Protecting your business from data corruption events

Nick Clayton and Dave Clitherow
IBM

November 2018
Session DB

Agenda

- Background
- Concepts
- Safeguarded Copy overview
- GDPS support

Background

The economic impact of cyber threats incidents

Cyber threats have become increasingly common. Data breaches continue to be costlier and result in more consumer records being lost or stolen, year after year

Average total cost of a data breach:

$3.86 million

Average total one-year cost increase:

6.4%

Average cost per lost or stolen record:

$148

One-year increase in per capita cost:

4.8%

Likelihood of a recurring material breach over the next two years:

27.9%

Average cost savings with an Incident Response team:

$14 per record

The 2018 Cost of a Data Breach Study by the Ponemon Institute: https://www.ibm.com/account/reg/us-en/signup?formid=urx-33316

Cyber threats to enterprise data

Cyber threats to enterprise data are increasing from a range of different sources including:

- External Malware Infection
- External Hacking
- Insider Threats

Depending on the platform different risks are seen as most likely. For core systems running on IBM Z or IBM Power Systems, many organisations believe the threat from a privileged insider is the greatest risk

Similar loss or corruption of data is still also possible from other causes such as

- Application error
- Operational error

Solutions to reduce the risk of financial losses should handle a wide range of possible scenarios

Regulatory and cyber-security guidance

Regulators are starting to provide guidance on protecting from these issues and the clients are listening

Federal Financial Institutions Examination Council

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

National Association of Insurance Commissioners

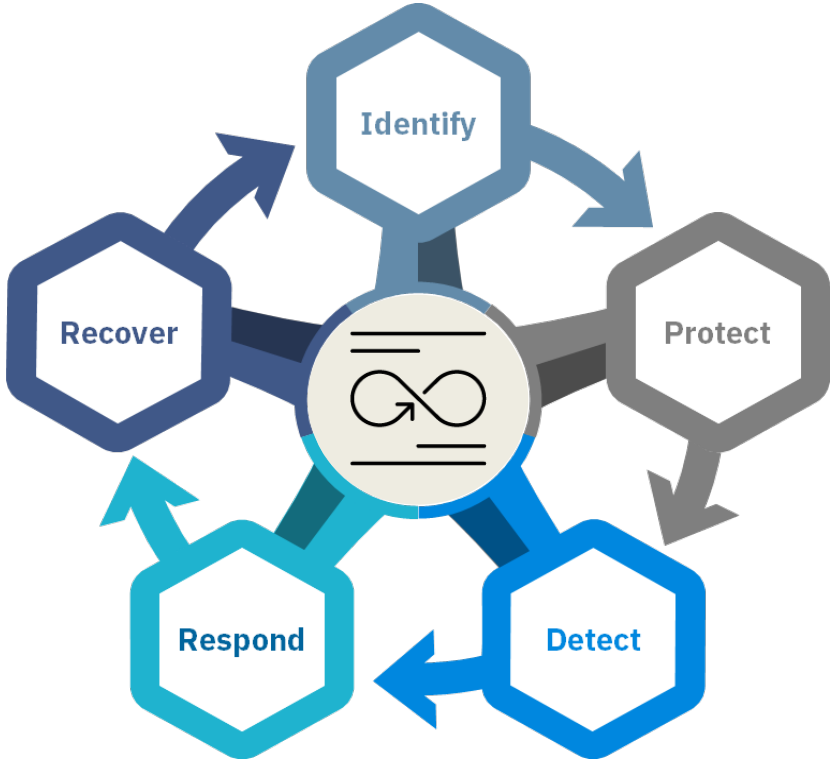
"... It is vital for state insurance regulators to provide effective cyber-security guidance regarding the protection of the insurance sector's data security and infrastructure."

Cyber Resiliency Framework

The Storage environment is an important element of an end to end cyber resiliency strategy. Orchestrate and simplify your disaster recovery management to reduce risk and improve availability, efficiency and business confidence with IBM Storage.

IBM Resiliency Services can provide an assessment of client's environment for a proactive, integrated plan from the following perspectives:

- Organization
- Technology Environment
- Data Security
- Information Protection
- Risk Management
- Threat & Vulnerability Management
- Continuity of Business Operations
- Policy & Governance
- Cyber Security Program
- Asset Management
- Identity & Access Management
- Change & Config
- Event & Incident Response
- Collaboration & Communication
- Partner Eco-System
- Training & Awareness

