IBM GDPS Active/Active Overview and Planning

GDPS Active/Active architectural overview

Hints and tips for GDPS Active/Active deployment

Planning for GDPS Active/Active

Lydia Parziale
Juliet Candee
Jiong Fan
Paulo Shimizu
Sidney Varoni Jr
Shu Xie

Redbooks

ibm.com/redbooks

International Technical Support Organization

IBM GDPS Active/Active Overview and Planning

March 2015

SG24-8241-00

Note: Before using this information and the product it supports, read the information in "Notices" on page vii.

First Edition (March 2015)

This edition applies to Version 1, Release 4, of GDPS Active/Active.

Contents

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX®
CICS®
DB2®
DRDA®
GDPS®
Geographically Dispersed Parallel Sysplex™
Global Technology Services®
HyperSwap®
IBM®
IMS™
InfoSphere®
MVS™
NetView®
OMEGAMON®
Parallel Sysplex®
Redbooks®
Redbooks (logo) ®
System Storage®
System z9®
System z®
Tivoli®
WebSphere®
z/OS®
z/VM®
z9®
zEnterprise®

The following terms are trademarks of other companies:

Evolution, and Kenexa device are trademarks or registered trademarks of Kenexa, an IBM Company.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

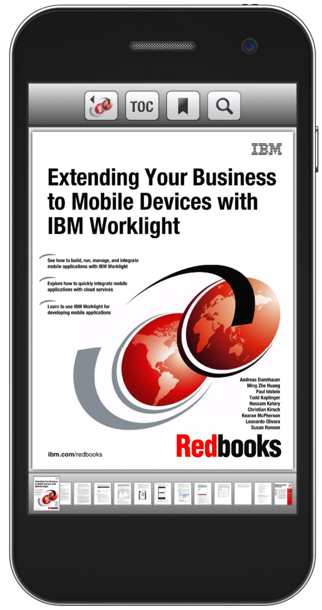
Other company, product, or service names may be trademarks or service marks of others.

Find and read thousands of IBM Redbooks publications

- Search, bookmark, save and organize favorites
- Get up-to-the-minute Redbooks news and announcements
- Link to the latest Redbooks blogs and videos

Get the latest version of the Redbooks Mobile App

iOS **Download Now** Android



Promote your business in an IBM Redbooks publication

Place a Sponsorship Promotion in an IBM® Redbooks® publication, featuring your business or solution with a link to your web site.

Qualified IBM Business Partners may place a full page promotion in the most popular Redbooks publications. Imagine the power of being seen by users who download millions of Redbooks publications each year!

ibm.com/Redbooks
About Redbooks → Business Partner Programs

THIS PAGE INTENTIONALLY LEFT BLANK

Preface

IBM® Geographically Dispersed Parallel Sysplex™ (GDPS®) is a collection of several offerings, each addressing a different set of IT resiliency goals. It can be tailored to meet the recovery point objective (RPO), which is how much data can you are willing to lose or recreate, and the recovery time objective (RTO), which identifies how long can you afford to be without your systems for your business from the initial outage to having your critical business processes available to users.

Each offering uses a combination of server and storage hardware or software-based replication, and automation and clustering software technologies.

This IBM Redbooks® publication presents an overview of the IBM GDPS active/active (GDPS/AA) offering and the role it plays in delivering a business IT resilience solution.

This book covers the following products:

- GDPS Active/Active V1.4
- IBM Tivoli® System Automation for z/OS® V3.3 (+SPE APAR) or V3.4
- IBM Tivoli NetView® for z/OS V6.2
- IBM Tivoli NetView Monitoring for GDPS V6.2
- IBM Multi-site Workload Lifeline for z/OS V2.0
- IBM InfoSphere® Data Replication for DB2® for z/OS V10.2.1
- IBM InfoSphere Data Replication for IMS™ for z/OS V11.1
- IBM InfoSphere Data Replication for VSAM for z/OS V11.1
- IBM Tivoli Monitoring V6.3
- z/OS V1.13
- IBM WebSphere® MQ V7.0.1 (required for DB2 data replication)
- IBM CICS® Transaction Server for z/OS V5.1 (required for VSAM data replication)
- CICS VSAM Recovery for z/OS V5.1 (required for VSAM data replication)
- DB2 for z/OS V9 or higher (workload dependent)
- IMS V11 (workload dependent)

Authors

This book was produced by a team of specialists from around the world working at the International Technical Support Organization, Poughkeepsie Center.

Lydia Parziale is a Project Leader for the ITSO team in Poughkeepsie, New York, with international experience in technology management that includes software development, project leadership, and strategic planning. Her areas of expertise include business development and database management technologies. Lydia is a certified PMP and an Open Group Certified IT Specialist with an MBA in Technology Management and has been employed by IBM for over 25 years in various technology areas.

Juliet Candee is a Senior Technical Staff Member with the IBM Systems and Technology Group in IBM Poughkeepsie. She has 25 years of experience in IBM System z® development and design, and the System z brand. Her areas of expertise include System z transaction processing, platform infrastructure, System z business continuity technical strategy, and design. She is currently working as an international assignee in IBM China’s High End Center of Competence, focusing on the architecture and design of GDPS Active-Active solutions for high-end banking clients.

Jiong Fan is an Executive IT Specialist from the IBM Global Technology Services® organization in IBM China. He has more than 15 years of experience in China large banking account support. He has worked at IBM for 18 years. His areas of expertise include Sysplex, DB2, Performance Management, Data Center Consolidation, and Management.

Paulo Shimizu is a Senior Systems Programmer at Bradesco bank in Brazil. He has 24 years of experience in Mainframe and z/OS field. He holds a degree in Systems Analysis from Universidade Paulista and specialization in IT Managerial from FIEO University. His areas of expertise include z/OS, Sysplex, Systems Automation, and GDPS.

Sidney Varoni Jr is an IT Specialist from Global Technology Services organization in IBM Brazil. He has eight years of experience working in complex z/OS environments, having worked in Operations and z/OS Support areas at the IBM Global Delivery Center in Hortolandia. He currently works at the IBM System z services delivery organization in Sao Paulo. He holds a bachelor degree in Computer Science from Faculdade Politecnica de Jundiai. His areas of expertise include z/OS, Sysplex, and GDPS.

Shu Xie is an IT Specialist with Systems and Technology Group of IBM China. She has 5 years of experience in z/OS and System z business continuity technical field. She holds a master's degree in System-on-Chip Design from the Royal Institute of Technology. Her areas of expertise include z/OS, Sysplex, and GDPS.

Thanks to the following people for their contributions to this project:

Serge Bourbonnais
STSM and Lead Architect for InfoSphere Replication Server development, IBM Silicon Valley Lab, San Jose, CA

Joseph Welsh II
IBM Lab Service System z, US

Paul Cadarette
STSM and Lead Architect for InfoSphere Classic Products, IBM US

Pierre Cassier
GDPS and z/OS Performance IT Specialist, Montpeller, IBM France

Michael G. Fitzpatrick
Performance Design, z/OS Communications Server, System z software designer, Durham, NC US

Miao Zheng
Client Technical Advisor for ICBC (Industrial and Commercial Bank of China), IBM China

Thanks to the authors of the following IBM Redbooks publications:

- *GDPS Family: An Introduction to Concepts and Capabilities*, SG24-6374:
  - David Clitherow
  - Sim Schindel
- *Understanding and Using Q Replication for High Availability Solutions on the IBM z/OS Platform*, SG24-8154
  - Chuck Ballard
  - Jason Arnold
  - Rich Briddell
  - Heverson Campelo
  - Cecile Madsen

– Jayanti Mahapatra
– Eduardo Pingarilho

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an email to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

1

Introduction

This chapter describes the concepts and business value of the GDPS Active/Active solution. It includes the following sections:

- GDPS Active/Active solution concepts
- Benefits of using GDPS Active/Active

1.1 GDPS Active/Active solution concepts

This section provides a high-level description of the GDPS Active/Active solution.

1.1.1 Evolution of GDPS Active/Active solution

As government regulations become more stringent on enterprise financial systems, business continuous availability and disaster recovery requirements, IT faces increasing challenges to reduce both planned and unplanned outages. As these enterprise financial institutes accelerate their strategy to transform into global companies, the higher the demand for providing highly available, efficient business services also grow tremendously. Therefore, the requirement for higher level of availability, security, and non-disruption of their information systems and core business services evolves from an all-or-nothing approach to a solution that can provide application granularity.

There are many GDPS products for managing mainframe high availability and disaster recovery other than GDPS Active/Active solution. These offerings are based on synchronous and asynchronous disk hardware replication techniques. They are described in *GDPS Family: An Introduction to Concepts and Capabilities*, SG24-6374.

To achieve the highest levels of availability and minimize the recovery time for planned and unplanned outages, some clients have deployed GDPS/PPRC Active/Active configurations, also known as GDPS/PPRC multi-site workload configuration, which are based on synchronous disk replication. This configuration requires the following characteristics:

- All critical data must be PPRCed and IBM HyperSwap® enabled
- All critical CF structures must be duplexed
- Applications must be sysplex enabled and use cross-site data sharing

This solution can provide an RPO of zero and an RTO of a few minutes. However, signal latency between sites can potentially affect online workload response time, and throughput, and batch duration. As a result of this, sites typically are separated by less than 20 km fiber distance. Therefore, GDPS/PPRC Active/Active does not present a solution for enterprise clients with a site distance greater than 20 km.

The GDPS products based on asynchronous disk replication, GDPS/XRC and GDPS/GM, provide for unlimited site separation. However, they require restarting the workload from the failed site in the recovery site, and this typically takes 30 - 60 minutes. Thus, these products are not able to achieve the RTO of seconds goal that is required by some enterprise clients.

The GDPS products based on disk replication have limitations in achieving the aggressive RTO and RPO goals while supporting sufficient site separation. IBM needs to provide a solution that can provide for mission critical workloads with stringent recovery objectives that cannot be achieved using existing GDPS solutions.

For these reasons, the GDPS Active/Active solution was designed to significantly reduce the planned outrages for maintenance and upgrades, and provide business continuous availability during an unplanned workload or site failure. This does not mean that the solution is designed to substitute for the existing availability solutions, such as Parallel Sysplex or existing products in the GDPS family. Instead, these solutions can be used to complement the GDPS Active/Active solution to ensure an even higher level of reliability and availability in customer's IT and business environment.

Table 1-1 summarizes the positioning of major categories of GDPS solutions.

Table 1-1 From High Availability to Continuous Availability

GDPS/PPRC	GDPS/XRC or GDPS/GM	GDPS Active/Active
Failover model	Failover model	Near CA model
Recovery time ~ 2 min	Recovery time < 1 hour	Recovery time < 1 min
Distance < 20 km	Unlimited distance	Unlimited distance

1.1.2 GDPS Active/Active solution concepts

The GDPS Active/Active solution manages two or potentially more sites that are separated by unlimited distances, running the same application and having the same data to provide cross-site workload balancing, continuous availability, and disaster recovery. This is a paradigm shift from a failover model to a continuous availability model.

Figure 1-1 describes an overview of the concepts of the GDPS Active/Active solution.

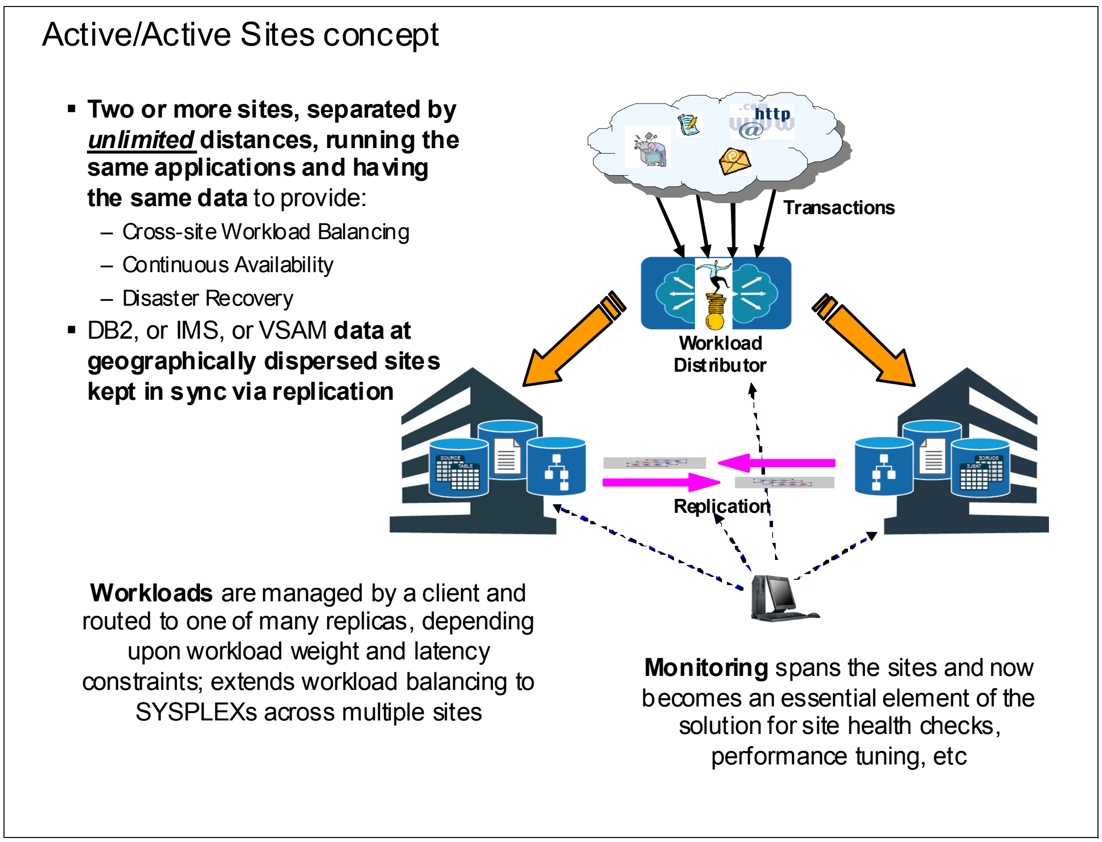


Figure 1-1 GDPS Active/Active Sites Concept

Active/Active Sites

The GDPS Active/Active solution currently supports a two-site environment. A site is equivalent to a production sysplex (which can span more than one physical site) where one or more Active/Active workloads are running and managed by GDPS.

There are redundant workload instances for each workload. Each workload instance can run in each of the Active/Active sites. At any time, for each Update Active/Active update workload, one site is actively processing transactions and the other site is on standby. The standby site has all of the infrastructure components (LPARs, systems, middleware, and so on) and applications so that it is ready to receive work. Active/Active query workloads can be distributed between sites based on customer policy and current replication latency.

Active/Active workload

In the GDPS Active/Active solution, a workload is an aggregation of the following items:

- Software

  User-written applications such as COBOL programs, and the middleware runtime environment (CICS regions, InfoSphere Replication Server instances, DB2 or IMS subsystems, and so on)

- Data

  A related set of objects that must preserve transactional consistency and optionally referential integrity constraints (for example, DB2 Tables, IMS databases, and VSAM files)

- Network connectivity

  One or more TCP/IP addresses and ports (for example, 10.10.10.1:80)

Each workload has a separate configuration. The GDPS Active/Active solution supports the following configurations:

- Active/standby configuration

  An active/standby configuration consists of an active workload instance running in a sysplex at one site, and a standby workload instance at another site.

- Active/query configuration

  An active/query configuration consists of an active workload instance running in a sysplex at one site, and a standby workload instance at another site, and an associated query workload instance running in each sysplex at each site.

Two types of workloads are supported in a GDPS Active/Active environment:

- Update or read/write workloads

  These workloads run in an active/standby configuration. At any point in time, an update workload is only active at one site and receiving transactions routed to it. The updated data from the active instance of the workload is copied to the database instance that runs at the standby site. When a planned or unplanned outage of an active workload instance occurs, transactions are directed to the workload instance running at the standby site.

- Query or read-only workloads

  These workloads run in an active/query configuration. A query workload is associated with an update workload, and operates against the data objects that are updated by the active instance of that update workload. At most two query workloads can be associated with an update workload. A query workload can be actively running at both sites. Workload distribution between sites is based on policy options, and the currency of the data at the standby site.

Data replication

GDPS Active/Active solution relies on software-based asynchronous replication techniques to synchronize DB2, IMS, and VSAM data between sites. The replication technology consists of capture engines, apply engines, and a transport infrastructure. Capture engines monitor the source database for committed transaction data. These data are captured and placed in a transport infrastructure for transmission to a target location, where the apply engines apply the data in real time to an active copy of the database.

The GDPS Active/Active solution supports the following software replication products:

- IBM InfoSphere Data Replication (IIDR) for DB2 for z/OS
- IBM InfoSphere Data Replication (IIDR) for IMS for z/OS
- IBM InfoSphere Data Replication (IIDR) for VSAM for z/OS

Workload distribution and workload balancing

Workload distribution and workload balancing in a GDPS Active/Active environment is achieved by the IBM Multi-site Workload Lifeline for z/OS (refer to as Lifeline) product and the external load balancers.

Lifeline provides routing recommendations to the external load balancers through the open-standard Server/Application State Protocol (SASP) API, which is documented in RFC4678 and can be found at:

https://tools.ietf.org/html/rfc4678

Lifeline can provide distribution recommendations to multiple tiers of load balancers. Distribution recommendations are built based on health data that are collected from all LPARs across both sites. There are first-tier and second-tier load balancers. Site recommendations are directed to first-tier load balancers to route new connections for a workload to the selected site. Within the selected site, server application recommendations are directed to second-tier load balancers to route new connections for a workload to specific server applications. Sysplex Distributor can take the role as the second-tier load balancer. In this case, no server application recommendations are provided by Lifeline.

The capability to switch between workload instances extends workload balancing to sysplexes across multiple sites. Additionally, when a planned or unplanned outage occurs, a workload is switched to its alternate workload instance.

Monitoring of the Active/Active environment

Monitoring is an essential component for the GDPS Active/Active solution. NetView Monitoring for GDPS monitors workload and replication status, workload and site health checks, software replication performance, routing decisions, and so on. Monitoring spans the Active/Active sites and alerts on any exceptions detected. This monitoring information is then forwarded to IBM Tivoli Monitoring for display or to trigger specific situations.

For more information, see Chapter 5, “Controlling and monitoring” on page 49.

1.2 Benefits of using GDPS Active/Active

GDPS Active/Active solution provides continuous availability for critical business applications. At the same time, the system resources and near real-time production data available on the alternate site can be used for workload balancing and data analytic workloads exploring large amount of real-time data.

1.2.1 Reduce planned and unplanned outages for critical applications

GDPS Active/Active solution provides continuous availability for critical business applications. It is designed to eliminate planned outages while reducing the effect of unplanned outages.

- Planned outages include application upgrades, database management system, major software and system maintenance, and so on.
- Unplanned outages include application errors, sysplex-wide component failures, site failure, and so on.

There are redundant workload instances and production data in an Active/Active environment. Each workload instance can run on a separate sysplex at a different site, accessing the same data. During a planned upgrade or maintenance window, or when an unplanned outage occurs, GDPS Active/Active can switch a specific, some, or all of the Active/Active workloads to an alternate site to provide business continuity.

1.2.2 Isolation from catastrophic failures

GDPS Active/Active solution supports separate sysplexes run in sites separated by extended distances. Such loosely coupled topologies provide isolation and protection from sysplex-wide failures. When an unplanned site outage occurs, GDPS Active/Active can switch to a workload instance running at an alternate site to recovery and resume business.

1.2.3 Both sites running workloads

Active-Active sties infrastructure allows for dynamic workload distribution and workload balancing between sites to fully use resources in both production sites. The invested resources and near real-time data can also be used to run read-only type workloads. These include data extraction type batch applications to reduce batch window in primary site, or live business reporting and historical details query to route away from core online transactions in primary site.

2

Architectural overview

The design of the GDPS Active/Active solution is a paradigm shift from a failover model to a near continuous availability model. The other GDPS solutions are built upon storage-based replication. Because data on storage is not readily accessible, in general it takes a longer time to recover from an outage. GDPS Active/Active solution is an asynchronous software replication-based solution to provide business continuity with unlimited distance. The solution is designed for mission critical workloads that have stringent recovery objectives that cannot be achieved using existing GDPS products. The objective is to provide near continuous availability at the workload level granularity to enable a flexible implementation by business priorities.

This chapter provides an architectural overview of the GDPS Active/Active solution. This chapter includes the following sections:

- Components of GDPS Active/Active
- GDPS Active/Active product
- Multi-Site Workload Lifeline for z/OS
- Software data replication products
- IBM Tivoli Monitoring and IBM Tivoli NetView for z/OS

2.1 Components of GDPS Active/Active

GDPS Active/Active is for mission critical workloads that have stringent recovery objects, which cannot be achieved by storage replication-based GDPS offerings:

- RTO nearly zero, measured in seconds
- RPO nearly zero, measured in seconds
- Non-disruptive planned switch, in granularity of workload
- Any distance

GDPS Active/Active achieves the highest level of availability and minimal recovery impact for unplanned outage. Unlike other GDPS solutions, which are relaying on hardware replicating data, GDPS Active/Active uses software-based asynchronous replication techniques for copying the data.

Figure 2-1 describes the components and communication flows in a GDPS Active/Active environment.

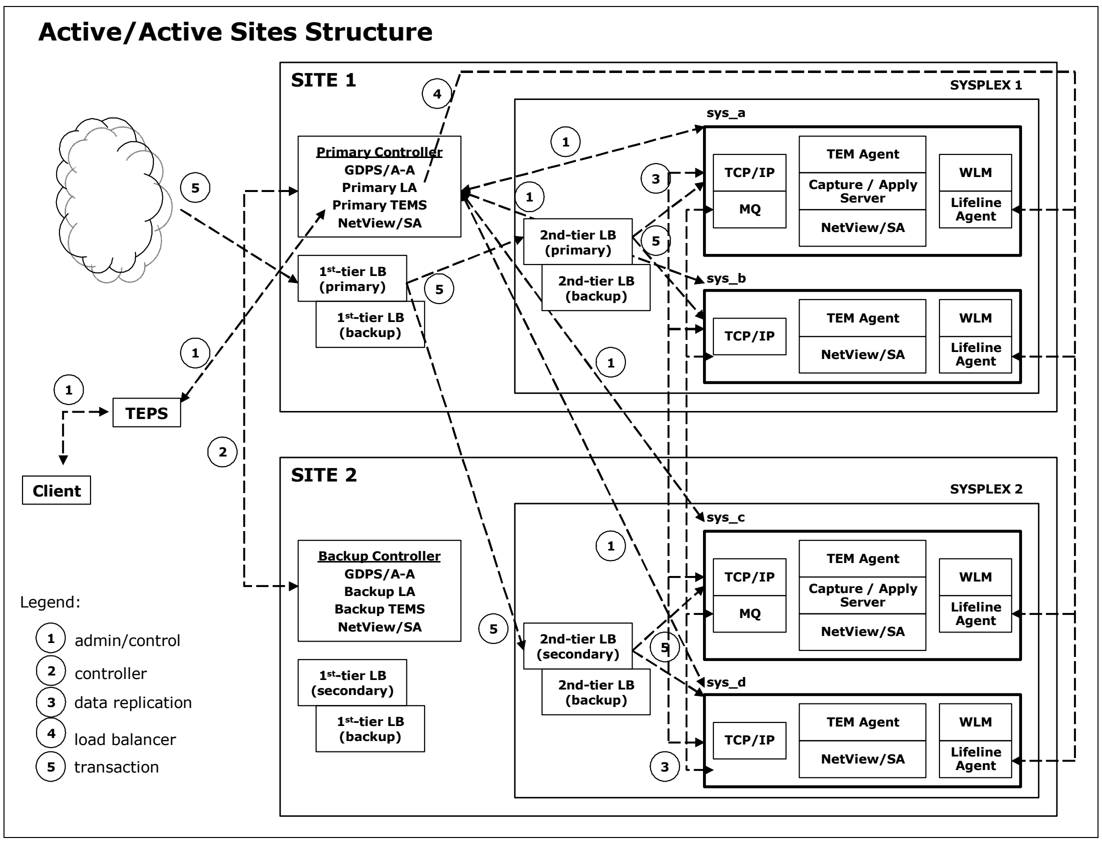


Figure 2-1 GDPS Active/Active Sites Structure

Administration and Control

First, two controllers are required in a GDPS Active/Active environment for redundant purposes. The GDPS controllers should be configured as monoplexes, one at each site. One is designated as the master controller, and the other is the backup controller. The master controller hosts the GDPS Master, the Primary Lifeline Advisor, and the NetView Enterprise Master functions. They work together to provide a central point of control for the systems and workloads participating in a GDPS Active/Active environment.

IBM Multi-site Workload Lifeline for z/OS consists of Lifeline Advisors and Lifeline Agents. The Lifeline Advisor runs on the Controller and provides information to the external Load Balancer on where to distribute transactions, and provides information to GDPS on the health of the GDPS Active/Active environment. The Lifeline Agent runs on all production LPARs with Active/Active workloads defined and provides information to the Lifeline Advisor on the health of the workloads and the systems. The Lifeline Advisor uses this information to calculate the routing recommendations and communicates the routing instructions to the external Load Balancer by using the SASP protocol. The Lifeline Agent also runs some workload operation requests, such as Reset connection requests, sent from the Lifeline Advisor.

NetView component runs on all systems, providing automation and monitoring functions. System Automation component runs on all systems, and provides system automation infrastructure for workload and server management functions. System Automation also provides remote communication capability to enable GDPS to manage sysplexes from the outside.

IBM Tivoli Monitoring components (TEP, TEPS, and TEMS) provide monitoring infrastructure, plus alerting and situation management for the workload and replication status in the GDPS Active/Active environment. TEMS on the Controller provides communication to the Tivoli Monitoring components that are running on the distributed platforms.

Controller High Availability

The primary and backup Controllers provide high availability by communicating by using heartbeats periodically. If the master controller fails, the backup Controller performs a takeover. In this case, the Lifeline Advisor function, the Enterprise Master NetView function, and the GDPS Master functions are switched to the backup Controller.

Replication

In a GDPS Active/Active environment, the data is kept in-sync through software replication. The IBM InfoSphere Data Replication (IIDR) products, by using the capture changed data at the source site and transaction replays at target site technique, manage the synchronization of updated database data between sites. For each workload, the Capture engine at the source site collects the changed updates from the database log, transmitting the data through the network between sites, and deliver the changed data to the Apply engine at the workload target site. The Apply engine reconstructs and writes the transaction updates to the corresponding database. The replication direction and latency information is reflected back to the controller so that subsequent routing recommendations for the workload can be calculated.

Workload Distribution

Figure 2-1 on page 12 shows first-tier Load Balancer and second-tier Load Balancer. First-tier load balancer provides site selection based on Lifeline Advisor recommendation, whereas Second-tier Load Balancer provides LPAR selection also based on Lifeline Advisor's recommendation.

When a workload transaction arrives at the first-tier load balancer, based on the routing recommendation provided by the Lifeline Advisor, it is routed to the workload's currently active site. When the transaction arrives at the second-tier load balancer within that site, the second-tier load balancer routes the transaction to an LPAR based on the Lifeline Advisor's recommendation.

In a normal Sysplex environment, Sysplex Distributor can take the role as a second-tier Load Balancer without being SASP-compliant. In this case, the Lifeline Advisor does not provide routing recommendation for distributing the transaction within the site.

2.2 GDPS Active/Active product

Before taking a closer look at how GDPS Active/Active works, this section provides a conceptual view of GDPS Active/Active environment and briefly covers some concepts you must know.

2.2.1 Active/Active sites concept

For one GDPS Active/Active solution, two or more sites at a theoretically unlimited distance, run the same application with same data, providing cross-site workload balancing, continuous availability, and disaster recovery. All sites run 'live' infrastructure and maintain a copy of data (might have delay due to synchronization) so that all sites are ready to accept workload distribution.

2.2.2 Active/Active site configuration options

There are two different workload types in a GDPS Active/Active configuration:

Active/Standby
: In this configuration, all transactions within one workload are statically routing to one site and can fail over to the other site in case of workload failure. Infrastructures are all active on both sites. It is the fundamental paradigm shift from a failover model to a continuous availability model. In an Active/Standby configuration, each site is identical with the same data, the same hardware, and the same applications.

Active/Query
: Where read-only transactions within one workload can be split and routed to both sites at the same time. An Active/Query configuration also allows querying data on either site. Workload distribution between the sites is based on policy options, and takes into account environmental factors such as the latency for replication that determines the age (or currency) of the data in the standby site. There is no data replication associated with a query workload because there are no updates to the data.

These workload types are determined by the parameter CONFIGURATION_TYPE, which is named in the WKLOADDESC System Automation policy entry.

