Cyber Resilience and Safeguarded Copy

2022 TPF Users Group Conference
March 27-30, Dallas, TX
Main Tent

—

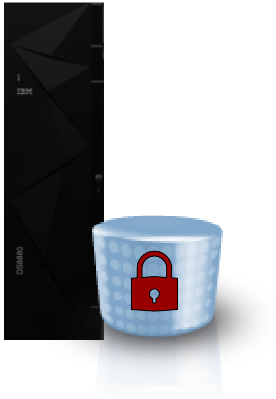
Theresa Brown, Copy Services Architect
Beth Peterson, DS8000 Storage Architect
Randy Blea, Copy Services Manager Architect
Chris Filachek, z/TPF DASD Architect

IBM Z

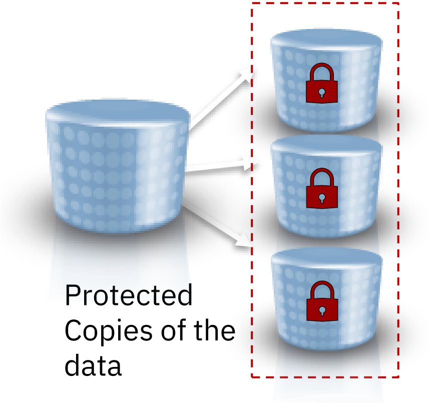
Cyber Resilience

and Safeguarded Copy

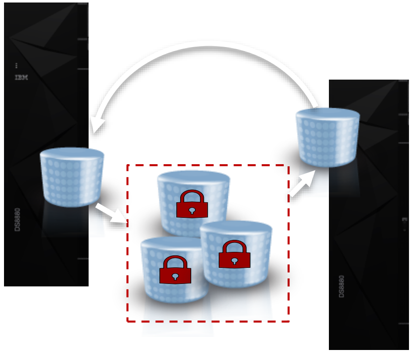
Key storage requirements to increase Cyber Resilience



1. Provide additional security capabilities to prevent privileged users from compromising production data as well as protected copies of the data


Protected Copies of the data

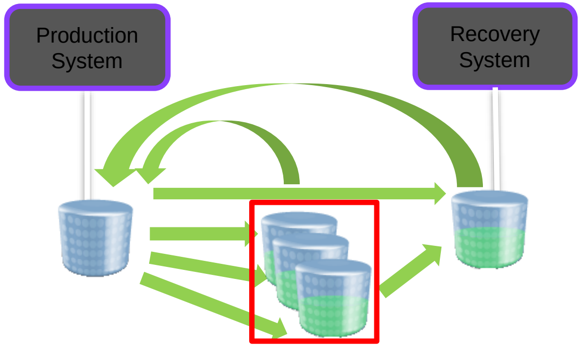
2. Provide capabilities to regularly create secure, point in time copies of the data for Logical Corruption Protection scenarios



3. Provide functionality that enable different use cases to restore corrupted data from Logical Corruption Protection copies

Protection Copies Concept

Source devices are where the protection copies are taken from. These could be production devices or taken from a HA/DR copy using data replication



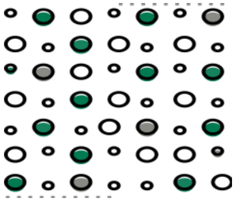
Recovery devices enable IPL of systems for forensic analysis or other purposes

Protection devices provide one or more logical protection copies and are not accessible by any system. Additional security measures aim to protect these from inadvertent or malicious actions

Requirement for Logical Data Protection

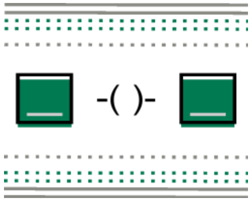
In addition to traditional high availability and disaster recovery, there are some requirements to provide complete protection against content level destruction of data.

The major design requirements for logical corruption protection are:



Granularity

We must be able to create multiple safety copies in order to minimize data loss in case of a corruption incident



Isolation

The safety copies must be isolated from the active production data so that it cannot be corrupted by a compromised host system (this is also known as air gap)

Immutability

The safety copies must be protected against unauthorized manipulation

Use cases for protection copies

Catastrophic
Recover the entire environment back to the point in time of the copy as this is the only recovery option

Forensic
Start a copy of the production systems from the copy and use this to investigate the problem and determine what the recovery action is

Surgical
Extract data from the copy and logically restore back to the production environment

Validation
Regular analytics on the copy to provide early detection of a problem or reassurance that the copy is a good copy prior to further action

Offline Backup

Backup the copy of the environment to offline media to provide a second layer of protection

Safeguarded Copy - Objectives

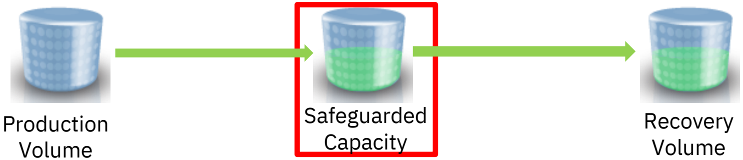
Enable the capturing of many (up to 500) Point in Time images of a production environment with optimised capacity usage and minimized performance impact.

Enable a previous Point in Time to be made available on another set of volumes while the production environment continues to run and copied back to the production volumes if necessary

Secure the data for the Safeguarded Copies to prevent this data from being compromised either accidentally or deliberately.

