What’s new/changed in GDPS® V4.8?

On March 31, 2025, IBM® has made available Version 4 Release 8 of GDPS Metro, GDPS Metro HyperSwap® Manager, GDPS Global – GM, GDPS Metro Global – GM, and GDPS Continuous Availability.

This document describes at a high level:

- New function and changes in GDPS V4.8 solutions, including new function added in GDPS V4.7 via continuous delivery.
- Preview of items planned to be released via continuous delivery in the coming months.
- Any formal GDPS Statements of Direction beyond the preview of planned new function already mentioned.
- End of support information for GDPS releases.

General recommendation

The minimum level of z/OS® required to run GDPS 4.8 will be z/OS® 2.5.

A reminder that in GDPS 4.7, as part of the IBM ‘Words Matter’ initiative to remove wording that could be considered as offensive, derogatory, or demeaning, the word ‘master’ has been replaced with the word ‘primary’ within GDPS. Commonly use terms such as ‘master controlling system’ will now be referred to as ‘primary controlling system’. This change will apply to both GDPS code and GDPS documentation. Please be aware that this change will impact some GDPS messages and hence could affect any locally written automation.

What's new or changed in GDPS Metro

The following new capabilities or procedures have been included in the GDPS Metro V4.8 solution or via continuous delivery through the service stream since GDPS Metro V4.7 was made available:

- GDPS role-based security has been extended as follows:
  - Introduction of an extension of the GDPSCTL security profiles to protect GDPS Scripts.
- Enhancements have been made to the GDPS Security Definition Utility (GEOSEC) to support the new role-based security profiles listed above to enable the definition of these profiles via this utility.
- The default role-based security setting SECURITY= GDPS OPTION has been changed from NOSAF to SAF.
- A new Standard Actions panel has been added to provide an LPAR (physical) view.
  - This new panel will show LPAR Name / LPAR Status / System Type / System Name as well as the GDPS System / GDPS Status / GDPS Type.
  - This will provide visibility of which GDPS systems currently running on a specific CEC and should reduce the chance of an operator accidently taking action on the wrong system.
- New reports for testing or loading a new DASD configuration or site table refresh.
  - The report provides information for current configuration plus the new configuration and highlights any differences between the two configurations. Items covered as follows:
    - Disk subsystems (DISKSUBSYSTEM statement in GEOPARM).
    - CKD LSS pairs and devices (LSS & MIRROR statements in GEOPARM).
    - PPRC path (Path and LINK statements in GEOPARM).
  - These new reports provide an easy way to validate that the changes that are about to made are in line with expectations.
  - This report will also provide the ability to understand what changed and when the last change to the DASD configuration was made.
- New enhancement to provide the identification of active Concurrent Copy (CC) session(s) during a planned HyperSwap.
  - If a HyperSwap fails, previously the failure message simply stated, "Active CC sessions found". Now the system that sets the lock is identified for faster remediation.
- Added support for GDPSIOST for post-HyperSwap host access cleanup and managing Utility device dynamic path grouping
- New parameters SYNCTGT and LINKMINI are added to GDPSMNT

- A new LCP Manager scheduler has been introduced enabling various tasks to be managed directly by GDPS rather than having to use an external scheduler.
  - A new capture scheduler has been introduced to enable LCP to schedule Safeguarded copy captures. GDPS can auto allocate schedule times based on frequency and number of profiles defined or schedules can be set manually.
  - A new monitor scheduler has been introduced which enables monitors to be set at minute rather than hour granularity. The ability to set a specific start time is now supported rather than the monitor being initiated immediately.
- LCP Manager has introduced quiesce and resume capability.
  - The quiesce capability will suspend capturing / releasing and can optionally stop mirroring into the vault.
  - The resume capability will restart capturing / releasing at the next scheduled time.
  - This capability includes support for role-based security and dual control.
- Enhancements to recovery of open capture in LCP Manager.
  - Performing a recover of an open capture will no longer take an additional ‘invalid’ capture.
- Consistency of filtering across all GDPS products.
  - Enhanced filtering capability on some specific panels.

