GDPS v4.9 Technical Update: New Capabilities for HA, DR, and Cyber Resilience

Steven Cook
GDPS Development
cooksd@us.ibm.com

Megan Hampton
GDPS Development
hamptonm@us.ibm.com

VM Workshop
June 10-12, 2026

IBM

Agenda

- GDPS 4.9 Important Information
- GDPS Metro
- GDPS Global
- GDPS CA
- GDPS LCP Manager
- Data Migration Procedures
- Tech Preview
- Statement of Direction

GDPS 4.9 Important Information

Megan

GDPS Support levels

- The minimum level of z/OS® required to run GDPS 4.9 will be **z/OS 3.1**
- The GDPS 4.9 GUI/REST API Liberty server will require Java 21 runtimes and higher.
- Starting with APAR PH69626 (targeted for 2Q 2026), the GDPS 4.7 and 4.8 GUI/REST API Liberty server will support running in Java 8 runtimes **and higher**, rather than just Java 8 runtimes.

GDPS Solutions

- Capability also available in GDPS HyperSwap Manager will feature the **GDPS HM** tag
- Capability also available in GDPS Metro Global will feature the **GDPS MGM** tag

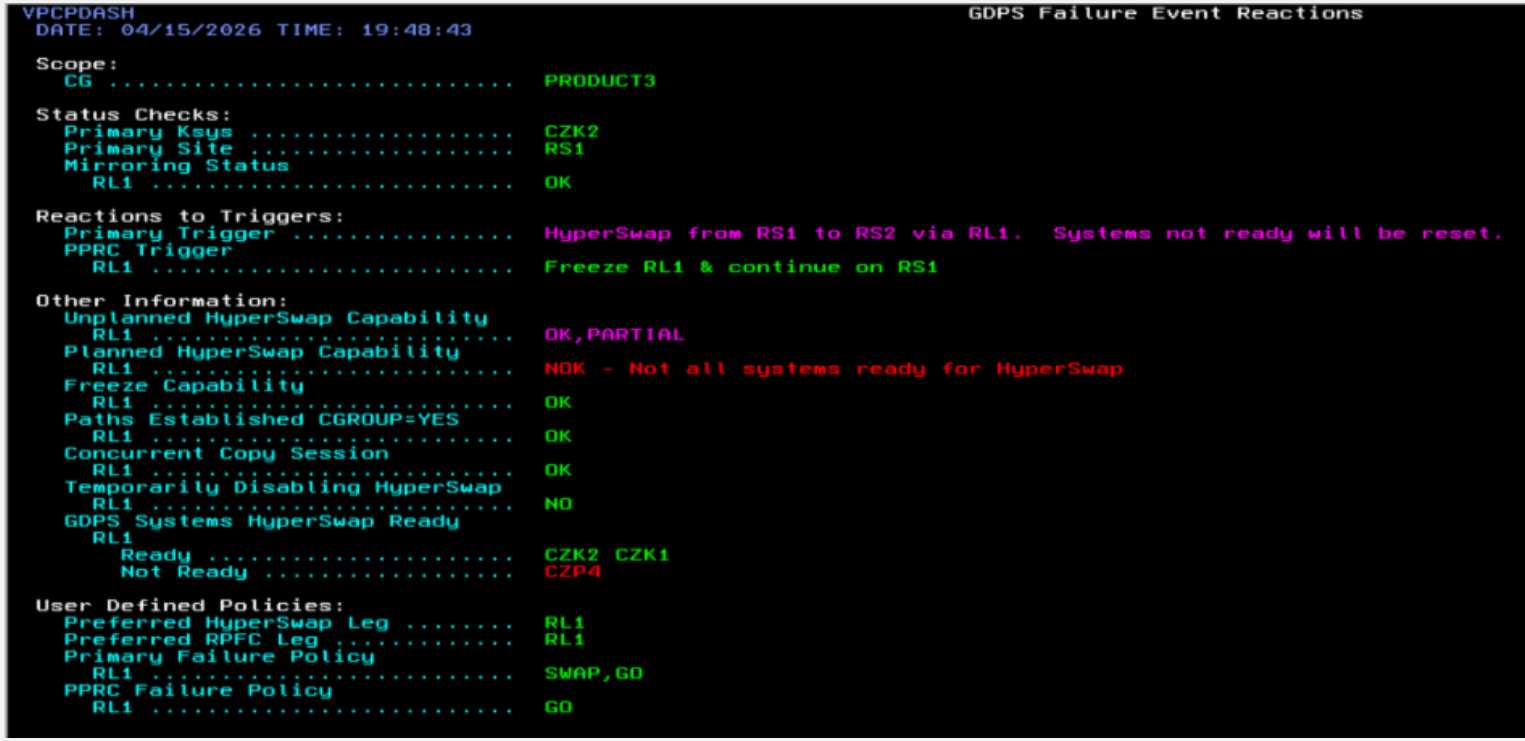
GDPS Metro

Steven

Operational visibility and usability

A new Metro Dashboard 3270 panel provides an at-a-glance view of environment readiness and a plain language summary of how GDPS will react to primary, PPRC, and hybrid failure triggers, helping operators validate expected behavior before taking action.

GDPS GUI support will be available via SPE after GA



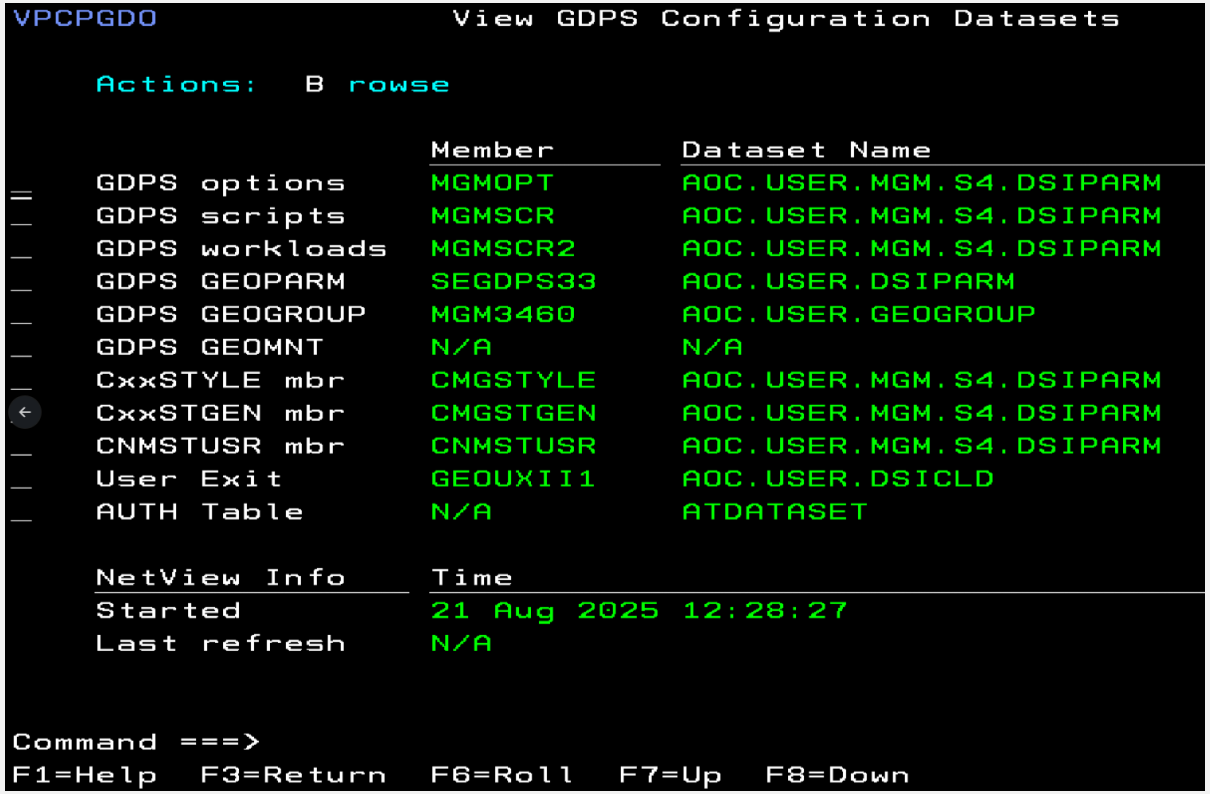
Operational visibility and usability

A new Configuration Information 3270 panel enables read-only browsing of key GDPS and NetView configuration members from the 3270 interface, making it easier to verify critical configuration without requiring TSO access.

Selected 3270 panels now adapt to the terminal screen size instead of being limited to 24x80, with support up to 62x160 on eligible panels, improving readability and reducing scrolling.

GDPS GUI support will be available via SPE after GA

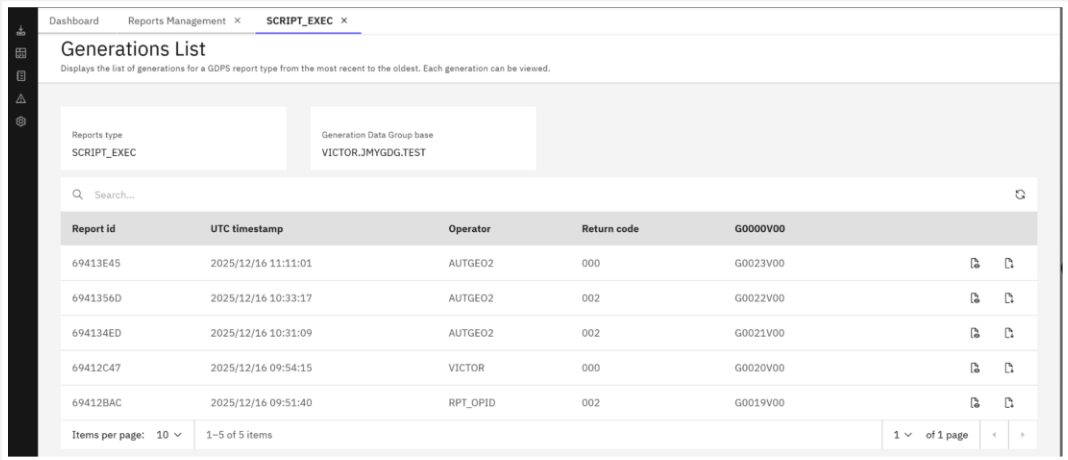
Auditing for Role-based security has been enhanced to provide a new GEO message detailing all security actions taken in GDPS

