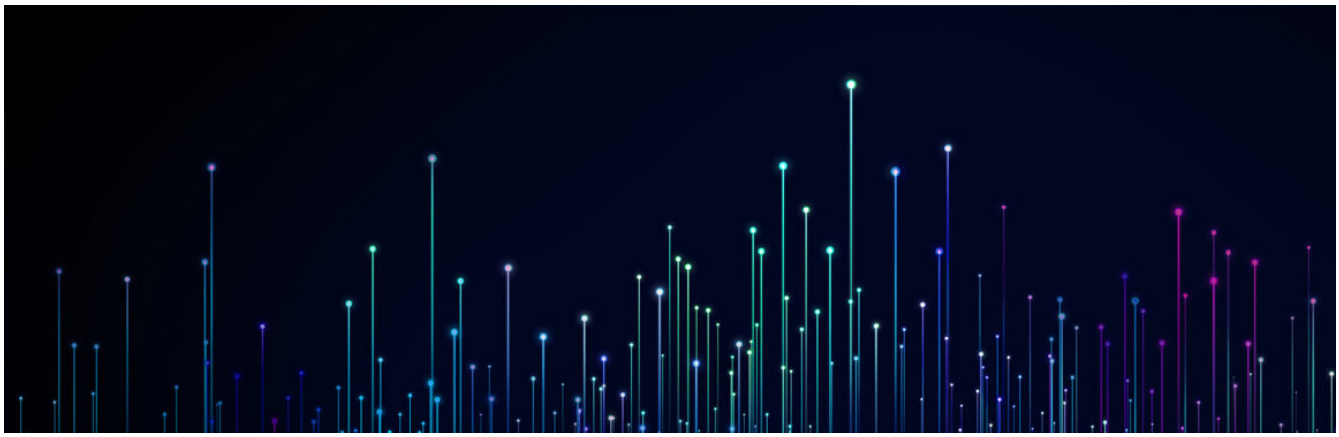
HOT TOPICS

Improving Protection against Logical Data Corruption

IBM has improved the DS8000 FlashCopy and Safeguarded Copy solutions managed by IBM Copy Services Manager by significantly enhancing their performance and minimizing application impact for these solutions.



By: Randy Blea, Tariq Hanif, Tabor Powelson, Bill Rooney
Published: November 2nd, 2021
Read time: 5 minutes

The demand for storage continues to increase—but with this increase comes an increased risk of a cyber-attack. The news is full of stories about data corruption incidents, which range from ransomware attacks to internal malicious users corrupting data. When data is corrupted, multi-site disaster recovery and high-availability solutions may end up not providing protection because the corrupted data is copied to all of the sites. And while traditional backup solutions, such as point-in-time replication or backing up to tape, offer some protection against data corruption, those technologies have limits on either the number of backups or the frequency in taking the backups.

The frequency with which backups are taken is vital for a customer. Data corruption and cyber attacks are not always easy to detect. If the corruption affects business-critical data, a solution that takes frequent backups might save a business millions of dollars, prevent government fines, or even prevent the loss of the business itself. However, as many businesses have found out, frequency has a cost other than storage.

To take either application-consistent or crash-consistent backups, the application or the remote replication solution for the data has to use some mechanism to ensure consistency. If you are taking the backups at a remote site and using asynchronous replication, pausing the replication can enable this to be done without any host impact.

However, if your backup solution is creating the backup directly off the volumes attached to the host or from the secondary of synchronous replication, then write I/O from the host is blocked while the backup is created. In other words, in these situations, the more frequently you take a backup, the more application impact you might experience.

This article discusses how IBM has made critical enhancements to both DS8000 Safeguarded Copy and DS8000 FlashCopy solutions managed by IBM Copy Services Manager that can help customers increase the frequency of their backups while minimizing the application impact.

