

Best Practices for IBM DS8000 and IBM z/OS HyperSwap with IBM Copy Services Manager

Thomas Luther

Alexander Warmuth

Marcelo Takakura



Storage



IBM Redbooks

**Best Practices for IBM DS8000 and IBM z/OS
HyperSwap with IBM Copy Services Manager**

May 2019

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

First Edition (May 2019)

This edition applies to IBM Copy Services Manager (CSM) V6.2.3 with IBM DS8000 Version 8.5.

© Copyright International Business Machines Corporation 2019. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	vii
Trademarks	viii
Preface	ix
Authors	ix
Now you can become a published author, too!	x
Comments welcome	x
Stay connected to IBM Redbooks	x
Part 1. Introduction and planning	1
Chapter 1. Introduction	3
1.1 IBM Copy Services Manager overview	4
1.2 CSM licenses	5
1.2.1 CSM licenses for z/OS platforms	5
1.2.2 CSM licenses for distributed server platforms	6
1.3 z/OS HyperSwap overview	7
1.3.1 z/OS HyperSwap: Not so basic anymore	8
1.3.2 CSM sessions that support HyperSwap	9
1.3.3 z/OS HyperSwap functions	9
1.3.4 HyperSwap sequence	11
1.3.5 Planned and unplanned HyperSwap	12
1.4 CSM and HyperSwap communication flow	13
1.5 GDPS Metro solutions	14
1.6 IBM Resiliency Orchestration and CSM	15
Chapter 2. IBM Copy Services Manager and IBM z/OS HyperSwap implementation topologies	19
2.1 CSM connection type overview	20
2.1.1 TCP/IP-based connections to storage systems	21
2.1.2 FICON based connections to storage systems	21
2.1.3 Host connections to z/OS LPARs	23
2.2 z/OS relevant address spaces for CSM	25
2.2.1 HyperSwap or Hardened Freeze address spaces	25
2.2.2 z/OS IP host connection relevant address spaces	26
2.2.3 z/OS CSM Server relevant address spaces	26
2.2.4 Summary of relevant z/OS address spaces	27
2.3 Implementation scenarios	27
2.3.1 General considerations for all implementation scenarios	27
2.3.2 IBM z/OS CSM server Basic Edition implementation	28
2.3.3 CSM server on z/OS with standby CSM on z/OS	29
2.3.4 CSM server on z/OS with standby on distributed platform	31
2.3.5 HyperSwap management by CSM servers outside of Sysplex	32
2.3.6 HyperSwap management by CSM servers on DS8880 HMCs	34
2.3.7 Cascaded MGM or Multi Target MM-GM with local HyperSwap	35
2.3.8 Multi Target MM-MM with 3-site HyperSwap	37
2.3.9 CSM servers with FICON only storage connections	39
Chapter 3. Prerequisites for various implementation topologies	43

3.1 TCP/IP Communication requirements.	44
3.2 Prerequisites for z/OS HyperSwap	45
3.2.1 IBM z/OS APARs for HyperSwap and other CSM functions.	45
3.2.2 z/OS APARs for Multiple Target Peer-to-Peer Remote Copy and HyperSwap . .	46
3.2.3 z/OS HyperSwap configuration prerequisites	47
3.3 Prerequisites for z/OS IP host connections.	49
3.4 Prerequisites for DS8000 storage controllers	49
3.5 Prerequisites for Hitachi Virtual Storage Platform storage controllers	51
Part 2. Installation and Configuration	53
Chapter 4. CSM Installation on IBM z/OS	55
4.1 SMPE installation	56
4.2 Post SMPE installation tasks	56
4.2.1 Create Users.	56
4.2.2 Create and mount the CSM file system	58
4.2.3 Perform CSM installation in UNIX System Services	60
4.2.4 Create started tasks for CSM server.	62
4.3 Update the CSM installation	63
Chapter 5. IBM z/OS IP host connection setup	65
5.1 Configuration tasks overview	66
5.2 Disable encryption for z/OS IP host connections	67
5.3 Configure z/OS users for HyperSwap tasks and z/OS IP host connections	68
5.4 Configure HyperSwap tasks with socket port	70
5.5 Create z/OS certificates	72
5.5.1 Certificate considerations when multiple LPARs connect to CSM server.	72
5.5.2 CA Certificate generation	72
5.5.3 Create server certificate and keyring	74
5.5.4 Sample CLISTs.	76
5.6 Export CA certificate	77
5.7 Configure AT-TLS policy.	78
5.8 Configure the z/OS TCP/IP policy agent (PAGENT).	80
5.9 Generate a Java keystore file for the CSM server	83
5.9.1 Create Java keystore file	83
5.9.2 Transfer the keystore file to the CSM servers.	90
5.10 Create the CSM IP host connection	91
5.11 Troubleshoot CSM z/OS IP host connection errors	95
Chapter 6. Implementing z/OS HyperSwap.	97
6.1 HyperSwap address spaces and started tasks.	98
6.2 IBM z/OS configuration for HyperSwap	99
6.2.1 Install the latest PTFs for z/OS HyperSwap	100
6.2.2 HyperSwap related console commands	100
6.2.3 Enable critical paging	100
6.2.4 Sharing volumes with systems outside the Sysplex	101
6.2.5 Hardware reservations	102
6.2.6 Message control	103
6.2.7 Reduce delays of HyperSwap triggers	107
6.2.8 Enable I/O timeouts to trigger a HyperSwap.	108
6.2.9 Couple Data Set considerations	109
6.2.10 IPL considerations	114
6.2.11 Allocation and esoteric names	117
6.2.12 JES3 considerations	117

6.2.13 JES2 considerations	117
6.2.14 Enhanced Catalog Sharing considerations	118
6.2.15 Cache fast write avoidance	119
6.2.16 Concurrent Copy avoidance	121
6.2.17 Z Global Mirror (XRC) interactions	121
6.2.18 FlashCopy usage in a HyperSwap environment	121
6.2.19 Coexistence with other products that use UCB swaps	124
6.2.20 Special HyperSwap considerations for use with other applications	125
6.2.21 SMF Recording	126
Part 3. Management and Operations	127
Chapter 7. Managing z/OS HyperSwap with IBM Copy Services Manager	129
7.1 Prepare session and enable HyperSwap	130
7.1.1 Assign discovered Sysplex to CSM session	130
7.1.2 Enable HyperSwap for a session	131
7.1.3 HyperSwap configuration settings	132
7.1.4 HyperSwap active	134
7.1.5 Check HyperSwap status in z/OS	135
7.2 HyperSwap usage scenarios	136
7.2.1 General remarks about CSM session management	136
7.2.2 Starting a HyperSwap session	138
7.2.3 Planned HyperSwap	139
7.2.4 Resynchronizing replication after a HyperSwap	140
7.2.5 Further considerations	141
7.3 Characteristics of different HyperSwap capable session types	142
7.3.1 Basic HyperSwap session	142
7.3.2 Three-site session types with remote replication for disaster recovery	143
7.3.3 Three-site Multiple Target MM - MM session	147
7.3.4 Four-site session MM - GM w/ Site 4 Replication	151
7.3.5 HyperSwap management for asymmetrical replication topologies	152
Chapter 8. Additional operational considerations	155
8.1 CSM monitoring, logging and alerting	156
8.1.1 CSM monitoring	156
8.1.2 CSM logging	158
8.1.3 CSM alerting	159
8.2 Operational considerations for z/OS	159
8.2.1 z/OS HyperSwap commands	159
8.2.2 z/OS messages related to HyperSwap	164
8.2.3 HyperSwap alerting	165
8.2.4 HyperSwap sequence logging example	165
8.2.5 HyperSwap failures	166
8.3 Testing unplanned HyperSwap	167
8.3.1 z/OS initiated unplanned HyperSwap	168
8.3.2 Forcing an IO error to trigger an unplanned HyperSwap	168
8.4 Reconfigure replicated Count Key Data storage devices	169
8.4.1 Relabel existing replication devices	169
8.4.2 Create new replication devices	170
8.4.3 Delete existing replication devices	172
8.4.4 Resize existing replication devices	173
8.5 Troubleshooting	174
8.5.1 Recovering boxed devices	174
8.5.2 Resolving fenced devices	177

8.5.3 Recovering from Secondary In Use By System	179
8.5.4 Recovering from missing or stale NED	180
8.5.5 Additional hints and tips	181
8.5.6 Creating support information	181
Appendix A. Checklists	183
Checklist for implementation planning	184
Checklist for CSM installation on z/OS	184
Checklist for z/OS IP host connection setup	185
Checklist for z/OS HyperSwap implementation	186
Related publications	189
References	189
IBM Redbooks	189
Help from IBM	190

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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, MD-NC119, Armonk, NY 10504-1785, US

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 jurisdictions 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 provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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 actual people or business enterprises 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. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at <http://www.ibm.com/legal/copytrade.shtml>

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

AIX®	IBM Spectrum Control™	RMF™
DS8000®	IBM Spectrum Virtualize™	Storwize®
Easy Tier®	IBM Z®	System z®
FICON®	MVS™	Tivoli®
FlashCopy®	NetView®	WebSphere®
GDPS®	Parallel Sysplex®	XIV®
HyperSwap®	Passport Advantage®	z Systems®
IBM®	ProductPac®	z/OS®
IBM FlashSystem®	RACF®	z/VM®
IBM SmartCloud®	Redbooks®	
IBM Spectrum™	Redbooks (logo)  ®	

The following terms are trademarks of other companies:

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

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.

Preface

Many IBM® z/OS® customers require their applications to be available 24x7. Whether the business requirements are high availability (HA), disaster recovery (DR), or business continuity, IBM HyperSwap® technology can provide an adequate solution. HyperSwap is the industry standard and is provided as several different implementation options to meet the various business needs of the IBM System z® and z/OS customer base.

IBM Copy Services Manager (CSM) enables you to manage z/OS HyperSwap and helps you manage planned and unplanned actions in an z/OS environment from an open systems environment.

This IBM Redbooks® publication provides best practices for the planning, implementing, integrating, and managing z/OS HyperSwap with CSM.

Authors

This book was produced by a team of specialists from around the world.

Thomas Luther is a consulting IT Specialist in Germany and holds a degree in electrical engineering. He has worked for the IBM EMEA Storage Competence Center for 21 years. His areas of expertise include storage copy services and replication management software, z/OS HyperSwap implementations, and z/OS data migrations with IBM Transparent Data Migration Facility (IBM TDMF). He also published various white papers for IBM Tivoli® Storage Productivity Center for Replication and CSM.

Alexander Warmuth is a Consulting IT Specialist in IBM EMEA Storage Competence Center. Working in technical sales support, he designs and promotes new and complex storage solutions; drives the introduction of new products; and provides advice to customers, Business Partners, and sales. His main areas of expertise are high-end storage solutions and business resilience for IBM z® Systems® and Linux. He joined IBM in 1993 and has worked in storage technical sales support since 2001. Alexander holds a diploma in Electrical Engineering from the University of Erlangen, Germany.

Marcelo Takakura is an IT Specialist with the IBM Brazil Lab Services Storage team. He has worked at IBM since 2009 and in storage management since 2002, mainly with IBM storage products such as DFSMS, TS7700, IBM DS8000® storage systems, and z/OS data migration and availability (tape copy, IBM TDMF, IBM z/OS Data Set Mobility Facility (zDMF), copy services, CSM, and HyperSwap). His areas of expertise include installing, configuring, and supporting z/OS storage products.

This project was managed by:

Bert Dufrasne
IBM Redbooks

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

Rendy Blea, Nick Clayton, William Rooney, Robert Tondini, Nathalie Arlhac
IBM

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 IBM Redbooks 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, IBM Redbooks
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>



Part 1

Introduction and planning

This part provides an overview of IBM Copy Services Manager (CSM) and z/OS HyperSwap, and presents various implementation scenarios with their options, advantages, and limitations. It also describes the prerequisites for various implementation options.



Introduction

This chapter provides an overview of IBM Copy Services Manager (CSM) and IBM z/OS HyperSwap. It describes CSM licenses and provides a brief comparison with the IBM Geographically Dispersed Parallel Sysplex® (GDPS®)HyperSwap solution.

1.1 IBM Copy Services Manager overview

CSM (formerly *IBM Tivoli Storage Productivity Center for Replication*, which is a component of IBM Tivoli Storage Productivity Center and IBM SmartCloud® Virtual Storage Center (VSC)) manages copy services in IBM storage environments. Copy services designate features that are used by storage systems to configure, manage, and monitor data replication functions. For the DS8000 storage system, these copy services include IBM FlashCopy®, Metro Mirror (MM), Global Mirror (GM), Metro Global Mirror (MGM), and Multiple Target Peer-to-Peer Remote Copy (MT-PPRC) data replication functions.

CSM is available for installation on various distributed server platforms, such as Windows, Linux, IBM AIX®, and z/OS. It is also preinstalled on the Hardware Management Consoles (HMCs) of each DS8880 storage system. There are several license models for CSM, which are described in 1.2, “CSM licenses” on page 5. For a complete list of supported storage systems and server platforms, see the [CSM supported storage system matrix](#).

CSM automates key replication management tasks to help you improve the efficiency of your storage replication. Figure 1-1 shows a high-level illustration of the architecture.

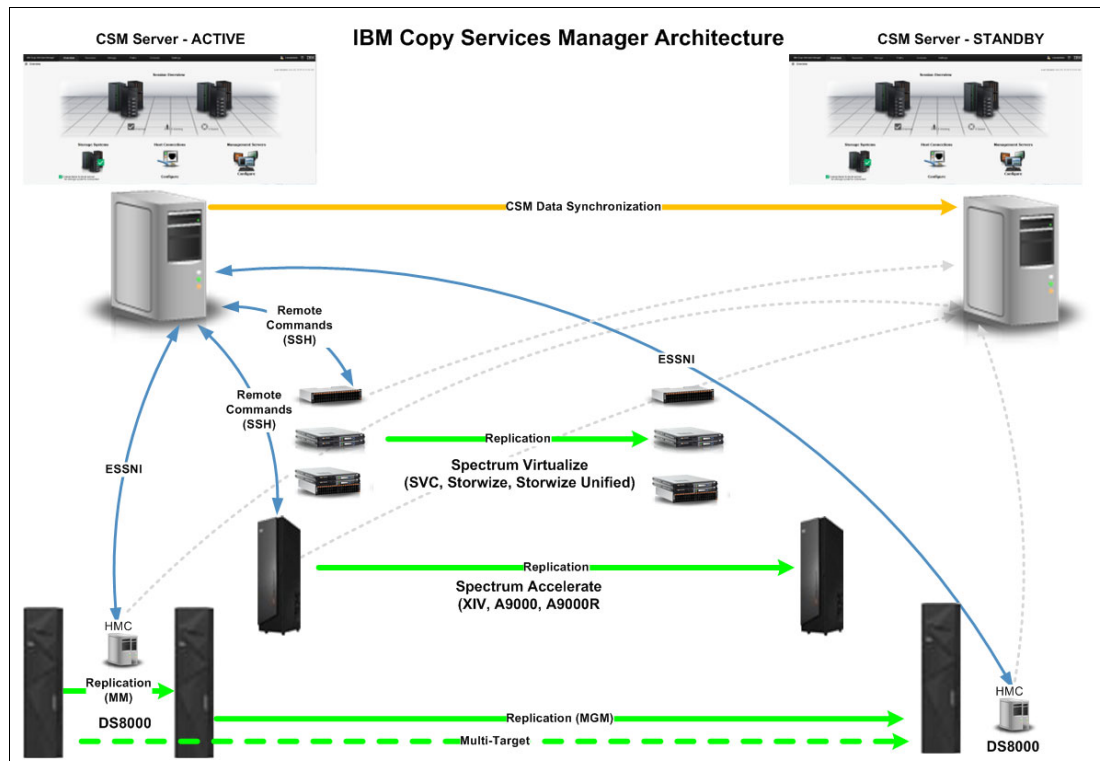


Figure 1-1 IBM Copy Services Manager architecture

CSM offers a simple web browser-based GUI to configure, automate, manage, and monitor all important data replication tasks in your environment, including the following tasks:

- ▶ Manage and monitor multi-site environments to meet disaster recovery (DR) requirements.
- ▶ Automate the administration and configuration of data replication features.
- ▶ Keep data on multiple related volumes consistent across storage systems during a planned or unplanned outage.
- ▶ Recover to a remote site to reduce the downtime of critical applications.

- Provide high availability (HA) for applications by using IBM HyperSwap technology.
- Practice recovery processes while DR capabilities are maintained.

For more information about CSM, see *IBM Copy Services Manager Implementation Guide*, SG24-8375.

1.2 CSM licenses

This section provides an overview of the available licensing options for CSM. Generally, the CSM license type depends on the operating system platform where the CSM server is installed and operated. The proper license type for your implementation scenario might depend on your requirements. For planning purposes, see 2.3, “Implementation scenarios” on page 27.

1.2.1 CSM licenses for z/OS platforms

As of CSM V6.2.3, there are two different license versions of CSM for installation on z/OS:

- IBM Copy Services Manager for z/OS (CSM Program Number 5698-E01):
 - FMID HIWN62C, JIWN62Z (CSM 6.2.x)
 - FMID HIWN62H, JIWN62X (CSM 6.2.3)

Licensed per TB Value Units for replicated source capacity

- IBM Copy Services Manager for z/OS Basic Edition (CSM Program Number 5698-E02)
 - FMID HIWN62C (CSM 6.2.x)
 - FMID HIWN62H (CSM 6.2.3)

No charge license per machine (service and subscription fees apply)

Both license versions can be obtained from [IBM Shopz](#).

Table 1-1 provides an overview of the different capabilities of these two versions.

Table 1-1 CSM for z/OS and CSM for z/OS Basic comparison

Feature	CSM for z/OS	CSM for z/OS Basic
Help simplify and automate complex replication tasks without scripts.	Yes	Yes
Support IBM DS8000; IBM SVC; IBM Storwize® V5000, V7000, V7000 Unified, V3700, and V3500; IBM FlashSystem® V9000, V840, A9000, and A9000R; and IBM XIV® systems.	Yes	DS8000 only
Support Hitachi Virtual Storage Platform (VSP)	Yes	Yes
Manage both z/OS Count Key Data (CKD) and distributed Fixed Block (FB) volumes.	Yes	Only z/OS attached CKD volumes
Help automate setting up volume pairs.	Yes	Yes
Support FlashCopy, MM, GC, GM, MGM, and MT-PPRC.	Yes	Only MM HyperSwap for HA (no DR) and FlashCopy

Feature	CSM for z/OS	CSM for z/OS Basic
Monitor replication progress.	Yes	Yes
Provide email and SNMP alerts.	Yes	Yes
Support practice volumes.	Yes	No
Support consistency groups.	Yes	Only one Basic HyperSwap session
Support AIX Open HyperSwap.	Yes	No
Support z/OS HyperSwap or Hardened Freeze management.	One HyperSwap and multiple Hardened Freeze functions per sysplex	One Basic HyperSwap session within a sysplex
Support in-band IBM FICON® commands.	Yes	Yes
Supported server operating system.	z/OS	z/OS
Entitled for distributed CSM Server installation image	Yes	No

For more information about the differences between z/OS HyperSwap and Basic HyperSwap, see 1.3.1, “z/OS HyperSwap: Not so basic anymore” on page 8.

Both CSM V6.2.x for z/OS versions also include the following no charge products:

► IBM Copy Services Manager FlashCopy Manager for IBM Z®

The CSM FlashCopy Manager is a z/OS ISPF utility that integrates FlashCopy processing into z/OS batch processing. It is a stand-alone utility that does not require CSM, but is supported by any of the CSM for z/OS versions.

– CSM Program Number 5698-E01, 5698-E02:

- FMID HIWN62G (CSM V6.2.x bundled)
- FMID HIWN62I (CSM V6.2.3 bundled)

► IBM Copy Services Manager DSCLI for IBM Z

The CSM DSCLI is the DS8000 DSCLI that can be installed in z/OS UNIX System Services. It is the same Java application as DSCLI for distributed platforms. It is a stand-alone utility that does not require CSM, but it is supported by any of the CSM for z/OS versions.

– CSM Program Number 5698-E01, 5698-E02:

- FMID HIWN62E (CSM V6.2.x bundled)
- FMID HIWN62J (CSM V6.2.3 bundled)

For more information about these products, see [IBM Knowledge Center](#).

1.2.2 CSM licenses for distributed server platforms

CSM V6.2.x can be licensed for installation on a distributed platform through any of the following programs:

- ▶ IBM Copy Services Manager licensed from IBM Passport Advantage® (5725-Z54):
 - Entitled for installation on any distributed server platform.
 - Entitled to activate a preinstalled CSM server on a DS8880 HMC.
 - Licensed per TB Value Units for replicated source capacity.
 - Enablement through a license key compressed file from Passport Advantage. Enablement on DS8880 HMC requires that you extract a key string from the license key compressed file.
- ▶ IBM Copy Services Manager through DS8880 Advanced Function (5641-CSM)
 - Entitled to activate a preinstalled CSM server on a DS8880 HMC.
 - Licensed per TB Value Units for replicated source capacity,
 - Enablement through a data storage feature activation (DSFA) key on the configured DS8880 storage system.
- ▶ IBM Copy Services Manager through IBM Spectrum™ Control or VSC entitlement:
 - Entitled for installation on any distributed server platform.
 - *No entitlement* for a preinstalled CSM server on a DS8880 HMC.
 - Licensed per TB Value Units for managed IBM Spectrum Control™ capacity.
 - Enablement through a CSM license key compressed file from Passport Advantage.

Depending on the license order mechanism, you have different methods to enable the CSM server on a distributed platform. After the CSM server is enabled, other CSM servers can be enabled with the same key if the total source terabytes that are replicated across all primary CSM servers (not counting standby servers) is covered by the TB Value Units that were purchased. By using the CSM GUI *Advanced Tools* panel, you can export the license key.

This method provides flexibility to enable a standby CSM server on any other distributed platform. The license that is exported can either be a license compressed file or a key string, depending on the platform where the enabled CSM server is running.

CSM on a DS8880 HMC cannot be enabled through a license compressed file. It can be enabled only by a CSM license key string or by a DS8880 DSFA key that must be applied through the DS8000 GUI or DSCLI. For more information about DSFA, see [Data storage feature activation](#).

If the CSM license order mechanism provides only a CSM license compressed file (csm-license.zip), you must convert it to a CSM key string to activate CSM on the DS8880 HMC. For more information, see [IBM Knowledge Center](#).

None of these CSM distributed platform licenses are entitled to obtain a CSM for z/OS installation image. However, independent of the server platform where CSM is running, CSM can manage CKD and FB storage devices from any of the CSM supported storage systems.

Additionally, z/OS HyperSwap or Hardened Freeze can be managed from any distributed CSM server platform after a z/OS IP host connection is configured. With this flexibility, you can select a suitable CSM license based on the required implementation topology, as described in 2.3, “Implementation scenarios” on page 27.

1.3 z/OS HyperSwap overview

IBM invented the HyperSwap technology. HyperSwap was first shipped with the full-function GDPS/PPRC HyperSwap solution in 2002 and with the GDPS/PPRC HyperSwap Manager subset solution in 2005. The IBM GDPS Metro HyperSwap Manager (formerly known as GDPS/PPRC HM) and full-function GDPS Metro (formerly known as GDPS/PPRC) offerings provide continuous availability and Disaster Recovery solutions for single-site and multiple-site z/OS, IBM z/VM®, and Linux on System z environments.

z/OS HyperSwap was first introduced in April 2008 on z/OS V1.9 with specific APARs and managed by Tivoli Storage Productivity Center for Replication V3.4. Initially, this was a single-site solution that provided an HA capability for disk storage failures.

This single-site solution was supported by Tivoli Storage Productivity Center for Replication with a specific session type called *Basic HyperSwap*. Therefore, z/OS HyperSwap was often referred to as Basic HyperSwap, and also to distinguish the solution capabilities from the full-function GDPS HM offerings.

1.3.1 z/OS HyperSwap: Not so basic anymore

z/OS HyperSwap became a standard component of the z/OS Input/Output Supervisor (IOS) with z/OS 1.10. Since then, many enhancements were made to the z/OS HyperSwap component and new session types were introduced in Tivoli Storage Productivity Center for Replication to use the z/OS HyperSwap enhancements. The full z/OS HyperSwap capabilities are also supported in CSM, which replaced Tivoli Storage Productivity Center for Replication at the end of 2015.

Afterward, further enhancements were made to support z/OS HyperSwap in 3-site and even 4-site replication topologies. The latest enhancement in CSM V6.2.3 is z/OS HyperSwap support in a new session type called *MM - GM with Site 4 replication*. The major differences between the original Basic HyperSwap solution and the full z/OS HyperSwap solution are listed in the sections that follow.

z/OS Basic HyperSwap features

The following features are available in z/OS Basic HyperSwap:

- ▶ Single-site HA solution that extends IBM Parallel Sysplex® HA capabilities to HA capabilities of storage devices.
- ▶ It is not a DR solution. It is not designed to handle MM link failures that can occur in cross-site configurations and does not guarantee consistent MM secondary devices for DR.
- ▶ It is offered as a no additional charge license through IBM Copy Services Manager for z/OS Basic Edition (5698-E02).

z/OS HyperSwap features

The following features are available in z/OS HyperSwap:

- ▶ HA solution that extends IBM Parallel Sysplex HA capabilities to the availability capabilities of storage devices in 2-, 3-, or 4-site DR configurations:
 - Two-site MM topologies
 - Three-site multi-target MM - MM topologies
 - Three-site multi-target and cascaded MM - GM topologies
 - Four-site MM - GM with site 4 replication session

- ▶ It provides DR capabilities and maintains consistent MM secondary devices for recovery after rolling disaster situations.
- ▶ It is supported by any of the chargeable licenses of CSM listed in 1.2, “CSM licenses” on page 5.

In this book, we usually refer to the full z/OS HyperSwap solution when we describe HyperSwap capabilities and usage. When we use the term *Basic HyperSwap*, we refer to the specific original solution and special CSM session type Basic HyperSwap.

1.3.2 CSM sessions that support HyperSwap

CSM supports z/OS HyperSwap with many session types. The following list provides an overview of supported sessions with IBM DS8000 storage systems as of CSM V6.2.3:

- ▶ Basic HyperSwap (two sites):
 - Basic HyperSwap H1-H2
 - Pure HA solution, no DR support
- ▶ MM Failover/Failback (two sites):
 - HyperSwap H1-H2
- ▶ MGM (three sites, cascaded):
 - HyperSwap H1-H2
- ▶ MGM with Practice (three sites, cascaded):
 - HyperSwap H1-H2
- ▶ MM - MM (three sites, multi-target):
 - HyperSwap H1-H2
 - HyperSwap H1-H3
 - HyperSwap H2-H3
- ▶ MM - GM (three sites, multi-target):
 - HyperSwap H1-H2
- ▶ MM - GM with Practice (three sites, multi-target):
 - HyperSwap H1-H2
- ▶ MM - GM with Site 4 replication (four sites, regional HA protection capabilities):
 - HyperSwap H1-H2
 - HyperSwap H3-H4

1.3.3 z/OS HyperSwap functions

z/OS HyperSwap is part of the IOS component of z/OS. It can be configured through CSM, which controls the HyperSwap session configuration; the PPRC path and pair management; and the communication to the HyperSwap Manager address space.

z/OS HyperSwap supports one active HyperSwap configuration within a sysplex. This configuration can support a 2-site MM topology, but also a 3-site multiple target MM-MM topology with HyperSwap capability between any of the three sites. All primary volumes in the HyperSwap configuration are monitored for freeze triggers and HyperSwap triggers.

Additionally, the z/OS HyperSwap Manager supports multiple *MM configurations* for Hardened Freeze. An MM configuration for Hardened Freeze can support 2-site MM

topologies and 3-site multi-target MM-MM topologies. Loaded MM configurations are only monitored for freeze triggers on the primary volumes. Whenever a freeze trigger is hit, the HyperSwap Manager performs the Hardened Freeze sequence for the affected MM configuration and purges the configuration afterward.

The Hardened Freeze sequence consists of a freeze and optional unfreeze operation for the involved logical control unit (LCU) pairs. I/O may continue on primary devices after an unfreeze operation or after the Extended Long Busy (ELB) condition from the freeze expires (the default is 2 minutes). This situation results in consistently suspended MM pairs, which allows manual failover capabilities in rolling disaster failure scenarios.

The HyperSwap Manager monitors the loaded HyperSwap configuration for HyperSwap triggers. Whenever a HyperSwap trigger is hit, the HyperSwap Manager performs a HyperSwap sequence, which implicitly includes the Hardened Freeze sequence. The HyperSwap sequence is explained in more detail in 1.3.4, “HyperSwap sequence” on page 11.

Figure 1-2 illustrates the I/O flow before and after a HyperSwap.

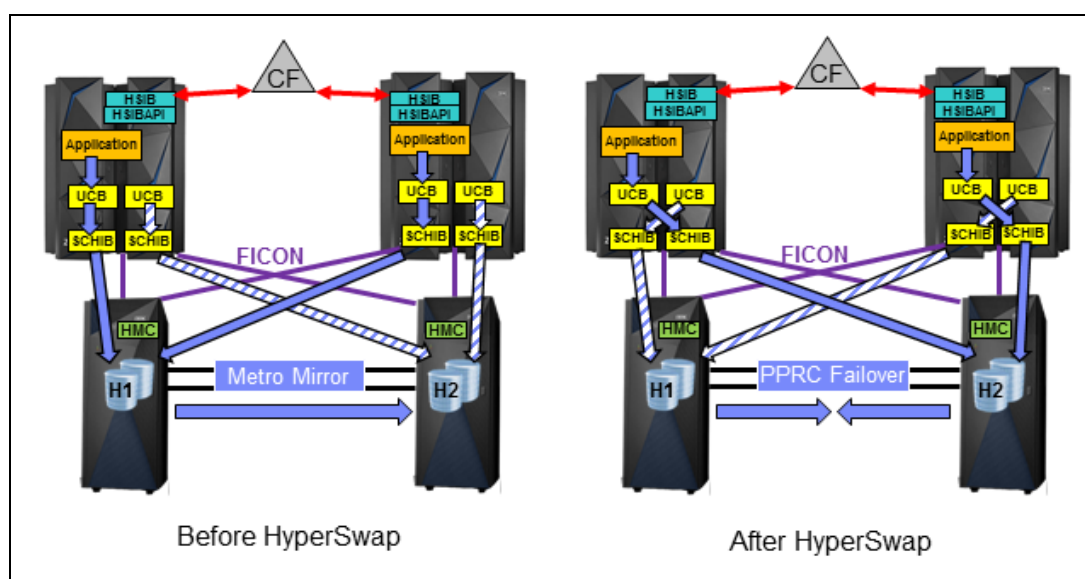


Figure 1-2 I/O flow before and after a HyperSwap

On the left, we see applications running in z/OS logical partitions (LPARs) on either site. They access their volumes through a z/OS control block that is called a *Unit Control Block* (UCB). Every device in z/OS is represented by a unique UCB. Each UCB in turn points to another control block called a *Sub-Channel Information Block* (SCHIB) that is used to communicate with the I/O device. In normal operation, the UCBs point to the primary devices that are in the MM Full Duplex state with the secondary devices.