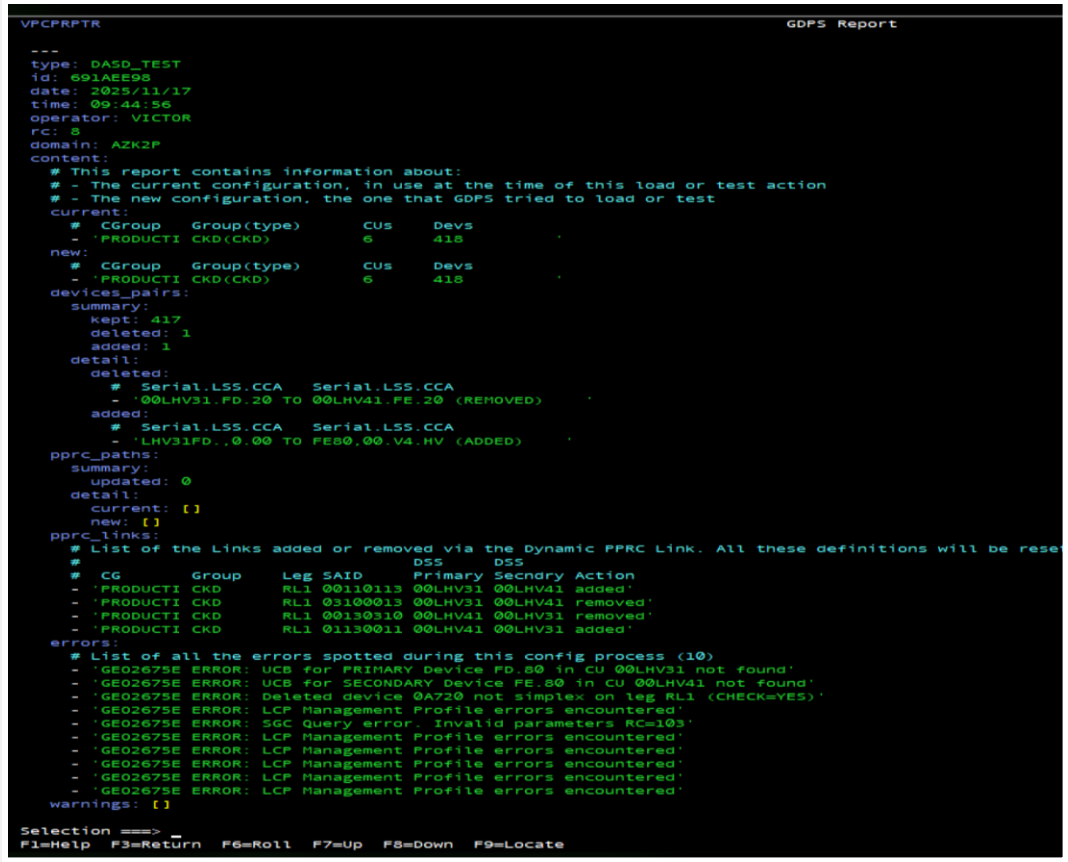


Standardized YAML reports

GDPS Metro now generates standardized YAML reports that are retained as multiple historical versions (GDG generations).

Reports are created automatically when validating or updating key configuration artifacts such as DASD configuration, site table, options, and scripts, and for selected operational executions (for example, script execution and HyperSwap).

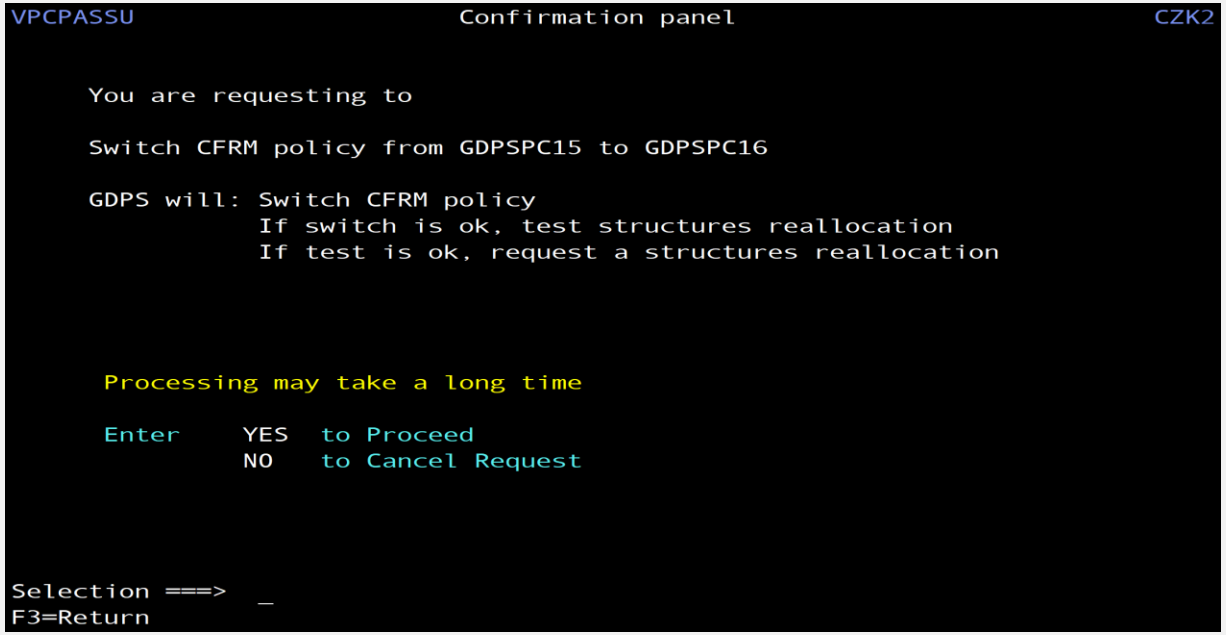




GDPS MGM GDPS HM

Enhanced sysplex management

Coupling facility management is enhanced to reduce risk when activating new CFRM policies: GDPS performs a DISPLAY XCF/REALLOCATE TEST first and proceeds with the reallocate only when the test indicates it can complete successfully.



Improved problem determination

A new informational message (GEO562I) is issued when GDPS is about to stop or reset systems as part of unplanned processing, improving problem determination by logging that a removal/reset is happening and providing the associated reason.

Before
GDPS was killing systems as part of unplanned event within raising specific alerts or messages that can be trapped

After
A new dedicated GEO562I message will be issued every time GDPS has to kill a system or every time a system is killing itself. Objective is to simplify problem determination and to allow customer to automatically react to this kind of event if they want.

New messages:
GEO562I SYSTEM ' sys' WILL BE REMOVED/RESET REASON: FREEZE
GEO562I SYSTEM ' sys' WILL BE REMOVED/RESET REASON: HYPERSWAP FAILED (MVS QUIESCE)
GEO562I SYSTEM ' sys' WILL BE REMOVED/RESET REASON: PRIMARY EVENT
GEO562I SYSTEM ' sys' WILL BE REMOVED/RESET REASON: Wrong subchannel set (MVS QUIESCE)
GEO562I SYSTEM ' sys' WILL BE REMOVED/RESET REASON: SPLIT SYSPLEX EVENT

Availability improvements

Consistent FlashCopy processing no longer briefly disables HyperSwap.

HyperSwap protection will remain enabled while GDPS coordinates the consistent FlashCopy operation, reducing exposure during consistency activities.

Before
HyperSwap capability had to be suspended during the execution of the consistent FlashCopy to prevent potential problems.

Typical messages visible from SDF when using Consistent FlashCopy:

```
GEO089I Consistent FlashCopy I/O queueing started
Disabling HyperSwap prior to ConsistentFlashCopy on leg RLx
HYPERSW DISABLE LEG(RLx)
GEO090I Consistent FlashCopy I/O queueing ended
Attempting to re-enable HyperSwap on leg RLx
HYPERSW ON LEG(RLx)
HyperSwap is re-enabled on leg RLx
```

In a large config, this suspension can take several seconds

After
No HyperSwap disablement required anymore during a Consistent FlashCopy action.
No exposure anymore if an unplanned event occurs during the execution of the consistent FlashCopy.