Effect of the Frequency of Logical Corruption Protection on Application Impact

IBM Copy Services Manager is an IBM product designed specifically to make it easier for customers to manage and monitor their replication needs with IBM Storage. With Copy Services Manager, customers can create complex multi-site replication solutions and tie those to a FlashCopy or Safeguarded Copy session. By creating a Scheduled Task on the Copy Services Manager server, customers can define the frequency of the FlashCopy flashes or the Safeguarded Copy backups. It is this combined solution, as well as the number of recovery points the customer retains, that defines their Logical Corruption Protection solution.

But whether the solution involves FlashCopy flashes or Safeguarded Copy backups, to ensure that the copy is consistent, application I/O must be temporarily halted (using an Extended Long Busy) across all volumes in the Copy Services Manager session. This stops all dependent writes before any of the application I/O can be resumed. This process creates a crash-consistent copy of the data.

Figure 1 gives a high-level idea of how this process works every time a FlashCopy or Safeguarded Copy backup is created. As you can imagine, the more volumes there are in the session, the longer it might take to freeze all the volumes to create the consistency group.

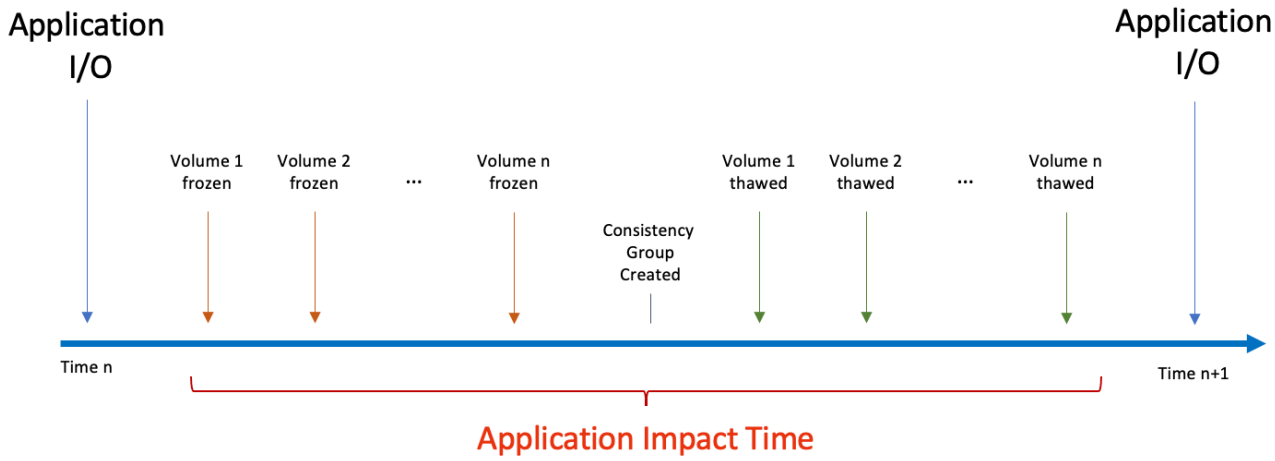


Figure 1: High-Level View of Application Impact Time

While it is always important to minimize the time between when the first volume in the session is frozen and the last volume is thawed, it becomes increasingly more important as the frequency of the flash or backup increases as well. This is because it’s

one thing to see application impact once a day, but an entirely different thing when your logical corruption-protection solution creates flashes or backups every hour or every half hour to provide as many recovery points as possible.

Limitations in the Existing Solution

While Copy Services Manager was designed to minimize the application impact time in taking a FlashCopy or Safeguarded Copy backup, there are still limitations.

When the Copy Services Manager is installed on a Distributed server or running preinstalled on a DS8000 HMC, the commands that are used to coordinate the creation of the FlashCopy or Safeguarded Copy backup are issued through IP-based communication. This IP-based communication into the DS8000 might experience network interruptions or bottlenecks in the interface, assuming that interface is shared with other commands, queries, and management tools. All of these factors could cause greater application impact than desired in some circumstances.

