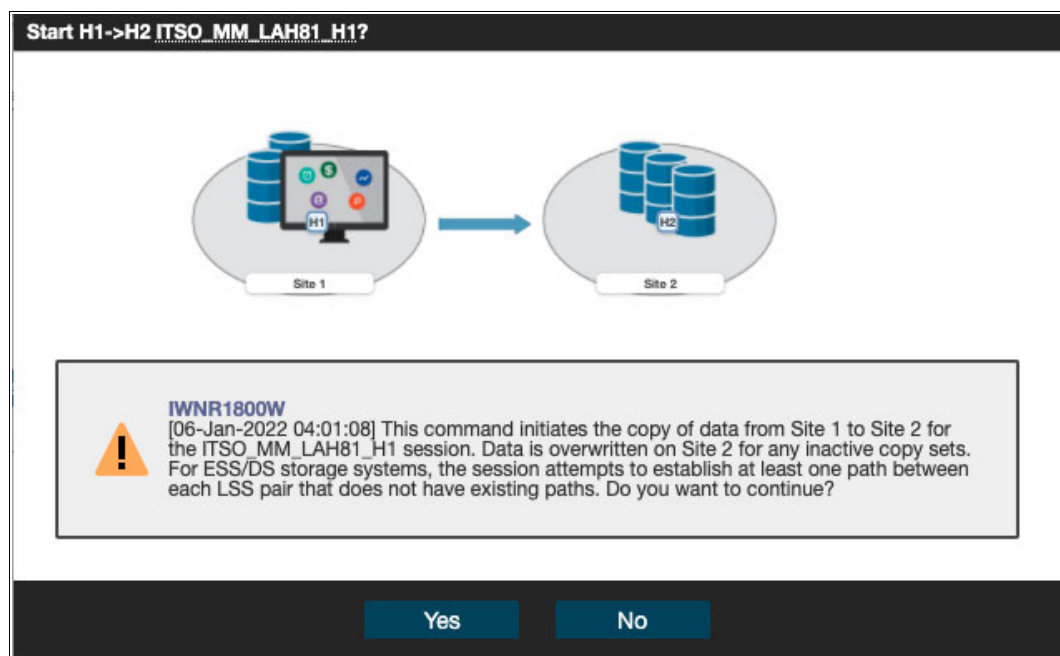


Figure 4-121 Confirming replication from the H1 to H2 volumes

27. As shown in Figure 4-122, the MM session status is Normal and the state is Prepared.

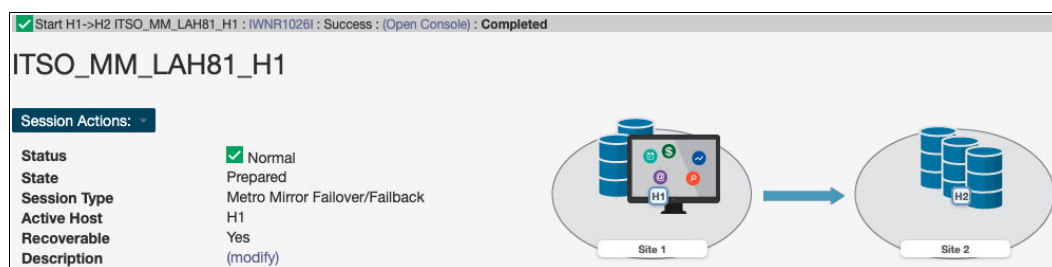


Figure 4-122 Metro Mirror replication restored

The replication direction is from H1 to H2 volumes, as it was before you initiated the whole process of restoring Safeguarded Copy backup. You can start your production workloads from H1 volumes.

4.3.5 Restoring a backup to production from H1 in a Multi-Target Metro/Global Mirror session

The steps that are described in this section are applicable for restoring a Safeguarded Copy backup from the primary H1 volume to the secondary H2 volume and replicate it back to the primary (H1) volume in a Multi-Target (MT) MM-GM topology / session.

In this example, we use the following sessions:

- ▶ ITSO_MT-MM-GM_LAH81_ACA91 - production MM session:
 - H1 MM primary volumes and GM primary volumes
 - H2 MM secondary volumes
 - H3 GM secondary volumes
- ▶ ITSO_SGC_LAH81 - Safeguarded Copy session:
 - H1 Safeguarded Copy source volumes, but also H1 MM primary and GM primary volumes that are defined in ITSO_MT-MM-GM_LAH81_ACA91
 - R1 Recovery volumes

Before we show each step in detail, here is a summary with the required steps to restore a backup to production from H1 volumes in an MT-MM-GM session:

1. Associate the Safeguarded Copy session with the MT-MM-GM session to be restored.
2. If you established a Safeguarded Copy Scheduled Task for the session and want to initiate a restore, you might disable this task to avoid extra Safeguarded Copy backups.
3. Use **Recover Backup** for the Safeguarded Copy session, and then select the required backup.
4. Perform data analysis on the recovery system.
5. Stop production applications (if not already done).
6. Suspend the associated MT-MM-GM session.
7. Use **Restore to production** from the Safeguarded Copy session.
8. Use **Start H2>H1** from the MT-MM-GM session.
9. Fail over or fail back the MM leg to start the production workload from H1 volumes and restore the original replication directions for the MT-MM-GM session.

To restore the R1 volumes to the H1 production MM primary volumes, complete the following steps:

1. Create a Safeguarded Copy session association with an MM session by selecting **View/Modify** → **Session Associations** → **Add/Update Association**, as shown in Figure 4-123.

Note: The association of the Safeguarded Copy session with the corresponding replication session can be done anytime before starting the restore to production process. However, a best practice is to create the association during the process of configuring the Safeguarded Copy session.

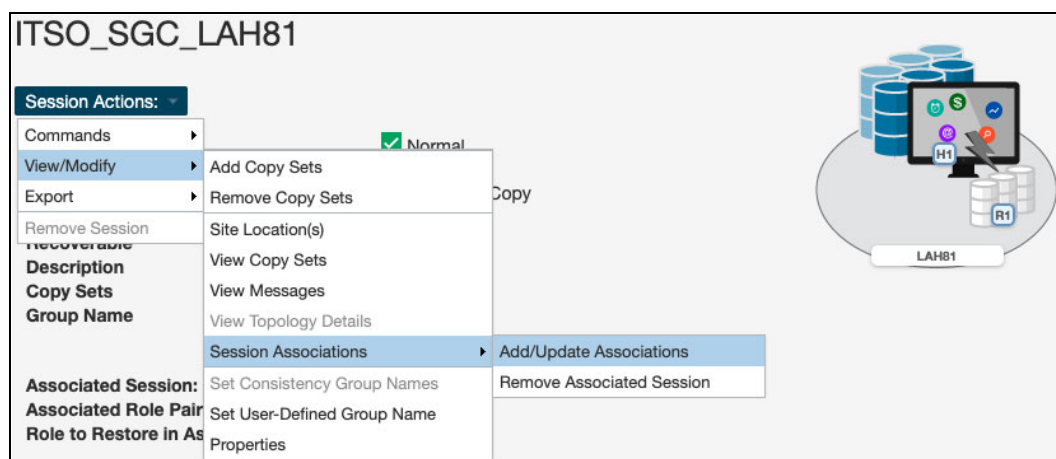


Figure 4-123 Creating a Safeguarded Copy session association

2. In Figure 4-124, select the session that you want to associate to this Safeguarded Copy session. Also, specify the session volumes role pair and specific volume role.

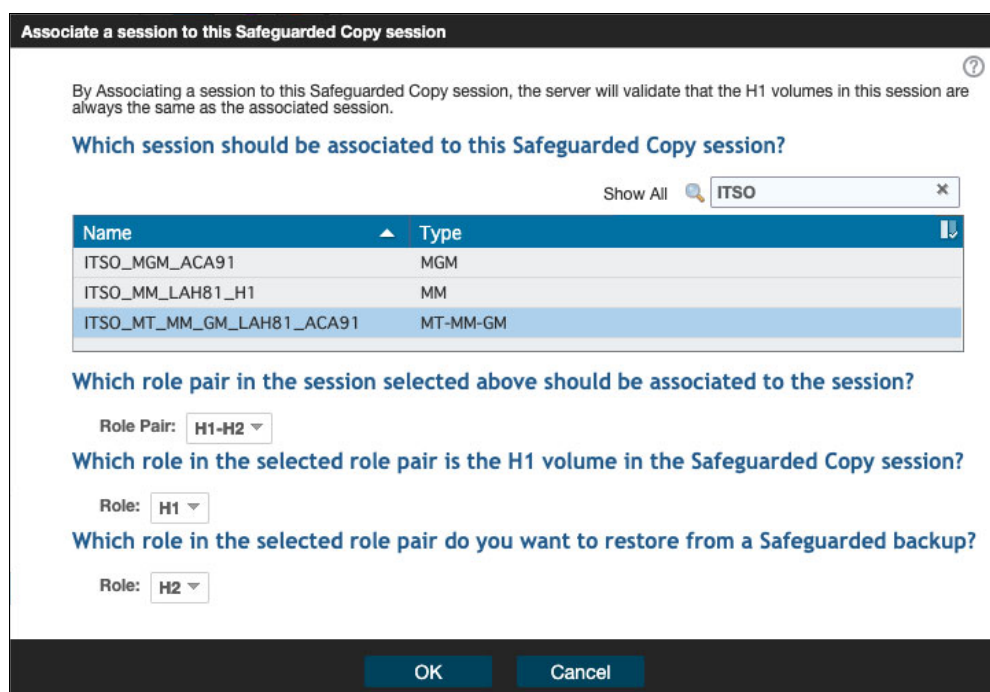


Figure 4-124 Associate a session to this Safeguarded Copy session

Use the filter to narrow the list of sessions. In our example, we associated the MM session ITSO_MM_LAH81_H1 and selected the **H1-H2** Role Pair.

- Choose which of the previously selected role pair volumes will be the Safeguarded Copy source volumes. Because the Safeguarded Copy in our example is taken from the MM primary volumes, the answer to “Which role in the selected role pair is the H1 volume in the Safeguarded Copy session?” is H1.

The role selection for the last question “Which role in the selected role pair do you want to restore from a Safeguarded backup?” in our example is H2 because you cannot restore the backup to the Safeguarded Copy source volume (see Figure 4-124 on page 199).

- Start backup recovery to the recovery volumes. From the Safeguarded Copy **Session Actions** menu, select **Commands**, and then click **Recover Backup**, as shown in Figure 4-125.

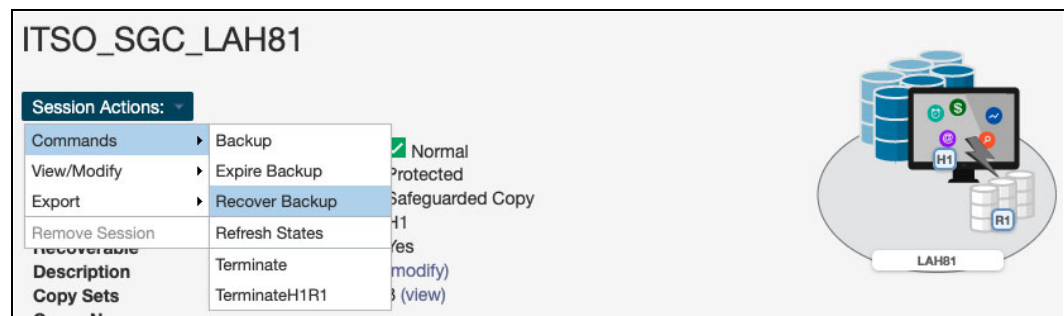


Figure 4-125 Recover Backup

- The new window includes a list of all available backup versions. Select the required backup and click **Yes** to start the backup recovery to the recovery volumes (see Figure 4-126).

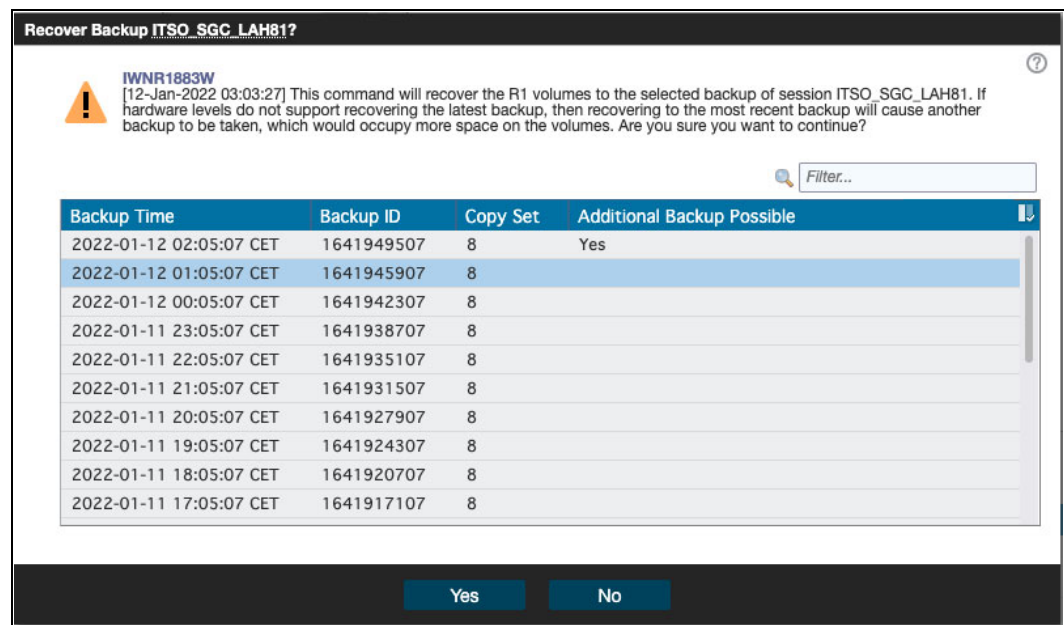


Figure 4-126 Selecting the required backup version

- Wait for the IWN1026I message, which indicates that **Recover Backup** completed successfully (see Figure 4-127 on page 201).