2.2.3 GDPS Active/Active Workload

To support the switchable workload mechanism, the GDPS Active/Active solution comes with supporting architectures, including asynchronized data replication and intelligent workload distribution. Based on these components and their integration, GDPS, with the advantage of monitoring and automation, provides a central control to achieve one-key-switch function and automation recovery from a sudden failure.

The GDPS Active/Active solution is based on workloads. Workloads that are involved in the GDPS Active/Active solution can be distributed to different sites, either in an Active/Query mode or Active/Standby (or Update) mode.

This section describes the different scopes of workloads.

Query Workload

Transactions associated with the Active/Query workload cannot do any updates to data. The Active/Query workload can be routed to either sites or both. If this is what is wanted, use an Active/Query configuration. An Active/Query workload must be associated with one update workload. When latency of associated data replication exceeds a predefined threshold, the Active/Query workload would switch to ensure that the data queried does have much of a delay.

Update Workload

An update workload contains transactions with update data associated with this workload. Not all transactions within an update workload must be update transactions. An update workload can only be routed to one site within an Active/Standby configuration at any time.

A workload is not only a transaction group. It is a combination of data, middleware, and network. In contrast to all other GDPS solutions, this design enhances continuous availability.

Although the objective of this book is not focused on the implementation of GDPS Active/Active, Appendix A, "IBM Global Technology Services and GDPS service offering" on page 97 provides more information about acquiring this service.

The System Automation policy

The workload definition is initiated in the GDPS controller SA Policy in User E – T Pairs (99).

User E-T pairs are used to define the GDPS configuration options for DOMAINS, OPTIONS, and WKLOADDESC plus SWITCH, CONTROL, and BATCH script definitions. These definitions are only required on your GDPS Controller systems. They are required even if you are using another automation product to automate your systems.

The workload is defined in the entry, WKLOADDESC. Parameters in the WKLOADDESC entry define attributes of a specified workload, such as the type of workload (active/query or active/standby), and latency threshold. Each workload must have one WKLOADDESC entry.

An example of the WKLOADDESC entry is shown in Figure 2-2.

```
User E-T Pairs (99) PDB 3 (Controller Systems)

Step 7 - Define the GDPS/A-A Workloads

----------------------------------------------------------------
| WKLOADDESC | WKL_NOVA_C2                                     |
----------------------------------------------------------------
| Keyword                                    | Data
--------------------------------------------------------------------------------------------
| WORKLOAD                                   | WKL_NOVA_C2
| TARGET_LIST                                | 'PLEXPT1,PLEXPT2'
| CONFIGURATION_TYPE                         | ACTIVESTANDBY
| REPLICATION_LATENCY                        | '8000,5000'
| DB2GROUP                                   | 'PLEXPT1(DSNCB02),PLEXPT2(DSNCB02)'
| WORKLOAD_FAILURE                           | PROMPT
| SITE_FAILURE                               | PROMPT
| CONSISTENCY_GROUPS                         | 'QMC2_CG01,QMC2_CG02,QMC2_CG03,QMC2_CG04,QMC2_CG05'
| CONSISTENCY_GROUP                          | 'QMC2_CG01,QCACB12,QAPCB12,QCACBA2,QAPCBA2'
| CONSISTENCY_GROUP                          | 'QMC2_CG05,QCACB12,QAPCB12,QCACBA2,QAPCBA2'
| CONSISTENCY_GROUP                          | 'QMC2_CG02,QCACB22,QAPCB22,QCACBB2,QAPCBB2'
| CONSISTENCY_GROUP                          | 'QMC2_CG03,QCACB32,QAPCB32,QCACBC2,QAPCBC2'
| CONSISTENCY_GROUP                          | 'QMC2_CG04,QCACB42,QAPCB42,QCACBD2,QAPCBD2'
```

Figure 2-2 Example of WKLOADDES Entry

The relationship of workload and associated infrastructures is defined in the production SA policy, IBM MVS™ Components (33). GDPS Active/Active workloads are mapped to SA applications (or application groups) so that applications are grouped under workloads. From a solution point of view, the transaction subsystem and replication subsystem need to be defined and controlled as “infrastructures” in a workload. SA tracks the individual members of the workload application group (APG) and reports to the GDPS Active/Active controller.

Lifeline configuration file

> **Note:** GDPS Active/Active does not specifically require the use of an SA Application Group, but considering the number of applications under a workload, you should group applications.

The Lifeline Advisor is responsible for detecting failures and determining whether a sysplex has failed entirely. The Lifeline Advisor configuration statement defines information about the lifeline advisor, agent, and outside load balancer on how they communicate with each other. Within the lifeline configuration file and using the **`cross_sysplex_list`** statement, workload names are linked to the load balancer IPs and ports of the application group. Each statement can present either one Active/Query or Active/Standby workload.

Q-Replication configuration

Q Replication, or Q-rep, is used by GDPS active/active continuous availability for data synchronization.

For a non-MCG workload, the workload is not defined directly in the Q-rep configuration. To map a workload to a database and replication infrastructure, the Q-map name must be the same as the workload name. In this case, the Q-map associated resources such as replication engines, send/receive queue and tables are all part of the workload.

For an MCG workload, the workload name *cannot* be the same as the Q-map name because for one workload there are multiple Q-maps mapping to it. Mapping of Q-maps and a workload is specified in the SA policy following the workload definition. Then, in the Q-rep configuration, define the Q-map in the same was as a non-MCG and there is one MCGSYNC table in one DB2, linking multiple Q-Maps into the MCG. The MCG name must be the same as the workload name. In this way, an MCG workload can link with the data infrastructure.

The link between an Active/Query workload and Active/Standby workload are defined in the lifeline configuration file following the **`query_workload_list`** statement. Parameters in this statement also specify the distribution type and distribution-specific options.

Load Balancer

Transactions arrive at the workload distributor, also known as the load balancer.

Components of a workload are not defined directly in the Load Balancer configuration file, but the concept of group applications applies to the load balancer as well. All application servers in one application group are defined in a load balancer and provide the same service for that client. A group is considered unavailable if all its applications are unavailable. A workload is considered unavailable on one site if one of its application groups is unavailable. Considering a workload of multiple application groups, if one of the groups is unavailable, the workload will fail on that site. Only one application group can be defined to each Active/Query workload.

2.2.4 GDPS Active/Active product

GDPS Active/Active product, like other GDPS products, is automation code, aiming at a higher level of high availability and disaster recovery. GDPS Active/Active controlling functions rely on control systems. GDPS Active/Active codes are not only installed on controller systems, but also on production systems (the ‘satellite code’).

GDPS Active/Active provides basic functions like other storage-based GDPS solutions provide, such as system-related functions (ACTIVATE/DEACTIVATE, RESET, LOAD), monitoring system and alerting, and batch script interface. More important, GDPS Active/Active solution controls transaction routing, and planned or unplanned switch. New connections can be routed to preferred site according to predefined policy.

GDPS Active/Active is the central control of all components that can be managed by GDPS Active/Active. Compared with traditional GDPS products, GDPS Active/Active manages more software components within the solution. Users can configure GDPS to fully control components to perform actions such as starting or stopping address spaces or key functions centered around workload routing and failure handling.

2.2.5 GDPS environment

Normally, in a GDPS Active/Active solution, two or more production sysplexes are in remote locations. Only one sysplex is recognized as active and an active/standby workload can be routed to this sysplex. Workload infrastructures should be active on both sites, which makes it ready to take over a workload whenever needed. Data replications are established between two sysplexes by software.

The controller systems are introduced by the GDPS Active/Active solution, providing a central control of the sysplexes and workloads belonging to GDPS Active/Active. Two controllers are required in a GDPS Active/Active environment for redundancy purposes, one on each site. The master controller is in charge of controlling at any time, whereas the backup controller stands by as backup, with communication to the master controller. The controller is introduced by GDPS Active/Active and is isolated from the production sysplex, which is monoplex on each site.

2.2.6 Graceful switch

Graceful switch is introduced by GDPS Active/Active to help ensure data integrity while processing planned workload switches. It releases users from the responsibility of data integrity during maintenance. When the environment is healthy, graceful switch is enabled. The prerequisites for this environment include but are not limited to the following items:

- Data latency (the measure of time delay that describes how long it takes for data to move from site 1 to site 2)
- Application servers are up and running normally on both sites.

Graceful switch can be triggered by a GDPS Active/Active predefined planned action script. It processes in four tiers to achieve RPO 0 (during a switch from Site 1 to Site 2):

- Tier 0: Quiesce batch: Reminding customer to stop batch before processing graceful switch
- Tier 1: Stop new connections routing to Site 1 (current active site)
- Tier 2: Wait for queue transactions to complete; cancel Online Workload and persistent connections; set fence on Site 1
- Tier 3: Wait for replication to complete; set fence on Site 2 to RW and switch workload to Site 2

The coded script, can complete the switch request in minutes, depending on the scope of data infrastructure included in the specific workload and system resources availability.

Note: GDPS provides an API to increment processor capacity temporarily known as capacity backup, or CBU, before routing transactions to a standby site.

Before doing a graceful switch, do a health check. Otherwise, you run the risk that the graceful switch to another site would fail or stop in a confused state. Verify the following before performing a graceful switch:

- Verify that the GDPS Active/Active needed operators are logged on.
- Variables are set correctly, such as Soft Fence.
- GDPS Active/Active related components are working correctly, such as z/OS, SA, Lifeline, and Replication.
- The following three GDPS components are on the same system:
  - NetView “Enterprise Master “
  - GDPS “Master “
  - Lifeline Advisor “Primary “

2.3 Multi-Site Workload Lifeline for z/OS

A workload is an aggregate of the following three components:

- Software, or user written applications and the middleware runtime environment (such as a CICS region and a DB2 subsystem)
- Data sources, or related set of objects that must preserve transactional consistency (such as DB2 tables)
- Network connectivity, or the one or more TCP/IP addresses and ports that map the applications or middleware.

There are multiple requirements for workload distribution function in a GDPS Active/Active solution. Transactions for a workload must be able to be directed to either site, based on the health and availability of the sites and the server applications for a workload. If the application servers for a workload are not available, it must be detected and reported as a workload failure. If all resources of a workload on a site are unavailable, it must be treated as a site failure. Workload must be able to switch gracefully between two sites to support site-wide maintenance. To fulfill this requirement, Multi-Site Workload Lifeline for z/OS was developed and as part of the GDPS Active/Active solution, integrates with other components.

Lifeline is a product that enables load balancing workload to two or more different sites that are separated by unlimited distances and running the same applications. Data replication is done between the two sites so that they have the same data. Application servers are requested to be active on both sites to process incoming workload request.

Lifeline provides high availability with load balancing and workload rerouting. As a key component of GDPS Active/Active solution, Lifeline plays a key role in resolving two major problems:

- Continuous availability for critical workloads
- Downtime for planned outage

Note: The Lifeline product only supports TCP/IP workload. In the future version, SNA-based workload will also be supported.

For more information about Multi-Site Workload Lifeline, see Chapter 4, “Workload distribution and balancing” on page 39.

2.4 Software data replication products

The GDPS Active/Active solution uses software data replication rather than storage-based replication technology. The main advantage of software data replication technology is that you can access data from both sites at the same time. Concurrent access to both sites’ data will dramatically reduce RTO in a continuous availability solution and make the GDPS Active/Active solution possible.

The key differences between software data replication and storage-based data replication are shown in Table 2-1.

Table 2-1 Software data replication versus hardware data replication

Replication technology	Mode	Distance	Impact to source workload	Data accessibility in target during replication	Transaction Consistency
Software data replication	Asynchronous	Unlimited	Almost no impact	Allowed	Preserved by replication product
Metro Mirror	Synchronous	Up to 300 KM	Impact write I/O performance	Not allowed	Needs help from subsystem restart
Global Mirror	Asynchronous	Unlimited	Almost no impact	Not allowed	Needs help from subsystem restart
XRC	Asynchronous	Unlimited	Impact I/O performance only when pacing happens	Not allowed	Needs help from subsystem restart

The GDPS Active/Active solution relies on asynchronous data replication to support unlimited distance. An Active/Active workload might need access to both sites data concurrently, preserving transaction consistency. Although the asynchronous storage-based data replication fits the Active/Standby solution perfectly, software data replication can support both Active/Standby and Active/Active solutions.

However, software data replication technology needs to read the replication log to capture the changes that are generated by the source subsystem. It does not support all types of data today. Currently, IBM products support the following data types:

- DB2 for z/OS data
- IMS data
- VSAM data

These are the corresponding products for the replication:

- IBM InfoSphere Data Replication for IMS for z/OS
- IBM InfoSphere Data Replication for VSAM for z/OS
- IBM InfoSphere Data Replication for DB2 for z/OS

Software data replication will preserve transaction consistency by only applying committed data and using dependency analysis to maintain the correct order. Software data replication latency comes from capture delay, transmit delay, and apply delay.

GDPS Active/Active needs to know the software data replication status and performance metrics to decide whether it can route workload to both sites in an Active/Query configuration or if it is ready to switch the Active/Active workload to a standby site. To do that, traditional software data replication products use the Event Integration Facility (EIF) to pass events to IBM Tivoli NetView for z/OS, and NetView generates an alert to notify GDPS and LifeLine.

GDPS Active/Active uses the Network Management Interface (NMI) to pull software data replication performance information for monitoring purposes. You can also use GDPS Active/Active to issue Q Replication commands, for example, to start or stop the queue. Q Replication provides data synchronization for GDPS Active/Active sites and the NMI for monitoring the replication environment from IBM Tivoli NetView for z/OS.

2.5 IBM Tivoli Monitoring and IBM Tivoli NetView for z/OS

GDPS Active/ Active relies on IBM Tivoli Monitoring and IBM Tivoli NetView. This section provides an overview of both.

2.5.1 IBM Tivoli Monitoring

IBM Tivoli Monitoring helps you optimize IT infrastructure performance and availability. This proactive system monitoring software manages operating systems, databases, and servers in distributed and host environments.

Tivoli Monitoring helps you identify and fix outages and bottlenecks that threaten key applications before they affect your environment:

- Proactively monitors system resources to detect potential problems and automatically respond to events.
- Provides dynamic thresholds and performance analytics to improve incident avoidance.
- Improves availability and mean-to-time recovery with quick incident visualization and historical look for fast incident research.
- Collects data that you can use to drive timely performance and capacity planning activities to avoid outages from resource over-utilization.
- Facilitates system monitoring with a common, flexible, and intuitive browser interface and customizable workspaces.

For more information about, see 5.3, “IBM Tivoli Monitoring” on page 50.

2.5.2 IBM Tivoli NetView for z/OS

IBM Tivoli NetView for z/OS provides enhanced management for business-critical IT network infrastructure and availability:

- Provides key capabilities and advanced functions related to networking, automation, and enhanced enterprise integration (management functions that work in cooperation with other products).

- Supports heterogeneous networks that include both SNA and TCP/IP and supports changing network and system requirements that exist on System z. NetView provides the ability through a single console to manage your entire network.
- Provides high availability and automation enhancements for improving overall system availability, problem diagnostics, problem determination, and management to increase operations efficiency and effectiveness.
- Improved enterprise resiliency for continuous availability combined with IBM GDPS Active/Active support.

For more information, see 5.9, “IBM Tivoli NetView for z/OS and IBM Tivoli NetView Monitoring for GDPS” on page 57.

3

GDPS and data replication

This chapter describes how the data replication software work and how they interact with GDPS Active/Active.

This chapter includes the following sections:

- Data replication overview using software
- IBM InfoSphere Data Replication for DB2 in GDPS Active/Active
- IBM InfoSphere Data Replication for VSAM in GDPS/AA
- IBM InfoSphere Data Replication for IMS in GDPS/AA

3.1 Data replication overview using software

The GDPS Active/Active solution relies on software-based asynchronous replication techniques to synchronize DB2, IMS, or VSAM data between sites.

The replication technology consists of capture engines, apply engines, and a transport infrastructure. Capture engines monitor the source database for committed transaction data, which is captured and placed in a transport infrastructure for transmission to a target location. In the target location, apply engines write the data in real time to an active copy of the database.

Figure 3-1 shows how the data flows in this scenario.

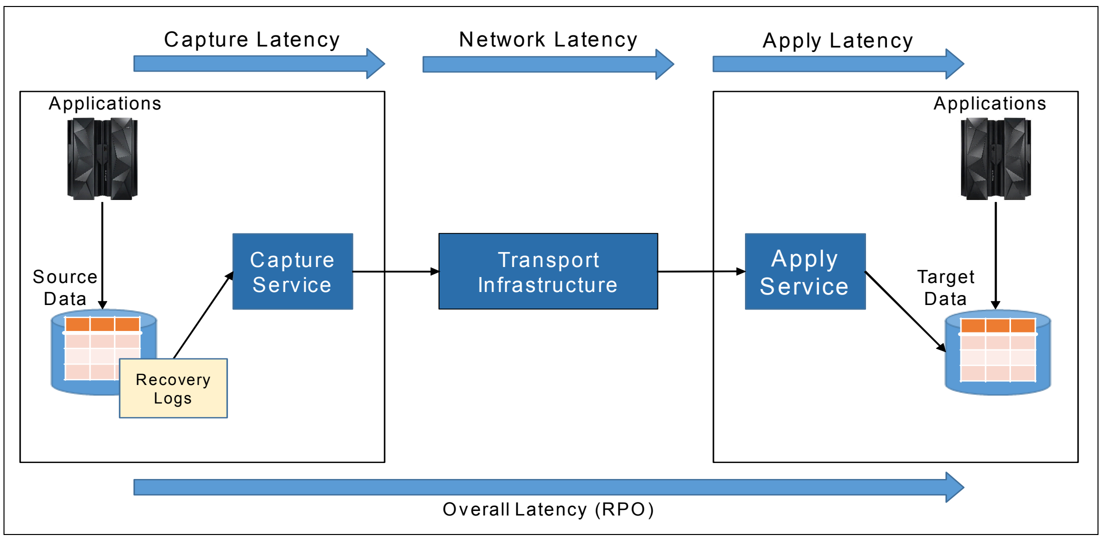


Figure 3-1 Data Replication flow

As of today, the source data types to be replicated are supported through these software-based replication techniques:

- DB2 using IBM InfoSphere Data Replication (IIDR) for DB2 for z/OS
- IMS using IBM InfoSphere Data Replication (IIDR) for IMS for z/OS
- VSAM using IBM InfoSphere Data Replication (IIDR) for VSAM for z/OS

DB2 replication relies on IBM MQ queues to send data from the source workload site to the target workload site. IMS and VSAM replication relies on TCP/IP as the communication interface by using different host names and ports to differentiate the source and target sites.

Each of these replication techniques are described in this chapter.

3.2 IBM InfoSphere Data Replication for DB2 in GDPS Active/Active

IBM InfoSphere Data Replication (IIDR) for DB2 for z/OS is the product that delivers Q Replication technology, which is an asynchronous log capture and transaction replay DB2 replication solution that is required for the GDPS Active/Active solution to provide Active/Active continuous availability.

3.2.1 How does IIDR for DB2 work?

This section will not teach you IIDR for DB2, but just to provide enough information for you to understand how IIDR for DB2 works in the GDPS Active/Active solution. If you want to understand the design of IIDR for DB2, you can find detailed information in *Understanding and Using Q Replication for High Availability Solutions on the IBM z/OS Platform*, SG24-8154. For installation and configuration of IIDR for DB2, you can find additional information in the IBM InfoSphere Data Replication Information Center at:

http://pic.dhe.ibm.com/infocenter/iidr/v10r2m1/

This section includes these topics:

- Q Replication
- Q Replication queue map definition
- Consistency Group (CG) and Multiple Consistency Group (MCG)

Q Replication

IIDR for DB2 for z/OS provides various replication technologies, which include Q Replication, SQL Replication, Event Publishing, and Change Data Capture. The GDPS Active/Active solution uses Q Replication technology for DB2 data in z/OS. Q Replication replicates DB2 data asynchronously. At the source site, Q replication reads the DB2 logs, then transmits the committed unit of work (UOW) information to the target. At the target site, Q Replication generates the SQL again based on the received message, then applies it to the target database with the same UOW information in the correct order for the same data. The data flow is shown in the Figure 3-2.

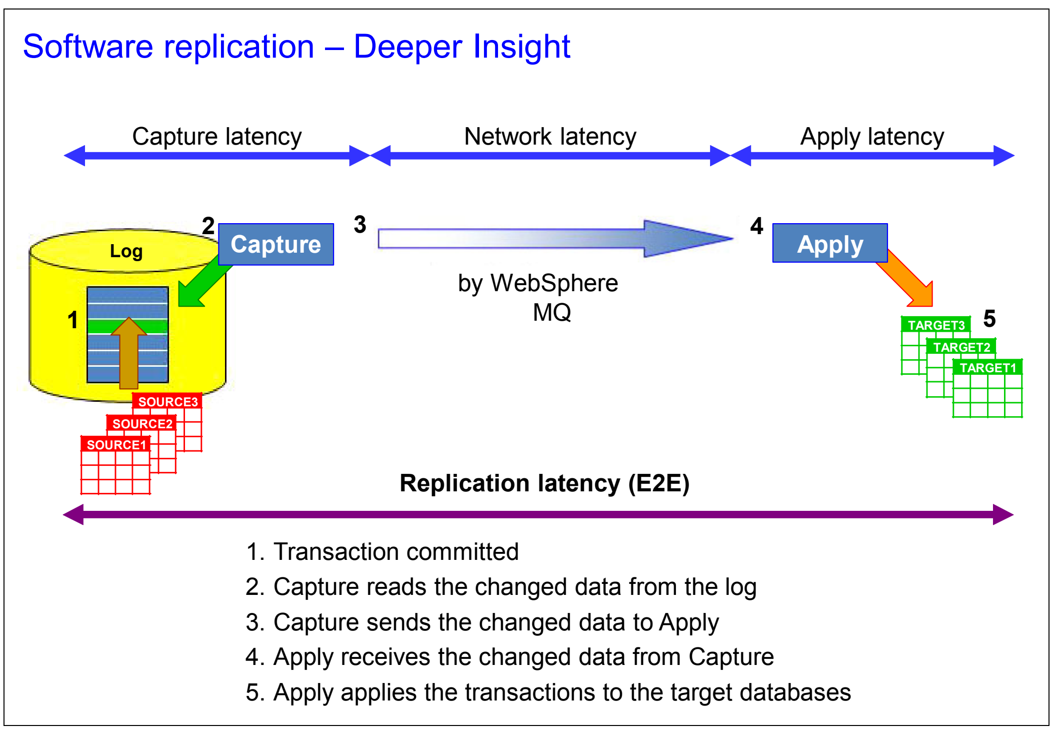


Figure 3-2 Q Replication flow chart

In a replicated environment, data integrity is one of the most important points to be considered. Q Replication enforces it by the following methods:

- Q Replication will only pass committed units of work to the target site to make sure that all data are clean
- Q Replication also applies committed data in a unit of work fashion at the target site to maintain the transaction consistency
- When using parallel apply technology, the order that changes are applied to the target site can be different from the source. However, if there are multiple changes to a single record, Q Replication uses dependency checking to make sure that these changes are applied in the correct order at the target site, by applying them serially.

Q Replication queue map definition

Q Replication uses IBM WebSphere MQ for z/OS to transmit messages without loss and in the correct order.

MQ Objects

The following is a summary of the WebSphere MQ objects that are required to replicate data from a Q Capture program on one node to a Q Apply program on another node in a unidirectional configuration, with a brief description of their usage:

Queue manager	A program that manages queues for Q Capture programs, Q Apply programs, and user applications. One queue manager is required on each system where a Q Capture or Q Apply program runs.
Send queue	A queue that directs data, control, and informational messages from a Q Capture program to a Q Apply program or user application. In remote configurations, this is defined as a remote queue on the source system corresponding to the receive queue on the target system. Each send queue should be used by only one Q Capture program, but multiple send queues can be associated to the same receive queue on the target system.
Receive queue	A queue that receives data and informational messages from a Q Capture program to a Q Apply program. This is a local queue on the target system.
Administration queue	A queue that receives control messages from a Q Apply program or a user application to the Q Capture program. This is a local queue on the system where the Q Capture program runs. There is a remote queue definition on the system where the Q Apply program or a user application runs, corresponding to the administration queue where the Q Capture program runs.
Restart queue	A queue that holds a single message that tells the Q Capture program where to start reading in the DB2 (recovery) log after a restart. This is a local queue on the source system. Each Q Capture program must have its own restart queue.
Spill queue	A model queue that you define on the target system to hold transaction messages from a Q Capture program while a target table is being loaded. The Q Apply program creates these dynamic queues during the loading process that is based on the model queue definition, and then deletes them. A spill queue (with any user-defined name) can be specified at the subscription level.

For multidirectional replication configurations, two sets of WebSphere MQ objects are defined for replicating data from and to each node.

The WebSphere MQ objects must be defined for Q Replication. Their definitions are stored in the Q Replication control tables.

Q Replication queue map

Q Replication queue maps include the WebSphere MQ send queue, receive queue, and administration queue that participate in a replication configuration. When Q subscriptions are created, they are added to an existing replication queue map.

Queue Map is the most important concept in GDPS Active/Active solution configuration. Later on, you can find out how to use Queue Map to link Q Replication with MQ and GDPS/AA code.

Consistency Group (CG) and Multiple Consistency Group (MCG)

When you use multiple receive queues to replicate a workload, you can synchronize the apply process across receive queues to ensure that a time-consistent point can be restored, even if data is lost for one of the queues, before switching the workload to a standby site in unplanned events.

This function is used for disaster recovery. It is used only if you use more than one receive queue to replicate the tables that need to be recovered.

> **Note:** If you split the changed tables of same units of work into two receive queues, the transaction consistency in the target site cannot be guaranteed during replication. User applications must handle it if they need to access the data at the target site then. Eventually, data in the target site becomes consistent through the actions of the synchronization function.

At the highest level, synchronizing one or more Q Apply programs across multiple receive queues involves the following concepts:

1. Consistency Groups (CGs)

   In a CG, all tables are replicated by using the same replication queue map. The Q Apply program maintains transactional consistency for this set of tables by applying dependent transactions in the source commit order and applying other transactions in parallel. A Q Apply program preserves consistency per receive queue.

2. Multiple Consistency Groups (MCGs)

   An MCG is a set of consistency groups that are used for replicating a workload. Replication for all consistency groups can be synchronized to ensure that data loss for any consistency group does not prevent restoring transaction consistency on a common time stamp before a failover.

   Define a multiple consistency group name and assign the group to a set of queue maps by using the ASNCLP command line program. When the queue maps share a common multiple consistency group name, you can enable synchronized apply across the receive queues. The synchronization can be dynamically turned on and off.

   When you enable synchronized apply, you can:

   – Specify how often each Q Apply browser thread checks to see whether it should apply the next available changes. This process ensures that Q Apply is not applying changes that are not available for other queues in the group. Otherwise, data loss would prevent data from being synchronized before a failover for disaster.

   – Choose between two different synchronization modes.

   – Use a command to start or stop synchronization for the group.

Note: To support MCG, the Q Capture and Q Apply programs must be at Version 10.2.1 or later, and the control tables must be upgraded to architecture level 1021 or later.

The IBM GDPS Active/Active continuous availability solution supports multiple consistency groups for a workload and uses the synchronized apply function that is provided by Q Replication. All GDPS operations on a workload are carried out for each consistency group that is processing the workload. For example, a **STOP REPLICATION** command for a workload operates on all replication queue maps (consistency groups) that are used for replicating the tables that are modified by the workload.

3.2.2 IIDR for DB2 architectural overview

To replicate the data from one system to the other, IIDR for DB2 uses a few components, as shown in Figure 3-3.