On the right, we see the result of a HyperSwap operation. The UCB pointer to the SCHIB representing the primary device is changed to point to the SCHIB representing the secondary device. This situation is often referred to as *UCB swap*, which is a transparent operation for any application working with z/OS volume identifiers/labels (*volser*).

Note: If there are system applications in use that depend on device addresses, they might not be compatible with the HyperSwap operation and fail to access the device after a HyperSwap.

After a HyperSwap, both storage devices are in a *PPRC Failover state* and the PPRC state for both devices shows as *MM Primary Suspended*. Both devices enabled a change recording bitmap to mark each changed track on either site to support an incremental resynchronization at a later point.

We describe the implementation of z/OS HyperSwap in detail in Chapter 6, “Implementing z/OS HyperSwap” on page 97.

Note: After a HyperSwap and before data replication is restarted, the old primary devices can potentially be accessed for I/O, although they contain invalid data. z/OS HyperSwap provides mechanisms to prevent this situation, but you might have to take special care in nonstandard situations. For more information, see 6.2.4, “Sharing volumes with systems outside the Sysplex” on page 101.

1.3.4 HyperSwap sequence

A planned or unplanned HyperSwap sequence consists of multiple steps that are called *phases*. Here is a detailed description for each of the phases:

1. Phase: Validate I/O connectivity.

In this phase, z/OS checks connectivity to the secondary devices. If all LPARs have connectivity to their secondary devices, then HyperSwap proceeds. If one or more LPARs fail the connectivity check, the action that HyperSwap does depends on the HyperSwap options that you specified in the CSM session properties:

- If you chose to *Partition the systems out of the Sysplex* upon a HyperSwap error, every system failing connectivity validation enters a 0B5 wait state code and is partitioned out of the sysplex. HyperSwap proceeds on the remaining LPARs (this is the default setting for *unplanned* HyperSwap errors).
- If you chose to *Disable HyperSwap* upon a HyperSwap error, the HyperSwap operation is backed out. Depending on the type of disk failure, it can lead to a sysplex outage (this is the default setting for *planned* HyperSwap errors).

2. Phase: Freeze primary storage devices and quiesce DASD I/O to volumes.

In this phase, z/OS sends freeze commands to all of the logical subsystem (LCU) pairs that are defined in the HyperSwap session. As a result of the freeze, the storage system removes all logical PPRC paths between the frozen LCU pairs, and all affected primary PPRC devices in these LCUs enter an ELB state, which prevents further write I/O. Additionally, z/OS stops issuing I/O to any primary device in the HyperSwap configuration.

3. Phase: Fail over PPRC (MM) pairs.

In this phase, z/OS sends PPRC failover commands to all device pairs that are defined in the HyperSwap session. The PPRC status for the former secondary devices changes from *Secondary Full Duplex* to *Primary Suspended*. This status enables the I/O capability to the former secondary devices.

4. Phase: Swap UCBs to redirect volumes to auxiliary storage devices.

In this phase, all z/OS LPARs in the sysplex swap certain contents of their UCB pairs to point to the former secondary devices.

5. Phase: Resume DASD I/O to volumes.

In this phase, z/OS resumes I/O requests to the volume UCBs (that are now pointing to the former secondary devices). When this step is complete, the system and all applications resume normal I/O activity.

6. Phase: Perform a Soft-Fence action on all the primary storage devices.

In this phase, z/OS tries to perform a Soft-Fence of the former primary devices on the storage system. A Soft-Fenced device does not allow any I/O. This behavior is extra integrity protection to prevent I/O to obsolete devices after the ELB condition is removed.

If devices are shared with external LPARs outside the sysplex, they are not aware when a HyperSwap occurred and potentially might continue to work with obsolete volume content. A Soft-Fence action prevents such a scenario and an accidental IPL from the old primary devices. Soft-Fence is a storage controller feature. If the storage controller does not support Soft-Fence, this phase completes without any tasks.

7. Phase: Unfreeze primary storage devices.

This is an optional step that depends on the CSM session *MM Suspend Policy*. It has two policies:

- *Hold I/O after Suspend*: This policy corresponds to the HyperSwap session console status *Stop: Yes*. It means that the unfreeze action will *not* be performed. The ELB condition remains active on the former primary devices until their ELB timeout expires (the default is 2 minutes). This policy is also called the *Freeze & Stop policy*.
- *Release I/O after Suspend*: This policy corresponds to the HyperSwap session console status *Stop: No*. It means that the unfreeze action will be performed, which removes the ELB condition immediately from the former primary devices. This is the default MM Suspend Policy for all CSM session types. It is also called the *Freeze & Go policy*.

Note: The MM Suspend Policy is applied during HyperSwap processing and Hardened Freeze processing, but the Hardened Freeze does not require a HyperSwap.

8. Phase: Clean up activities.

In this phase, z/OS tries to release RESERVEs that are outstanding on the old primaries and perform other cleanup tasks.

9. Phase: Purge the HyperSwap configuration.

Purges the HyperSwap configuration. This step prevents more HyperSwap or freeze triggers from causing unwanted actions before replication from the new primary devices is reestablished and a new configuration is loaded and activated.

1.3.5 Planned and unplanned HyperSwap

A HyperSwap operation can be planned or unplanned.

Planned HyperSwap

The planned HyperSwap function provides the following capabilities:

- ▶ Transparently switch all UCBs of the primary PPRC disk devices to point to the secondary PPRC disk devices to redirect I/O transparently to applications.
- ▶ Perform storage system maintenance and planned site maintenance without requiring any applications to be quiesced.
- ▶ Perform periodic testing of the HyperSwap function.
- ▶ Perform PPRC based data migration from old to new disk storage systems and perform transparent I/O redirection to a new storage controller without application downtime.

Planned HyperSwaps are usually initiated through CSM by the **HyperSwap** session command, or alternatively by the **SETHS SWAP IBM MVS™** command.

Unplanned HyperSwap

The unplanned HyperSwap function can transparently redirect I/O to use secondary PPRC devices if there are unplanned outages of the primary PPRC disk devices. The unplanned HyperSwap function keeps production systems active during a primary disk storage system failure.

An unplanned HyperSwap is triggered by the following conditions:

- ▶ Any disk storage system condition that can cause a permanent I/O error to be returned to the application.
- ▶ The channel subsystem in the IBM Z processor detects that it no longer has a path to a primary disk device.
- ▶ The z/OS system command **SETIOS HYPERSWAP** can be used to trigger an unplanned HyperSwap for test purposes.

The execution sequences of a planned or unplanned HyperSwap are similar.

Note: CSM is not involved in triggering unplanned HyperSwaps, and it is not required for the execution of the HyperSwap sequence.

Event triggers

The sequence of events to trigger an unplanned HyperSwap operation is as follows:

1. An application sends an I/O request to a disk volume.
2. The underlying disk device or the channel subsystem returns a permanent I/O error or a *No path available* status to z/OS.
3. z/OS routines that monitor I/O activity determine that this event is a HyperSwap trigger and send an event notification (ENF Signal) to the HyperSwap management address space within the Sysplex that is acting as the HyperSwap master to let it know that a HyperSwap trigger was detected.
4. At this point, the HyperSwap begins.

The duration for detecting an I/O error or missing paths might vary. The I/O and path recovery times can be reduced to minimize the duration until an unplanned HyperSwap is triggered. For more information, see 6.2.7, “Reduce delays of HyperSwap triggers” on page 107.

1.4 CSM and HyperSwap communication flow

CSM provides the configuration interface for z/OS HyperSwap and manages MM replication, and z/OS HyperSwap monitors I/O for HyperSwap or freeze events autonomously after it has a configuration that is loaded by CSM. To load a configuration, you must define CSM sessions that include an MM role pair that can be enabled for either HyperSwap or Hardened Freeze. After the CSM session starts and all MM pairs reach a *Full Duplex* state (the *Prepared* state in CSM), CSM loads the MM pair configuration in the z/OS HyperSwap Manager.

After the HyperSwap Manager receives the configuration, it validates the devices and PPRC states across all LPARs in the sysplex and activates HyperSwap (or Hardened Freeze) for the loaded configuration. After a configuration is active, the z/OS HyperSwap Manager can autonomously react on freeze and HyperSwap events, even if communication to the active CSM server is lost. The z/OS HyperSwap Manager can react only once to an event for each loaded configuration. After the required PPRC actions are performed, for example, freeze/unfreeze or HyperSwap, the affected configuration is purged.

Afterward, all MM relationships stop replication (*MM Suspended* state) and CSM must either resume or fail back the suspended MM relationships and reload the configuration into z/OS HyperSwap Manager again after all MM pairs regain the *Full Duplex* state.

If a CSM session has a HyperSwap or Hardened Freeze configuration loaded, CSM also continuously polls the status of the HyperSwap Manager. If there are unexpected changes, it changes the CSM session state. Based on such a state change, it can also send alerts through email and SNMP to notify operations of an issue or a HyperSwap occurrence.

1.5 GDPS Metro solutions

z/OS HyperSwap that is managed by CSM provides a solution for disk storage HA and DR in the sysplex. However, it does not integrate advanced sysplex maintenance, recovery tasks, or system automation as in the various GDPS Metro offerings.

Generally, CSM and z/OS HyperSwap are suited for environments that need HA and DR for z/OS disk storage devices without requiring deeper sysplex management and availability integration. In contrast, the various GDPS Metro offerings can provide sophisticated sysplex availability and recovery automation for z/OS platforms, and for z/VM and Linux on IBM Z on various storage devices.

Table 1-2 shows some of the key criteria of GDPS -managed HyperSwap solutions and z/OS HyperSwap that is managed by a fully entitled CSM server.

Table 1-2 GDPS Metro and z/OS HyperSwap key criteria

Features	GDPS Metro ^a	CSM z/OS HyperSwap
Provides fast swapping of UCBs that is transparent to applications	Yes	Yes
Code hardened to avoid hangs (page faults or locks)	Yes	Yes
Failure management provided by	GDPS	z/OS
FlashCopy support	Yes	Not integrated in HyperSwap managed relationships
zGM (XRC) support	Yes, including incremental resync	Tolerated, but no incremental resync support
IBM DS8000 Easy Tier® Heat Map Transfer (HMT) utility	Yes	Yes
Sysplex availability management (Couple Data sets)	Yes	No
Requires an active LPAR at a remote recovery site	Yes (GDPS controls the LPAR.)	No (The CSM server can run on any platform, for example, DS8880 HMC)
Automated recovery	Yes (Full system-level automation)	No (PPRC Recovery must be manually triggered if it is not part of HyperSwap; there is no system level management.)
Management scope	LPAR management, remote IPL, Sysplex resources, disk, and tape	Disk storage only

Features	GDPS Metro ^a	CSM z/OS HyperSwap
User interfaces	ISPF panels, web GUI, and TSO commands	CSM web GUI, CSMCLI, and MVS commands
Cost	Service offering	Basic HyperSwap: CSM for z/OS Basic Edition - no charge ^b z/OS HyperSwap: CSM licensed edition on any server platform - charge
Platforms supported	z/OS, z/VM, and Linux on IBM Z	z/OS
Storage systems supported	IBM, EMC, and HDS in PPRC mode	IBM, and HDS in PPRC mode
Disk devices	CKD and FB	CKD
Software required	System automation IBM NetView®	CSM (includes IBM WebSphere® Liberty)

a. GDPS has adopted new namings starting with Version 4.1 - refer to Figure 1-3

b. "IBM Copy Service Manager for z/OS Basic Edition" is a no-charge disk availability only solution that supports only one Basic HyperSwap session.

For reference, Figure 1-3 shows the renaming of GDPS related offerings.

Former name	New name full	New name short
GDPS/PPRC HM	GDPS Metro HyperSwap Manager	GDPS HM
GDPS/PPRC	GDPS Metro	GDPS Metro (single leg)
GDPS/MTMM	GDPS Metro	GDPS Metro (dual leg)
GDPS/XRC	GDPS Global – XRC	GDPS XRC
GDPS/GM	GDPS Global – GM	GDPS GM
GDPS/MzGM	GDPS Metro Global – XRC	GDPS MzGM
GDPS/MGM	GDPS Metro Global – GM	GDPS MGM
GDPS/Active-Active	GDPS Continuous Availability	GDPS AA
GDPS Virtual Appliance	GDPS Virtual Appliance	GVA

Figure 1-3 GDPS offerings new names (starting with Version 4.1)

1.6 IBM Resiliency Orchestration and CSM

In 2016, IBM announced the [acquisition of Sanovi Technologies](#).

The addition of this orchestration technology to the IBM resiliency portfolio enables an increased ability to help simplify and automate general DR processes; manage recovery workflows; and reduce recovery time, operating costs, and DR drill testing time. The outcome was the release of the IBM Resiliency Orchestration product, which is shown in Figure 1-4 on page 16.

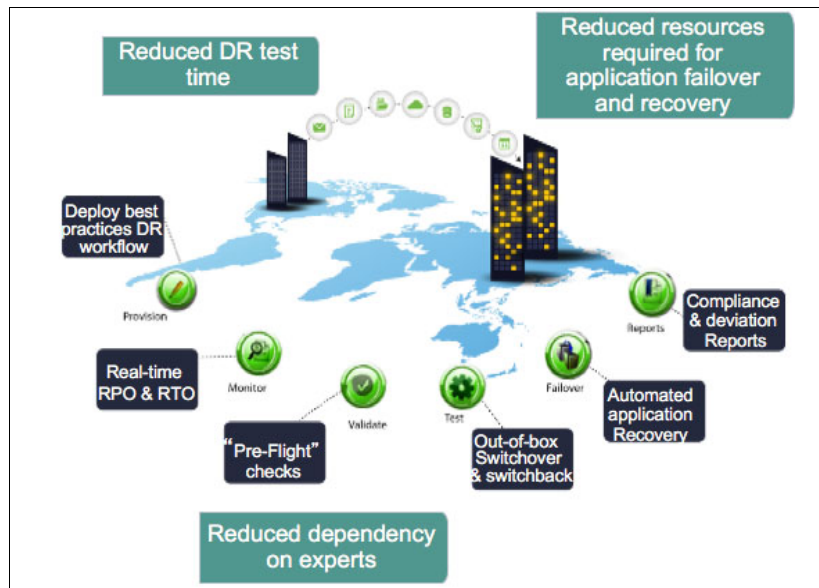


Figure 1-4 IBM Resiliency Orchestration

At the beginning of 2018, IBM Resiliency Orchestration V7.2 SP2 was released, which combines the expertise of CSM with the experience of Resiliency Orchestration. Starting with Version 7.2 SP2, IBM Resiliency Orchestration provides z/OS LPAR protection by using CSM to support the following features:


- ▶ Monitoring (Data RPO, RTC, Datalog, and Replication)
- ▶ Switchover
- ▶ Switchback
- ▶ Failover Test Exercise
- ▶ Failover

IBM Resiliency Orchestration provides workflows for IBM Z with its z/CMD command processor. Using these workflows, you can communicate with your z/OS systems by using any of the following methods:

- ▶ z/OS console commands
Any z/OS command or JES command can be run by using an *IBM RO* workflow.
- ▶ TSO commands
Any TSO command can be run.
- ▶ REXX, CLIST, and etc commands
An interface to run REXX, CLIST, or similar processes
- ▶ Batch Job interface
This interface enables workflows to submit batch jobs and have their output examined for specific condition codes.

The results from the previous commands, scripts, or job condition codes can all be returned to the Disaster Recovery Management server for more workflow development and actions. By combining the z/CMD workflows with CSM replication management, customers can build an end-to-end solution for their DR needs. For more information, see the following resources:

- ▶ [Automating Your Disaster Recovery Environment with IBM Resiliency Orchestration and CSM](#)
- ▶ [IBM Resiliency Orchestration](#)



IBM Copy Services Manager and IBM z/OS HyperSwap implementation topologies

This chapter provides an overview of various implementation and connection topologies for IBM Copy Services Manager (CSM). It also describes how z/OS HyperSwap can optionally be integrated to manage high availability (HA) of Count Key Data (CKD) devices. The chapter explains the various CSM server connection types to storage systems and to z/OS logical partitions (LPARs) and provides implementation examples to describe their advantages and limitations.

2.1 CSM connection type overview

A CSM server can manage various types of copy services for a wide range of storage systems. CSM supports Fixed Block (FB) storage devices and can also manage copy services for enterprise storage systems that support CKD devices of type 2105/2107. To manage CKD devices, CSM uses TCP/IP connections to the IBM storage system management interface, for example, the DS8000 Hardware Management Console (HMC).

Additionally CSM can manage IBM and Hitachi Virtual Storage Platform (VSP) CKD devices through a FICON connection with a z/OS LPAR, which has the CKD devices defined in its I/O configuration. With a FICON connection, the CSM server communicates through the z/OS Input/Output Supervisor (IOS) to the back-end storage controller to query the device status and to send copy services commands through *Channel Command Words*.

When using a FICON connection, CSM does not need to be installed on the z/OS LPAR, but CSM may be connected to the LPAR through a z/OS IP host connection that can be configured on the LPAR and on the CSM servers.

Here are more details for the two different types of storage system connections that CSM servers can use to manage CKD storage devices:

- ▶ TCP/IP-based storage system connections

CSM communicates with storage systems through their native TCP/IP-based storage system interface. For DS8000 storage systems, CSM connects to the DS8000 HMC to manage all existing storage devices. A TCP/IP-based storage system connection is mandatory if FB devices of any of the supported enterprise storage systems must be managed by CSM.

- ▶ FICON based storage system connections

CSM can use the FICON channel to communicate to storage systems by using a *z/OS Direct Connection*. By using this connection, CSM manages the CKD storage devices that are defined on z/OS LPARs that are used by CSM as a communication proxy. CKD devices of type 2105/2107 can be managed with this method for the following storage systems:

- IBM DS8000 storage systems (all models)
- Hitachi VSP / VSP G1000

A z/OS Direct Connection (FICON) can be defined if either of the following requirements is met:

- The CSM server is running on a z/OS LPAR and connected to the IOS through an embedded *z/OS native Host Connection*.
- The CSM server is connected to a z/OS LPAR through a *z/OS IP Host Connection*.

A z/OS Direct Connection (FICON) to manage CKD devices is required if there is no TCP/IP-based storage system connection. It is best practice to always define a FICON based storage system connection for management of CKD devices because of the following reasons:

- It provides CSM with a redundant communication path for copy services management on CKD devices.
- It is the preferred channel for the CSM server to communicate to manageable LCUs.
- It provides better performance for copy services management than the IP-based storage system communication channel.

Apart from storage system connections, CSM servers also support *z/OS Host Connections* to communicate to the z/OS IOS and the HyperSwap Manager.

A z/OS Host Connection can either be a z/OS native Host Connection (Java Native Interface (JNI)), if CSM is running on a z/OS LPAR, or a z/OS IP Host Connection between the CSM servers and external z/OS LPARs.

z/OS Host Connections are used for the following purposes:

- ▶ Enables CSM servers to establish a FICON-based storage connection to manage copy services of FICON attached storage devices of a z/OS LPAR.
- ▶ Enable CSM servers to manage z/OS HyperSwap or Hardened Freeze of a connected sysplex.

Although a z/OS native Host Connection is limited to the z/OS LPAR where the CSM server is running, a z/OS IP Host Connection can be established to any z/OS LPAR. This capability allows any type of CSM server to manage CKD devices and HyperSwap of any or multiple sysplexes. It provides a lot of implementation flexibility because the CSM servers can be running on a distributed server platform or on an IBM DS8880 HMC but still manage CKD devices or HyperSwap.

The following sections explain the various storage and host connection types in more detail.

2.1.1 TCP/IP-based connections to storage systems

CSM servers use a TCP/IP connection to communicate to the management interfaces of supported IBM storage systems. Depending on the type of the storage system, it might be an authenticated connection to the HMCs (DS8000 storage system) or to the storage controllers directly (Storwize family, SVC, XIV, or IBM FlashSystem systems). To establish an authenticated connection, you must have a user account on the storage system that has sufficient privileges to manage copy services or other tasks that should be controlled by the CSM servers.

A TCP/IP storage system connection is optional for z/OS storage device management (CKD devices), but it is mandatory for FB storage device management or other advanced DS8000 features that can be managed by CSM:

- ▶ DS8000 Easy Tier HMT utility
- ▶ DS8000 Metro Mirror (MM) Heartbeat
- ▶ DS8880 Safeguarded Copy (This is a temporary restriction until z/OS APAR OA56173 is implemented to support Safeguarded Copy management through a FICON connection.)

Note: If the password of the CSM user expires on the connected storage system, the storage system is disconnected. You cannot change the password through CSM directly. The password for the CSM user account must be changed on the storage system itself and afterward it must be updated in the properties of the affected TCP/IP-based CSM storage system connection.

2.1.2 FICON based connections to storage systems

A FICON based storage system connection can be established to either IBM DS8000 or Hitachi VSP storage controllers. These controllers must have 2105/2107-based CKD devices that are defined on the z/OS LPAR that is either running the CSM server or connected to an external CSM server through a z/OS IP host connection.

After CSM can communicate with IOS, it can manage copy services for the defined CKD devices even if they are offline to z/OS. The CSM communication to IOS can be either through an internal z/OS native Host Connection (if the CSM server is running on a z/OS LPAR) or through a z/OS IP Host Connection that is established between the CSM server and one or more z/OS LPARs.

After any of these host connections are established, you can add a storage system as a z/OS Direct Connection (FICON) in CSM. During the creation of a z/OS Direct Connection, the CSM server lists the storage systems that are FICON attached to any of the connected z/OS IOS.

Note: FICON based device management works for only CKD devices that are defined to the z/OS LPARs that have an established host connection to the CSM server. Storage devices that are not defined in the LPARs I/O configuration can be managed only through a TPC/IP-based storage system connection.

A FICON based connection provides an additional redundant communication path to manage CKD devices. The FICON based connection is usually the preferred CSM communication channel if multiple connection types exist with the storage device (unless CSM must manage features that are not supported yet over FICON).

Note: CSM does not support TCP/IP-based storage connections to third-party storage controllers. Therefore, Hitachi VSP storage controllers can be attached and managed only with a z/OS Direct Connection (FICON).

A FICON based storage system connection does not require authentication for the CSM server, so there is no password that can expire and cause a connection loss.

Note: If the CSM server is connected to the z/OS LPAR through a z/OS IP host connection, the certificate or the account password that is used for the z/OS IP host connection might expire and cause a host connection loss, which results in a FICON connection loss as well.

In a CSM server HA setup with active and standby CSM servers, all storage and host connection definitions are replicated between the CSM servers. However, each CSM server must be able to establish its connections individually for full management capabilities after a *takeover* on the standby CSM server. Therefore, you must ensure that each of the CSM servers has the connection capability to manage all the required storage devices.

If the primary CSM server runs on z/OS and uses the z/OS Direct Connection (FICON) but the secondary server runs on a remote distributed platform server, you can meet this requirement by using a z/OS IP Host Connection that can be used by the secondary CSM server as a proxy to establish a z/OS Direct Connection (FICON) as well.

Note: It might difficult to meet this requirement if only FICON based connections are used. In such a case, if the standby CSM server is connected to or running on a remote z/OS LPAR, for example, a maintenance LPAR at a cold disaster recovery (DR) site, it might be that this LPAR cannot attach all primary storage devices through a FICON channel.

Although the standby CSM server can still manage primary devices through FICON through the z/OS IP host connection to LPARs of the managed sysplex, it loses this capability if the z/OS IP host connection breaks or the connected LPARs of the sysplex become unavailable.

2.1.3 Host connections to z/OS LPARs

CSM supports two different types of host connections to z/OS LPARs:

- z/OS native host connections

A z/OS native Host Connection is configured and established automatically by CSM servers that are installed on a z/OS LPAR and running in the underlying z/OS Unix System Services. The z/OS native Host Connection cannot be modified or deleted.

The z/OS native Host Connection is also used to communicate to the z/OS HyperSwap application programming interface (API) address space through a JNI communication channel when HyperSwap or Hardened Freeze is managed by a z/OS CSM server within the same sysplex. In that case, there is no TCP/IP involved in the CSM/HyperSwap communication, and no security must be configured for this type of connection.

Note: CSM servers that are running on a distributed platform do not support z/OS native Host Connections. If a CSM server on z/OS replicates the native host connection to a standby server on a distributed platform, the standby server ignores and deactivates this host connection type.

- z/OS IP host connections

A z/OS IP host connection can be configured for CSM servers on any platform. It is a TCP/IP-based connection to a specific z/OS LPAR that must run the HyperSwap address spaces and serve an IP address or host name that can be used for the connection. z/OS IP host connections require authentication, and by default they must also be configured to use encryption. The HyperSwap management address space must be configured with the **SOCKPORT** parameter to allow such authenticated IP connections from CSM servers.

The HyperSwap address spaces are used as proxy to connect CSM to the LPAR IOS to provide a communication path for its FICON device management. Furthermore, the z/OS IP host connection provides a communication path for CSM to manage optionally z/OS HyperSwap or Hardened Freeze of the sysplex where the connected LPAR is running.

Note: A z/OS IP host connection requires that the HyperSwap address spaces (HSIB and HSIBAPI) are active and HSIB is using the **SOCKPORT** parameter to define the port that is used to establish the connection. If encryption is enabled for the z/OS IP host connections (default), the LPAR must also run the PAGENT address space with a loaded Application Transparent Transport Layer Security (AT-TLS) policy that describes the certificates that are used to encrypt and decrypt traffic over the HSIB socket port. For more information, see 2.2, “z/OS relevant address spaces for CSM” on page 25.

Figure 2-1 illustrates the communication flow from an internal CSM server and an external CSM server to FICON attached CKD devices through a z/OS IP host connection and a FICON based storage system connection.

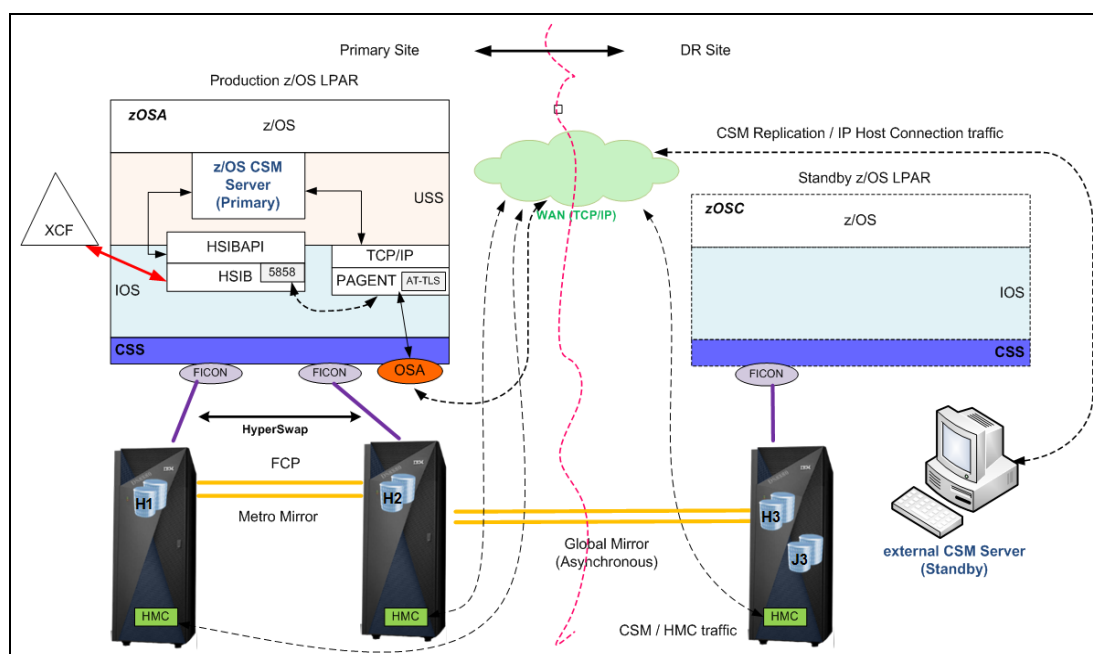


Figure 2-1 IBM z/OS IP host connection and FICON communication flow

It is a best practice to secure the IP host connections by using AT-TLS encryption. By default, this encryption is required by CSM. Optionally, encryption for z/OS IP host connections can be disabled on CSM servers for a simplified setup, or for testing and debugging purposes.

Note: If encryption is used, there are certificates that might expire and cause a connection loss. To avoid such communication losses, certificates should be renewed in time and updated on the LPARs and the CSM servers for the defined z/OS IP host connections.

Each z/OS IP host connection also requires a user ID and password on the LPAR with sufficient authority to use the HyperSwap Manager IP socket connection.

Note: If the password expires or the user is revoked on the LPAR, the z/OS IP host connection fails. CSM does not support changing the host connection password directly. The password must be changed on the z/OS LPAR and then updated in the corresponding CSM z/OS IP host connection properties.

2.2 z/OS relevant address spaces for CSM

CSM can interact with z/OS to manage HyperSwap and Hardened Freeze functions. Furthermore, an external CSM server can connect to the LPAR IOS by using a z/OS IP host connection that uses the HyperSwap address spaces as communication proxy. This section explains all CSM relevant z/OS address spaces and which CSM feature requires them.

2.2.1 HyperSwap or Hardened Freeze address spaces

The following two address spaces are required for z/OS HyperSwap or Hardened Freeze management:

HSIB	This is the HyperSwap Management address space (IOSHMCTL program). It loads and monitors configurations, and coordinates HyperSwap or Freeze management within the sysplex through the Coupling Facility.
HSIBAPI	This is the HyperSwap Management API address space (IOSHSAPI program). It is used to translate the JNI communication from CSM to the HSIB address space. It is required for full HSIB functionality.

Both of these address spaces must be active on each LPAR in the sysplex. You can accomplish this task by adding simple procedures to SYSx.PROCLIB, and then issuing **START procmemname** commands manually, or by including the commands in the COMMNDxx member of your SYSx.PARMLIB. The start commands for these procedures are shown in Example 2-1.

Example 2-1 Starting HyperSwap address spaces

```
START HSIBAPI,SUB=MSTR
START HSIB,SUB=MSTR
```

It does not matter in which order you start or stop both address spaces. However, HSIB is not ready until HSIBAPI is active. If you start HSIB first, you might see the IOSHM0500E error in the syslog, as shown in Example 2-2.