Volume Terminology

The **Production Volume** is the source volume for a Safeguarded Copy relationship. Depending on the specific client topology this could be a Metro Mirror, Global Mirror or z/OS Global Mirror primary or secondary volume or a Simplex volume.
**Maximum Volume Size = 2 TB



The **Safeguarded Capacity** is a thin provisioned volume associated on a 1:1 basis with a Production Volume. It is not accessible to hosts and does not consume a host volume number. Updates written to the production volume cause tracks to be copied into the Safeguarded Capacity to allow Recovery to a number of specific Backup Copies which are created each time a Consistency Group is formed
**Maximum Size = 16 TB

The **Recovery Volume** is the target volume for a Safeguarded Copy Recovery which enables a prior Backup Copy to be accessed by a host attached to this volume. The Recovery Volume would typically be thin provisioned but this is not mandatory

Safeguarded Copy - Capabilities

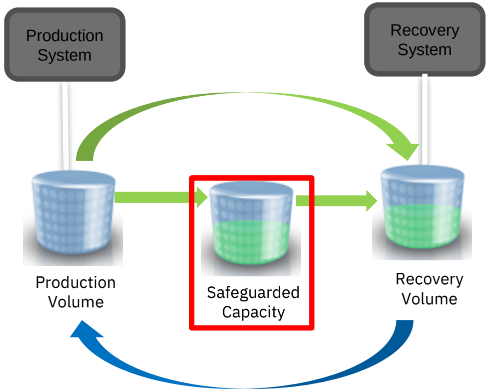
- Safeguarded Copy provides up to 500 backup copies to restore data in case of logical corruption or destruction of primary data
  - The Safeguarded Capacity does not consume any of the regular DS8K volume addresses

- Management and data consistency is provided by CSM or GDPS and copies can be maintained at production and/or recovery sites

- Data can be restored to an additional recovery copy and can be used or copied to the source device depending on scenario

- Targets protected against malicious actions with additional security provided through unique user roles

Create additional copy of any recovery point or current time for Recovery or Forensic analysis



Copy data back from the Recovery Volume depending on the scenario

Easy Tier and Safeguarded Copy

Extents that are allocated as Safeguarded Backup Capacity are not monitored by Easy Tier

After being written, Safeguarded Backup data normally is not accessed at all

Easy Tier classifies all extents allocated to a Safeguarded Backup as cold, once the next backup is initiated

Cold extents are candidates for demotion to the slowest storage tier available in the extent pool

It is good practice to set the Easy Tier Allocation Order to “High Performance”

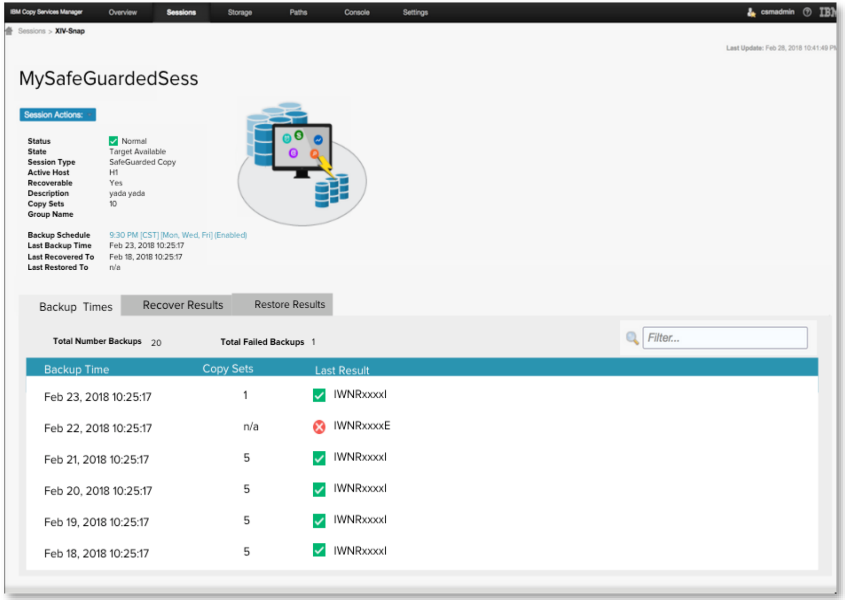
This causes new extents for Safeguarded Copy Capacity to be allocated in the best performing storage tier available and avoids performance impacts from writing Safeguarded Copy Backup data

Every time a new backup is initiated, extents from previous backups are marked cold, and will be moved to a lower tier if space is needed

Security considerations

Safeguarded Copy prevents backup data being compromised either intentional or deliberately, like accidentally delete backup version(s) or even production volumes

1. Safeguarded copies cannot be created, deleted, or recovered manually using the DS8900 management interfaces
2. Administrators need at least two interfaces in order to create, enable and manage Safeguarded Copy
   - DS8900 DS CLI or GUI are needed to create Backup capacity
   - IBM Copy Services Manager (CSM) or GDPS is needed to enable and manage Safeguarded Copy tasks
   - Access to one or the other interface can be limited and restricted to specific storage administrators
3. Different user roles and authority levels can be used to manage production source volumes, backup capacity and recovery volumes
4. Production volumes which are in a Safeguarded Copy relationship can not be deleted from DS8900 GUI or DSCLI even with the force command