When the Copy Services Manager server is installed on a z/OS system, the server can take advantage of the FICON-based connectivity to any storage systems connected to the z/OS system, by going through the I/O Supervisor (IOS) component of z/OS. This connection can provide more stability than the IP communication; however, running Copy Services Manager on z/OS has its own limitations. For ease of management, it may make sense to include system volumes such as Page Packs, Couple Datasets, and volumes accessed or required by Copy Services Manager within the copy configuration. Even if the data on these devices are not necessarily needed to recover applications following a corruption event, it would be unfortunate to find out later that a dataset that should have been backed up was not backed up. You could choose to simply back up every volume in a configuration rather than just the ones that might be needed. The limitation that this causes is that Copy Services Manager running on z/OS might have dependencies on those local system volumes. This means that when Copy Services Manager issues the freeze as part of a FlashCopy or as part of a Safeguarded Copy backup, the freeze of the system volumes could lead to Copy Services Manager freezing itself, leaving it unable to complete the process or issue the thaws, as shown in Figure 2. If Copy Services Manager hangs, customers might see even longer application impact times and might lose data consistency.

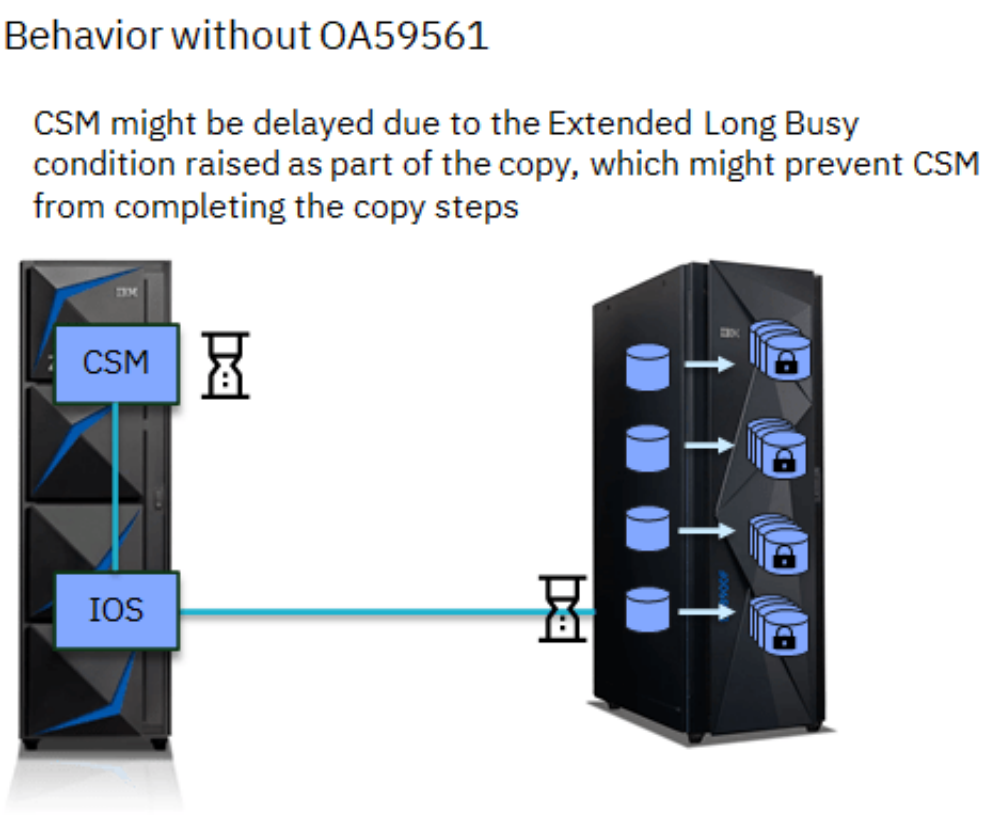


Figure 2: Behavior without OA59561

How IOS helps this

Starting with Copy Services Manager 6.2.11 with IOS APAR OA59561, IOS can now avoid such delays by performing the critical steps of Safeguarded Copy on behalf of Copy Services Manager. This support works by having Copy Services Manager build all the necessary Channel Command Words (CCWs) and packaging them to IOS as one logical group, then having IOS issue all the CCWs before returning to Copy Services Manager. Figure 3 outlines the Safeguarded Copy steps and identifies the critical ones performed by IOS.