Example 2-2 HyperSwap Manager address space not ready error

```
N 4000000 SYSTEM1 18143 09:03:24.43 STC00035 00000010 *IOSHM0500E HyperSwap API
address space not started
N 8000000 SYSTEM1 18143 09:03:24.46 STC00035 00000010 *IOSHM0803E HyperSwap
Disabled
```

After both address spaces are active, you should see the IOSHM0807I message that is shown in Example 2-3.

Example 2-3 Successful start of the HyperSwap address spaces

```
N 4000000 SYSTEM1 18143 09:03:24.46 STC00035 00000010 IOSHM0807I HyperSwap
Management Address Space ready
```

2.2.2 z/OS IP host connection relevant address spaces

The following z/OS address spaces are required for a (secure) z/OS IP host connection from an external CSM server:

HSIB	This is the HyperSwap Management address space (IOSHMCTL program) with the SOCKPORT parameter. It is required as a communication proxy between external CSM servers and z/OS IOS.
HSIBAPI	This is the HyperSwap Management API address space (IOSHSAPI program). It is used to translate the JNI communication from CSM to the HSIB address space. It is required for full HSIB functionality.
BHIHSRV	This is the HyperSwap Socket Server address space (IEESYSAS program). It is internally managed by HSIB and started for each established z/OS IP host connection. It controls the socket connection to the specific CSM server.
PAGENT	This is the z/OS Communication Server Policy Agent address space. It is required for AT-TLS and provides encryption and decryption capabilities and filtering capabilities for TCP/IP traffic. It is used to secure all traffic through the z/OS IP host connection.

When HSIB with the **SOCKPORT** parameter is active on an LPAR, it listens for incoming connection requests from an authenticated CSM server on the defined socket port. HSIB requires the HSIBAPI address space for full functionality and for converting the JNI communication from the CSM servers. Both are required even if no HyperSwap or Hardened Freeze configuration is loaded.

After the z/OS IP host connection is established, HSIB starts an internally managed BHIHSRV address space (IEESYSAS) that controls the established TCP/IP socket connection. A separate BHIHSRV address space is started for each z/OS IP host connection.

The PAGENT address space is required to use AT-TLS policies for encryption of the z/OS IP host connection. After PAGENT is active with the proper policy definition, it applies the defined certificates to intercept and encrypt any TCP/IP traffic through the defined HSIB socket port. Figure 2-1 on page 24 illustrates the communication flow through the various address spaces.

2.2.3 z/OS CSM Server relevant address spaces

If CSM is running on z/OS, the following address spaces are relevant:

IWNSRV	This address space hosts WebSphere Liberty Profile and the CSM server application running in Unix System Services.
IWNAUTH	This optional address space hosts the CSM authentication server application running in Unix System Services. It is required only if the CSM LDAP authentication service is required. This is the case if CSM or DS8000 HMC users are authenticated through an LDAP server.

Both address spaces start as started tasks. For more information about how to configure the IWNSRV and IWNAUTH jobs and started tasks, see [IBM Knowledge Center](#).

For an example of how to configure these started tasks, see 4.2.4, “Create started tasks for CSM server” on page 62.

2.2.4 Summary of relevant z/OS address spaces

Table 2-1 summarizes the required z/OS address spaces depending on the required implementation options.

Table 2-1 CSM relevant z/OS address space summary

Implementation option	z/OS address spaces	Where to run
z/OS HyperSwap or Hardened Freeze	HSIB	On each LPAR in the sysplex.
	HSIBAPI	On each LPAR in the sysplex.
z/OS IP host connection (unsecure)	HSIB	On the LPAR that is used for the z/OS IP host connection. Requires the SOCKPORT parameter.
	HSIBAPI	On same LPAR as HSIB
	BHIHSRV (IEESYSAS)	Managed internally by HSIB on the same LPAR (one starts for each z/OS IP host connection to the LPAR).
z/OS IP host connection (encrypted)	HSIB	On the LPAR that is used for the z/OS IP host connection. Requires the SOCKPORT parameter.
	HSIBAPI	On the same LPAR as HSIB.
	BHIHSRV (IEESYSAS)	Managed internally by HSIB on the same LPAR (one starts for each z/OS IP host connection).
	PAGENT	On the LPAR that is used for the z/OS IP host connection. Requires an AT-TLS policy file, and certificate and keyring.
CSM server on z/OS	IWNSRV	On the LPAR hosting the CSM server.
	IWNAUTH	On the same LPAR as IWNSRV if CSM LDAP Authentication Service is required.

2.3 Implementation scenarios

This section describes various implementation scenarios covering various replication topologies. The listed implementation options, their advantages, and their limitations might help to evaluate the most appropriate CSM implementation scenario to meet your requirements and service level agreements. They might also help to identify the required CSM license type, as described in 1.2, “CSM licenses” on page 5.

2.3.1 General considerations for all implementation scenarios

While you are planning the best CSM implementation scenario for your environment, there are some common considerations:

- ▶ If you implement CSM on z/OS, the CSM Authentication Server address space is an optional service that can be started, with the CSM Server address space on the same z/OS LPAR. The CSM Authentication Server provides LDAP-based authentication for CSM users or DS8000 HMC users. If the CSM Authentication Server is being used, it needs an IP connection with the LDAP servers.

Note: If you install the z/OS CSM server on z/OS ZFS/HFS volumes that are part of a CSM managed MM configuration, make sure to enable either Hardened Freeze or HyperSwap for this session.

If Hardened Freeze or HyperSwap is enabled, the freeze and unfreeze is processed by the HyperSwap address spaces. Otherwise, the CSM server must perform the freeze and unfreeze sequence itself and might freeze its own processing:

- This situation can occur upon unplanned freeze triggers (for example, a suspended primary MM device) or when you issue a **Suspend** command to the CSM session.
 - A freeze results in an Extended Long Busy (ELB) condition for all primary MM devices in the session, which prevents write I/Os for the configured ELB timeout (the default is 2 minutes).
 - While the ELB condition is active on ZFS/HFS volumes that are used by the CSM application, it cannot proceed with the unfreeze operation.
- In general, it is best practice to run the active CSM server on the site with the primary MM devices, especially if HyperSwap or Hardened Freeze is not used, which provides another instance that monitors for freeze events to ensure consistent MM secondary devices upon replication failures.

Without HyperSwap or Hardened Freeze, the active CSM server is the only instance that monitors the primary MM devices for freeze events, and performs a freeze (and optional unfreeze) operation if necessary to ensure consistency of the MM secondary devices. This monitoring and processing requires a solid communication channel to the primary storage devices, either through FICON or through the storage system native management interface (DS8000 HMC).

The more distance or components that are involved in this communication path, the higher the risk that it breaks during a rolling disaster before the PPRC freeze events. If the active CSM server is isolated from either receiving freeze events or processing the freeze sequence, a consistent split of the secondary MM devices cannot be guaranteed.

Note: A worst case scenario can be an active CSM server with DS8000 HMC TCP/IP connections running in the secondary site, and an incident in the primary site first breaks the cross-site IP network and then the cross-site SAN/FICON network. In this case, CSM cannot perform the freeze when the replication links fail, which might lead to inconsistent secondary MM devices because of partially suspended MM relations.

2.3.2 IBM z/OS CSM server Basic Edition implementation

The CSM server for z/OS Basic Edition has the following limitations:

- It supports only the *Basic HyperSwap* session type.
- It supports only CKD device replication (as configured in the Basic HyperSwap session).
- It supports only a single CSM Server on z/OS (no standby CSM server and no CSM server on distributed platforms supported).

Note: The Basic HyperSwap session reacts only on HyperSwap triggers, and not on Freeze events. This means that PPRC link errors, which result in suspended primary devices, do not trigger a consistent Freeze of the Basic HyperSwap session.

With these limitations, the CSM Basic HyperSwap solution only provides storage HA, while remote DR capability is not guaranteed. Consistency of the secondary MM devices cannot be maintained for various failure scenarios, for example rolling disasters or partial mirroring errors.

Figure 2-2 shows the implementation topology for a Basic HyperSwap session solution.

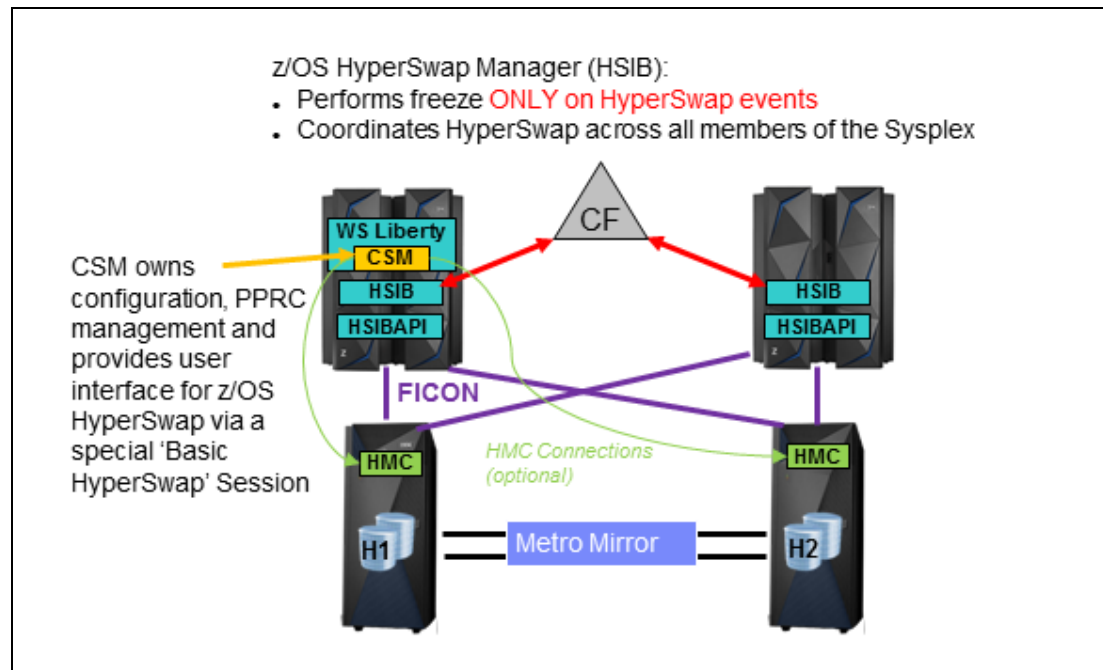


Figure 2-2 Basic HyperSwap solution

The following options are available for a Basic solution:

- Implementation options:
 - HMC connections can optionally be used to manage DS8000 Easy Tier HMT utility or provide a redundant communication path to the managed FICON devices.
- Advantages:
 - No charge solution for z/OS storage HA.
- Limitations:
 - No remote DR consistency guaranteed.
 - No standby or external CSM server supported.
 - Only z/OS attached CKD devices can be managed (IBM and 3rd party 2105/2107 devices).

2.3.3 CSM server on z/OS with standby CSM on z/OS

The fully licensed CSM server for z/OS entitles users for the z/OS SMPE CSM installation image and CSM installation images for other supported distributed platforms. It also allows the definition of a CSM standby server.

Figure 2-3 illustrates the implementation of an active and a standby CSM server on z/OS, and how they optionally interact with the z/OS HyperSwap Manager.

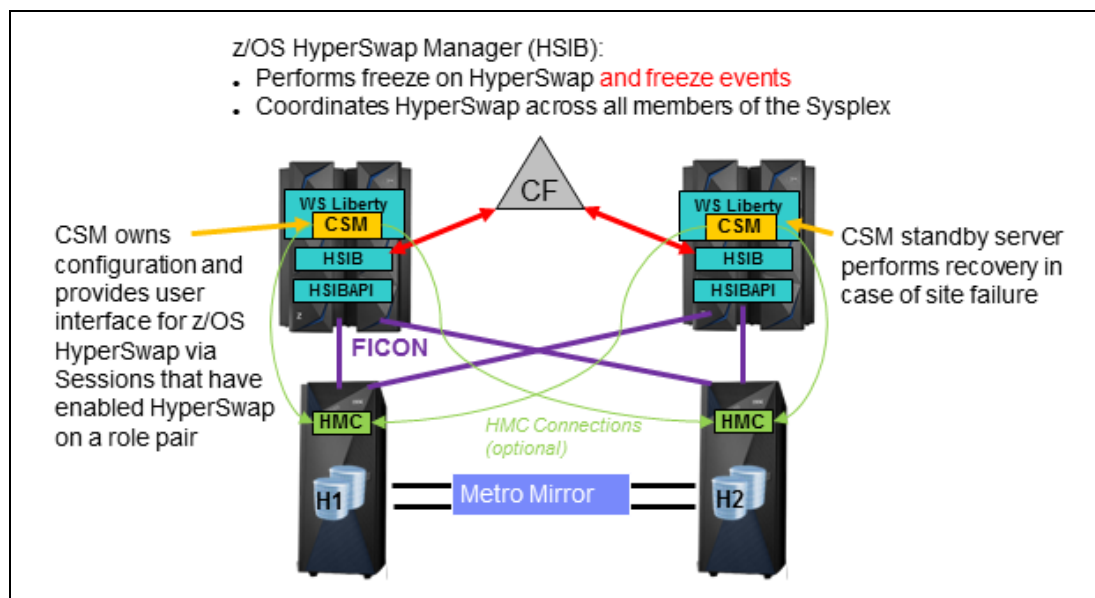


Figure 2-3 Active and standby CSM server on z/OS

The following options are available with standby CSM on z/OS:

► Implementation options:

- Although the standby CSM server is optional, it is good practice to run it on an LPAR at the other site, especially if HyperSwap is not used. This configuration enables quick manual recovery in case of primary site outages.
- You can optionally use HyperSwap and/or Hardened Freeze, which requires that HSIB and HSIBAPI address spaces are active on each LPAR. Otherwise, these address spaces are not required.
- The HMC IP connections from the CSM servers are optional but advised:
 - Required for Easy Tier HMT utility or MM Heartbeat management.
 - Required for management of devices not defined to the active CSM server LPAR.
 - Provide a redundant communication path for all FICON connected IBM 2105/2107 CKD devices.

► Advantages:

- Licensed solution for z/OS storage DR and optional HA. HyperSwap or Hardened Freeze can be enabled.
- Enables you to manage any CSM supported storage type and replication, for example:
 - You can use it to manage Global Mirror (GM) to remote data centers.
 - You can also use it to manage Storwize, FlashSystem, and XIV FB storage replication for distributed platforms.

► Limitations:

- No DR on Sysplex outages if both CSM servers are running within the same Sysplex.
- The CSM standby server at the remote site requires an active z/OS LPAR. This might drive z/OS license costs for cold DR sites which typically do not run active LPARs.
- HyperSwap or Hardened Freeze for another Sysplex requires a z/OS IP host connection to the external Sysplex (not illustrated in this scenario).

2.3.4 CSM server on z/OS with standby on distributed platform

Figure 2-4 illustrates a similar implementation of the fully licensed CSM edition for z/OS, but with a standby CSM server that is not running within the Sysplex. The CSM standby server can be running on z/OS, for example on a maintenance LPAR, or on a distributed server.

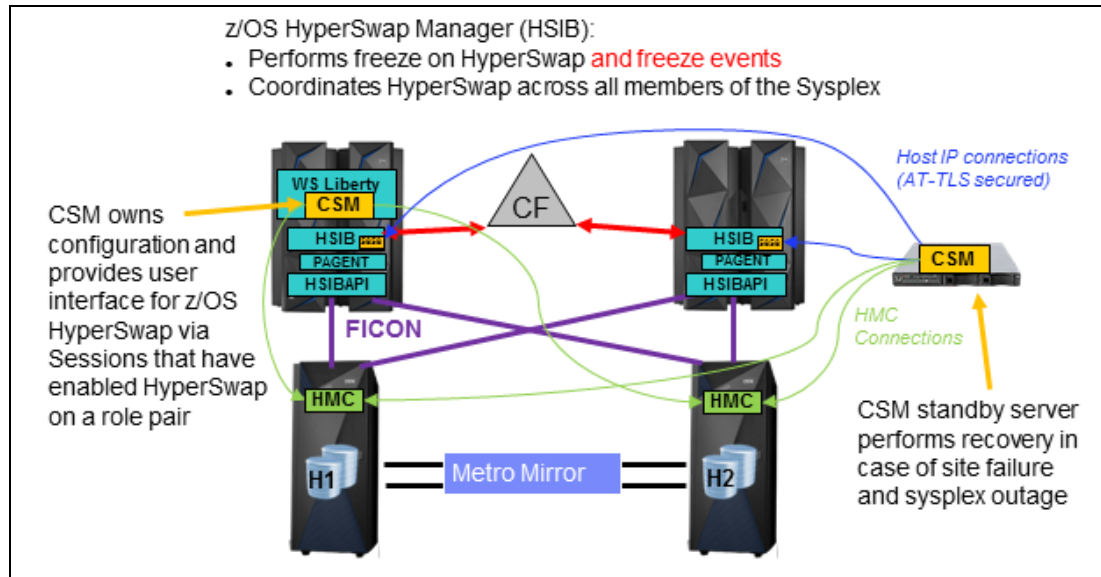


Figure 2-4 Active z/OS CSM server and external standby CSM server

The following options are available with standby on a distributed platform:

- ▶ Implementation options:
 - The standby CSM server can run on z/OS or a distributed platform server:
 - This allows quick manual recovery in case of primary site outages, but also in case of Sysplex outages.
 - If DS8880 is in use on the DR site, the standby CSM server could also run on the DS8880 HMC, avoiding the need for a dedicated CSM server.
 - HyperSwap and/or Hardened Freeze can be configured. This requires that HSIB and HSIBAPI address spaces are active on each LPAR of the managed Sysplex.
 - IBM z/OS IP host connections require that dedicated LPARs are configured with the PAGENT, HSIB, and HSIBAPI address spaces, and that the **HSIB SOCKPORT** parameter is used. This connection is optional, but required in case of the following situations:
 - You need the ability to manage HyperSwap or Hardened Freeze from a standby server.
 - You operate third party storage devices, which can be managed only through FICON (for example, Hitachi VSP).
 - The DS8000 HMC IP connections from the CSM servers are required in case of:
 - Easy Tier HMT utility or MM Heartbeat management.
 - CSM management of devices is not defined to the IOS on the LPARs where CSM is running or connected to.
 - Providing a redundant communication path to FICON connected IBM devices, for example to perform a PPRC Failover in case of Sysplex outage to enable IPL from secondary devices.

- Advantages:
 - Licensed solution for z/OS storage DR and optional HA. HyperSwap or Hardened Freeze can be enabled.
 - DR capability on Sysplex outage because the standby CSM server is running outside of Sysplex with DS8000 HMC IP connections from the standby CSM server.
 - Support for DR capability in cold DR sites without active LPARs with DS8000 HMC IP connections from the standby CSM server.
 - Enables you to manage any CSM supported storage type and replication:
 - GM to remote Data centers
 - IBM Spectrum Virtualize™ FB storage replication for distributed platforms
 - The solution can be extended to manage HyperSwap or Hardened Freeze of multiple Sysplexes. Both CSM servers require z/OS IP host connections to LPARs from each Sysplex that should be managed.
- Limitations:
 - Without z/OS IP host connection to other Sysplexes, HyperSwap or Hardened Freeze can be managed only within Sysplex.

2.3.5 HyperSwap management by CSM servers outside of Sysplex

Figure 2-5 illustrates an implementation where no CSM server runs within the managed Sysplex.

The external CSM server can run on a distributed platform, or on an external z/OS LPAR (in that case, it must be a fully licensed CSM for z/OS edition). Independently of the CSM server platform, both CSM servers use a z/OS IP host connection to communicate with the HyperSwap Manager and IOS.

Therefore, both CSM servers can also utilize a z/OS Direct Connection (FICON) to manage the CKD devices of the IOS attached storage controllers. This scenario is used if you plan to implement distributed platform CSM servers to manage HyperSwap or Hardened Freeze, or if you plan to manage multiple Sysplexes by a single pair of external CSM servers.

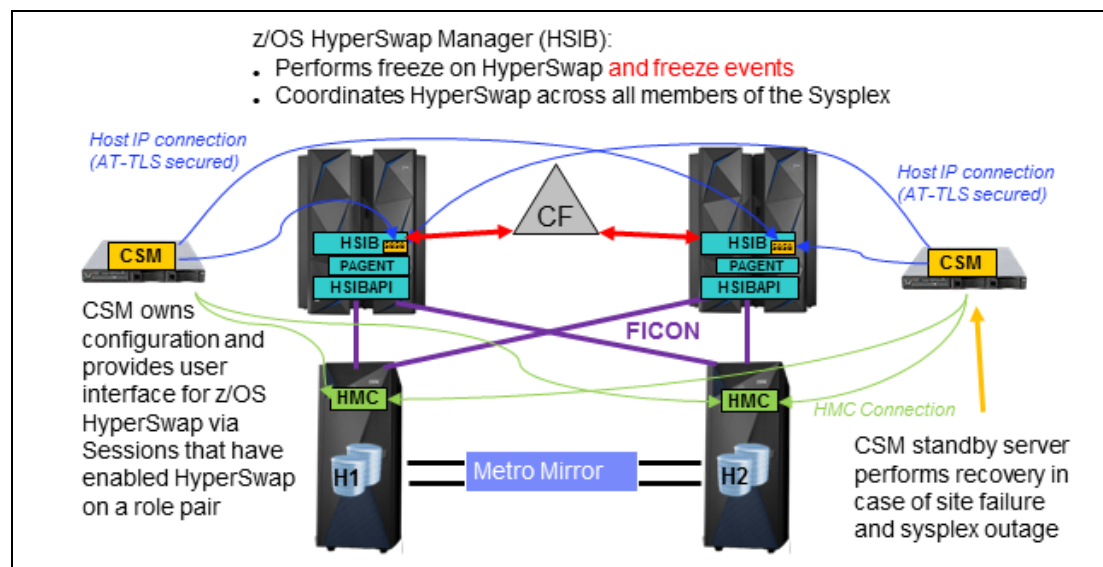


Figure 2-5 Active and standby CSM server on external servers

The following options are available outside of Sysplex:

► Implementation options:

- Both CSM servers can run on external z/OS LPARs or distributed platform servers. This enables quick manual recovery in case of primary site outages, but also in case of Sysplex outages.
- HyperSwap or Hardened Freeze can be used optionally. This option requires that HSIB and HSIBAPI address spaces are active on each LPAR of the managed Sysplex.
- IBM z/OS IP host connections require that dedicated LPARs are configured with the PAGENT, HSIB, and HSIBAPI address spaces, and that the **HSIB SOCKPORT** parameter is used. This connection is required for both external CSM servers:
 - HyperSwap or Hardened Freeze management of one or multiple Sysplexes.
 - Replication management through a FICON storage connection (optional for IBM DS8000 but required for Hitachi VSP storage devices).
- The DS8000 HMC IP connections from the CSM servers are required in case of the following situations:
 - Easy Tier HMT utility or MM Heartbeat management.
 - CSM management of devices is not defined to the IOS on the LPARs where CSM is running or connected to.
 - Providing a redundant communication path to FICON connected IBM devices, for example to perform storage recovery in case of Sysplex outage to enable IPL from secondary devices.

► Advantages:

- Licensed solution for z/OS storage DR and optional HA. HyperSwap or Hardened Freeze can be implemented.
- DR capability on Sysplex outage, because both CSM servers are running outside of Sysplex with HMC IP connections from CSM servers.
- DR capability in cold DR sites without active LPARs by using HMC IP connections from CSM servers.
- Enables you to manage any CSM supported storage type and replication:
 - GM to remote Data centers
 - IBM Spectrum Virtualize FB storage replication for distributed platforms
- Can be extended to manage HyperSwap or Hardened Freeze of multiple Sysplexes (not illustrated in this scenario).
- For DS8000 MM configurations without HyperSwap, it is advised to use Hardened Freeze configurations. This enables the Sysplex as a second instance to monitor and react to Freeze events autonomously, even if all z/OS IP host connections are lost or the active CSM server is disconnected from the DS8000 HMCs.

► Limitations:

HyperSwap or Hardened Freeze, and FICON storage connections, can be managed or monitored only if at least one z/OS IP host connection is connected into the managed Sysplex.

2.3.6 HyperSwap management by CSM servers on DS8880 HMCs

Figure 2-6 illustrates a special instance of managing z/OS HyperSwap by external CSM servers. In this solution, you run the CSM servers on DS8880 HMCs. All DS8880 models with firmware R8.1 or later are delivered with CSM software preinstalled on the HMCs. By default, the preinstalled CSM server has no license key applied and provides only limited capabilities.

However, with an appropriate CSM license key you can activate its full feature set. See *IBM DS8880 Integrated Copy Services Manager and LDAP Client on the HMC*, REDP-5356 for details.

Note: If you have a CSM license file (csm-license.zip), you need to convert it to a key string to activate CSM on the DS8880 HMC.

For more information, see the [Converting a license file to a string key](#) IBM Knowledge Center page.

For a MM with HyperSwap configuration, it is a preferred practice to activate the CSM servers on one of the HMCs of each of the two DS8880 storage systems, which are distributed across the sites. If you plan for z/OS HyperSwap or Hardened Freeze, both CSM servers need a z/OS IP host connection to communicate to the z/OS HyperSwap Manager and IOS. In that case, both CSM servers can also be configured with a z/OS Direct Connection (FICON) to manage CKD devices of the IOS attached storage controllers, as shown in Figure 2-6.

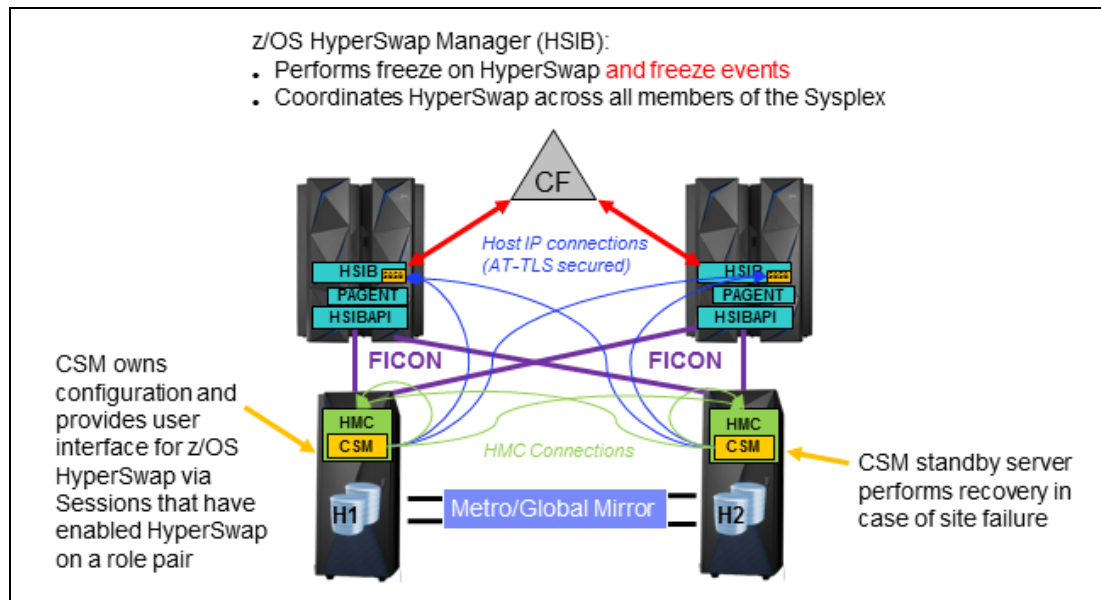


Figure 2-6 Active and standby CSM Server on DS8880 HMCs

The following options are available on DS8880 HMCs:

- Implementation options:
 - Both CSM servers run on different DS8880 HMCs:
 - For proper DR, spread the CSM servers across different DS8880 HMCs and across different sites.
 - This enables quick manual recovery in case of primary site outages, but also in case of Sysplex outages.

- HyperSwap and/or Hardened Freeze are supported. This requires that HSIB and HSIBAPI address spaces are active on each LPAR of the managed Sysplex.
- IBM z/OS IP host connections require that selected LPARs are configured with the PAGENT, HSIB, and HSIBAPI address spaces, and that the **HSIB SOCKPORT** parameter is used. This connection is required for both CSM servers for the following instances:
 - HyperSwap or Hardened Freeze management.
 - Replication management through a FICON storage connection to provide a redundant management path for IOS attached CKD devices.
- Even if CSM is running on the DS8880 HMC, the HMC IP connections from the CSM servers to the storage systems are required for the following situations:
 - Easy Tier HMT utility or MM Heartbeat management.
 - CSM management of devices not defined to the IOS on the LPARs where CSM is connected to.
 - A redundant communication path to FICON connected IBM devices.
- Advantages:
 - Licensed solution for z/OS storage DR and HA:
 - CSM is already pre-installed on DS8880 HMCs and just needs to be activated with license keys.
 - HyperSwap or Hardened Freeze can be enabled.
 - DR capability on Sysplex outage because both CSM servers are running outside of Sysplex with HMC IP connections from CSM servers.
 - Solution supports DR capability in cold DR sites without active LPARs with HMC IP connections from CSM servers.
 - Enables you to manage any CSM supported storage type and replication:
 - GM to remote Data centers.
 - IBM Spectrum Virtualize FB storage replication for distributed platforms.
 - Can be extended to manage HyperSwap or Hardened Freeze of multiple Sysplexes (not illustrated in this scenario).
 - For DS8000 MM configurations without HyperSwap, it is advised to utilize Hardened Freeze configurations.
- Limitations:
 - HyperSwap or Hardened Freeze, and FICON storage connections, can be managed and monitored only if at least one z/OS IP host connection is connected.
 - Scalability of CSM on DS8880 HMCs is limited by HMC physical resources, and supports management of up to 4 different storage systems.
 - CSM license keys provided through the IBM Spectrum Control or IBM SmartCloud Virtual Storage Center (VSC) program entitlement cannot be applied on HMC CSM servers. For more details about available CSM licenses, see 1.2, “CSM licenses” on page 5.

2.3.7 Cascaded MGM or Multi Target MM-GM with local HyperSwap

Figure 2-7 on page 36 illustrates a CSM server implementation to manage 3-site replication, using either a cascaded Metro Global Mirror (MGM) or a multi target Metro-Mirror Global-Mirror topology with IBM DS8000.

For both topologies, the third site is a remote site at larger distance, which cannot be used for synchronous replication, or to host active LPARs that share the same Sysplex. The third site is considered a DR site, which is used after a regional disaster, when the primary and the secondary site failed, or after the whole Sysplex failed.

Usually there are no active z/OS LPARs on the DR site, except a small maintenance LPAR that might be continuously active. If there is no active z/OS LPAR at all on the DR site, the standby CSM server should be installed on an external server platform at the DR site. This configuration enables quick takeover of the CSM management and a fast CSM session recovery if the local sites fail or the whole Sysplex fails.