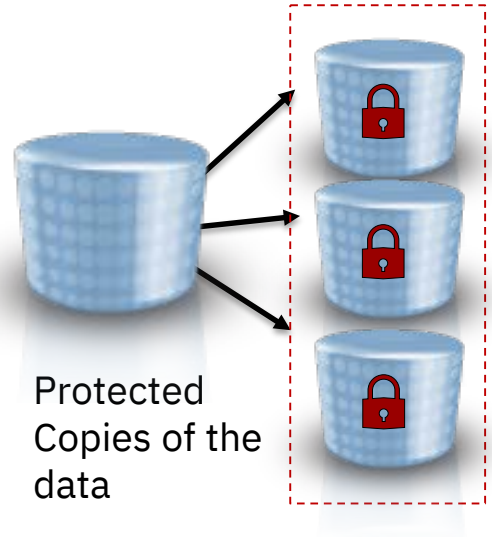


Click here to know more about IBM Business Resiliency Services

Concepts

Key storage requirements to increase cyber resiliency

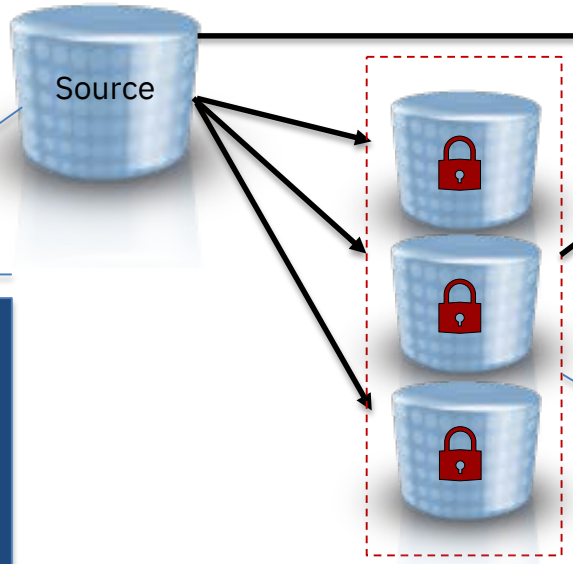
1. Provide additional security capabilities to prevent privileged users from compromising production data as well as protected copies of the data



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

Logical protection copies



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 are used to logically restore back data to the production environment or to investigate a problem and determine what the recovery action is

Protection devices provide one or more logical protection copies and are not accessible by any system. Additional security measures aim to protect these from being modified or deleted due to user errors, malicious destruction or ransomware attacks

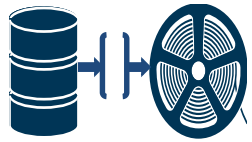
Use cases for protection copies

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

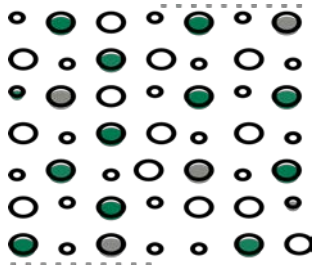


Offline Backup
Backup the copy of the environment to offline media to provide a second layer of protection

Requirement for Logical Data Protection

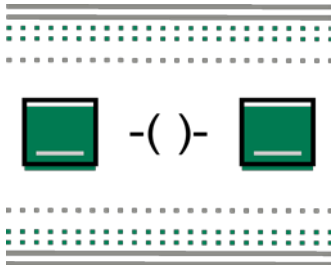
In additon to traditiona high availability and disatster recovery, there are some requirements to provide complete protection against content level destruction of data.

The major design requirements for logical corruption protection are:



Granularity

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



Isolation

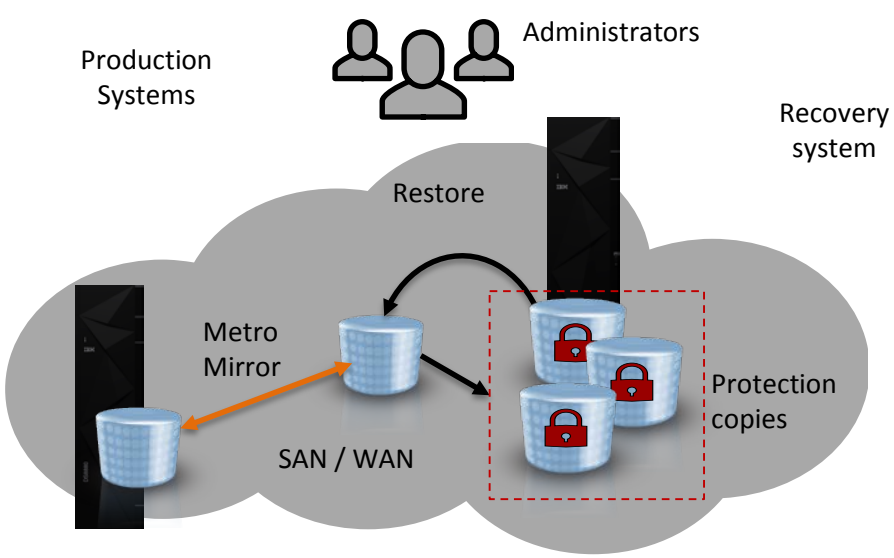
The safety copies must be isolated from the active production data so that it cannot be corrupted by a compromised host system (this is also known as air gap)