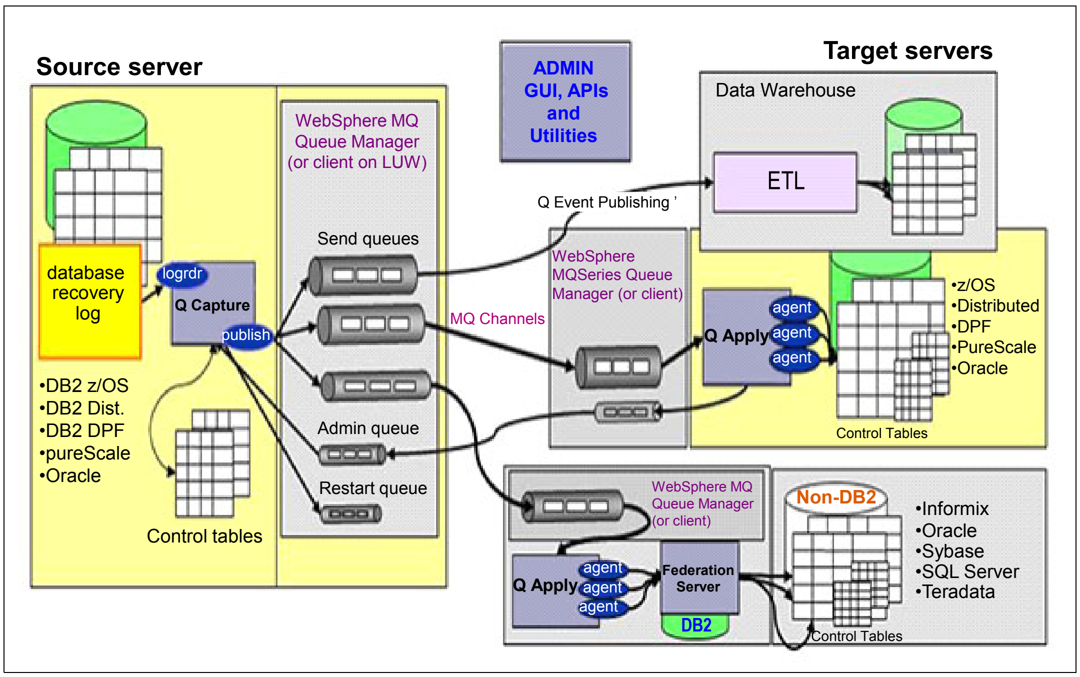


Figure 3-3 Q Replication architecture

The key components that are part of the replication engine are:

- Source server (which contains the data to be replicated)
- Q Capture (which reads the logs of the source server and generates the messages)
- WebSphere MQ (which transfers the messages to the target site with a guarantee)
- Q Apply (which applies the changes to the target server)
- Target Servers (which applies the changes to the target database)

3.2.3 IIDR for DB2 and GDPS Active/Active

The Q Replication technology that is provided by IBM InfoSphere Data Replication for DB2 for z/OS is a replication engine component of GDPS Active/Active solution. This section describes how IIDR for DB2 interacts with the other GDPS Active/Active components.

Q replication configuration

GDPS Active/Active solution relies on Q Replication to replicate DB2 data in z/OS. You need to configure Q Replication first to support the GDPS Active/Active function. The following are the main configuration tasks of Q Replication:

1. Create WebSphere MQ objects
2. Create Q Replication control table
3. Create Q Replication Queue Map
4. Create Q Subscription
5. Create Q Replication MCG (optional)

A Queue Map is used to identify source and target for each consistency group that is used for replicating a workload. You define Queue Map with MQ queues as a consistency group. Then, create a Q Subscription to indicate which table will use which Queue Map. All tables assigned to same Queue Map are in one CG. In this case, the CG has same scope as the Queue Map.

Multiple CGs or Queue Maps are allowed for one workload. In the case of multiple CGs or Queue Maps, define an MCG group for Q Replication. Typically MCG would be used as the workload name.

GDPS configuration

Workload is the key to GDPS configuration. Link the Q Replication with GDPS using the GDPS Workload definition. Information on the GDPS Workload definition can be found in the *GDPS Active/Active 1.4 Planning and Implementation Guide,* ZG24-1767.

Active-Active workload

An Active-Active (A-A) site solution is two or more sites separated by extended distances running the same applications and using the same data to provide cross-site balancing, continuous availability, and disaster recovery. As such, it is the aggregation of these items:

- Software: User-written applications (for example, a COBOL program) and the middle ware runtime environment (such as CICS region, InfoSphere Replication servers, and DB2 subsystems).
- Data: A set of related objects that must have transactional consistency maintained and optionally referential integrity constraints preserved (such as DB2 Tables, VSAM files, and IMS databases).
- Network connectivity: One or more TCP/IP addresses or host names and ports (for example, 10.10.10.1:80).

The consistency of the data is important. Keep data that belongs to the same consistency group in the same workload. Define networks and applications that access data from the same consistency group in the same workload as well. This helps ensure data consistency when moving the workload.

Link the GDPS and Q Replication configuration by GDPS Workload name and Q Replication consistency group name. If you are not using an MCG, make the GDPS Workload name the same as the related Q Replication queue name. By doing this, GDPS will know that the tables belong to the same consistency group. If using MCGs, the GDPS Workload name should be same as the related Q Replication MCG name. Doing this will identify that all Queue Maps belong to same MCG for GDPS.

Control

Using the configuration that is outlined in “Active-Active workload” on page 29, GDPS Active/Active will recognize the Q Replication consistency group and issue Q Replication commands to interact with Q Replication.

Monitor

GDPS Active/Active needs to monitor the Q Replication status and receive alerts from Q Replication. You can see the flow in Figure 3-2 on page 25.

Network Management Interface

You can use Tivoli NetView Monitoring for GDPS to monitor the health of the Q Replication environment between sites in a GDPS/ Active-Active configuration. Tivoli Monitoring provides a unified and high-level view of the performance and status of the different products that are part of GDPS/ Active-Active (IMS Replication, VSAM Replication, Q Replication, and Load Balancer Advisor). For more detailed replication performance information, tuning, and troubleshooting, use the Q Replication Dashboard.

Monitoring from Tivoli is performed by using the NMI, which is a request-reply protocol that uses an AF_UNIX socket. GDPS Active/Active does not query the Q Capture or Q Apply monitor tables. Instead, it uses this new interface to issue NMI requests to the Q Capture and Q Apply programs to obtain performance information.

The Network Management Interface is implemented by the Q Apply and Q Capture programs, through which NMI client applications can request operational data that include status and performance information, for example replication latency. To enable this interface, you must set two parameters for both the Q Capture program and Q Apply program, `nmi_enable` and `nmi_socket_name`.

Event Integration Facility

You can specify that the Q Apply program generate event notifications for specific conditions such as when average replication latency is exceeded or a receive queue stops.

For GDPS Active/Active, events can be sent as EIF messages over a TCP/IP IPv4 socket for use by IBM Tivoli NetView for GDPS. These events are consumed by NetView Event/Automation Services (E/AS) by using an adapter called the Event Receiver. This adapter converts events to an internal format that can be processed by other NetView functions such as automation.

In GDPS Active/Active configurations, it is expected that events that are reported through E/AS will reflect conditions that require an immediate response to be handled through automation. For example, an event called “workload average max latency exceeded” when generated by the Q Apply program, might cause workload connections to be switched from Site 1 to Site 2. EIF messages are sent to both the primary and backup controllers by using TCP/IP. After receiving events, the primary controller reacts but the backup controller ignores them.

For more detailed information about the configuration of IIDR for DB2, see:

http://pic.dhe.ibm.com/infocenter/iidr/v10r2m1/topic/com.ibm.swg.im.iis.repl.qrepl.doc/topics/iiyrqcsoaacfg.html

3.3 IBM InfoSphere Data Replication for VSAM in GDPS/AA

To allow VSAM workloads to be part of GDPS Active/Active, you must have IBM IIDR for VSAM installed in your production LPARs. This section provides an overview of how it works, and how it relates to GDPS/AA.

Note: At the time this book was written, Transactional VSAM (DFSMStvs), non-CICS updates using VSAM record-level sharing (RLS), and VSAM linear data sets (LDSs) are not supported for replication using IIDR for VSAM for z/OS. Consider other replication methods and techniques to protect such workloads for high availability disaster recovery (HADR) purposes.

3.3.1 How does IIDR for VSAM work?

IBM InfoSphere Data Replication for VSAM is a replication engine that runs on z/OS. Its main purpose is to replicate VSAM data and their changes from a source to a target system, in a near-real time fashion, typically in geographically dispersed locations. To do so, you must have IIDR for VSAM installed in both the source and the target partitions, and they must have network connectivity between them.

To maintain synchronized replicas, IIDR for VSAM reads replication logs that are in system logger log streams, which contain log records of insert, update, delete, and commit changes that are run in the VSAM source data sets, and apply these changes to the target VSAM data sets through a CICS region running at the target partition. The age of the target data depends on the latency between the source and target servers, and whether the target is able to apply the changes at the same speed as they are done in the source. This is key to avoid queuing replication data, thus decreasing the latency and therefore the RPO. The lower the overall latency, the newer the data is at the target system.

IIDR for VSAM is *unidirectional*, which means you can only send changes from one site to another instead of in both directions at once, for the same workload. It other words, you can only have one active site with transactions or programs doing updates to VSAM data for a single workload. It is also possible to have different active sites processing different workloads, but you must ensure that they are using separate replication infrastructure (VSAM data sets, log streams, log readers, apply servers, and CICS regions) to avoid data conflicts. This replication infrastructure is more detailed in the 3.3.2, "IIDR for VSAM architectural overview" on page 31. For more information, see *IBM InfoSphere Data Replication for VSAM for z/OS Guide and Reference*.

3.3.2 IIDR for VSAM architectural overview

To replicate the data from one system to the other, IIDR for VSAM uses the components that are shown in Figure 3-4.

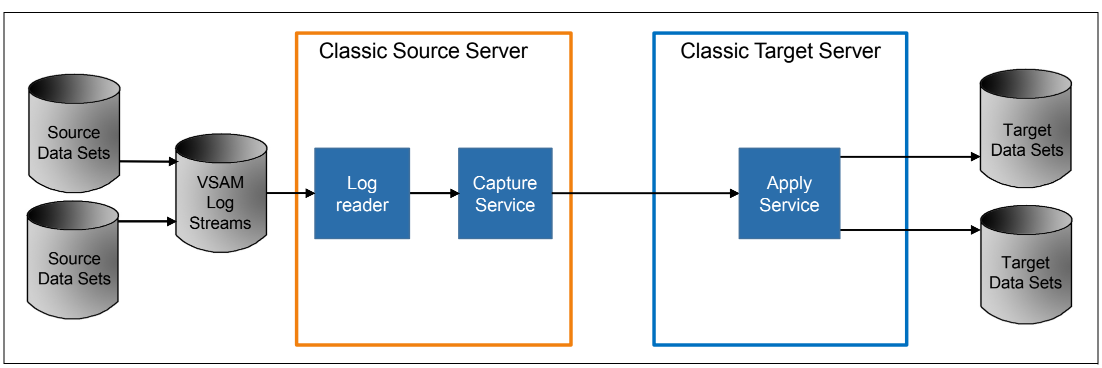


Figure 3-4 VSAM Replication flow

The following are key components of the replication engine:

- VSAM source and target data sets (which contain the data to be replicated)
- VSAM log streams (which contain the replication logs)
- Classic data servers (running on both the source and the target partitions)
- CICS region at the target to apply the changes to VSAM target data sets

When any update is done in the VSAM source data sets, the CICS Transaction Server (CICS TS) or CICS VSAM Recovery (CICS VR) are used for logging the details of these changes to VSAM log streams. The Classic source server then reads these changes through its log reader service. It then packages them as change messages that describe each insert, update, delete, and commit operations on the data; and sends the change messages through the capture service by using TCP/IP to the Classic target server, which is located at a different site. The target server applies the VSAM file changes through a target CICS region running on the same z/OS logical partition (LPAR) as the Classic target server.

To replicate the changes to the VSAM target data sets, the target CICS region uses a z/OS IP CICS socket (or CICS listener) to communicate with the apply service that runs in the Classic target server. There must be one CICS target region per Classic target server, with a CICS listener started.

The apply service establishes multiple connections with CICS by using the z/OS IP CICS socket when the server starts:

- A connection to the CICS replication utility, which runs replication processing functions on behalf of the apply service.
- A connection to each instance of a CICS replication writer that is started, which write VSAM source updates to their associated VSAM target data sets.

As changes arrive at the target server, the apply service schedules independent work for an active CICS replication writer by sending each change on a specific connection.

Note: If you are setting up multiple replication environments, you must set up one z/OS IP CICS socket per target CICS region.

Log Stream considerations in data sharing and non-data sharing environments

You must define log streams in both data sharing and non-data sharing environments. The type of log stream that you define depends on whether you access the log stream from one LPAR or from multiple LPARs, as follows:

- If you only access a log stream from one LPAR, you can use a DASD-only log stream or you can use a coupling facility log stream.
- If you access a log stream from more than one LPAR, you need a data sharing environment and a coupling facility log stream.

In a data sharing environment, you must define log streams in a coupling facility to enable logging operations to access the same log stream across all participating LPARs in the sysplex, as multiple LPARs can generate inserts, updates, and deletes to the same VSAM data set. The target CICS region can write changes from all LPARs in the correct order and maintain transactional consistency.

3.3.3 IIDR for VSAM and GDPS/AA

IBM InfoSphere Data Replication for VSAM is a replication engine component of GDPS Active/Active. To relate IIDR for VSAM to GDPS/AA, this section describes the concepts of *Subscriptions*, *Transactions*, and *Events*.

Subscriptions

The data sets that support a specific application are organized and mapped to what is called a *subscription*, which consists of a unique combination of source data sets, user-configurable memory caches, and communication paths. A subscription is a URL that identifies the Classic target server plus TCP/IP connection between the capture and apply services.

Because of its autonomous structure, replication can be started, stopped, and maintained for a subscription independently of other subscriptions. Stopping replication for one subscription has no effect on the operations of others. To accomplish this, IIDR for VSAM maintains a *bookmark* database (a VSAM data set file) which contains information that provides a restart position for each subscription if replication stops.

Units of recovery (UORs) and transactions

UOR is a group of operations that are either committed or backed out as a group. These operations represent a *transaction*, such as an online transaction, or similar changes that applications generate. It is also possible to configure the capture server to treat multiple transactions as a single transaction. IIDR for VSAM also groups multiple changes into transactions for non-transactional changes. Changes to unrecoverable data sets and changes captured by CICS VR are automatically grouped into transactions to provide more efficient use of system resources while minimizing latency.

For each source UOR, the apply service runs the following actions in sequence:

1. Apply the changes to the target VSAM data sets using CICS file control requests.
2. Update the bookmark database with the new restart position for the subscription, if necessary.
3. Commit the UOR.

A subscription maintains the sequence of transactions as they occur at the source by applying changes to a specific record in the correct order.

Events

To participate in GDPS/AA, the classic data server needs to be configured to send EIF events to an event server, through a TCP/IP connection.

The Classic data server emits EIF events to the event server based on three factors:

- Subscription state
- Subscription apply latency
- Heartbeat event

NetView E/AS is used to convert these events into network management vector transport (NMVT) formatted alerts that are forwarded to the NetView hardware monitor, where they are filtered and routed to the NetView automation table. The NetView program validates the information in the alert, and if the information passes validation, it is forwarded to the Lifeline Advisor and GDPS components.

Naming convention for subscriptions and workloads

One significant consideration from a GDPS perspective is related to naming conventions. In VSAM replication, you must define *subscription*. The name of the subscription for a workload must match the workload name as you define it to GDPS. If you do not follow this requirement, GDPS will not be able to control the replication using scripts or the GDPS windows.

3.3.4 Minimizing latency (and RPO) and improving replication performance by using parallel apply

Parallel apply can improve the performance of your replication environment by applying UORs concurrently to target data sets. It also enables you to minimize latency by writing all available work across your subscriptions in near-real time. Two main goals are taken into account: *Latency* and *Consistency*. Because low latency is also a high priority in replication, your subscription design must optimize the trade-off between latency and maintaining precise order.

Latency

Low latency is also a high priority in replication processing, as it is directly related to the RPO of the target data sets. To achieve parallelism, Data Replication for VSAM applies transactions in strict order only to a single record. To keep latency low, it applies changes to a target data set almost immediately after an application commits a UOR in the source data set. However, in some cases the contents of a target data set can lag behind the source:

- Planned or unplanned replication outages
- Large UORs that take longer to process
- High volumes of updates
- Heavy load or burst conditions

In situations like these, applying updates to the target data sets might lag behind the source updates until the condition causing the slowdown is resolved. A very large UOR can lag behind because the source server only sends committed UORs to the target. This means that a UOR cannot start apply processing until it is complete at the source. Both the source and target servers use caching mechanisms to ensure that maximum throughput is achieved in these situations.

Consistency

In parallel apply processing, transactions can be applied to the target in a different order than they were applied at the source if any *dependent* transactions are applied first. IIDR for VSAM maintains consistency by applying transactions in the correct sequence at a record level. For example, a withdrawal from your bank account might succeed only if the bank first completes your transfer to that account.

Within a single subscription, dependencies on UORs that update the same data set record are a limiting factor. In this case, IIDR for VSAM places a higher priority on maintaining the precise order of changes as they occurred at the source data set. For transactions that change separate records or data sets, it places lower priority on maintaining a strict sequence. Parallel apply processing is likely to write transactions out of order when any of these conditions are true:

- The subscription is processing concurrent transactions at the source.
- The source transactions modify different records in the same data set.
- The source transactions modify different data sets.

This less stringent approach to maintaining order enables the target server to run more parallel processing.

Important: Transactions that change data sets in more than one subscription can result in splitting a UOR into two or more apply UORs that arrive at the target data sets in an unpredictable order. For this reason, Data Replication for VSAM cannot maintain consistency for transactions that modify data sets in multiple subscriptions. Design your subscriptions to include all data sets that are related to a single business application, such as customers or inventory, to keep the number of such transactions to a minimum.

Restriction: You might not get the full performance benefits of parallel apply if UORs insert entry-sequenced data set (ESDS) records into the same data set. The system performs dependency analysis that causes these UORs to be applied serially.

3.4 IBM InfoSphere Data Replication for IMS in GDPS/AA

To allow IMS workloads to be part of GDPS Active/Active, you must have IIDR for IMS installed in your production LPARs. This section provides an overview of how it works, and how it relates to GDPS/AA.

3.4.1 How does IIDR for IMS work?

IBM InfoSphere Data Replication for IMS is a replication engine that runs on z/OS. Its main purpose is to replicate IMS data and their changes from a source to a target system, in a near-real time fashion, typically in geographically dispersed locations. To do so, you must have IIDR for IMS installed in both the source and the target partitions, and they must have network connectivity between them.

To maintain synchronized replicas, IIDR for IMS reads log records that describe changes made to the source IMS, which are in IMS logs and contain records of insert, update, delete and commit changes done in the IMS databases, and apply these changes to the target IMS databases through a program specification block, or *apply PSB*, running at the target partition.

An apply PSB contains a program communication block (PCB) for each target database. An apply service schedules the first apply PSB for each subscription and applies changes to the target database. IIDR for IMS requires an apply PSB for each subscription.

The age of the target data depends on the latency between the source and target servers, and whether the target is able to apply the changes at the same speed as they are done in the source. This is key to avoid queuing replication data, decreasing the latency and the RPO. The lower the overall latency, the newer the data is at the target system.

IIDR for IMS is *unidirectional*, which means you can only send changes from one site to another instead of in both directions at once, for the same workload. Therefore, you can only have one active site with transactions or programs doing updates to an IMS database for a single workload. It is also possible to have different active sites processing different workloads, but you must ensure that they are using separate replication infrastructure (IMS databases, IMS logs, log readers, apply servers, IMS PSBs, and so on) to avoid data conflicts. This replication infrastructure is detailed in 3.4.2, “IIDR for IMS Architectural Overview” on page 36. For more information, see *IBM InfoSphere Data Replication for IMS for z/OS Guide and Reference.*

3.4.2 IIDR for IMS Architectural Overview

To replicate the data from one system to the other, IIDR for IMS uses the components shown in Figure 3-5.

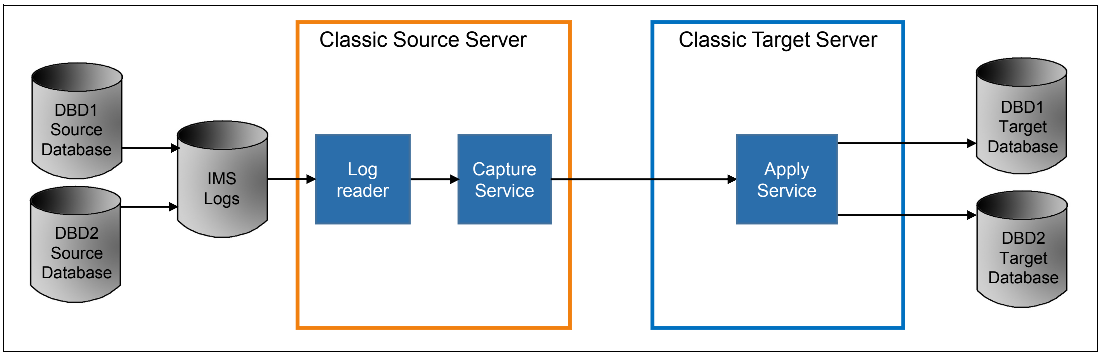


Figure 3-5 IMS Replication flow

The following are the key components of the replication engine:

- IMS source and target databases (which contain the data to be replicated)
- IMS logs (which contain the updates log records that are read by capture processing)
- Classic data servers (running on both the source and the target partitions)
- PSB region at the target to apply the changes to IMS target databases

The Classic source server uses a log reader to process IMS log data and capture changes to a source database. Capture processing then packages these changes as change messages that describe insert, update, delete, and commit operations on the data. The source server sends the change messages to the target server that applies the changes to the target IMS database, running on the same z/OS LPAR as the Classic target server. The Classic target server also runs a database resource adapter (DRA) service to communicate with the IMS DRA interface and manage access to IMS. IIDR for IMS uses the DRA to apply changes to the target databases.

IIDR for IMS can capture changes from a single DB/DC or DBCTL subsystem. It can also capture changes from hundreds or thousands of shared databases in an IMS data sharing environment. You can capture updates from multiple IMS DL/I batch jobs, DB/DC subsystems, or DBCTL subsystems in a sysplex. IIDR for IMS also supports high availability environments that implement FDBR (Fast Database Recovery) regions.

IMS replication uses significant network bandwidth and requires TCP/IP links between the source and target LPARs to operate effectively at high speeds. All replicated data and the control messages necessary to maintain replication flow over the network connection.

3.4.3 IIDR for IMS and GDPS/AA

IBM InfoSphere Data Replication for IMS is a replication engine component of GDPS Active/Active. To relate IIDR for IMS with GDPS/AA, there are a few concepts that this section will describe: *Subscriptions*, *Transactions*, and *Events*.

Subscriptions

A subscription is defined much the same as IIDR for VSAM (see Subscriptions), except that instead of data sets that support an application, the IMS databases support the application.

Because of its autonomous structure, replication can be started, stopped, and maintained for a subscription independently of other subscriptions. Stopping replication for one subscription has no effect on the operations of others. To accomplish this, IIDR for IMS maintains a *bookmark* database (an IMS database) which contains information that provides a restart position for each subscription if replication stops.

Units of recovery (UOR) and transactions

A UOR is a group of operations that are either committed or backed out as a group. These operations represent a *transaction*, such as an online transaction or similar changes that applications generate. It is also possible to configure the capture server to treat multiple transactions as a single transaction.

For each source UOR, the apply service runs the following actions in sequence:

1. Apply the changes to the target IMS databases.
2. Update the bookmark database with the new restart position for the subscription, if necessary.
3. Commit the UOR.

A subscription maintains the sequence of transactions as they occur at the source by applying changes to a specific record in the correct order.

Events

To participate in GDPS/AA, Classic data server needs to be configured to send EIF events to an event server, through a TCP/IP connection.

The Classic data server emits EIF events to the event server based on three factors:

- Subscription state
- Subscription apply latency
- Heartbeat event

NetView E/AS is used to convert these events into NMVT formatted alerts, which are forwarded to the NetView hardware monitor, where they are filtered and routed to the NetView automation table. The NetView program validates the information in the alert, and if the information passes validation, it is forwarded to the Lifeline Advisor and GDPS components.

Naming convention for subscriptions and workloads

One significant consideration from a GDPS perspective is related to naming conventions. In IMS replication, you must define *subscription*. The name of the subscription for a workload must match the workload name as you define it to GDPS. If you do not follow this requirement, GDPS will not be able to control the replication using scripts or the GDPS windows.

3.4.4 Minimizing latency (and RPO) and improving replication performance by using Parallel apply

Parallel apply, as described in 3.3.4, “Minimizing latency (and RPO) and improving replication performance by using parallel apply” on page 34, can also improve the performance of your replication environment when using IBMS by applying UORs concurrently to target databases. It also enables you to minimize latency by writing all available work across your subscriptions in near-real time. Two main goals are taken into account: *Latency* and *Consistency*. Because low latency is also a high priority in replication, your subscription design must optimize the trade-off between latency and maintaining precise order.

Latency

Low latency is also a high priority in replication processing, as it is directly related to the RPO of the target databases. To achieve parallelism, Data Replication for IMS applies transactions in strict order only to a single record. To keep latency low, it applies changes to a target database almost immediately after an application commits a UOR in the source database. However, in some cases the contents of a target database can lag behind the source:

- Planned or unplanned replication outages
- Large UORs that take longer to process
- High volumes of updates
- Heavy load or burst conditions

In situations like these, applying updates to the target databases might lag behind the source updates until the condition causing the slowdown is resolved. A very large UOR can lag behind because the source server only sends committed UORs to the target. This means that a UOR cannot start apply processing until it is complete at the source. Both the source and target servers use caching mechanisms to ensure that maximum throughput is achieved in these situations.

Consistency

In parallel apply processing, transactions can be applied to the target in a different order than they were applied at the source if any *dependent* transactions are applied first. IIDR for IMS maintains consistency by applying transactions in the correct sequence at a record level. For example, a withdrawal from your bank account might succeed only if the bank first completes your transfer to that account.

Within a single subscription, dependencies on UORs that update the same database record are a limiting factor. In this case, IIDR for IMS places a higher priority on maintaining the precise order of changes as they occurred at the source database. For transactions that change separate records or databases, it places lower priority on maintaining a strict sequence. Parallel apply processing is likely to write transactions out of order when any of these conditions are true:

- The subscription is processing concurrent transactions at the source.
- The source transactions modify different records in the same database.
- The source transactions modify different databases or partitions.

This less stringent approach to maintaining order enables the target server to run more parallel processing.

Important: Transactions that change data sets in more than one subscription can result in splitting a UOR into two or more apply UORs that arrive at the target data sets in an unpredictable order. For this reason, Data Replication for IMS cannot maintain consistency for transactions that modify databases in multiple subscriptions. Design your subscriptions to include all databases that are related to a single business application, such as customers or inventory, to keep the number of such transactions to a minimum.

Restriction: You might not get the full performance benefits of parallel apply if a UOR changes segments that do not have a unique concatenated key. The source server analyzes the UOR to determine whether changed segments have no keys, or sequence fields are missing. If so, subscription processing switches between parallel processing and serial processing as required. The number of changes that affect this type of segment determines the extent to which the subscription uses serial apply processing. Also, you cannot define a subscription for parallel apply if a database participates in logical relationships between different physical databases.

4

Workload distribution and balancing

This chapter describes the IBM Multi-site Workload Lifeline for z/OS, how it load balances TCP/IP workloads across two sites, and how it interacts with other components in a GDPS Active/Active solution. It is intended to help you better understand Lifeline's role within the GDPS Active/Active solution.

IBM Multi-site Workload Lifeline enables intelligent load balancing of workloads across two sites at unlimited distance to achieve nearly continuous availability. It plays an integral role in the GDPS Active/Active solution and provides the following benefits:

- Improved performance: New connections of workloads are routed to the applications, servers, and systems most capable of processing them so that transaction response time is reduced. System resources are used more efficiently.
- Improved availability: New connections of workload can be routed to available applications and systems when some of them down. Outages for maintenance updates or other planned events can be minimized.
- Reduced recovery time: Reduce Recovery Time Objective from hours to minutes. With disk replication, traditional DR solutions recover on standby site by restarting systems or applications. Normally that takes hours and IT services are out for this period. With Lifeline working within GDPS/AA solution, workload can be switched to the standby site in minutes.

This chapter includes the following sections:

4.1 Key concepts

Multi-site Workload Lifeline determines the availability of the server applications that make up a workload, the capacity of the systems where the server applications reside, and other metrics. Multi-site Workload Lifeline uses this information to provide recommendations to two tiers of load balancers.

The first tier of load balancers must be hardware appliances that support a protocol called Server/Application State Protocol (SASP, which is described in RFC 4678). Multi-site Workload Lifeline provides recommendations to this first tier on which site new workload transactions should be directed. The second tier of load balancers can either be hardware appliances that support SASP or the z/OS sysplex distributor. The second tier load balancers receive the workload transactions from the first tier load balancers and are then responsible for directing the transaction to one instance of the server application within the selected site. If the second tier load balancer is a hardware appliance, then Multi-site Workload Lifeline provides recommendations to this tier on which server application within the site is best able to handle the new workload transaction.

In Figure 4-1, the Workload Distribution box makes up the software and hardware that is required to perform load balancing of workloads. Multi-site Workload Lifeline determines the availability of the server applications that make up a workload, the capacity of the systems where the server applications reside, and other metrics.

The Multi-site Workload Lifeline (as part of the Workload Distribution box in Figure 4-1) provides distribution of workload requests between the sites. It can route around a failed site or around failed workloads on a site. Multi-site Workload Lifeline dynamically selects a site based on ability of site to handle additional workload, or based on custom configuration for the workload. The Data Replication box implements software-based replication to keep data sources in sync between sites, which allows the data to be accessed from either site, at unlimited distance between the sites. The Control and Monitoring box manages and monitors each workload defined in the configuration.