Optionally, HyperSwap or Hardened Freeze can be used between the local sites. For a cascaded topology, the GM continues to run after a HyperSwap to the intermediate site. For a multi target topology, CSM can be configured to automatically resynchronize the GM target site after a HyperSwap in order to reestablish DR capability automatically.

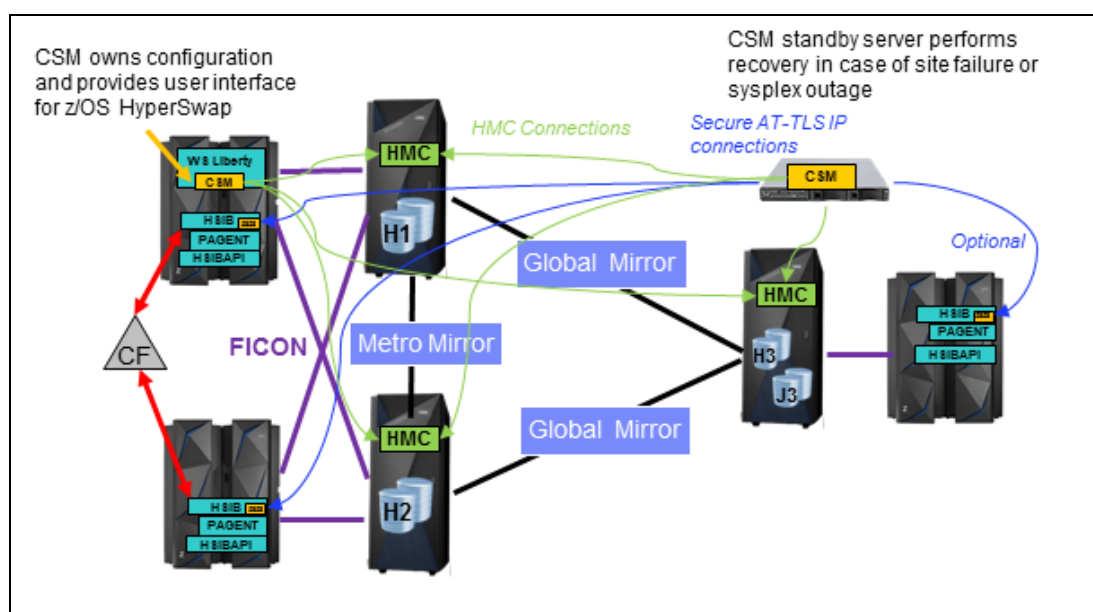


Figure 2-7 CSM server example for three sites with remote DR site

The following options are available with local HyperSwap:

- Implementation options:
 - The active CSM server can either be installed on a z/OS LPAR in the Sysplex, or on an external server platform. If the CSM server runs externally, it will need a z/OS IP host connection into the Sysplex if HyperSwap or Hardened Freeze management is required.
 - The standby CSM server on the DR site can either run on an external z/OS maintenance LPAR (if available) or on a distributed platform server, such as the DS8000 HMC.
 - HyperSwap or Hardened Freeze can be used:
 - This requires that HSIB and HSIBAPI address spaces are active on each LPAR of the managed Sysplex.
 - All external CSM servers need a z/OS IP host connection into the Sysplex that should be managed.

- z/OS IP host connections require that selected LPARs are configured with the PAGENT, HSIB, and HSIBAPI address spaces, and that the **HSIB SOCKPORT** parameter is used. This connection is required for the following instances:
 - HyperSwap or Hardened Freeze management from CSM servers running outside of the Sysplex.
 - Replication management through a FICON storage connection to provide a redundant management path for IOS attached CKD devices.
- The HMC IP connections from the CSM servers are required for these situations:
 - Easy Tier HMT utility or MM Heartbeat management.
 - CSM management of devices not defined to the IOS on the LPARs where CSM is running or connected to, for example storage devices on the 3rd site.
 - Redundant communication paths to FICON connected IBM devices.
- Advantages:
 - Licensed solution for z/OS IBM DS8000 storage DR (local and remote) and optional local HA, HyperSwap, or Hardened Freeze can be enabled between the local sites.
 - Incremental resync capabilities are provided for both DS8000 3-site topologies.
 - Local and remote DR capability on Sysplex outage because both CSM servers can be running outside of Sysplex.
 - The solution supports DR capability in cold DR sites without active LPARs. Dedicated standby CSM server platform can be avoided if CSM is enabled on remote DS8880 HMC.
 - Solution can be extended to manage HyperSwap or Hardened Freeze of multiple Sysplexes (not illustrated in this scenario).
- Limitations:
 - HyperSwap or Hardened Freeze, and FICON storage connections, can be managed or monitored from external CSM servers only if at least one z/OS IP host connection is connected.
 - An active CSM server running on z/OS will also need an HMC IP connection to manage storage on a third site, because there is likely no FICON connection to third site storage devices.

2.3.8 Multi Target MM-MM with 3-site HyperSwap

Figure 2-8 on page 38 illustrates an implementation with 3-site replication at metro distance, using a multi target Metro-Mirror Metro-Mirror topology with IBM DS8000. Each of the two target sites contains a synchronous mirror and can be used for DR as well as storage HA for the Sysplex. HyperSwap can be optionally enabled for any or all of the synchronous replication legs. If HyperSwap is active for both legs at the same time, you can configure a site switch preference or let HyperSwap automatically choose a target site for the HyperSwap.

CSM can be configured to automatically resynchronize the remaining target sites after a HyperSwap to reestablish DR capability. If HyperSwap capability is configured between the remaining sites, it will also be activated automatically once the target sites reach MM Full Duplex state.

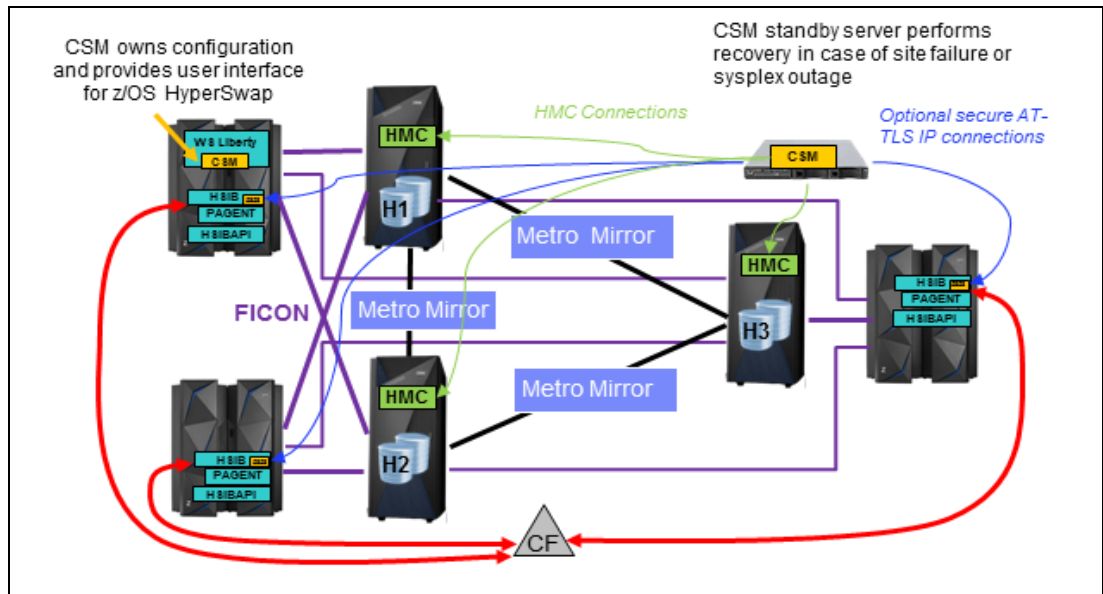


Figure 2-8 CSM server example for three sites with multi target MM

The following options are available for 3-site HyperSwap:

► Implementation options:

- The active CSM server can either be installed on a z/OS LPAR in the Sysplex, or on an external server platform. If the CSM server runs externally, it will need a z/OS IP host connection into the Sysplex if HyperSwap or Hardened Freeze management is required.
- The standby CSM server on any of the secondary sites can either run on an external z/OS maintenance LPAR (if available) or on a distributed platform server, such as the DS8880 HMC.
- HyperSwap or Hardened Freeze can be used:
 - This requires that HSIB and HSIBAPI address spaces are active on each LPAR of the managed Sysplex.
 - All external CSM servers need a z/OS IP host connection into the Sysplex that should be managed.
- IBM z/OS IP host connections require that dedicated LPARs are configured with the PAGENT, HSIB, and HSIBAPI address spaces, and that the **HSIB SOCKPORT** parameter is used. This connection is required for the following instances:
 - HyperSwap or Hardened Freeze management from CSM servers running outside of the Sysplex.
 - Replication management through a FICON storage connection to provide a redundant management path for IOS attached CKD devices.
- The HMC IP connections from the CSM servers are required for the following situations:
 - Easy Tier HMT utility or MM Heartbeat management.
 - CSM management of devices not defined to the IOS on the LPARs where CSM is running or connected to.
 - Redundant communication path to FICON connected IBM devices.

- ▶ Advantages:
 - Licensed solution for z/OS IBM DS8000 storage DR and HA on 2 target sites at metro distance.
 - HyperSwap can be enabled between any of the 3 sites. Hardened Freeze can only be enabled in general for the session (active for all or no sites).
 - Incremental resync capabilities for all 3 sites.
 - Automated restart capability for MM (and HyperSwap) between remaining sites after a HyperSwap.
 - DR capability on Sysplex outage because any of the CSM servers can be running outside of Sysplex.
 - Solution can be extended to manage HyperSwap or Hardened Freeze of multiple Sysplexes (not illustrated in this scenario).
- ▶ Limitations:
 - HyperSwap or Hardened Freeze, and FICON storage connections, can be managed or monitored from external CSM servers only if at least one z/OS IP host connection is active.
 - Sysplex HA might not be fully adoptable to storage HA:
 - This depends on the distribution of active Sysplex LPARs across the 3 sites, and the placement of the alternate Couple Data Sets, which must not be part of the multi target MM configuration.
 - Because only a single set of alternate CDS can be defined on either of the MM target sites, proper planning must be performed for the Sysplex availability.

2.3.9 CSM servers with FICON only storage connections

Figure 2-9 on page 40 illustrates a possible implementation scenario when the CSM servers can use only FICON based storage connections to manage CKD storage devices. For instance, this might be required in the following instances:

- ▶ If CSM is running on z/OS but the LPARs have no TCP/IP connection to the DS8000 HMCs network, for example because of customer security policies.
- ▶ For management of 3rd party storage systems (Hitachi VSP), for which CSM does not support IP connections.

If any of the CSM servers runs outside of the Sysplex to be managed, this CSM server needs a z/OS IP host connection to an LPAR that has attached the FICON devices to be managed.

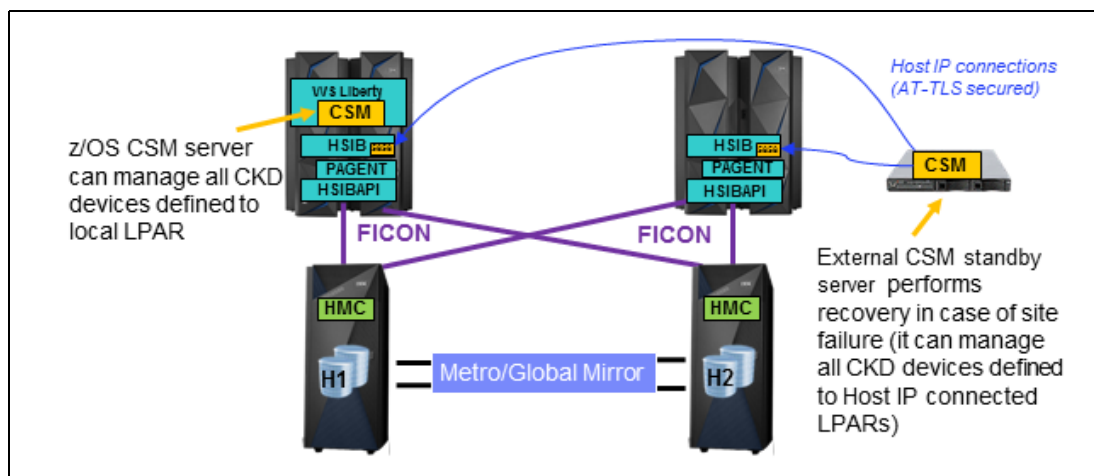


Figure 2-9 CSM server example without TCP/IP connection to storage systems

The following options are available for FICON only storage connections:

► Implementation options:

- The standby CSM server can run on an external z/OS LPAR or a distributed platform server:
 - This enables quick manual recovery in case of primary site outages, but also in case of Sysplex outages.
 - If DS8880 is in use on the DR site, the standby CSM server can also run on the DS8880 HMC, which prevents the need for a dedicated CSM server platform.
- HyperSwap and/or Hardened Freeze can be used. This requires that HSIB and HSIBAPI address spaces are active on each LPAR of the managed Sysplex.
- IBM z/OS IP host connections require that selected LPARs are configured with the PAGENT, HSIB, and HSIBAPI address spaces, and that the **HSIB SOCKPORT** parameter is used. This connection is required for any external CSM server.

► Advantages:

- Licensed solution for z/OS storage DR and HA.
- HyperSwap or Hardened Freeze can be enabled.
- DR capability on Sysplex outage because a standby CSM server can be running outside of the Sysplex.
- Solution can be extended to manage HyperSwap or Hardened Freeze of multiple Sysplexes (not illustrated in this scenario).

► Limitations:

- External CSM servers require z/OS IP host connections to LPARs from each Sysplex that should be managed.
- Solution does not support fast DR capability in cold DR sites without active z/OS LPARs. Site recovery would require a z/OS LPAR that has the secondary CKD devices attached and can be used by CSM to initiate the PPRC Failover to enable IPL from secondary devices.

- The following features cannot be used without DS8000 HMC IP connections:
 - Easy Tier HMT utility or MM Heartbeat management.
 - CSM management of devices not defined to the IOS on the LPARs where CSM is running or connected to.
 - Redundant communication path to FICON connected IBM devices.
 - Only FICON connected CKD storage devices can be managed.



Prerequisites for various implementation topologies

This chapter reviews the requirements for each of the components that may be installed as part of the IBM Copy Services Manager (CSM) and IBM z/OS HyperSwap solutions discussed in this book.

3.1 TCP/IP Communication requirements

Any TCP/IP connection that is established between CSM servers and storage systems or z/OS logical partitions (LPARs) require that the ports used are reachable in the communication network. If firewalls are in use, they must be configured to allow connections via these dedicated/configured ports. This configuration includes also operating system firewalls of the CSM server platform or the z/OS LPARs. Table 3-1 lists the required ports for incoming/outgoing TCP/IP traffic on the CSM server platform.

Table 3-1 IP ports used by CSM for management

CSM servers	Default Port
CSM server GUI	9558, 9559
CSM Server CLI	9560
CSM server high availability (HA) Connection	9561
CSM LDAP Authentication Service (optional)	9562

To ensure a CSM server can communicate to the storage systems or z/OS LPARs, ensure that all CSM servers can send outgoing TCP/IP packets to following ports as defined in Table 3-2.

Table 3-2 IP ports used by CSM for storage and host connections

Storage Systems	Port
DS8000 Hardware Management Console (HMC) connection	1750, 1751
SVC, Storwize family, FlashSystem V	443, 22
XIV, FlashSystem A	7778
z/OS LPAR	Default Port
z/OS IP host connection	5858

More detailed port requirements can be found in IBM Knowledge Center on the CSM [Ports](#) page.

Attention: If the CSM server is running on a DS8880 HMC, consider using the default z/OS LPAR communication port 5858, which is pre-defined in the HMC firewall rules. As of CSM 6.2.3, a non-default port configuration requires engagement of IBM DS8000 product support to modify the HMC firewall rules accordingly.

3.2 Prerequisites for z/OS HyperSwap

z/OS HyperSwap functionality requires the following minimum supported releases:

- ▶ z/OS 1.13 or higher. Ensure to be on a supported z/OS level:
 - z/OS 1.13 went out of support on Sep. 30, 2016
 - z/OS 2.1 went out of support on Sep. 30, 2018
- ▶ CSM 6.0 or higher

Make sure that you have all the current z/OS APARs installed. To check latest available APARs, see 6.2.1, “Install the latest PTFs for z/OS HyperSwap” on page 100.

3.2.1 IBM z/OS APARs for HyperSwap and other CSM functions

The following minimum z/OS APARs are required at the time of writing this book. The first ones are mainly relevant for z/OS 1.13 only, but check the latest ones for z/OS 2.x as well:

- ▶ APAR OA37632 (pre z/OS 2.x only):
 - HyperSwap enhancements (Metro Mirror (MM) event aggregation, improved HyperSwap triggers, suspension of MM even if HyperSwap disabled), MM Hardened Freeze support
 - <https://www.ibm.com/support/docview.wss?uid=isg10A37632>
- ▶ APARs OA44066, OA40862 (pre z/OS 2.x only):
 - Support IR after unplanned HyperSwap in MGM session
 - <https://www.ibm.com/support/docview.wss?uid=isg10A44066>
 - <https://www.ibm.com/support/docview.wss?uid=isg10A40862>
- ▶ APAR OA50053:
 - HyperSwap status in **DISPLAY HS,STATUS** command is inconsistent with message IOSHM0803E and IOSHM0805I
 - <https://www.ibm.com/support/docview.wss?uid=isg10A50053>
- ▶ APAR OA50798 (pre z/OS 2.x only):
 - HyperSwap session shows warning instead of severe status
 - <https://www.ibm.com/support/docview.wss?uid=isg10A50798>
- ▶ APAR OA50868:
 - Reduce XCF CDS recovery delay in HyperSwap environments
 - <https://www.ibm.com/support/docview.wss?uid=isg10A50868>
- ▶ APAR OA50914:
 - Relax status checking for HyperSwap, especially relevant for JES3
 - <https://www.ibm.com/support/docview.wss?uid=isg10A50914>
- ▶ APAR OA51429:
 - New function APAR to support Input/Output Supervisor (IOS) FICON discovery enhancements of CSM 6.2.0
 - Allows CSM to update FICON device status every 5 minutes instead of every hour
 - This APAR requires that HyperSwap address spaces are active on the LPAR with the CSM FICON connection
 - <https://www.ibm.com/support/docview.wss?uid=isg10A51429>

- ▶ New Functions APAR OA53082 (recommended):
 - New function APAR to enhance handling of HyperSwap PPRC secondary devices
 - Allows UBNALLOC as well as boxed device cleanup during configuration load
 - Supports new **SETIOS** parameter **HYPERSWAP** to trigger unplanned HyperSwap by command
 - <https://www.ibm.com/support/docview.wss?uid=isg10A53082>
- ▶ New Functions APAR OA53143 (optional):
 - New function APAR to optionally suppress physical control unit (PCU) single point of failure (SPOF) health checks for HyperSwap managed volumes
 - <https://www.ibm.com/support/docview.wss?uid=isg10A53143>
- ▶ New Functions APAR OA55151 (recommended):
 - New function APAR to monitor that the PPRC consistency group flag is on for all LSS/Device pairs in the HyperSwap configuration
 - <https://www.ibm.com/support/docview.wss?uid=isg10A55151>
- ▶ New Functions APAR OA56173:
 - New function APAR for IOS to support SafeGuarded Copy management of FICON attached DS8000 storage controllers
 - Enables CSM to manage SafeGuarded Copy through a z/OS Direct Connection storage attachment (FICON)
 - Without this APAR, SafeGuarded Copy management requires an HMC IP storage connection from the CSM server to DS8000 HMCs
 - <https://www-01.ibm.com/support/entdocview.wss?uid=isg10A56173>

This list might not be complete. Make sure that you have all the latest z/OS HyperSwap APARs installed.

3.2.2 z/OS APARs for Multiple Target Peer-to-Peer Remote Copy and HyperSwap

DS8000 Multiple Target Peer-to-Peer Remote Copy (MT-PPRC) with HyperSwap is supported on z/OS V1.13 or later with the following minimum APARs at the time of writing this book:

- ▶ APAR OA44240 (pre z/OS 2.x only):
 - Provides the IOS infrastructure for MT-PPRC and HyperSwap PTFs UA90740/UA90741/UA90742
 - <https://www.ibm.com/support/docview.wss?uid=isg10A44240>
- ▶ APAR OA47113 (pre z/OS 2.x only):
 - Problems with OA44240 -IOSHSAPI ABEND878, z/OS HyperSwap disabled, or z/OS HyperSwap Policy incorrect
 - <https://www.ibm.com/support/docview.wss?uid=isg10A47113>
- ▶ APAR OA46683 (pre z/OS 2.x only):
 - Enables MT-PPRC for Basic HyperSwap and GDPS HM
 - <https://www.ibm.com/support/docview.wss?uid=isg10A46683>

- ▶ APAR OA43661 (pre z/OS 2.x only):
 - Enables MT-PPRC support for DFSMS. Full support requires the following APARs:
 - OCEOV APAR (OA43661)
 - Device Support APAR (OA43662)
 - AOM/DEVSERV APAR (OA43663)
 - DEVMAN APAR (OA46198)
 - IOS/BCP APAR (OA46173)
 - SDM APAR (OA43654)
 - ICKDSF APAR (PM99490)
 - <https://www.ibm.com/support/docview.wss?uid=isg1OA43661>
- ▶ New Functions APAR OA52282:
 - New function APAR to support hybrid MT-PPRC HyperSwap MM and Hardened Freeze
 - Take appropriate actions against a particular relationship in the event of a HyperSwap or PPRC suspension
 - Support periodic status updates to CSM so that they are always received even if CSM has been stopped and restarted
 - <https://www.ibm.com/support/docview.wss?uid=isg1OA52282>
- ▶ New Functions APAR OA56215:
 - New function APAR to allow CSM to request information related to a particular HyperSwap configuration whose name is provided on a Ping request (required for proper status monitoring once two HyperSwap configurations of a Multiple Target MM-MM configuration are loaded)
 - <https://www.ibm.com/support/entdocview.wss?uid=isg1OA56215>

This list might not be complete. Make sure that you have all the latest z/OS HyperSwap and MT-PPRC APARs installed.

3.2.3 z/OS HyperSwap configuration prerequisites

The following list contains some general configuration prerequisites for HyperSwap. For more detailed z/OS configuration considerations, see 6.2, “IBM z/OS configuration for HyperSwap” on page 99:

- ▶ All LPARs in the Sysplex must participate in the HyperSwap configuration and must run the HyperSwap management address spaces (HSIB and HSIBAPI)
- ▶ All LPARs in the Sysplex must have defined access to all devices in the HyperSwap configuration (physical and logical). This means that there must be defined UCBs, subchannels, and valid paths to the devices.
 - There is no need that all devices are online on each LPAR
 - Only z/OS attached volumes are supported by z/OS HyperSwap
- ▶ Monoplex configuration: HyperSwap uses XCF couple data sets to save state information. In order to use HyperSwap for only a single z/OS image, you must set it up as a Monoplex, meaning a Sysplex with a single image (**PLEXCFG=MONOPLEX** in **SYSx.PARMLIB**), and not simply a single, standalone MVS system (**PLEXCFG=XCFLOCAL** in **SYSx.PARMLIB**).
- ▶ All system and application data, including page data sets and JES work volumes, must be replicated and be part of the HyperSwap configuration (with the exception of certain XCF Couple Data Sets).

- ▶ XCF Couple Data Sets (CDS) are the only data sets that should not be located on volumes involved with HyperSwap and therefore should not be replicated by PPRC, to avoid them becoming subjected to a Freeze operation. The primary and alternate CDS should be distributed on the primary and secondary storage controller, so that the z/OS XCF mechanism is used to asynchronously update the alternate CDS on the other storage controller.

Important: There is one exception to this rule. The LOGR Couple Data Sets should be replicated by PPRC and be part of the HyperSwap configuration. Therefore, they need to be located on different volumes than the other Couple Data Sets.

- ▶ Primary and secondary storage controllers must be FICON attached to all LPARs in the Sysplex (or Monoplex).
- ▶ A symmetric I/O channel and alias (PAV) configuration for primary and secondary storage controllers is a good practice to avoid large I/O performance differences after a HyperSwap or site switch.
- ▶ If zHyperLink attachment is additionally configured for the primary devices, but not for the secondary devices due to zHyperLink distance limitations (150 m), a noticeable I/O performance degradation might occur after a HyperSwap.
- ▶ Do not share the HyperSwap managed devices with LPARs outside of the Sysplex. Doing so nonetheless will affect the foreign system or application in case of a HyperSwap event. The foreign system is not aware when the primary device becomes obsolete after a HyperSwap. DS8000 with newer firmware releases supports a *Soft Fence* capability. It will be used by HyperSwap to soft fence old primary devices, and further I/O to this device is blocked by the storage controller.

This capability provides additional data integrity protection for foreign LPARs that might still try to access obsolete devices after a HyperSwap. The *Soft Fence* capability requires the following minimum firmware levels on older DS8000 models:

- DS8800 - R6.3 SP6 Bundle 86.31.95.0 LMC 7.6.31.1150
- DS8700 - R6.3 SP6 Bundle 76.31.79.0 LMC 6.6.31.670
- DS8870 - R7.1.7 bundle 87.10.133.0 LMC 7.7.10.354
- ▶ It is a good practice to avoid sharing LCUs in a HyperSwap configuration with LCUs not participating in the HyperSwap configuration. A HyperSwap performs a *Freeze* operation on the managed logical control unit (LCU) pairs, which removes all their PPRC paths and causes an *Extended Long Busy* (ELB) condition on all primary PPRC devices between the frozen LCU pairs. For this reason, you should not share the same storage controller LCU pairs between different CSM MM or HyperSwap sessions.
- ▶ For each PPRC pair in your HyperSwap configuration, both the primary and the secondary device must have MIDAW either enabled or disabled:
 - You cannot mix MIDAW-enabled and MIDAW-disabled devices in the same PPRC pair.
 - z/OS HyperSwap itself currently performs no validation of this requirement.
- ▶ Sufficient command authorization for TSO users that monitor/manage HyperSwap. The following security facility authorities are required to issue HyperSwap operator commands:
 - **SETHS ENABLE/DISABLE/SWAP** requires UPDATE authority to profile MVS.SETHS in the OPERCMDS class.
 - **DISPLAY HS** requires READ authority to profile MVS.DISPLAY.HS in OPERCMDS class.
 - **SETIOS HYPERSWAP** requires UPDATE authority to profile MVS.SETIOS.IOS in the OPERCMDS class.

3.3 Prerequisites for z/OS IP host connections

A CSM z/OS IP host connection has the following requirements on the z/OS LPARs which are used to establish the connection:

- ▶ APAR OA40866 (z/OS 1.13 only):
 - New z/OS 1.13 function: Basic HyperSwap Sockets Server
 - <https://www.ibm.com/support/docview.wss?uid=isg10A40866>
- ▶ An IP address/hostname served by the LPAR for external z/OS IP host connections

The IP address/hostname can be virtualized, for example through z/OS Virtual IP Addressing (VIPA), which allows hostname/IP movements to other LPARs. When an IP address is moved to another LPAR that is prepared for CSM z/OS IP host connections, the CSM host connection will fail and must be re-established. This is managed automatically by the CSM server, but leads to a short interruption of the host connection.
- ▶ Use of unique Sysplex names:
 - Avoid the use of duplicate Sysplex names, especially the Sysplex name *LOCAL*. *LOCAL* is the Sysplex name in the IBM-supplied default **COUPLE00** member of **SYSx.PARMLIB**.
 - The name *LOCAL* has no special meaning to XCF, but if you eventually wish to manage two or more Sysplexes (or Monoplexes) from a single CSM instance, they will need to have unique Sysplex names because the Sysplex name must be associated to the CSM sessions.
- ▶ Define the socket port to be used on z/OS LPARs for the z/OS IP host connections from CSM servers:
 - The default port is 5858, but it can be customized.
 - The used port must be available on the z/OS LPAR. You can check used ports with the TSO command **NETSTAT**.

Important: If the CSM server is running on a DS8880 HMC, consider using the default z/OS LPAR communication port 5858, which is pre-defined in the HMC firewall rules. As of CSM 6.2.3, a non-default port configuration requires IBM DS8000 product support to modify the HMC firewall rules accordingly.