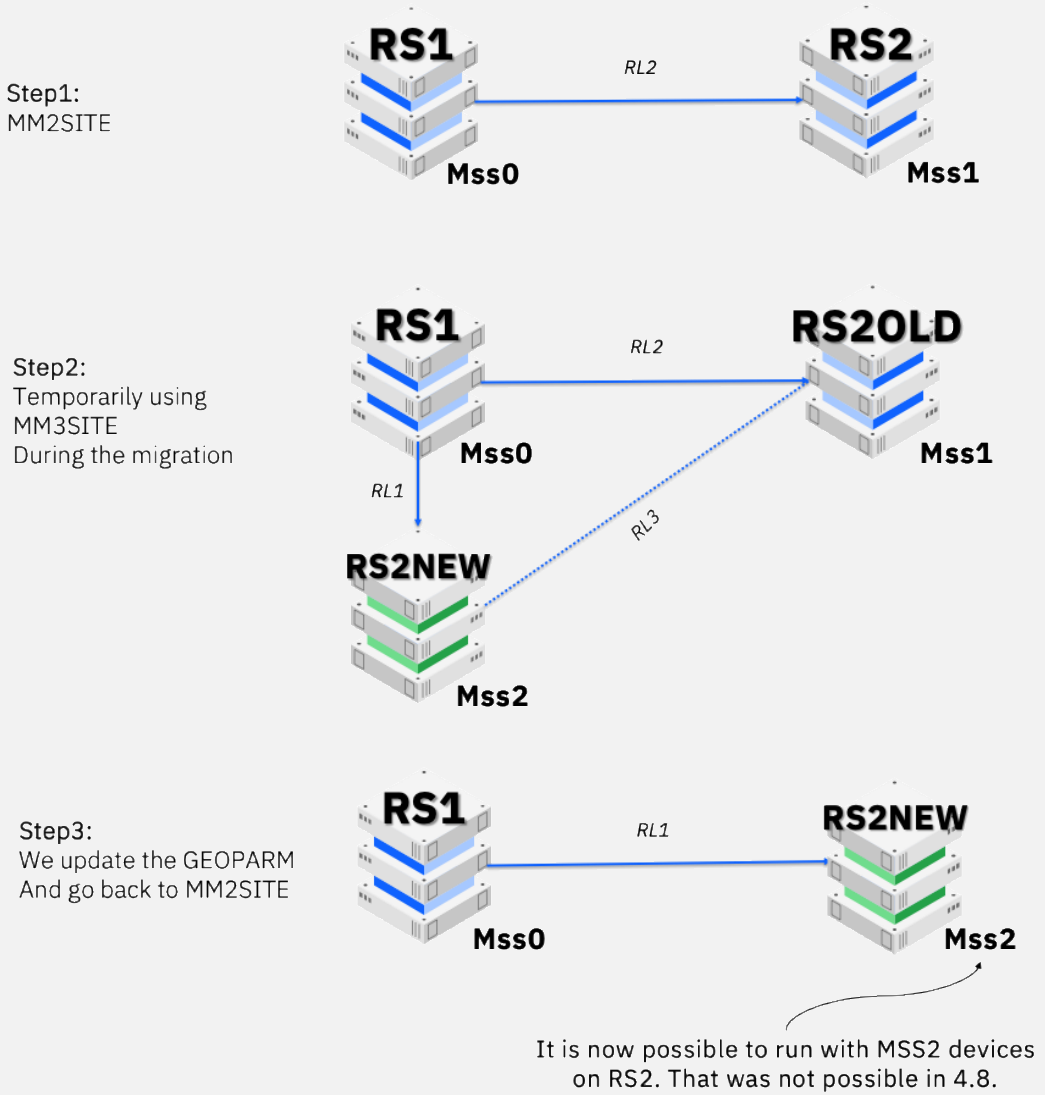
Typical messages visible from SDF when using Consistent FlashCopy after this code change:

```
GEO089I Consistent FlashCopy I/O queueing started
GEO090I Consistent FlashCopy I/O queueing ended
```

DASD configuration flexibility

Subchannel-set (MSS) rules are relaxed to allow more flexible device-to-site mappings, reducing unnecessary constraints during DASD migration and technology refresh scenarios while preserving HyperSwap and freeze protections.

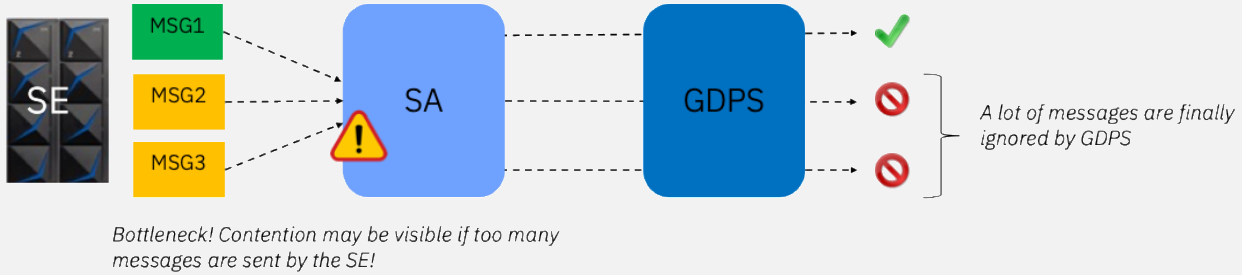
MSS3 devices will soon be supported in GDPS Metro



BCPii Message Filtering

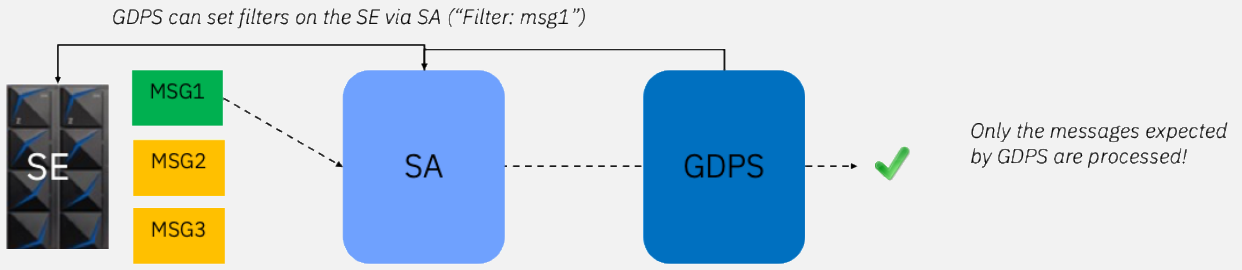
BCPii message filtering improves the reliability of message-driven IPL monitoring by subscribing only to the message patterns GDPS requires, reducing contention from high-volume message streams during load processing.

Before:
- All BCP messages sent from SE to GDPS through SA causing contention



Bottleneck! Contention may be visible if too many messages are sent by the SE!

After:
- GDPS can tell SA the messages that he wants to receive (via a CGLOBAL)
- SA will ask the Support Element to set some filters accordingly
- Messages are filtered and only the messages needed by GDPS are sent by the SE through SA.

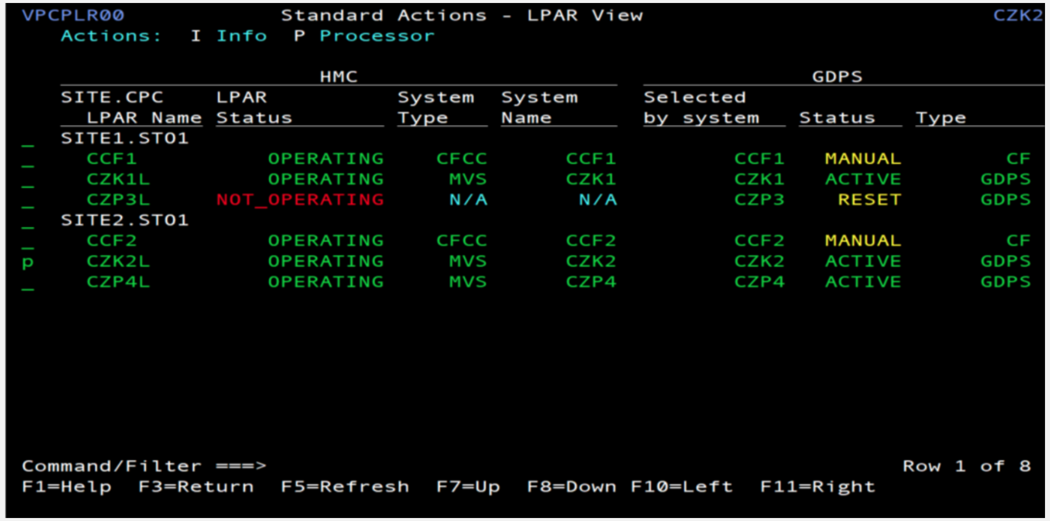


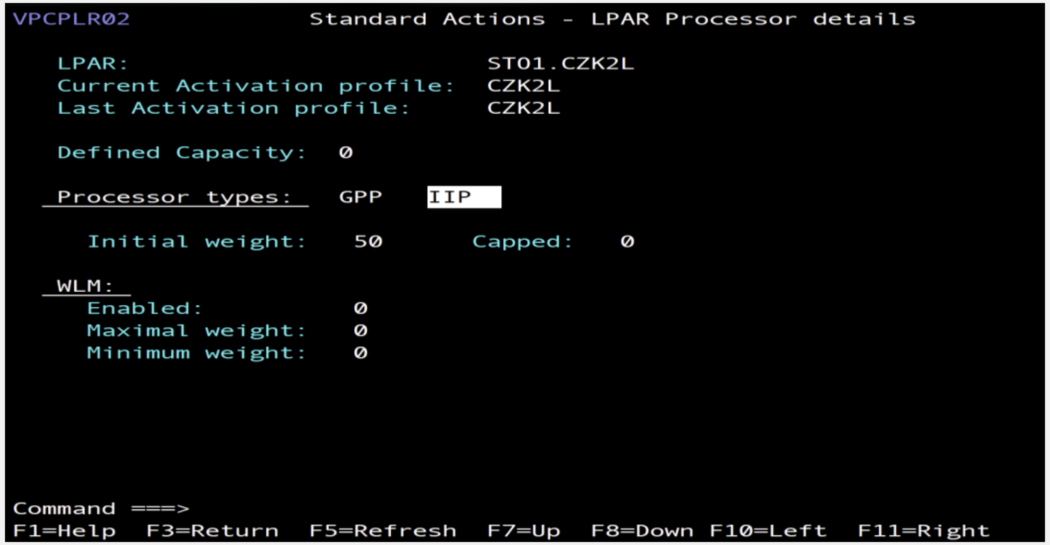
Lower risk of contention, only the filtered messages are sent to SA

View and update LPAR Image (ICNTL) values

LPAR capacity and weight management is extended through BCPii to allow operators and automation to view and modify key LPAR attributes such as defined capacity and processing weights.

Support is provided through panels, with the new CAPACITY ICNTL script statement, and REST APIs.