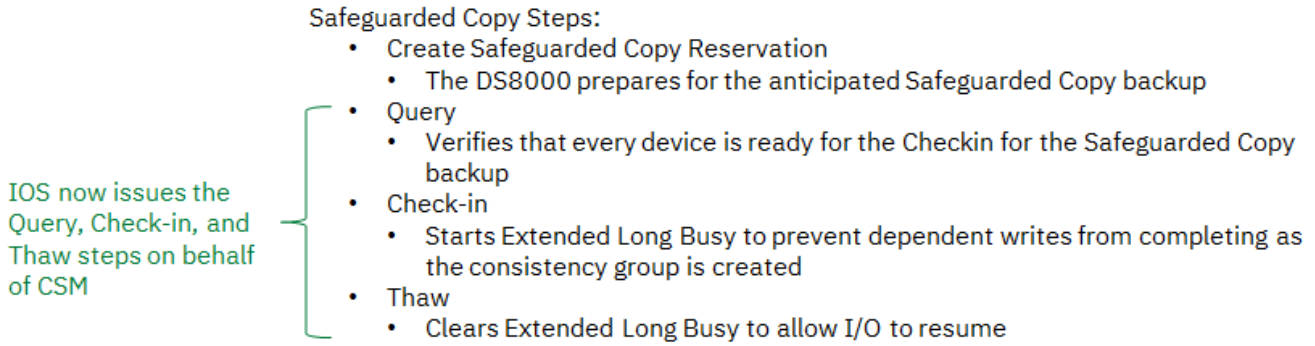


Figure 3: Safeguarded Copy Steps with OA59561

IOS is a lot closer to the hardware than Copy Services Manager is and can issue these FICON CCW commands much faster than Copy Services Manager would be able to.

This directly helps performance by avoiding any unnecessary delays between the copy steps, so now the total elapsed time of the copy is almost entirely the length of time the hardware takes to perform the requests. This greatly reduces software delays in the copy steps.

Neither the FlashCopy target volumes nor the Safeguarded Copy recovery volumes need to be attached to the z/OS system taking the backups.

As in z/OS HyperSwap and Hardened Freeze configurations, the code path for IOS performing the FlashCopy or Safeguarded Copy is “hardened” to prevent the possibility of hangs during the copy process. This means that you are free to include system volumes such as Page Packs, Couple Datasets, and other volumes required by Copy Services Manager within the copy configuration. Once Copy Services Manager requests the copy, the critical steps are performed within IOS without the need to communicate back to Copy Services Manager until the copy completes. Thus we avoid any possibility of Copy Services Manager “freezing itself” during the copy process.

Figure 4 shows the logical view of Copy Services Manager sending IOS the necessary information for the Safeguarded Copy or FlashCopy steps, and IOS performing the steps without hanging.