What's new or changed in GDPS Metro HM

The following new capabilities or procedures have been included in the GDPS Metro V4.8 HyperSwap Manager solution or via continuous delivery through the service stream since GDPS Metro HM V4.7 was made available:

- The default role-based security setting SECURITY= GDPS OPTION has been changed from NOSAF to SAF.
- New reports for testing or loading a new DASD configuration or site table refresh.
  - The report provides information for current configuration plus the new configuration and highlights any differences between the two configurations. Items covered as follows:
    - Disk subsystems (DISKSUBSYSTEM statement in GEOPARM).
    - CKD LSS pairs and devices (LSS & MIRROR statements in GEOPARM).
    - PPRC path (Path and LINK statements in GEOPARM).
  - These new reports provide an easy way to validate that the changes that are about to made are in line with expectations.
  - This report will also provide the ability to understand what changed and when the last change to the DASD configuration was made.
- New enhancement to provide the identification of active Concurrent Copy (CC) session(s) during a planned HyperSwap.
  - If a HyperSwap fails, previously the failure message simply stated, "Active CC sessions found". Now the system that sets the lock is identified for faster remediation.
- Added support for GDPSIOST for post-HyperSwap host access cleanup and managing Utility device dynamic path grouping
- Consistency of filtering across all GDPS products.
  - Enhanced filtering capability on some specific panels.

What’s new or changed in GDPS Global - GM

The following new capabilities or procedures have been included in the GDPS Global – GM V4.8 solution or via continuous delivery through the service stream since GDPS GM V4.7 was made available:

- GDPS role-based security has been extended as follows:
  - Introduction of an extension of the GDPSCTL security profiles to protect GDPS Scripts.
- Enhancements have been made to the GDPS Security Definition Utility (GEOSEC) to support the new role-based security profiles listed above to enable the definition of these profiles via this utility.
- The default role-based security setting SECURITY= GDPS OPTION has been changed from NOSAF to SAF.
- Support has been added for topology setting GM 2-site to have GM secondary disks defined in subchannel sets 1, 2 or 3 in addition to the previously supported subchannel set 0.
- New report for testing or loading a site table refresh.
  - The report contains the output of the site table load or test most recently performed. This includes:
    - Site table syntax validation processing.
    - Site table refresh execution or test results.
    - Site table refresh completion on all participating systems.
  - This new report provides an easy way to validate that the changes that are about to made are in line with expectations.
  - This report will also provide the ability to understand what changed and when the last change to the site table was made via Site Table refresh.

What’s new or changed in GDPS Metro Global - GM

In addition to the new functions provided in the individual products that constitute the GDPS Metro Global – GM (MGM) offering, the following new capabilities or procedures have been included in the GDPS MGM V4.8 solution or via continuous delivery through the service stream since GDPS MGM V4.7 was made available:

- A new GDPS topology has been introduced, GDPS Metro Global Mirror 6-site (MGM 6-site).
  - Building out from the existing MGM 3-site and MGM 4-site topologies, GDPS now supports enhanced resiliency by enabling 3 copies of data to be managed synchronously in the active region with MGM 6-site topology.
  - This new topology addresses the Statement of Direction (SOD) item that was first listed in the GDPS 4.6 SOD.
- A new priced feature has been introduced, GDPS Solutions Manager (GSM).
  - This feature enables simplified systems management for clients with multiple sysplexes managed by GDPS.
  - It can consolidate up to 3 GDPS controlling system pairs into a single sysplex (2 LPARs) to reduce complexity and lower system management overhead.
  - Initial support for MGM 4-site and MGM 6-site topologies.
- The region awareness support and the REGION script statement usage have now been extended to all MGM 4-site environments, including the new support for MGM 4-site without LCP and MGM 4-site with external LCP.
- New report for testing or loading a site table refresh.
  - The report contains the output of the site table load or test most recently performed.
    This includes:
    - Site table syntax validation processing.
    - Site table refresh execution or test results.
    - Site table refresh completion on all participating systems.
  - This new report provides an easy way to validate that the changes that are about to made are in line with expectations.
  - This report will also provide the ability to understand what changed and when the last change to the site table was made via Site Table refresh.

What’s new or changed in GDPS Continuous Availability

The following new capabilities or procedures have been included in the GDPS Continuous Availability V4.8 solution and enhancements delivered via continuous delivery through the service stream for GDPS CA V4.7:

- GDPS role-based security has been extended as follows:
  - Introduction of an extension of the GDPSCTL security profiles to protect GDPS Scripts.
- Enhancements have been made to the GDPS Security Definition Utility (GEOSEC) to support the new role-based security profiles listed above to enable the definition of these profiles via this utility.
- The default role-based security setting SECURITY= GDPS OPTION has been changed from NOSAF to SAF.
- Enhanced Workload degradation detailed messages (GEO1149E)
  - In the event of workload degradation, new GDPS messages and SDF alerts are now created with information that is relevant to the cause of the workload degradation. Previously this information was only available in System Automation and a high level of SA knowledge was required to interpret the information.