Last Update: Feb 28, 2018 10:41:49 PM

MySafeGuardedSess

Status	✓ Normal
State	Target Available
Session Type	SafeGuarded Copy
Active Host	H1
Recoverable	Yes
Description	yada yada
Copy Sets	10
Group Name	
Backup Schedule	9:30 PM [CST] [Mon, Wed, Fri] (Enabled)
Last Backup Time	Feb 23, 2018 10:25:17
Last Recovered To	Feb 18, 2018 10:25:17
Last Restored To	n/a

Total Number Backups 20   Total Failed Backups 1

Backup Time	Copy Sets	Last Result
Feb 23, 2018 10:25:17	1	✓ IWNRxxxxI
Feb 22, 2018 10:25:17	n/a	✗ IWNRxxxxE
Feb 21, 2018 10:25:17	5	✓ IWNRxxxxI
Feb 20, 2018 10:25:17	5	✓ IWNRxxxxI
Feb 19, 2018 10:25:17	5	✓ IWNRxxxxI
Feb 18, 2018 10:25:17	5	✓ IWNRxxxxI

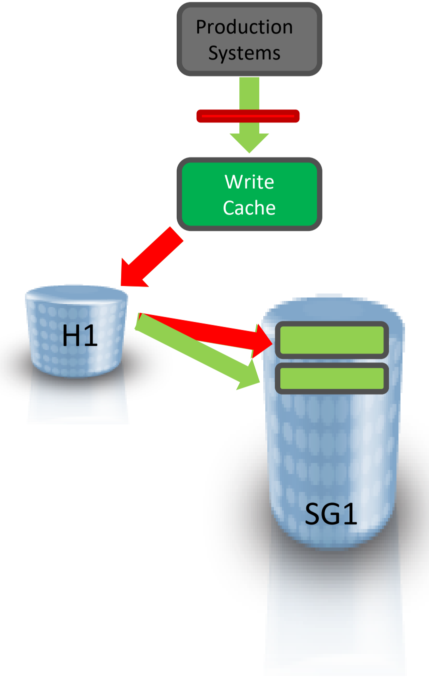
Creating a Consistency Group / Backup Copy

As with FlashCopy Consistency Groups, Safeguarded Copy uses the extended long busy (ELB) processing.

Create a Reservation on all volumes for the Consistency Group which sets up structures and prepares for the creation of a new Backup Copy. If this fails for any volume we can cancel the Reservation and report an error to the user without affecting the existing Backup Copies. Writes are not prevented during the reservation process

As part of the reservation creation, a commit scan is performed to harden all tracks currently in the write cache for the volume.

While a reservation exists, any new writes that require data to be stored in the Backup Volume will perform this copy synchronously



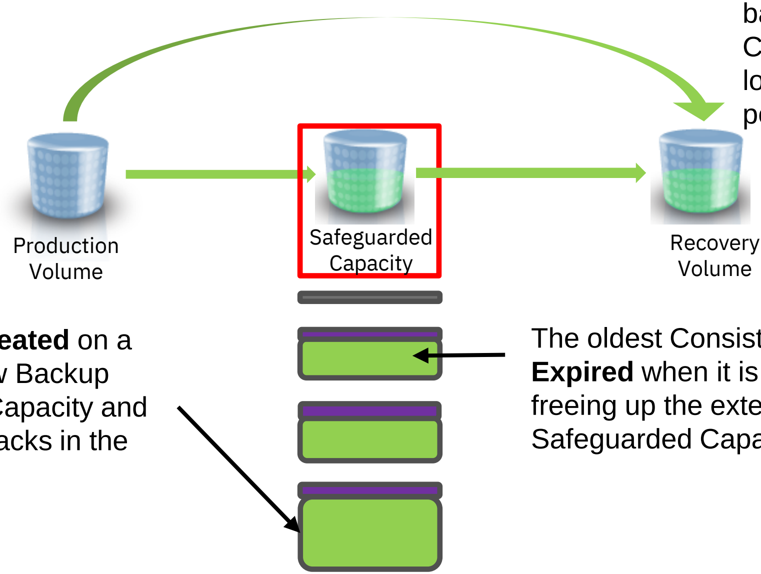
Checkin the Reservation for all LSS involved in the consistency group with a single command for each LSS. Writes are prevented on each volume in the LSS as it is checked in to create a consistent point in time for the Backup Copy so this process is performance critical to minimise impact to production writes

Complete the Checkin on each LSS allowing writes to continue and new updates to be stored in the Log for the new Backup Copy

Operational Action Summary

****Restoring** from the Safeguarded Backups directly to the Production Volume is **NOT** supported in the initial release

A Backup Copy can be **Recovered** from the Safeguarded Capacity to the Recovery Volume. This uses the current state of the Production Volume as the baseline for the Recovery with the Consistency Group used to provide a logical view of the volume at the previous point in time.