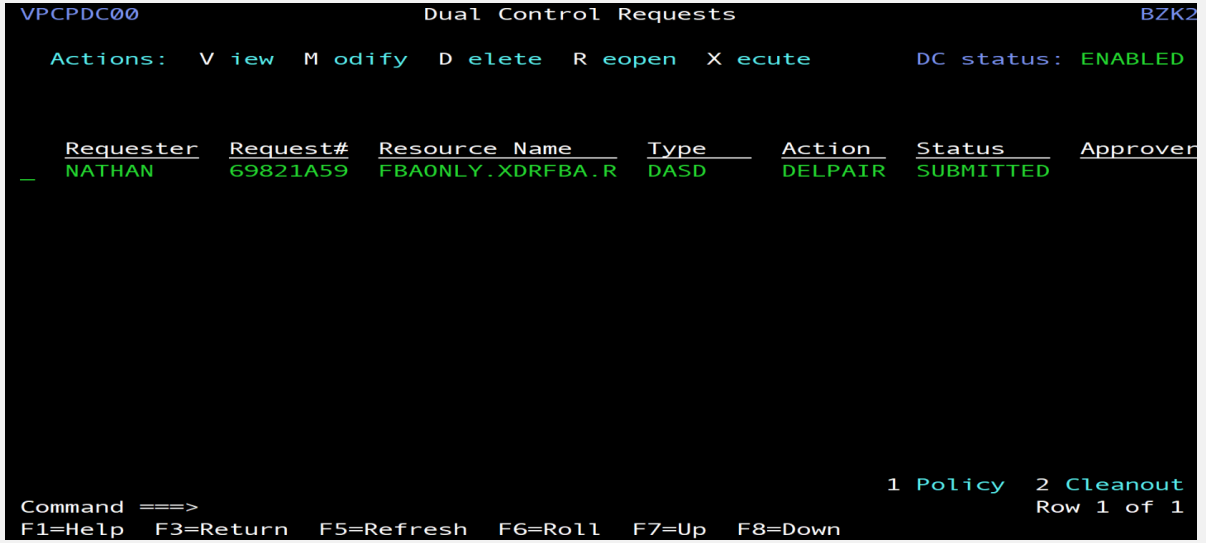
Dual control for config and DASD actions

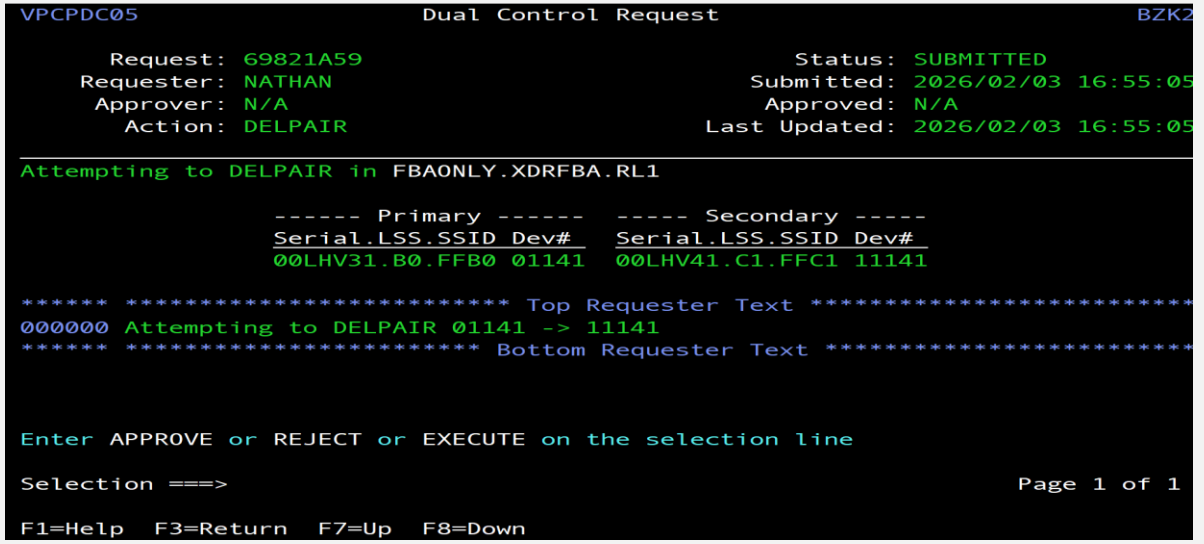
GDPS 4.9 introduces dual control protection for selected high-impact configuration and storage actions, reducing the risk of unintended or unauthorized changes. When enabled, sensitive actions—such as refreshing or loading configuration changes and DELPAIR operations—require separation of duties between the requester and an authorized approver.

Requests are tracked through a dedicated interface, where approvers can review and act based on defined roles. Policy-driven controls provide flexibility while strengthening governance, auditability, and operational safety for critical GDPS activities.

4.9 update includes protection for:

- DASD: Delpair device pairs
- CONFIG:
  - Load GDPS Configuration
  - Refresh GDPS Options





GDPS Global

Megan

Enhanced check state validation for DASD config changes

New enhancements to the check state validation used when changing the Global Mirror disk storage configuration.

In addition to verifying that devices being removed are in a SIMPLEX state, GDPS now performs broader consistency checks, including ensuring that primary devices and logical subsystems are not joined to an active GM session, that FlashCopy relationships are not present where unsupported, and that session-level attributes are not modified while a session is active.

Check State

When set to YES, this option will tell GDPS to check that:

- Devices removed are in a SIMPLEX state
- GM primary devices removed are not joined to the GM session
- GM primary LSSs removed are not defined to the GM session
- GMFC devices removed are not in a FC relation
- FC1 devices removed are not in a FC relation
- A GM session removed is not active
- Changing SNBR is not done on an active session
- Changing utility devices LSS for the session master disk subsystem is not done on an active session

A check that fails will result in failure of the whole config action without any changes being done. Setting this to NO tells GDPS to not perform these checks or just issue warnings in some cases. The default is YES.

MTFO default changed to YES for GM2SITE topologies

With GDPS 4.9, the MTFO option for GM2SITE topologies now defaults to MTFO(YES). Previously, MTFO defaulted to NO and had to be explicitly enabled.

During migration from GDPS 4.8, environments that require the existing behavior must explicitly specify MTFO(NO); otherwise, MTFO(YES) is assumed.

Migrating GDPS code from 4.8 to 4.9

For a classic migration, also known as a rolling migration, take the following steps:

1. With both K-sys and R-sys at the 4.7 GDPS level.
2. Stop and restart the K-sys (or R-sys) at the 4.8 code level.
3. Stop and restart the R-sys (or K-sys) at the 4.8 code level.

> **Note:** the big bang approach is also available.

|< GDPS Global - GM 4.9 change the topology option MTFO() default from MTFO(NO) to MTFO(YES). For more information, see GDPS Options. If the MTFO() option is not specified on the GM2SITE options keyword, then it must be either:

1. Explicitly specified as MTFO(NO) if the current default MTFO(NO) setting is to be kept as is, or
2. Specified as MTFO(YES) if changing the environment into to a multi-target capable or tolerant one. This must be combined with any other changes needed for multi-target support. For more information, see GDPS and Multi-target PPRC considerations.

Explicitly specifying MTFO(NO) or changing to MTFO(YES) must be done before any Kg or Kr is migrated to 4.9. Note that a MTFO(NO) to MTFO(YES) (or vice versa) change also requires a DASD config and that **`GDPSCHG MIGRATE GMMODE`** is used on any running GM sessions so the GM joins are converted to the correct type. For further information, see GDPSCHG. >|

>|

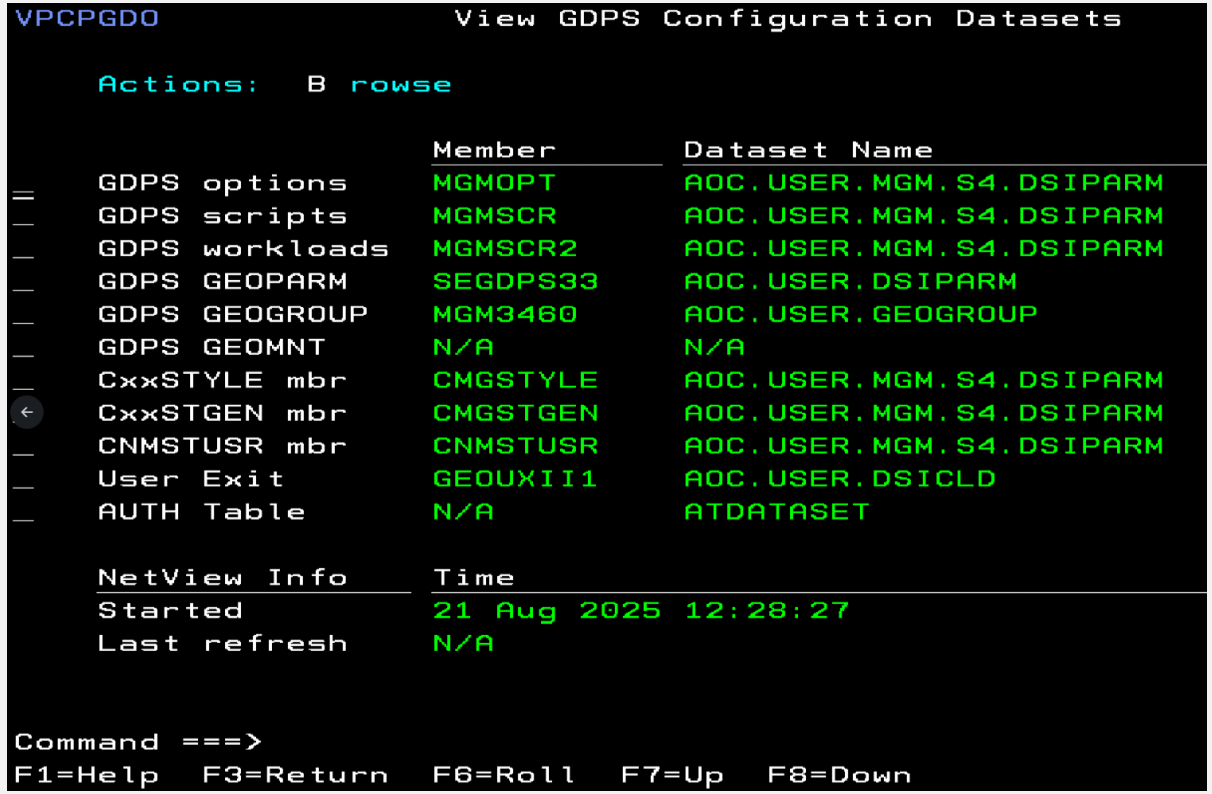
Operational visibility and usability

A new Configuration Information 3270 panel enables read-only browsing of key GDPS and NetView configuration members from the 3270 interface, making it easier to verify critical configuration without requiring TSO access.

Selected 3270 panels now adapt to the terminal screen size instead of being limited to 24x80, with support up to 62x160 on eligible panels, improving readability and reducing scrolling.