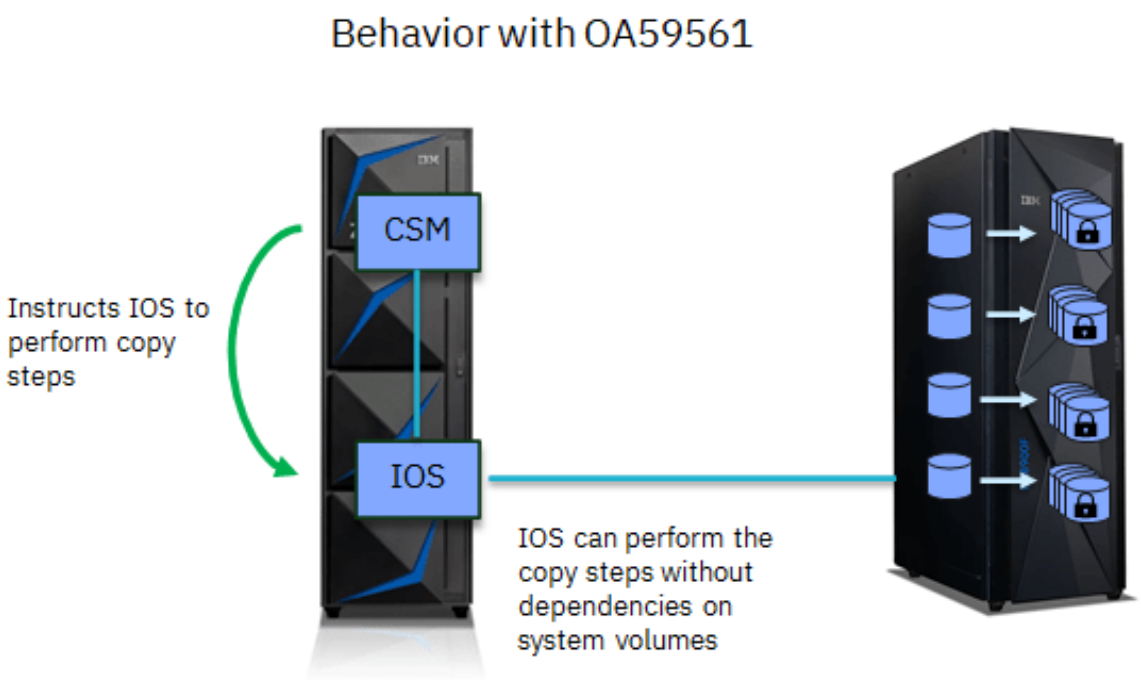


Figure 4: Behavior with OA59561

Performance of Solution

Tests were performed in the IBM lab, comparing the application impact time for various device configurations before and after the enhancement. In the case of Safeguarded Copy backups, tests were performed with configurations containing 1K, 3K, 5K, and 10K source devices on a single DS8000 storage system. The results showed that the Safeguarded Copy impact time with the enhanced method was 65-95% shorter than without the enhancement. (See Figure 5.)