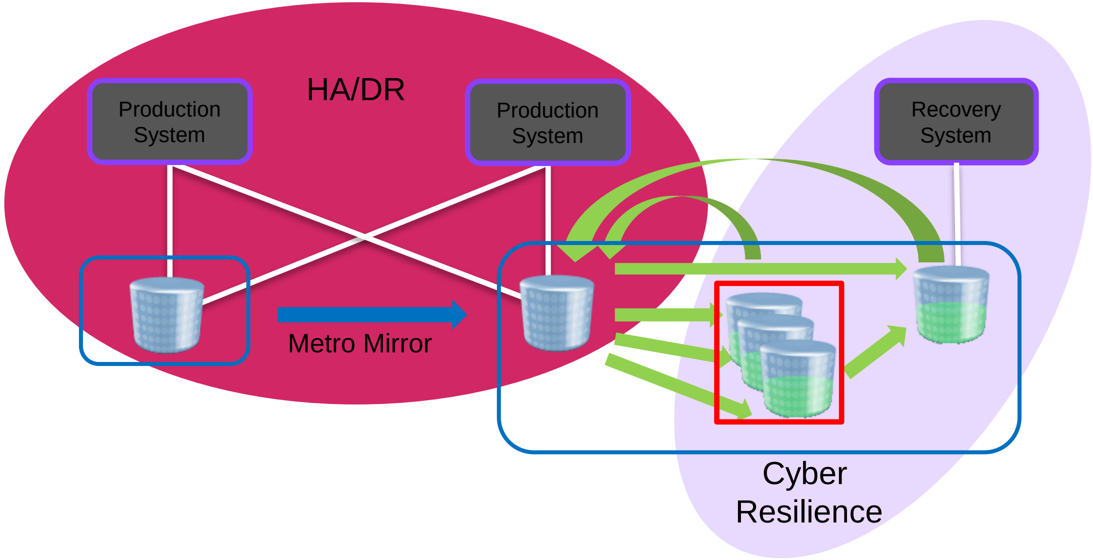


Consistency Groups are **Created** on a regular basis creating a new Backup Copy on the Safeguarded Capacity and storing copies of updated tracks in the Consistency Group

The oldest Consistency Group can be **Expired** when it is no longer required freeing up the extents in the Safeguarded Capacity

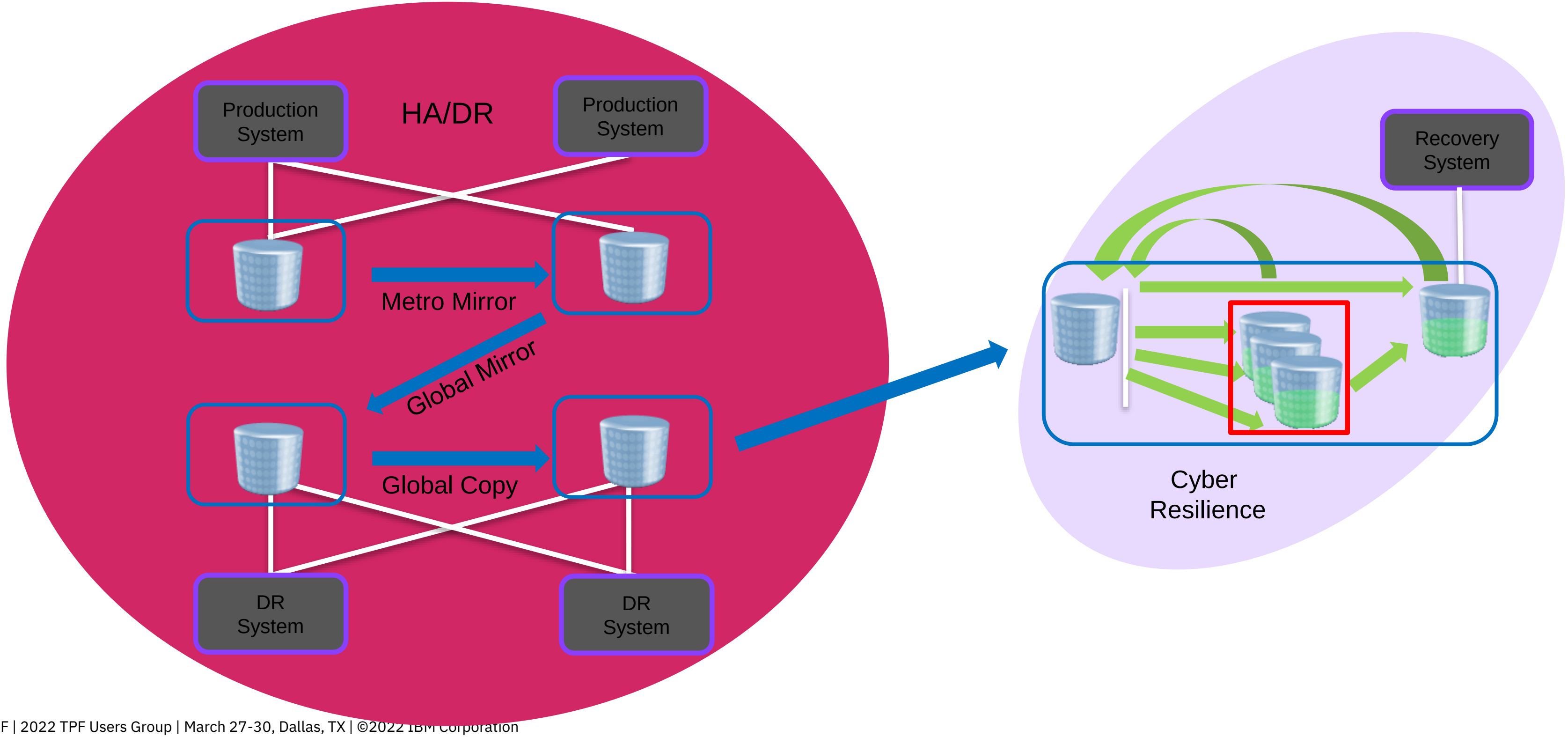
Virtual Isolation

Protection copies added to one or more **existing storage systems** in the HA/DR topology