GDPS GUI support will be available via SPE after GA

Auditing for Role-based security has been enhanced to provide a new GEO message detailing all security actions taken in GDPS



View and update LPAR Image (ICNTL) values

LPAR capacity and weight management is extended through BCPii to allow operators and automation to view and modify key LPAR attributes such as defined capacity and processing weights.

Support is provided with the new CAPACITY ICNTL script statement, and REST APIs.

```
VPCPFLFX                        View Planned Action                        CZK2


Requested action: AMODC02091_13                          Number of steps: 2
Script Group:     SCRDFLT
      Nbr  Script statement
      1    COMM=CAPACITY ICNTL OK: PT + PWI
      2    CAPACITY=ICNTL LPAR(STO1.CZK2L) PT(IIP) PWI(50)
```

```
VPCPFLFX                        View Planned Action                        CZK2


Requested action: AMODC02091_10                          Number of steps: 2
Script Group:     SCRDFLT
      Nbr  Script statement
      1    COMM=CAPACITY ICNTL OK: DEFCAP UPDATE
      2    CAPACITY=ICNTL LPAR(STO1.CZK2L) DEFCAP( 0)
```

Enhanced 3270 panels

GDPS 4.9 introduces a refreshed set of 3270 panels to improve usability and consistency with the broader GDPS user interface.

The updated panels modernize the layout and presentation of Global Mirror information, making session status, device relationships, paths, and copy activity easier to interpret during day-to-day operations.

```
VPCPMSR1  GDPS Global - GM  Kr-sys       REMOTE view                    MVS2
Actions:  V View

Session:  02  PROD2      Status: RUNNING   LSSs: 4    Pairs: 144

       Primary      ->  Secondary
 Type  CU / LSS         CU / LSS                      Pairs
_ CKD DS8910_1/48 ->  DS8910_3/4A                      64
_ CKD DS8910_1/4B ->  DS8910_3/4D                      16
_ CKD DS8910_2/4B ->  DS8910_3/4C                      16
_ FB  DS8910_1/CA ->  DS8910_3/CF                      48
```

```
VPCPMSR1  GDPS Global - GM  Kr-sys       REMOTE view                    MVS

Session:  02  PROD2      Status: RUNNING   LSSs: 4    Pairs: 144
Actions:  V iew

       Primary          Secondary
 Type  CU / LSS     ->  CU / LSS                      Pairs
_ CKD  DS8910_1/48 ->  DS8910_3/4A                     64
_ CKD  DS8910_1/4B ->  DS8910_3/4D                     16
_ CKD  DS8910_2/4B ->  DS8910_3/4C                     16
_ FB   DS8910_1/CA ->  DS8910_3/CF                     48
```

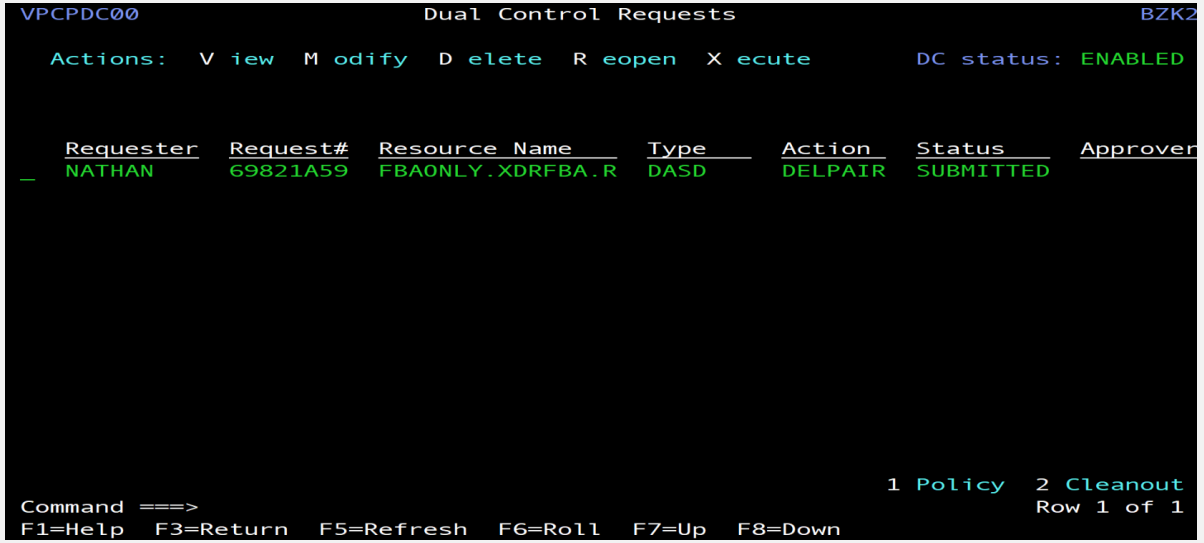
Dual control for config and DASD actions

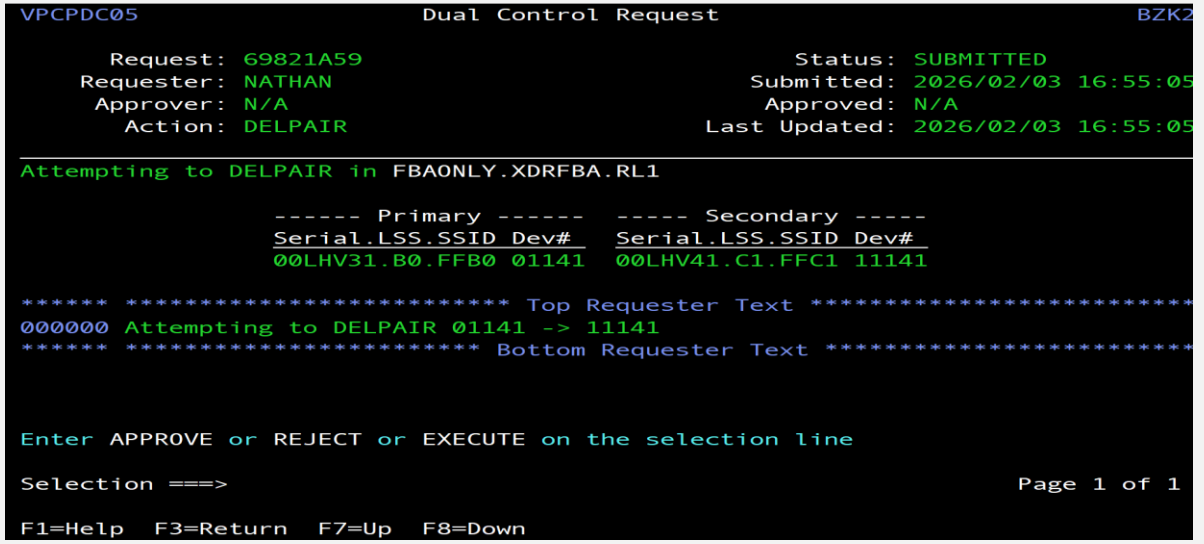
GDPS 4.9 introduces dual control protection for selected high-impact configuration and storage actions, reducing the risk of unintended or unauthorized changes. When enabled, sensitive actions—such as refreshing or loading configuration changes and DELPAIR operations—require separation of duties between the requester and an authorized approver.

Requests are tracked through a dedicated interface, where approvers can review and act based on defined roles. Policy-driven controls provide flexibility while strengthening governance, auditability, and operational safety for critical GDPS activities.

4.9 update includes protection for:

- DASD: Delpair device pairs
- CONFIG:
  - Load GDPS Configuration
  - Refresh GDPS Options





GDPS CA

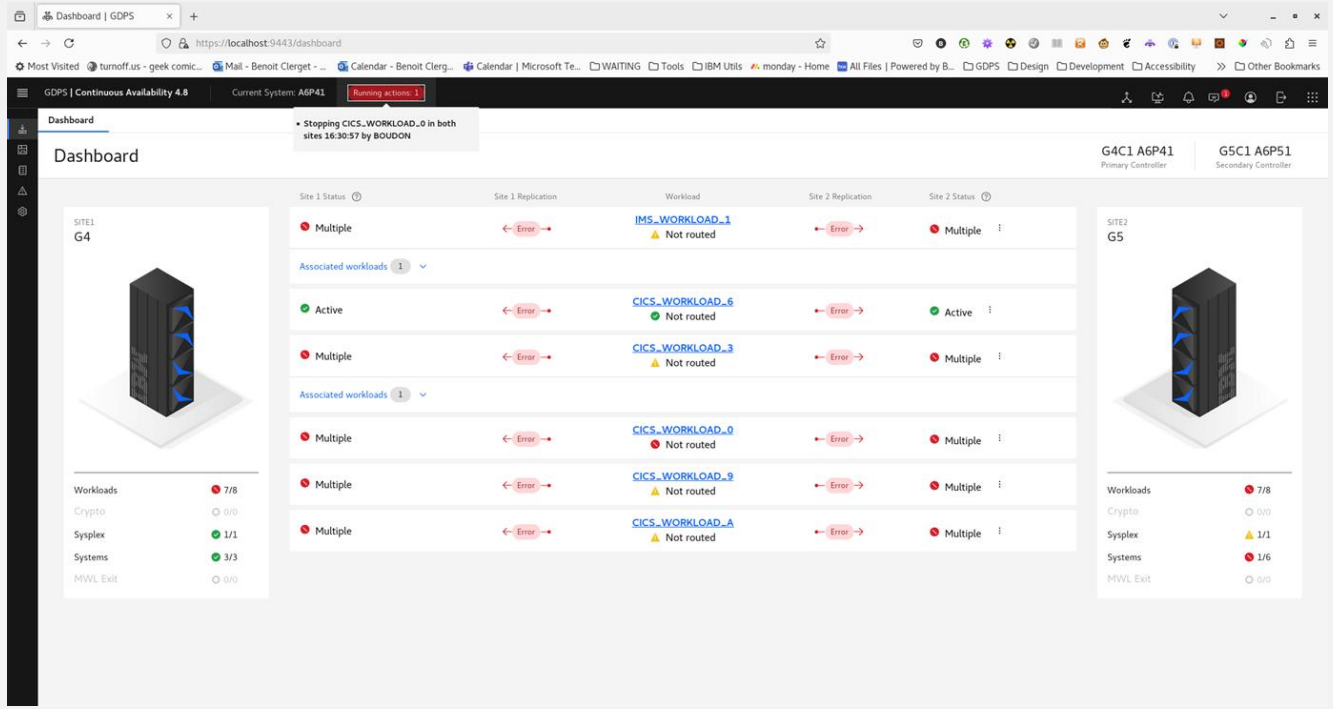
Steven

Updated Graphical User Interface

GDPS 4.9 introduces an updated Graphical User Interface (GUI) for GDPS Continuous Availability.