Immutability

The safety copies must be protected against unauthorized manipulation

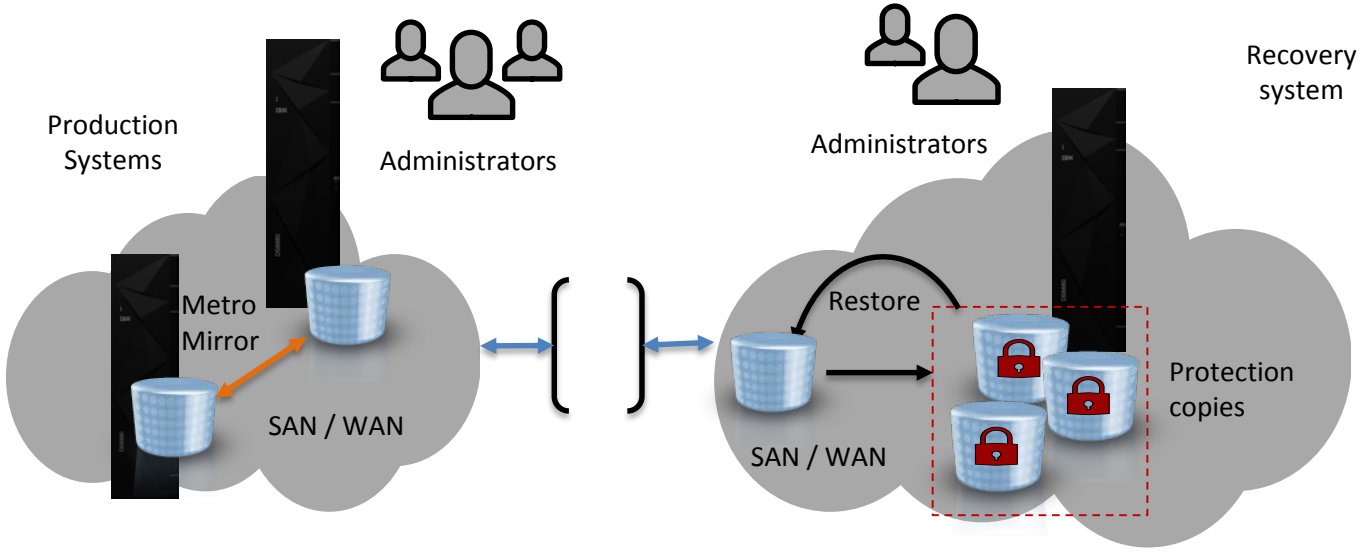
Virtual and physical isolation of protection copies

Virtual isolation



- ✓ The protection copies are created in one or more storage systems in the existing high availability and disaster recovery topology
- ✓ The storage systems are typically in the same SAN or IP network as the production environment

Physical isolation



- ✓ Additional storage systems are used for the protection copies
- ✓ The storage systems are typically not on the same SAN or IP network as the production environment
- ✓ The storage systems have restricted access and even different administrators to provide separation of duties

Safeguarded Copy Overview

Objectives for Safeguarded Copy

1. Allow creation of many recovery copies across multiple volumes or storage systems with optimized capacity usage and minimum performance impact

2. Secure the data for the Safeguarded Copies to prevent it from being accidentally or deliberately compromised

3. Enable any previous recovery point to be made available on a set of recovery volumes while the production environment continues to run

4. Do not consume DS8000 device numbers and host device addresses (UCBs in mainframe environments)

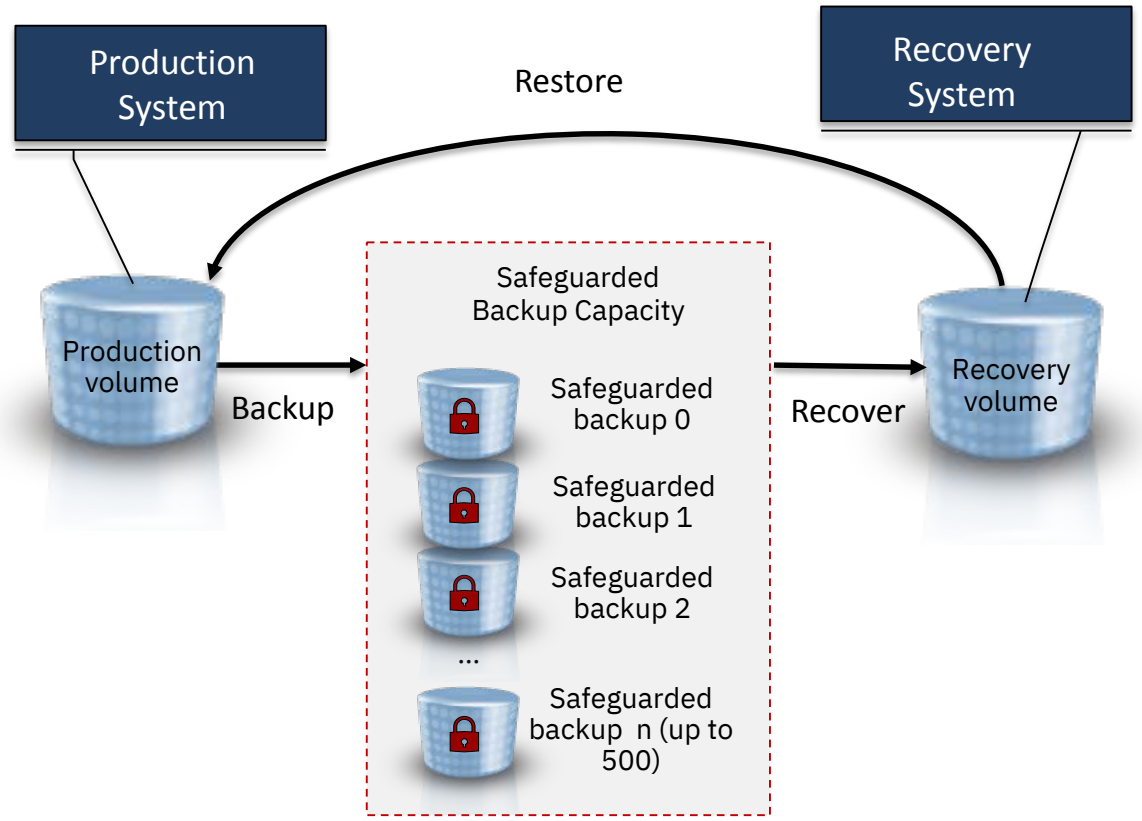
- Safeguarded Copy does not replace FlashCopy and both technologies remain relevant in Logical Corruption Protection scenarios