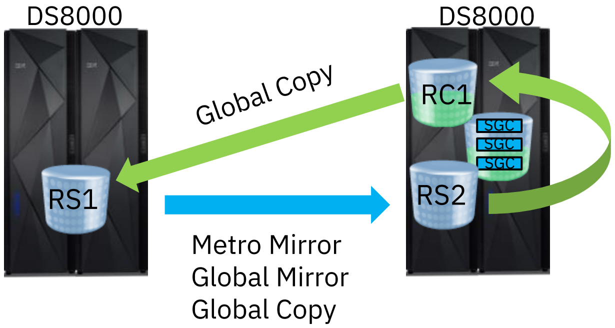


Physical Isolation

Protection copies added to one or more **additional storage systems** physically isolated from the HA/DR topology



Safeguarded Copy Restore to Production



Hill: A line of business owner can meet regulatory SLAs for application recovery following a catastrophic cyberattack against production data by enabling an incremental copy of data back to production.

Details: Enable a user to restore a recovered Safeguarded Copy back to a Production copy of data using an incremental Global Copy rather than the full Global Copy required today.

The Global Copy is performed back to the PPRC pair of the Safeguarded Source device (RS1 in the picture) enabling this to be done both in physical isolation and virtual isolation scenarios.

The amount of data copied back and time to copy will depend on the time and changes since the particular backup that is being restored

Managing Copy Services with

IBM Copy Services Manager

IBM Copy Services Manager

Simplify Your Replication

Easy to install. Easy to Setup. Easy to Manage.

Provides Automation for Advanced Copy Services

Single Point of Control Across Environment

Designed to Scale For Thousands of Relationships

RPO Monitoring and Historical Reporting

One Step Recovery

Simplifies the recovery process in multi-site replication, protecting customer data while keeping costs down

Provides support for both distributed and mainframe data
Supports DS8900F and Spectrum storage systems

Installable across all major platforms:
Windows, Linux, AIX, z/OS, Linux for z Systems
And now pre-installed on the DS8000 HMC

Disaster Recovery and High Availability

Manages z Systems HyperSwap and
supports Power HA HyperSwap to create highly available solutions in Metro Mirror and Metro Global Mirror Environments

Practice As You Would Recover with CSM Practice Volumes

Issue the ‘Flash’ command to back up your remote site and automatically restart replication so that you can practice while maintaining DR capabilities

Protect Your Data

Warning Prompts
User Roles
Site Awareness
Dynamic Images
Event and Threshold Alerts

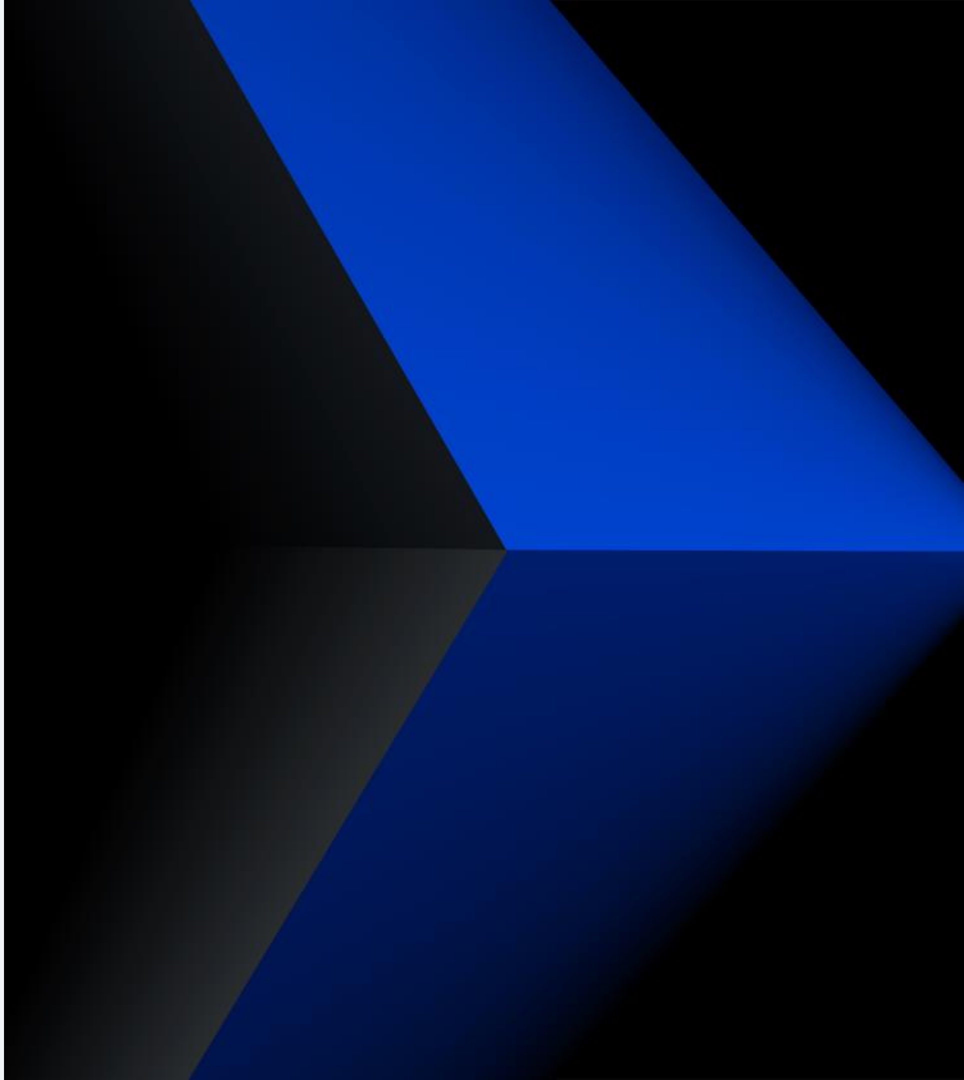
* See your IBM Representative for further details.