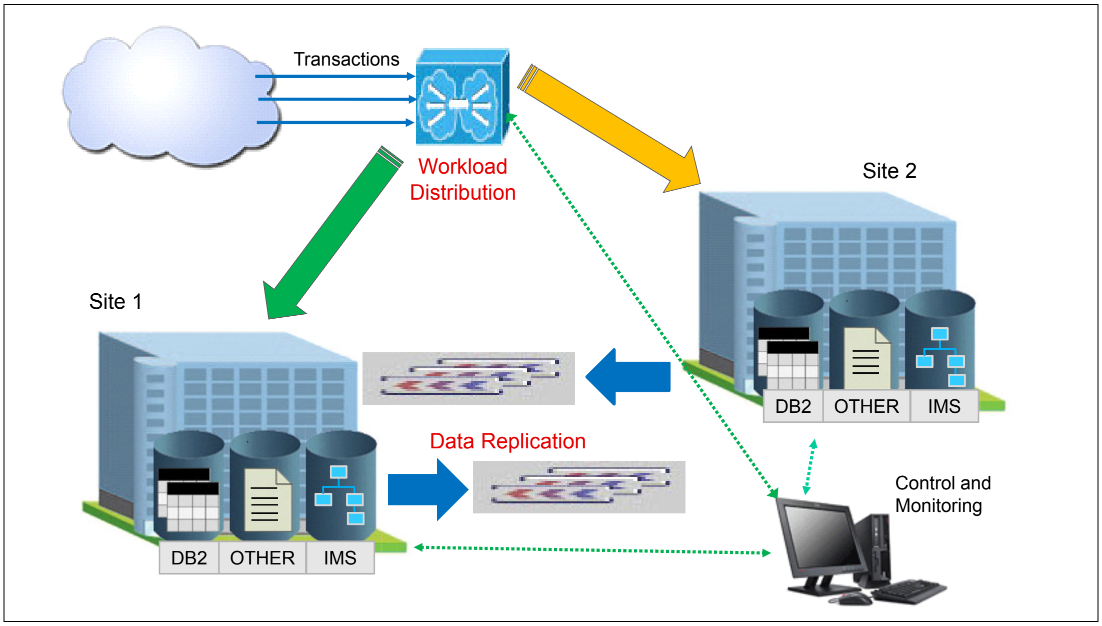


Figure 4-1 Multi-site Workload Lifeline

4.2 Multi-site Workload Lifeline Components

Multi-site Workload Lifeline consists of Lifeline Advisors and Lifeline Agents. Advisors run on controllers with an address space and Agents run on each production system where application servers controlled by the GDPS Active/Active solution run. At any time, only one Advisor on the GDPS Active/Active master controller acts as the primary Advisor. It communicates with the load balancer Lifeline Agents and a secondary Lifeline Advisor to accomplish monitoring and the workload routing tasks.

The primary Lifeline Advisor talks to its peer to update workload state information periodically. The secondary Advisor uses this information to tell whether the primary Advisor is 'up' or not. If the primary Advisor is 'down', it takes over the primary role.

4.2.1 Lifeline Advisor

Lifeline Advisor is the key component of Lifeline, providing recommendations to the load balancer on workload distributions. It provides the first tier load balancer with recommendations about which site workload should be routed to. Based on the recommendation, an Active/Query workload can be routed to one site that is preferred, or both sites at the same time. For Active/Standby workloads, it can only be routed to one site. Lifeline Advisors maintain a control list that allows the external load balancer, the secondary Lifeline Advisor, and Lifeline Agents to talk to it. For more information about internal and external Lifeline communications, see 4.2.3, "Lifeline communication route".

Lifeline Advisor has three main responsibilities:

- Monitor site status
- Provide recommendations to route workloads
- Switch workloads for planned and unplanned outages

4.2.2 Lifeline Agent

Lifeline Agents are running on production systems where workload infrastructures are running. Agents get instructions from the Advisor about which applications servers on their LPARs need to be monitored. They monitor the health and availability of these application servers and periodically send the information to Lifeline Advisor.

4.2.3 Lifeline communication route

Figure 4-2 on page 42 demonstrates the Multi-site Workload Lifeline communication routes, which have these characteristics:

- Flow 1 shows the communication between the Lifeline Advisor and the first and second tier load balancers. The advisor provides recommendations to the first tier load balancers about which site to route new transactions for a workload. The advisor can also provide recommendations to the second tier load balancers about which server application within the site to route a new transaction to.
- Flow 2 shows the communication between the lifeline advisor running on the primary controller and each of the lifeline agents running on the LPARs in both sites. The agents gather information about the LPAR where they are active and the server applications for workloads that are on that LPAR. This information is communicated to the advisor, which uses that information to generate distribution recommendations. The advisor also uses this information to determine when all server applications for a workload are no longer available so that it can show a workload failure.

- Flow 3 shows the communication between the lifeline advisor, called the primary advisor, on the primary controller, and a backup lifeline advisor, called the secondary advisor, on the secondary controller. The primary advisor provides workload state information to the secondary advisor. During a failure of the primary advisor, the secondary advisor assumes the role of primary advisor and maintains the current state of all workloads.
- Flow 4 shows the first to second tier connection load balancing.
- Flow 5 shows the load balancing from the second tier to the server instance.

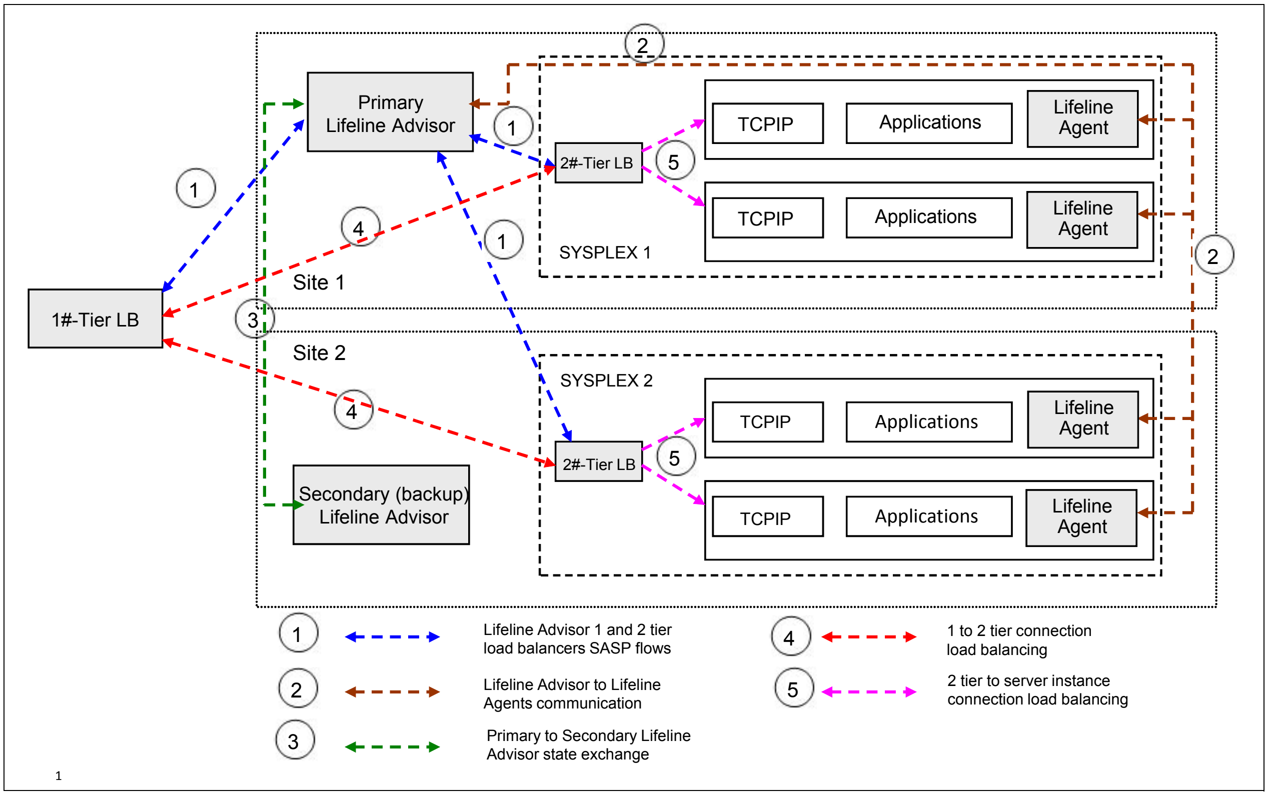


Figure 4-2 Multi-site Workload Lifeline communication routes

Lifeline Advisor to load balancer communication

Lifeline Advisor talks to the load balancer by using the SASP to give advice on workload distribution. Lifeline does not handle workload distribution. It only gives recommendations.

The first tier of load balancers must be hardware appliances that support a protocol called SASP (as described in RFC 4678). Multi-site Workload Lifeline provides recommendations to this first tier on which site new workload transactions should be directed. Different types of applications accessing the shared data can be defined in different groups. The key element here is that all systems have a collective object that refers to “all similar services” that makes it easier to work with them as a single unit. Based on recommendations from the Lifeline Advisor, the load balancer selects a site and forwards the request to the second-tier load balancers.

Note: Application groups are defined in the first tier load balancer. Workload failure is recognized if all application servers in any group are all unavailable, so you might want to group applications of the same type or the same importance level. Well planned application groups avoid low importance applications switching for unnecessary reason and increase workload granularity. Only one application group can be defined in one query workload. If you need more than one application groups, you need to put that in another Active/Query workload, but associated it with the same Active/Standby workload.

The second tier of load balancers can either be hardware appliances supporting SASP or the z/OS sysplex distributor. The second tier load balancers receive the workload transactions from the first tier load balancers and are then responsible for directing the transaction to one instance of the server application within the selected site. If the second tier load balancer is a hardware appliance, then Multi-site Workload Lifeline provides recommendations to this tier on which server application within the site is best able to handle to new workload transaction.

In some configurations, the second-tier load balancers are also external using SASP and they receive recommendations from the Advisors to route workload within the sysplex.

When second-tier load balancers are internal, known as z/OS sysplex distributors, they receive the recommendations from the z/OS communication servers directly.

Load balancing within one site can be processed by other components, but not the second-tier load balancer. In this configuration type, these components are defined as an intermediary node.

Lifeline Advisor to Lifeline Agent communication

Lifeline Advisor sends information about all server applications it wants the Lifeline Agents to monitor. Lifeline Agents gathers information from the Lifeline Advisor about the list of applications that are configured to receive workload requests. The Lifeline Agent works on each LPAR where applications run to monitor and gather the health of applications from a TCP/IP perspective. The TCP/IP status is monitored for the specified applications to determine whether there are problems. This information is transferred back to the Lifeline Advisor and used for recommendations of workload distribution to the load balancer. Additionally, this information is used to monitor workload failures.

In some cases, the user must send a request to drop active connections. This request is sent by the Lifeline Advisor and routed to the Lifeline Agents, with the list of server applications, to reset any active connections for them.

Lifeline Advisor to Lifeline Advisor communication

The Lifeline primary Advisor on the master controller communicates with the Lifeline Advisor on the backup controller. The master controller sends the workload status to the backup controller. When the primary Lifeline Advisor fails, the backup controller takes the role of primary and maintain the state of workloads.

Lifeline Advisor to Support Element communication

The Hardware Management Console (HMC) and Support Element (SE) on each central processor complex (CPC) typically communicate over a network that is separate from the network used for TCP/IP communications. The Lifeline Advisor communicates with the SE by using the Base Control Program internal interface (BCPii) services to periodically query all interconnected CPCs and the images (LPARs) on these CPCs over this network to determine whether the images are available.

You need to grant Lifeline Advisors general authority to use the BCPii, including authority to specific resources such as the interconnected CPCs and images on those CPCs.

Lifeline Advisor to NMI communication

Lifeline Advisor provides a Network Management Interface (NMI) that you can use to monitor Lifeline metrics and statistics, such as LPAR and system availability, information of connected load balancers, Agents and Advisors, application server and workload status, and distribution recommendations for server applications. For more information about the Lifeline Advisor and NMI, see:

http://www-01.ibm.com/support/knowledgecenter/SSLTBW_2.1.0/com.ibm.zos.v2r1.hals001/aqsa01ref7.htm

4.3 Interaction with other components within GDPS Active/Active

GDPS Active/Active, IBM Multi-site Workload Lifeline for z/OS and Tivoli NetView are all independent products running in the z/OS environment. They all support multi-system environments and each product has their own management role, such as the Lifeline Primary Advisor role. The Enterprise Master for NetView can establish connections to NetView programs that are outside the sysplex in which it resides and have data forwarded to it. As of NetView V6R1, this function supports an Active/Active enterprise master NetView program for the GDPS Active/Active Continuous Availability solution. You can have a single enterprise master NetView program for the discovery manager and Active/Active functions, or you can have separate enterprise master NetView programs for these two functions.

To integrate with other components within the GDPS Active/Active solution, the Lifeline Primary Advisor must run on the same system where the NetView Enterprise Master and GDPS Active/Active Master Controller run.

When a planned or unplanned outage occurs on the master controller, the master roles of the following GDPS Active/Active solution components move to the backup controllers at the same time:

- Lifeline: Primary Advisor
- NetView: Enterprise Master
- GDPS Active/Active: Master Controller

For planned changes, the GDPS Active/Active web interface has a central control point to move all three master roles together to the backup controller. Any takeover command issued manually against any product is not recommended as there will be improper reporting of the environment status and GDPS will lose control.

For an unplanned failure, when the Lifeline Secondary Advisor discovers that the connection to the Primary Advisor is missing, it generates a warning message to the backup controller. GDPS on the backup controller captures this message and issues a prompt. The system operator is required to reply to the prompt for takeover, so that all master roles of the three components switch from the master controller to the backup.

Note: Lifeline itself provides options to do takeover automatically or manually following a Primary Advisor failure. For the GDPS Active/Active solution, manual takeover must be configured to cooperate with GDPS Active/Active management.

4.3.1 Lifeline recommendation on workload distribution

Active/Query workload connections are distributed to a site based on routing type and average replication latency. Replication latency is the average delay between the time an update transaction for a workload to the active site is replicated and when it is applied to the standby site.

There are two routing types for an Active/Query workload: *Dynamic* and *static*.

Dynamic workload routing distribution between sites is based on availability and the health of server applications within each site. Static workload routing distribution between sites is based on a configured percentage.

For dynamic workload routing, the user is able specify the distribution options of **`toactive`** and **`tostandby`**. The option **`toactive`** indicates a gradual favoring of the site where the associated Active/Standby workload is active as database replication latency increases. The option **`tostandby`** indicates a gradual favoring of the site where the associated Active/Standby workload is standby as database replication latency increases.

For the **static** distribution type, the distribution option is **`percentage 1-99`**, of new workload connections that will be routed to the active site with the remaining new workload connections distributed to the standby site.

> **Note:** When you define the Lifeline distribution type as **`static`**, you cannot activate an Active/Query workload with the Site keyword. Otherwise, the distribution type configuration will be ignored and workload will be only routed to one site that is specified with **`Site`** keyword.

Lifeline provides suggestions to the first-tier load balancer in the format of **NET WEIGHT**. For an Active/Standby workload, it is a 0 or 1. When 0, it means that no workload is being routed to the second-tier load balancer, whereas a 1 indicates that the Active/Standby workload can be routed to this second-tier load balancer.

For Active/Query workloads, the **NET WEIGHT** value ranges from 0 - 64. A higher weight indicates that the site where the second-tier load balancer routes to can handle more requests for the workload than the alternate site.

When an Active/Query workload is configured as **`static`**, the sum of all members' weight on this site is adjusted to the configured percentage. When it is configured as **`dynamic`**, the weight reflects the site's capacity for processing new connections for this workload.

NET WEIGHT is based on a combination of WLM weight, Communication Server weight from the Lifeline Agents, and data replication latency information from the replication product. For the second-tier load balancer, **NET WEIGHT** only represents the capability among server applications within one application group.

WLM weight

The Workload Manager (WLM) weight is server-specific. It reflects how much displaceable capacity is available on the target system at the importance level of the server application. For a first-tier load balancer group, the WLM weight is not applicable because the registered members are second-tier load balancers. For a second-tier load balancer group, the value is a composite weight, in the range 0 - 64, that indicates the sum of the proportional CP, zAAP, and zIIP weights for the server application.

Replication latency

Replication components (for example, Q-Rep) generate Event Integration Facility (EIF) messages. The NetView Event/Automation Service (E/AS) receives these messages and converts them into network management vector transport (NMVT) format alerts. An NMVT is an SNA request unit that contains solicited or unsolicited data, such as line statistics and generic alerts. The alerts are then filtered in the NetView Hardware Monitor and routed to the NetView Automation Table. Finally, the Automation Table traps the alerts and forwards them to the Lifeline Advisor and GDPS Active/Active components. Latency is a key factor that needs to be considered when making routing direction decisions.

> **Note:** Information from the following events is forwarded to the Lifeline Advisor for Active/Query workloads:
>
> ```
> AA_replication_reset_average_latency_met
> AA_replication_critical_average_latency_exceeded
> AA_replication_constrained_average_latency_exceeded
> AA_replication_critical_average_latency_exceeded
> AA_replication_max_latency_exceeded
> AA_replication_heartbeat
> AA_replication_workload_down
> ```

Communication server weight

This weight is calculated based on availability of the actual application server and the workload capability that it can process that is sent to it by TCP/IP. This design protects new connections from routing to stalled server instances or one that are waiting on a queue. Agents are responsible for getting this information from all active LPARs on both sites and sending it to the Lifeline Advisor.

For a first-tier load balancer group, the communication server (CS) weight is not applicable because the registered members are second-tier load balancers. For a second-tier load balancer group, the CS weight value range is 0 - 100. A higher weight indicates that the server application is able to handle more workload requests than a server application in the same group with a lower weight.

Weight information of workloads can be displayed by issuing the Lifeline `MODIFY` command. For more information about this command, see the IBM *Multi-site Workload Lifeline User's Guide*, SC27-4653

4.3.2 Lifeline in graceful switch

Graceful switch is a key function that GDPS Active/Active provides to achieve a nondisruptive switch of workloads without loss of data during planned outages. Lifeline routes workloads between two sites based on a request from GDPS Active/Active. Before a planned outage, all update workload connections are directed to a single site. Workload connection direction is achieved by issuing the Lifeline command `MODIFY.` To ensure graceful movement, a key requirement is that updates to a database can only occur on one site at any time. Lifeline takes charge of workload movement to ensure that update workload connections are only directed to one site. Graceful switch goes through the following steps with Lifeline actions:

1. New connections to active site must be blocked, by issuing the Lifeline command `MODIFY QUIESCE` against target workload.
2. Wait until all existing transactions of current workloads are complete.

3. Drop non-stopped transactions by issuing the Lifeline command **`MODIFY DEACTIVATE`** against target workload.
4. Redirect all new transaction connections to new site, by issuing the Lifeline command **`MODIFY ACTIVATE`** against target workload on standby site.

4.3.3 Failure detection

Lifeline can detect workload failures or site failures. Workload status can be monitored by Agents, and Lifeline Advisor will determine whether there is workload failure based on information collected from the Agents. If Lifeline Advisor determines that a workload failure has occurred, it will redirect workload to the standby site automatically or manually. Also, Lifeline Advisor can detect site failure using information that is provided by the SE or the HMC. If all LPARs are down or not healthy on the active site, Lifeline Advisor will redirect all workloads to the other site automatically.

5

Controlling and monitoring

This chapter describes the architecture of the IBM Tivoli Monitoring products and provides information to help you plan your deployment and prepare for IBM Geographically Dispersed Parallel Sysplex (GDPS) Active/Active controlling and monitoring.

High availability is the main reason for running existing workloads on IBM GDPS Active/Active.

This chapter includes the following sections:

- Overview
- Prerequisite software for controlling and monitoring
- IBM Tivoli Monitoring
- IBM Tivoli System Automation for z/OS
- IBM Multi-site Workload Lifeline for z/OS
- Middleware
- IBM GDPS Active/Active monitor processing
- IBM GDPS Active/Active Monitor processing during a workload or site failure
- IBM Tivoli NetView for z/OS and IBM Tivoli NetView Monitoring for GDPS
- IBM OMEGAMON XE Family
- IBM GDPS Active/Active web interface

5.1 Overview

IBM GDPS Active/Active provides a comprehensive continuous availability and business continuity solution to support two or more data center sites separated by unlimited distance to achieve recovery point objective (RPO) and recovery time objective (RTO) goals.

IBM NetView, IBM System Automation, and the IBM Lifeline Agent run on all production systems, monitoring the system, the workload on the system and replication latency, and providing information to the Active/Active controllers.

These include monitoring of workload status, the IBM Multi-Site Workload Lifeline product, replication products, and other managed elements, as well as automation of events and processes for the solution to reduce recovery time and increase efficiency in the use of system resources.

5.2 Prerequisite software for controlling and monitoring

Refer to the GDPS website to find the most current list of prerequisites for GDPS/Active-Active:

http://www.ibm.com/systems/z/advantages/gdps/getstarted/gdpsaa.html

5.3 IBM Tivoli Monitoring

Several components of the IBM Tivoli Monitoring product are used in the overall monitoring of aspects such as the workload within the GDPS Active/Active environment.

> **Note:** If your enterprise is already using the required level of IBM Tivoli Monitoring, there is no need to implement additional monitoring or portal server infrastructure for IBM GDPS Active/Active.

5.3.1 Overview of IBM Tivoli Monitoring

IBM Tivoli Monitoring products monitor the performance and availability of distributed operating systems and applications. These products are based on a set of common service components, referred to collectively as Tivoli Management Services. Tivoli Management Services for z/OS components provide security, data transfer and storage, notification mechanisms, user interface presentation, and communication services in an agent-server-client architecture.

5.3.2 Components of the monitoring architecture

IBM Tivoli Monitoring products use a set of service components shared by a number of other product suites. These include IBM Tivoli OMEGAMON® XE monitoring products, IBM Tivoli Composite Application Manager products, System Automation for z/OS, and Web Access for Information Management. The information in this section is also relevant to these products.

Tivoli Monitoring products, and others products that share Tivoli Management Services, participate in a server-client-agent architecture. Monitoring agents for various operating systems, subsystems, databases, and applications (known collectively as Tivoli Enterprise

Monitoring Agents) collect data and send them to a Tivoli Enterprise Monitoring Server. Data are accessed from the monitoring server by Tivoli Enterprise Portal clients. A Tivoli Enterprise Portal Server provides presentation and communication services for these clients. Several optional components such as a historical data warehouse extend the functionality of the framework (see Figure 5-1).

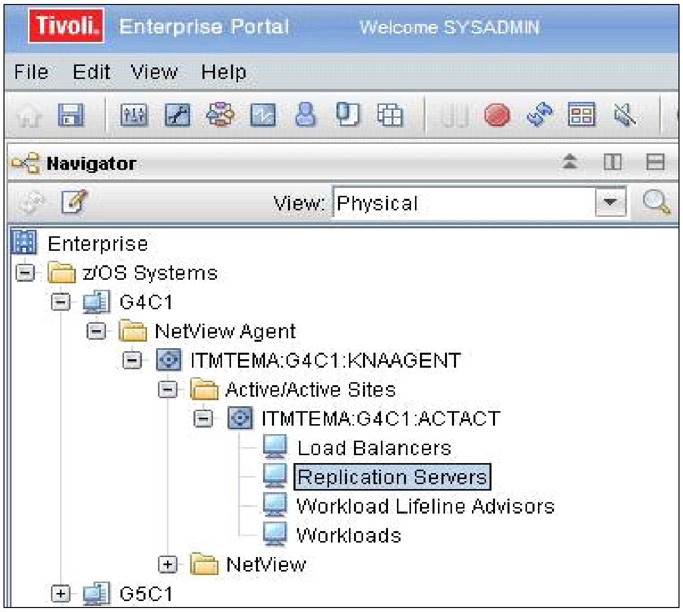


Figure 5-1 Tivoli Enterprise Portal

5.3.3 IBM Tivoli Monitoring components

The following are some of the required components for IBM Tivoli Monitoring:

- Tivoli Enterprise Monitoring Server
- Tivoli Enterprise Portal Server
- Tivoli Enterprise Portal or Portal Client
- Tivoli Enterprise Monitoring Agents
- Tivoli Management Services for z/OS

Tivoli Enterprise Monitoring Server

The Tivoli Enterprise Monitoring Server is the collection and control point for performance and availability data, and alerts received from monitoring agents (for example, the NetView agent). It is also responsible for tracking the online or offline status of monitoring agents.

The portal server communicates with the monitoring server, which in turn controls the remote servers and monitoring agents that might be connected to it directly.

Because of the number of functions the monitoring server performs, large-scale environments usually include a number of monitoring servers to distribute the load. One of the monitoring servers is designated the hub monitoring server, and the remaining servers are termed remote monitoring servers. Each remote monitoring server must be on its own computer and have a unique monitoring server name (node), but the architectures of various remote monitoring servers can differ from each other and from the hub monitoring server. In other words, a remote monitoring server running on UNIX can report to a hub monitoring server running on Windows.

The portal server communicates with the hub, which in turn controls the remote servers and any monitoring agents that might be connected to it directly.

Tivoli Enterprise Portal Server

The Tivoli Enterprise Portal Server provides the core presentation layer for retrieval, manipulation, analysis, and preformatting of data. The portal server retrieves data from the hub monitoring server in response to user actions at the portal client, and sends the data back to the portal client for presentation. The portal server also provides presentation information to the portal client so that it can render the user interface views suitably.

Tivoli Enterprise Portal or Portal Client

Tivoli Enterprise Portal is the interface to the monitoring products. The Tivoli Enterprise Portal consists of the Tivoli Enterprise Portal Server and one or more clients.

The Tivoli Enterprise Portal Server (referred to as the portal server) manages data access through user workspace consoles (the portal clients). The portal server connects to a hub monitoring server. It retrieves data from the hub in response to user actions at a portal client, and sends the data back to the portal client for presentation. The portal server also provides presentation information to the portal client so that it can render the user interface views suitably.

The portal server uses DB2 for the workstation or a Microsoft SQL database to store various artifacts related to presentation at the portal client.

The portal client provides access to the Tivoli Enterprise Portal. There are two kinds of portal client:

- Browser client interface (automatically installed with Tivoli Enterprise Portal Server): The browser client can be run using Microsoft Internet Explorer or Mozilla Firefox. It connects to a web server running in the Tivoli Enterprise Portal Server. Running the browser client is supported only on Windows, Linux, and IBM AIX® computers.
- Desktop client interface: A Java-based graphical user interface on a Windows or Linux workstation. After the desktop client is installed and configured, you can use it to start Tivoli Enterprise Portal in desktop mode. You can also download and run the desktop client using Java Web Start, as discussed in Java Web Start clients.

Tivoli Enterprise Monitoring Agents

Monitoring agents are data collectors. Agents monitor systems, subsystems, or applications; collect data; and pass the data to Tivoli Enterprise Portal through the monitoring server. The agents pass commands from the user to the system, subsystem, or application. An agent interacts with a single system or application and, in most cases, is on the same computer where the system or application is running.

There are two types of monitoring agents:

- Operating system (OS) agents that monitor the availability and performance of the computers in your monitoring environment. An example of an OS agent is the Monitoring Agent for Windows OS, which monitors Windows XP, Windows 2000, and Windows 2003 operating systems.
  - Agentless monitor: This enables a remote node to monitor the health of nonessential desktop operating systems by using a standard monitoring API such as SNMP and thus is also called a remote OS agent.
  - System Monitor Agent: These lighter-weight agents (they require a much smaller footprint than full-function Tivoli Monitoring OS agents) are configured locally to the agent node. This configuration enables them to be deployed autonomously (in other

words, without the support of a Tivoli Enterprise Monitoring Server). In this deployment, they send SNMP event information directly to an SNMP Event Collector such as IBM Tivoli Netcool/OMNIbus. The System Monitor Agents are meant as a replacement for the OMNIbus System Service Monitor agents.

- Other agents (referred to as application agents or non-OS agents) that monitor the availability and performance of systems, subsystems, and applications. An example of a non-OS agent is IBM Tivoli Monitoring for Microsoft Exchange, which monitors the Microsoft Exchange Server.

IBM Tivoli Monitoring also provides a customizable agent called the Tivoli Universal Agent. You can use this agent to monitor most types of data that you can collect in your environment. For example, you can use it to monitor the status of your company's website to ensure that it is available. For more information about the Tivoli Universal Agent, see the *IBM Tivoli Universal Agent User's Guide*.