- FlashCopy provides an instantly accessible copy of a production volume or and for multiple FlashCopies where each copy is independent from the others

Safeguarded Copy for logical data protection

IBM DS8880 Safeguarded Copy prevents sensitive point in time copies of data from being modified or deleted due to user errors, malicious destruction or ransomware attacks

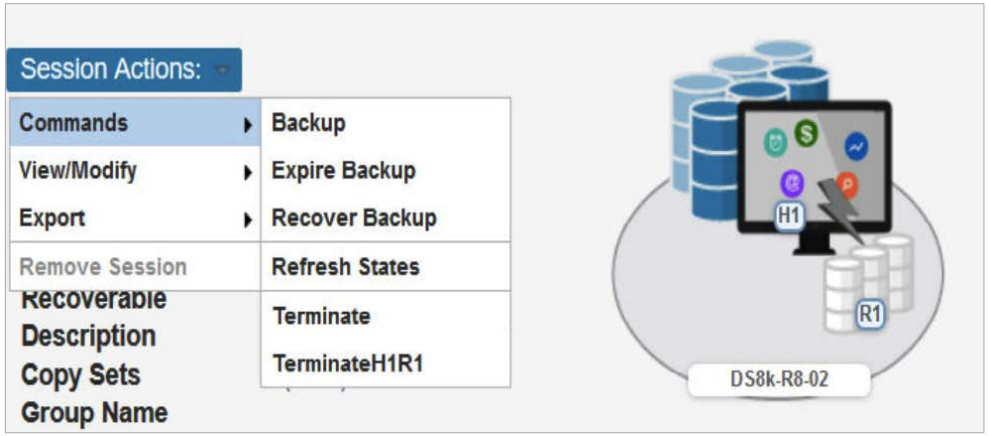
1. Safeguarded Copy provides functionality to create up to 500 recovery points for a production volume
2. These recovery points are called Safeguarded Backups
3. The Safeguarded Backups are stored in a storage space that is called Safeguarded Backup Capacity (SGBC)
4. The Safeguarded Backups are hidden and non-addressable by a host
5. The data can only be used after a Safeguarded Backup is recovered to a separate recovery volume.
6. Recovery volumes can be accessed using a recovery system and used to restore production data.

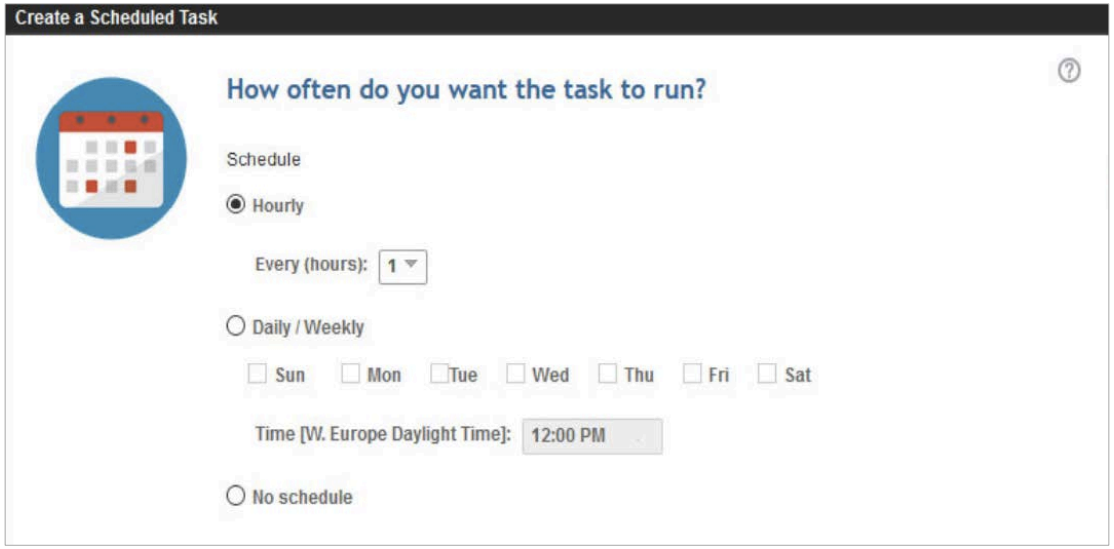


Managing Safeguarded Copies

IBM Copy Service Manager (CSM) provides highly secure and efficient capabilities to manage Safeguarded Copy tasks including:

- Create and monitor Safeguarded Copy sessions.
- Create Safeguarded Copy Backups
  - Manual backups
  - Periodical Backups with CSM Scheduler
- Expire Safeguarded Copy Backups
  - Manual expiration
  - Automatic expiration
- Recover a Safeguarded Copy Backup
- Display Volumes of a Safeguarded Copy Backup
- Terminate a Safeguarded Copy session

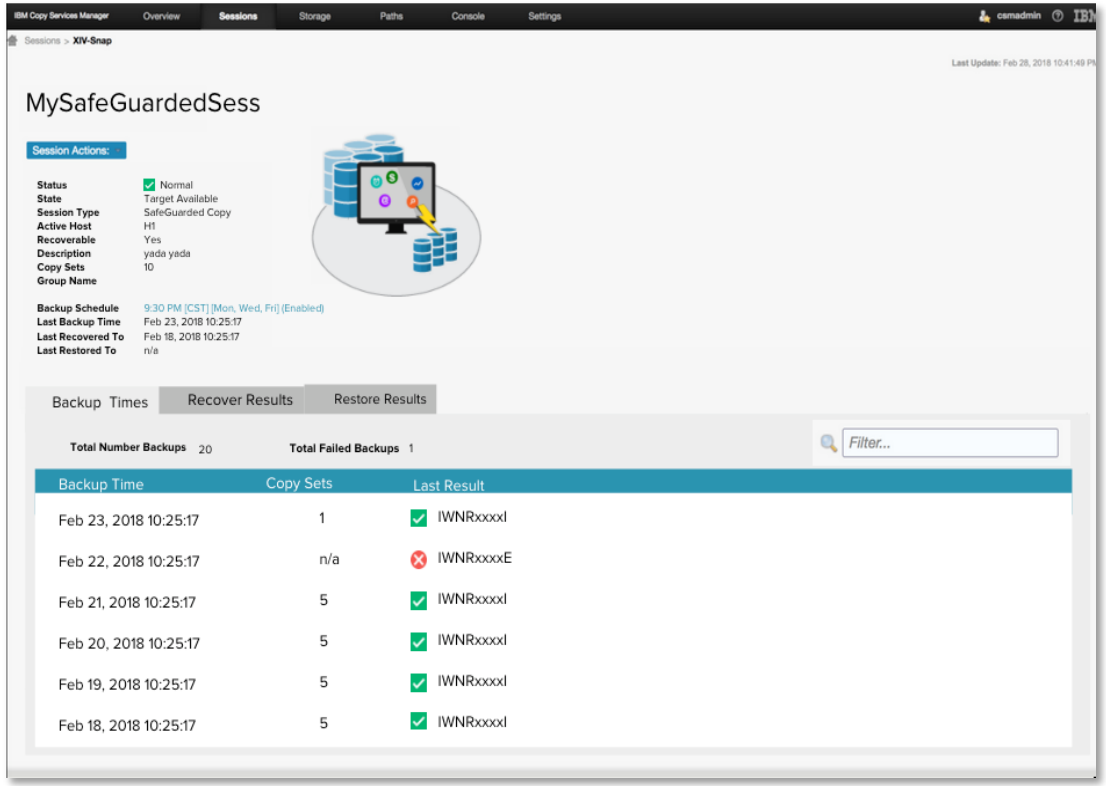




Security considerations

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 DS8880 management interfaces
2. Administrators need at least two interfaces in order to create, enable and manage Safeguarded Copy
   - DS8880 DS CLI or GUI are needed to create Backup capacity
   - IBM Copy Services Manager 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 DS8880 GUI or DSCLI even with the force command



GDPS Support

GDPS Support for Logical Corruption Protection

GDPS 4.1 in March 2018 introduced a new Logical Corruption Protection feature enabled via IFAPRDxx