Functions to be removed in the next release of GDPS

No items are planned to be removed in the next release of GDPS.

GDPS Continuous Delivery Preview

The following functions are currently planned to be released in the coming months through the GDPS 4.8 service stream:

- Provide GDPS LCP Manager integration into a GSM environment. The initial support will be for MGM 4-site and MGM 6-site topologies only.

GDPS Statements of direction

For your planning purposes, the previous section, "GDPS Continuous Delivery Preview", includes several specific enhancements that are expected to be released within the coming months.

In addition, the following statements of direction are being made or remain in place at this time:

- IBM intends to develop an extension to the GDPS Logical Corruption Protection (LCP) Manager that does not require GDPS Metro or GDPS GM to be managing the HA/DR remote copy for a client but can interface with the IBM Copy Services Manager (CSM) for those replication management functions otherwise provided by GDPS Metro or GDPS Global – GM.

  The purpose of this new capability is to provide the automation platform for CSM clients with IBM DS8000® storage to adopt the IBM Z® Cyber Vault solution with GDPS LCP Manager providing the ability to drive the recovery, data validation and restoration of Safeguarded Copy backups taken within the environment.

  This support will initially be focused on clients using CSM to manage Metro Mirror 2-site configurations with physical or virtual isolation of the IBM Z Cyber Vault, and CSM clients using GM 2-site with physical isolation or Safeguarded Copy backups taken on the GM primary devices. This new capability of the GDPS LCP Manager will need to run as a standalone GDPS Controlling System in a z/OS image that is also running IBM Z NetView® and IBM Z System Automation as normal for GDPS.

- IBM intends to extend the automation framework provided by GDPS LCP Manager for the IBM Z Cyber Vault solution to provide automation of data validation as follows:

  1. Infrastructure Validation (Type 1), to validate the system can IPL from a consistent, point-in-time copy (taken via FlashCopy® or Safeguarded Copy) of Production.
  2. Subsystem Validation (Type 2), to validate the system can start all required subsystems from the copy such as CICS®, IMS™, Db2® etc.
  3. Initiation of Application Validation (Type 3), client created scripts to validate specific Application Data in the copy.
  4. Extend the automation framework to provide validation for Linux® guests running under z/VM®

- IBM intends to extend GDPS LCP Manager to consume event notification from the IBM Threat Detection for z/OS product (5698-CA1).This will enable automated, policy-driven actions to be taken based on identified anomalies.

- IBM intends to extend the integration between GDPS LCP Manager and the IBM Z Backup Resiliency product (5698-BR1) specifically in surgical recovery of data sets in an IBM Z Cyber Vault context to automate the process of extracting specific versions of datasets from a Safeguarded Copy backup to make them available for restoration into production.

- IBM intends to enhance the IBM Z Cyber Vault solution with 'Application Roll Forward' capability. The initial capability will be for Db2 with support for other subsystems such as IMS to follow later. This new capability will enable clients to leverage secured Db2 archive logs to roll forward from their last good Safeguarded copy closer to the point in time of data of corruption to reduce their RPO.

End of support

In accordance with the GDPS “n, n-2” support policy, support for GDPS V4.6 will be discontinued on March 31, 2026 and that support will be discontinued for GDPS V4.7 on March 31, 2027.

GDPS does offer a limited extended support option for clients who need to run an older version or release of GDPS for some specific reason. There are restricted terms and conditions for this limited extended support which can be made available on request to GDPS@US.IBM.COM. The limited extended support is available for a further 4 years after a release reaches the end of normal support. Any issues raised with a release older than 7 years will be handled on a best efforts basis so long as a valid extended support contract remains in place.

Support for System Automation for Multi-Platforms (SA MP) 4.1.0.7 will be discontinued on March 31st, 2025. Therefore, support for SUSE12 and RHEL7 in GDPS V4.5 will not be available beyond March 31st, 2025, even where an extended support contract is in place for GDPS.

(C)Copyright IBM Corporation 2025
IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.
03/25

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

All client examples cited or described are presented as illustrations of the manner in which some clients have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions. Contact IBM to see what we can do for you.

It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective.

IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.