You can also create your own IBM Tivoli Monitoring agent by using the Agent Builder, a set of tools for creating agents and adding value to existing agents. Using the Agent Builder, you can quickly create, modify, and test an agent to collect and analyze data about the state and performance of different resources, such as disks, memory, CPU, or applications. The builder creates a data provider that allows you to monitor three types of data:

- Availability: Process and service availability, and functionality tests.
- Windows event log: Specific information from the Windows Event Log.
- External data sources: Data from external sources such as Windows Management Instrumentation (WMI), Performance Monitor (PerfMon), Simple Network Management Protocol Version 1 (SNMP V1), external scripts, and log files.

With the Agent Builder's customizable graphical user interface installer, you can create agent-installation packages for easy agent distribution. A key feature of the installer is its ability to package and distribute extensions to existing agents. This allows you to develop new situations, queries, and workspaces for an existing IBM Tivoli Monitoring agent. For complete information about the Agent Builder, see the *IBM Tivoli Monitoring: Agent Builder User's Guide*.

In most cases, the recommended choice for customized agents is the Agent Builder.

Tivoli Management Services for z/OS

Tivoli Management Services for z/OS is an IBM Tivoli Management Services Engine that provides common functions such as communications, multithreaded runtime services, diagnosis (memory dumps), and logging. It works with the Tivoli Enterprise Monitoring Server, monitoring agents, and OMEGAMON components of OMEGAMON XE products running on z/OS.

5.3.4 IBM Tivoli Monitoring operational considerations

The Tivoli Enterprise Portal workspaces provide a monitoring interface to the overall solution, allowing you to set up specific situations for alerting of conditions such as latency reaching a certain threshold or details of such things as the current log relative byte address (RBA) within the replication environment.

If you have implemented the Tivoli Enterprise Monitoring Server on one of the z/OS Controllers, or another z/OS system and you shut down that system, such as for maintenance, you need to consider the impact this has on your monitoring environment. A key item to consider is the movement of the Tivoli Enterprise Monitoring Server to another z/OS image. If this is required as part of the normal operations process, there are these considerations.

- First, the connection between the Tivoli Enterprise Monitoring Server and the Tivoli Enterprise Portal Server will be lost. You need to decide how to re-establish this connection to have data flow from the z/OS systems to the Portal Server. Your procedures need to take this into account.
- Second, the Tivoli Enterprise Monitoring Server maintains a historical database of information gathered by the monitoring agents. Depending on where you restart your Tivoli Enterprise Monitoring Server, this database might not be available in that location and as a result, information can be split across a number of database instances.

These operational considerations, among others such as where you might already be using IBM Tivoli Monitoring for monitoring your distributed environment, can be used to determine where to host your Tivoli Enterprise Monitoring Server.

5.4 IBM Tivoli System Automation for z/OS

IBM Tivoli System Automation for z/OS is a key component of GDPS Active/Active. It provides the automation policy repository in addition to managing the automation of the workload and systems elements. System Automation for z/OS also provides the capability for GDPS to manage and monitor systems in multiple sysplexes.

Note: System Automation for z/OS is required for GDPS Active/Active even if you have another automation product in your environment. Special considerations must be taken into account for such environments to ensure that the monitoring of the environment is kept current and for GDPS to coordinate actions with the other automation product.

5.5 IBM Multi-site Workload Lifeline for z/OS

This product provides intelligent routing recommendations to external load balancers for server instances that can span two sysplexes or sites. IBM Multi-site Workload Lifeline for z/OS can also provide ‘second tier’ routing decisions to server instances with a single site or sysplex if required, similar to Sysplex Distributor. The IBM Multi-site Workload Lifeline for z/OS product consists of Advisors and Agents.

For more information, see the Chapter 4, “Workload distribution and balancing” on page 39.

5.6 Middleware

Components such as IBM CICS regions or IBM DB2 subsystems form a fundamental part of the IBM GDPS Active/Active environment. They provide the applications with the services required to process the workload. To maximize the availability characteristics of the GDPS Active/Active environment, applications and middleware must be replicated across multiple images in the active and standby Parallel Sysplexes to provide local failover during component failure. Automation needs to be in place to ensure clean startup/shutdown and local recovery of these critical components. To use IBM GDPS Active/Active for workloads that use VSAM replication, you must be using IBM CICS.

Note: Even having IBM CICS Transaction Server for z/OS as the transaction processing environment, you must also be using IBM CICS VSAM Recovery for logging the changes to VSAM data sets for any non-CICS-based workloads.

5.6.1 Application Middleware for IBM GDPS Active/Active

Table 5-1 lists the application middleware required for IBM GDPS Active/Active.

Table 5-1 Application middleware required for IBM GDPS Active/Active

Application Middleware	IBM GDPS Active/Active Systems
DB2 for z/OS V9 or higher	Yes - Workload dependent
IMS V11	Yes - Workload dependent
WebSphere MQ V7.0.1	MQ is only required for DB2 data replication
CICS Transaction Server for z/OS V5.1	Yes - Workload dependent
CICS VSAM Recovery for z/OS V5.1	Yes - Workload dependent

CICS TS and CICS VR are required when using VSAM replication for A-A workloads.

5.7 IBM GDPS Active/Active monitor processing

IBM GDPS has a built-in monitor that runs every five minutes to check the status of the environment and alert you to any out-of-line situations it discovers. There are no external controls for you to customize or set up to enable the monitor, and it cannot be turned off. The monitor runs in both GDPS Controllers.

The following actions are carried out during the GDPS monitoring process:

- Ensures connectivity to, and ensures that the other GDPS Controller is active. If the other controller is not active, then an SDF alert is issued.
- Checks to see whether System Automation is active. If not active, the process tries again a number of times. If still not active, the process stops with an error message and SDF alert.

If System Automation is active, GDPS checks the following areas:

- Connectivity is active to all defined production systems.
  - If systems expected to be active are found not to have connectivity, an SDF alert is generated.
- Checks that the production system is loaded where it ought to be and updates its information if the system is found to be, for example, running in a different partition.
- Checks that defined workloads are running in both the active and standby sysplexes.
  - If workloads are found to be not running in both sites (which is the expected state), then an SDF alert is generated.

Monitors the Geographically Dispersed Parallel Sysplex (HMC) automation interface:

- If GDPS Monitor1 detects that the BCP Internal Interface is not operational, it attempts to reinitialize the interface.
- If GDPS/PPRC co-operation is being used, the currently selected load table entry in GDPS/PPRC and GDPS Active/Active for each system is checked and if they are not the same, an alert message is issued.

The monitor runs the GDPS message health check. This checks to determine whether the messages GDPS relies upon for automation are defined correctly and if there is any user-written automation in place that might affect delivery of the message to GDPS.

The processing involves the following phases:

- Check the MPF list to ensure that the messages are passed to automation.
- Check the message automation table to see whether there are any "user" entries for the messages required by GDPS, and, if so, whether they are located before the inclusion of the GDPS-supplied entries in the automation table concatenation.
- Check to see whether the messages are handled by NetView MRT processing.

If a problem is discovered, then an SDF alert and message are issued for each message found to have a problem.

5.8 IBM GDPS Active/Active Monitor processing during a workload or site failure

In addition to the regular monitor processing on a five-minute interval, GDPS runs a monitor when a workload failure or site failure incident is detected.

In this scenario, when the monitor runs, it checks for the following exceptions:

- Is the HMC LAN functional in the site containing the standby workload?
- Is there WAN connectivity to the site containing the standby workload?
- Are the standby workload servers functional from a Lifeline perspective so a switch of workload routing is possible?
- Are the active or standby workload servers in a degraded state, from a Lifeline perspective?

If the monitor finds no exceptions, then the workload or site switch is not considered to be affected by the status of the systems in the standby site. If problems are found, this triggers a message as part of the switch prompt, rather than a message that indicates that the switch can occur.

5.9 IBM Tivoli NetView for z/OS and IBM Tivoli NetView Monitoring for GDPS

The IBM NetView monitoring capabilities help you create an automated, cross-platform disaster recovery solution at virtually any distance between a primary site and a recovery site. They provide these enhanced capabilities:

- Automation of events and process
- Monitoring of workload status
- Monitoring of the IBM Multi-site Workload Lifeline product
- Monitoring of replication products and other managed elements

The IBM NetView product in conjunction with the Tivoli NetView Monitoring for GDPS product are prerequisites for IBM GDPS Active/Active automation and management. In addition to being the operating environment for GDPS, the IBM NetView products provide monitoring capability, in conjunction with the NetView agent for the following additional functions:

- IBM Multi-site Workload Lifeline for z/OS
- IBM InfoSphere Data Replication for DB2 for z/OS
- IBM InfoSphere Data Replication for IMS for z/OS
- IBM InfoSphere Data Replication for VSAM for z/OS

5.9.1 IBM NetView Agent

The IBM Tivoli NetView for z/OS Enterprise Management Agent is used to pass information from the z/OS NetView environment to the Tivoli Enterprise Portal. This information is used to provide a view of your enterprise from which you can drill down to more closely examine components of each system being monitored. The IBM NetView agent requires IBM Tivoli Monitoring (see Chapter 5.3, “IBM Tivoli Monitoring” on page 50).

5.9.2 IBM GDPS Integration

IBM Tivoli NetView for z/OS provides the base for all IBM GDPS solutions and provides the following capabilities:

- Automation platform
- Capacity to build a state machine
- Communication between NetView programs
- Audit trail using the Consolidated Audit, NetView, and z/OS log (Canzlog)

IBM NetView for z/OS is also a major component of the IBM GDPS Active/Active Continuous Availability solution, which provides the following capabilities:

- Sampled and real-time monitoring capacity using the Tivoli Enterprise Portal and the 3270 command interface for the Multi-Site Workload Lifeline and replication products that make up the solution
- Failover capability for the Active/Active Enterprise Master NetView program
- Automation for all data collection and events

5.10 IBM OMEGAMON XE Family

IBM Tivoli OMEGAMON XE provides detailed monitoring and problem management for IBM System z and IBM zEnterprise® systems. This software is designed to improve visibility, usability, and performance.

5.10.1 Tivoli OMEGAMON XE on z/OS

Tivoli OMEGAMON XE on z/OS provides the following benefits:

- Helps improve problem resolution efficiency by requiring fewer steps to find a root cause performance impact in near real time, which helps increase availability.
- Provides an IBM 3270-based user interface capable of viewing the entire enterprise-wide environment from a single screen. This expansive enterprise view is designed to increase visibility, control, and automation.
- Simplifies installation, configuration, and maintenance using self-describing agents and parameter library methodology. With this feature, you can enhance IT productivity.
- Supports a redesigned IBM OMEGAMON architecture to provide cloud support throughout hybrid environments. This feature also helps reduce software costs and the need for mainframe resources.

Note: Additional products such as IBM Tivoli OMEGAMON XE on z/OS, IBM Tivoli OMEGAMON XE for DB2, IBM Tivoli OMEGAMON XE for CICS on z/OS, and IBM Tivoli OMEGAMON XE for IMS can optionally be deployed to provide specific monitoring of products that are part of the Active/Active sites solution.

5.11 IBM GDPS Active/Active web interface

The web interface is a browser-based interface designed to improve operator productivity. It provides the same functional capability as the 3270-based window, such as providing management capabilities for Remote Copy Management, Standard Actions, Sysplex Resource Management, and SDF Monitoring using simple point-and-click. In addition, users can open multiple windows to allow for continuous status monitoring, while performing other GDPS/PPRC management functions.

Note: The *only* user interface to GDPS Operator functions such as Standard Actions and planned action script execution is the GDPS web Interface, which is based on the NetView Web Application. There is no 3270 interface for GDPS functions in GDPS Active/Active.

The IBM GDPS Active/Active web-based graphical user interface, shown in Figure 5-2, has three sections:

- A menu bar on the left with links to the main IBM GDPS Active/Active options
- A window list on top allowing switching between multiple open frames
- An active task frame where the relevant information is displayed and activities are performed for a selected option

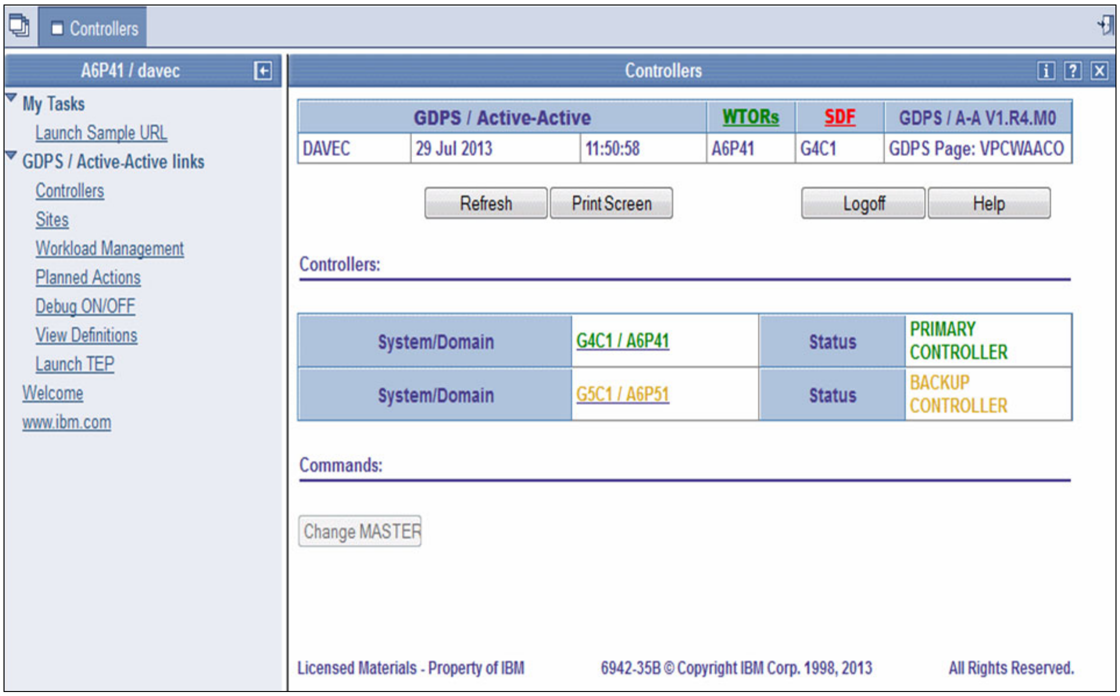


Figure 5-2 Initial window of GDPS user interface

5.11.1 Controllers windows and functions

When an operator accesses the GDPS Active/Active web interface, the initial window that is displayed is the Controllers window as shown in Figure 5-3 on page 60. This window identifies the Controller systems for this GDPS Active/Active environment. In this example, they are the systems named G4C1 (NetView Domain ID A6P41), which is the Primary Controller (or Master) system, and G5C1 (NetView Domain ID A6P51), which is the Backup Controller.

The top of the menu bar on the left shows that the operator is logged on to the Controller system with domain ID of A6P41, which is the Primary Controller.

In this position, the operator can only perform actions such as STOP, which is a graceful shutdown, LOAD or RESET the LPAR, and so on, against the other Controller. GDPS does not allow disruptive actions to be performed against the system that the operator is logged on to.

At the bottom of the frame, you see a disabled **Change MASTER** button. This button, when selectable (it is only selectable when you are logged on to the Backup Controller), allows you to make the current Backup Controller the new Master Controller. That is, it allows you to perform a Controller switch.

5.11.2 GDPS Standard Actions

Because the operator is normally logged on to the Primary Controller, the operator is only allowed to perform actions against the Backup Controller. When the Backup Controller is selected, the window shown in Figure 5-3 is displayed. In this window, you see that GDPS Standard Actions can be performed against the other Controller system, which in this case is the Backup Controller.

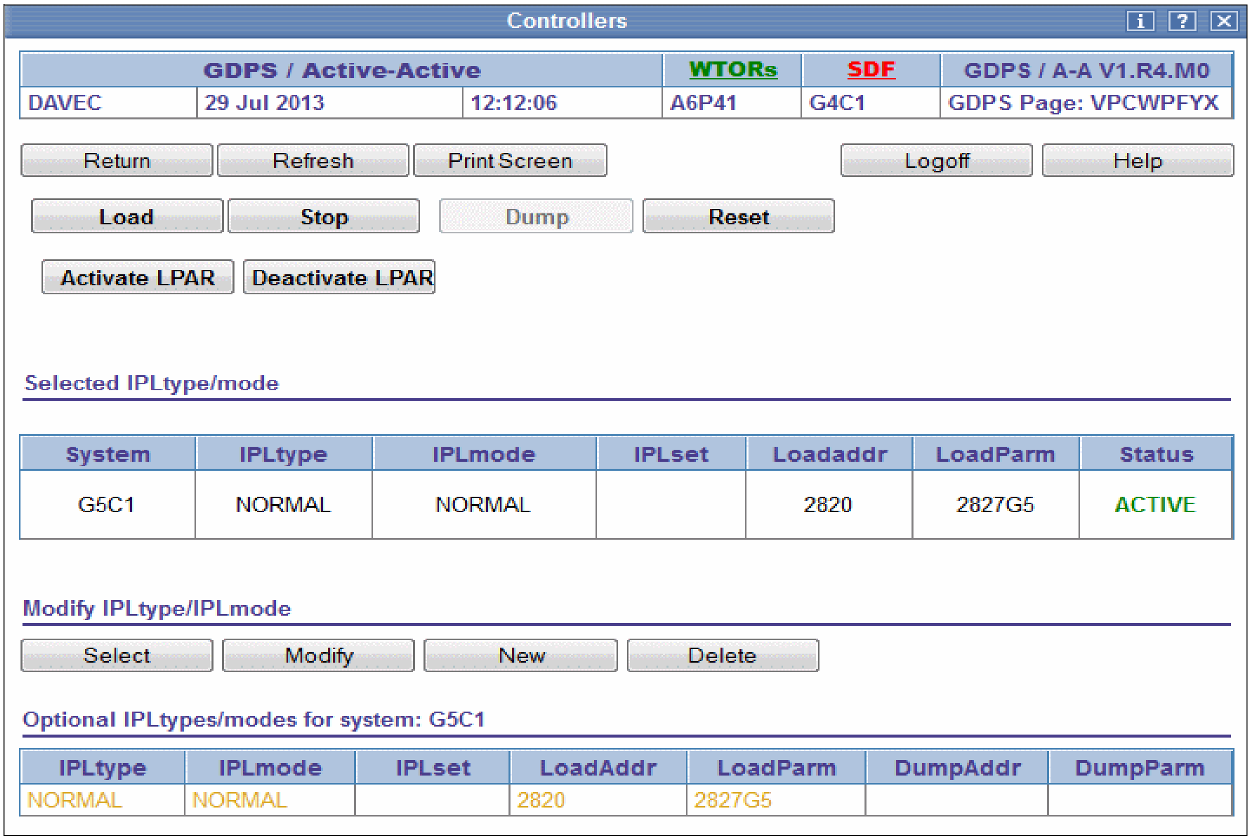


Figure 5-3 Standard actions window

Figure 5-3 shows the following GDPS Standard Actions that can be performed against the selected target system, available as buttons in the frame:

- LOAD
- STOP (graceful shutdown)
- RESET
- Activate LPAR
- Deactivate LPAR

Modification and selection of Load Address and Load Parameters to be used during a subsequent LOAD operation Most of the GDPS Standard Actions require actions to be carried out on the HMC. The interface between GDPS and the HMC is through the Base Control Program internal interface (BCPii). GDPS uses the BCPii interface provided by System Automation for z/OS.

When a specific Standard Action is selected by clicking the button for that action, there are further prompts and windows for operator action such as confirming that you really want to perform the operation. Although this example shows using GDPS Standard Actions to perform operations against the other Controller, in a GDPS Active/Active environment you use the same set of Standard Actions to operate against production systems in the environment.

If certain actions are performed as part of a compound workflow (such as planned shutdown of an entire site where multiple systems will be stopped, the LPARs for multiple systems RESET and Deactivated, and so on), then you will typically not use the web interface. Instead, you perform the same actions through the GDPS scripting interface. The GDPS *LOAD* and *RESET* Standard Actions (available in the Standard Actions window or the SYSPLEX script statement) allow specification of a *CLEAR* or *NOCLEAR* operand. This provides operational flexibility to accommodate customer procedures, eliminating the requirement to use the HMC to perform specific *LOAD* and *RESET* actions.

IBM GDPS Active/Active provides support for taking a stand-alone memory dump using the GDPS Standard Actions window. The stand-alone memory dump can be used against any System z operating system defined to GDPS. Customers using GDPS facilities to perform HMC actions no longer need to use the HMC for taking stand-alone memory dumps.

5.11.3 Sites windows and functions

The Sites task, when selected from the menu on the left side on every web interface frame, allows you to perform GDPS Standard Actions against the production systems within your GDPS Active/Active environment. An example of the window that is displayed when you select this task is shown in Figure 5-4. The window provides a view of the status of the systems within the sites. The upper window in the display shows normal status, with all systems active. The lower window gives a clear indication of a problem in Site G5, where neither of the two expected systems are active.

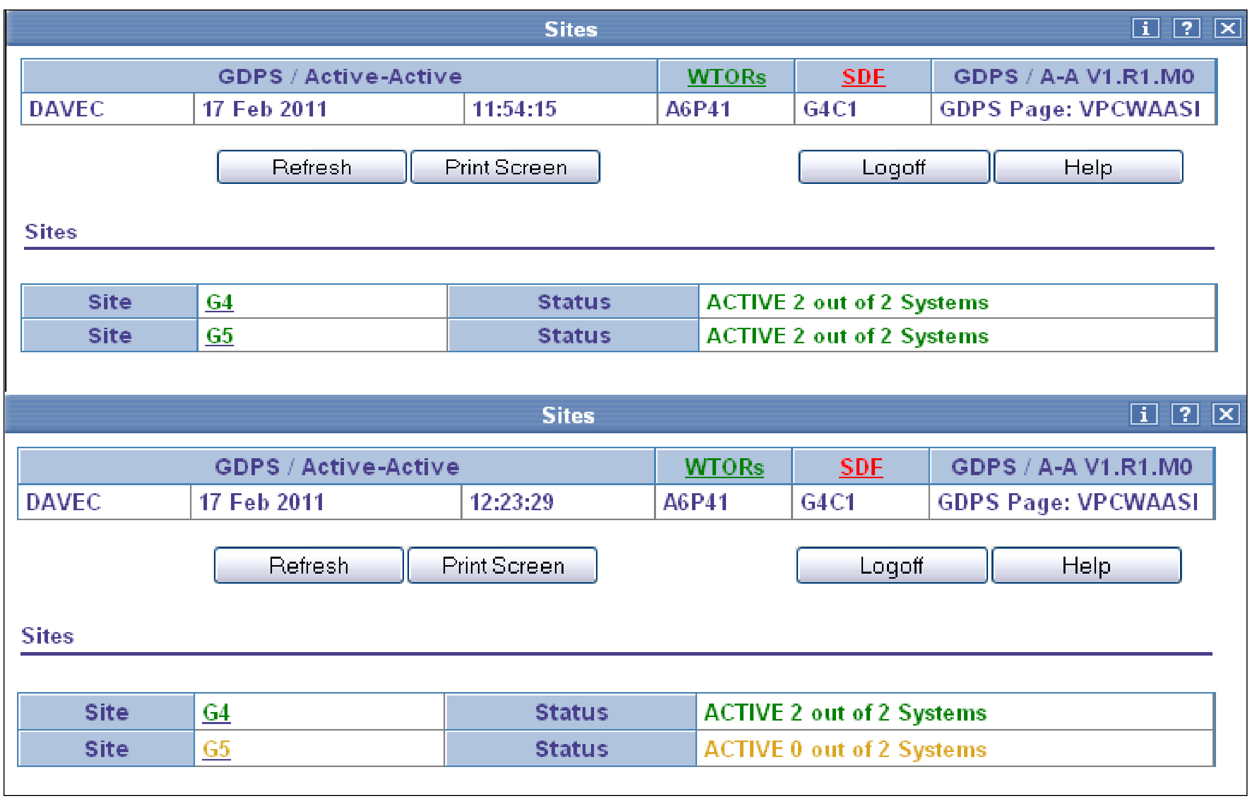


Figure 5-4 Sites window and functions

Essentially, apart from the standard header information, this window allows you to select which of the sites you want to interact with. You simply click the site name. Figure 5-5 shows the frame that is displayed when, in this example, G4 is selected.

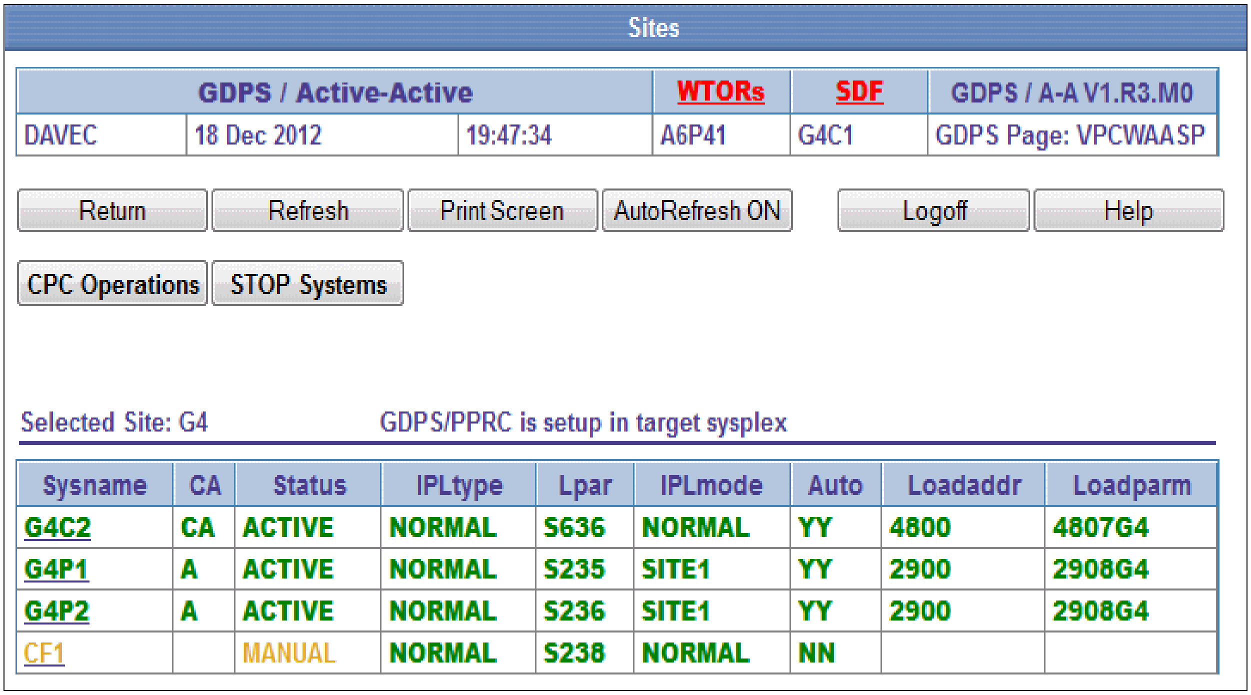


Figure 5-5 Sites window after site/sysplex G4 is selected

You can then select the specific system that you want to use as a target for a GDPS Standard Actions operation. Performing Standard Actions, such as STOP, LOAD, RESET, and so on, against a production system is identical to performing such actions against a Controller as shown on Figure 5-3 on page 60 and described on 5.11.2, “GDPS Standard Actions” on page 60.

5.11.4 Workload Management windows and functions

The Workload Management task, selected from the menu bar, displays the Workload Management window. An example of this window is shown in Figure 5-6. This window shows and provides an at-a-glance high-level status summary for all workloads, both updates and queries, that are defined for this GDPS environment.