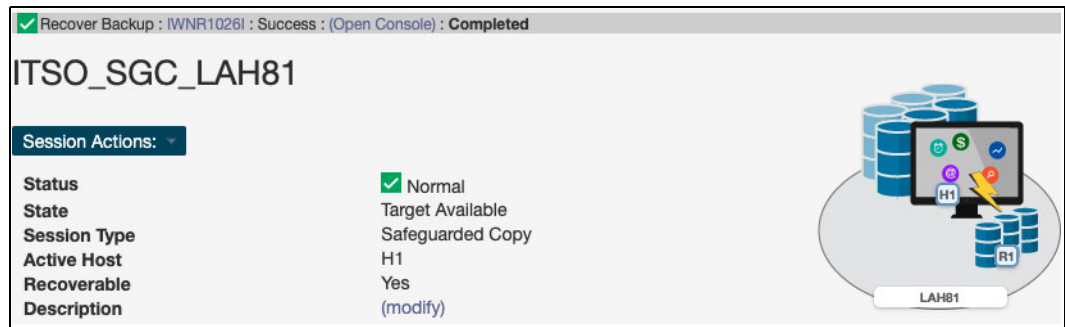


Figure 4-127 Recover Backup completed

At this stage, you can start validating data from the recovery system. If the data in this backup version is still corrupted, you can end the H1-R1 relationship (click **Terminate H1-R1**) and recover another backup version (starting at step 4 on page 200).

Important: Before proceeding to the next step, continue validating backup versions until you find the version that is not corrupted. Ensure that your production applications are not running (no I/Os to production volumes) before you click **Restore Backup**, as described in the next steps.

Also, all changes that are made during the validation process on recovery volumes are lost and not restored to the production volumes.

7. In the CSM Sessions window, select the associated replication session. In our example, which is shown in Figure 4-128, we used the ITSO_MM_LAH81_H1 MM session. Select **Session Actions** → **Commands** → **Suspend**.

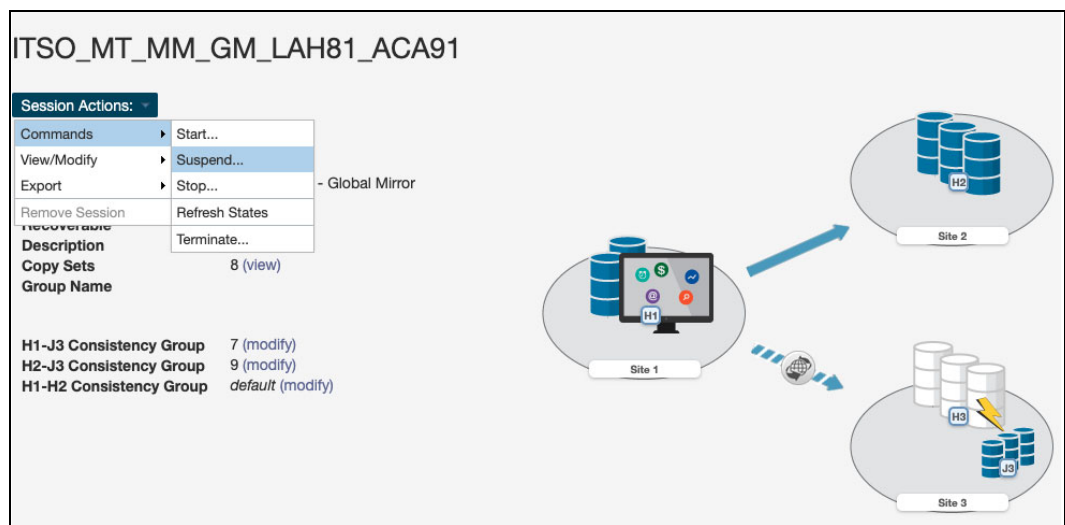


Figure 4-128 Suspending the associated session

8. Make sure that you suspend both legs and click **Yes** to continue (see Figure 4-129).

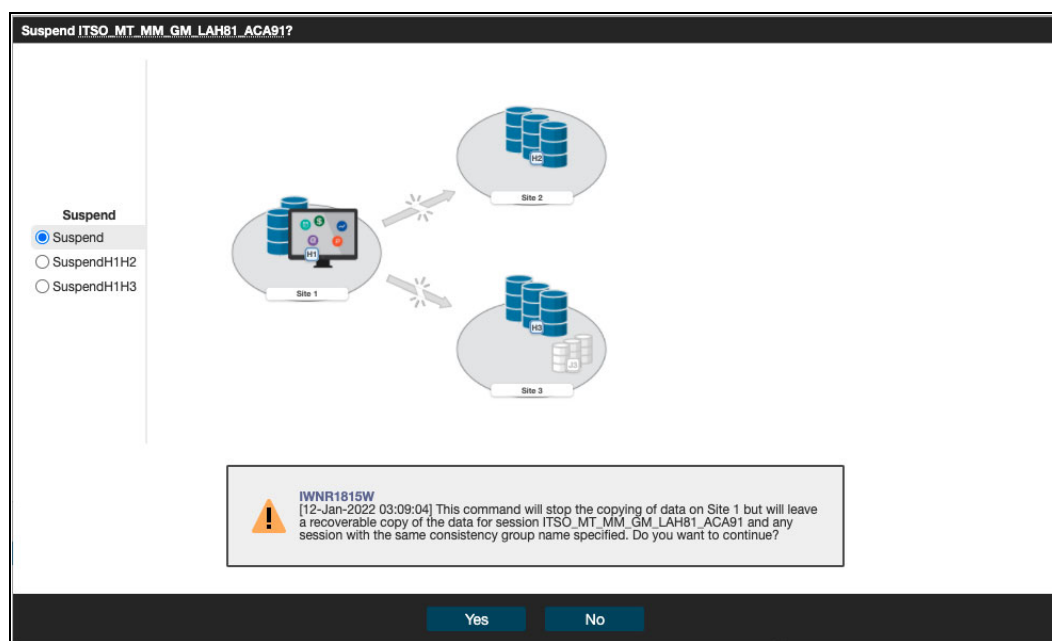


Figure 4-129 Confirming Suspend

9. Return to the Safeguarded Copy session. In our example, the session is ITSO_SGC_LAH81. Select **Session Actions** → **Restore Backup to Production** (see Figure 4-130).

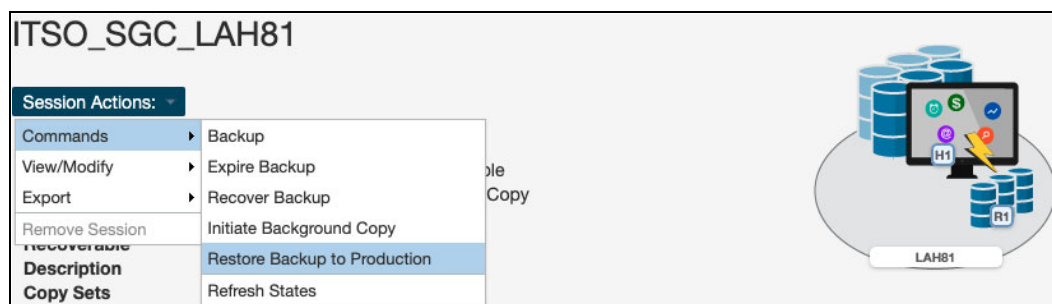


Figure 4-130 Safeguarded Copy Restore Backup

10. A confirmation window opens. Click **Yes** to continue (see Figure 4-131).

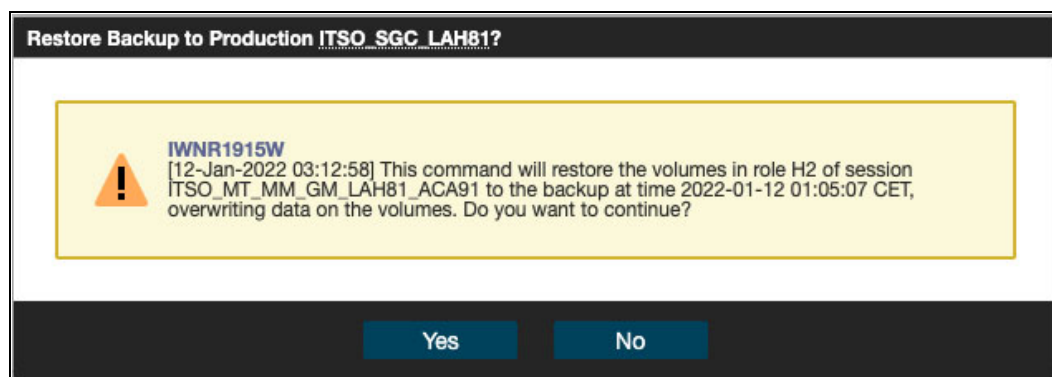


Figure 4-131 Confirming Restore Backup

11. The Safeguarded Copy session State changes to Restoring, as shown in Figure 4-132. In the Detailed Status section, you can monitor the restore progress.

Figure 4-132 Restore Backup completed

[illegible]

Figure 4-133 Restore Backup to production volumes completed

12. After the Safeguarded Copy restore to the H2 volumes is completed, the ITSO_MT-MM-GM_LAH81_ACA91 MT MM-GM session is still suspended. As shown in Figure 4-134, the MM leg has replication direction arrows pointing to each other, meaning that you may recover either H1 or H2 volumes and start replication from either direction.

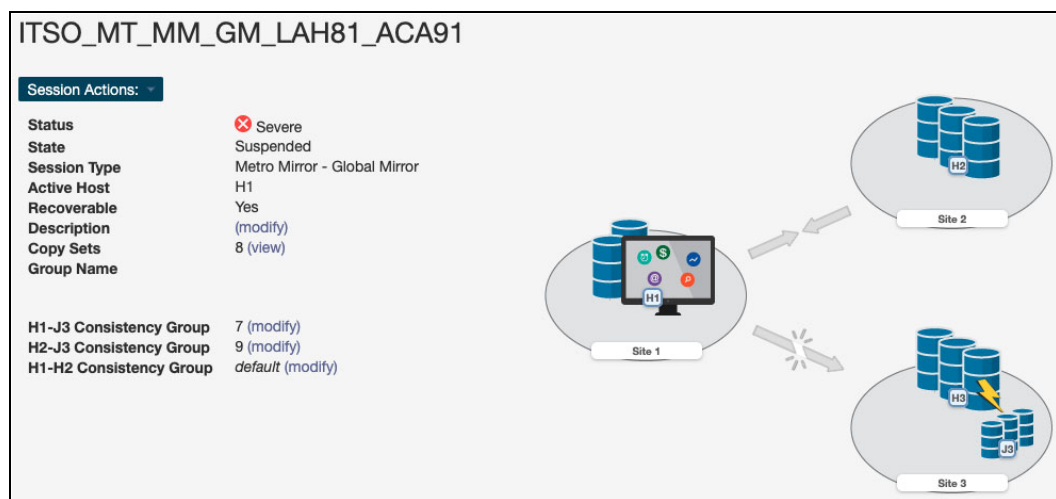


Figure 4-134 Suspended MT MM-GM session

13. Now that the Safeguarded Copy is restored successfully to the H2 MM secondary volumes and before you start replication from H2 to H1, shut down all systems and applications on the primary H1 volumes. Select **Session Actions** → **Commands** → **Recover** for the MT MM-GM session, as shown in Figure 4-135.