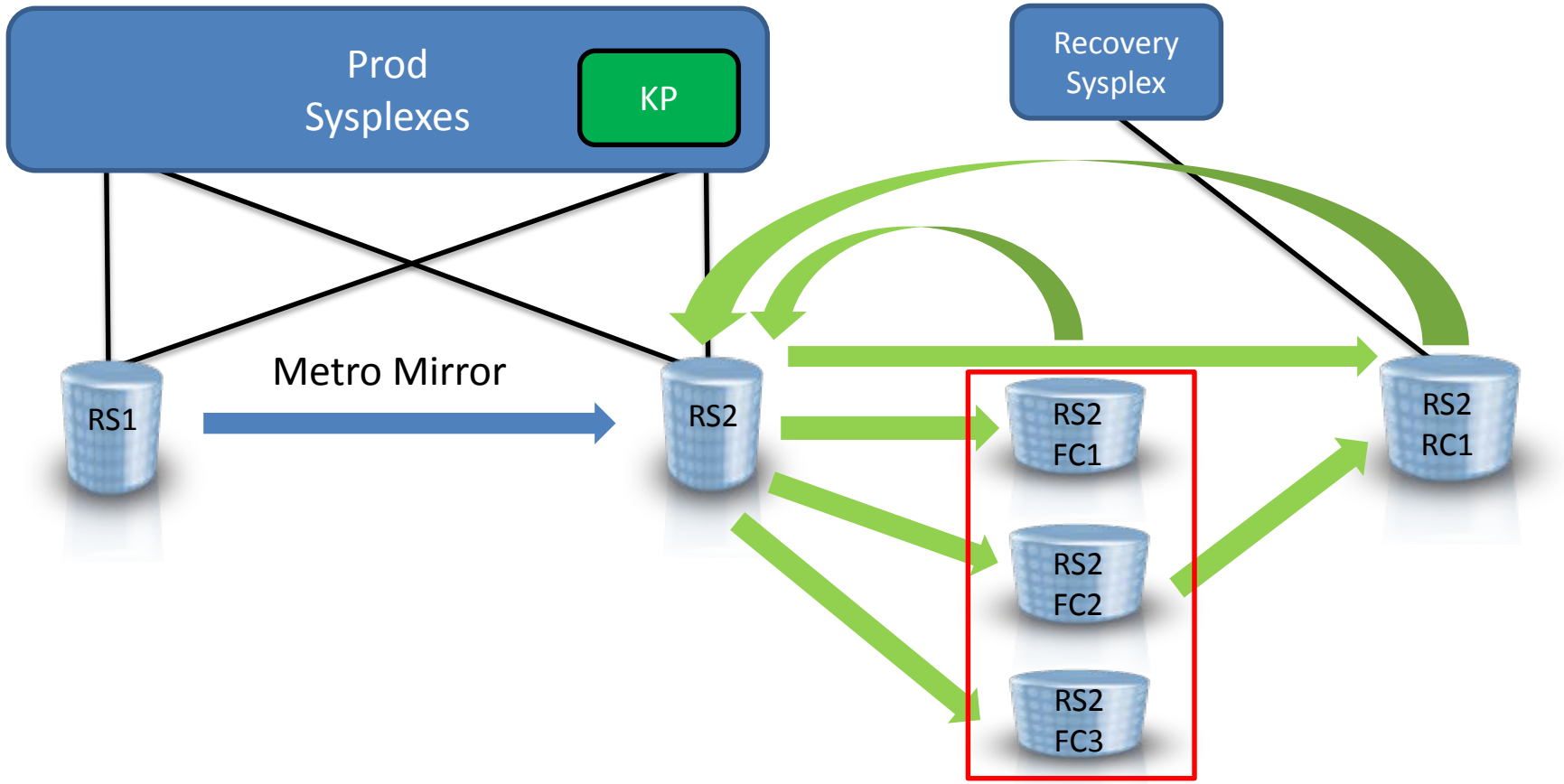
- Enables up to 10 LCP FlashCopies plus a single Recovery Copy
  - No UCB required for these copies in the system taking the Point-in-Time copy
  - UCB required in recovery systems to address the Recovery Copy

- Users must decide between Logical or Physical Isolation topology for their LCP copies
  - First Logical Isolation topology delivered for GDPS Metro
  - First Physical Isolation topology delivered for GDPS Metro Global – GM 4-site solution
    - PROCEDUREs provided to manage the actions required to create PiT copy

- Physical Isolation topologies defined within the GDPS GEOGROUP definition

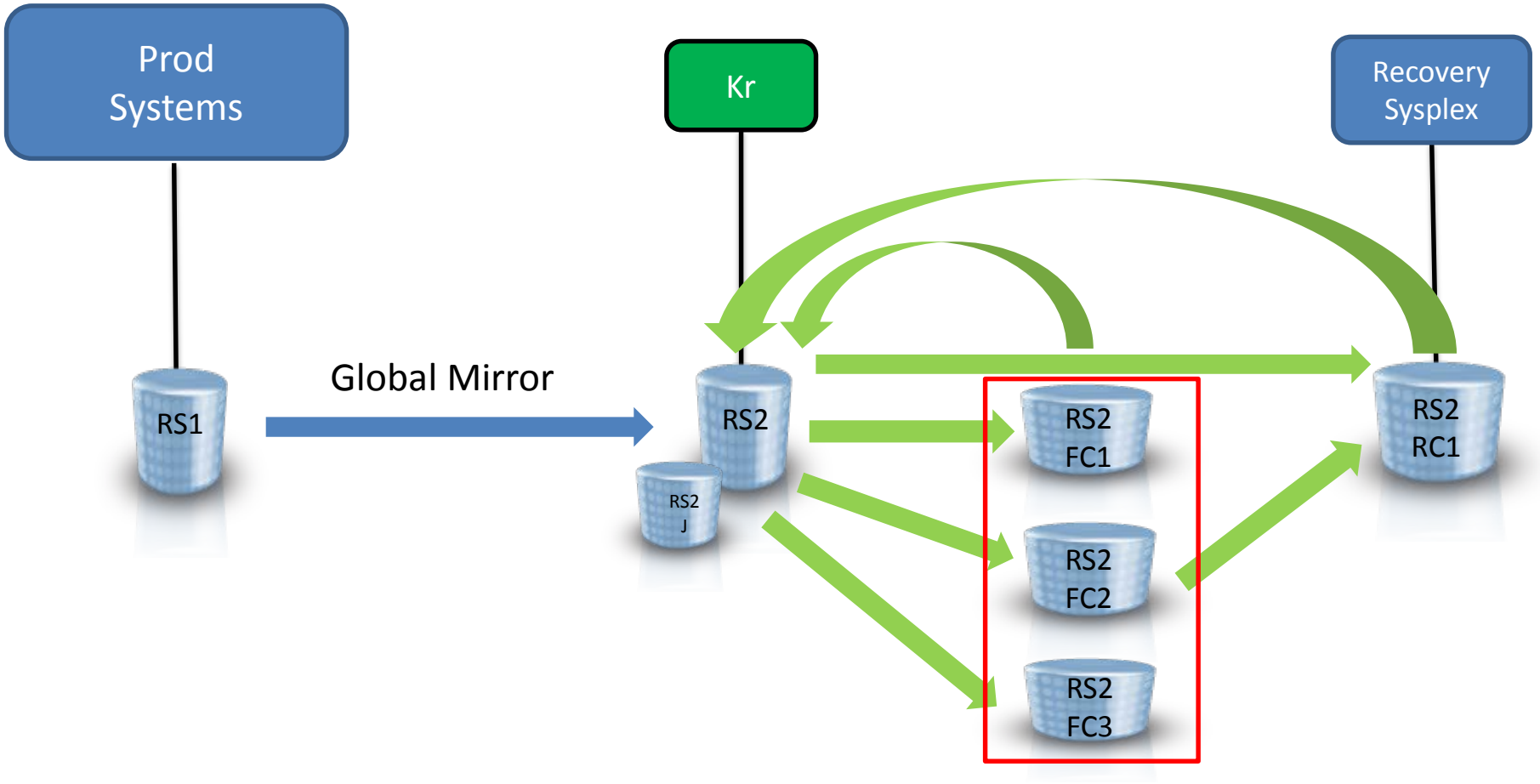
- Additional SPEs planned for delivery during 2018 and 2019 for incremental rollout of function
  - RESTORE and RECOVER being delivered soon