3.4 Prerequisites for DS8000 storage controllers

The following section is a list of DS8000 or HMC related pre-requirements for CSM and HyperSwap management:

- ▶ DS8000 with SSLv3 encrypted HMC connections are not supported anymore by CSM. SSLv3 was completely disabled in CSM 6.2.0 and later due to its vulnerability. This removed the backward compatibility to older DS8000 systems, which still required SSLv3 encryption for the HMC connection. However, these older DS8000 systems should be upgraded to a later firmware release that includes the *SSLv3 Poodle Attack* patch. The following minimum DS8000 firmware levels are required to connect to CSM 6.2.0 and later:
 - DS8870 R7.2 Versions 87.2x.xx.x and later
 - DS8870 R7.3 Versions 87.3x.xx.x and later
 - DS8870 R7.4 Versions 87.4x.xx.x and later
 - DS8800 R6.3 Versions 86.31.142.0 and later
 - DS8700 R6.3 Versions 76.31.121.0 and later

- For a list of actual recommended firmware levels, see the recommended DS8000 firmware levels web page:

<https://www.ibm.com/support/docview.wss?uid=ssglS1004456>

- Active Copy Services licenses as required per storage system model and replication type
- A DS8000 HMC user is needed, with a minimum authority of `op_copy_services` for use by CSM servers. If CSM will be used with enhanced DS8000 diagnostic features like *Warmstart* or *On Demand Dumps*, the DS8000 HMC user must have *admin* authority. It is good practice to define dedicated users for CSM use.
- The SSIDs of all LCUs in all DS8000 systems in a HyperSwap configuration must be unique. Otherwise, the HyperSwap configuration load will fail with a *Device not found* error and the syslog will show the message `IEC334I DUPLICATE SUBSYSTEM`. The SSID of an LCU can be changed, but may be disruptive because it requires you to complete the following steps:
 - Remove all copy service relations for all volumes in the LCU
 - Remove all PPRC paths that are defined for this LCU
 - You might have to vary all volumes in the LCU offline/online, or issue these commands to clear and rebuild the Storage Subsystem Status Control Block (SSSCB) Device Tables:
 - **DS QD,SSID=xxxx,DELETE** (xxxx = old SSID)
 - **VARY ONLINE,dddd** (dddd = all LCU devices on which the SSID has to be updated)
 - **DS QD,SSID=yyyy,VALIDATE** (yyyy = new SSID)
- In a z/OS HyperSwap configuration, MM *Critical Mode* is not supported. If existing MM relations are to be used in a HyperSwap configuration, they must be established without the Critical Mode setting. A MM relation with Critical Mode enabled can be changed by the following actions:
 - Suspending the PPRC relation
 - Resuming the MM relation without Critical Mode

This can also be accomplished by CSM. When the CSM session is started, it assimilates existing PPRC pairs without a new copy. If the Critical Mode is still enabled, you can simply **Suspend** the session when it is in *Prepared* state, and **Start** it again from the *Suspended* state. CSM will resume all PPRC relations without the Critical Mode.
- Specific requirements if you run CSM on a DS8880 HMC:
 - Minimum DS8880 firmware must be R8.1 or later
 - Number of managed Storage Systems is limited to 4 (due to HMC hardware limitations)
 - z/OS IP host connections from CSM on HMC to z/OS LPARs require DS8880 firmware 8.2.1 or later (default port 5858 allowed in HMC firewall rules)
 - Use default ports for various CSM services, because only default ports are enabled in HMC firewall rules

For an actual list of CSM supported storage systems, see the CSM 6.2 storage system support matrix:

<http://www.ibm.com/support/docview.wss?uid=ssglS7005411>

3.5 Prerequisites for Hitachi Virtual Storage Platform storage controllers

Hitachi tested and declared support for CSM and z/OS HyperSwap for their Hitachi Virtual Storage Platform (VSP) storage controllers. This support is valid for the following CSM session types:

- ▶ Basic HyperSwap
- ▶ MM Failover/Failback where both, HyperSwap or Hardened Freeze can be enabled

Hitachi documented the required VSP storage controller configuration in the *Hitachi Virtual Storage Platform G1000 Hitachi TrueCopy for Mainframe User Guide*:

<https://www.hds.com/assets/pdf/vsp-g1000-hitachi-truecopy-for-mainframe-user-guide-v-02.pdf>

Some specific Hitachi VSP system option modes must be configured for functionality and support (see the “*Planning for Basic HyperSwap function-Tivoli Storage Productivity Center for Replication support*” chapter). Set the following system option modes accordingly:

- ▶ **Mode 114 = OFF** (default)
Automatic port switching during ESTPATH/DELPATH is disabled.
- ▶ **Mode 484 = ON** (default **OFF**)
PPRC path QUERY is displayed with the New Spec.
- ▶ **Mode 769 = ON** (default **OFF**)
The retry operation is disabled when the path creation operation is executed (retry operation is not executed).

Not documented by Hitachi, but the following additional system option mode might be required for CSM:

- ▶ **Mode 573 = ON** (default **OFF**)
The ESTPAIR CASCADE option is allowed.

The cascaded PPRC option is always used by CSM and does not provide any impact to normal PPRC operation, but it ensures future flexibility when PPRC relations must be cascaded for whatever reason. Per default, the Hitachi VSP G1000 does not support the cascaded PPRC option. Therefore the required system option mode must be changed accordingly for a CSM MM Failover/Failback session. For specific system mode details, see the latest Hitachi VSP User and Reference Guides.

Note: The CSM session type *Basic HyperSwap* is the only type that does not use the PPRC Cascade option for PPRC relations. That means for HyperSwap usage via a CSM Basic HyperSwap session, the Option Mode 573 can remain **OFF**.

Because Hitachi performs all CSM and HyperSwap solution tests with their storage controllers, Hitachi VSP customers need to confirm full solution support for CSM and HyperSwap with Hitachi directly.



Part 2

Installation and Configuration

This part describes the installation and configuration of the required elements for the desired implementation topology. It covers the implementation of IBM Copy Services Manager (CSM) on IBM z/OS, z/OS IP host connection, and z/OS HyperSwap.



CSM Installation on IBM z/OS

IBM Copy Services Manager is a Java based application that is delivered with a lightweight version of IBM WebSphere Application Server called *WebSphere Liberty Profile* (WLP), or *Liberty*. The WLP installation is integrated in the CSM installation process and does not require any special considerations or configuration settings.

The overall CSM installation on z/OS includes the SMPE installation of the CSM for z/OS product images according to the Program Directory, as well as some post-SMPE installation tasks. The post-installation tasks create users for the CSM server, a UNIX System Services file system (ZFS or HFS) for the product installation, and the execution of the installation job to install a new CSM server instance or update an existing one.

Note: This section is *only required for CSM installation on z/OS*. It can be skipped if you only want to configure HyperSwap or a z/OS IP host connection.

4.1 SMPE installation

In order to perform the CSM SMPE installation on z/OS, you need to obtain your CSM for z/OS installation files from Shopz and follow the *IBM Copy Services Manager for z Systems Program Directory* or the *IBM Copy Services Manager Basic Edition for z Systems Program Directory*, which you can find in IBM Knowledge Center:

https://www.ibm.com/support/knowledgecenter/SSESK4_6.2.3/com.ibm.storage.csm.help.doc/fqz0_r_publications.html

The following tasks perform the SMPE installation of Copy Services Manager:

- ▶ Configure jobs
- ▶ Run jobs without errors

The SMPE installation places the CSM installation packages into the specified installation root folder in UNIX System Services. It also installs the CSM sample jobs, for instance into the SYS1.SAMPLIB data set. The CSM sample jobs usually start with the IWN prefix and need to be modified for the subsequent post-installation tasks.

Note: It is a good practice to copy the sample jobs to your own CSM control data set and make necessary customizations there. Otherwise, any modifications to the jobs in the SAMPLIB data set will be overwritten with the next CSM SMPE installation, for example if you install a CSM PTF.

4.2 Post SMPE installation tasks

After you complete the SMPE installation, you have to perform some post-installation tasks, as described in IBM Knowledge Center on the CSM page *Postinstallation tasks for IBM Z*:

https://www.ibm.com/support/knowledgecenter/SSESK4_6.2.3/com.ibm.storage.csm.help.doc/frc_t_post_install_for_zos.html

The following sections describe the post installation tasks in more detail, and provide examples. If you installed an updated CSM version or PTF for an existing CSM instance, you can skip this section and continue with 4.3, “Update the CSM installation” on page 63.

4.2.1 Create Users

First, you need to create or modify existing users that will be used for the default CSM administrator account and for the CSM server started tasks. If you have IBM z/OS RACF® as a security facility, you can modify and issue the RACF commands defined in the following jobs:

- ▶ **IWNRACF1**
 - Creates the CSM default administrator, which must be used later in the installation job **IWNINSTL** (**CSM_USER**=#*csm_user variable*)
 - It is the initial user that can first log into the CSM GUI or CLI. This user has CSM administrative privileges and can add CSM access to other users (or groups) that are defined in the z/OS security facility with an OMVS segment, or LDAP users, if LDAP authentication services will be configured on the CSM server.
- ▶ **IWNRACF2**

- Creates the user ID that is associated with the CSM server address space (IWNSRV)
- This user ID requires access to the UNIX System Services production directory of CSM as set later in the installation job **IWNINSTL** (<path_prefix>/opt/IBM/CSM)

If you do not use the RACF security facility, consult your security facility documentation for appropriate commands to create the required z/OS users and permissions.

In general, RACF group names and OMVS group IDs (GIDs) have to be unique when they are associated with different user IDs (UIDs). Any authorities that are granted to the group are inherited by the users in that group. All OMVS IDs must be unique for all user IDs.

Each CSM server user ID needs the following attributes:

- ▶ The CSM default administrator should have *no* Time Sharing Option (TSO) segment. No person should be able to log in to TSO with the CSM default administrator user ID.
- ▶ Each user that is assigned to a CSM user role must have an associated password that is not expired. The user password cannot be changed through the CSM GUI or CLI. Therefore CSM access is impossible if the security facility or LDAP responds that the provided user password is expired or revoked.
- ▶ Eligible z/OS users require an OMVS segment with both, a valid OMVS ID and OMVS GID. The OMVS segment is required for CSM to be able to query and display the z/OS user on the CSM **Add User** page.

Note: To avoid unauthorized access, it is a good practice to protect the CSM default administrator user after adding additional administrative users or groups to the CSM server. To do so, change the default user to a functional user without a password.

Additional CSM users do not require any file or folder access control modifications in UNIX System Services.

In Example 4-1, we create a consolidated CSM default administrator **CSMADMIN**, which will also be associated with the CSM address space started tasks IWNSRV and IWNAUTH. We consolidated the RACF commands of **IWNRACF1** and **IWNRACF2** and customized the parameters as following:

- ▶ #group_name = CSM
- ▶ #gid = 200
- ▶ #csm_user = CSMADMIN
- ▶ #uid = 400
- ▶ #ussPath = /u/CSMADMIN
- ▶ #csm_pw = SECRET
- ▶ #interval = NOINTERVAL

Example 4-1 Create consolidated user account for CSM administrator and address spaces

```

/* Define Copy Services Manager login user ID                                */
ADDGROUP CSM OMVS(GID(200))
ADDUSER CSMADMIN DFLTGRP(CSM) OMVS(UID(400) +
    HOME(/u/CSMADMIN) +
    PROGRAM(/bin/sh)) +
    NAME('Copy Services Manager User ID')
ALU CSMADMIN PASSWORD(SECRET) NOEXPIRED
PASSWORD INTERVAL(NOINTERVAL) USER(CSMADMIN)

/* Define the started profiles.                                              */
RDEF STARTED IWNSRV.* UACC(NONE) STDATA(USER(CSMADMIN) +

```

```

GROUP(CSM) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))
/* If you plan on utilizing LDAP on the system define also IWNAUTH */
RDEF STARTED IWNAUTH.* UACC(NONE) STDATA(USER(CSMADMIN) +
GROUP(CSM) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))

SETOPTS RACLIST(STARTED) GENERIC(STARTED) REFRESH

/* Permit access to ANT.REPLICATIONMANAGER. */
RDEFINE FACILITY ANT.REPLICATIONMANAGER UACC(NONE)
PERMIT ANT.REPLICATIONMANAGER CLASS(FACILITY) +
ID(CSMADMIN) ACCESS(CONTROL)

SETOPTS RACLIST(FACILITY) REFRESH

```

You may need to consult your z/OS security administrator to successfully issue the required security facility commands.

4.2.2 Create and mount the CSM file system

CSM is supported under the UNIX System Services *z/OS File System (zFS)* or *Hierarchical File System (HFS)*. The preferred file system to use is zFS since it shows improved performance characteristics over HFS, and is the strategic direction for z/OSUSS file systems. If you already have an HFS file system, you can optionally migrate it to zFS. For more details, refer to the z/OS UNIX System Services Knowledge Center page *Migrating the HFS file system to the zFS file system*:

https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.2.0/com.ibm.zos.v2r2.bpxb200/hfszfsmi.htm

To create and mount a file system for CSM, you can follow any of these links:

- Creation of zFS file system for CSM

Refer to the CSM Knowledge Center page *Configuring the IWNCRZFS job*:

https://www.ibm.com/support/knowledgecenter/SSESK4_6.2.3/com.ibm.storage.csm.he1p.doc/csm_t_config_iwncrzfs.html

- Creation of HFS file system for CSM

Refer to the CSM Knowledge Center page *Configuring the IWNCRHFS job*:

https://www.ibm.com/support/knowledgecenter/SSESK4_6.2.3/com.ibm.storage.csm.he1p.doc/frc_t_config_iwncrhfs.html

- Mount the file system for CSM

The **IWNIMNT** sample job contains the commands to mount the created FS file system. To mount an HFS file system, you have to modify the job accordingly. For more details refer to the CSM Knowledge Center page *Configuring the IWNIMNT job*:

https://www.ibm.com/support/knowledgecenter/SSESK4_6.2.3/com.ibm.storage.csm.he1p.doc/frc_t_config_iwnimnt.html

The file system creation and mount tasks have to be performed by a TSO user with sufficient privileges:

- To mount and unmount UNIX System Services file systems

- To create, modify, delete files and directories in UNIX System Services file systems, including the root file system (UNIX System Services uid=0) and UNIX System Services uid=0 privileges or at least:
 - **CONTROL** access to **SUPERUSER.FILESYS**
 - **UPDATE** access to **SUPERUSER.FILESYS.MOUNT**
 - **READ** access to **SUPERUSER.FILESYS.CHOWN**
 - **READ** access to **SUPERUSER.FILESYS.CHANGEPERMS**
 - **READ** access to **SUPERUSER.FILESYS.PFSCtl**

In Example 4-2, we create a zFS file system by utilizing the **IWNCRZFS** job in the **SYS1.SAMPLIB** data set. We customized the parameters as following:

- #CSM.ZFS = **CSM.ZFS**
- #VOLUME = **CSMFS1**

Example 4-2 Create zFS filesystem for CSM server

```

/* Jobcard
/* Jobcard
//CREATZFS EXEC PGM=IDCAMS,REGION=64M
//SYSPRINT DD SYSOUT=A
//SYSIN DD *
    DEFINE                                +
        CLUSTER                          +
            (NAME('CSM.ZFS'))            +
            LINEAR                        +
TRK(50000,5000)                          +
        VOLUME(CSMFS1)                  +
SHAREOPTIONS(3))
/*
/* Format zFS - Note lowercase below for PARM in FORMTZFS
//FORMTZFS EXEC PGM=IOEAGFMT,REGION=64M,
// PARM='-aggregate CSM.ZFS -compat'
//SYSPRINT DD SYSOUT=A
//STDOUT DD SYSOUT=A
/*

```

Now you mount the new filesystem. In Example 4-3, we use the **IWNIMNT** job in the **SYS1.SAMPLIB** data set. We customized the parameters as follows:

- Path and mount point = **/opt/IBM/CSM**
- #CSM.ZFS = **CSM.ZFS**

Example 4-3 Mount CSM server filesystem

```

/* Jobcard
/* Jobcard
//IWNIMNT EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
    PROFILE WTPMSG MSGID
    TIME

/* Make sure mountpoints exist. */
MKDIR '/opt/IBM' MODE(7,5,5)
MKDIR '/opt/IBM/CSM' MODE(7,5,5)

```

```

/* Mount the zFS or HFS. */
MOUNT FILESYSTEM('CSM.ZFS') TYPE(ZFS) +
    MODE(RDWR) +
    MOUNTPOINT('/opt/IBM/CSM')
/*

```

Note: Make sure that the file system is automatically mounted during IPL. Otherwise CSM cannot be automatically started during the IPL.

4.2.3 Perform CSM installation in UNIX System Services

You must run the **IWNINSTL** job for the initial CSM server installation in OMVS, and for any CSM server upgrade after SMPE installation of CSM PTFs on z/OS. Refer to the Knowledge Center page *Configuring the IWNINSTL job* for details on customizing and submitting the **IWNINSTL** job:

https://www.ibm.com/support/knowledgecenter/SSESK4_6.2.3/com.ibm.storage.csm.help.doc/frc_t_post_install_for_zos_run_iwninstl.html

In Example 4-4, we use the **IWNINSTL** job in the **SYS1.SAMPLIB** data set and customize the parameters as following:

Example 4-4 Customizing IWNINSTL job

```

CLASSPATH=/usr/lpp/IBM/CSM/scripts
CSM_USER=CSMADMIN
CSM_GRP=CSM
CSM_InstallRoot=/usr/lpp/IBM/CSM
CSM_ProductionRoot=/opt/IBM/CSM
TIME_ZONE=Europe/Berlin
CLIENT_PORT=9560
HA_PORT=9561
GUI_PORT=9559
AUTH_PORT=9562
ENABLE_LDAP=false
/*CSM_ADDR_OWNER=#csm_addr_owner
/*

```

A separate CSM_ADDR_OWNER is not required in our example, since we use the default CSM admin user also as CSM address space owner. For details on usable WebSphere Java Timezone identifiers for TIME_ZONE, you can refer to:

<http://ibmurl.hursley.ibm.com/0FQW>

Optionally you can refer to Timezone IDs on Wikipedia (see TZ* identifier - Case sensitive):

https://en.wikipedia.org/wiki/List_of_tz_database_time_zones

Review the comments of the **IWNINSTL** sample job and make sure to fulfill all requirements. You must ensure that your jobcard or step specifies a **REGION OM**, otherwise the installation may fail due to insufficient resources.

The **IWNINSTL** job runs an installation script in OMVS. This script performs modifications to directory and file owners, their groups and their Access Control Lists. Therefore the **IWNINSTL** job must be submitted by a TSO user with sufficient OMVS privileges to create, modify, delete

files and directories in UNIX System Services file systems, including the root file system. In detail, the user that submits the **IWNINSTL** job needs to have:

- ▶ **READ** access to **BPX.FILEATTR.APF**
- ▶ **READ** access to **BPX.FILEATTR.PROGCTL**

If this user does not have the required OMVS privileges by default, he will need to be raised to superuser privileges as part of the **IWNINSTL** job. There exists a **su** option for **BPXBATCH** jobs, which is described in the z/OS UNIX System Services Knowledge Center page *Switching in and out of superuser authority*:

https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.bpxb200/swit.htm

- ▶ Option 1 describes a pipe into **su**. It is a simple modification to the **IWNINSTL** job, but depending on your code page settings, you need to ensure to use a proper OMVS pipe character ('|' or '!'):

Example 4-5 IWNINSTL job option to pipe execution into su

```
//IWNINSTL EXEC PGM=BPXBATCH
//STDPARM DD *
SH -PathPrefix-/usr/lpp/IBM/CSM/scripts/installCSM.sh | su
```

- ▶ Option 2 describes another way to leverage **su** which can be applied by a simple modification in the sample **IWNINSTL** job:

Example 4-6 IWNINSTL job option to leverage su prior execution

```
//IWNINSTL EXEC PGM=BPXBATCH
//STDPARM DD *
SH su
//STDIN DD *
PATH '-PathPrefix-/usr/lpp/IBM/CSM/scripts/installCSM.sh',PATHOPTS=(ORDONLY)
```

To verify a successful installation, review the output and error logs of the installation script. Their default location in UNIX System Services is as follows:

- ▶ /etc/install_CSM.log
- ▶ /etc/install_CSM_err.log

The file names and locations of those log files can be modified by **IWNINSTL** job parameters:

Example 4-7 IWNINSTL job parameters for log file locations

```
//STDOUT DD PATH='-PathPrefix-/etc/install_CSM.log',
//      PATHOPTS=(OCREAT,OAPPEND,OWRONLY),
//      PATHMODE=(SIRWXU),
//      PATHDISP=KEEP
//STDERR DD PATH='-PathPrefix-/etc/install_CSM_err.log',
//      PATHOPTS=(OCREAT,OAPPEND,OWRONLY),
//      PATHMODE=(SIRWXU),
//      PATHDISP=KEEP
```

In case you have to troubleshoot a failed initial installation and need to force another full WebSphere Liberty installation, you can specify the following parameter in your **IWNINSTL** job:

FORCE_FULL_INSTALL=TRUE

This will reinstall Liberty with the default customization based on the **IWNINSTL** job parameters. Any post installation customization of Liberty property files will be lost when using this option. This option must not be used or set to FALSE when running the **IWNINSTL** job for a CSM update.

4.2.4 Create started tasks for CSM server

The CSM server consists of the following address spaces, usually running as started tasks:

- ▶ **IWNSRV** (required)
- ▶ **IWNAUTH** (optional, only required for LDAP user authentication services)

For a detailed explanation of these address spaces, see 2.2, “z/OS relevant address spaces for CSM” on page 25.

To launch these address spaces as started tasks, you configure appropriate jobs in the **PROCLIB** system library. CSM provides sample jobs in **SYS1.SAMPLIB**. See the following IBM Knowledge Center CSM pages for details about customizing the **IWNSRV** and optional **IWNAUTH** jobs:

- ▶ https://www.ibm.com/support/knowledgecenter/SSESK4_6.2.3/com.ibm.storage.csm.help.doc/frc_t_config_proclib_liberty.html
- ▶ https://www.ibm.com/support/knowledgecenter/SSESK4_6.2.3/com.ibm.storage.csm.help.doc/csm_t_config_iwnauth.html

After the job definitions are created in the **PROCLIB** system library, you can start these address spaces in one of the following ways:

- ▶ Issue the MVS **START** command manually, for example **START IWNSRV**
- ▶ Include the **START** command in the **COMMNDxx** member of your **SYSx.PARMLIB** data set, so it launches automatically during IPL. Alternatively, you can also add it to your system automation facility.

In our scenario, we customized the **IWNSRV** and **IWNAUTH** jobs in the **SYSx.PROCLIB** system library, as shown in Example 4-8 and Example 4-9.

Example 4-8 IWNSRV launch job

```
//IWNSRV PROC PARMS='csmServer'
//*-----
// SET INSTDIR='/opt/IBM/CSM/wlp'
// SET USERDIR='/opt/IBM/CSM/wlp/usr'
//*-----
//* Start the server
//*-----
//STEP1 EXEC PGM=BPXBATSL,REGION=OM,TIME=NOLIMIT,
// PARM='PGM &INSTDIR./lib/native/zos/s390x/bbgzsrv &PARMS'
//WLPUDIR DD PATH='&USERDIR.'
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
```

Example 4-9 IWNAUTH launch job

```
//IWNAUTH PROC PARMS='csmAuth'
//*-----
// SET INSTDIR='/opt/IBM/CSM/wlp'
// SET USERDIR='/opt/IBM/CSM/wlp/usr'
```

```

/*-----
/* Start the server
/*-----
//STEP1 EXEC PGM=BPXBATSL,REGION=OM,TIME=NOLIMIT,
// PARM='PGM &INSTDIR./lib/native/zos/s390x/bbgzsrv &PARMS'
//WLPUDIR DD PATH='&USERDIR.'
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*

```

To stop the IWNSRV or IWNAUTH started tasks, you can issue the MVS **STOP** command, as shown in Example 4-10.

Example 4-10 Stop CSM server and authentication server

```

STOP IWNSRV
STOP IWNAUTH

```

4.3 Update the CSM installation

If you need to install a CSM PTF or a new version of CSM, see the detailed upgrade description available in IBM Knowledge Center for CSM under *Upgrading on z/OS*:

https://www.ibm.com/support/knowledgecenter/SSESK4_6.2.3/com.ibm.storage.csm.help.doc/frg_t_upgrade_tpcrz_server.html

We describe the high-level tasks necessary to upgrade a CSM server that is configured in a CSM server high availability (HA) relationship in the following list:

1. Perform the SMPE installation of the PTF or updated installation images on all logical partitions (LPARs) you want to upgrade CSM on.
2. Verify that the synchronization of the CSM standby server is complete and that all active sessions are not in a transitory state, such as **Preparing**, **Suspending**, or **Recovering**.
3. Move the CSM management to the secondary CSM server by issuing the **Takeover** command on the standby server.
4. On the primary server, remove the standby server from the HA relationship definition. The active CSM on the secondary server continues to manage the sessions during the upgrade process on the primary server.
5. Stop the CSM address spaces on the primary server by issuing the following commands:
 - **STOP IWNSRV**
 - **STOP IWNAUTH**
6. Run your customized **IWNINSTL** job again to complete the upgrade on the primary server. For more details on customizing the **IWNINSTL** job, see the information about post-SMPE installation in 4.2.3, “Perform CSM installation in UNIX System Services” on page 60.
7. If the sessions did not change their state during the upgrade, restart CSM on the primary server. Verify that it shows all sessions in the same state as they were before the upgrade.
8. Repeat steps 4 through 7 on the secondary server.
9. Reestablish the HA relationship that was originally set up between the primary and secondary server



IBM z/OS IP host connection setup

The IBM z/OS IP host connection is a connection from an IBM Copy Services Manager (CSM) server to a z/OS logical partition (LPAR), which must run the HyperSwap address spaces and serve an IP address that can be used for the connection.

The HyperSwap Manager address space can be configured with the **SOCKPORT** parameter to allow authenticated IP connections from CSM servers. It is used as a proxy to connect CSM to the LPAR Input/Output supervisor (IOS) in order to provide a communication path for its FICON device management. Furthermore it provides a communication path for CSM to manage z/OS HyperSwap or Hardened Freeze of the Sysplex where the connected LPAR is running.

Note: A z/OS IP host connection requires that the HyperSwap address spaces (HSIB & HSIBAPI) are active and HSIB is using the **SOCKPORT** parameter to establish the connection. If encryption is enabled for the z/OS IP host connections (default), the LPAR must also run the PAGENT address space with a loaded Application Transparent Transport Layer Security (AT-TLS) policy that describes the certificates to be used to encrypt/decrypt traffic over the HyperSwap Manager socket port.

For a detailed explanation of these required address spaces, see 2.2, “z/OS relevant address spaces for CSM” on page 25.

5.1 Configuration tasks overview

The high-level configuration tasks required to set up a z/OS IP host connection from the CSM server are shown in Table 5-1. You perform the majority of these configuration tasks on the LPARs that are used for the z/OS IP host connection.

Table 5-1 IBM z/OS configuration tasks depending on CSM version and security

z/OS tasks overview	Before CSM 6.1.5	CSM 6.1.5 or later	Without encryption
Configure z/OS users for HyperSwap started tasks and host connection authentication	YES	YES	YES
Configure HyperSwap Manager (HSIB) to use a TCP/IP port for incoming connections from CSM servers	YES	YES	YES
Create z/OS certificates: <ul style="list-style-type: none">► Obtain CA certificate from trusted CA or create self signed CA certificate► Create server certificate signed with CA certificate► Create RACF key ring with HyperSwap user ID and connect it to certificates Note: If CSM is on Hardware Management Console (HMC), make sure certificate key size is at least 2048	YES	YES	-
Export CA certificate to a file for use by CMS server	YES	YES	-
Configure AT-TLS policy via policy template or z/OSMF: <ul style="list-style-type: none">► Define the incoming HSIB port to apply the policy► Define the key ring to be used for the encryption► Note: If CSM is on HMC, use only TLSv1.2 protocol and use strong ciphers	YES	YES	-
Configure z/OS PAGENT to use the AT-TLS policy	YES	YES	-

The CSM server itself simply needs the public key of the z/OS certificate in its keystore repository to establish an encrypted z/OS IP host connection.

Table 5-2 provides an overview of the required CSM server tasks.

Table 5-2 CSM server configuration tasks depending on CSM version and security

CSM tasks overview	Before CSM 6.1.5	CSM 6.1.5 or higher	Without encryption
Generate Java keystore file for CSM servers: <ul style="list-style-type: none"> ► Create keystore file via IKEYMAN or IKEYCMD and add exported CA certificate ► Transfer Java keystore to CSM server(s) and activate via CSM restart 	YES	-	-
Create the CSM host connection via CSM GUI/CLI	YES	YES	YES
Add the certificate to the host connection via GUI	Not supported	YES	-
If CSM is on HMC, make sure that the HSIB port is unblocked in the HMC firewall	No z/OS IP host connection support from DS8880 HMCs	YES	YES

Note: Starting with DS8880 R8.2, the default HSIB port 5858 is open in the HMC firewall. For older releases or non default HSIB port implementations you need IBM DS8000 product support to modify the HMC firewall settings to open required ports.

The following sections contain more details for each of the listed tasks. For a complete task flow and additional considerations, review all sections.

For additional details about securing the CSM z/OS IP host connections, you can also refer to 7.1.3 “Securing TCP/IP communication for CSM: An overview” and 7.1.4, “Securing communication between z/OS HyperSwap and the CSM Server” in *IBM Copy Services Manager Implementation Guide*, SG24-8375:

<http://www.redbooks.ibm.com/abstracts/sg248375.html?Open>

5.2 Disable encryption for z/OS IP host connections

WARNING: Encryption for z/OS IP host connections is required by default. Disabling it may be useful for a quick and simplified test setup or for connection debugging, because it eliminates the complexity of a secure AT-TLS setup. For productive environments, it is good practise to leave security enabled, and configure proper TLS 1.2 and AT-TLS encryption.

The CSM server z/OS IP host connection settings are configured via the `zosclient.properties` file. The file is located in UNIX System Services in the folder shown in Example 5-1.

Example 5-1 CSM server property files location

```
path_prefix/opt/IBM/CSM/wlp/usr/servers/csmServer/properties/
```

In order to avoid direct property file modifications in the CSM server file system, CSM 6.1.5 introduced the CSMCLI **chsystem** command to modify settings in the CSM property files through a user interface. The **chsystem** command syntax and usage is described in IBM Knowledge Center for CSM:

https://www.ibm.com/support/knowledgecenter/en/SSESK4_6.2.3/com.ibm.storage.csm.help.doc/frg_r_cli_chsystem.html

To disable encryption for z/OS IP host connections on a CSM server, you can issue the CSMCLI command shown in Example 5-2.

Example 5-2 Disable encryption for z/OS IP host connections

```
chsystem -f zosclient -p  
com.ibm.ess.api.client.zos.ip.ZOSSocketConnectionMonitor.ENCRYPTION -v false
```

By default, this property does not exist in the `zosclient.properties` file. It is added and set to `false` by the **chsystem** command. You need to restart the CSM server to activate changed encryption settings for the z/OS IP host connections.

To enable encryption again, the property can either be removed manually or set to `true` using the **chsystem** command, as shown in Example 5-3.

Example 5-3 Enable encryption for z/OS IP host connections

```
chsystem -f zosclient -p  
com.ibm.ess.api.client.zos.ip.ZOSSocketConnectionMonitor.ENCRYPTION -v true
```

Important: In a CSM server high availability (HA) environment with active and standby CSM servers, any CSM server property change must be performed on both CSM servers individually. The server property files are not replicated.

If the encryption setting is only disabled on the active CSM server but not on the standby server, you may run into a situation where the active CSM server connects successfully to the defined z/OS LPAR, but the standby server fails to connect. This may limit management capabilities after you perform a **takeover** command on the standby CSM server.

5.3 Configure z/OS users for HyperSwap tasks and z/OS IP host connections

In order to launch the HyperSwap address spaces, you need z/OS users to assign to these tasks. You need an additional z/OS user for the external CSM servers to authenticate against the HyperSwap Manager socket server.

IBM Knowledge Center for CSM provides RACF sample jobs to create those users and assign proper permissions to them. For more details, see *Configuring the IWNRACT jobs*:

https://www.ibm.com/support/knowledgecenter/SSESK4_6.2.3/com.ibm.storage.csm.help.doc/frc_t_config_iwnracf.html

You modify and issue the RACF commands defined in the following jobs to create the necessary users with proper permissions:

► **IWNRACT3**

- Creates the user IDs that are associated with the HyperSwap address spaces (HSIB and HSIBAPI).
- The specified user and group also require access to OMVS when the HyperSwap Socket Server is being used for a z/OS IP host connection.

See “HyperSwap address spaces and started tasks” on page 98 for more details about the users required for HyperSwap.

► **IWNRACT4**

- Creates the user IDs that are associated with the HyperSwap Socket Server address space (BHIHSRV).
- This job is only necessary if you are going to establish a z/OS IP host connection.