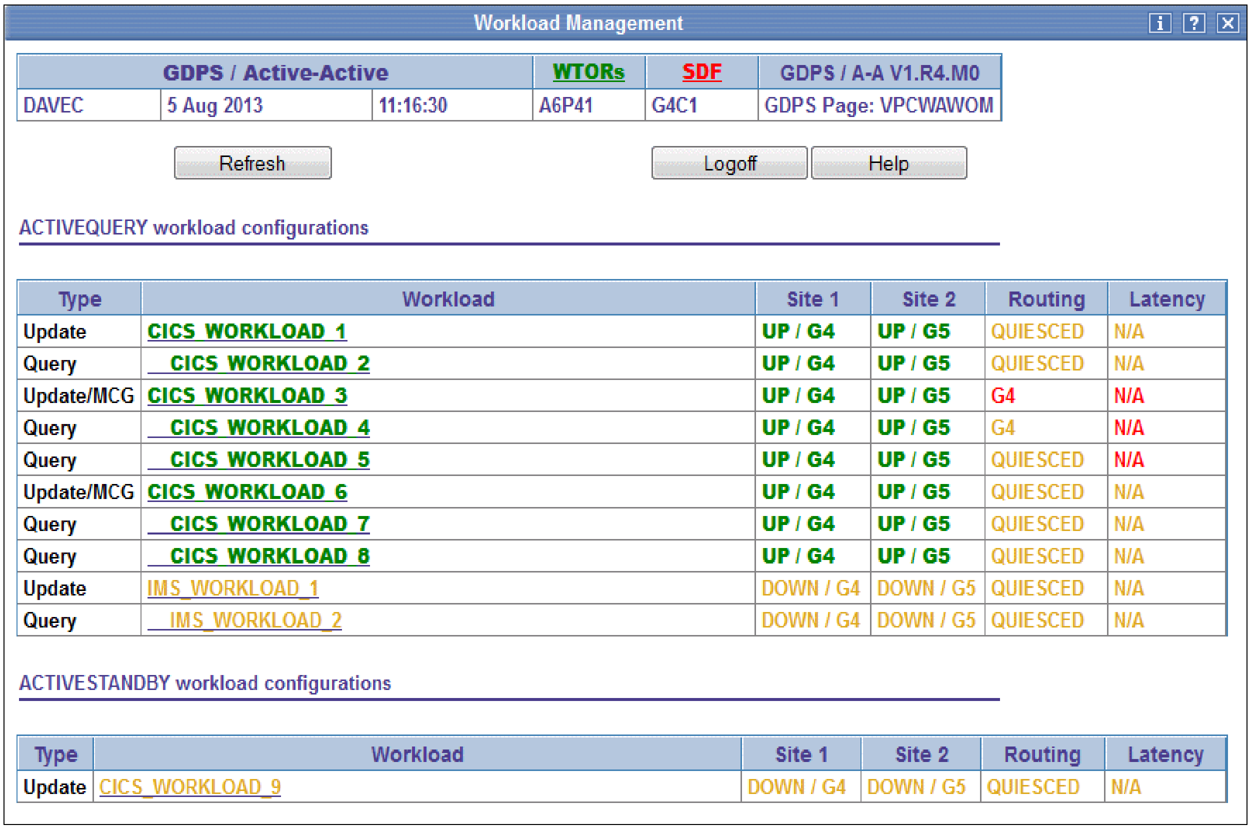


Figure 5-6 Workload Management window

The status that is shown in each of the sites is based on information from GDPS Monitoring and from System Automation running in the production systems in that site.

You can click any of the workload names to select the details window for that workload. An example of the Workload details window is shown in Figure 5-7.

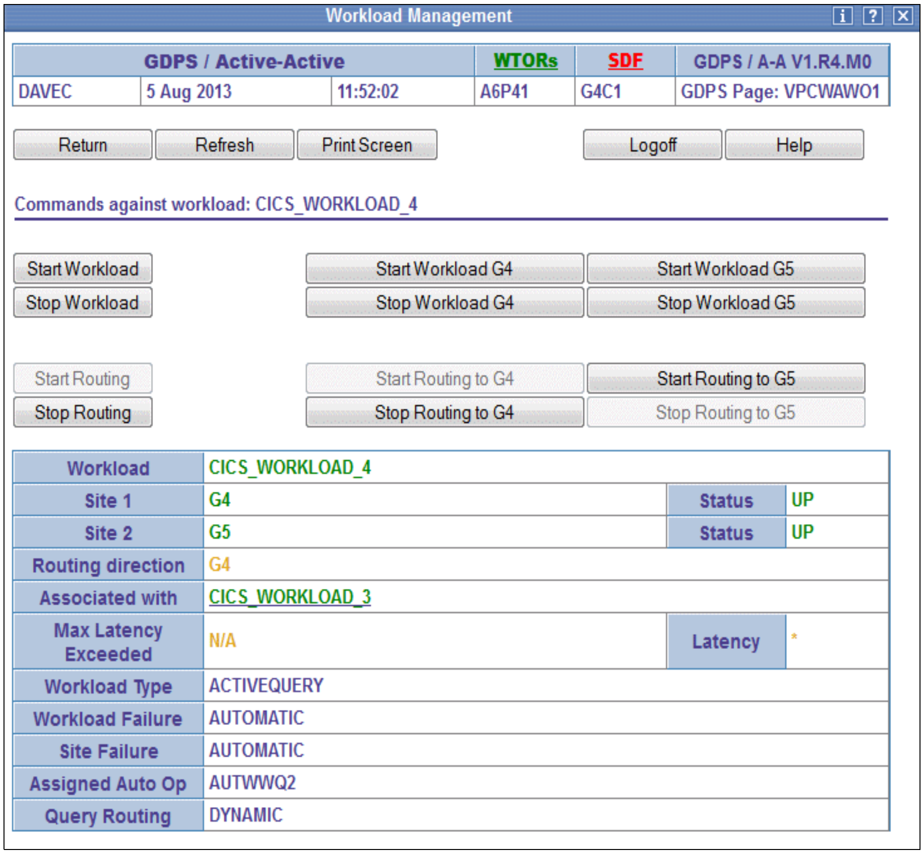


Figure 5-7 Workload details window

The Workload details window allows you to perform the operations against the selected workload such as Start/Stop of the workload or Start/Stop of routing for that workload to one site or the other.

In addition to these operations, the window provides further status details associated with the selected workload.

Similar to Standard Actions, there are GDPS script statements that perform these same operations. Typically, a script is used to perform these actions and Standard Actions for a compound/complex scenario such as an entire site shutdown.

5.11.5 Planned Actions windows and functions

IBM GDPS Active/Active Planned Actions are initiated from the Planned Actions window within the GDPS user interface. When you select the Planned Actions task from the menu bar, you see a Planned Actions window similar to that shown in Figure 5-8.

Planned Actions allows you to view and run scripts for planned scenarios such as site shutdown, site start, or CEC shutdown and start. You are presented with a list of scripts that you have already coded, anticipating a given planned scenario[1]. Along with the name of the script, you are also presented with a comment that describes what a specific script is intended for. You can then select a script for viewing and execution on this window.

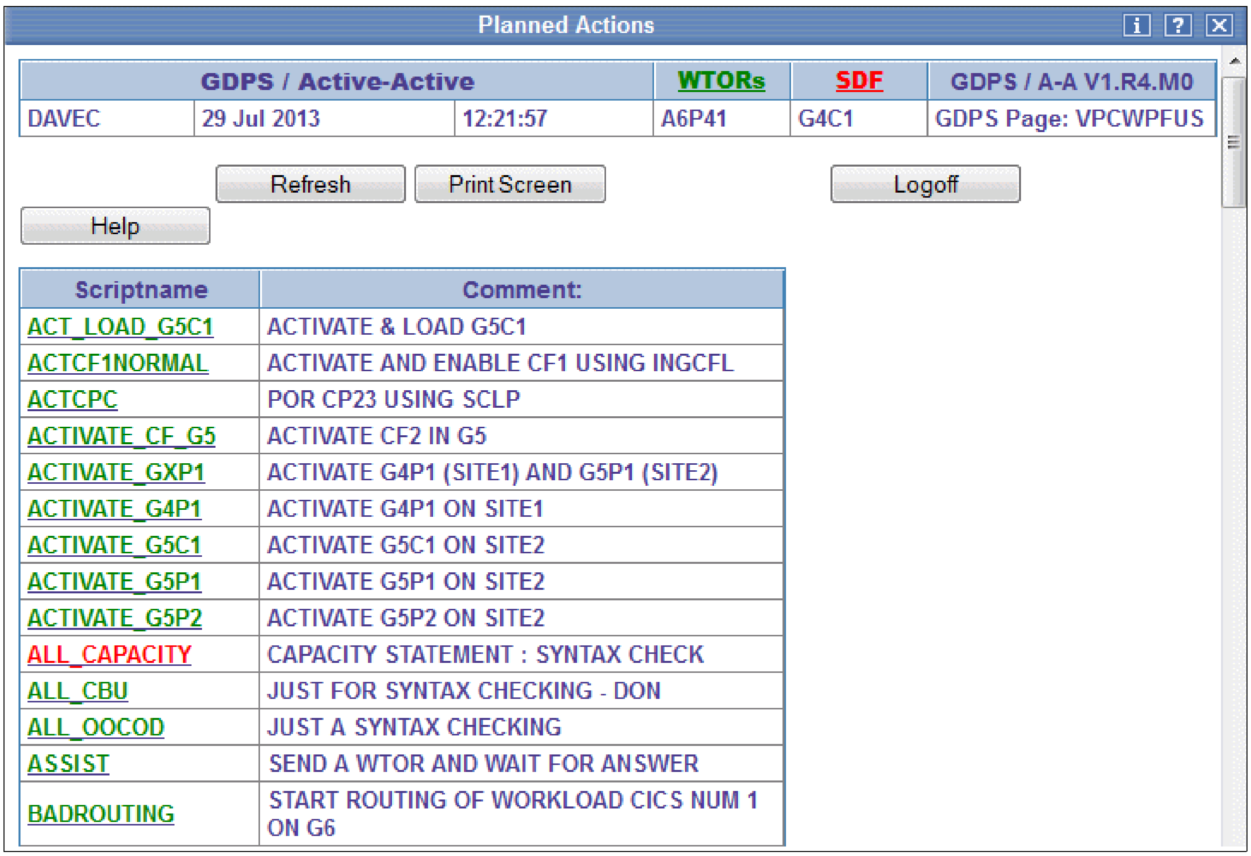


Figure 5-8 Sample Planned Actions Frame

[1] For example scripts, see Appendix E in the *GDPS/Active-Active 1.4 Planning and Implementation Guide*, ZG24-1767-02

When you select a script from the list, you are presented with a window that displays the actual script content as shown in Figure 5-9. On this window, after you view the actual script content, you can run it. If you choose not to run the script, you can click **Return**.

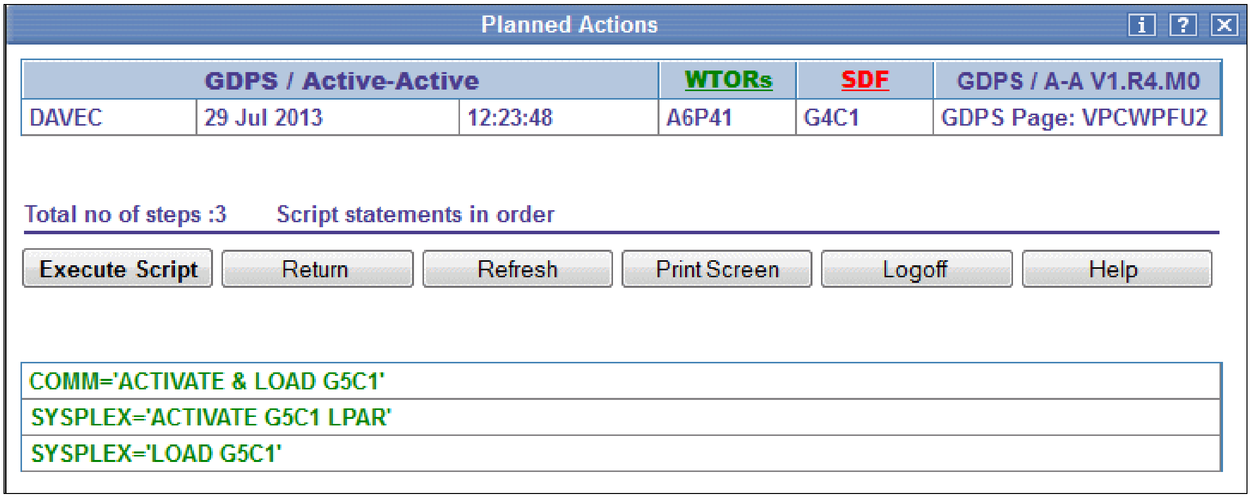


Figure 5-9 Planned Actions Script example

5.11.6 Launching Tivoli Enterprise Portal from the GDPS web interface

You can use the Launch TEP link on the menu bar to view information available through the Tivoli Enterprise Portal. Tivoli Enterprise Portal provides views and levels of detail pertaining to the GDPS Active/Active environment other than what is available through the GDPS web interface. When investigating a problem (for example, due to an alert that is raised in GDPS), it can be useful to launch Tivoli Enterprise Portal directly from the GDPS web interface and drill down into the views of your environment that are available through Tivoli Enterprise Portal.

After Tivoli Enterprise Portal is launched, you can drill down to GDPS Active/Active windows to view details pertaining to the IBM GDPS Active/Active Load Balancers, Replication Servers, Workload Lifeline Advisors, and Workloads.

Figure 5-10 shows the Tivoli Enterprise Portal views of Replication Servers. The bottom pane of the window contains summary information for the replicator associated with each of the workloads managed by IBM GDPS Active/Active. The graph provides details about the breakdown of latency for each of the replicators in the environment.

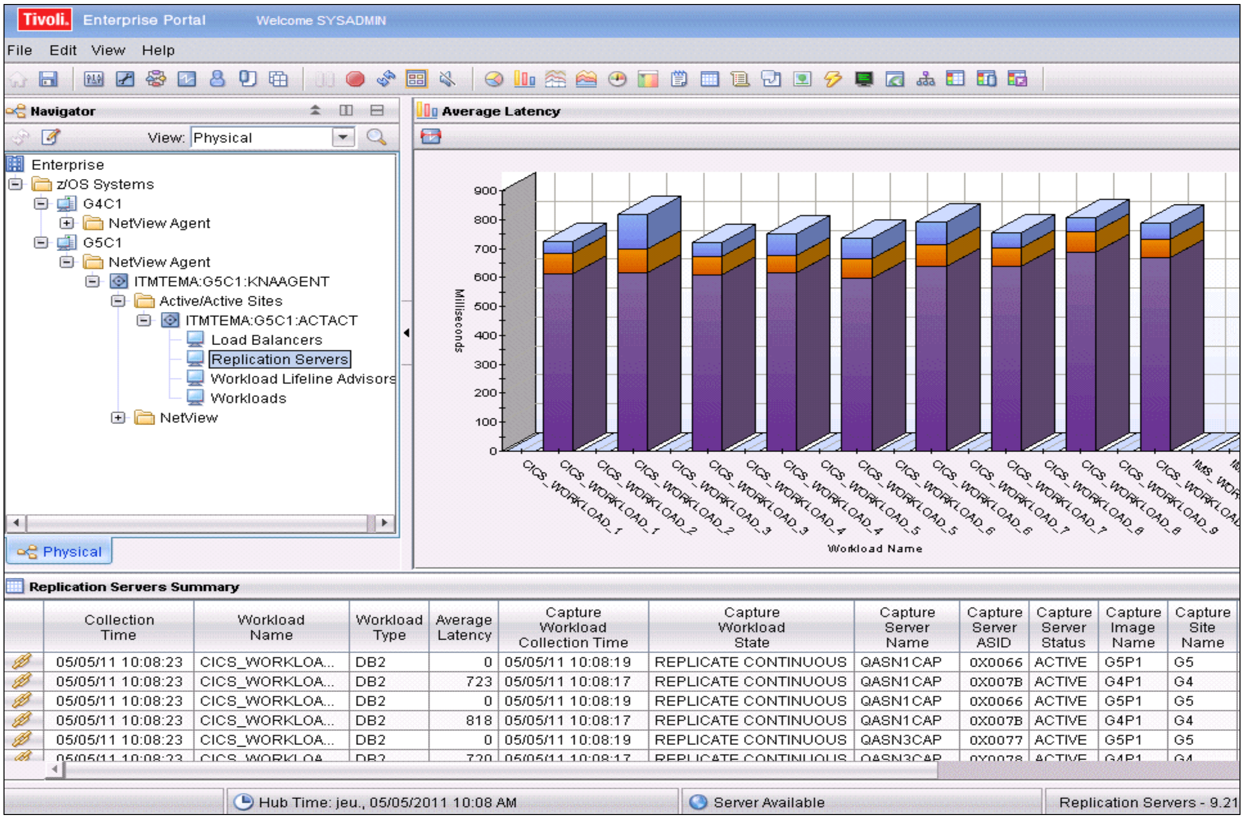


Figure 5-10 Launch Tivoli Enterprise Portal - Replication Servers window

The Tivoli Enterprise Portal, in addition to providing a monitoring interface to the overall solution, allows you to set up alerts for specific conditions such as the replication latency exceeding a certain threshold. The workload-related workspaces can also quickly show such things as the number of servers active in both sites and where the routing is active to. This information can be useful to correlate against that shown in the GDPS web interface to confirm the status of any particular resources.

5.11.7 Other web interface options

Other options available to the operator through the web interface and are discussed in *GDPS/Active-Active 1.4 Planning and Implementation Guide*, ZG24-1767-02:

- Status Display Facility (SDF)

  SDF is the focal point for monitoring the GDPS Active/Active environment. A link to SDF is available on the top portion of every web interface frame. For more information about SDF, see 5.11.8, “GDPS Active/Active monitoring and alerting” on page 68.

- Write to operator with reply (WTOR)

  Similar to SDF, the WTOR function is selectable on the top portion of every web interface frame. The WTOR function opens a new window to display any WTOR messages that are outstanding and provides the option to reply to any selected message.

- Turning Debug ON / OFF

  As a NetView-based automation application, IBM GDPS Active/Active uses the NetView log as the main repository for information logging. In addition to the NetView log, selected critical GDPS messages are also sent to the z/OS system log.

  The GDPS Debug facility enables logging in the NetView log, providing more detailed trace entries pertaining to the operations that GDPS is performing. If you encounter a problem, you might want to collect debug information for problem determination purposes. If directed by IBM support, you might need to trace execution of specific modules. The GDPS debug facility also allows you to select the modules to be traced. The Debug frame is presented when you select **Debug On/Off** on the menu bar.

- View definitions

  The view definitions option, also selected through the menu bar, allows you to view the various definitions and options related to GDPS that are in effect. The bulk of the GDPS definitions are made in the System Automation policy database. If you modify some of these definitions or for any other reason want to check what definitions GDPS is using, you can use this facility.

5.11.8 GDPS Active/Active monitoring and alerting

The GDPS Active/Active Controller systems perform periodic monitoring of resources and conditions that are critical or important for the healthy operation of the environment. For example, GDPS checks whether the workloads that are managed by GDPS are running on both the active and the standby sysplexes, whether the BCPii is functional, whether the connectivity from the Controller to the production systems is intact, current replication latency, and so on. If GDPS discovers any exception situations, it issues SDF alerts.

In addition to any exception condition that might be discovered through monitoring, IBM GDPS Active/Active also captures messages from other components in the environment that can be indicative of a problem and raises alerts.

The SDF is a facility that is provided by System Automation and is used as the primary status feedback mechanism for IBM GDPS Active/Active. SDF can be viewed by selecting the SDF link, which is available on the top portion of every IBM GDPS Active/Active web interface window.

So long as all is well and there are no alerts indicative of a potential issue with the environment, the SDF link on the GDPS web interface windows is displayed in green. If any SDF entry is displayed in a color other than green, it is indicative that there is an alert. For example, pink is used to report a problem that is not catastrophic, and red is used for a serious exception condition.

No matter which window operators view, they can click SDF on the top portion of the window to view the SDF window and check the alert.

In addition to using SDF to monitor the GDPS status, when Standard Actions or scripts are running, each step is displayed in the trace portion of the SDF window. This allows the operator to follow script execution.

The SDF view, when selected, is opened in a new window of your browser as shown in Figure 5-11.

The following areas are displayed in the window:

- A section showing Site-related alerts, split into two categories:
  - Workload-related alerts
  - Site-related or System-related alerts
- A section displays alerts relating to the GDPS Controllers.
- A section displaying trace entries.

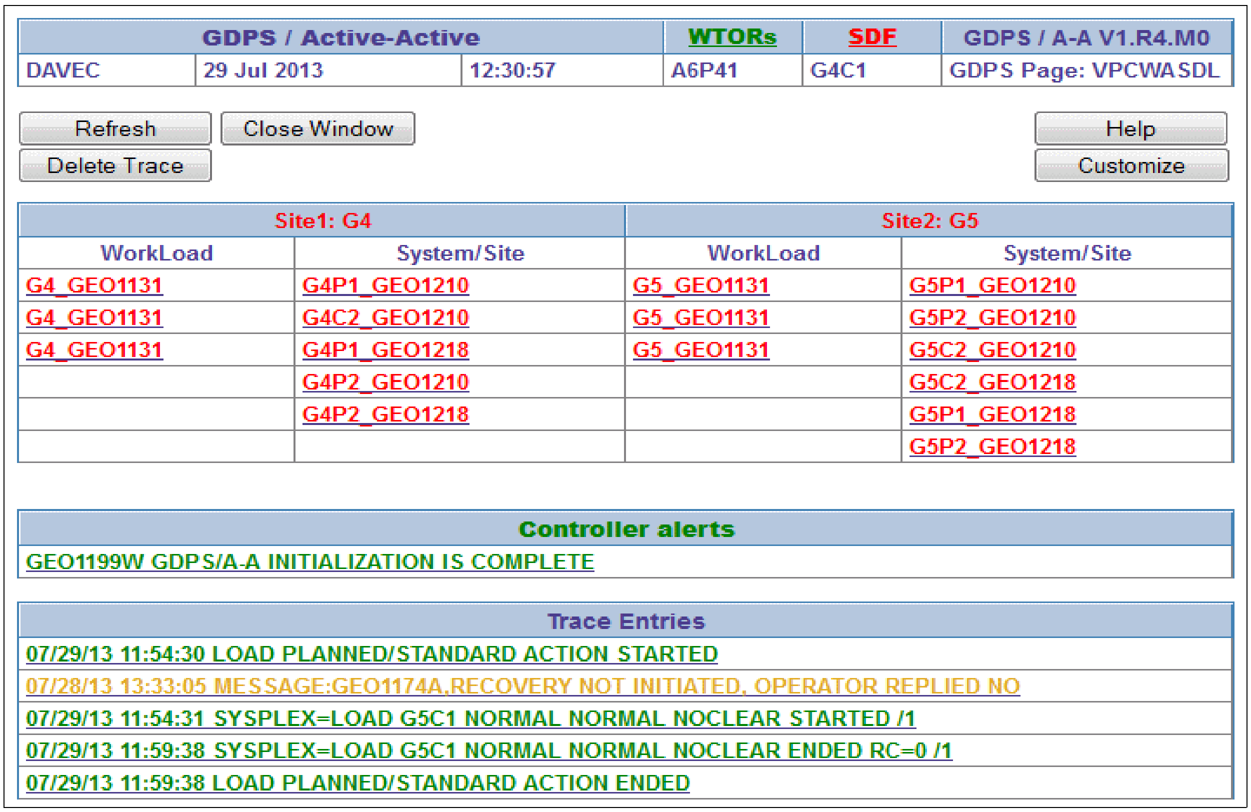


Figure 5-11 SDF view

For more information about any alert, simply click the alert. A new window is displayed with the details for the selected alert. For example, if you click the first alert on the upper left (G4_GEO1131 in red) in Figure 5-11 on page 69, you are presented with the window shown in Figure 5-12.

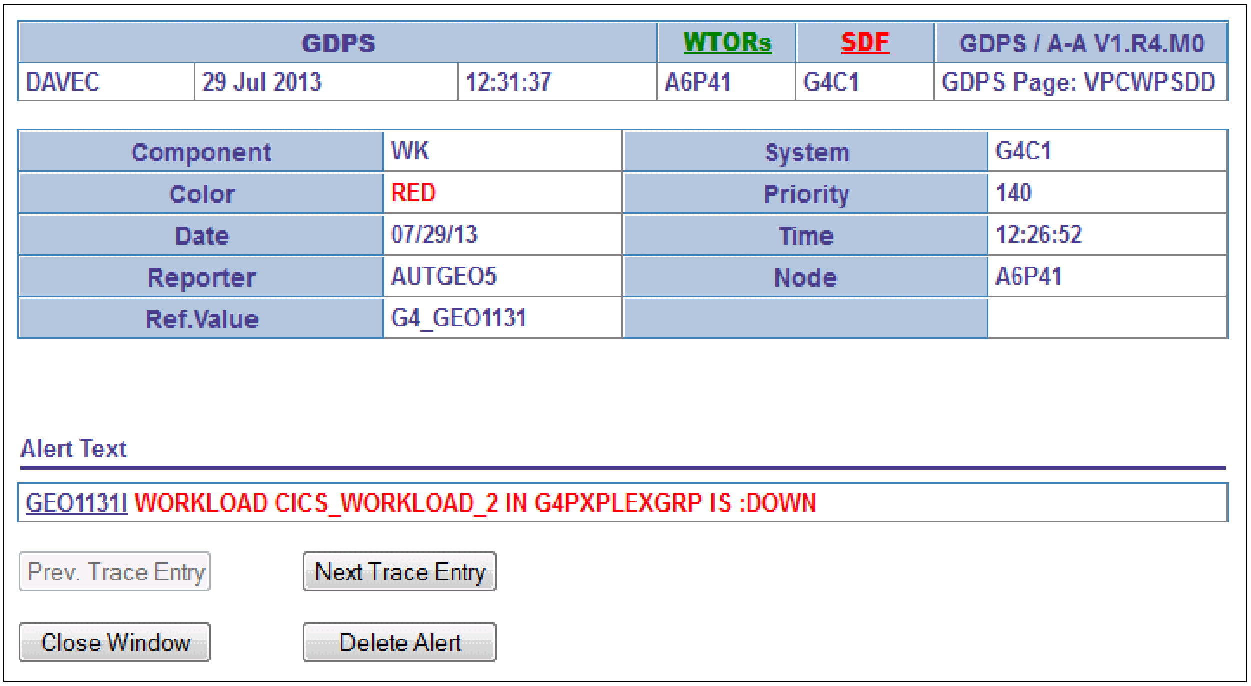


Figure 5-12 SDF Alert detail display

6

Planning considerations

This chapter describes the planning considerations pertaining to the Geographically Dispersed Parallel Sysplex (GDPS) Active/Active solution. This chapter includes the following sections:

- Prerequisites for each component
- Decision Point
- Checklist
- Hints and Tips

6.1 Prerequisites for each component

This section describes the main considerations, and product prerequisites and corequisites, for GDPS Active/Active solution planning.

6.1.1 Hardware prerequisites and corequisites

There is no specific hardware requirement from a z/OS perspective. Hardware must be capable of running the minimum prerequisite software levels for GDPS Active/Active as listed in 6.1.2, "Software prerequisites and corequisites".

There is a network prerequisite. Server/Application State Protocol (SASP) enabled network routers are required by the GDPS Active/Active solution to work as first tier load balancers. This protocol, described in RFC 4678, enables GDPS (through IBM Multi-site Workload Lifeline for z/OS) to instruct the router to direct transactions to one site or the other.

For more information about SASP, see 6.1.3, "Server/Application State Protocol (SASP)-compliant routing" on page 74.

The following are examples of SASP-compliant switches/routers:

- Cisco Catalyst 6500 Series Switch Content Switching Module
- F5 Big IP Switch
- Citrix NetScaler Appliance
- Radware Alteon Application Switch (Nortel appliance line)

6.1.2 Software prerequisites and corequisites

GDPS Active/Active solution consists of a number of software products working together to provide the necessary functions. If you have systems in the same Parallel Sysplex as the systems running Active/Active workloads, generally use GDPS to manage these systems. You need to have both NetView and System Automation for z/OS installed on these systems.

Table 6-1 on page 73 provides the product requirements, and lists where these products run in a GDPS Active/Active environment.

Table 6-1 Prerequisite Software Matrix

Prerequisite software	GDPS Controllers	Active/Active systems	Non-Active/Active systems
Operating system			
z/OS 1.13	YES	YES	YES
Restriction: GDPS Active/Active does not support z/OS images running under IBM z/VM®.			
Middleware			
DB2 for z/OS V9 or higher	NO	YES Workload-dependent	As required
IMS V11	NO	YES Workload-dependent	As required
WebSphere MQ V7.0.1	NO	See Note 1	As required
Note 1: WebSphere MQ is only required for DB2 data replication.			
CICS Transaction Server for z/OS V5.1	NO	YES Workload-dependent See Note 2	As required
CICS VSAM Recovery for z/OS V5.1	NO	YES Workload-dependent See Note 2	As required
Note 2: CICS TS and CICS VR are required when using VSAM replication for the Active/Active workloads.			
Replication			
InfoSphere Data Replication for DB2 for z/OS V10.2.1	NO	YES Workload-dependent	As required See Note 3
InfoSphere Data Replication for IMS for z/OS V11.1	NO	YES Workload-dependent	As required See Note 3
InfoSphere Data Replication for VSAM for z/OS V11.1	NO	YES Workload-dependent	As required See Note 3
Note 3: Non-Active/Active systems and their workloads can, if required, use Replication Server instances, but not in the same instances as the Active/Active workloads.			
Management and Monitoring			
GDPS Active/Active V1.4	YES	YES See Note 4	NO
Note 4: GDPS Active/Active satellite code needs to be installed on the production systems where the Active/Active workloads run.			
IBM Tivoli NetView Monitoring for GDPS V6.2	YES	YES	NO
IBM Tivoli NetView for z/OS V6.2	YES	YES	YES

Prerequisite software	GDPS Controllers	Active/Active systems	Non-Active/Active systems
IBM Tivoli System Automation for z/OS V3.3 (+SPE APARs) or V3.4	YES	YES	YES
IBM Multi-site Workload Lifeline for z/OS V2.0	YES	YES	NO
IBM Tivoli Monitoring V6.3 Fix Pack 1 or higher	YES See Note 5	NO See Note 6	NO
Note 5: For more information about the possible options of where to run the Tivoli Enterprise Monitoring Server and the Tivoli Enterprise Portal Server, see *Installation: Configuring GDPS Active/Active Continuous Availability Solution*, SC14-7477.			
Note 6: Optional IBM Tivoli Monitoring might be required on production systems for reasons other than GDPS Active/Active.			
IBM Tivoli Management Services for z/OS V6.3	YES See Note 7	NO	NO
Note 7: IBM Tivoli Management Services for z//OS is available separately, or can be included with the OMEGAMON products.			
Optional Monitoring products			
Additional products such as Tivoli OMEGAMON XE on z/OS, Tivoli OMEGAMON XE for DB2, and Tivoli OMEGAMON XE for IMS can optionally be deployed to provide specific monitoring of products that are part of the Active/Active sites solution.			