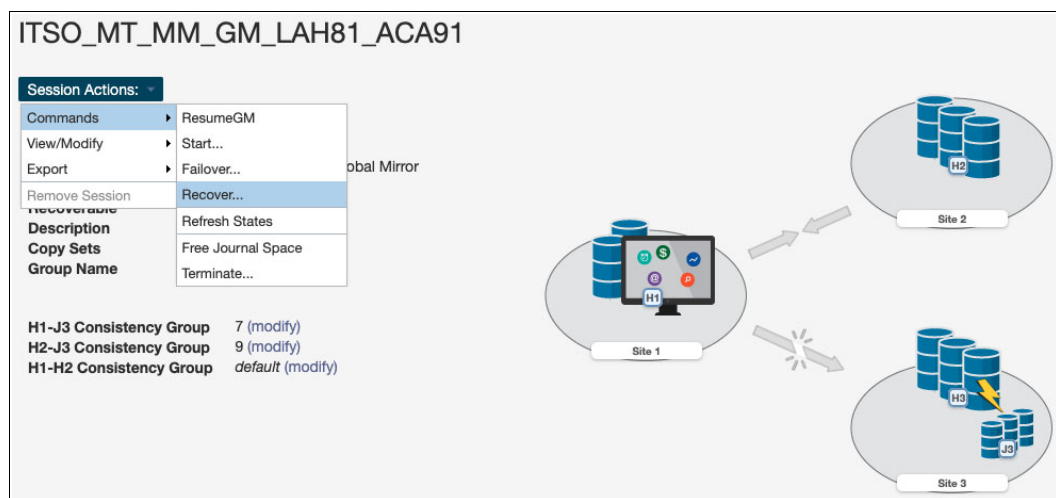


Figure 4-135 Recovering the H2 volume in an MT MM-GM session

14. Click **Recover H2** and click **Yes** to continue (see Figure 4-136 on page 205).

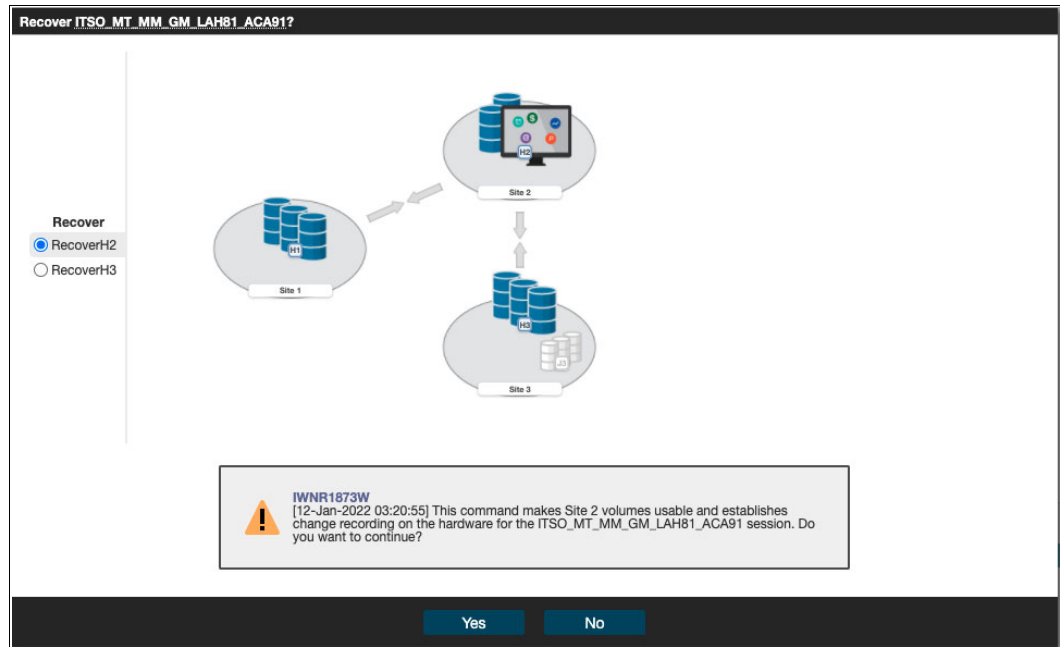


Figure 4-136 Confirming the recovery of H2

15. The MT MM-GM session changes to the Target Available state, as shown in Figure 4-137.

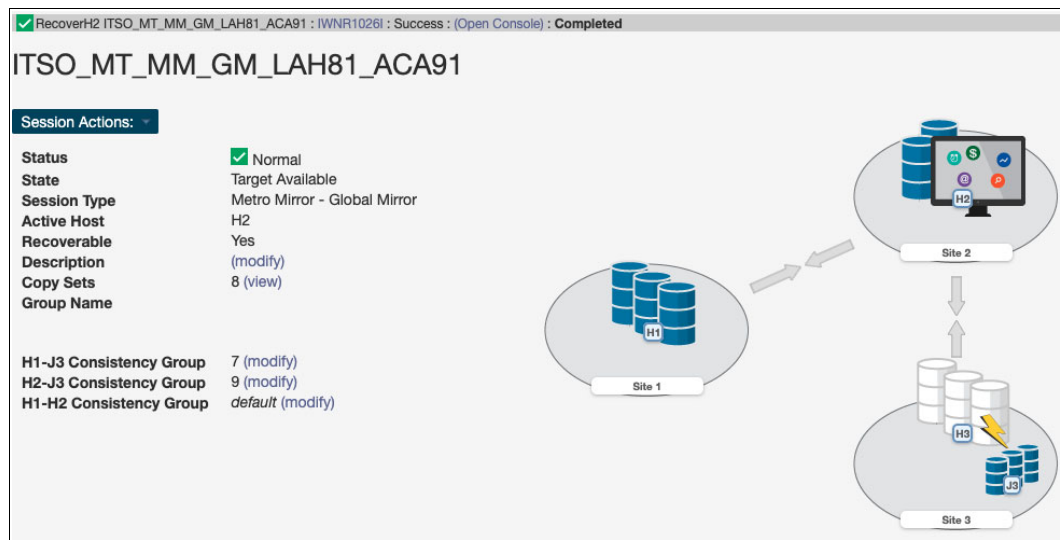


Figure 4-137 MT MM-GM in the Target Available state

16. Before you start replication from H2 to H1, shut down all systems and applications on the primary H1 volumes.

To enable **Start H2-H1**, select **Session Actions** → **Commands** → **Confirm Production at Site 2**, as shown in Figure 4-138.

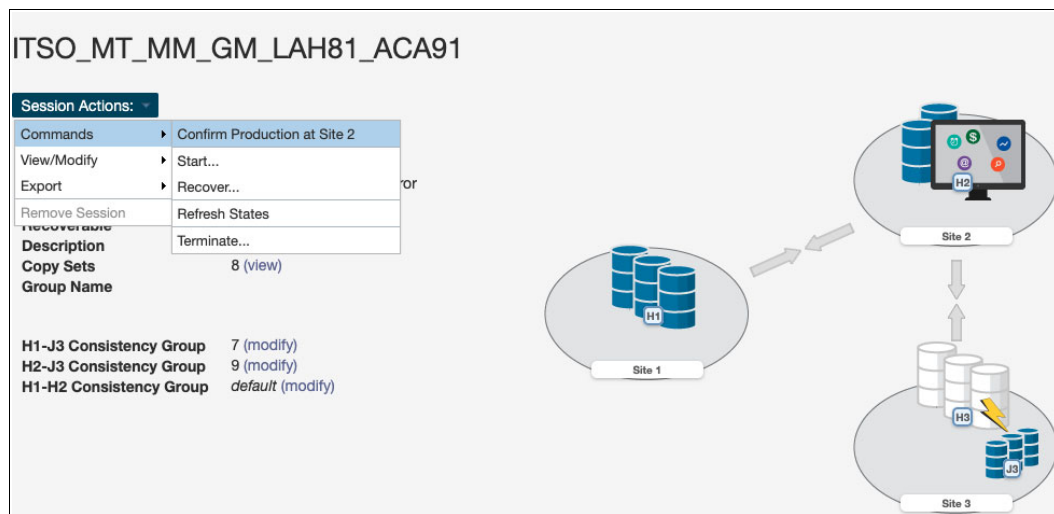


Figure 4-138 Confirm Production at Site 2

17. The window that is shown in Figure 4-139 is a confirmation to enable **Start H2-H1**.

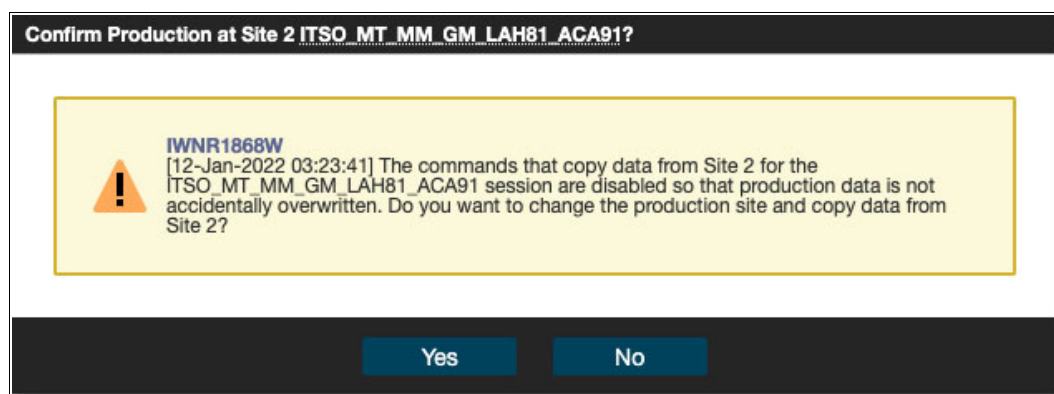


Figure 4-139 Confirm Production at Site 2

18. To start replicating the restored Safeguarded Copy data from H2 volumes to H1 volumes, select **Session Actions** → **Commands** → **Start** (Figure 4-140 on page 207). This action starts an incremental resync.

Note: Before you use **Start H2-H1**, consider the following extra steps:

- ▶ Perform an IPL from the H2 volumes and validate the environment before using **Start H2-H1**.
- ▶ Considering that at least all tracks that were restored from R1 to H2 will be resynchronized from H2 to H1 and stored in your open Safeguarded Copy backup, that process might use significant extra capacity. Depending on your requirements, you might expire all Safeguarded Copies and stop Safeguarded Copy before you use **Start H2-H1**.

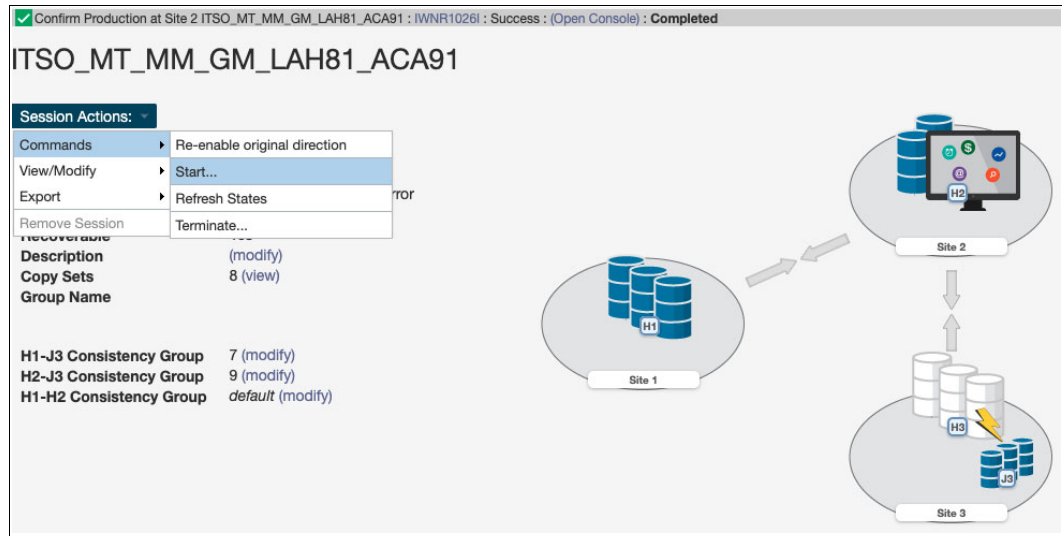


Figure 4-140 MT MM-GM: Start command

19. Select **Start H2->H1** and click **Yes** to continue (see Figure 4-141).

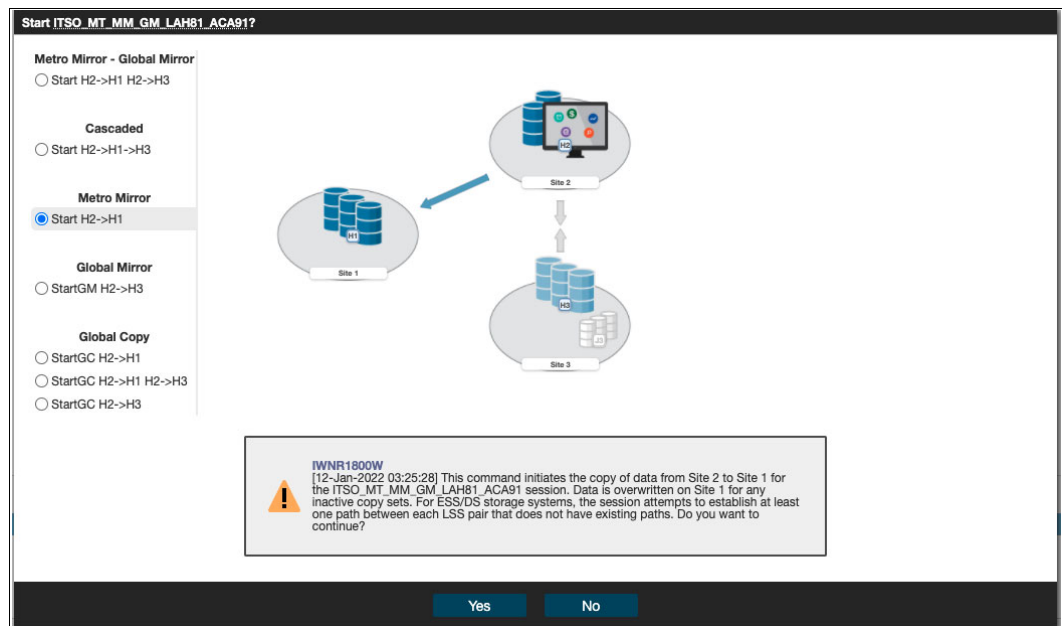


Figure 4-141 Start H2->H1

20. After the resynchronization between H2 and H1 volumes is completed, the session status is Severe and the state is Suspended (Partial) because the GM leg is still suspended (see Figure 4-142).