► **IWNRACT5**

- Creates the CSM z/OS IP host connection user ID and password.
- It is used by CSM servers to authenticate to the HyperSwap Sockets Server.

You can create separate users for each task, or consolidate multiple roles into a single TSO user. The following example demonstrates how to configure a consolidated user for all the HyperSwap address spaces and a separate user for z/OS IP host connection authentication:

► **BHIHGRP 100**

- Example group name and group ID for the users.

► **BHIHSRV 300**

- Example user name and user ID to run the HSIB and HSIBAPI started tasks for HyperSwap.
- It will also be used for internally started HyperSwap Socket Server address spaces BHIHSRV that are launched for each z/OS IP host connection.
- This user does not need a password and therefore can be a protected user.

► **BHIHUSR**

- Example user name that is used by the CSM servers for authentication to the HyperSwap Socket Server address space BHIHSRV.
- This user needs to get an unexpired password (in our example, *my_password*).
- The password interval can be defined as required by your security rules.

Note: If the password for the socket connection authentication expires, the socket connection will stop working. You have to make sure that the password is changed in time and that the changed password is also specified in the CSM socket connection definition. See “Create the CSM IP host connection” on page 91 for details.

Based on the **IWNRACFx** sample jobs, Example 5-4 shows the consolidated commands that are required to configure these users, groups, and started profiles appropriately in the RACF security facility.

Example 5-4 RACF commands to create consolidated HyperSwap users and profiles

```

/* Define the HyperSwap address space user ID and group.          */
ADDGROUP BHIHGRP OMVS(GID(100))
ADDUSER BHIHSRV DFLTGRP(BHIHGRP) OMVS(UID(300) HOME('/')) -
        NAME('HyperSwap Address Spaces') NOPASSWORD
ADDUSER BHIHUSR DFLTGRP(BHIHGRP) -
        NAME('Copy Services Manager Host Connection User ID')
ALU BHIHUSR PASSWORD(my_password) NOEXPIRED -
PASSWORD INTERVAL(xxx|NOINTERVAL) USER(BHIHUSR)

/* Define the started profiles.                                    */
RDEF STARTED HSIBAPI.* UACC(NONE) STDATA(USER(BHIHSRV) -
        GROUP(BHIHGRP) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))
RDEF STARTED HSIB.* UACC(NONE) STDATA(USER(BHIHSRV) -
        GROUP(BHIHGRP) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))
RDEF STARTED BHIHSRV.* UACC(NONE) STDATA(USER(BHIHSRV) -
        GROUP(BHIHGRP) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))
SETOPTS RACLIST(STARTED) GENERIC(STARTED) REFRESH

/* Define and Permit access to ANT.REPLICATIONMANAGER facility    */
RDEFINE FACILITY ANT.REPLICATIONMANAGER UACC(NONE)
PERMIT ANT.REPLICATIONMANAGER CLASS(FACILITY) ID(BHIHSRV) - ACCESS(CONTROL)
PERMIT ANT.REPLICATIONMANAGER CLASS(FACILITY) ID(BHIHUSR) - ACCESS(CONTROL)
SETOPTS RACLIST(FACILITY) REFRESH

```

If you perform a different user role consolidation, you must adopt the required RACF commands from the **IWNRACFx** sample jobs accordingly. If you do not use the RACF security facility, consult your security facility documentation for corresponding commands to create the required user roles and permissions.

5.4 Configure HyperSwap tasks with socket port

You have to create jobs or started tasks to launch the HyperSwap address spaces HSIB and HSIBAPI. The HyperSwap management address space HSIB must be configured with the **SOCKPORT** parameter as described in IBM Knowledge Center for CSM under *Preparing to use HyperSwap from z/OS*:

https://www.ibm.com/support/knowledgecenter/SSESK4_6.2.3/com.ibm.storage.csm.help.doc/frc_c_basichsconfig.html

Following are example jobs for the started tasks. Example 5-5 shows the job for the HSIBAPI address space.

Example 5-5 HSIBAPI address space

```

//HSIBAPI JOB MSGLEVEL=(1,1),TIME=NOLIMIT,REGION=0M
//          EXEC PGM=IOSHSAPI

```

Example 5-6 on page 71 shows the job for the HSIB address space using the default HyperSwap Socket port 5858.

Example 5-6 HSIB address space

```
//HSIB JOB MSGLEVEL=(1,1),TIME=NOLIMIT,REGION=0M
//IEFPROC EXEC PGM=IOSHMCTL,PARM='SOCKPORT=5858'
```

Note: The port that you specify with the **SOCKPORT** parameter must be opened in firewalls between the CSM servers and the LPAR where you configure the z/OS Host Connection. Port 5858 is the default port which is already enabled in DS8880 HMC firewall rules in case the CSM servers run on the HMC.

When you want to establish a z/OS IP host connection, both address spaces (HSIB and HSIBAPI) must be started on each LPAR used for connections from the external CSM servers. Both address spaces are required for a z/OS IP host connection, even if HyperSwap is not used. You can start these address spaces in one of the following ways:

- ▶ Issue the MVS **START** command manually.
- ▶ Include the **START** command in the **COMMNDxx** member of the **SYSx.PARMLIB** data set.

Note: It is preferred, although not required, that you start HSIBAPI before HSIB. HSIB does not get ready until HSIBAPI is running.

Example 5-7 shows the MVS **START** and **STOP** commands for the two address spaces.

Example 5-7 Start and stop of HyperSwap address spaces

```
START HSIBAPI,SUB=MSTR
START HSIB,SUB=MSTR

STOP HSIB
STOP HSIBAPI
```

After the HyperSwap tasks are active, verify that they are running under the user you specified in your RACF commands. Example 5-8 shows the running address spaces on the two LPARs MCECEBC and MZBCVS2 in the Sysplex.

Example 5-8 Running HyperSwap address spaces

```
COMMAND INPUT ==> DA                                SCROLL ==> CSR
PREFIX=HS* DEST=(ALL) OWNER=* SORT=SYSNAME/A SYSNAME=*
NP  JOBNAME  StepName ProcStep JobID   Owner   CPU%  CPU-Time SR Status SysName
    HSIBAPI  HSIBAPI             STC09135 BHIHSRV 0.00   4.59           MCECEBC
    HSIB     HSIB      STEP      STC09109 BHIHSRV 0.00  863.81           MCECEBC
    HSIBAPI  HSIBAPI             STC09136 BHIHSRV 0.00   4.72           MZBCVS2
    HSIB     HSIB      STEP      STC01416 BHIHSRV 0.01  770.76           MZBCVS2
```

For using the z/OS IP host connection, the HSIB Owner user ID (in our examples BHIHSRV) must be the one that you granted access to the FACILITY ANT.REPLICATIONMANAGER previously. It must also be used in the following sections to assign a RACF keyring with certificates for the encryption of the CSM z/OS IP host connection, because the owner of the HSIB task needs read access to the certificates.

Note: The BHIHSRV (IEESYSAS) address space is managed internally by HSIB and automatically started for each established host connection. It will also be stopped if the z/OS IP host connection is lost.

5.5 Create z/OS certificates

This section describes how z/OS certificates can be generated for the z/OS IP host connection encryption. The overall process to configure a z/OS certificate is as follows:

1. Use an existing or obtain a new Certificate Authority (CA) certificate (Root Certificate) and import it in z/OS security facility.
2. Create a new trusted server certificate signed by the CA certificate.
3. Create a key ring in the z/OS security facility and connect it to the trusted server certificate which is stored in the z/OS security facility database with the identities to be used for encryption.

The following sections describe each of those tasks in more detail.

5.5.1 Certificate considerations when multiple LPARs connect to CSM server

All CSM servers that connect to a z/OS LPAR, like the active and standby server, must have a copy of the z/OS HyperSwap Manager certificate in their z/OS Host Connection keystore. Prior to CSM 6.1.5, a z/OS Host Connection Java keystore (JKS) file had to be configured manually. Starting with CSM 6.1.5, a z/OS Host Connection certificate can be imported into the keystore using the CSM GUI.

If a CSM server connects to multiple z/OS LPARs, all of them must have AT-TLS active and configured. They can all use the same certificate, or each one can have its own. In the latter case, all certificates must be present in the CSM server keystore.

A combination of these options is also possible. For example, if the active and standby CSM server manage several HyperSwap sessions, with each Sysplex using a different certificate, which all LPARs within each Sysplex have in common.

5.5.2 CA Certificate generation

In order to create a new certificate to secure z/OS IP host connections, you first need a Certificate Authority (CA) certificate (or Root Certificate), which is used to sign a created server certificate.

Note: When CSM is running on a DS8880 HMC, you need a certificate with a key SIZE of at least 2048.

There are 3 ways to provide such a CA certificate:

- ▶ Use the default CA certificate that comes with CSM.
- ▶ Generate your own (self-signed) CA certificate within your z/OS security facility.
- ▶ Obtain a CA certificate from an established Certificate Authority, either your own company's or one of the public Certificate Authorities.

In the following sections we describe these 3 options.

Import the default CA certificate

Note: This is the easiest way to provide a CA certificate. However, it may violate your company security rules, because this CA certificate is not unique and publicly available.

The CSM installation places a default CA certificate in a file in the CSM installation space. Using this option to obtain a CA certificate is the most convenient one, but also least secure because the CA certificate is commonly provided with CSM. The following location is the default CSM CA certificate:

<CSM production root>/wlp/usr/servers/replicationServer/etc/zosKey.p12

Example 5-9 shows the location if CSM is running on z/OS.

Example 5-9 Default CSM CA certificate location on z/OS

/opt/IBM/CSM/wlp/usr/servers/replicationServer/etc/zosKey.p12

In order to work with this certificate file, you must copy into a z/OS data set on all z/OS LPARs that should be connected by this particular CSM server. You can use the following methods to place the certificate file into a data set:

- ▶ Use an FTP or SCP utility to upload the file into the UNIX System Services file space, and then use the **0GET** TSO command to place it into a z/OS data set.
- ▶ Use an FTP or SCP utility to upload the file into the UNIX System Services file space, and then use the **copy out** option of the **obrowse** tool to place it into a z/OS data set.
- ▶ Use an FTP utility to upload the file directly into a z/OS data set.

After the certificate data set is available on the LPAR, you must import the certificate to the z/OS security facility. Example 5-10 shows commands to import the certificate into RACF. The commands import the certificate and assign it a label and a password.

Example 5-10 Import certificate from data set into RACF

```
RACDCERT ADD(DATASETNAME) CERTAUTH WITHLABEL('CSM Certificate Authority') -  
KEYUSAGE(CERTSIGN) PASSWORD('PASSWORD') NOTAFTER(DATE(2028-12-31) -  
TIME(12:00:00))
```

The user-defined password *PASSWORD* must be provided, but will not be needed afterwards. NOTAFTER DATE and TIME specify the expiration timestamp of the certificate and can be changed as required.

Important: The corresponding CA certificate label (in this example '*CSM Certificate Authority*') is *case sensitive* and must be used throughout all subsequent commands that refer to the CA certificate.

Finally, perform a RACF refresh to make the new certificate available, as shown in Example 5-12 on page 74.

Create your own self-signed CA certificate

This is a convenient option if no CA certificate from an established Certificate Authority is already available. Example 5-11 shows how to create your own self-signed CA certificate using RACF commands.

Example 5-11 RACF commands to create self signed CA certificate

```
RACDCERT GENCERT CERTAUTH SUBJECTSDN -  
(OU('CSM Certificate Authority') O('CSM') C('DE')) KEYUSAGE(CERTSIGN) - SIZE(2048)  
WITHLABEL('CSM Certificate Authority')
```

Set the parameters OU, O, and C according to your organization's rules:

- ▶ OU('organization-unit-name')
- ▶ O('organization-name')
- ▶ C('country-code')

Important: The corresponding CA certificate Label (in our example '*CSM Certificate Authority*') is *case sensitive* and must be used throughout all subsequent commands that refer to the CA certificate.

Finally, perform a RACF refresh to make the new certificate available, as shown in Example 5-12.

For additional details about how to create such a CA certificate, you can also refer to chapter 7.1.5 “Generating a self-signed (CA) certificate in z/OS” in the Redbooks publication, *IBM Copy Services Manager Implementation Guide*, SG24-8375:

<http://www.redbooks.ibm.com/abstracts/sg248375.html>

Obtain a CA certificate from an established CA

You can also obtain the CA certificate from an establish Certificate Authority in a format that can be imported by your z/OS security facility. For the import process, you can follow the import steps as described in “Import the default CA certificate” on page 72.

Perform a RACF refresh, so that the new certificate is available.

After importing a new certificate into your z/OS security facility, you might have to perform a refresh operation to make the certificate available. Example 5-12 shows this action in RACF.

Example 5-12 RACF refresh

```
SETR CLASSACT(DIGTCERT)
SETR RACLIST(DIGTCERT)
SETR RACLIST(DIGTCERT) REFRESH
```

5.5.3 Create server certificate and keyring

Here, we describe the creation of a signed server certificate using the CA certificate. The sequence is independent of how you obtained the CA certificate previously.

Important: The corresponding CA certificate label (case sensitive) must be used here to refer to the CA certificate. In our example, we use our own created CA certificate '*CSM Certificate Authority*' from “Create your own self-signed CA certificate” on page 73.

Complete the following steps:

Note: When CSM is running on a DS8880 HMC, you need a CA certificate and a server certificate with a key SIZE of at least 2048. Otherwise a key size of 1024 might be sufficient to satisfy your security requirements.

1. Use your z/OS security facility to generate a new server certificate for the user ID that is associated with the HyperSwap Manager Socket Server process. It is the user that was created with the commands from sample job **IWNRACT4**. Example 5-13 on page 75 shows the required RACF commands to generate a signed server certificate.

Example 5-13 RACF commands to create signed server certificate

```
RACDCERT ID(BHIHSRV) GENCERT SUBJECTSDN(CN('CSM Client') -  
OU('Hyperswap Server') O('CSM') C('US')) -  
SIZE(2048) WITHLABEL('Hyperswap Manager') -  
SIGNWITH(CERTAUTH LABEL('CSM Certificate Authority')) -  
KEYUSAGE(HANDSHAKE) NOTAFTER(DATE(2028-12-31) TIME(12:00:00))
```

2. Set the parameters OU, O, and C according to your organization's rules using the following format:

- OU('organization-unit-name')
- O('organization-name')
- C('country-code')

3. Set the expiration date and time as required using the following format:

- NOTAFTER(DATE(yyyy-mm-dd) TIME(hh:mm:ss))

This specifies the local DATE and TIME after which the certificate is no longer valid. This parameter is required for durations that differ from the default of 1 year.

Note: When the certificate is expired, the communication between the CSM server and the LPAR will break and new certificates must be issued and configured on z/OS and the CSM server keystore database.

4. Next, you create a new keyring in your security facility for the user ID that is associated with the HyperSwap Manager Socket Server process. It is again the user that was created with the commands from sample job **IWNRRACF4**. Example 5-14 shows the required RACF command to generate a keyring. You can choose any keyring label, but note that these labels are case sensitive.

Example 5-14 RACF command to create a keyring

```
RACDCERT ID(BHIHSRV) ADDRING(csmkeyring)
```

5. Now connect the CA certificate to the created keyring. Example 5-15 shows the required RACF command (labels are case sensitive).

Example 5-15 RACF command to connect CA certificate to keyring

```
RACDCERT ID(BHIHSRV) CONNECT(CERTAUTH -  
LABEL('CSM Certificate Authority') RING(csmkeyring))
```

6. Then connect the created server certificate to the keyring as well. Example 5-16 shows the required RACF command (labels are case sensitive).

Example 5-16 RACF command to connect server certificate to keyring

```
RACDCERT ID(BHIHSRV) CONNECT(ID(BHIHSRV) LABEL('Hyperswap Manager') -  
RING(csmkeyring) default)
```

7. Give the user ID permission to read its own keyring, as shown in Example 5-17.

Example 5-17 RACF commands to grant keyring read permission to user

```
RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE)  
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(BHIHSRV) ACCESS(READ)
```

8. Finally, verify the certificates and keyring in your security facility. Example 5-18 shows how you can use the RACF **RACDCERT LIST** and **RACDCERT LISTRING** commands to confirm the generation of the keyring and the correct connection of the certificates.

Example 5-18 RACF commands to verify keyring and certificates

RACDCERT LIST(LABEL('Hyperswap Manager')) ID(BHIHSRV)

Digital certificate information for user BHIHSRV:

Label: Hyperswap Manager
Certificate ID: 2Qfi48Pk4sXZyKiXhZmipoGXQNSB1YGHhZ1A
Status: TRUST
Start Date: 2014/07/24 00:00:00
End Date: 2028/12/31 12:00:00
Serial Number:
>01<
Issuer's Name:
>OU=CSM Certificate Authority.0=CSM.C=DE<
Subject's Name:
>CN=CSM Client.OU=Hyperswap Server.0=CSM.C=DE<
Key Usage: HANDSHAKE
Key Type: RSA
Key Size: 2048
Private Key: YES
Ring Associations:
Ring Owner: BHIHSRV
Ring:
>csmkeyring<

RACDCERT LISTRING(csmkeyring) ID(BHIHSRV)

Digital ring information for user BHIHSRV:

Ring:
>csmkeyring<
Certificate Label Name Cert Owner USAGE DEFAULT

Hyperswap Manager ID(BHIHSRV) PERSONAL YES
CSM Certificate Authority CERTAUTH CERTAUTH NO

5.5.4 Sample CLISTs

The RACF commands to import the default CA certificate, or to create a local one, are also provided in two sample command lists (CLISTs) that you can find in the same directory as the default certificate. They are located in following folder if CSM is installed on z/OS:

<CSM production root>/wlp/usr/servers/replicationServer/etc

The sample CLISTs are called `CERTIMPT.sample` and `CERTCRE8.sample`. You can use them to perform the steps described in previous sections.

Note: Labels and names in the sample CLISTs might be different from the example provided in this book. Be aware that some of the labels and names are case-sensitive.

5.6 Export CA certificate

You have to export the CA certificate into a z/OS data set, make it available as a file for further use, and to import into the CSM keystore, as shown in Example 5-19. In the following examples, we use the data set name *CSM.LOCCERTA.CERT*.

Example 5-19 RACF commands to export certificate to data set

```
RACDCERT EXPORT (LABEL('CSM Certificate Authority') +  
CERTAUTH DSN('CSM.LOCCERTA.CERT') FORMAT(CERTDER))
```

You now transfer the exported CA certificate to a system from which you plan to configure the CSM z/OS IP host connection, for example the CSM server itself or your local workstation where you run the CSM GUI.

Note: For CSM versions earlier than 6.1.5, you must create or update the CSM keystore file manually. You create a Java Key Store (JKS) file using the IBM Key Management utilities, and then copy it to the CSM servers. Follow the CSM 6.1.4 instructions available in IBM Knowledge Center under *Configuring a secure communication between HyperSwap and the client*:

https://www.ibm.com/support/knowledgecenter/SSESK4_6.1.4/com.ibm.storage.csm.helpl.doc/frc_t_config_hyper_secure_connection.html

The easiest way to transfer a z/OS data set to a PC file is to use FTP. Because the certificate was exported in a binary mode, you also have to use a binary mode for the file transfer. Example 5-20 shows how to transfer the certificate data set to a Windows PC using plain FTP.

Example 5-20 Transfer a z/OS data set to a PC file

```
C:\Users\IBM_ADMIN>ftp mcecebc.mainz.de.ibm.com  
Connected to mcecebc.mainz.de.ibm.com.  
220-FTP Server (user 'home@de.ibm.com')  
220  
User (mcecebc.mainz.de.ibm.com:(none)): HOME  
331-Password:  
331  
Password:  
230-220-FTPD1 IBM FTP CS V2R2 at MCECEBC.MAINZ.DE.IBM.COM, 15:41:17 on  
2018-06-29.  
230-HOME is logged on. Working directory is "/u/home".  
ftp> bin  
Representation type is Image  
ftp> get 'CSM.LOCCERTA.CERT' 'csm.loccerta.cert'  
local: 'csm.loccerta.cert' remote: 'CSM.LOCCERTA.CERT'  
Port request OK.  
Sending data set CSM.LOCCERTA.CERT  
Transfer completed successfully.  
bytes received in 0.00 secs (173.9 kB/s)  
ftp> bye  
Quit command received. Goodbye.
```

You now find the received certificate file *csm.loccerta.cert* in your local directory from where you launched FTP, and you can import it as described in 5.10, “Create the CSM IP host connection” on page 91.

5.7 Configure AT-TLS policy

The AT-TLS policy is a configuration file for the z/OS PAGENT address space, which can either be created with the *z/OS Management Facility (z/OSMF)* or manually with a text editor using a policy template file.

z/OSMF is a no charge z/OS software component, but must be implemented separately. If it is available in your environment, it is the most convenient way to create the necessary AT-TLS policy. Chapter “7.1.7 Configuring AT-TLS on z/OS” in *IBM Copy Services Manager Implementation Guide*, SG24-8375 contains detailed instructions about how to create and upload a policy file with z/OSMF.

If z/OSMF is not available, a quick and convenient approach to create a policy file for the z/OS IP host connection is to use the provided policy template file. In this section, we explain how to adopt it to your environment. Consult your security and network administrators to meet your local security policies and configure PAGENT AT-TLS policy accordingly.

Note: The z/OS PAGENT policy configuration process must be performed for each z/OS LPAR that runs a HyperSwap Manager address space (HSIB) with an IP connection to one or more CSM servers. If you use different CA certificates per LPAR or Sysplex, make sure that you specify the correct labels for keyring and server certificates in the Traffic Type Specification section.

In our PAGENT configuration example, we use an OMVS policy file (*tlsPol.conf*) that is placed in `/etc/pagent` under a subfolder with the applicable IP stack name (*TCPIPBC*), as shown in Example 5-21.

Example 5-21 PAGENT configuration file

`/etc/pagent/TCPIPBC/tlsPol.conf`

Example 5-22 shows our TLS policy file. The parameters you have to adapt to your environment are marked in blue. The red parameters must remain as they are for full functionality and sufficient encryption strength to support CSM on DS8880 HMCs.

Make sure to use the correct labels (case-sensitive) to match the certificate and keyring previously configured in your z/OS security facility.

Example 5-22 PAGENT policy file

```
##
## AT-TLS Policy Agent Configuration file for:
## Image: MCECEBC
## Stack: TCPIPBC
##
TTLSRule CSM
{
  LocalAddr ALL
  RemoteAddr ALL
  LocalPortRangeRef portLR1
  RemotePortRangeRef portRR1
  Direction Both
  Priority 255
  TTLSGroupActionRef gAct_CSM
  TTLSEnvironmentActionRef eAct_CSM
```

```

TTLSTLSConnectionActionRef cAct_CSM
}
TTLSTLSGroupAction gAct_CSM
{
  TTLSEnabled On
}
TTLSTLSEnvironmentAction eAct_CSM
{
  HandshakeRole Server
  EnvironmentUserInstance 0
  TTLSKeyringParmsRef keyR1
}
TTLSTLSConnectionAction cAct_CSM
{
  HandshakeRole Server
  TTLSCTLS cipherParmsRef cipher1_TLS
  TTLSConnectionAdvancedParmsRef cAdv1_CSM
  CtraceClearText Off
  Trace 2
}
TTLSTLSConnectionAdvancedParms cAdv1_CSM
{
  SSLv3 Off
  TLSv1 Off
  TLSv1.1 Off
  TLSv1.2 On
  CertificateLabel Hyperswap Manager
  HandshakeTimeout 30
  SecondaryMap Off
}
TTLSTLSKeyringParms keyR1
{
  Keyring csmkeyring
}
TTLSTLSCTLS cipherParms cipher1_TLS
{
  V3CipherSuites TLS_RSA_WITH_AES_128_CBC_SHA256
  V3CipherSuites TLS_RSA_WITH_AES_256_CBC_SHA256
  V3CipherSuites TLS_RSA_WITH_AES_128_GCM_SHA256
}
PortRange portLR1
{
  Port 5858
}
PortRange portRR1
{
  Port 1024-65535
}

```

You can also see IBM Knowledge Center for CSM under *Creating and deploying a policy file for Application Transparent Transport Layer Security* for another AT-TLS policy file template:

https://www.ibm.com/support/knowledgecenter/SSESK4_6.2.3/com.ibm.storage.csm.help.doc/frc_t_create_policy_attls.html

5.8 Configure the z/OS TCP/IP policy agent (PAGENT)

The z/OS TCP/IP policy agent (PAGENT) is an optional software component to allow the IP stack to use policies. Policies can be defined for IP filtering and encryption. In order to secure CSM z/OS IP host connections, you only need the encryption capability. Therefore, the provided policy examples only contain encryption rules for the PAGENT. This policy (or encryption rules) must be activated now for the policy agent.

Ask your z/OS network administrator to reconfigure the appropriate TCPIP stack to activate or update the policy agent (PAGENT) on all required LPARs. Also see IBM Knowledge Center for z/OS describing the policy agent configuration as a started task:

https://www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.hal2001/startingpolicyagentasastartedtask.htm

Make sure that the Policy Agent address space is automatically started at IPL, for example by adding a **PROCLIB** member. The definition used to start the PAGENT must contain a statement that points to an existing configuration file.

Example 5-23 shows the PAGENT PROCLIB member in our environment. It points to the OMVS environment file */etc/pagent/pagent.env*, where the first level configuration is maintained.

Example 5-23 PAGENT configuration to use an OMVS environment file

```
//PAGENT PROC
//PAGENT EXEC PGM=PAGENT,REGION=0K,TIME=NOLIMIT,
// PARM='ENVAR("_CEE_ENVFILE=DD:STDENV")/-c /etc/pagent/page
// nt.conf -1 SYSLOGD'
//*
//STDENV DD PATH='/etc/pagent/pagent.env',PATHOPTS=(ORDONLY)
//*
//SYSPRINT DD SYSOUT=*
//SYSOUT DD SYSOUT=*
//*
//CEEDUMP DD SYSOUT=*,DCB=(RECFM=FB,LRECL=132,BLKSIZE=132)
```

Example 5-24 shows the content of this first-level file. It contains another reference to a PAGENT configuration file.

Example 5-24 PAGENT environment file example

```
LIBPATH=/usr/lib
TZ=MEZ-1MESZ,M3.5.0,M10.5.0
PAGENT_CONFIG_FILE=/etc/pagent/pagent.conf
PAGENT_LOG_FILE=/tmp/pagent2.log
```

The **PAGENT_CONFIG_FILE** parameter refers to the file */etc/pagent/pagent.conf*, which is shown in Example 5-25 and which finally contains a reference to the TLS policy.

Example 5-25 PAGENT configuration file

```
## Pagent Configuration for system MCECEBC
Loglevel 31 ## default 31
## Loglevel 255 ## for debugging purposes
AutoMonitorParms
{
MonitorInterval 600
```

```
RetryLimitCount 3
RetryLimitPeriod 600
}
TcpImage TCPIPBC FLUSH 600
## the policy file we created
TTLSTConfig /etc/pagent/TCPIPBC/tlsPol.conf
```

The TTLSTConfig parameter points to the policy configuration file created in “Configure AT-TLS policy” on page 78.

Note: *TCPIPBC* is the name of the IP stack that must be adapted to your LPAR configuration.

After you restart PAGENT, check in the LPAR syslog that the policy has been applied properly. If the IP stack is not configured for AT-TLS policies yet, you might see an info message in the syslog, as shown in Example 5-26.

Example 5-26 PAGENT policies not enabled message

```
EZD1579I PAGENT POLICIES ARE NOT ENABLED FOR TCPIPBC : TTLS
```

Follow the message description in IBM Knowledge Center for z/OS Communication Server under *EZD1579I*:

https://www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.halw001/ezd1579i.htm

Here is a message explanation summary:

The policies indicated by the type value that is defined in a configuration file are not enabled for the TCP/IP stack indicated by the image value. The policies are not enabled because the underlying stack function (for example, AT-TLS or IPsec) is not enabled on the stack.

System programmer response for type TTLS

If you want AT-TLS enabled, configure the stack for AT-TLS using the TTLS parameter on the TCPCONFIG statement in the TCP/IP profile. See the information about the TCPCONFIG statement in z/OS Communications Server: IP Configuration Reference for more information. See the information about the AT-TLS configuration in PROFILE.TCPIP in z/OS Communications Server: IP Configuration Guide for information about how to enable AT-TLS.

When the PAGENT configuration was changed, for example the policy definition or other PAGENT configuration file parameters, you need to reload the configuration. You can do this concurrently without restarting PAGENT via the MVS **MODIFY** command for the PAGENT address space, as shown in Example 5-27.

Example 5-27 Concurrent update of PAGENT configuration

MODIFY PAGENT,UPDATE

```
EZZ8443I PAGENT MODIFY COMMAND ACCEPTED
EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPIPBC : NONE
```

For additional details about how to modify PAGENT, see IBM Knowledge Center for z/OS Communications Server, on the *MODIFY command: Policy Agent* page:

https://www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.halu101/modpolagnt.htm

In order to verify the active PAGENT configuration, you can also list the active policy rules in OMVS with the **pasearch** command, as shown in Example 5-28.

Example 5-28 The pasearch command output

```
# pasearch
...
policyRule: CSM81
Rule Type: TTLS
Version: 3 Status: Active
Weight: 255 ForLoadDist: False
Priority: 255 Sequence Actions: Don't Care
No. Policy Action: 3
policyAction: gAct1BCSM
ActionType: TTLS Group
Action Sequence: 0
policyAction: eAct1BCSM
ActionType: TTLS Environment
Action Sequence: 0
policyAction: cAct1BCSM
ActionType: TTLS Connection
...
LocalPortFrom: 5858 LocalPortTo: 5858
RemotePortFrom: 1024 RemotePortTo: 65535
JobName: UserId:
ServiceDirection: Both
Policy created: Wed Sep 6 09:58:44 2017
Policy updated: Wed Sep 6 09:58:44 2017
...
TTLS Action: cAct1BCSM
Version: 3
Status: Active
Scope: Connection
HandshakeRole: Server
CtracedClearText: Off
Trace: 2
TTLSConnectionAdvancedParms:
SecondaryMap: Off
SSLv3: Off
TLSv1: Off
TLSv1.1: Off
TLSv1.2: On
CertificateLabel: Hyperswap Manager
TTLSCipherParms:
v3CipherSuites:
003C TLS_RSA_WITH_AES_128_CBC_SHA256
003D TLS_RSA_WITH_AES_256_CBC_SHA256
009C TLS_RSA_WITH_AES_128_GCM_SHA256
Policy created: Wed Sep 6 09:58:44 2017
Policy updated: Wed Sep 6 09:58:44 2017
```

5.9 Generate a Java keystore file for the CSM server

Important: Starting with CSM 6.1.5, you can directly upload the exported z/OS CA certificate into the CSM Java keystore using the CSM GUI. This method simplifies the overall setup process, avoids the need to create the keystore manually, and the CSM server does not need to be restarted to activate the new keystore/certificate for z/OS IP host connections.