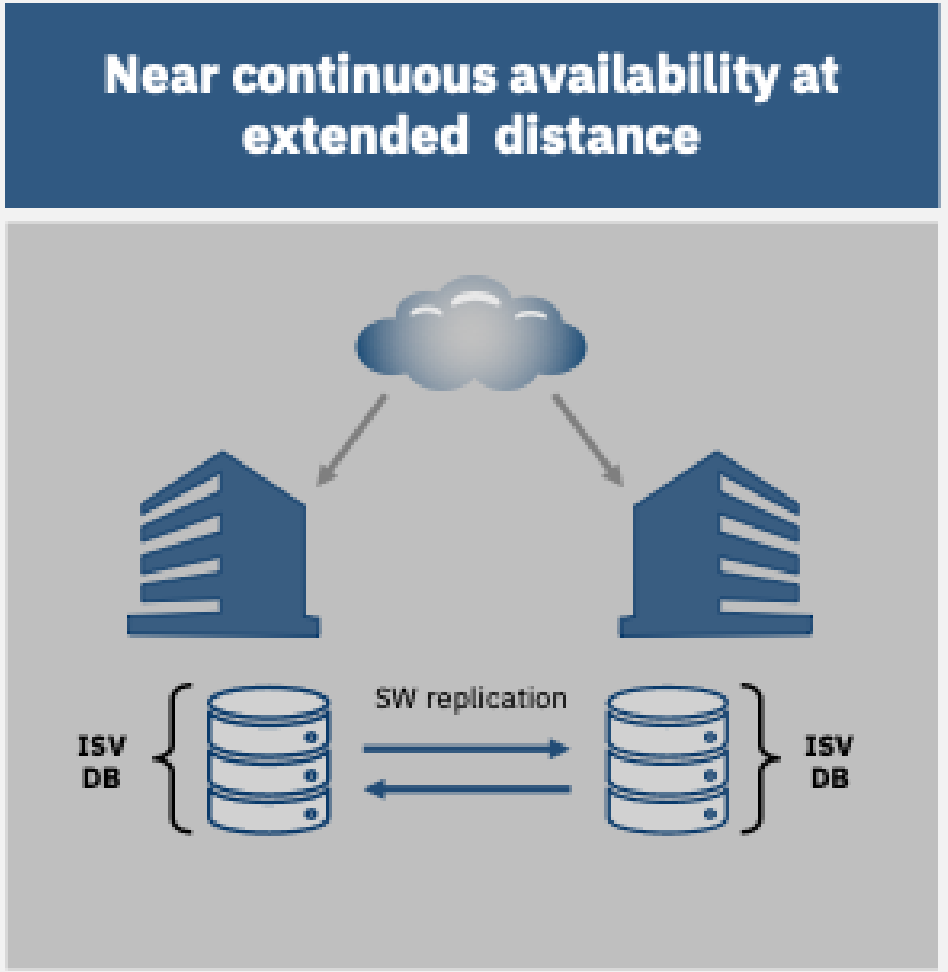
The GUI has been modernized by transitioning from the Dojo framework to the Carbon Design System, providing a more consistent, intuitive, and user-friendly experience.

This update delivers an improved look and feel along with enhanced usability, while preserving existing functionality and workflows.



Support for ISV-Managed Replication Workloads

GDPS Continuous Availability (CA) now supports a new workload type known as an ISV Workload, enabling CA to manage and automate failover for workloads that replicate data using independent software vendor (ISV) replication technologies, rather than IBM-provided Db2, IMS, or VSAM replication solutions.



LCP Manager

Megan

Integrated Type 1 Validation

GDPS 4.9 introduces support for automated Type 1 (Infrastructure) validation of Safeguarded Copy backups within the vault.

Validation in GDPS 4.9 enables the LCP Manager to:

- IPL recovery systems directly from RC(n) copies, collected either via a new capture or from an existing tagged capture.
- Monitor IPL progress using enhanced BCPii message filtering, delivering reliable checkpoint detection even in high-volume environments.
- Record validation results, associate them with captures, and automatically mark intervening captures as *validated*, *failed*, or *in-doubt* based on sequencing.
- Can be integrated with existing Type 2 (Data structure) and Type 3 (Data content) validation.

Figure 2. VPCPLV00, LCP Safeguarded validation summary

```
VPCPLV00       Logical Corruption Protection Safeguarded Validation         GIC3

Management Profile: SGC1VAL1                 Latest Capture: 2026/03/04.14:01:07
 Consistency Group: ZPRODI1.RS1           Latest Validation: 2026/03/04.14:01:13

  Actions:  I nfo

   Validation           Capture    Data Consistency
   UTC TimeStamp        Seqno      UTC TimeStamp         Source    RCn   Status
_  2026/03/04.14:01:13  69A83B23   2026/03/04.14:01:11   RS(1)     001   Failure
_  2026/03/04.13:02:05  69A82D48   2026/03/04.13:02:03   RS(1)     001   Success
_  2026/03/04.11:02:32  69A81143   2026/03/04.11:02:30   RS(1)     001   Success
_  2026/03/04.10:16:49  69A8068C   2026/03/04.10:16:48   RS(1)     001   Success
_  2026/03/04.10:04:53  69A803C0   2026/03/04.10:04:51   RS(1)     001   Aborted
_  2026/03/04.09:33:08  69A7FC4F   2026/03/04.09:33:07   RS(1)     001   Success
_  2026/03/04.08:54:24  69A7F33B   2026/03/04.08:54:23   RS(1)     001   Failure
_  2026/03/04.08:27:53  69A7EA47   2026/03/04.08:16:11   SGC(1)    001   Aborted
_  2026/03/03.16:05:34  69A70682   2026/03/03.16:04:22   SGC(1)    002   Aborted
_  2026/03/03.15:21:33  69A6F0B8   2026/03/03.14:31:24   SGC(1)    002   Aborted
_  2026/03/02.10:23:33  69A56520   2026/03/02.10:23:32   RS(1)     002   Aborted
_  2026/02/27.14:25:28  69A1A953   2026/02/27.14:25:27   RS(1)     001   Failure

Command/Filter ===> _                                                Row 1 of 16
F1=Help  F3=Return  F5=Refresh  F6=Roll  F7=Up  F8=Down
```

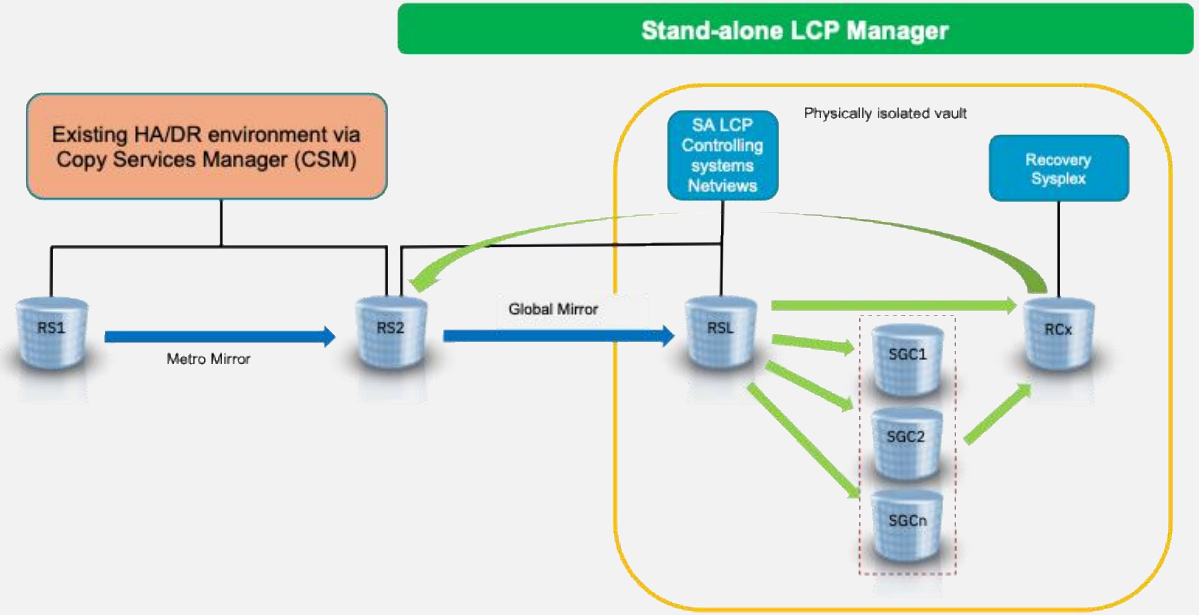
```
_VPCPLVI1                    LCP Validation Information                     GIC3

Management Profile: SGC1VAL1                   Capture Seqno: 69A83B23
 Consistency Group: ZPRODI1.RS1                 Capture Time: 2026/03/04.14:01:07
  Direct FlashCopy: RS(1) to RC(1)          Data Consistency: 2026/03/04.14:01:11
  Validation Seqno: 69A83B29                Validation Start: 2026/03/04.14:01:13
 Validation Status: Open                      Validation End: ..................

Validation                        Starting             Ending
Step          Status              UTC TimeStamp        UTC TimeStamp
IPL           Success             2026/03/04.14:01:13  2026/03/04.14:14:53
CUSTOM        Open                2026/03/04.14:14:53  ...................

System     System                          Load   Load      Flags
Name       Type    SA  CPC.LPAR            Addr   Parms     DAL..  IPL Status
CVP1       ZOS      Y  PS01.PS0138         0EA80  EA8798.1  .YY..  Success
CVP2       ZOS      Y  PS01.PS0139         EA80   EA8798.1  .YY..  Success
CF3        CF          PS01.PS0144                          YY...  Success

                                                                     Page 1 of 1
F1=Help  F3=Return  F5=Refresh  F6=Roll  F7=Up  F8=Down
```

Validation in GDPS 4.9 currently provides support for MM2SITE & MM3SITE with physical isolation only

Stand-Alone LCP Manager

LCP Manager capability for clients using CSM for HA/DR

- **Integrated validation:** Support for on-demand, automated Type 1 (Infrastructure) validation of Safeguarded Copy backups within the vault.
- **IPL Safeguarded Copies:** Standalone LCP enables you to easily IPL from specific SGC backup for regular validation or ad-hoc forensic analysis.
- **Productized capability:** Standalone LCP Manager is a fully supported offering from IBM. No need to worry about employees with key knowledge leaving the company and leaving you with scripts that no one knows how they work or how to support them.
- **Ongoing investment:** IBM is heavily investing in this space. By moving to LCP Manager, you will benefit from the ongoing enhancements to grow the value year after year with support for new generations of HW and SW and additional value provided at no additional cost beyond the annual S&S.