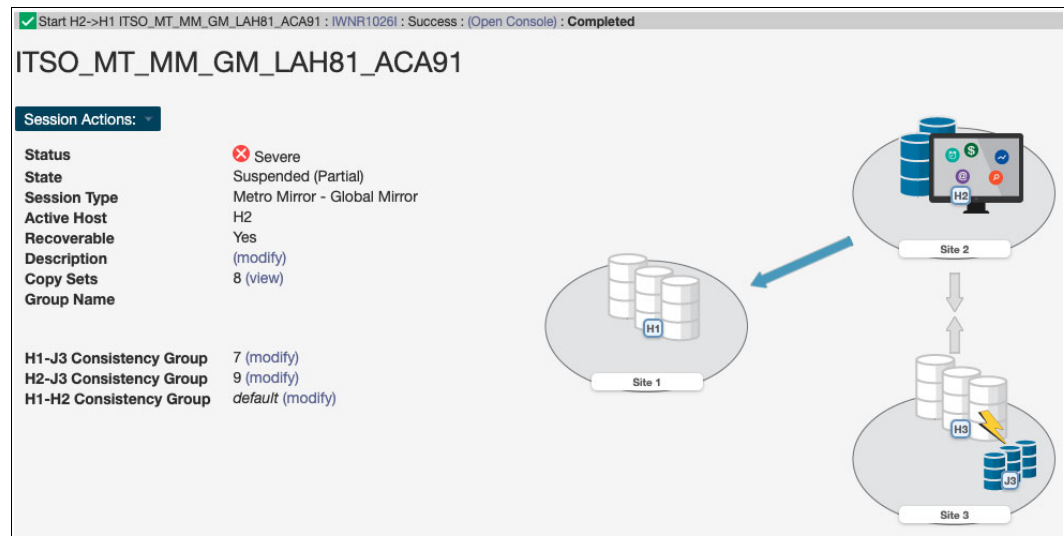


Figure 4-142 MT MM-GM session is Suspended (Partial) with H1 and H2 volumes fully synchronized

21. The next few steps are required to fail over the MM leg and start the production applications from the H1 volumes. Select **Session Actions** → **Commands** → **Suspend** (Figure 4-143).

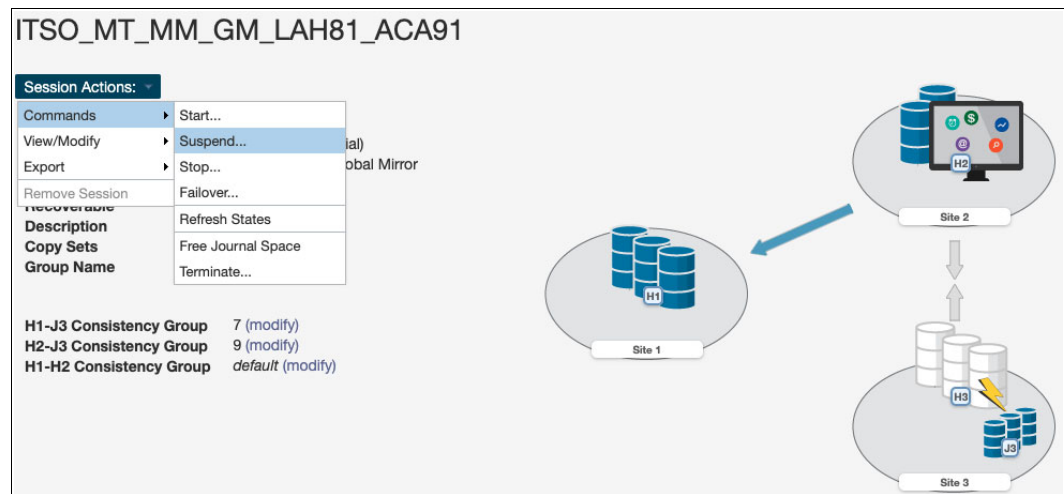


Figure 4-143 Suspending the MT MM-GM session

22. Confirm **SuspendH2H1** and click **Yes** to continue (see Figure 4-144 on page 209).

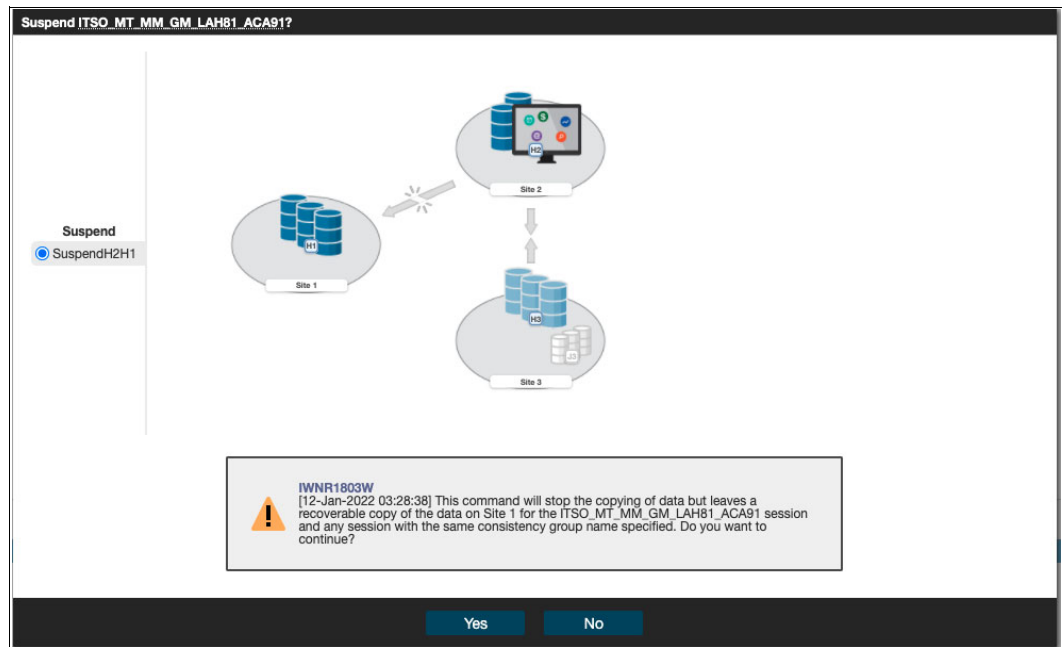


Figure 4-144 Confirming the suspension for the Metro Mirror session

23. The session status is Severe and the state is Suspended, as shown in Figure 4-145.

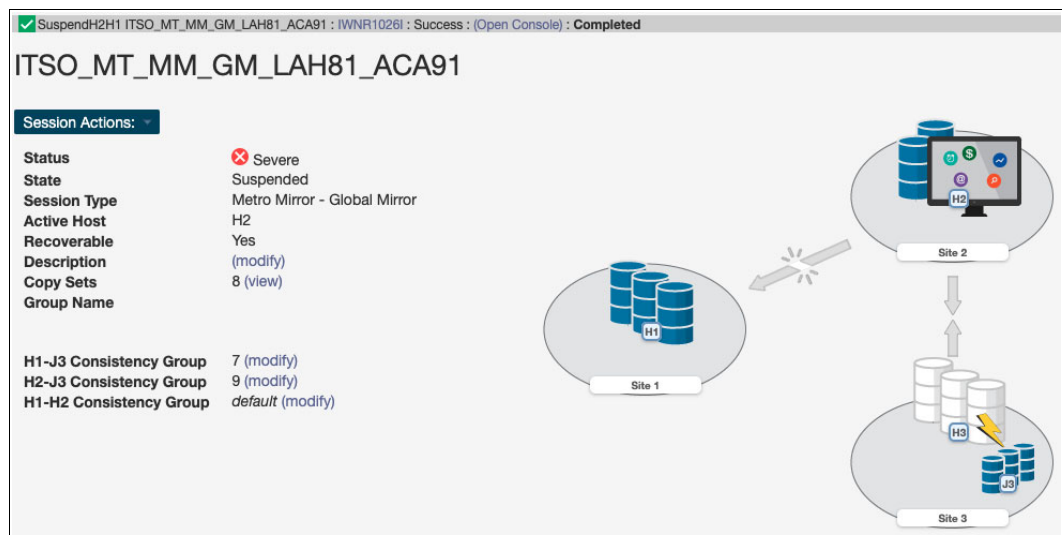


Figure 4-145 MT MM-GM session in the Severe status and the Suspended state

24. Select **Session Actions** → **Command** → **Recover** (see Figure 4-146).

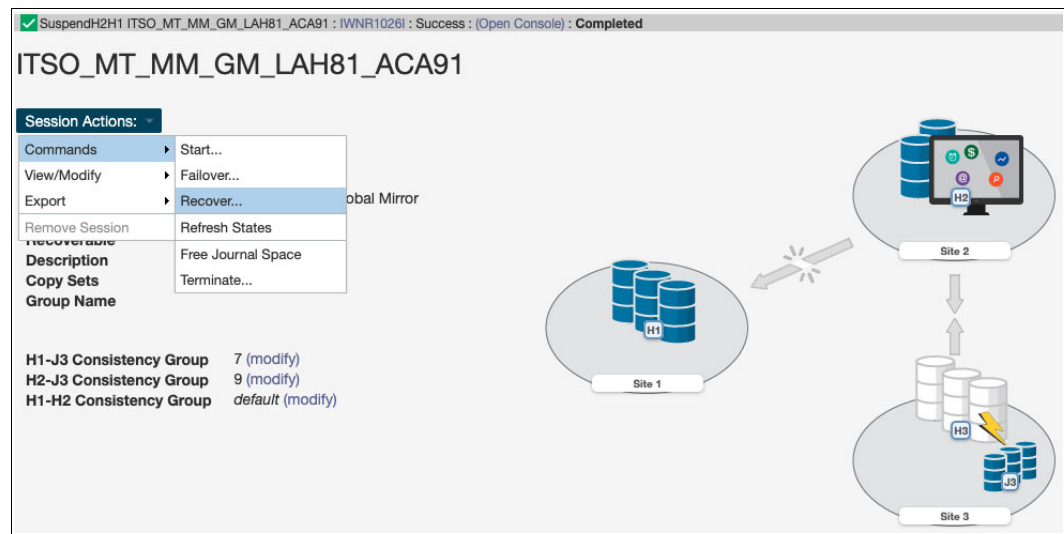


Figure 4-146 Recovering the MM session

25. Select **RecoverH1** and click **Yes** to continue (see Figure 4-147).

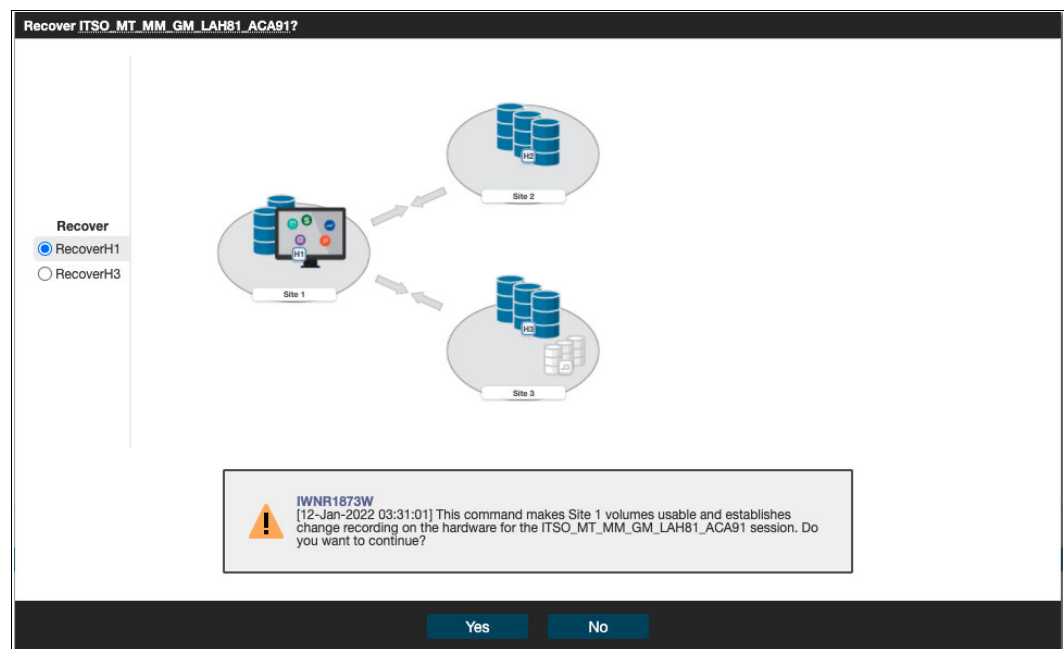


Figure 4-147 Confirming RecoverH1

26. After the recovery is completed, the session status changes to Normal and the state is Target Available (see Figure 4-148 on page 211).