6.1.3 Server/Application State Protocol (SASP)-compliant routing

SASP-enabled network routers are required by the GDPS Active/Active solution to work as load balancers. This capability, described in RFC 4678, enables GDPS (through IBM Multi-site Workload Lifeline for z/OS) to instruct the router where to direct the transactions. IBM Multi-site Workload Lifeline for z/OS defines two tiers of load balancing. The first-tier load balancer determines which site to route a new workload request to. The second-tier load balancer determines which server application instance within the sysplex to route a workload request to.

GDPS Active/Active requires that the first-tier load balancer is a SASP-compliant router. You can use Sysplex Distributor as the second-tier load balancer for workload distribution and workload balancing within the sysplex. In this case, no routing recommendations are provided by IBM Multi-site Workload Lifeline for z/OS.

6.1.4 Network Connectivity and bandwidth considerations

The WAN connections and the Hardware Management Console (HMC) LAN connections should be independent. If both WAN and HMC LAN connections share infrastructure, then the failure of one causes both communications paths to be unavailable. This situation can result in GDPS not being able to accurately assess and report the status of the environment.

The WAN is used by software replication to copy the data updates between sites. The WAN needs to provide the required bandwidth for software replication.

6.1.5 NetView Web Application requirements

The GDPS Active/Active user interface is provided through the NetView Web Application. A 3270-based user interface is not supported. This requires a server to host the NetView Web Application. The application can run under the Windows, AIX, or Linux operating systems. Details of the supporting server platforms, operating systems, and web browsers can be found in the readme file `znetview_webapp_readme_en.htm` in the `drive:/readmes` directory on the NetView V6R2 DVD, or in the `netview_installation_dir/doc` directory.

You should also have at least one NetView Web Application instance in each of your sites to provide high availability in case that one of the servers become unavailable.

6.1.6 Base Control Program internal interface (BCPii) considerations

BCPii is an internal HMC interface that is supported by System Automation. GDPS uses this interface through System Automation. This interface allows GDPS to communicate directly with the hardware for HMC automation functions, such as LOAD, ACTIVATE, and RESET.

BCPii supports IBM System z9® and higher hardware, and connections to HMC and Support Elements (SEs). Specific processor microcode levels are required, and prerequisite SE/HMC customization tasks that must be performed. For more information, see *System Automation for z/OS: Planning and Installation*, SC34-2751.

6.1.7 Software replication considerations

Software-based replication supports DB2, IMS, and VSAM data. The following are some of the many planning considerations for establishing a working software replication environment for your workloads:

- What production data needs to be replicated?
- How to handle failures in the underlying replication infrastructure
- Toleration and compensation of lost data following an unplanned workload or site failure
- How to resolve data conflicts after an unplanned outage
- How to establish a replication environment

For more information about the considerations of software replication, see *InfoSphere Data Replication for DB2 for z/OS and WebSphere Message Queue for z/OS: Performance Lessons*, REDP-4947, *IBM InfoSphere Data Replication for IMS for z/OS*, SC19-4174-00, and *IBM InfoSphere Data Replication for VSAM for z/OS*, SC19-4177-00.

From an infrastructure perspective, one common consideration for all software replication products is that of cross-site network bandwidth. Insufficient bandwidth can lead to an increase in the latency, resulting in an increased RPO, and can result in congestion in the replication components. IBM services are available to help you to plan your bandwidth requirements.

A naming convention is enforced by GDPS to tie the data replication to a specific workload. For DB2 data, the name of the queue map, as defined in DB2 replication, for a workload must match the workload name as defined to GDPS. Similarly, for IMS and VSAM data, the name of the subscription for a workload, as defined in IMS or VSAM replication, must match the workload name as defined to GDPS.

For some workloads, single capture and apply engines might not be sufficient to provide the throughput needed to copy all the data from the active site to the standby site. In this case, you need to use multiple consistency group support. This is at the workload level. GDPS supports up to 20 consistency groups (CGs) for each workload.

Currently, only DB2 replication provides multiple consistency group (MCG) support. With MCG support, when replicating data across multiple consistency groups, transactions that change tables assigned to different consistency groups are broken up and replayed at the target as independent partial transactions. Replication then operates with eventual consistency, meaning that transaction consistency is guaranteed only when all changes are replicated to the target site up to a common point-in-time.

When using MCG-mode for an update workload, if you have any associated query workloads running in the standby site, it can potentially return inconsistent results. Eventual transaction consistency is suitable for many read-only applications that can use the data if it is not stale beyond a certain threshold (set by policy in DB2 replication). You can consider defining the data to be required into one consistency group to eliminate the inconsistency results.

6.1.8 Sysplex configuration

The GDPS Active/Active solution requires a configuration of two Parallel Sysplex environments running Active/Active workloads, and two separate GDPS Controller systems. The Parallel Sysplex environments and the Controller systems must be assigned, one to each site.

GDPS Controller requirements

The two GDPS Active/Active Controllers must be set up as independent monoplexes. They are used to coordinate actions in the overall GDPS Active/Active environment. No Active/Active workload runs on the Controllers.

GDPS Controllers require network access to all systems in your GDPS Active/Active environment because communications between the systems and sites is through the network. This includes both WAN and HMC LAN network communication. You need to ensure that you have independent network access to your Controllers. This configuration means that even if the production sysplex in that site is unavailable, you can still operate the GDPS Active/Active environment.

You must ensure that sufficient write to operator (WTO) and write to operator with reply (WTOR) buffers are provided on the Controller systems to enable GDPS to operate correctly. When your Controllers are set up as monoplexes, the default value for RLIM, which defines the number of WTOR buffers, is 10. This number should be increased based on the size and complexity of the environment GDPS Active/Active is managing.

Active/Active Sysplex requirements

You have a choice to create new Parallel Sysplex environments for Active/Active workloads, or you can have Active/Active workloads and traditional workloads co-existing within the same Parallel Sysplex. Regardless which option you choose to deploy, you must consider the following considerations:

- Capacity considerations
- Time synchronization considerations

Capacity considerations

If all of your Active/Active workloads are running in one Parallel Sysplex, applying the updated data to the standby Parallel Sysplex, where no transaction processing is performed, you need to provide the capacity that your standby sysplex needs to do this. You also must provide enough capacity if the standby sysplex become fully active during a planned or unplanned switch.

You can consider the use of one of the IBM System z Capacity on Demand offerings, which include Capacity Backup (CBU), On/Off Capacity on Demand (OOCoD), and Capacity for Planned Events (CPE). GDPS provides automation for activating and bringing online the resources made available through these offers.

Time synchronization considerations

There is no requirement for the Active/Active Parallel Sysplexes to be in the same Server Time Protocol (STP) Coordinated Timing Network (CTN), because doing so would significantly limit the distance between the two sites to that supported by STP, which is 200 KM fiber distance with supported dense wavelength division multiplexing (DWDM).

However, from a replication standpoint, to ensure that latency between the two sites can be effectively calculated, the two sites should be as time coordinated as possible. For example, you can consider having the STP CTN in each site access an external time source such as a Network Time Protocol (NTP) time server.

6.2 Decision Point

This sections covers the decisions that need be made during the planning of a GDPS Active/Active solution.

6.2.1 Business decision

The GDPS Active/Active solution brings great value to Continuous Availability. It will dramatically reduce the planned outage window. The switch only takes several minutes. It also gives you another choice to handle unplanned event. You can immediately switch the workload to the standby site, and then fallback the changes in active site. Before it, you might have to spend a lot of time on problem determination and then trying the actions one by one. The challenge of existing emergency handling is not only having a long outage, but also that that outage window is hard to predict.

When GDPS Active/Active brings you to a higher level of Continuous Availability, it does need the resources to fulfill that function. You will need another SYSPELX in another site. You also need extra CPU to run the standby SYSPLEX and software-based replication. You will need new software products to support GDPS Active/Active function. A business decision needs to be made after you weigh the investment and the gain on the dramatic reduction of planned and unplanned outage.

6.2.2 Identify the workload

When you start the planning for GDPS Active/Active solution, you must understand your workload and the definition of Active/Active workload in GDPS Active/Active solution.

When describing workload, it is usually separated into online workload and batch workload. For online workload, you can further divide it by line of business. Active/Active workload has more strict definitions.

An Active/Active workload is a business-related definition. It is the aggregation of these items:

- Software: User-written applications (for example, a COBOL program) and the middle ware runtime environment (such as CICS region, InfoSphere Replication servers, and DB2 subsystems).
- Data: A set of related objects that must have transactional consistency maintained and optionally referential integrity constraints preserved (such as DB2 Tables, VSAM files, and IMS databases).
- Network connectivity: One or more TCP/IP addresses or host names and ports (for example, 10.10.10.1:80).

This definition is intended to preserve the transaction consistency of the data and make sure you can update data from one site only. Otherwise, you can end up with stranded data, and both versions will not be usable. For more information about how to link the Active/Active workload with software-based replication, see "IIDR for DB2 and GDPS Active/Active" on page 28.

To better understand the Active/Active workload, the rest of this section provides some examples.

Assumption

A banking environment normally has several applications with isolated data in the same SYSPLEX. These examples assume that a bank has two kinds of applications: Credit card applications and core banking applications, which handles the rest of the business outside of credit cards. Each application has its own data.

Scenario 1

In this first scenario, assume that the two applications are completely isolated from data and business logic. Assume the following system layout: Two applications use one DB2 data sharing group. DB2 tables set A supports a credit card application and DB2 tables set B supports the core banking application. The two applications can share the CICSPLEX, but use two sets of the terminal-owning region (TOR) and application-owning region (AOR). TOR and AOR set 1 receive the credit card workload, at the same time TOR and AOR set 2 receive a core banking request. TOR set 1 and TOR set 2 are separated by different IP and port combinations.

When the two applications are isolated from data and network connectivity, you can easily identify two Active/Active workloads. One is for the credit card application and the other is for core banking.

To define the Active/Active workload for the credit card application, GDPS Active/Active must be set up to replicate the CG for DB2 tables set A and the combination of IP and port for TOR set 1. For the core banking workload, you need do the same, but it should be the replication CG for DB2 tables set B and the combination of IP and port for TOR set 2.

Scenario 2

In this second scenario, a user needs to transfer money from a bank account to make a credit card payment. The user can start a transaction, which would proceed from TOR and AOR set 2 to call a program in AOR set 1 to finish the money transfer between core banking and the credit card. In this case, the data in DB2 tables set A and DB2 tables set B are updated in the same unit of work (UOW). Both DB2 tables set A and DB2 table set B must be replicated to maintain the transaction consistency in a standby site. For this reason, ideally you would only define one Active/Active workload, which includes both credit card and core banking applications.

To define the Active/Active workload for both credit card and core banking, set up the replication for GDPS Active/Active consistency groups for both DB2 tables set A and DB2 tables set B, and the combination of IP and port for TOR set 1 and TOR set 2.

> **Note:** The GDPS Active/Active solution can only support batch workloads today. You can find more information about batch workloads in "Handling batch" on page 94

6.2.3 Active/Standby or Active/Query Configuration

After you identify the Active/Active workload, you must decide to enable it using either an Active/Standby or Active/Query configuration. In an Active/Standby configuration, you run the identified workload on the active site. You can only run the workload in the standby site after a workload switch. You need to enable the Active/Query configuration if you want to run some query workloads on both the active site and standby site. Doing that, you can reduce the performance impact to Active/Standby workloads in the active site and fully use the CPU resource on the standby site. However, make sure that the query workloads on the standby site can tolerate the latency of the replication.

For more information, see *GDPS Active/Active 1.4 Planning and Implementation Guide,* ZG24-1767-02.

> **Note:** The GDPS Active/Active terms of Active/Standby and Active/Query configuration refers to Active/Standby workloads or Active/Query workload, which are at the workload level, not the site level.

6.2.4 Single consistency groups or multiple?

Software replication products replicate the data with transaction consistency for the GDPS Active/Active solution. When the changed data volume grows (more changed data), it is possible that you will see high latency. You need to be careful to use the performance reference data of software-based replication to estimate your throughput and latency. Make sure that you run your own test with real data and workloads to understand how much throughput a single CG can handle and what is the expected latency in your environment. The reason is that the latency varies even when the data change rate is the same. Different record lengths and number of fields affect latency.

In extreme case, you might have to split the CG to handle very large amounts of data changes to keep reasonable latency. In an IBM InfoSphere Data Replication (IIDR) for DB2 for z/OS multiple CG configuration, you can only get eventual consistency, which poses a challenge to an Active/Query configuration because transaction consistency cannot be maintained in real time. However, if you are able to group and handle all Query workload-related data into one CG, you can still have transaction consistency for those CG for Query workloads. You are able to enable Active/Query configuration with Multiple CG in this scenario. For more information about Multiple CG, see "Consistency Group (CG) and Multiple Consistency Group (MCG)" on page 27.

6.2.5 Disaster recovery (DR) solution option

Your site might have already implemented a DR solution. GDPS Active/Active provides support to integrate or cooperate with your DR solution.

In short, the primary focus for GDPS Active/Active is to provide near-continuous availability for your Active/Active (A/A) workloads. The GDPS Active/Active disk replication integration functions are designed to complement the GDPS Active/Active functions and bring disaster recovery provision for your entire production sysplexes under the control of GDPS Active/Active. This is done by integrating disk-based replication control into GDPS Active/Active, so that you are able to manage and control aspects of your disaster recovery provision for these sysplexes from a single point. Currently, this support is limited to controlling GDPS Metro/Global Mirror (GDPS/MGM) solutions that are implemented for your production sysplexes that are running both Active/Active and non-Active/Active workloads. You can find more information in “GDPS Active/Active integration with GDPS/MGM” on page 93.

The GDPS Active/Active solution also provides cooperation support with GDPS/PPRC. With this support, you can prevent interference from each other. You can find more information in “GDPS Active/Active co-operation with GDPS/PPRC” on page 92.

If you use the GDPS Active/Active disk replication integration functions, be aware that you can have stranded data in your DR solution. In an unplanned outage, you might have stranded updates or units of work held stored on the DR copy of the DASD that are not available in the target sysplex where the Active/Active workload is now running. You need to ensure that any collisions/exceptions are looked into to decide which copy of the data is correct when you resynchronize the standby site and recovered active site by DR copy of the DASD. You need to also prepare how to handle batch work if there is batch running during the DR. You can find more in “Handling batch” on page 94.

6.3 Checklist

Table 6-2 contains a checklist of the GDPS Active/Active main tasks for the planning and implementation phases.

> **Note:** This checklist was developed from real cases and intends to provide a guide for general purposes. Because the environment, workload, and requirements of each customer are different, you can use it as a starting point for your GDPS Active/Active solution.

Table 6-2 Checklist of GDPS Active/Active solution

Phase	Tasks	Description
Planning	Study the outage	See “Study the outage” on page 81 for more information.
Planning	Identify GDPS Active/Active workloads	See “Identify GDPS Active/Active workloads” on page 81 for more information.
Planning	Plan software data replication	See “Plan software data replication” on page 82 for more information.

Phase	Tasks	Description
Planning	Decide Active/Standby or Active/Query configuration	See “Decide on an Active/Standby or Active/Query configuration” on page 82 for more information.
Planning	Plan the workload distribution	See “Plan the workload distribution” on page 83 for more information.
Planning	Integrate with DR	See “Integrate with current disaster recovery plan” on page 83 for more information.
Planning	Plan the monitoring	See “Plan the monitoring” on page 83 for more information.
Planning	Other considerations	See “Other considerations” on page 83 for more information.
Planning	Plan GDPS Active/Active use cases	See “Plan GDPS Active/Active use cases” on page 84 for more information.
Implementation	Preparation	See “Preparation” on page 84 for more information.
Implementation	Installation	See “Installation” on page 84 for more information.
Implementation	Testing	See “Testing” on page 84 for more information.
Implementation	Production	See “Production” on page 85 for more information.
Implementation	Tuning	See “Tuning” on page 85 for more information.

6.3.1 Study the outage

Study existing outages to see how GDPS Active/Active solution can help. It will also give you an idea of what the objective and your expectation should be. Complete the following stages in the suggested approach:

- Collect main outage information in the history
- Understand what GDPS Active/Active solution is and how it can help these cases
- Determine an initial target

6.3.2 Identify GDPS Active/Active workloads

After you have an idea about how the GDPS Active/Active solution can help these cases, you need to identify the Active/Active workloads. The suggested approach includes these steps:

- Understand the workloads and the environment
- Analyze the workloads to identify and define the Active/Active workload entity, and map it into the related data source

- Understand the relationship between Active/Active workloads and non-Active/Active workloads, especially the impact to the data from non-Active/Active workloads, such as the batch workload
- Assess potential impact of global transaction or transactions, which come across different type of data source or multiple Data Sharing Group

6.3.3 Plan software data replication

In 6.3.2, “Identify GDPS Active/Active workloads” on page 81, you work out the relationship between the Active/Active workload and a specific data source. With that information, you are able to create consistency groups with the selected tables or VSAM files for a software data replication plan. The suggested approach includes these steps:

- Understand your software-based replication tool
- Understand any restrictions your software-based replication tool might have and review the data and application
- Collect information about the data source, which includes the data change rate during online and batch peak times
- Collect metadata information
- Create an initial plan based on reference case
- Perform a proof of concept (POC) test of software-based replication in your environment
- Estimate CPU resource, throughput, and latency base on the POC
- Decide on whether to use single CG or Multiple CG base on maximum latency and throughput from the POC
- Review the impact if you decide to use Multiple CG

6.3.4 Decide on an Active/Standby or Active/Query configuration

If you deciding to use multiple consistency groups, you need to decide whether you want to enable an Active/Standby or Active/Query configuration. Base this decision on the following considerations:

- Business requirements
  - Are these update workloads that will run in an Active/Standby configuration, or is this a read-only or query workload that is associated with data that is updated by other workloads?
  - Can your workloads be split in such a way to facilitate running queries separate from updates?
- Software data replication testing result
  - Which configuration provides you the best throughput and latency for your workload data change rates?
- Can your GDPS Query workload related tables be handled by a single consistency group?

If you decide to enable an Active/Query configuration, then you need to perform the following planning tasks:

- Define the Query workload tolerance latency and switch criteria
- Define the RTO and RPO for an Active/Active workload switch

6.3.5 Plan the workload distribution

After you finish the plan for the GDPS workload and data replication, you need to look at workload distribution. You must understand these items to plan for your workload distribution:

- IBM Multi-site Workload Lifeline for z/OS product, mechanism, and requirements
- Your existing network configuration and topology, and how it compares to the required network layer for the GDPS Active/Active solution
- Your identified workload data flow
- Requirements at the application layer to support the GDPS Active/Active solution

6.3.6 Integrate with current disaster recovery plan

You might already have a disaster recovery solution implemented before implementing the GDPS Active/Active solution. This is often done by integrating disk-based replication control into GDPS/Active-Active so that you can manage and control aspects of your disaster recovery provision for these sysplexes from a single point. GDPS Active/Active provides functions to integrate with existing DR solutions.

Before attempting to integrate with a disaster recovery plan, take the following into consideration:

- Review existing DR solution
- Decide how to integrate with GDPS Active/Active solution
- Refine DR RTO and RPO if needed

6.3.7 Plan the monitoring

Most likely, you have already set up a monitor architecture in your environment. GDPS Active/Active provides its own monitor function and interface. Determine whether GDPS Active/Active is able to be integrated into your existing monitoring architecture. The suggested approach includes these steps:

- Understand GDPS Active/Active solution provided monitor function and interface
- Review existing monitor architecture
- Decide to use separate monitoring or integrate it with existing monitoring
- Work out the integration plan and arrange the POC test

6.3.8 Other considerations

Determine what other applications support your infrastructure and operation but are not managed by the GDPS Active/Active solution. The following list includes but is not limited to other considerations you must check before implementing GDPS Active/Active:

- GDPS Active/Active pre-requirements
- Non-GDPS Active/Active workload considerations (such as batch applications)
- Naming convention between two sites
- Data exchange considerations between two sites
- Direct access storage device (DASD) level isolation considerations
- Tape library considerations between two sites
- Application considerations

- Operation considerations
- Maintenance considerations
- Other non-mainframe platform applications that might have to work with the GDPS Active/Active solution

6.3.9 Plan GDPS Active/Active use cases

The last GDPS Active/Active solution planning task is to list GDPS Active/Active use cases. This is similar to running your own proof of concept. After you are familiar with use cases pertinent to your business, you can work out a script to handle them. The suggested approach would be:

- List GDPS Active/Active use cases
- Plan GDPS Active/Active workload switch procedure
- Plan GDPS Active/Active site switch procedure
- Non-GDPS Active/Active workload consideration in both switch scenarios

6.3.10 Preparation

After planning, begin the implementation. First, set up the target site sysplex. You do not need a secondary site immediately, but you must have a second sysplex for installation and set up. The suggested approach includes these steps:

- Ready all the pre-requirements for software and hardware
- Prepare secondary site and target Sysplex
- Prepare the network between the two sites
- Set up Sysplex for target site

6.3.11 Installation

After you set up the sysplex for the target site, install all of the related products. The following are the main products:

- GDPS Active/Active product
- IBM Multi-site Workload Lifeline for z/OS
- Products for software data replication, such as IBM InfoSphere Data Replication for DB2 for z/OS

6.3.12 Testing

Set up the same environment for testing. Testing is important to ensure GDPS Active/Active meets your continuous availability objective. The suggested approach includes these steps:

- Function test each GDPS Active/Active component
- Performance test each GDPS Active/Active component
- Operation test each GDPS Active/Active component
- Integration and use case test with all GDPS Active/Active components

6.3.13 Production

After test, separate production into different phases to mitigate the risk. An example approach to this would be production based:

1. Software-based replication
2. Workload distribution
3. GDPS Active/Active
4. Site switch rehearsal for one selected workload
5. Full site switch for all workload

6.3.14 Tuning

After GDPS Active/Active has been put into production, you can tune the product for better recovery time objective (RTO) and recovery point objective (RPO). The most tuning work is performed in the following areas:

- For RPO: Software-based replication performance tuning
- For RTO: GDPS Active/Active script tuning for better RTO

6.4 Hints and Tips

This section provides some hints and tips.

6.4.1 Software data replication

This section describes software-based replication using IBM InfoSphere Data Replication for DB2 as a sample. The concept is similar to software-based replication for IMS and VSAM.

Software-based replication provides unlimited distance, asynchronous data replication with almost no impact to workload on the active site. It reads the active site log and replays the changes on the standby site. Software-based replication does have some restrictions. The following is an example of the restrictions that were found:

- If the operation did not generate a log, then software-based replication will miss that part of the change, which normally would be seen in the replication utility. In this case, you might have to run the utility at both sites then synchronize them, or simply populate the standby site with the active site data again.
- If you have a schema change or data structure change, then software-based replication might not be able to replicate it. There are several techniques to handle schema changes. For large-scale schema changes, you can find one solution in *The Value of Active-Active Sites with Q Replication for DB2 for z/OS An Innovative Customer Experience,* REDP-5140.
- Use a unique index on, at least, the standby site, otherwise there might be performance issues when running an Apply as the agent tries to locate the record on the standby site. In an extreme case, you might have duplicate records on the active site, and you can only change one of them using Load by Cursor on the active site. However, the Apply agent changes all duplicate records on the standby site. This results in only one change on the active site and multiple changes for duplicate records on the standby site. Data are out of sync between the two sites. To address this issue, either create a unique index from an existing column or add a field to uniquely identify the record on the active site.

Always familiarize yourself with the restrictions for your software-based replication application by first reading the product manuals.

Latency

Latency is a key performance indicator (KPI) for software-based replication. In unplanned outages that cause a switch, latency affects your RPO. In planned outages, the switch would affect your RTO because you must wait for the software-based replication to catch up for zero latency. This section lists some of the most common issues that arise during the different phases of replication.

Capture phase

If during the Capture phase, the data is read from the archive log, performance might degrade and lead to high latency.

In IBM InfoSphere Data Replication for DB2, Capture needs a compression dictionary to interpret the change log. Because it reads the log of compressed table spaces, this can cause high latency. However, if the data sets have been closed, it needs extra time to open the data sets to read the compression dictionary. You can enlarge the maximum open data set number setting in DB2 to avoid this problem.

Mass delete/change activity on the active site can easily raise the latency. In your batch workloads, you must commit more frequently, especially on mass deletes or changes to data to reduce the effect on latency. If the mass deletes or changes to data applies to multiple tables, then you can also split them into separate consistency groups to avoid this cause of latency.

Transmission phase

IBM InfoSphere Data Replication for DB2 relies on WebSphere MQ to transmit the messages with the guarantee of no data loss. To do so, WebSphere MQ needs to use write logs when it receives and sends the messages. When there is high throughput, these logs can become a bottleneck. You can use a multiple CG configuration to reduce the WebSphere MQ log I/O throughput, or you can run storage performance tuning for the WebSphere MQ log data set. For example, you can avoid placing WebSphere MQ log data sets on busy disk controllers that use a heavily used transmission link.

Apply phase

DB2 11 for z/OS requires the Q Capture and Capture programs from IBM InfoSphere Data Replication for DB2 for z/OS Version 10.2.1. The Q Apply and Apply programs at architecture level 1001 work with DB2 11 for z/OS. The replication Apply process is a DB2 application that uses the SQL interface. Therefore, it requires performance tuning and configuration like any other DB2 applications.

Additionally, the transaction replay command can be different from the source, although the result should be same. For example, you can run a table scan without using an index, then update-by-cursor on the active site. The transaction replay follows a unique index to locate and change the record on the standby site. The workload pattern can be different. so the I/O pattern will vary too. Therefore, the tuning method is different on the active site than the standby site.

The order of the changes applied on the standby site can be different from the active site because of the parallel apply function. However, you might have already optimized the batch behavior or sequence to avoid lock contention on the active site, so you might still have high lock contention on the standby site because of the order changes on the apply side. High lock contention leads to high latency. You can lower the lock size on the standby site to avoid the high lock contention for better throughput, but you must estimate the CPU processor usage from your test cases first. Testing is important because the workload and access patterns vary under different production scenarios.

DB2 table space RREPL status

You will want to prevent changes performed on the standby site that can introduce user error before the switch. The DB2 for z/OS RREPL table space option is a new option introduced for use with IBM InfoSphere Data Replication for DB2, which prevents the changes from CICS/TSO/CALL attachment or IBM DRDA®. It means that both online and batch workloads cannot update the tables in table spaces that are in RREPL status. It only accepts changes through the Resource Recovery Services attachment facility (RRSAF) attachment. IBM InfoSphere Data Replication for DB2 uses the RRSAF attachment to enforce software-based replication product can update the data and all other change is not allowed in standby site.

6.4.2 Workload distribution

If you decide to enable the GDPS Active/Active Active/Query configuration, then you need to further decide on your workload distribution policy. When a user wants to deploy an all or nothing strategy based on the latency, other users can distribute the Query workload to both sites for better usage of the resource.

If you want to distribute the workload to both sites, then Lifeline has two distribution types: Dynamic or Static. The dynamic type indicates, with the increase of replication latency, new workload connections that gradually favor the site that runs the Active/Standby workload, or opposite by your configuration. Static type allows user to define specific percentage, in the range of 1 - 99, to route new connections to active site.

You can also configure how the workload switches in an unplanned outage. When workload fails on one site, Lifeline detects it and reroutes the workload to the alternate site automatically or wait until Lifeline command is issued by the user manually.

For more information about workload distribution in an Active/Query configuration, see 4.3.1, “Lifeline recommendation on workload distribution” on page 45.

6.4.3 GDPS Active/Active site switch of workloads

This section covers some of the most common difficulties you can encounter in both your test and production environments along with possible workarounds.