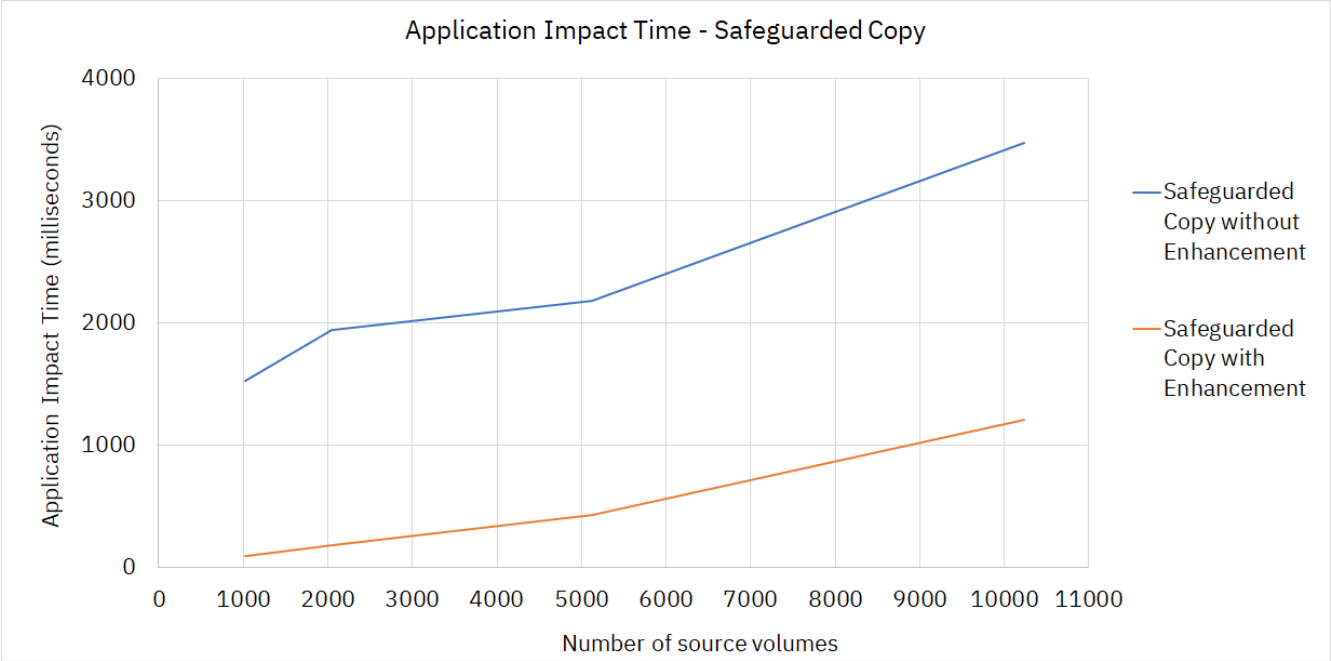


Figure 5: Application Impact Time, Safeguarded Copy

In the case of FlashCopies, tests were performed with configurations containing 1K, 3K, and 5K source devices also on a single DS8000 storage system. The results showed that the FlashCopy impact time with the enhanced method was 85-95% shorter than without the enhancement. (See Figure 6.)

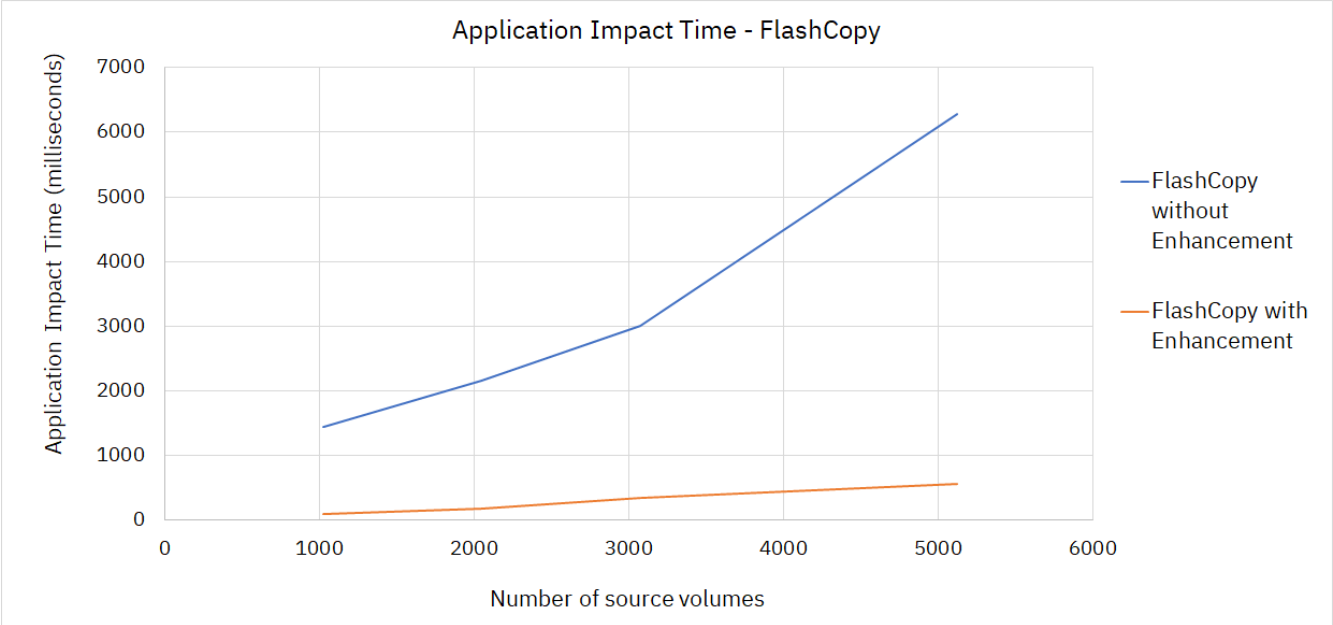


Figure 6: Application Impact Time, FlashCopy

This solution is suitable for FlashCopy or Safeguarded Copy for disaster recovery and

logical corruption protection in a production environment, and this enhancement greatly reduces application impact times.