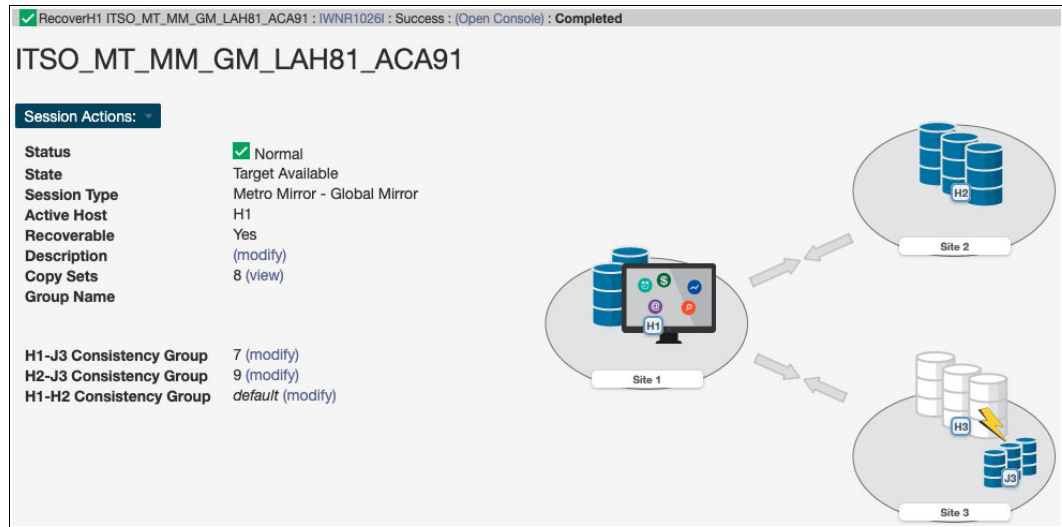


Figure 4-148 MT MM-GM session is in the Target Available state

27. To complete the failover and start production from the H1 volumes, select **Session Actions** → **Command** → **Confirm Production at Site 1** (as shown in Figure 4-149). This action is required to enable **Start H1-H2-H3**.

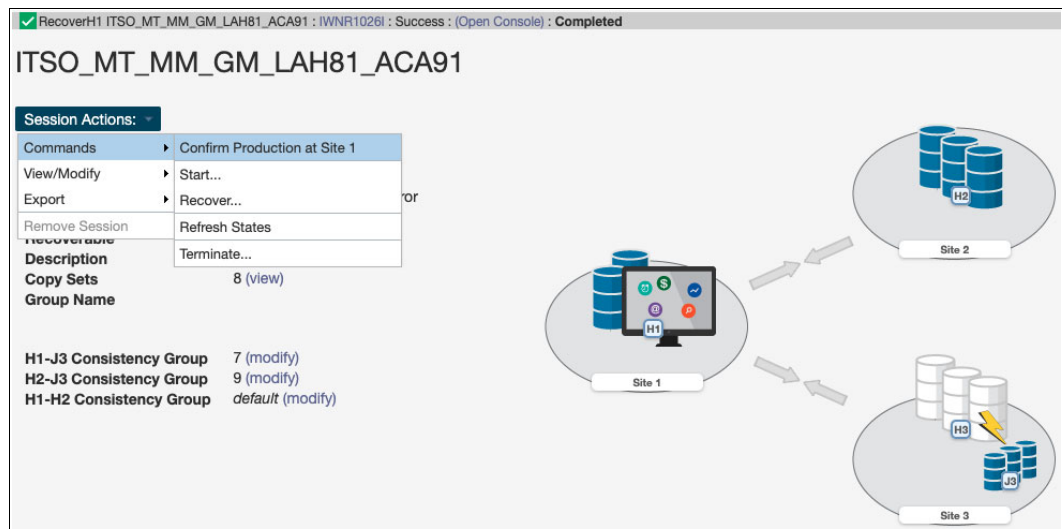


Figure 4-149 Confirm Production at Site 1

28. Click **Yes** to confirm **Start H1-H2-H3** enablement (see Figure 4-150).

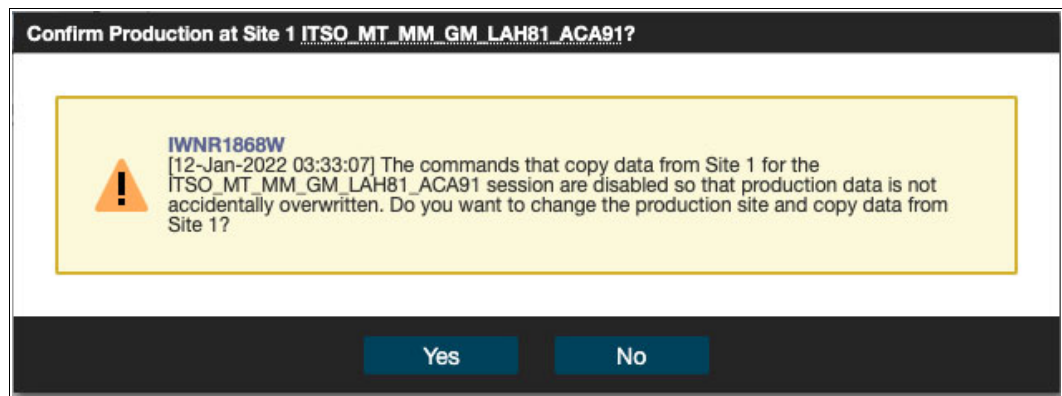


Figure 4-150 Confirm Production at Site 1

29. Start replication by selecting **Session Actions** → **Command** → **Start** (see Figure 4-151).

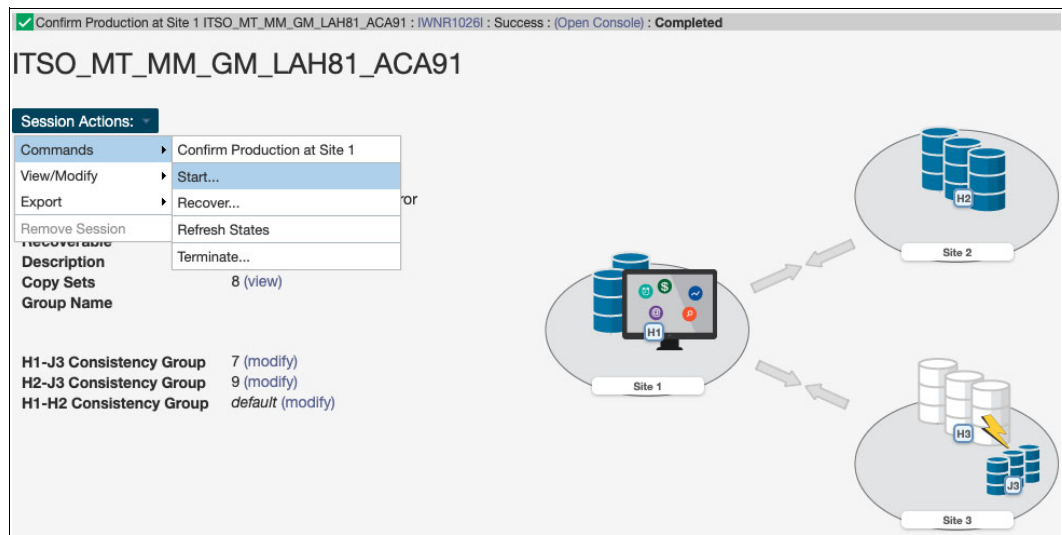


Figure 4-151 Starting the MT MM-GM session

30. Select **Start H1->H2 H1->H3** and click **Yes** to start replication from the H1 to H2 MM volumes, and from the H1 to H3 GM volumes (see Figure 4-152 on page 213).

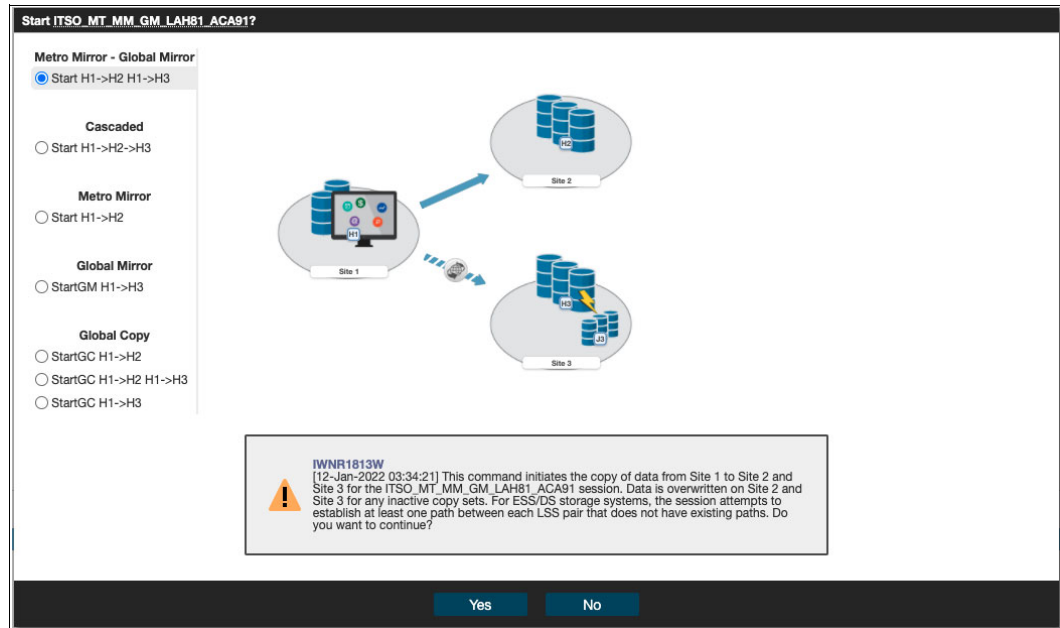


Figure 4-152 Starting replication for the MT MM-GM session

31.As shown in Figure 4-153, the MM session status is Normal and the state is Prepared.

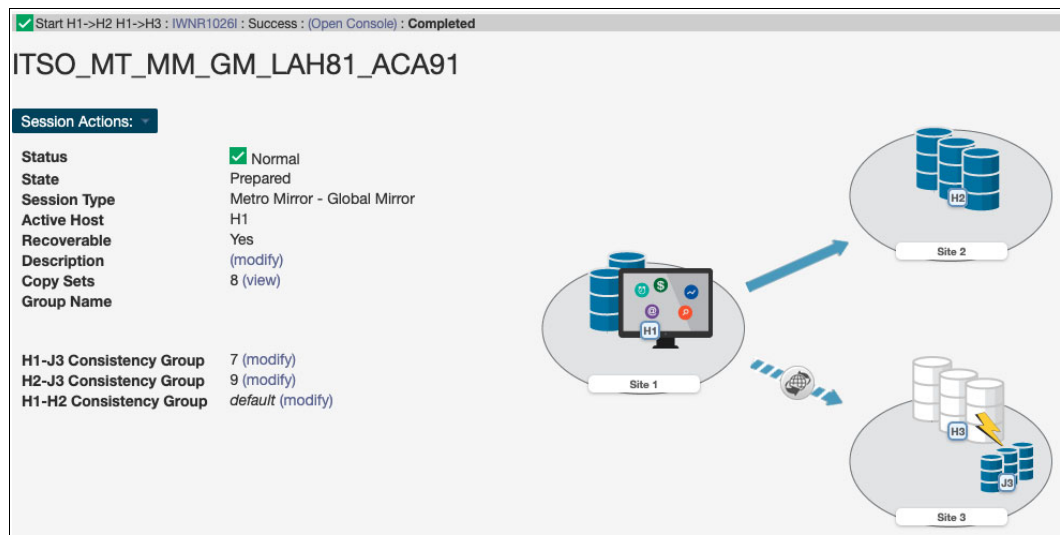


Figure 4-153 MT MM-GM session in the Normal status and the Prepared state

The replication direction is from H1 to H2 MM volumes and H1 to H3 GM volumes, as it was before you initiated the whole process of restoring Safeguarded Copy backup. You can now start your production workloads from the H1 volumes.

4.3.6 Restoring a backup to production for a Metro Mirror session with HyperSwap

In this section, we provide guidance about how to restore Safeguarded Copy backup into production volumes for MM sessions (2-site or 3-site with MT) after a HyperSwap event.

The following examples are included in this section:

- ▶ Restoring a backup to production from H2 after HyperSwap
- ▶ Restoring backup to production from H1 after HyperSwap

Restoring a backup to production from H2 after HyperSwap

This scenario describes a situation where logical corruption occurred after a planned HyperSwap event in an MM session, with Safeguarded Copy enabled on the H2 secondary MM volumes.

As shown in Figure 4-154, the production I/Os are on H1 volumes and the replication direction is from H1 to H2 with HyperSwap enabled.

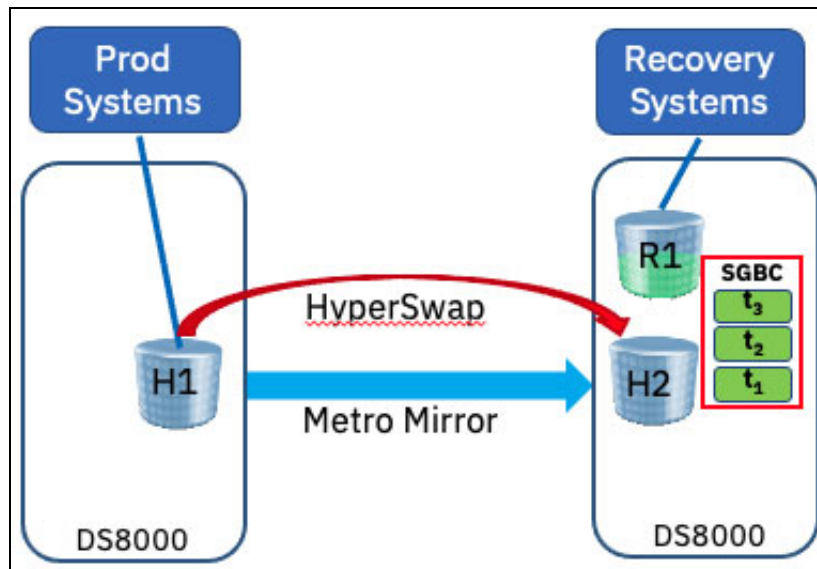


Figure 4-154 Metro Mirror with Safeguarded Copy on H2 volumes

After the planned HyperSwap is completed, the production system I/Os are on the H2 volumes, and the replication direction is from H2 to H1 volumes (as shown in Figure 4-155 on page 215).