Safeguarded Copy

and z/TPF

Disclaimer

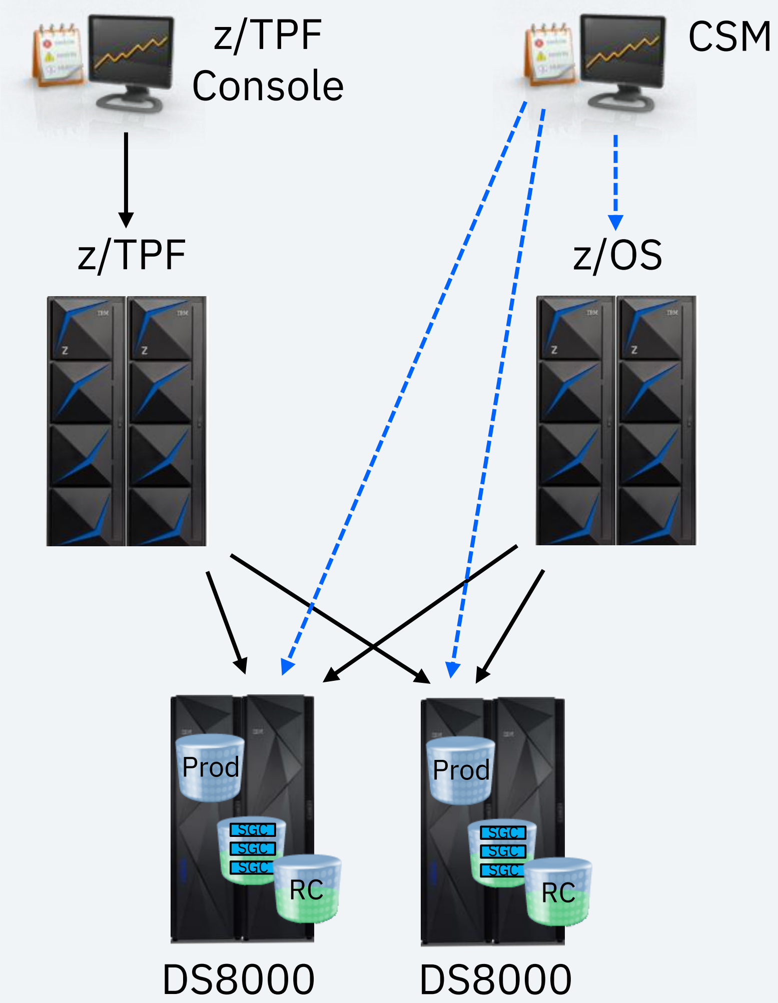
Any reference to future plans are for planning purposes only. IBM reserves the right to change those plans at its discretion. Any reliance on such a disclosure is solely at your own risk. IBM makes no commitment to provide additional information in the future.



Pain Points

To create safeguarded copies outside of the CSM schedule, I need to use a separate CSM GUI or command line to start and monitor the copy session. This means I need to watch both z/TPF and CSM.