Disclaimer

Actual performance results might vary for clients depending on the configurations, workloads running on the systems, and operating conditions.

System or Performance Test Setup

This test was performed with the following configuration:

- z/OS V2R3 LPARs with OA59561 on z15 CEC with shared processors, running DB2 workload simulating online transaction.
- DS8900F with 89.11.33.0 was used to collect performance measurements.
- Test configuration included mod1 (mostly), mod3, mod9, mod27, mod54, and 1 TB EAVs.

Performance Data Collection:

- FlashCopy test measurements data were collected using a single site test setup.
- Safeguarded Copy backup measurements were done with two site setups with HyperSwap active, with Safeguarded Copy backups taken of the H1 PPRC primary devices.

Practical Example

Safeguarded Copy backups and FlashCopies may be used in combination with other storage replication sessions. An example is shown with Safeguarded Copy backups taken off the primary devices in a Metro Mirror session.

In this example, you can create a Metro Mirror session, with or without HyperSwap, and you can also create a Safeguarded Copy session off the primary volumes, as shown in Figure 7. In this configuration your backups would be located at the primary site. Similar steps are used to take Safeguarded Copy off the Metro Mirror target volumes.

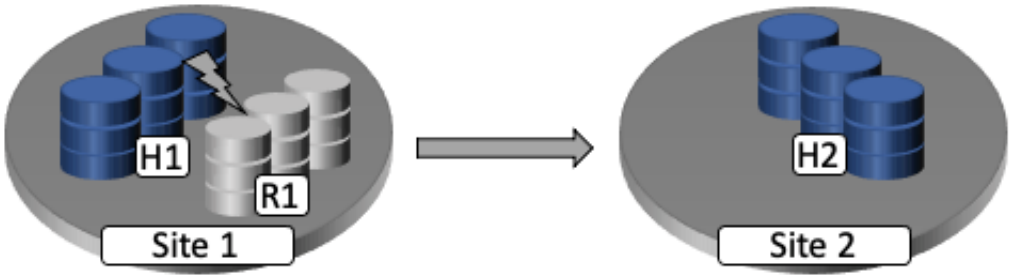


Figure 7: Safeguarded Copy in a Metro Mirror environment

To initiate backups automatically, you need to create a Scheduled Task in Copy Services Manager. For more information about creating a scheduled task in Copy Services Manager to manage Safeguarded Copy, see [Copy Services Manager Safeguarded Copy and FlashCopy Enhancements for z/OS Environments.]

How to Enable

To enable this function, the Safeguarded Copy or FlashCopy session must be updated to have a z/OS System or Sysplex association. To set this within Copy Services Manager, choose Session Actions -> View Modify -> Properties, then choose the appropriate System or Sysplex under the z/OS Management pulldown. Figure 8 shows an example screenshot in which the Safeguarded Copy session has an association to the z/OS Sysplex named PRODPLEX.