Test

Most testing environments have a constraint on resources, especially CPU. The GDPS Active/Active site switch of workloads is a CPU intensive task. If you have a CPU shortage, then you might have a long switch time or even failure of the switch because GDPS Active/Active sets a timer for each command. You need to make sure that the GDPS Active/Active related address space has higher priority and reserve enough CPU for the GDPS Active/Active systems to make testing results meaningful.

Production

When software-based replication runs the transaction replay on the standby site, it can only do it in one DB2 member and in one LPAR by only one Apply address space. Without a Query workload, it is the only access to the data of that consistency group in the whole sysplex on the standby site. In other DB2 members or LPARs, these data sets normally are closed without any activity for a certain period. In that case, there is not much DB2 data sharing processor burden because the data is not group buffer pool (GBP) dependent. It reduces the CPU cost of software-based replication.

Note: A data set is GBP-dependent if it is open on more than one DB2 member, and it is open for read/write on at least one member.

However after the switch, when workloads come in, you must pay processor cycles to open thousands if not more than tens of thousands of data sets in other DB2 members and LPARs now. A transaction response time spike or batch time-out can happen if the workload is too high. To mitigate it, you can select the most often used data sets and open them in other DB2 members or LPARs before the switch. If you do that, then replication processor burden might come up because all changes in the target carry data sharing processor burden now. In planning, you need to decide based on the consideration of all of this processor usage.

7

Other Considerations

This chapter describes other considerations for GDPS Active/Active solution planning.

This chapter includes the following sections:

- Application considerations
- Storage-based replication considerations
- Handling batch

7.1 Application considerations

From an application point of view, typically, workloads are classified as online workload and batch workload. GDPS Active/Active mainly monitors and manages online workloads. The user must handle the batch workload and integrate it with GDPS Active/Active.

7.1.1 Online workload consideration

Consider the following workload points:

- Workload

  Considering latency induced by asynchronous software data replication, a Query workload on the standby site should tolerate a delay. For example, historical data query workloads can be routed to the standby site because they do not require real-time data. You should determine the maximum latency that your query workload will tolerate. You must switch the Query workload back to the active site if the maximum latency tolerance is exceeded.

  Besides processing Query workloads, the standby site can also be positioned as an analytic hub based on its near real-time data property. Workloads, for example read only batches such as data extraction for data warehouses, benefit from running in a standby site. These non-online workloads improve the utilization of resources on the standby site and reduce the effect on mission critical workloads on the active site.

  To support workload switch on both sites, application servers and databases need to be active on both sites. Application modules and settings on both sites must be synchronized before a switch. Maintenance processes on both sites must be enhanced for a workload switch as well.

- Workload distribution

  Currently, the GDPS Active/Active solution only supports TCP/IP connections. The GDPS Active/Active solution tolerates both TCP/IP short life connections and long life connections. For long, live connections, in an Active/Standby configuration, it is not an issue because connections are always routed to the preferred site until a manual switch or workload failure occurs. In an Active/Query configuration, Lifeline provides a mechanism to reset long, live connections periodically so the session has a chance to connect to another site based on real-time performance information. You can customize the interval for the reset in the Lifeline configuration.

  In an Active/Query configuration, Lifeline supports both Dynamic and Static routing. With a dynamic routing configuration, Lifeline selects the site with the higher capacity to process new connections for the Query workload. With a static routing configuration, new connections are distributed to two sites based on your weights setting. This should be planned based on application and business requirements.

- Unplanned switch and data loss

  GDPS Active/Active supports planned switch by the graceful switch function. Zero data loss is ensured in a planned switch. Graceful switch blocks all new connections, then purges all running Active/Active workloads based on timer settings. It also prompts the user to stop all batch workloads. The standby site takes over the Active/Active workload until all committed changes arrive and are applied to the standby site. With these actions, planned switches achieve an RPO of 0 and an RTO in seconds.

  However, in an unplanned switch scenario, you might not have time to perform all these actions because of the nature of asynchronous data replication, so data loss can happen. One solution is to use the application log to get lost data back.

The following conditions trigger an unplanned switch:

– Active workload failure
– Active site failure
– Connection between controller and production systems using HMC LAN failure

7.1.2 Batch optimization

Software data replication can only cover DB2, IMS, and VSAM data. Most batch files are sequential data sets or partitioned data sets (PDS), which are not supported by the GDPS Active/Active solution today.

Planned switch

The first step of a graceful switch in a planned switch is a prompt to allow the user to stop the running batch. It is the user's responsibility to make sure that the graceful switch does not continue until all related batch workloads are stopped. If batch workloads must be run on the standby site after the switch, all batch-related data must be replicated to the standby site, for example by PPRC. Then, ensure that they are synchronized with GDPS Active/Active managed data. When you stop the related batch workload in an active site, it is easy to synchronize the batch files with GDPS Active/Active managed data.

Unplanned switch

In an unplanned outage when batch is running, batch files are not managed by GDPS Active/Active. Updates to batch-related data is synchronized to a target site outside of GDPS Active/Active. You might not have time to stop the related batch workloads in an unplanned switch. In this case, batch files might not be consistent with database data or VSAM files that are replicated by GDPS Active/Active.

For more about batch consideration, see “Handling batch” on page 94.

7.2 Storage-based replication considerations

As described in “Data replication” on page 8, GDPS Active/Active relies on software-based replication techniques to synchronize data between sites, and currently supports three types of data:

- DB2
- IMS
- VSAM

These techniques are described in Chapter 3, “GDPS and data replication” on page 23.

The primary purpose of GDPS Active/Active is to provide near-continuous availability for Active/Active workloads with unlimited distances. The solution is not intended to be a replacement for the current storage-based replication technologies (such as Peer-to-Peer Remote Copy, Global Mirror, and z/OS Global Mirror). Rather, it is an option to help customers achieve better availability for critical applications. Today, GDPS Active/Active mainly supports online workloads. For other workloads and data, other replication solutions will often be necessary.

GDPS Active/Active supports controlled integration with other disk-based replication solutions. At the time of writing, this support includes GDPS/MGM that is implemented in your production sysplexes that are running both Active/Active and non-Active/Active workloads. You must have incremental resynchronization configured in the GDPS/MGM to take advantage of the integrated functions. This does not mean you cannot have other replication solutions installed, but they will be transparent to GDPS Active/Active. Also, if you already have GDPS/PPRC implemented or are planning to implement it, you must run GDPS/PPRC version 3.10 with current PTFs or later so that the actions taken by GDPS Active/Active or GDPS/PPRC do not cause the other to be seen as potential failures. This co-operation between both solutions is described in 7.2.1, "GDPS Active/Active co-operation with GDPS/PPRC" on page 92.

7.2.1 GDPS Active/Active co-operation with GDPS/PPRC

Figure 7-1 shows a high-level architectural view of how GDPS/PPRC fits in a GDPS Active/Active environment.

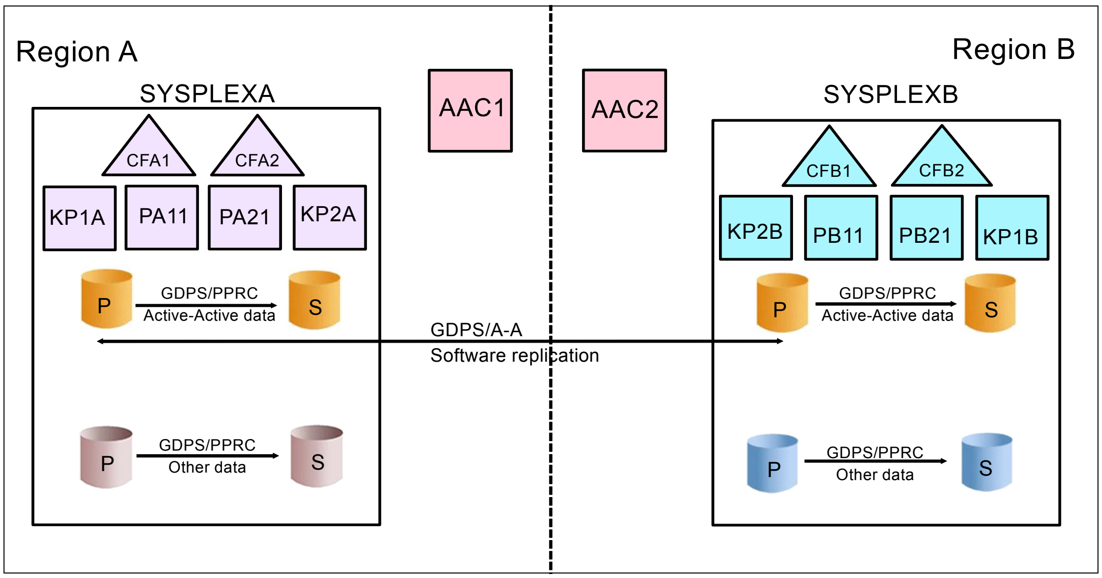


Figure 7-1 GDPS Active/Active co-operation with GDPS/PPRC

In each of the sites you have a separate Parallel Sysplex with its own GDPS/PPRC. For more information about GDPS/PPRC, see *GDPS Family: An Introduction to Concepts and Capabilities*, SG24-6374.

In a GDPS Active/Active environment where you have already implemented (or will implement) GDPS/PPRC to manage data replication and systems management within your Active/Active sysplexes, there are a number of considerations to be taken into account. These considerations are associated with where and how systems management functions, such as the **LOAD** and **STOP** Standard Actions, are run.

Consider that you are running a **STOP** action against a system from GDPS Active/Active. Without awareness of this, GDPS/PPRC interprets the system as having failed and issues a **Takeover** prompt, even though this was a planned action and no system had actually failed. Likewise, in the opposite direction, GDPS Active/Active can interpret GDPS/PPRC actions as potential workload failures. GDPS co-operation avoids such situations.

In addition to the awareness aspects described, GDPS also provides a locking mechanism, so that when an action is carried out in one environment, say GDPS Active/Active, the objects being acted on are prevented from having actions carried out against them by GDPS/PPRC. There is one exception to this where an autonomic action is required by GDPS/PPRC to ensure data integrity, such as resetting a system that is not responding to a HyperSwap request. This type of action is able to override any held locks.

GDPS also provides the ability for site table selections to be passed from GDPS/PPRC to GDPS Active/Active, so that the currently selected entry in both environments has the same load address, load parameter, and so on.

Finally, the cooperation between GDPS Active/Active and GDPS/PPRC ensures that when a HyperSwap is taking place in the GDPS/PPRC environment, the buttons in the GDPS Active/Active web application for managing software replication are disabled. This is because any such commands issued during the swap process are likely to hang, as the replication engines will not be able to perform any I/O until the swap is complete.

Note: The GDPS/PPRC co-operation support does not extend to include the management of any VM systems being managed using xDR capabilities, or any non-GDPS systems that are managed using foreign systems support.

7.2.2 GDPS Active/Active integration with GDPS/MGM

The GDPS Active/Active integration with GDPS/MGM is intended to bring to the production environment a higher level of protection. It takes advantage of the near-continuous availability provided by GDPS Active/Active, in unlimited distances, and also the resiliency and Disaster Recovery readiness provided by GDPS/MGM.

Figure 7-2 shows an environment with both GDPS Active/Active and GDPS/MGM are implemented.

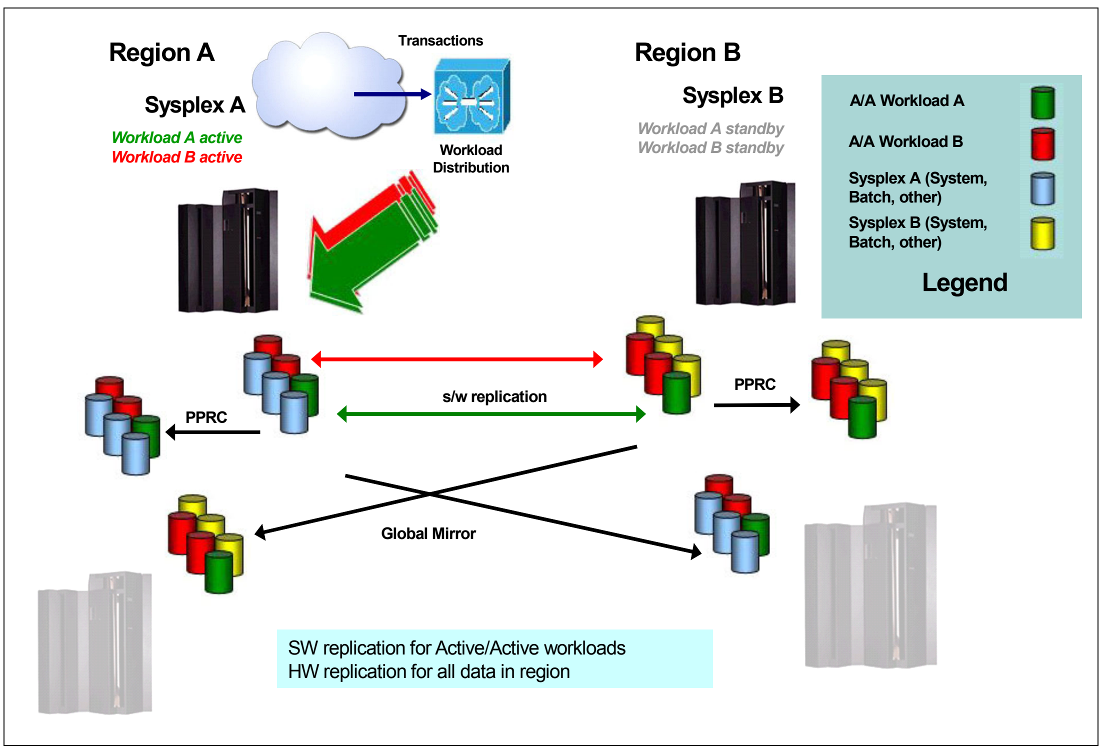


Figure 7-2 GDPS Active/Active integration with GDPS/MGM

The integration between GDPS Active/Active and GDPS/MGM is provided by the Disk Replication Manager (DRM), which is code that is packaged as part of the GDPS/AA software product. It runs as a separate NetView instance and provides the interface between GDPS/AA and GDPS/MGM. For redundancy purposes, there are normally two instances of

DRM in a GDPS Active/Active environment, one primary and other backup, in case the primary is not available for some reason.

A number of scenarios are supported through disk replication integration, as follows:

- Initial start of replication
- Suspend replication
- Restart a suspended mirror
- Stop replication
- Prepare the DR copy for a DR test
- Initiate a planned switch to the DR copy for a sysplex
- Initiate disaster recovery for a sysplex
- Return to normal configuration following a DR invocation or planned switch

Using the GDPS Active/Active Controller to perform GDPS Active/Active related operations and the hardware replication actions greatly simplifies operations because all of these actions are performed from a single point of control. Without this integration, it would be necessary to run different steps of a complex operation (such as a planned region switch of an entire sysplex) by running different steps on multiple different controlling systems.

The disk integration function provides simple, high-level primitives whereby a single script statement coordinates performing of multiple disk replication-related operations across the GDPS/PPRC and GDPS/GM environments that comprise the GDPS/MGM configuration. For example, assume that you want to run a planned region switch of Sysplex A to its DR hardware replica in Region B. First, you need to switch the Active/Active workloads to run in Sysplex B, after which you can stop all of the systems in Sysplex A. Both of these actions can be performed using native GDPS Active/Active functions. Next, to power on Sysplex A on the hardware replica in Region B, there are multiple disk replication-related steps. These steps are not detailed here, but some must be performed by the GDPS/PPRC Controlling system, and others must be performed by the GDPS/GM Controlling system.

With the GDPS Active/Active disk integration capability, all of these disk replication steps are boiled down to a single script statement (for this example, **`DISKREPLICATION SWITCH SYSPLEX=SYSPLEXA PLANNED`**), which is initiated from and coordinated by the GDPS Active/Active Controller.

In summary, GDPS Active/Active with GDPS/MGM provide a comprehensive set of capabilities to automate out-of-region, near-continuous availability (for Active/Active workloads) and disaster recovery (for all workloads) for your production sysplexes using GDPS Active/Active as the single point of control.

> **Note:** Make sure that the GDPS/PPRC cooperation support is also established when using GDPS Active/Active and GDPS/MGM integration.

7.3 Handling batch

Batch needs special consideration because GDPS Active/Active does not manage batch workloads, and IBM software data replication products only support DB2, IMS, and VSAM data today.

7.3.1 Batch workload

Batch workloads are different on each client. Looking at the most common batch workloads, they normally involve the following data elements:

- Control files used for batch scheduling applications or tools
- Batch files, which are typically sequential data sets or PDS
- User data in DB2, IMS, VSAM, or other database products

The most common flow of batch processing involves these phases:

- Generate intermediate files for further processing. For example, read data from VSAM or a database, filter it and write the output to batch files.
- Update data in the target data source or generate a report, read the batch intermediate files as input, then process and write back to VSAM or database.

7.3.2 Challenges of the batch workload to GDPS Active/Active

Batch workloads bring challenges to GDPS Active/Active.

Software data replication only supports DB2, IMS, and VSAM at the time of writing. Therefore, changes in batch files, which can be sequential date sets or a PDS, cannot be captured from an active site and applied to a standby site. All changes in batch will be missed on the standby site and you will need to replicate the batch data either by an application or a storage replication solution.

Batch workload scheduling applications or tools use their own files to store a batch job status. Like batch files, these files are normally sequential data sets or PDS. You will need to replicate it by application or storage replication solution too.

If you use different solutions to replicate these elements of batch, they can become out of sync. In the worst case, you might not be able to resume the batch on the standby site without user intervention.

7.3.3 Solution

This section outlines a potential solution to handling batch workloads in a GDPS Active/Active environment. To make this example simple, the following naming conventions are used for a three site configuration:

- Active site Sysplex: SYSPLEXA
- Standby site Sysplex: SYSPLEXB

The easiest way to handle batch in GDPS Active/Active solution is to ensure that there is no running batch during the Active/Active workload or site switch. During a GDPS Active/Active graceful switch, a GDPS Active/Active script prompts the user to stop related batch on the active site. If you stop your batch workloads, then all you need to do is run replication of your batch files and control files of batch scheduling applications or tools with the last changes to the standby site. Avoid running related batch on the active site after the switch. By doing this, all three elements of the related batch workloads on the standby site will remain synchronous.

However, if you have an unplanned event, then you face the challenge of the batch running when you try to perform the switch. In this case, the data elements can become out of sync. It is the user responsibility to handle resumption of the batch on the standby site.

One best practice is to include stopping batch in your emergency handling process. Most customers still have an emergency handling window for unplanned events when the active site systems can still respond to your commands. If you do so, the treatment of batch is similar to a planned switch case.

In the worst case of an unplanned event, the active site will not take any commands. One option is to use your existing DR solution (for example the MGM) to continue the workload, which creates a longer RTO but you do not need to worry about the batch if all workloads of the active site are important. If the Active/Active workload is so important, then you must switch the workload and resume it immediately.

When you start your active site from the DR copy, and populate changes from the standby site back into the active site, you might strand updates or units of work stored on the DR copy of the DASD that are not available to the standby site where the Active/Active workload is now running. You must ensure that any collisions or exceptions are looked into to decide which copy of the data is correct when you synchronize the active site and the standby site. You can only run batch on the active site after all these issues are fixed. You should not run batch on the standby site because it can make the things worse. For more information about running batch on the standby site, see *The Value of Active-Active Sites with Q Replication for DB2 for z/OS An Innovative Customer Experience,* REDP-5140.

A

IBM Global Technology Services and GDPS service offering

This appendix covers the IBM Global Technology Services organization, its offerings which include but are not limited to GDPS, and also answer the following questions:

- What is IBM Global Technology Services?
- What are GDPS service offerings and how do they address business requirements?
- How do I contact IBM for GDPS services?

What is IBM Global Technology Services?

IBM Global Technology Services (GTS) is an IBM organization that offers end-to-end IT and business process services supported by an unmatched global delivery network, and delivers the skills and expertise required to meet your IT infrastructure challenges. The variety of services delivered by IBM GTS include, but are not limited to:

- Application management services

  Application services that enable you to thrive in today's global, mobile, and social environments
- Business continuity

  Optimize business continuity, improve regulation management, and enable quicker recovery from unanticipated disasters
- Cloud services

  Reinvent your business with the power of cloud computing
- Data center services

  Build and manage highly efficient data centers that respond to change and drive innovation
- Enterprise mobility

  Plan, manage, and secure complex mobile environments
- IT infrastructure services

  Transform your IT infrastructure to achieve critical business and IT goals
- IT outsourcing

  Partner to drive innovation
- IT strategy

  Develop the correct IT strategy to support business objectives
- Security services

  Protect your enterprise from complex IT security threats while reducing costs
- Technical support services

  Simplify management and streamline maintenance of multivendor environments

For more information about each of these offerings, consult your IBM representative, or visit the IBM Global Technology Services website at:

`http://www.ibm.com/services/`

What are GDPS service offerings and how do they address business requirements?

GDPS is a collection of several offerings, each addressing a different set of IT resiliency goals that can be tailored to allow your business to achieve its own continuous availability and disaster recovery goals. Each offering uses a combination of server and storage hardware or software-based replication, and automation and clustering software technologies, many of which are described in this book.

GDPS is designed to provide not only resource sharing, workload balancing, and near continuous availability benefits of a Parallel Sysplex environment, but it can also enhance the capability of an enterprise to recover from disasters and other failures, and manage planned exception conditions. In addition to the infrastructure that makes up a given GDPS solution, IBM also offers services, particularly for the planning and implementation of GDPS and optionally for subsequent related activities, to ensure that the solution meets and fulfills your business objectives These include *Technical Consulting Workshop* and *IBM Installation Services for GDPS*, briefly described below.

Technical Consulting Workshop

TCW is a two-day workshop where GTS specialists work with your representatives to understand your business objectives, service requirements, technological directions, business applications, recovery processes, and cross-site and I/O requirements. High-level education on GDPS is provided, along with the service and implementation process. Various remote and local data protection options are evaluated.

GTS specialists present a number of planned and unplanned GDPS reconfiguration scenarios, with recommendations on how GDPS can assist you in achieving your objectives. At the conclusion of the workshop, the following items are developed: Acceptance criteria for both the test and production phases, a high-level task list, a services list, and project summary.

IBM Installation Services for GDPS

The IBM installation services for GDPS include the following items:

- Helps during planning, configuring, and automation code customization
- Provides onsite assistance
- Provides an automated, cross-platform disaster recovery solution (GDPS/PPRC, GDPS/PPRC HyperSwap Manager, GDPS/XRC, GDPS/GM, GDPS/MGM, GDPS/MzGM, and GDPS Active/Active)
- Includes onsite delivery, configuration, implementation, and testing
- Provides training for your support staff
- Provides centralized management of your data replication and recovery environment using automated technologies to help provide an end-to-end disaster recovery solution

> **Note:** The services also include project management and support throughout the engagement, and assistance to help you implement any prerequisite software.

Through proper planning and exploitation of the GDPS technology, enterprises can help protect their critical business applications from an unplanned or planned outage event. When comparing GDPS with other near continuous availability and Disaster Recovery solutions, the following factors must be also considered:

- Do you want to improve your application availability?
- Does the solution handle both planned and unplanned outages?
- Which solution meets the RTO of your business? Note that you might have different RTOs for the different applications in your organization. RTO for your critical applications should be as small as possible.

- Which solution meets the RPO of your business? Note that you might have different RPOs for the different applications in your organization. Data loss for your critical applications should be none or minimal when there is an outage or disaster.
- Do you want to minimize the cost of taking repetitive volume memory dumps, transporting the cartridges to a safe place, and keeping track of which cartridges should be moved to which location and at what time?
- What is the cost of disaster recovery drills?

The ease of planned system, disk, Remote Copy, and site reconfigurations that is offered by GDPS allows your business to reduce the onsite manpower and skill that are required for these functions. GDPS can enable a business to control its own near continuous availability and disaster recovery goals.

GDPS Offerings

The following list provides brief descriptions of each GDPS offering, with a view of which IT resiliency objectives it is intended to address. More details are included in separate chapters in this book:

- GDPS/PPRC

  Near-CA or DR solution across two sites separated by metropolitan distances. The solution is based on the IBM PPRC synchronous disk mirroring technology.
- GDPS/PPRC HyperSwap Manager

  Near-CA solution for a single site or entry-level DR solution across two sites separated by metropolitan distances. The solution is based on the same technology as GDPS/PPRC, but does not include much of the systems automation capability that makes GDPS/PPRC a more complete DR solution.
- GDPS/XRC

  DR solution across two sites separated by virtually unlimited distance between sites. The solution is based on the IBM XRC asynchronous disk mirroring technology (also branded by IBM as z/OS Global Mirror).
- GDPS/Global Mirror

  DR solution across two sites separated by virtually unlimited distance between sites. The solution is based on the IBM System Storage® Global Mirror technology, which is a disk subsystems-based asynchronous form of remote copy.
- GDPS Metro/Global Mirror

  Either a 3-site or a symmetrical 4-site configuration is supported:

  - GDPS Metro/Global Mirror 3-site: A three-site solution that provides CA across two sites within metropolitan distances and DR to a third site, in a different region, at virtually unlimited distances. It is based on a cascading mirroring technology that combines PPRC and Global Mirror.
  - GDPS Metro/Global Mirror 4-site: A symmetrical four-site solution that is similar to the 3-site solution in that it provides CA within region and DR cross region. In addition, in the 4-site solution, the two regions are configured symmetrical such that the same levels of CA and DR protection is provided, no matter which region production runs in.

- GDPS Metro/z/OS Global Mirror

  A three-site solution that provides CA across two sites within metropolitan distances and DR to a third site at virtually unlimited distances. It is based on a multitarget mirroring technology that combines PPRC and XRC (also known as z/OS Global Mirror on IBM storage subsystems).
- GDPS Active/Active

  A multisite CA/DR solution at virtually unlimited distances. This solution is based on software-based asynchronous mirroring between two active production sysplexes running the same applications with the ability to process workloads in either site.

How do I contact IBM for GDPS services?

To learn more about any of the items described in this book, or any other information about GDPS, contact your local IBM representative or send an email to:

`mailto:gdps@us.ibm.com`

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

IBM Redbooks

The following IBM Redbooks publications provide additional information about the topic in this document. Note that some publications referenced in this list might be available in softcopy only.

- *GDPS Family: An Introduction to Concepts and Capabilities, SG24-6374*
- *InfoSphere Data Replication for DB2 for zOS and WebSphere Msg Q for zOS,REDP-4947-00*

You can search for, view, download or order these documents and other Redbooks, Redpapers, Web Docs, draft and additional materials, at the following website:

ibm.com/redbooks

Other publications

These publications are also relevant as further information sources:

- "GDPS: The Enterprise Continuous Availability / Disaster Recovery Solution," David Petersen at:
  http://freebooks9.org/g/gdps-the-enterprise-continuous-availability-disaster-w14899/
- *GDPS/Active-Active 1.4 Planning and Implementation Guide*, ZG24-1767-02
- *IBM InfoSphere Data Replication for IMS for zOS v11.1 Guide and Reference*, SC19-4174-00
- *IBM InfoSphere Data Replication for VSAM for zOS v11.1 Guide and Reference*, SC19-4177-00
- *IBM Multi-site Workload Lifeline User's Guide*, SC27-4653
- *NetView for zOS v6.2 - Installation Configuring the GDPS Active-Active Continuous Availability Solution*, SC14-7477-02

Online resources

These websites are also relevant as further information sources:

- IBM Tivoli NetView

  http://www-03.ibm.com/software/products/en/tivoli-netview-zos
- IBM Tivoli Monitoring

  http://www-03.ibm.com/software/products/en/tivomoni

- Overview of IBM Tivoli Monitoring

  http://pic.dhe.ibm.com/infocenter/tivihelp/v30r1/index.jsp?topic=%2Fcom.ibm.itm.doc_6.2.2fp2%2Ftep_overview.htm
- IBM OMEGAMON XE Family

  http://www-03.ibm.com/software/products/en/omegamon-xe-zos
- IBM Global Technology Services

  http://www.ibm.com/services/

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

IBM Redbooks

IBM GDPS Active/Active Overview and Planning

(0.2”spine)
0.17”<->0.473”
90<->249 pages

IBM GDPS Active/Active Overview and Planning

GDPS Active/Active architectural overview

Hints and tips for GDPS Active/Active deployment

Planning for GDPS Active/Active

IBM Geographically Dispersed Parallel Sysplex (GDPS) is a collection of several offerings, each addressing a different set of IT resiliency goals. It can be tailored to meet the recovery point objective (RPO), which is how much data can you are willing to lose or recreate, and the recovery time objective (RTO), which identifies how long can you afford to be without your systems for your business from the initial outage to having your critical business processes available to users.

Each offering uses a combination of server and storage hardware or software-based replication, and automation and clustering software technologies.

This IBM Redbooks publication presents an overview of the IBM GDPS active/active (GDPS/AA) offering and the role it plays in delivering a business IT resilience solution.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-8241-00 ISBN 0738440620