CSM 6.1.5 or later is also required to enable security for z/OS IP host connections when CSM is running on a DS8880 HMC, because manual file modifications on the HMC are not supported. When CSM 6.1.5 or later is used, you can skip this section with the manual creation of the keystore file.

The CSM server is a Java application that cannot access raw certificates, but it requires certificates in the Java keystore (JKS) format. This section explains how to create a JKS file and import the z/OS CA certificate into the JKS file. It also explains how to transfer and activate the JKS file on the CSM server platform.

The JKS file creation can be accomplished with the **iKeyman** GUI utility or the **ikeycmd** command line utility that is provided with any IBM Java JRE or JDK. If you have an IBM JRE on a distributed server platform, you can use the GUI utility. If you create the JKS file in z/OS OMVS, you can only use the command line utility. If you need to obtain an IBM JRE or SDK, see the IBM developer kits for Java SDK:

<https://developer.ibm.com/javasdk/>

Note: If you use the default certificates that are shipped with CSM, you can also skip this chapter because a matching JKS file is already provided on the CSM server.

5.9.1 Create Java keystore file

This section describes the steps required to create a Java keystore file.

GUI Option: Create Java keystore using iKeyman

Perform the following steps:

1. From the IBM JRE or SDK bin folder, start **iKeyman**.
2. When the *IBM Key Management* GUI is launched, click the **Create a new key database file** icon or the menu item **Key Database File** → **New**.

Figure 5-1 shows how to create a new key database file.

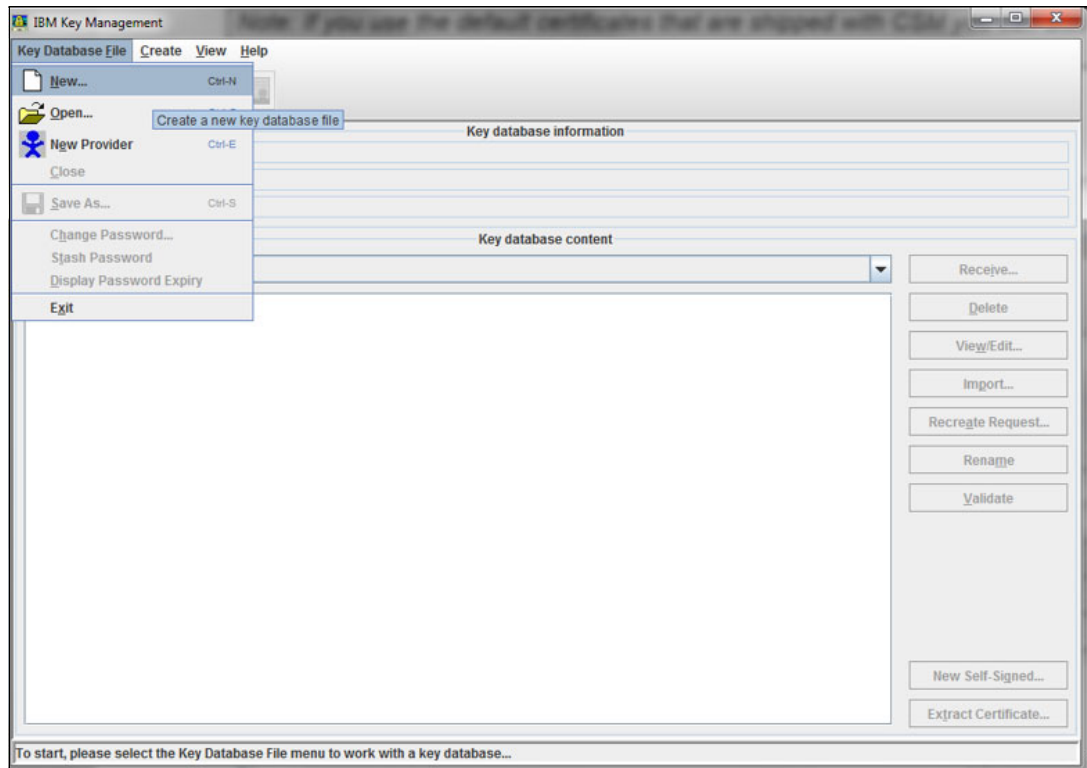


Figure 5-1 IBM Key Management GUI

3. This action opens a dialog where you have to provide a location and a name for the new keystore file. You can use the filename **zosTrust.jks**, which is the name required by the CSM server. Figure 5-2 shows the parameters you have to enter to create the keystore file.

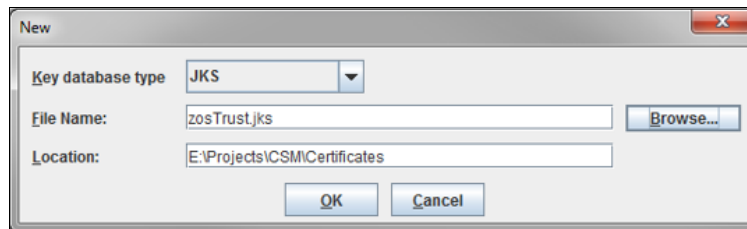


Figure 5-2 New keystore file parameters

4. Click **OK**. Another dialog displays and prompts for a password. Figure 5-3 shows the password prompt.

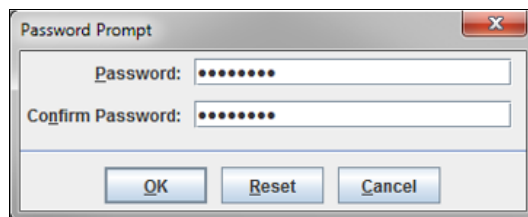


Figure 5-3 Password prompt window

5. You have to enter a non-trivial password. However, it will not be needed anymore during the keystore creation.

Note: You will need the keystore password only, if you have to change the JKS file at a later point in time, using either **iKeyman** or **ikeycmd**. For example, you will need it again to add new or to update existing certificates.

6. Now you can add the exported certificate file to the new Java keystore file. At the top of the *Key database content* section, from the drop-down list select **Signer Certificates** → **Add**. Figure 5-4 shows how to add Signer Certificates.

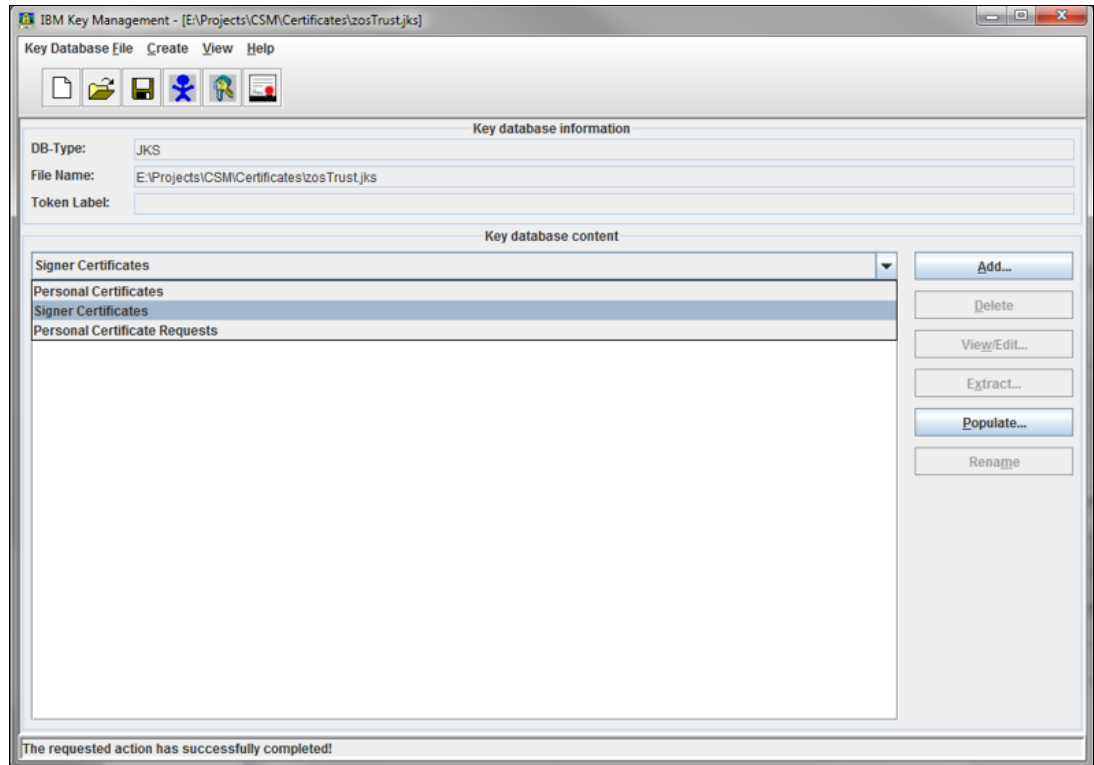


Figure 5-4 Adding Signer Certificates

Note: Instead of **Add** there may be a **Receive** button, depending on the **iKeyman** version.

7. Figure 5-5 shows how to enter or browse the file name and location of the certificate file, in our example *esm.loccerta.cert*.

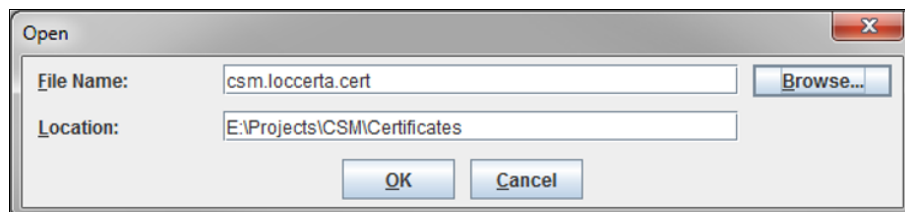


Figure 5-5 Open window

- After confirming with **OK** there is another dialog, prompting you to enter a label for the certificate. Enter any label name you like and confirm with **OK**. Figure 5-6 shows how to enter a label.

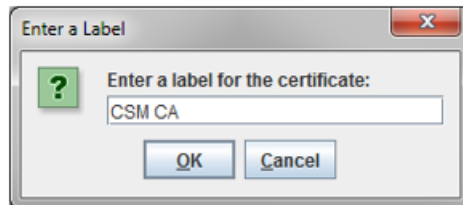


Figure 5-6 Enter a label window

Note: The certificate label names in the keystore file are not case-sensitive and will not be used throughout the remaining configuration process. They are just used to organize the certificates in the keystore file, and therefore must be unique within the keystore if multiple certificates will be added.

The keystore file is now ready with your added CA certificate, and you should see the label that you entered in the *IBM Key Management* GUI main window.

Figure 5-7 shows the added certificate label, which is *esm ca* in our example.

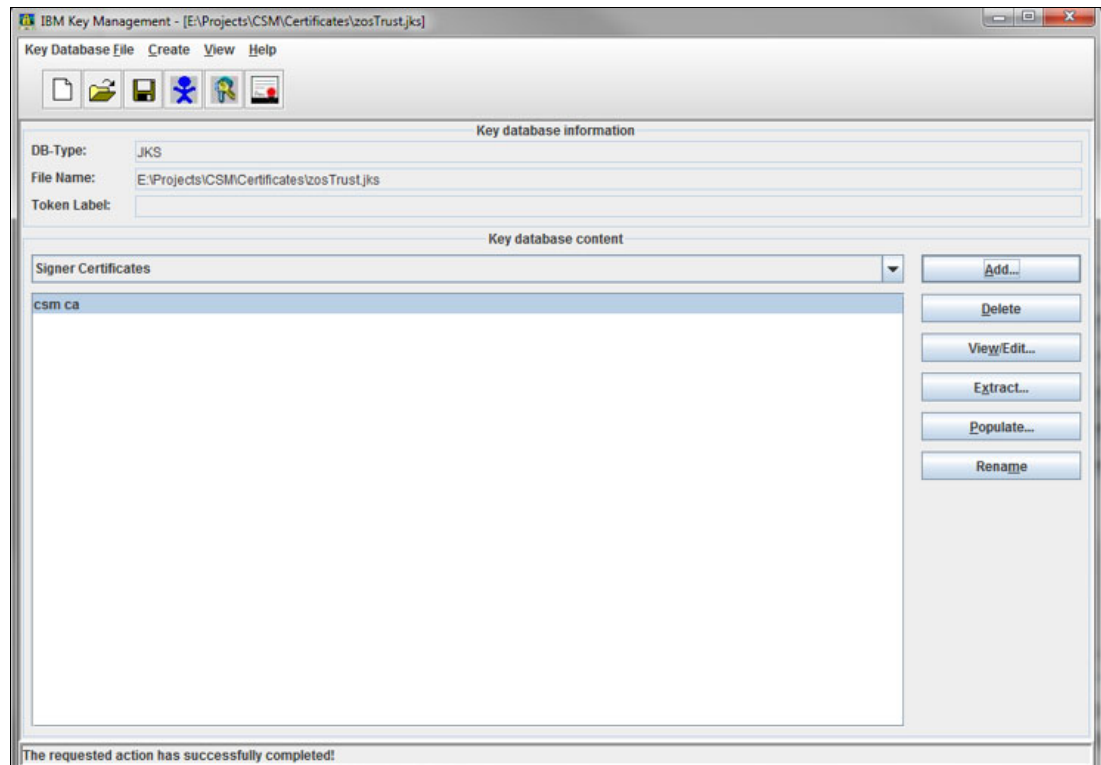


Figure 5-7 Adding certificates

If you use different CA certificates in a multi Sysplex configuration, you need to add the additional CA certificates as well, repeating the previous step. Use meaningful labels to distinguish the different CA certificates when you have to modify the keystore file again in future.

Command line option: Create Java keystore using ikeycmd in OMVS

Because we have no graphical capabilities in UNIX System Services/OMVS to run **iKeyman**, use the command line-based IBM key management tool **ikeycmd**. Make sure that you have transferred the exported certificate data set via binary mode into an OMVS file where you also run **ikeycmd**. In our Example 5-29, we transferred it to the following location.

Example 5-29 Certificate data location

`/u/home/csm.loccerta.cert`

In order to get an overview of **ikeycmd** commands and options, run **ikeycmd -help [command [option]]**, as shown in Example 5-30.

Example 5-30 The ikeycmd help

```
# ikeycmd -help
Object Action Description
-----
-keydb -changepw Change the password for a key database
-convert Convert the format of a key database
-create Create a key database
-delete Delete a key database
-expiry Display password expiry
-list Currently supported types of key database.
-stashpw Stash the password of a key database into a file
-cert -add Add a CA Certificate
-create Create a self-signed certificate
-delete Delete a certificate
-details Show the details of a specific certificate
-export Export a personal certificate and associated private key
into a PKCS12 file or a key database
-extract Extract a certificate from a key database
-getdefault Show the default personal certificate
-import Import a certificate from a key database or a PKCS12 file
-list List certificates in a key database
-listsigners List signer certificates delivered with ikeyman
-modify Modify a certificate (NOTE: the only field that may be
modified is the trust field)
-populate Populate with included CA Certificates
-receive Receive a certificate
-rename Rename a certificate
-setdefault Set the default personal certificate
-sign Sign a certificate
-validate Validate a certificate path
-certreq -create Create a certificate request
-delete Delete a certificate request from a certificate request
database
-details Show the details of a specific certificate request
-extract Extract a certificate from a certificate request database
-list List all certificate requests in a certificate request
database
-recreate Re-create a certificate request
-seckey -create Create a secret key
-delete Delete a secret key
-details Show the details of a specific secret key
-export Export secret keys to a file
```

-import Import secret keys from a file
-list List all secret keys in a key database
-rename Rename a secret key
-version Display iKeyman version information
-help Display this help text

The following section describes how you can use **ikeycmd** to create a new keystore file as required by CSM, and then import the certificate into the keystore.

Note: The following **ikeycmd** commands are example commands. They assume that you have the IBM JRE/SDK binary folder in your **PATH** variable to ensure that the **ikeycmd** executable can be located on your system without using the fully qualified path name. You need to modify the **blue** parameters according to your environment. The **red** parameters are important and required as is for proper functionality.

Complete the following steps:

1. First you need to create a new Java keystore (JKS) file using following command from your OMVS home folder. In Example 5-31, we use the home folder /u/home and create a new keystore file named *myzosTrust.jks*.

Example 5-31 Create keystore file

```
# ikeycmd -keydb -create -db myzosTrust.jks -pw password -type jks
```

This will create the keystore file in your current folder, as shown in Example 5-32.

Example 5-32 Created keystore file

```
/u/home/myzosTrust.jks
```

2. You can specify your preferred keyfile name and password. Note that the keyfile name and password is required each time that you want to access or modify the keystore file in subsequent commands.
3. Next you need to import the CA certificate file into the keystore as trusted certificate, as shown in Example 5-33.

Example 5-33 Import certificate into keystore

```
# ikeycmd -cert -add -db myzosTrust.jks -pw password -file  
'/u/home/csm.loccerta.cert' -label 'CSMCA' -trust enable
```

Note: In case you get an error due to an unrecognized certificate, ensure that the certificate file was transferred with binary mode to OMVS.

4. Now you can list the certificates in your keystore, as shown in Example 5-34.

Example 5-34 List keystore certificates

```
# ikeycmd -cert -list -db myzosTrust.jks -pw password  
Certificates in database /u/home/myzosTrust.jks:csmca
```

5. You can also list the certificate details, as shown in Example 5-35. Make sure that it shows Trust Status: enabled.

Example 5-35 List certificate details

```
# ikeycmd -cert -details -db myzosTrust.jks -pw password -label csmca
Label: csmca
Key Size: 2048
Version: X509 V3
Serial Number: 02
Issued by: OU=CSM Certificate Authority, O=CSM, C=DE
Subject: OU=CSM Certificate Authority, O=CSM, C=DE
Valid: From: Friday, August 7, 2015 12:00:00 AM CEST To: Thursday, December 31,
2026 10:59:59 PM CET
Fingerprint: 44:4C:BC:3E:0F:16:A0:A5:A9:0F:2C:13:3D:C9:EF:D9:D6:4F:2F:FF
Extensions:
- AuthorityKeyIdentifier: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: b6 df 66 41 8c db 93 75 df 71 f9 10 1d 18 bc 4f ..fA...u.q.....0
0010: 35 a8 fd cd 5...
]
]

- BasicConstraints: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
CA:true
PathLen:2147483647
]

- KeyUsage: digital_signature, non_repudiation, key_encipherment,
data_encipherment, key_agreement, key_certsign, crl_sign, encipher_only,
decipher_only
- SubjectKeyIdentifier: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: b6 df 66 41 8c db 93 75 df 71 f9 10 1d 18 bc 4f ..fA...u.q.....0
0010: 35 a8 fd cd 5...
]
]

Signature Algorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Trust Status: enabled
```

If you use different CA certificates in a multi LPAR or multi Sysplex configuration, you need to add the additional CA certificates as well, repeating the previous steps to import the certificate files. Use meaningful labels to distinguish the different CA certificates when you have to modify the keystore file again in the future.

5.9.2 Transfer the keystore file to the CSM servers

You have to place the previously created Java keystore file into a dedicated directory of the CSM servers. The keystore must be named `zosTrust.jks` and be placed into the directory shown in Example 5-36 to be used by CSM.

Example 5-36 CSM keystore file for host connection certificates

```
<CSM production root>/wlp/usr/servers/replicationServer/etc/zosTrust.jks
```

If CSM is running on z/OS, Example 5-37 shows the default location of the keystore file for z/OS IP host connection certificates.

Example 5-37 z/OS CSM keystore file for host connection certificates

```
/opt/IBM/CSM/wlp/usr/servers/replicationServer/etc/zosTrust.jks
```

A good practice is to back up or rename the original `zosTrust.jks` file prior transferring your own `zosTrust.jks` file. Example 5-38 shows how you can create a copy of the original file in the keystore folder.

Example 5-38 Backup original CSM keystore file prior replacement

```
# cd /opt/IBM/CSM/wlp/usr/servers/replicationServer/etc
# cp zosTrust.jks zosTrust.jks.bak
```

If you created your keystore file on another server than the CSM server, you need to transfer your keystore file to the CSM server now. An easy method is FTP transfer in binary mode, as illustrated in Example 5-39. We use the FTP command line tool from a Windows server where we created our keystore file with `ikeyman` and transfer it to the CSM server running on a z/OS LPAR.

Example 5-39 Transfer your keystore file to CSM server

```
C:\Users\IBM_ADMIN>ftp mcecebc.mainz.de.ibm.com
Connected to mcecebc.mainz.de.ibm.com.
220-FTP Server (user 'home@de.ibm.com')
220
User (mcecebc.mainz.de.ibm.com:(none)): HOME
331-Password:
331
Password:
230-220-FTPD1 IBM FTP CS V2R2 at MCECEBC.MAINZ.DE.IBM.COM, 15:41:17 on
2018-06-29.
230-HOME is logged on. Working directory is "/u/home".
230

ftp> bin
Representation type is Image

ftp> cd /opt/IBM/CSM/wlp/usr/servers/replicationServer/etc
HFS directory /opt/IBM/CSM/wlp/usr/servers/replicationServer/etc is the current
working directory.

ftp> put myzosTrust.jks zosTrust.jks
local: myzosTrust.jks remote: zosTrust.jks
Port request OK.
```

```
Storing data set /opt/IBM/CSM/wlp/usr/servers/replicationServer/etc/zosTrust.jks
Transfer completed successfully.
bytes sent in 0.00 secs (6701.9 kB/s)
```

```
ftp> bye
Quit command received. Goodbye.
```

Make sure that the transferred keystore file on the CSM server is named `zosTrust.jks`. If you used a different name so far for your keyfile, you can either rename it during the transfer or afterwards on the CSM server.

After putting the new `zosTrust.jks` file in place on the CSM server, restart CSM in order to recognize the new keystore file with the valid certificates for secure z/OS IP host connections.

Note: To use the secure z/OS IP host connections from the primary and the standby CSM server, you need to copy and activate the JKS file on both CSM servers.

5.10 Create the CSM IP host connection

You must create and configure a z/OS IP host connection for at least one of the LPARs in a Sysplex that is to be managed by the CSM servers. CSM can use multiple z/OS IP host connections per Sysplex. It does not have to be connected to the LPAR that acts as the HyperSwap Master (which is controlled internally by HSIB and may change dynamically).

For redundancy, it is a good practice to connect two LPARs per Sysplex. This configuration allows CSM to switch to the second connection in case the primary connected LPAR is not available.

Note: HyperSwap or Hardened Freeze are not dependent on a functional z/OS IP host connection from the CSM servers after they are activated. A CSM z/OS IP host connection must be functional only for loading a HyperSwap or Hardened Freeze configuration. If CSM uses only a FICON storage connection via the z/OS IP host connection without a redundant HMC storage connection, a loss of the last z/OS IP host connection will also disable CSM storage management capabilities.

A z/OS IP host connection between CSM and the HyperSwap Manager HSIB on an LPAR requires that HSIB with the **SOCKPORT** Parameter, and HSIBAPI and PAGENT with proper policy configuration, are running on that LPAR.

To create a host connection via the CSM GUI, complete the following steps:

1. Select **Storage** → **Host Connections** → **Add Host Connection**, as shown in Figure 5-8.



Figure 5-8 Add Host Connections in CSM GUI

2. In the **Add Host Connection** dialog, enter the IP address or host name of the LPAR that was configured with the encryption policy, and the host connection user ID and password that was set up previously with the permissions defined in the **IWNRACF5** sample job. Figure 5-9 shows how to define the z/OS IP host connection.

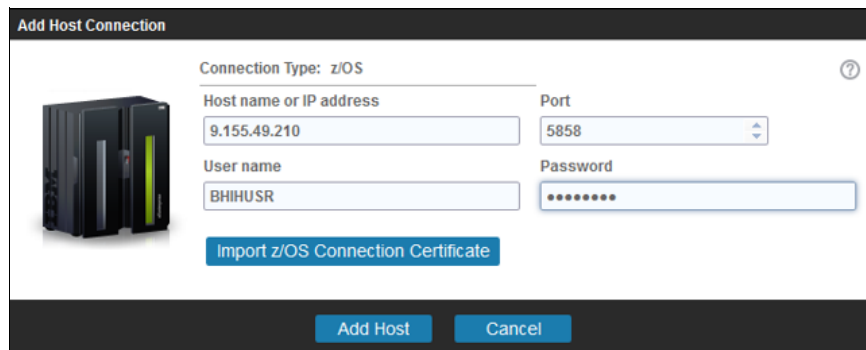


Figure 5-9 Add Host Connection dialog

3. If you use CSM 6.1.5 or later, you can import the CA certificate file that was exported according to 5.6, “Export CA certificate” on page 77. Click the **Import z/OS Connection Certificate** button.
4. A file selection dialog opens and you can browse for the certificate file on your local system.
5. After you selected and confirmed the file, you return to the **Add Host Connection** dialog and the selected certificate file will be shown next to the import button. When you click **Add Host**, the z/OS IP host connection definition will be created and the GUI will transfer the certificate to the CSM server and import it into its keystore repository.


If the z/OS IP host connection configuration was done properly on the z/OS LPAR and the CSM server, CSM will be able to connect to the LPAR that serves the defined IP address.

All host connection definitions are replicated to a connected standby CSM server. Starting with CSM 6.2.3, an imported or updated host connection certificate is also synchronized to the standby CSM server keystore file.

Note: If you use CSM 6.2.2.x or earlier and you import the host connection certificate through the CSM GUI, you have to manually import the host connection certificate on the standby CSM server as well. To do so, edit the replicated host connection definition in the standby CSM server GUI and use the **Import z/OS Connection Certificate** button to import the certificate.

If the z/OS Host Connection from the standby CSM server still fails, delete and re-create the complete z/OS Host Connection definition on the active CSM Server. Upon re-creation, you can skip the certificate import because it already exists in the keystore of the active and standby CSM servers. The z/OS Host Connection should now connect from both CSM servers.

Storage > Host Connections



Host Connections

Last Update: 29.06.2018 18:27:00

Add Host Connection

Select Action

Host System	Port	Type	Local Status
9.155.49.210	5858	ZOS_IP	Connected
9.155.49.211	5858	ZOS_IP	Connected
ZOS_NATIVE_CONNECTION		ZOS_NATIVE	Connected

Note: The z/OS native Host Connection is only shown if the CSM server is running on z/OS. CSM servers on distributed platforms cannot establish a z/OS native Host Connection. Even if the connection exists in the replicated CSM repository, it is hidden in the CSM GUI of a distributed platform server.

Example 5-40 BHIHSRV address spaces for established z/OS IP host connections (2)

```

MCECEBC CEB3      (ALL)      PAG 0 CPU/L      3/ 1      LINE 1-2 (2)
COMMAND INPUT ==> DA
PREFIX=IEESYSAS* DEST=(ALL) OWNER=* SORT=StepName/A SYSNAME=*
NP  JOBNAME StepName ProcStep JobID      Owner      Real  Paging      SIO      CPU% SysName
    IEESYSAS BHIHSRV  IEFPROC STC05138 BHIHSRV  1731    0.00  0.00    0.00 MCECEBC
    IEESYSAS BHIHSRV  IEFPROC STC05444 BHIHSRV  1596    0.00  0.00    0.00 MCECEBC

MCECEBC CESS DISPLAY (ALL)      ALL      LINE 1-2 (2)
COMMAND INPUT ==> PS
PREFIX=BHIHSRV* DEST=(ALL) OWNER=* SORT=JOBNAME/A SYSNAME=*
NP  JOBNAME JobID      Status      Owner      State CPU-Time      PID      Command
    BHIHSRV      RUNNING      BHIHSRV  1R      1091.13  50334952 BHIITPC
    BHIHSRV      RUNNING      BHIHSRV  1R      1.32    67112164 BHIITPC

```

Example 5-41 OMVS netstat to verify active z/OS IP host connection

```
# netstat -a | grep 5858
HSIB      00022426 0.0.0.0..5858          0.0.0.0..0           Listen
HSIB      00022438 9.155.49.210..5858     9.155.114.38..57267  Establish
HSIB      00022434 9.155.49.210..5858     9.155.49.210..49257  Establish
IWNSRV    00022433 9.155.49.210..49257    9.155.49.210..5858   Establish
```

The first line shows the opened HSIB socket port which listens for incoming z/OS IP host connections. The next two lines show the two established connections, from CSM server 9.155.114.38 and 9.155.49.210. Because 9.155.49.210 is the local LPAR that runs the CSM servers on z/OS, you also see the outgoing connection to the HSIB socket port in the last line.

After the z/OS IP host connection is created, CSM can recognize the connected Sysplex and the storage systems that are defined to the connected LPAR(s). A recognized Sysplex can then be assigned to a session that you want to manage with HyperSwap or Hardened Freeze.

To assign a CSM session to a Sysplex, go to the session properties and associate the Sysplex to the session. This action enables the HyperSwap property tabs or options for the CSM session if they were not available before. Figure 5-11 shows an example View/Modify Properties dialog. See 7.1.1, “Assign discovered Sysplex to CSM session” on page 130 for more details about Sysplex association.

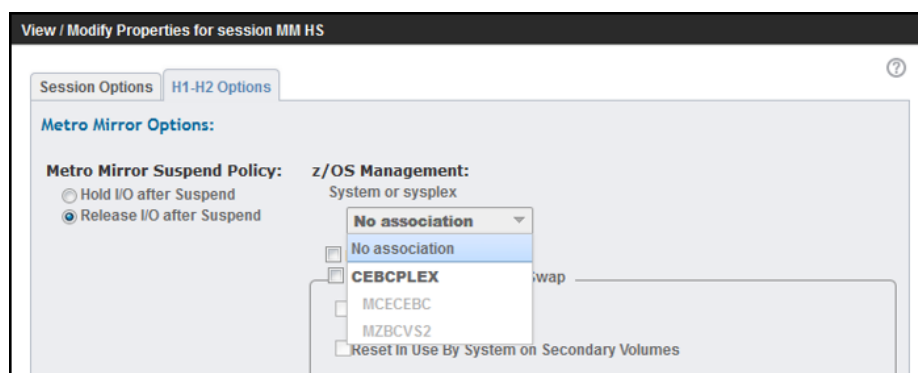


Figure 5-11 Sysplex association in CSM session properties dialog

Note: In the drop-down list to assign a recognized Sysplex, CSM only lists the LPARs that are connected to the CSM server. These are not necessarily *all* LPARs that are defined in the Sysplex.

If your CSM server is not running on z/OS, the z/OS IP host connections also allow you to add a *z/OS Direct Storage Connection* (FICON) for all devices that are defined to the connected LPARs:

1. In the CSM GUI, go to the Storage Systems panel and click **Add a Storage System**.
2. Then select **z/OS Direct Storage Connection**. You see a consolidated list of defined storage systems from all connected LPARs and you can select the ones to which you want to establish a FICON connection. Figure 5-12 on page 95 shows how to add a storage system via z/OS Direct Connection (FICON).