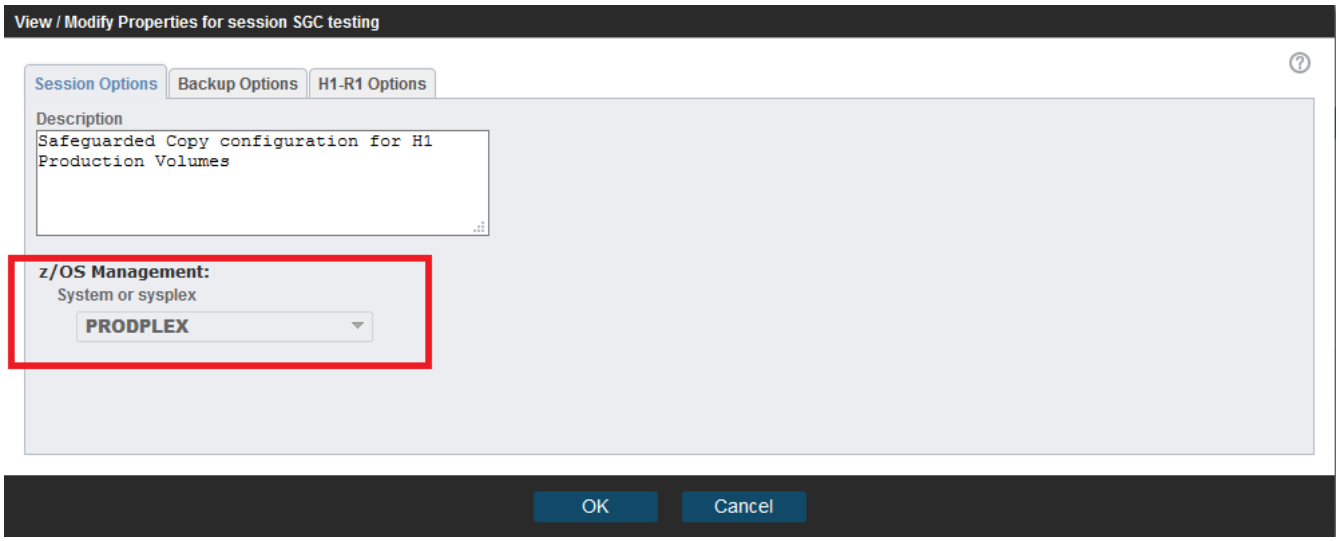


Figure 8: How to Enable

Requirements

This Enhancement has the following requirements:

- Copy Services Manager 6.2.11
- IOS APAR OA59561 applied on the z/OS System to which Copy Services Manager connects
- The z/OS System or Sysplex association for the copy session must be set
- All volumes in the session, other than Safeguarded Copy recovery volumes and FlashCopy targets, must be attached and available to the z/OS system that is associated with the copy session
- The CRITICALPAGING function must be enabled in z/OS

Estimating Safeguarded Copy Backup Capacity

Regular backups may encounter backup capacity errors if adequate backup capacity is not configured for the source volumes. The backup capacity required for each source volume depends on how frequently backups are created, the backup retention policy, and the amount of data written during each backup interval.

Copy Services Manager version 6.2.11 and above provides an Extent Space Efficient (ESE) Sizer session type that makes it easier to make capacity sizings for ESE FlashCopy and Safeguarded Copy. It does this by querying the DS8000 Write

Monitoring bitmap available on DS8800 and DS8900 and generating Excel spreadsheets.

That information, along with knowledge of backup frequency and retention policy, can be used to determine the backup capacity for the safeguarded source volumes. For more detailed information about using a Copy Services Manager ESE Sizer session and how the collected data can be used to calculate backup capacity for safeguarded source volumes, see
DS8000® Safeguarded Copy and Extent Space Efficient (ESE) FlashCopy® capacity sizing by using the new Copy Services Manager ESESizer functionality.

About the authors

Randy Blea is a software architect at IBM with over 20 years of technical experience in the field of copy services. His responsibilities include setting the strategic vision and technical architecture for IBM Copy Services Manager, an enterprise replication management solution for copy services and disaster recovery management on IBM storage devices.

Tariq Hanif is a Senior Software Engineer. In 2003, he joined IBM z/OS System Verification group to test z/OS with a focus on z/OS HyperSwap, Storage Replication Solutions, Disaster Recovery and Parallel Sysplex®.

Tabor Powelson focuses on z/OS I/O and Z storage replication, and is a developer for z/OS HyperSwap. He joined IBM in 2009 after receiving his B.S. degree in Software Engineering and Mathematics from Clarkson University.

William Rooney was a Senior Technical Staff Member in the System Z Operating Systems Development organization in Poughkeepsie, NY. He had over 40 years of experience with IBM in System Z and z/OS.

Nick Clayton contributed to the technical review of this article.

Martha Burns contributed to the editorial review of this article.