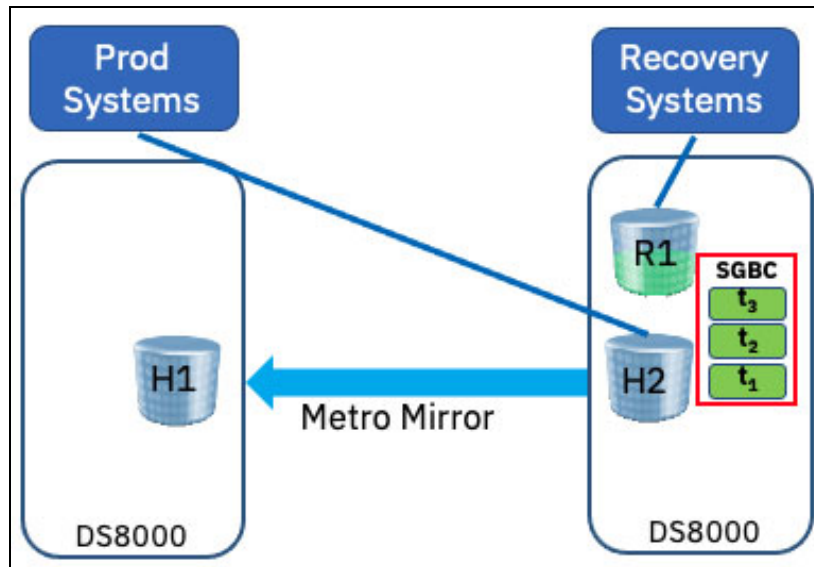


Figure 4-155 Planned HyperSwap with resync to the H1 volumes

If logical corruption is detected after the HyperSwap event, complete the following steps:

1. Find the closest backup before corruption.
2. Recover the backup to the R1 volumes.
3. Start validation from the recovery system (keep validating other backup versions if this one is not the correct version to restore to production).
4. Initiate the HyperSwap to the H1 volumes.
5. Follow the procedure that is described in 4.3.1, “Restoring a backup to production from H2 in an MM session” on page 162.

In an unplanned HyperSwap event, fix the HyperSwap trigger issue (for example, physical disk failure) and re-establish replication between the H2 and H1 volumes. Then, you can start with the restore backup to production volume procedure.

Restoring backup to production from H1 after HyperSwap

This scenario describes the situation when logical corruption occurred after a planned HyperSwap event in an MM session, with Safeguarded Copy enabled on the H1 secondary MM volumes.

As shown in Figure 4-156, the production I/Os are on H1 volumes and the replication direction is from H1 to H2, with HyperSwap enabled.

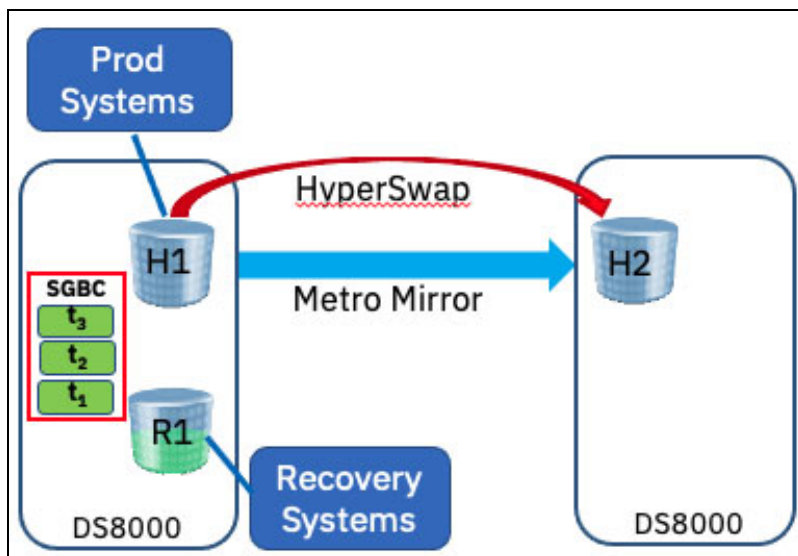


Figure 4-156 Metro Mirror with Safeguarded Copy on the H1 volumes

After the planned HyperSwap is completed, the production systems I/Os are on the H2 volumes, and the replication direction is from the H2 to H1 volumes (as shown in Figure 4-157).

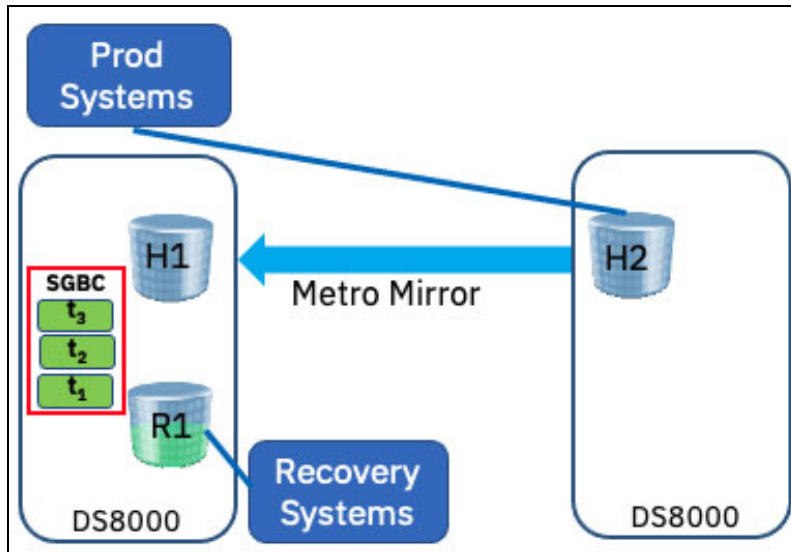


Figure 4-157 Planned HyperSwap with resync to H1 volumes

If logical corruption is detected after the HyperSwap event, complete the following steps:

1. Find the closest backup before corruption.
2. Recover the backup to the R1 volumes.
3. Start validation from the recovery system (keep validating other backup versions if this one is not the correct version to restore to production).

4. Initiate the HyperSwap to the H1 volumes.
5. Follow the procedure that is described in 4.3.4, “Restoring a backup to production from H1 in an MM session” on page 187.

In an unplanned HyperSwap event, fix the HyperSwap trigger issue (for example, physical disk failure) and re-establish replication between the H2 and H1 volumes. Then, you can start with the restore backup to production volume procedure.

4.4 Scheduled tasks examples with Safeguarded Copy topologies

As explained in 2.2, “HA, DR, and HADR with Safeguarded Copy topologies” on page 23, the Safeguarded Copy integrates with various DS8000 HA, DR, and HADR solutions.

In this section, we provide some scheduled tasks examples when Safeguarded Copy is associated with 2-Site and 3-Site HADR solutions:

- ▶ Two sites:
 - MM
 - GM
- ▶ Three sites:
 - Cascaded GM (two CSM sessions)
 - MGM
 - MT MM-MM
 - MT MM-GM

Note: CSM features the following 4-Site session types:

- ▶ MT MM-MM and cascaded GC from one MM leg
- ▶ MT MM-GM and cascaded GC from GM leg

The following 4-Site topologies are a combination of two CSM session types:

- ▶ MT MM-MM + cascaded GM session from one MM leg
- ▶ MT MM-GM + cascaded GM session from either MM or GM leg
- ▶ MGM + cascaded GM session

Therefore, when scheduling tasks for any of the 4-site topologies, refer to the two and three site topology examples that are provided in this chapter and combine them by specifying the correct session and role pair commands.

The use of the CSM Scheduler makes sense, especially if you manage your current HADR environment with CSM and you might need to coordinate this session with a Safeguarded Copy session to create a consistent backup.

Safeguarded Copy copies that are taken from MM or GM primary volumes are consistent and do not require any further action on the MM or GM session.

However, to take a consistent backup from GM secondary volumes, you must pause the GM session with consistency (suspend GM), and then take the Safeguarded Copy backup. Finally, resume the GM session.

Unlike GM secondary volumes, MM secondary volumes always are in a full duplex state with primary MM volumes; therefore, the MM session does not need to be suspended. However, in some situations, the MM session state can change to Suspending or Preparing, which causes potential data consistency exposure of secondary MM volumes. With CSM Scheduled Tasks, you can check the MM session state before you take a Safeguarded Copy backup.

In addition, CSM Scheduler can call an external script from your application server. For example, you might run a script to quiesce an application before taking a Safeguarded Copy backup.

As shown in Figure 4-158, after you create a scheduled task, in the Add Action window, select **Type** → **Run External Script**. In this window, you must provide the server host name or IP address with the credentials that will be used to create the SSH connection to the server that is specified by the Hostname field.

The screenshot shows a dialog box titled "Add Action" with a question mark icon in the top right corner. The dialog is divided into several sections, each with a blue header:

- What action will the task perform?**: A dropdown menu labeled "Type:" is set to "Run External Script".
- What hostname and port should we connect to via SSH?**: Two input fields. The "Hostname" field has a red asterisk (*) and is empty. The "Port (optional)" field is empty.
- What userid and password should be used?**: Two input fields. The "Userid" field has a red asterisk (*) and is empty. The "Password" field is empty.
- What command should be issued through SSH?**: A single input field labeled "Command" with a red asterisk (*) and is empty.
- How long should the action wait before timing out?**: A single input field labeled "Time (minutes):" with the value "5".
- What string in the command output will indicate a successful completion? (optional)**: A single input field labeled "Success string" is empty.

At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Figure 4-158 Run External Script from CSM scheduled task

Optionally, you can specify the time (in minutes) for the action to wait before timing out in addition to the success string value that can be used to determine whether the command ran successfully. If a success string is not specified, then the command is considered successful, and CSM continues with the actions in the scheduled task.

4.4.1 Metro Mirror with Safeguarded Copy

Scheduling a task for Safeguarded Copy from the H1 MM primary volume is simple and requires only one action: use **Backup**.

However, when H2 MM secondary volumes are Safeguarded Copy protected, you can include another task to check the session state. This inclusion might be done because some specific situations exist where H2 MM secondary volumes can change to the Pending state:

- ▶ A user suspends one or more volumes.

The CSM session is in the Suspending state (not fully suspended, and consistency across all volumes is not yet created).

- ▶ Remote Pair FlashCopy (RPFC) is not enabled.

Without RPFC enabled, MM secondary volumes move to Duplex Pending (or Secondary Pending) whenever the FlashCopy is taken to the MM primary volume. While in the Duplex Pending (Secondary Pending) state, the MM secondary volumes are not consistent with the MM primary volumes. Therefore, the MM session moves to the Preparing state.

To ensure that the Safeguarded Copy from MM secondary volumes is a consistent point-in-time copy, the session state must be Prepared before taking the Safeguarded Copy backup.

The following actions must be included in the CSM scheduled task with MM and Safeguarded Copy on MM secondary volumes:

1. Wait for Prepared state for MM session.
2. Use **Backup** on the Safeguarded Copy session.

Note: For Step 1, you can specify the wanted wait time (in minutes) before the task times out and fails. The default value is 60 minutes.

The scheduled task example for MM and Safeguarded Copy sessions is shown in Figure 4-159.

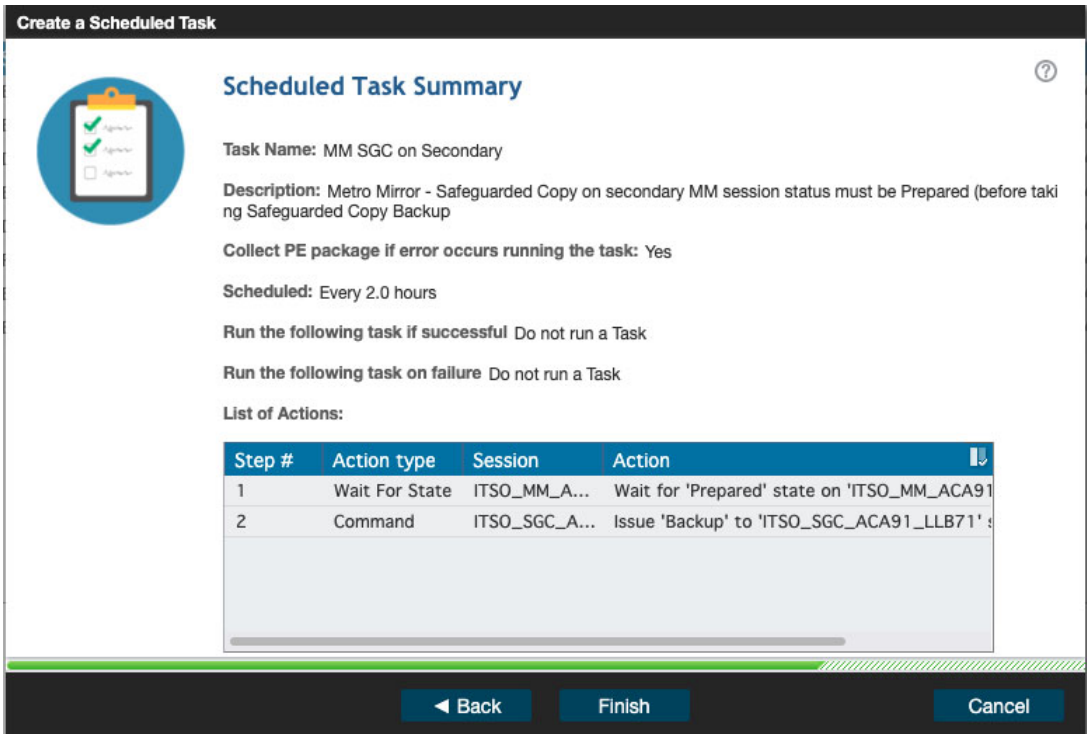


Figure 4-159 Metro Mirror and Safeguarded Copy scheduled task example

4.4.2 Global Mirror with Safeguarded Copy

Scheduling a task for Safeguarded Copy from the H1 GM primary volumes is simple and requires only one action: use **Backup**.