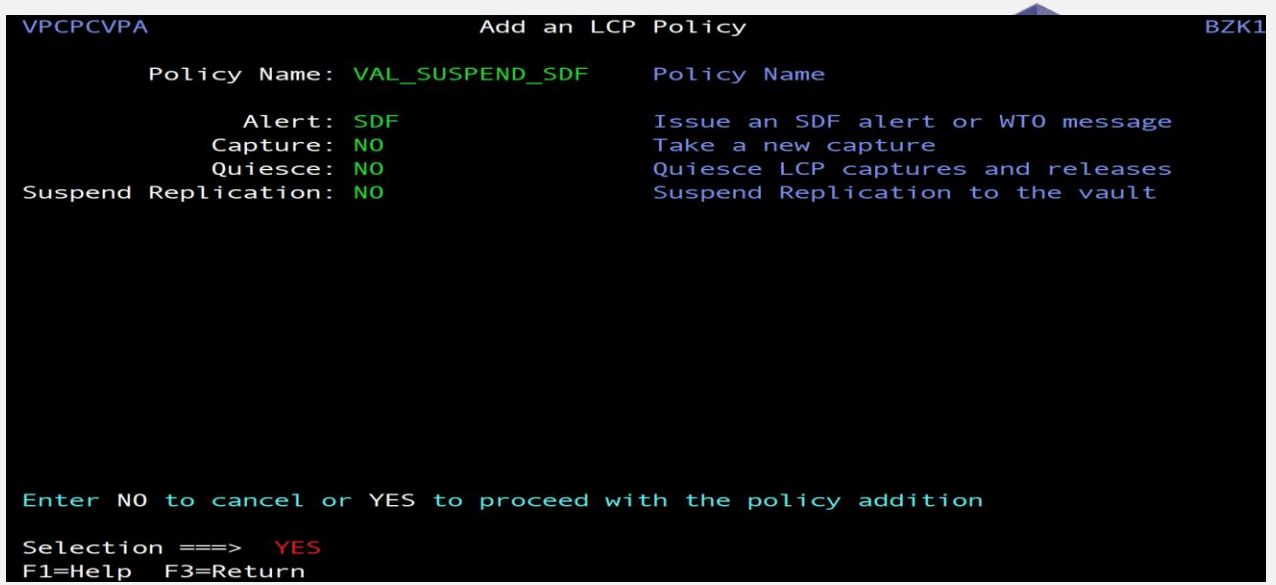


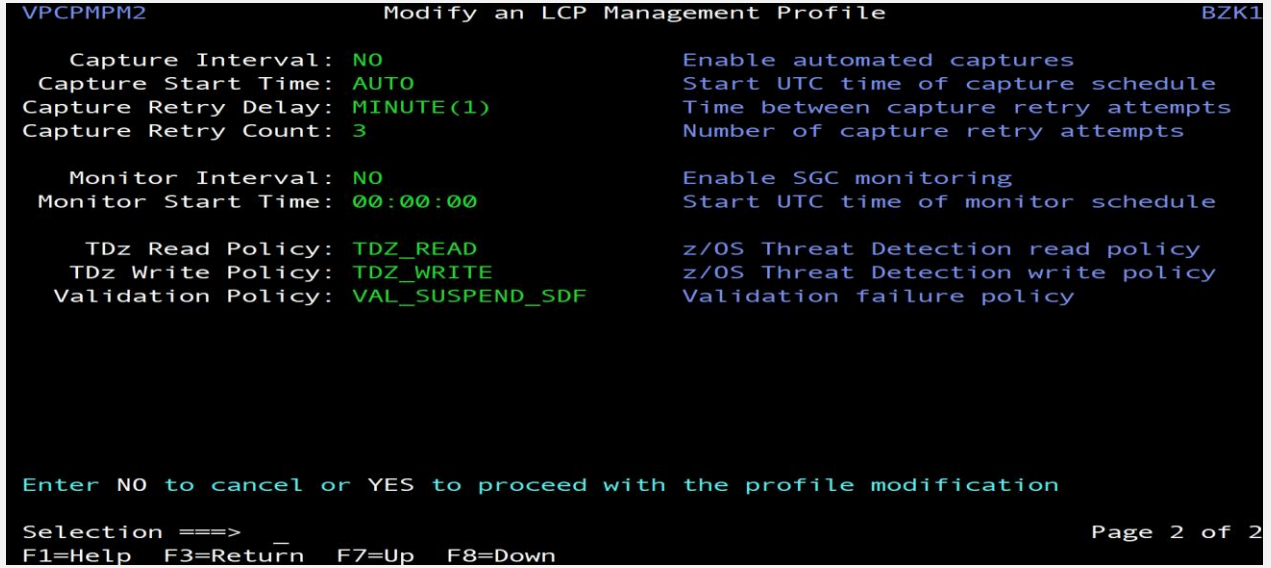
NOTE: Currently supports Metro Mirror 2-site and Multi-Target Metro Mirror 3-site topologies

Integration with Threat Detection for z/OS

Upon receiving a TDz alert, the LCP Manager consults configured LCP policies — defined per management profile per event type (READ or WRITE) — to determine which automated actions to take. Supported actions include:

- Issuing alerts (WTO / SDF).
- Taking a new SGC capture to preserve a forensic state.
- Quiescing LCP operations to stop further changes.
- Suspending replication into the vault to prevent out-of-space events and internal roll-offs.





Stand-Alone LCP Manager and pure z/OS Proxy environments are not supported in this initial release

Additional LCP Enhancements

Support for 1,024 captures with IBM DS8000 G10

LCP now supports up to 1,024 Safeguarded Copy backups on IBM DS8000 G10 hardware, aligning with new IBM DS8000 platform capabilities and enabling deeper retention windows for IBM Z Cyber Vault customers.

LCP Manager RAS Enhancements

Improved Reliability, Availability, and Serviceability (RAS) includes:

SDF message stream simplification (phase STARTED messages suppressed upon matching END SUCCESSFULLY).

More informative LCP messages including phase duration, appended sequence numbers, and improved diagnostics for partial captures and validation errors.

LCP Scheduler Automatic Retry

Automatic retry logic extends the LCP Scheduler's ability to recover from transient conditions by retrying captures within configured delay windows. This improves operational stability in high-activity environments.

Data Consistency Timestamp saved with every SGC capture

Each Safeguarded Copy capture now stores a precise data consistency timestamp, recorded at check-in. Panels allow users to toggle between traditional sequence-based timestamps and true data timestamps. This is critical for surgical recovery workflows, for example with IBM Z Backup Resiliency.

IPL Information saved with each SGC capture

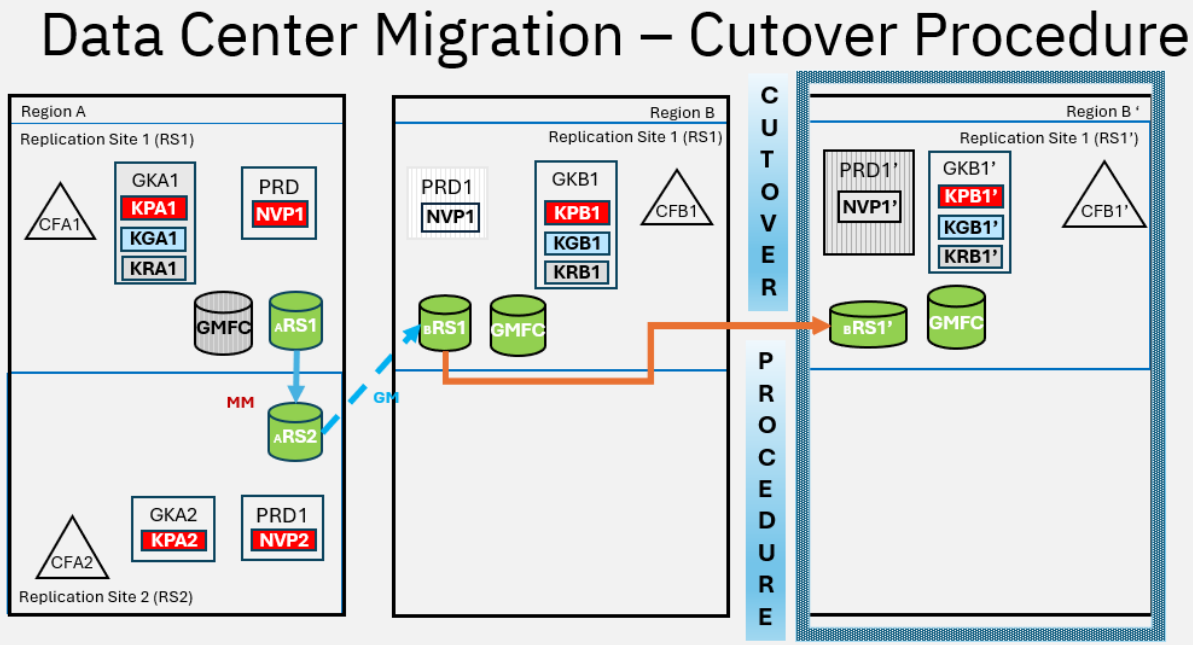
For every capture, LCP now records the currently selected LCP IPL information for potential later use. This however is only done for those systems that are defined for automated validation in the GEOGROUP. This improves repeatability and accuracy of validation and forensic recovery.