Virtual Airgap examples – GDPS Metro

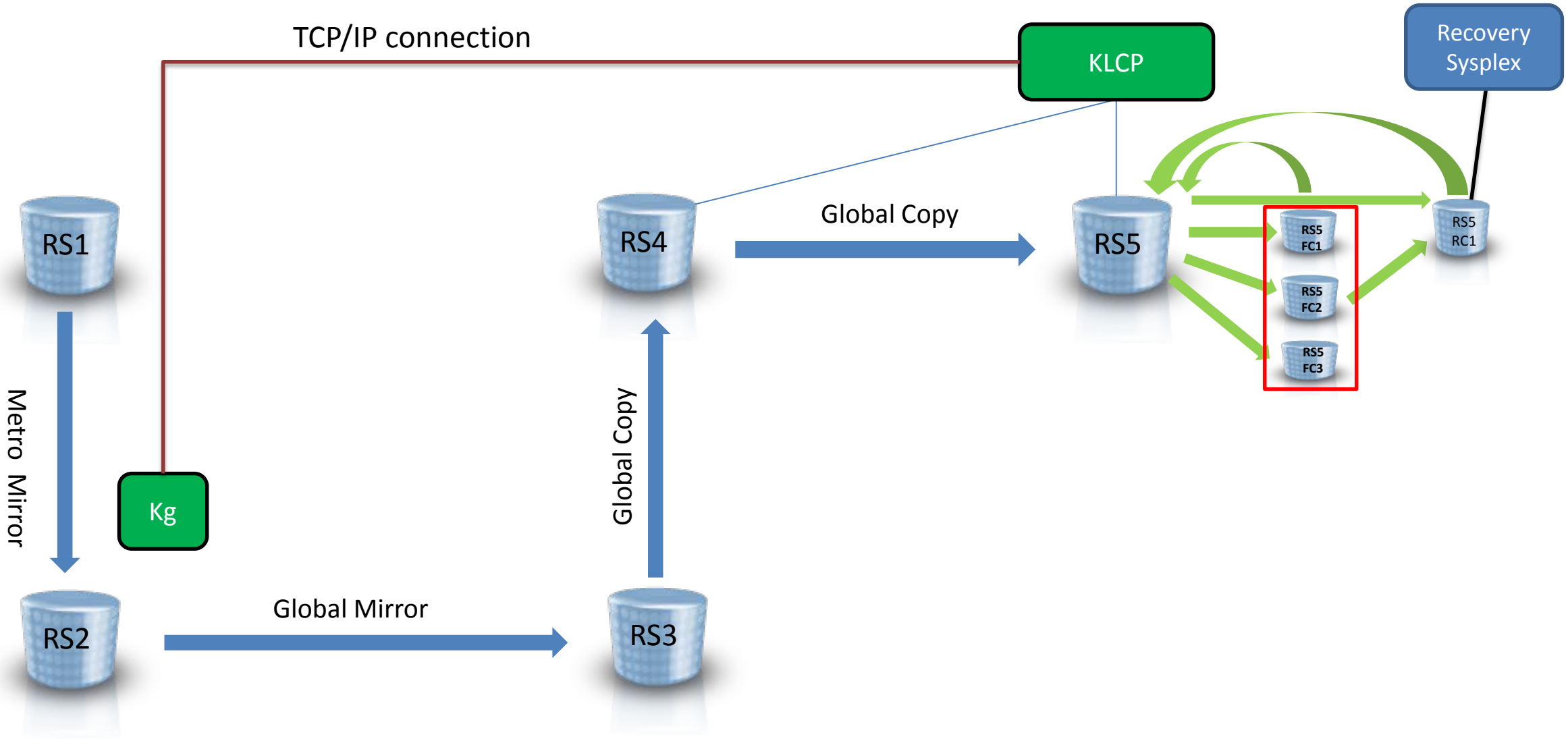


- Consistent FlashCopy creation will cause limited production impact
- LCP Copies can be off RS1 or RS2 copies
- Same applies for Metro Dual Leg configurations