To take a consistent Safeguarded Copy backup from H2 GM secondary volumes, include the following actions in the Scheduled Task:

1. Pause the GM session with consistency (suspend the GM Session).
2. Wait until the GM Session is in the Suspended state; then, create a Safeguarded Copy backup by using **Backup**.
3. Restart GM session by using **Resume GM** or **Start H1-H2**.

Note: For step 2, you can specify the wanted wait time (in minutes) before the task times out and fails. The default value is 60 minutes.

Resume GM is available on CSM 6.2.10 and later. It is more suitable as it is used after a brief session suspension. If a long suspension occurred or **Recover** is used after suspension, use **Start H1-H2** instead.

An example of such a scheduled task is shown in Figure 4-160.

Modify a Scheduled Task

Scheduled Task Summary

Task Name: ITSO_SGC_LAH81_LLB71

Description: Global Mirror - Safeguarded Copy on GM secondary

Collect PE package if error occurs running the task: Yes

Scheduled: Every 2.0 hours

Run the following task if successful Do not run a Task

Run the following task on failure Do not run a Task

List of Actions:

Step #	Action type	Session	Action
1	Command	ITSO_GM_LA...	Issue 'Suspend' to 'ITSO_GM_LAH81_LLB71' s
2	Wait For State	ITSO_GM_LA...	Wait for 'Suspended' state on 'ITSO_GM_LAH8
3	Command	ITSO_SGC_L...	Issue 'Backup' to 'ITSO_SGC_LAH81_LLB71' s
4	Command	ITSO_GM_LA...	Issue 'ResumeGM' to 'ITSO_GM_LAH81_LLB71

◀ Back Finish Cancel

Figure 4-160 Scheduled Task example to coordinate a GM session with a Safeguarded Copy session

4.4.3 Cascaded Global Mirror with Safeguarded Copy

The cascaded GM with Safeguarded Copy topology often is used when physical isolation is required for Safeguarded Copy and it is suitable for customers that need more frequent backups. Therefore, a Safeguarded Copy copy is taken from the cascaded GM H2 secondary volumes. For more information about use case examples and planning, see Chapter 2, “Planning and considerations” on page 21.

The cascaded GM configuration consists of the following sessions:

- ▶ Production GM session: Production workload is on H1 volumes
- ▶ Cascaded GM session: H2 volumes that are physically isolated and protected with Safeguarded Copy

The H2 secondary volumes of the production GM session also are defined as cascaded H1 primary volumes of the cascaded GM session. Considering that Safeguarded Copy protects the H2 secondary GM volumes of the cascaded GM session, the association must be defined in the Safeguarded Copy session (as described in 4.3.3, “Restoring a backup to production from H3 in cascaded GM sessions” on page 176).

Although the CGs are regularly formed on the production GM session, the cascaded GM session forms a CG only after pausing with consistency the production GM session (suspend). Only then is the CG formed for the cascaded GM session and the Safeguarded Copy backup can be taken.

Note: In addition to Safeguarded Copy Backup Capacity planning, you must plan for the cascaded GM Journal volumes space if they are thin-provisioned (ESE). The GM Journal volumes space requirements depend on how frequently you suspend the production GM session to take the Safeguarded Copy backup. Therefore, this cascaded GM topology is more suitable for when more frequent Safeguarded Copy backups are needed.

The following steps are actions that are required to take the consistent Safeguarded Copy backup from H2 secondary volume of a cascaded GM session:

1. Suspend the cascaded GM session.
2. Suspend the production GM session.
3. Wait for the production GM to be suspended.
4. Wait for the cascaded GM to be suspended.
5. Resume the production GM session.
6. Use the Safeguarded Copy Backup action.
7. Resume the cascaded GM session.

Note: For steps 3 and 4, you can specify the wanted wait time (in minutes) before the task times out and fails. The default value is 60 minutes.

After steps 3 and 4 are complete, you can add a step to validate role pair consistency to ensure that the GM sessions are paused with consistency.

Figure 4-161 shows all actions that are required in a scheduled task for coordinating cascaded GM and Safeguarded Copy sessions.

Step #	Action type	Session	Action
1	Command	ITSO_CASCA...	Issue 'Suspend' to 'ITSO_CASCADE_GM_LAH8
2	Command	ITSO_GM_A...	Issue 'Suspend' to 'ITSO_GM_ACA90_LAH81'
3	Wait For State	ITSO_GM_A...	Wait for 'Suspended' state on 'ITSO_GM_ACA'
4	Wait For State	ITSO_CASCA...	Wait for 'Suspended' state on 'ITSO_CASCADE'
5	Command	ITSO_GM_A...	Issue 'ResumeGM' to 'ITSO_GM_ACA90_LAH8
6	Command	ITSO_CASCA...	Issue 'Backup' to 'ITSO_CASCADE_SGC_LAH8
7	Command	ITSO_CASCA...	Issue 'ResumeGM' to 'ITSO_CASCADE_GM_LAI

Figure 4-161 Scheduled Task example to coordinate a cascaded GM session with a Safeguarded Copy session

4.4.4 Metro/Global Mirror (cascaded) with Safeguarded Copy

MGM is a cascaded session. The H1 volume is the MM primary. H2 is the MM secondary, and because it is a cascaded volume, it is also a GM primary. H3 is a GM secondary.

Scheduling a task for Safeguarded Copy from the H1 MM primary volume is simple and it requires only one action: use **Backup**.

Therefore, in this section we provide two scheduled task examples:

- ▶ MM H2 secondary volumes are protected with Safeguarded Copy.
- ▶ GM H3 secondary volumes are protected with Safeguarded Copy.

MM H2 secondary volumes are protected with Safeguarded Copy

When H2 MM secondary volumes (cascaded volumes and also H1 GM primary volumes in MGM session) are Safeguarded Copy protected, you can include more tasks to check the session state. This addition is possible because some specific situations might exist when H2 MM secondary volumes might not be fully consistent:

- ▶ A user suspends one or more volumes.
The session is in the Suspending state (not fully suspended, and consistency across all volumes is not yet created).
- ▶ RPFC is not enabled.
Without RPFC enabled, MM secondary volumes move to Duplex Pending (or Secondary Pending) whenever the FlashCopy is taken to the MM primary volume. While in the Duplex Pending state, the MM secondary volumes are not consistent with the MM primary volumes. Therefore, the MM session moves to the Preparing state.

To ensure that the Safeguarded Copy from MM secondary volumes is a consistent point-in-time copy, the session state must be Prepared before taking the Safeguarded Copy backup.

The following steps can be included in the CSM scheduled task with MM and Safeguarded Copy on MM secondary volumes:

1. Wait for the Prepared state for the MM session.
2. Use **Backup** on the Safeguarded Copy session.

Note: For step 1, you can specify the wait time (in minutes) before the task times out and fails. The default value is 60 minutes.

The scheduled task example for MM and Safeguarded Copy sessions is shown in Figure 4-162.

Step #	Action type	Session	Action	
1	Wait For State	ITSO_MGM	Wait for 'Prepared' state on 'ITSO_MGM' session	
2	Command	ITSO_SGC	Issue 'Backup' to 'ITSO_SGC' session	

Figure 4-162 Scheduled task actions for Safeguarded Copy backup taken off MM secondary volumes

GM H3 secondary volumes are protected with Safeguarded Copy

To take a consistent Safeguarded Copy backup from H3 GM secondary volumes in an MGM session, the following steps must be included in the scheduled task:

1. Click **Suspend H2-H3** (GM leg only).
2. Wait until the GM leg is in the Suspended state.

Note: You can add a step to validate role pair consistency to make sure that the GM sessions are paused with consistency.

3. Create Safeguarded Copy backup by using **Backup**.
4. Restart GM leg by using **Start H2-H3**.

Note: For step 2, you can specify the wait time (in minutes) before the task times out and fails. The default value is 60 minutes.

An example of a scheduled task is shown in Figure 4-163.

Step #	Action type	Session	Action
1	Command	ITSO_MGM	Issue 'SuspendH2H3' to 'ITSO_MGM' session
2	Wait For State	ITSO_MGM	Wait for 'SuspendedH2H3' state on 'ITSO_MGM'
3	Command	ITSO_SGC	Issue 'Backup' to 'ITSO_SGC' session
4	Command	ITSO_MGM	Issue 'Start H2->H3' to 'ITSO_MGM' session

Figure 4-163 Scheduled task actions for Safeguarded Copy backup taken off GM Secondary volumes

4.4.5 Multi-Target Metro Mirror-Metro Mirror with Safeguarded Copy

A Multi-Target Metro Mirror-Metro Mirror (MT MM-MM) session consists of MM H1 primary volumes, MM H2 secondary volumes, and MM H3 secondary volumes.

Scheduling a task for Safeguarded Copy from H1 MM primary volumes is simple and it requires only one action: use **Backup**.

When H2 or H3 MM secondary volumes are Safeguarded Copy protected, you can include extra activity tasks to check the session state. This addition is possible because some specific situations might exist where H2 or H3 MM secondary volumes might not be fully consistent:

- ▶ A user suspends one or more volumes.

A session is in the Suspending state (not fully suspended, and consistency across all volumes is not yet created).

- ▶ RPFC is not enabled.

Without RPFC enabled, MM secondary volumes move to the Duplex Pending (or Secondary Pending) state whenever the FlashCopy is taken to the MM primary volume. While in the Duplex Pending state, the MM secondary volumes are not consistent with the MM primary volumes. Therefore, the MM session moves to the Preparing state.

Note: RPFC can be enabled on only one leg of the MT MM-MM session.

To ensure that the Safeguarded Copy from MM secondary volumes is a consistent point-in-time copy, the session state must be Prepared before taking the Safeguarded Copy backup.

The following steps must be included in the CSM scheduled task with MM and Safeguarded Copy on MM secondary volumes:

1. Wait for the Prepared state for the MM session.
2. Use **Backup** on the Safeguarded Copy session.

Note: For step 1, you can specify the wait time (in minutes) before the task times out and fails. The default value is 60 minutes.

The scheduled task example for MT MM-MM and Safeguarded Copy sessions is shown in Figure 4-164 on page 225. The same scheduled tasks are used regardless whether the Safeguarded Copy is taken off the H2 or H3 volumes.

Step #	Action type	Session	Action
1	Wait For State	ITSO_MT MM-MM	Wait for 'Prepared' state on 'ITSO_MT MM-M
2	Command	ITSO_SGC	Issue 'Backup' to 'ITSO_SGC' session

Figure 4-164 Scheduled task actions for Safeguarded Copy backup taken off MM Secondary volumes

4.4.6 Multi-Target Metro Mirror-Global Mirror with Safeguarded Copy

A Multi-Target Metro Mirror-Global Mirror (MT MM-GM) session consists of MM H1 primary volumes, MM H2 secondary volumes, and GM H3 secondary volumes.

Scheduling a task for Safeguarded Copy from H1 MM primary volumes is simple and it requires only one action: use **Backup**.

Therefore, in this section we provide two scheduled task examples:

- ▶ MM H2 secondary volumes are protected with Safeguarded Copy.
- ▶ GM H3 secondary volumes are protected with Safeguarded Copy.

MM H2 secondary volumes are protected with Safeguarded Copy

When H2 MM secondary volumes are Safeguarded Copy protected, you can include extra activity tasks to check the session state. This addition is possible because some specific situations might exist when H2 MM secondary volumes might not be fully consistent:

- ▶ A user suspends one or more volumes.
A session is in the Suspending state (not fully suspended, and consistency across all volumes is not yet created).
- ▶ RPFC is not enabled.
Without RPFC enabled, MM secondary volumes move to the Duplex Pending (or Secondary Pending) state whenever the FlashCopy is taken to the MM primary volume. While in the Duplex Pending state, the MM secondary volumes are not consistent with the MM primary volumes. Therefore, the MM session move to the Preparing state.

To ensure that the Safeguarded Copy from MM secondary volumes is a consistent point-in-time copy, the session state must be Prepared before taking the Safeguarded Copy backup.

The following steps must be included in the CSM scheduled task with MT MM-GM and Safeguarded Copy on MM secondary volumes:

1. Wait for the Prepared state for the MM session.
2. Use **Backup** on the Safeguarded Copy session.

Note: For step 1, you can specify the wait time (in minutes) before the task times out and fails. The default value is 60 minutes.