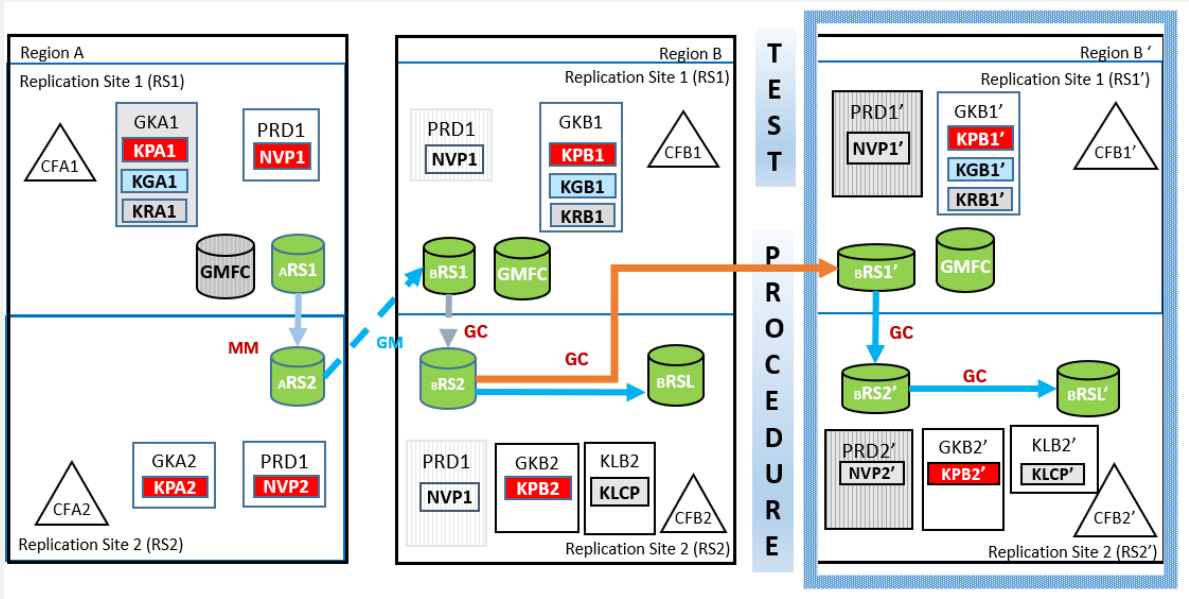
Data Migration Procedures

Steven

Data Migration Procedures

- Increased footprint of data migration processes in the documentation. These processes are:
  - Standardized
  - Supported
  - Tested
  - Documented in the MGM Manuals
- MGM4SITE Data Center Migration currently available
- MGM3SITE Data Center Migration available for 4.9 GA
- Documented CEC migration processes available post 4.9 GA
- Documented, supported DASD Migration processes available post 4.9 GA





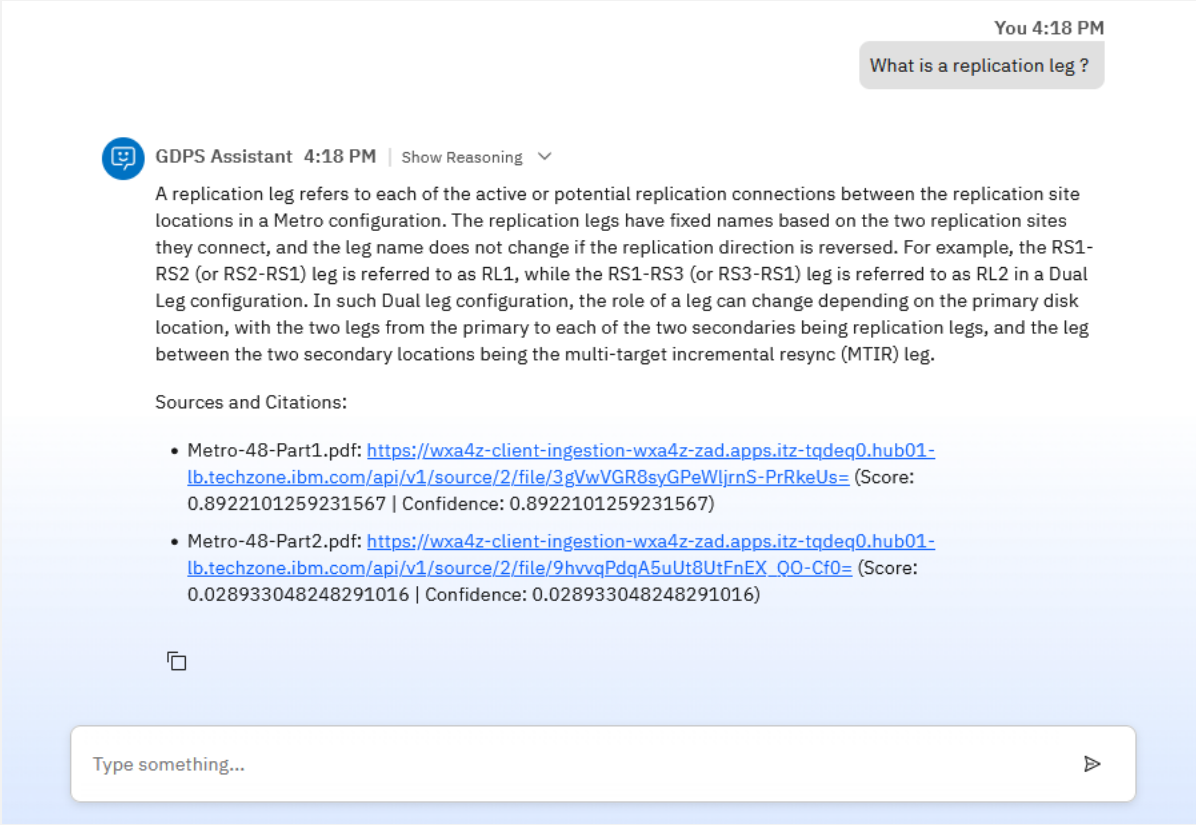
Tech previews

Steven

GDPS Knowledge Agent – tech preview

The AI-enabled GDPS Knowledge Agent is built upon, and requires a licensed version of IBM watsonx Assistant for Z to enable the following capabilities:

- Domain-specific knowledge integration: Integrates GDPS documentation, automation assets, and resiliency patterns into a retrieval-augmented generation (RAG) pipeline to ensure accurate and relevant responses.
- Context-aware conversational handling: Preserves session context across multi-turn interactions, enabling support for complex use cases such as disaster recovery orchestration and policy customization.
- Secure and scalable deployment: Leverages the enterprise-grade security of IBM watsonx Assistant for Z, including role-based access control and seamless integration with IBM Z environments.
- Applicable to GDPS Metro, Global, Metro Global & CA



Statement of Direction

Steven

GDPS Statement of Direction - Complete

- GDPS will introduce Dual Control for GDPS LCP Manager to provide a maker/checker function for pervasive changes, on top of the role elevation capability that is possible with the existing role-based security controls.
- GDPS will be enhanced to support clients who have the requirement for MM3SITE in both regions as opposed to MM2SITE (MGM6SITE)
- GDPS will provide an automation framework as part of the LCP Manager for regular Data Validation in the IBM Z Cyber Vault.
- GDPS plans to extend the Logical Corruption Protection (LCP) Manager capabilities to integrate with GDPS HM and CSM – to deliver a Cyber Vault automation platform for clients using GDPS HM and CSM for replication management.
- IBM intends to extend GDPS LCP Manager to consume event notification from the anti-malware solution for z/OS described in associated z/OS Statement of direction: IBM intends to deliver anti-malware for IBM z/OS and enable policy-driven actions to be taken based on the event.

Green text: Delivered in GDPS 4.7
Blue text: Delivered in GDPS 4.8
Purple text: Delivered in GDPS 4.9

GDPS 4.9 Statement of Direction

- IBM intends to extend the integration between GDPS LCP Manager and the IBM Z Backup Resiliency product (5698-BR1) to provide real-time notification of Safeguarded Copy lifecycle events to IZBR, including internal rolloff events. These Safeguarded Copy rolloffs will be reported as they occur using the same reporting mechanisms as existing Monitor3 and TDz events within GDPS. With real-time event notifications from LCP Manager, IZBR can further improve the efficiency and accuracy of forensic analysis and recovery operations that leverage Safeguarded Copy backups.
- IBM intends to create a new supported GDPS topology, Metro Mirror 4-site (MM4SITE). This enhancement is intended to extend existing three-site Metro configurations by providing 4 site symmetric resiliency. This will provide additional site separation and placement flexibility, enabling more resilient and versatile high-availability and disaster-recovery designs. The MM4SITE topology is designed to help clients address more complex failure scenarios and operational requirements while continuing to leverage GDPS Metro automation for coordinated storage and system management.
- IBM intends to enhance LCP Manager to provide support for additional GDPS topologies with IBM Db2 Expert Recovery Pro ‘Db2 Roll Forward’ capability.
- IBM intends to enhance Stand-Alone LCP Manager to provide support for Global Mirror 2-site topologies.
- IBM intends to deliver a new GDPS priced feature, the GDPS Common Consistency Group. This will enable a single GDPS control environment to manage a common consistency group for z/OS CKD devices and OPEN Fixed Block Devices.
- IBM intends to extend IBM Threat Detection for z/OS integration within GDPS LCP Manager to support notifications generated by the IBM DS8000 FCM4 threat detection capability.

Additional information

Steven

Additional Information

Websites:

- GDPS https://www.ibm.com/products/gdps
- IBM Z https://www.ibm.com/z
- IBM Z Resiliency https://www.ibm.com/z/resiliency
- Storage https://www.ibm.com/storage
- Redbook – GDPS Family: An Introduction to Concepts and Capabilities
  http://www.redbooks.ibm.com/abstracts/sg246374.html?Open

GDPS Website resources

- GDPS: The Enterprise Continuous Availability / Disaster Recovery Solution white paper
- GDPS Pre-requisite Information
- GDPS Training Schedule Links
- GDPS Hardware Qualification Letters
- E-mail: gdps@us.ibm.com


Thank you!