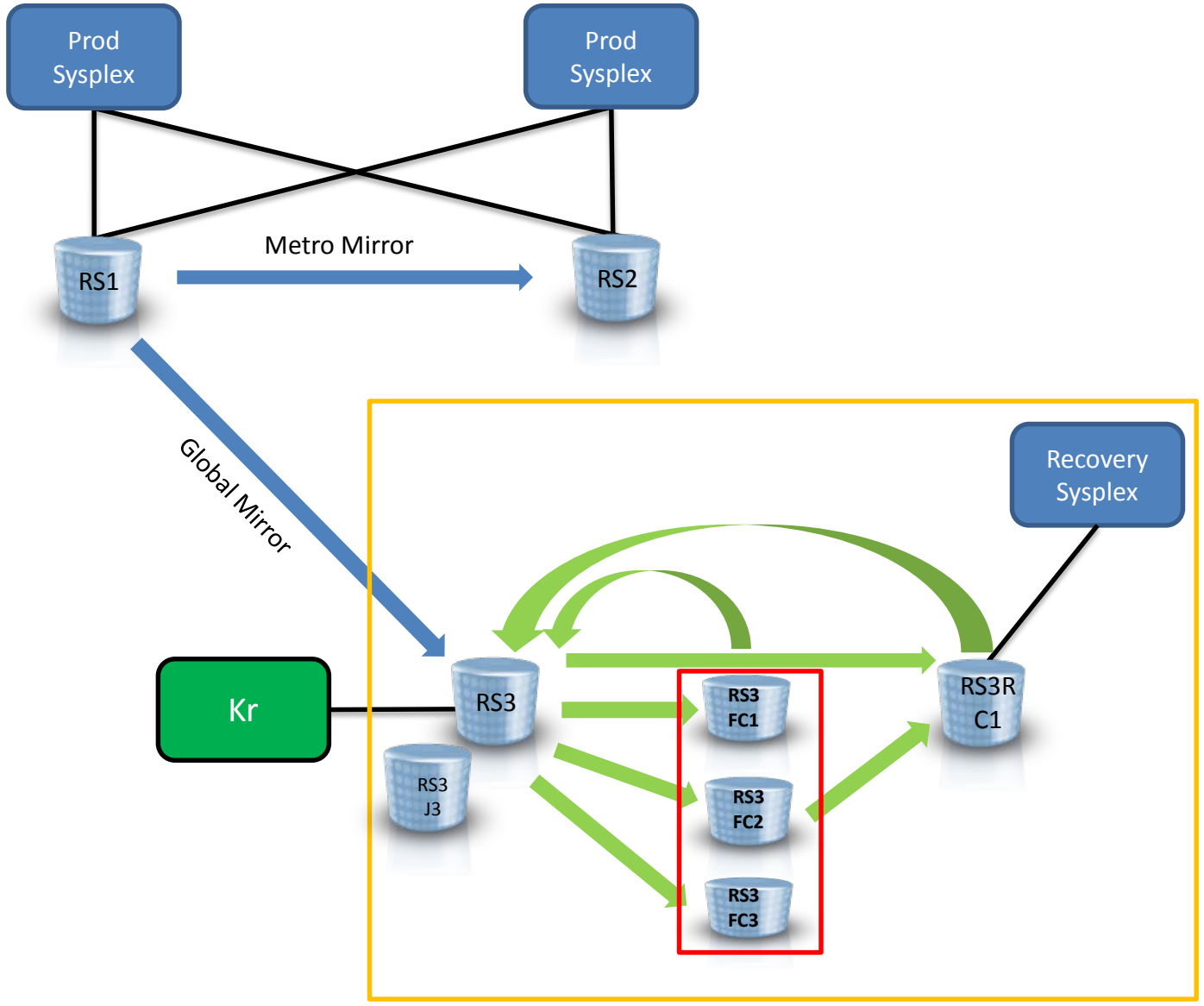
Virtual Airgap examples – GDPS GM



Physical Airgap examples – GDPS MGM 4-site



Physical Airgap examples – GDPS Metro



Logical Corruption Protection Environment physically isolated in Global Mirror secondary site – can be from RS1 or RS2 but needs to be MT capable

GDPS Support – What's next

- GDPS Metro Physical Isolation topology
- GM Virtual Isolation topology
- MGM 3-site support (Physical & Virtual Isolation)
- LCP Management profiles
- Extensions to recover and restore to exploit the LCP management profiles
- MGM 4-site Region Switch procedures with incremental resync
- Safeguarded Copy support
- Security enhancements
- RESTful API for exploitation of other components
- ….

We want your feedback!

- Please submit your feedback online at ….
  - http://conferences.gse.org.uk/2018/feedback/DB

- Paper feedback forms are also available from the Chair person

- This session is DB