Derrick
operator

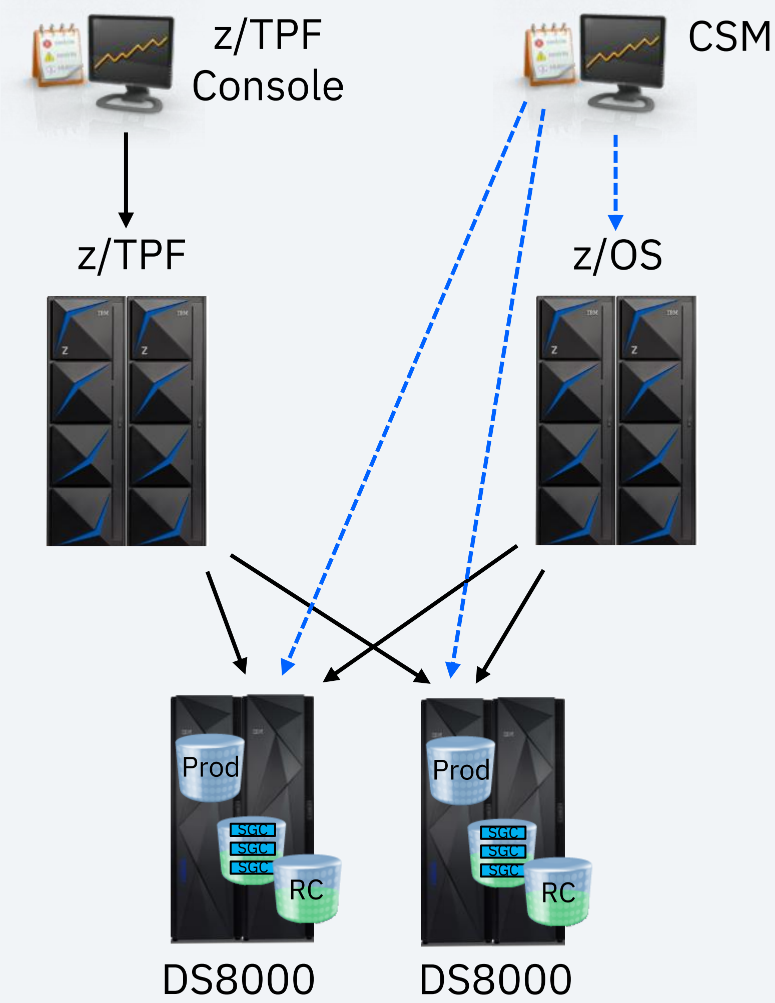


Pain Points

To minimize impact to z/TPF I/O's, key parts of the safeguarded copy process need to be driven through z/OS and FICON channels.

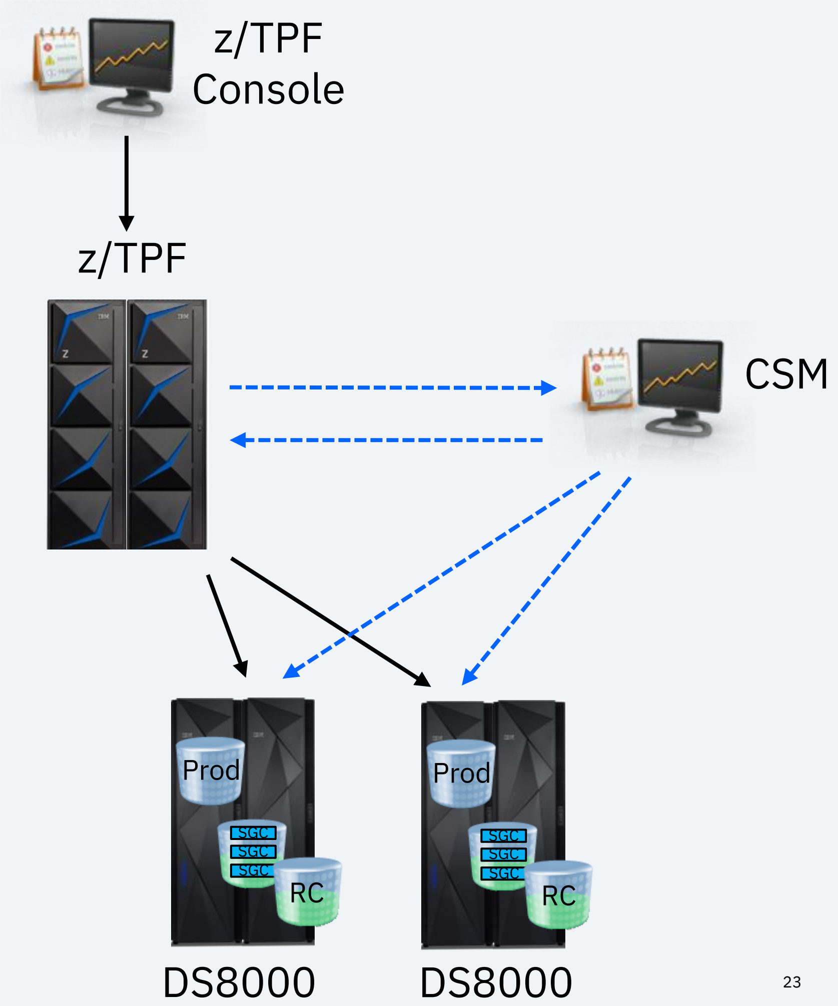
This requires having us to have a z/OS system connected to z/TPF production volumes.

Arthur
enterprise architect



Value Statement

An operator can use the z/TPF console to start and stop safeguarded copies without requiring a z/OS system and with minimal impact to z/TPF I/O's.