The scheduled task example for MT MM-GM and Safeguarded Copy sessions is shown in Figure 4-165.

Step #	Action type	Session	Action
1	Wait For State	ITSO_MT MM-GM	Wait for 'Prepared' state on 'ITSO_MT MM-G
2	Command	ITSO_SGC	Issue 'Backup' to 'ITSO_SGC' session

Figure 4-165 Scheduled task actions for Safeguarded Copy backup taken off MM Secondary volumes

GM H3 secondary volumes are protected with Safeguarded Copy

To take a consistent Safeguarded Copy backup from H3 GM secondary volumes in an MT MM-GM session, the following steps must be included in the scheduled task:

1. Use **Suspend H1-H3** (GM leg only).
2. Wait until the GM leg is in the SuspendedH1H3 state (Partially Suspended).

Note: You can add a step to validate the role pair consistency to make sure that the GM sessions are paused with consistency.

3. Create a Safeguarded Copy backup by using **Backup**.
4. Restart the GM leg by using **Resume GM** or **StartGM H1-H3**.

Note: For step 2, you can specify the wait time (in minutes) before the task times out and fails. The default value is 60 minutes.

Resume GM is more suitable because it is used after a brief session suspension. If a long suspension exists or you use **Recover** after suspension, use **StartGM H1-H3** instead.

An example of such a scheduled task is shown in Figure 4-166.

Step #	Action type	Session	Action
1	Command	ITSO_MT MM-GM	Issue 'SuspendH1H3' to 'ITSO_MT MM-GM' s
2	Wait For State	ITSO_MT MM-GM	Wait for 'SuspendedH1H3' state on 'ITSO_M
3	Command	ITSO_SGC	Issue 'Backup' to 'ITSO_SGC' session
4	Command	ITSO_MT MM-GM	Issue 'ResumeGM' to 'ITSO_MT MM-GM' sess

Figure 4-166 Scheduled task actions for Safeguarded Copy backup taken off GM Secondary volumes



A

Other Safeguarded Copy topologies

This appendix presents several Safeguarded Copy topologies. These topologies show how you can combine Safeguarded Copy with IBM Copy Services Manager (CSM) practice volumes.

This appendix covers the following topic:

- “Safeguarded Copy topologies” on page 228

Safeguarded Copy topologies

The Global Mirror (GM) with Practice - Safeguarded Copy Physical Isolation topology is shown in Figure A-1.

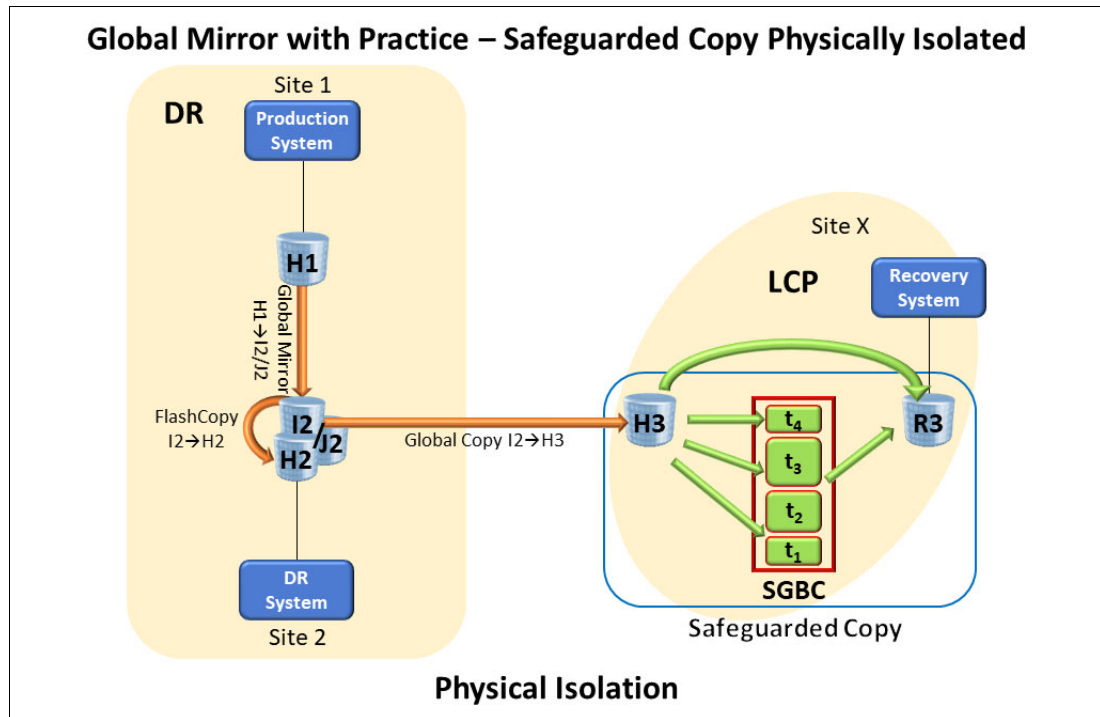


Figure A-1 Global Mirror with Practice - Safeguarded Copy Physical Isolation

The Multi-Target (MT) Metro/Global Mirror (MGM) with Practice - Safeguarded Copy Physical Isolation topology is shown in Figure A-2.

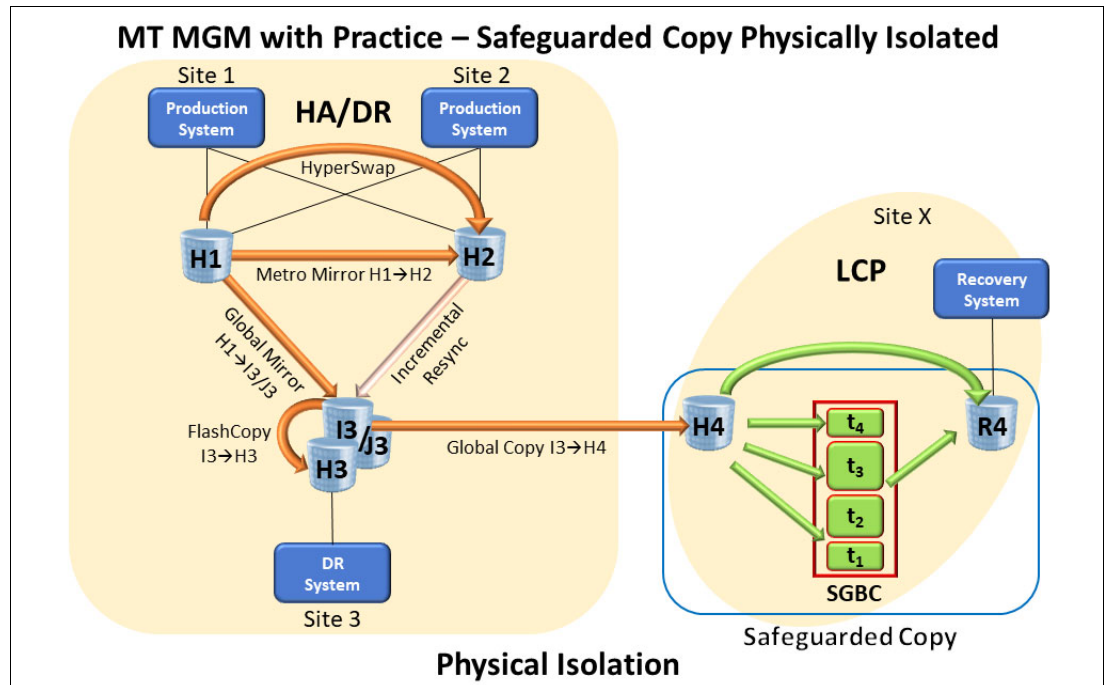


Figure A-2 Multi-Target Metro/Global Mirror with Practice - Safeguarded Copy Physical Isolation

The Cascaded MGM with Practice - Safeguarded Copy Physical Isolation topology is shown in Figure A-3.

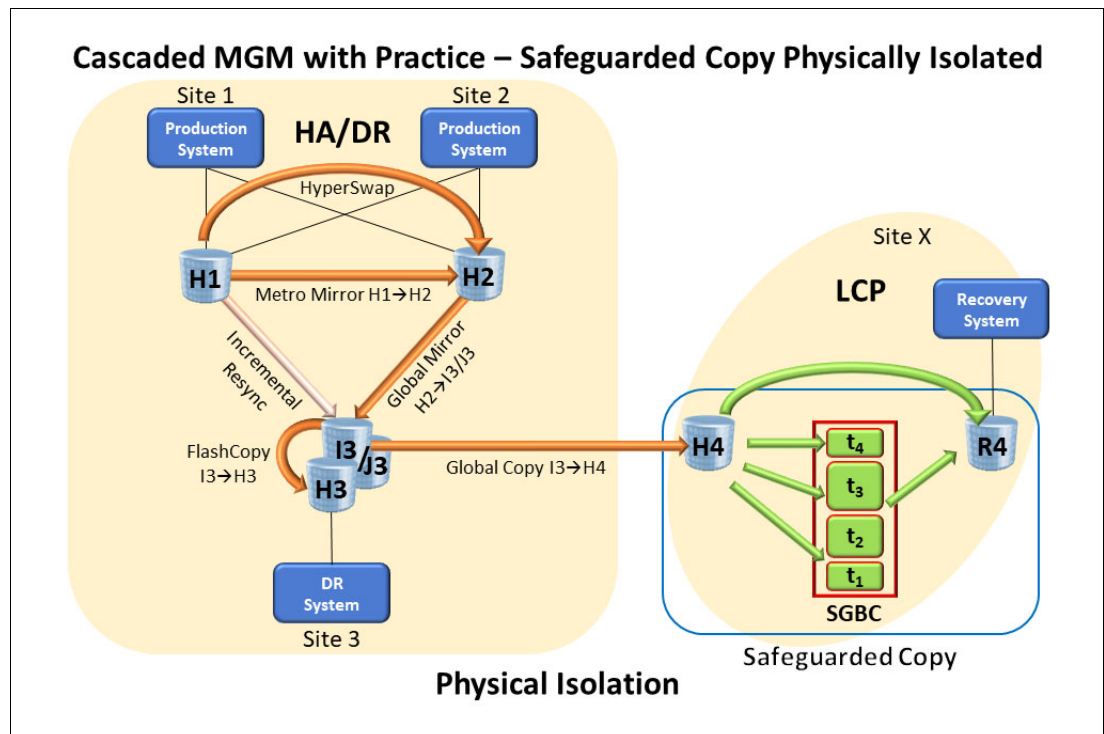


Figure A-3 Cascaded Metro/Global Mirror with Practice - Safeguarded Copy Physical Isolation

Abbreviations and acronyms

CG	Consistency Group	RPO	recovery point objective
CKD	Count Key Data	RTO	recovery time objective
CLI	command-line interface	RVU	Resource Value Unit
CR	cyber resilience	SLA	service level agreement
CS	Copy Services	WORM	Write-Once, Read-Many
CSM	Copy Services Manager		
CSMCLI	Copy Services Manager command-line interface		
DNS	Domain Name System		
DR	disaster recovery		
DVE	Dynamic Volume Expansion		
EBA	European Banking Authority		
ELB	Extended Long Busy		
ESE	Extent Space Efficient		
FB	Fixed Block		
FFIEC	Federal Financial Institutions Examination Council		
GDPS	Geographically Dispersed Parallel Sysplex		
GM	Global Mirror		
HA	high availability		
HADR	high availability and disaster recovery		
HCD	Hardware Configuration Definition		
HDD	hard disk drive		
HMC	Hardware Management Console		
HPFE	High Performance Flash Enclosure		
IBM	International Business Machines Corporation		
IODF	Input/Output Definition File		
Ix	intermediate		
LCP	logical corruption protection		
LSS	logical subsystem		
MGM	Metro/Global Mirror		
MM	Metro Mirror		
MT	Multi-Target		
NAIC	National Association of Insurance Commissioners		
OID	object ID		
OOS	out-of-sync		
PPRC	Peer-to-Peer Remote Copy		
RPFC	Remote Pair FlashCopy		

Related publications

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

IBM Redbooks

The following IBM Redbooks publications provide more information about the topic in this document. Some publications that are referenced in this list might be available in softcopy only:

- ▶ *IBM DS8000 Copy Services: Updated for IBM DS8000 Release 9.1*, SG24-8367
- ▶ *IBM Storage DS8900F Architecture and Implementation: Updated for Release 9.3.2*, SG24-8456
- ▶ *IBM Storage DS8900F Product Guide Release 9.3.2*, REDP-5554

You can search for, view, download, or order these documents and other Redbooks, Redpapers, web docs, drafts, and additional materials at the following website:

ibm.com/redbooks

Other publications

The following publications also are relevant as further information sources:

- ▶ *IBM DS8000 Series Command-Line Interface User's Guide*, SC27-8526
- ▶ *IBM DS8900 Introduction and Planning Guide*, GC27-8525

Online resources

The following websites also are relevant as further information sources:

- ▶ DS8000 System Storage Interoperation Center (SSIC):
<https://www.ibm.com/systems/support/storage/ssic/>
- ▶ IBM DS8000 at IBM Documentation:
<https://www.ibm.com/docs/en/ds8900>
- ▶ IBM Support: Fix Central:
<https://www.ibm.com/support/fixcentral>

Help from IBM

IBM Global Services

ibm.com/services



REDP-5506-04

ISBN 0738461202

Printed in U.S.A.

Get connected