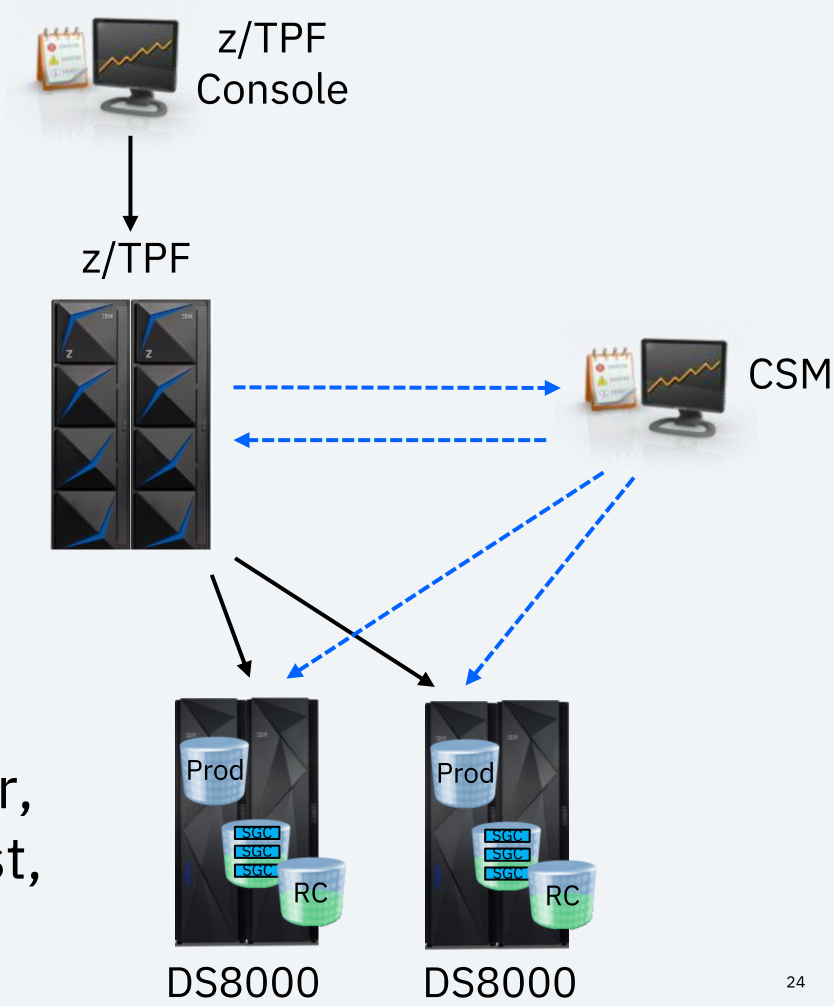


Technical Details

- z/TPF commands communicate directly with CSM to initiate the copy process

- Key safeguarded copy commands are issued by z/TPF over FICON to minimize the impact to z/TPF I/O

- Initial setup of safeguarded copy, restoring due to corruption, disaster, etc., creating backup images for test, is done through the CSM GUI



We want sponsor users!

Our development cycle is driven by your feedback.

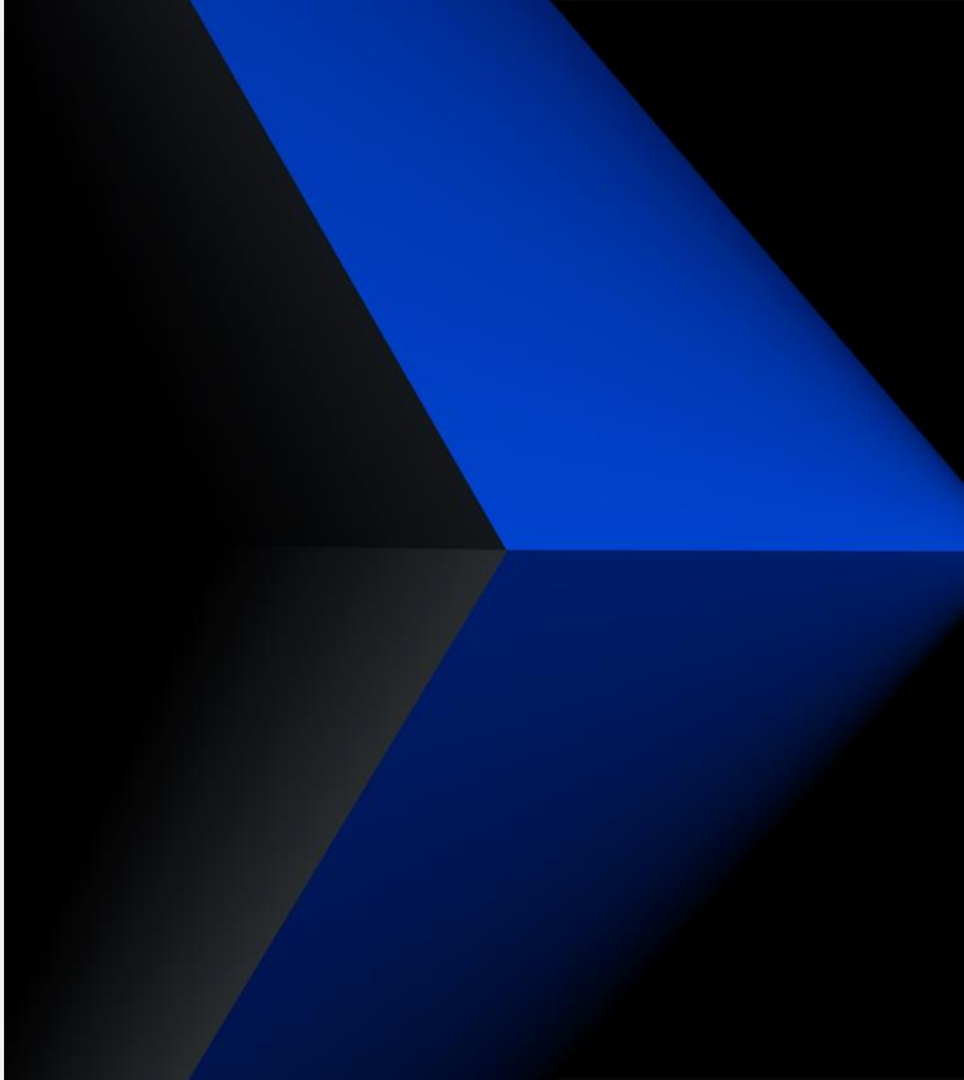
We are looking for sponsor users to assist in design and implementation, targeting the following personas:

- Operators
- Enterprise architects

We expect to begin engaging with the sponsor users in 2H 2022.

If you are interested in participating as a sponsor user, please contact:

Chris Filachek (filachek@us.ibm.com)



Thank you