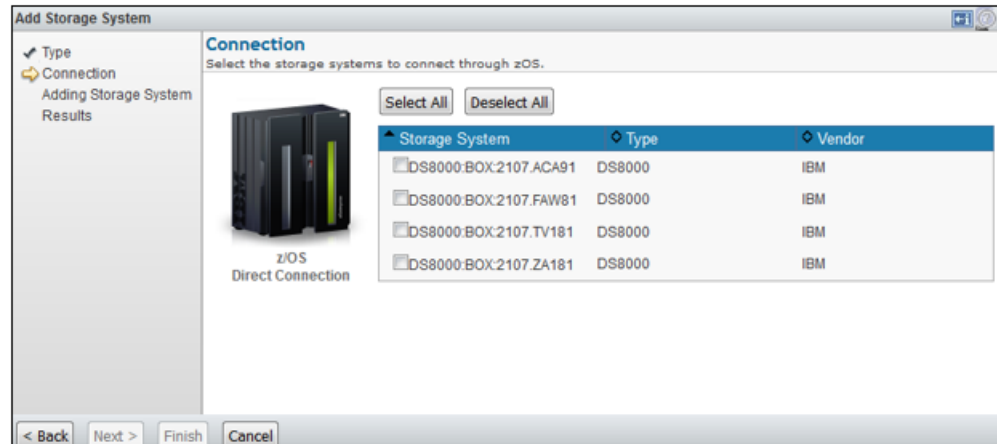


Figure 5-12 Add storage system via z/OS Direct Connection (FICON)

5.11 Troubleshoot CSM z/OS IP host connection errors

When a z/OS IP host connection has been defined in CSM, CSM continuously retries to establish a connection to the defined IP address until the connection is established. If the status shows Disconnected, you can click the status and see a possible reason. Figure 5-13 shows an example of such a connection error.

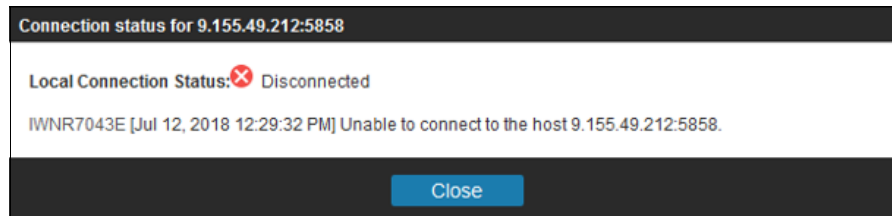


Figure 5-13 Connection error details

The z/OS IP host connection errors can also be found in the CSM Console log. When you click the error message code, you get more details and possible corrective actions. Example 5-42 shows the details of the displayed message IWN7043E.

Example 5-42 Message code details

IWN7043E

Message Text:

[timestamp] Unable to connect to the host hostname.

Explanation:

Unable to contact the destination host name and port.

Action:

Verify the following: The host name and port are correct. The IOSHMCTL program is running on the target z/OS system with the SOCKPORT parameter specified. The z/OS system is version 1.13 or higher, and has the appropriate prerequisites for IP communication. There are no firewalls that are blocking communication between the copy services management server and the z/OS host. Ensure that the encryption settings match between the z/OS system and the copy services management server.

You should also verify the z/OS system log of the LPAR that you are trying to connect to. It may contain permission or authentication errors, or other hints as to why the connection or the secure handshake was not established.

The following list includes possible root causes in case of z/OS IP host connection errors:

- ▶ No connection can be established:
 - Verify that there is no firewall issue.
 - Verify that the HSIB address space (IOSHMCTL program) is started with the SOCKPORT parameter.
 - Verify that the HSIBAPI address space (IOSHSAPI program) is started.
 - You may use **telnet** from the CSM server to test a connection to the LPAR IP and port:
telnet <IP/hostname> <sockport>.
 - If the port or IP/hostname is not reachable, **telnet** times out.
 - If the port is open, **telnet** should switch to an empty screen, because no **telnet** response is received from the LPAR. But this validates that the port is reachable.
 - Verify LPAR syslog for permission or authentication errors.
 - Verify that the z/OS IP host connection user password has no Expired flag in your security facility. The password must be permanently set.
 - Verify that PAGENT is running and has loaded a proper AT-TLS policy for the host connection port.
- ▶ TLS/SSL handshake errors in syslog:
 - Verify that the owner of the HSIB and HSIBAPI started tasks, and the z/OS IP host connection user, have proper permissions to the certificates and keyring as well as to the security facility ANT.REPLICATIONMANAGER.
 - Verify that the CA certificate was exported from your security facility and imported into the CSM server keystore repository.
 - Make sure that the certificate is not expired.
 - If CSM is used on DS8880 HMC, make sure that at least TLS 1.2 protocol is used with proper Ciphers, and that the certificate key size is at least 2048.



Implementing z/OS HyperSwap

After installing IBM Copy Services Manager (CSM) there are some tasks that you must complete before using HyperSwap. This chapter describes steps for customizations of z/OS systems that need to be considered activating and using z/OS HyperSwap.

6.1 HyperSwap address spaces and started tasks

IBM z/OS HyperSwap requires two address spaces on each logical partition (LPAR) in a Sysplex:

- ▶ HSIB (IOSHMCTL program)
- ▶ HSIBAPI (IOSHSAPI program)

For detailed explanations of these address spaces, see 2.2.1, “HyperSwap or Hardened Freeze address spaces” on page 25. To launch the HyperSwap address spaces as started tasks, you first need to have a z/OS user that you can assign to these tasks. IBM Knowledge Center for CSM provides RACF sample jobs to create the required user and assign proper permissions. They can be found on the *Configuring the IWNRACTF jobs* page:

https://www.ibm.com/support/knowledgecenter/SSESK4_6.2.3/com.ibm.storage.csm.help.doc/frc_t_config_iwnracf.html

The user definition for the HyperSwap address spaces, including support for z/OS IP host connections, is described in 5.3, “Configure z/OS users for HyperSwap tasks and z/OS IP host connections” on page 68.

If you do not need a z/OS IP host connection, you only need to modify or issue the RACF commands defined in the following job:

▶ **IWNRACTF3**

- Defines the user and group IDs that are associated with the HyperSwap address spaces (HSIB and HSIBAPI)
- The user and group that are specified do not technically require access to OMVS if a z/OS IP host connection is not required. However, it is good practice to configure the OMVS segment if a z/OS IP connection will be configured at a later point.

The following example shows how to configure the user and group for all HyperSwap address spaces:

▶ **BHIHGRP 100**

- Example group name and group ID for the users

▶ **BHIHSRV 300**

- This user does not need a password and therefore can be a protected user
- Example user name and ID to run the HSIB and HSIBAPI started tasks for HyperSwap

Based on the IWNRACTF3 sample job, Example 6-1 shows the required RACF commands.

Example 6-1 IWNRACTF3 definition commands for HyperSwap user

```
/* Define the HyperSwap address space user ID and group. */
ADDGROUP BHIHGRP OMVS(GID(100))
ADDUSER BHIHSRV DFLTGRP(BHIHGRP) OMVS(UID(300) HOME('/')) -
    NAME('HyperSwap Address Spaces') NOPASSWORD

/* Define the started profiles. */
RDEF STARTED HSIBAPI.* UACC(NONE) STDATA(USER(BHIHSRV) -
GROUP(BHIHGRP) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))
RDEF STARTED HSIB.* UACC(NONE) STDATA(USER(BHIHSRV) -
GROUP(BHIHGRP) PRIVILEGED(NO) TRUSTED(NO) TRACE(YES))
SETROPTS RACLIST(STARTED) GENERIC(STARTED) REFRESH
```

If you do not use the RACF security facility, please consult your security facility documentation for corresponding commands to create the required user roles and permissions.

When the user and group for the HyperSwap address spaces and tasks is defined, you configure appropriate jobs in the **PROCLIB** system library for the HSIB and HSIBAPI started tasks. This is described in 5.4, “Configure HyperSwap tasks with socket port” on page 70. However, if you do not need a z/OS IP host connection, you can omit the **SOCKPORT** parameter in the HSIB job. Example 6-2 shows the job for the HSIBAPI address space.

Example 6-2 HSIBAPI address space

```
//HSIBAPI JOB MSGLEVEL=(1,1),TIME=NOLIMIT,REGION=0M
//          EXEC PGM=IOSHSAPI
```

Example 6-3 shows the job for the HSIB address space without the **SOCKPORT** parameter.

Example 6-3 HSIB address space without the SOCKPORT parameter

```
//HSIB JOB MSGLEVEL=(1,1),TIME=NOLIMIT,REGION=0M
//IEFPROC EXEC PGM=IOSHMCTL
```

You can start these address spaces in one of the following ways:

- ▶ Issue the MVS **START** command manually.
- ▶ Include the **START** command in the **COMMNDxx** member of the **SYSx.PARMLIB** data set.

Note: It is preferred, although not required, that you start HSIBAPI before HSIB. HSIB does not get ready until HSIBAPI is running.

Example 6-4 shows the MVS **START** and **STOP** commands for the two address spaces.

Example 6-4 Start and stop of HyperSwap address spaces

```
START HSIBAPI,SUB=MSTR
START HSIB,SUB=MSTR

STOP HSIB
STOP HSIBAPI
```

6.2 IBM z/OS configuration for HyperSwap

IBM z/OS related configuration items and best practices are discussed in the IBM Redbooks publication, *IBM Tivoli Storage Productivity Center for Replication for System z*, SG24-7563, Chapter 6: “Basic HyperSwap customization and use”:

<http://www.redbooks.ibm.com/abstracts/sg247563.html>

During the last couple of years, additional configuration topics and best practices evolved and are discussed in the following sections. We review the essential information necessary for each of the topics to allow you to decide whether they are relevant for your environment, and how you can apply the necessary tasks.

For a proper HyperSwap preparation of your environment, also see 3.2, “Prerequisites for z/OS HyperSwap” on page 45.

6.2.1 Install the latest PTFs for z/OS HyperSwap

To ensure that you have the latest z/OS APARs, updates, and *Program Temporary Fixes* (PTFs) required to support z/OS HyperSwap, you can get the latest IBM HOLDDATA and then use the **IBM.Function.HyperSwap** fix category to select and apply the appropriate PTFs, or to identify any PTFs that are missing.

The latest HOLDDATA is supplied with all IBM products and service offerings (SMPE RECEIVE ORDER, Shopz, ServiceLink, Custom-built Product Delivery Option (CBPDO), IBM ProductPac®, ServerPac, and SystemPac) and can be obtained from the HOLDDATA website:

<http://service.software.ibm.com/holdata/390holddata.html>

Use the full two-year file only. After receiving the latest HOLDDATA, you can use the SMPE command **REPORT MISSINGFIX** to identify missing HyperSwap PTFs, as shown in Example 6-5.

Example 6-5 SMPE REPORT MISSINGFIX command

```
SET BDY(GLOBAL).  
REPORT MISSINGFIX ZONES(tgtzone)  
FIXCAT(IBM.Function.HyperSwap).
```

Generally, it is good practice to have all Input/Output Supervisor (IOS), replication, and DFSMS related components updated with the latest APARs.

6.2.2 HyperSwap related console commands

IBM z/OS provides a couple of MVS system commands to display HyperSwap information and perform certain HyperSwap related actions. See 8.2.1, “z/OS HyperSwap commands” on page 159 for a list of these commands and their important use cases. Some of them require sufficient command authorization for TSO users that monitor and manage HyperSwap. The following security facility authorities are required to issue HyperSwap operator commands:

- ▶ **SETHS ENABLE/DISABLE/SWAP** requires UPDATE authority to profile MVS.SETHS in the OPERCMDS class.
- ▶ **DISPLAY HS** requires READ authority to profile MVS.DISPLAY.HS in the OPERCMDS class.
- ▶ **SETIOS HYPERSWAP** requires UPDATE authority to profile MVS.SETIOS.IOS in the OPERCMDS class.

6.2.3 Enable critical paging

A HyperSwap can fail if the address spaces that are required for HyperSwap have page faults. To avoid a swap failure because of page faults, you must enable the CRITICALPAGING function. Enable Critical Paging via the FUNCTIONS statement of the **COUPLExx** member in **SYSx.PARMLIB** in each LPAR of the Sysplex, as shown in Example 6-6.

Example 6-6 Enabling CRITICALPAGING parameter

```
FUNCTIONS ENABLE(CRITICALPAGING)
```

Note: You cannot enable the Critical Paging function using the **SETXCF** command, therefore *activation of Critical Paging requires an IPL.*

To verify whether critical paging is active, use the MVS command **DISPLAY XCF, COUPLE**, as shown in Example 6-7.

Example 6-7 MVS command DISPLAY XCF, COUPLE

```

COMMAND INPUT ==> /D XCF, COUPLE                                SCROLL ==> CSR
RESPONSE=MCECEBC
IXC357I 17.37.22 DISPLAY XCF 166
SYSTEM MCECEBC DATA
      INTERVAL   OPNOTIFY   MAXMSG   CLEANUP   RETRY   CLASSLEN
          165         168       2000        15        10        956
...
OPTIONAL FUNCTION STATUS:
...
      CRITICALPAGING                                ENABLED      DISABLED
...

```

You can find further details for system analysis and storage requirements with regard to critical paging in the following IBM Support Flashes:

<http://www-01.ibm.com/support/docview.wss?uid=tss1flash10733>
<http://www-01.ibm.com/support/docview.wss?uid=tss1wp101800>

6.2.4 Sharing volumes with systems outside the Sysplex

One wants to avoid any sharing of volumes that are part of a HyperSwap configuration with systems outside of the HyperSwap managed Sysplex.

LPARs outside of the Sysplex are not aware when a HyperSwap takes place and might continue attempting to access the old primary volumes. This can lead to data integrity exposures. Furthermore, sharing volumes with outside systems usually requires the use of the hardware Reserve/Release mechanism to serialize access to these volumes. The use of RESERVEs is not supported with HyperSwap.

HyperSwap will also try to Soft Fence old primary devices after a HyperSwap in order to prevent data integrity issues if devices are accessible from LPARs outside of the Sysplex.

Sharing volumes with outside systems that have read access only does not harm the managed Sysplex. However, it might lead to loss of access or data integrity issues on the outside system, because they continue to try to read from the old primaries. If you need to share disk volumes with outside systems that also have write access, you must exclude them from the HyperSwap configuration.

Carefully examine and resolve all possible shared device scenarios in your environment. Some common scenarios include the following possibilities:

- ▶ Cross Sysplex disk sharing, which might include write capability/reserves from either Sysplex.
- ▶ Shared devices for transferring data out of the Sysplex. Typically these devices are read/write to the Sysplex, and read only to other systems.
- ▶ IBM RMF™ LSPACE collection by other systems.
- ▶ Tape Library & Tape device scheduling software, which commonly requires a shared disk to manage data between systems.
- ▶ VM, VSE, Linux for IBM z, and TPF systems sharing disks with the Sysplex.

6.2.5 Hardware reservations

HyperSwap does not support hardware reserves on HyperSwap managed volumes. A HyperSwap session cannot be enabled if there is an outstanding hardware reserve against a device that is defined in the session. All RESERVEs that target HyperSwap managed volumes must be converted to GRS Global ENQs. Global ENQs provide I/O serialization between the LPARs in a Sysplex. They do not provide serialization across multiple Sysplexes or Monplexes.

Converting RESERVEs to Global ENQs

There is an ENQ/RESERVE/DEQ Monitoring Tool (**ISGAUDIT**) that can help you to identify the RESERVEs in your environment. It also helps to identify and remove any EXCLusion rules that relate to HyperSwap managed disks. **ISGAUDIT** is shipped with z/OS. For more details, see IBM Knowledge Center for z/OS, *MVS Planning: Global Resource Serialization (GRS)*, under *Using the ENQ/RESERVE/DEQ monitor tool*:

https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.ieag400/emon.htm

Run this tool from time to time on your systems to ensure that there are no RESERVEs set against your HyperSwap managed disks. To convert all RESERVEs to Global ENQs, perform the following steps:

1. Run the ENQ/RESERVE/DEQ Monitor with filtering REQTYPE of NCRESERVE to gather reports on non-converted RESERVEs issued by the system.
2. Use the GRSRNLxx member of **SYSx.PARMLIB** to add an RNLDEF customization parameter.
3. To convert any RESERVE that might be issued against volumes that are managed by HyperSwap to Global ENQs, use a PATTERN entry.
4. The **RNLDEF** parameter in Example 6-8 will convert all RESERVEs to Global ENQs.

Example 6-8 RNLDEF parameters to convert RESERVEs to Global ENQs

RNLDEF	RNL(CON)	TYPE(PATTERN)	QNAME(*)
--------	----------	---------------	----------

For more information about converting RESERVEs to Global ENQs, see the page *GRSRNLxx (global resource serialization resource name lists)* in the latest version of the z/OS MVS Initialization and Tuning Reference:

https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.ieae200/grsrnl.htm

When all RESERVEs are converted to GRS Global ENQs, the ENQs might take longer to resolve if the ISGLOCK structure is too small to process each global ENQ independently. If this situation occurs, you might have to increase the size of your ISGLOCK structure. For information about GRS, including guidelines about how to resize the ISGLOCK structure, see the latest version of the z/OS MVS Initialization and Tuning Reference:

- ▶ https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.ieag400/grsdiag.htm
- ▶ https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.ieag400/isglock.htm

Movement of RESERVE during HyperSwap

Although RESERVEs are not allowed when loading HyperSwap, they can occur after a HyperSwap session has been enabled. In this case, HyperSwap manages the RESERVEs issued to primary devices by attempting to move them from the primary devices to their secondaries.

However, if the event that triggered the HyperSwap was the loss of all paths from the system holding the RESERVE to the disk, the disk system clears the RESERVE. This switch potentially enables other systems to gain the RESERVE before HyperSwap can move it.

In addition, the scope of a HyperSwap is a single Sysplex (or Monoplex). HyperSwap ensures that all systems accessing HyperSwap managed devices have stopped using the old primaries, before swapping over to the secondary (new primary). So if RESERVEs are actually being used to serialize devices between two or more Sysplexes, there is no guarantee that both Sysplexes will swap at exactly the same time. For these reasons, RESERVEs are generally not supported on HyperSwap managed devices.

A special exclusion from this rule might be HyperSwap in a Monoplex. Because GRS Global ENQs provide I/O serialization between multiple LPARs within a Sysplex, it does not provide any benefit to a Monoplex that is actually a Sysplex with only a single LPAR. If the Monoplex devices are defined as SHARED so that they could be brought online to other systems in emergency cases, it might be better to use RESERVEs to have some additional protection benefit.

Note: As discussed in 6.2.4, “Sharing volumes with systems outside the Sysplex” on page 101, it is a good practice to avoid sharing HyperSwap devices across Sysplexes or Monoplexes for normal operations.

6.2.6 Message control

Messages concerning PPRC and HyperSwap are written to the z/OS SYSLOG or OPERLOG. z/OS HyperSwap messages start with an IOSHS prefix (HyperSwap application programming interface (API) Service address space) or IOSHM prefix (HyperSwap Management address space). You can find further details about HyperSwap messages in 8.2.2, “z/OS messages related to HyperSwap” on page 164 and at the following IBM Support link:

https://www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.ieam900/idg68675.htm

Detailed HyperSwap messages are logged by the LPAR acting as the HyperSwap Master System. Use the **MODIFY HSIB,D** MVS command to find out which LPAR is used as the HyperSwap Master. For more details, see 8.2.1, “z/OS HyperSwap commands” on page 159.

The following sections describe some log settings and options to reduce the amount of logged messages related to HyperSwap. They can be adjusted in various members of the **SYSx.PARMLIB** data set. The relevant members are described in the following sections. For more information about any of the following topics, see IBM Knowledge Center for z/OS, *MVS Initialization and Tuning Reference*:

https://www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.ieae200/toc.htm

Console and log buffers for large amount of messages

HyperSwap as well as large PPRC configurations can produce a large amount of log messages and may require an increase of log buffers. They can be adjusted in the following members of the **SYSx.PARMLIB** data set:

► **CONSOLxx**

- During a HyperSwap, a very large number of messages can be produced. To minimize the possibility that console buffer shortages will impact operations during a HyperSwap, increase the number of console buffers allowed. These buffers today occupy above-the-line storage. You can specify a large value without impacting your system. See the **MLIM** parameter on the **CONSOLxx** **INIT** statement.
- The large number of messages produced during a HyperSwap are also written to the system log (**SYSLOG** and/or **OPERLOG**). To minimize the possibility that a log buffer shortage will impact operations during the HyperSwap, increase the number of log buffers that you allow. See the **LOGLIM** parameter on the **CONSOLxx** **INIT** statement.

► **IEASYSxx**

- To accommodate a larger number of log buffers, you might have to increase the amount of extended CSA (ECSA) storage allowed on your systems. It is specified in the second value of the **CSA** parameter. Add approximately 150 bytes of additional ECSA for every 1000 additional log buffers.
- HyperSwap control blocks occupy extended SQA (ESQA) storage and you may have to increase the amount of ESQA storage on your systems. It is specified in the second value of the **SQA** parameter. For each PPRC device pair, 32 bytes are required, and for each LSS an additional 1100 bytes. A configuration of ten thousand PPRC device pairs needs in the order of 320 KB.

Message aggregation to avoid console flooding

Disk storage systems maintain the Metro Mirror (MM) status of all their devices. Any change in this status, such as a volume going from **FULL DUPLEX** to **SUSPENDED**, causes the storage system to send a state change interrupt to all hosts that have that volume online. Each z/OS LPAR that receives this interrupt issues the **IEA494I** message to the console, as shown in Example 6-9.

Example 6-9 Message for a suspended volume:

```
IEA494I devn,volser,PPRC PAIR SUSPENDED,SSID=ssid,CCA=cc
```

You can find more details for message **IEA494I** in IBM Knowledge Center for z/OS, *MVS System Messages Guide*:

https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.iam600/m009814.htm

This message, and others, are issued for each PPRC pair whenever a HyperSwap occurs. The HyperSwap processes a Freeze (which results in suspended primary devices) and a PPRC Failover. If you have thousands of volumes in your HyperSwap session, you will see thousands of these messages at the operator consoles. This large number of messages can cause WTO buffer shortages and impact the operation of your systems.

You can reduce the number of messages by using the Message Processing Facility (MPF) to keep these messages completely off of your consoles and the Message Flood Automation in your Sysplex, which allows you to establish thresholds for certain messages.

In the following sections, we describe the **SYSx.PARMLIB** members, where you can configure message processing and Message Flood Automation:

► **MSGFLDxx**

In a HyperSwap or PPRC environment, you can suppress the PPRC state change message IEA494I as shown in Example 6-10.

Example 6-10 Message Flood Automation for IEA494I

```
MSG IEA494I LOG,NOAUTO,NODISPLAY,NORETAIN,NOIGNORE
```

This suppresses the message from the consoles when it is produced in large quantities in a short period of time. Usually only the first entries are relevant to see which devices might have triggered an unexpected state change.

► **MPFLSTxx**

The messages listed in Example 6-11 can always be suppressed from the consoles by using the following MPF specifications.

Example 6-11 Messages to be suppressed

```
IOS000I,SUP(ALL),AUTO(NO)  
IOS017I,SUP(ALL),AUTO(NO)  
IOS109E,SUP(ALL),AUTO(NO)  
IOS251I,SUP(ALL),AUTO(NO)  
IOS444I,SUP(ALL),AUTO(NO)  
IOS450E,SUP(ALL),AUTO(NO)  
IOS291I,SUP(ALL),AUTO(NO)  
IEA476E,SUP(ALL),AUTO(NO)
```

PPRC summary event notification for suspend events

The PPRC summary event notification feature (PPRCSUM) significantly reduces the amount of messages written to the console when PPRC relationships are suspended. The PPRCSUM feature is a storage controller capability and supported by IBM DS8000 systems using firmware 6.2 and later.

It must be explicitly enabled on a z/OS LPAR by enabling the PPRCSUM attribute in the **SYSx.PARMLIB** member **DEVSUPxx**. **DEVSUPxx** specifies the installation defaults for device support options and is processed during the NIP phase of an IPL.

After IPL, you can use the system command **SET DEVSUP=XX** to activate any **DEVSUPxx** changes. Refer to IBM Knowledge Center for z/OS, *MVS Initialization and Tuning Reference* for a detailed explanation of the **DEVSUPxx** parameters:

https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.ieae200/devsup.htm

To control the PPRCSUM feature, modify **DEVSUPxx** parameters as following:

► **DISABLE (PPRCSUM)**

PPRC suspend notification for individual devices is displayed in message IEA494I (Default setting)

► **ENABLE (PPRCSUM)**

The Device Manager will use message IEA075I instead of IEA494I to report devices that transition to PPRC suspended state

If you enable PPRCSUM, the system will issue an IEA075I message every 5 seconds, or when the last device in the storage logical control unit (LCU) has suspended, to summarize the PPRC state for all devices in the LCU. This behavior continues until all PPRC state transitions have completed. The IEA075I message format is shown in Example 6-12.

Example 6-12 IEA075I message format

```
IEA075I  PPRC SUMMARY,SSID=xxxx,DEVICE
NED=tttt.mmm.ggg.pp.ssssssssssss.uuuu,SECSSID=yyyy(Dddd Pppp
Ssss),SECSSID=zzzz(Dddd Pppp Ssss),SECSSID=yyyy(Dddd Pppp Ssss),SECSSID=zzzz(Dddd
Pppp Ssss),SUSPENDED=aaa,PPRC=bbb,TOTAL=ccc,{REASON=SUSPEND(rr),text |
REASON=UNKNOWN(rr)}
```

The summary counters per LCU are:

- ▶ SUSPENDED: Number of suspended devices in LCU
- ▶ PPRC: Number of PPRC devices in LCU
- ▶ TOTAL: Number of total devices in LCU

More details for the IEA075I message can be found in the z/OS Knowledge Center, *z/OS MVS System Messages*:

https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.iam600/idg63198.htm

If you have enabled PPRCSUM on some LPARs but not on others, you get summary notifications on the LPARs where it is enabled, and you will continue to get device-level SCI notifications on the LPARs that are not enabled. Only disk storage systems that support PPRCSUM provide summary notifications to LPARs enabled for PPRCSUM. Storage systems that do not support this capability continue to provide device-level notifications to all LPARs, regardless of whether it has PPRCSUM enabled or not.

Note: If the PPRCSUM feature is enabled or disabled after IPL, one device in every LCU must be varied online to activate the change.

To view active device manager settings, you can use the MVS command **MODIFY DEVMAN,REPORT**. Example 6-13 shows PPRCSUM activated.

Example 6-13 Report command output

```
COMMAND INPUT ==> /F DEVMAN,REPORT
RESPONSE=MCECEBC
DM0003OI DEVICE MANAGER REPORT
**** DEVMAN ****
* FMID: HDZ2220 *
* APARS: UA83367 UA80876 UA81756 UA77616 UA83895 *
* OPTIONS: REFVTOC REFUCB PPRCSUM SSR PPRCMT *
* HPF FEATURES DISABLED: NONE *
* MULTIPLE INCREMENTAL FLASHCOPY: CHANGE RECORDING V2 *
* EASY-TIER FOR SOFTWARE DEFINED STORAGE *
* NO SUBTASKS ARE ACTIVE *
**** DEVMAN ****
```

6.2.7 Reduce delays of HyperSwap triggers

There is a featured article on page 59 of the August 2016 *z/OS Hot Topics Newsletter*, that describes the IOS recovery time limit as well as the path recovery options to speed up recovery times and to raise HyperSwap triggers faster in the z/OS environment:

<https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZS103027USE&>

By default, the z/OS IOS processes errors independently per device, even if the devices share a common hardware component. By using a `PATH_SCOPE` value of `CU`, along with reduced `PATH_THRESHOLD` and `PATH_INTERVAL` parameters, you can reduce the amount of time and the number of errors that it would take for IOS to remove a path for an LCU when the error is consistent on a given path. As such, the I/O error recovery time can be reduced significantly in order to declare I/O errors faster in a HyperSwap environment and trigger the HyperSwap sooner after the first I/O error occurs.

Limit the z/OS I/O recovery time

The IOS Limited Recovery time setting will limit the timeout value for I/Os used by IOS Dynamic Pathing Validation, which was seen delaying XCF I/O in some cases. The timing of IOS Dynamic Pathing Validation works as follows:

- ▶ Without `LIMITED_RECTIME` set, IOS will use a timeout value of 15 seconds, followed by 2 retries of 5 seconds each. So, this is a maximum total delay of: 15 seconds + 5 seconds + 5 seconds * (number of paths). Considering 8 paths, this could lead to 200 seconds delay until an I/O error to Couple Data Sets is declared and a **PSWITCH** to the alternate is performed. This pathing validation also delays the ENF signal for No Path Available, which triggers an unplanned HyperSwap.
- ▶ With `LIMITED_RECTIME` specified, that value is used, and no retries will be performed. So this is a maximum total delay of: (`LIMITED_RECTIME` value) * (number of paths). Considering again 8 paths and a `LIMITED_RECTIME` value of 2 seconds, the delay until an I/O error to Couple Data Sets is declared will be reduced to 16 seconds.

The IOS limited recovery time can be set in the `IECIOsx` member of `SYSx.PARMLIB`, as shown in Example 6-14.

Example 6-14 Set z/OS limited recovery time

```
RECOVERY LIMITED_RECTIME=2,DEV=DASD
```

The `LIMITED_RECTIME` value specified is a trade off between being resilient in the Sysplex and avoiding delays for a HyperSwap environment. If there are concerns that 2 seconds may be too aggressive, you can decide what value is best for your environment. A value of 7 or 8 seconds can be a considerable trade off.

The IOS Limited Recovery time setting is documented in IBM Knowledge Center for z/OS, *MVS Initialization and Tuning Reference*:

https://www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.ieae200/ieae200359.htm

Change scope of z/OS I/O path recovery

By default, path recovery is performed independently per device, even if they share a common hardware entity. To shorten specific I/O recovery times further, you can change the scope from a device level to a CU level. The relevant parameters in `IECIOsx` member of `SYSx.PARMLIB` are shown in example Example 6-15 on page 108.

Example 6-15 Path recovery parameters:

```
PATH_SCOPE=CU
PATH_INTERVAL=1
PATH_THRESHOLD=3
```

This combination of parameters leads to the system taking a path to an LCU offline if three errors are detected within one minute. If three errors for the same path for one LCU are detected within one minute, the system assumes that this path is experiencing a problem such that it would be advisable to take it offline until the problem can be corrected.

The `PATH_INTERVAL` value is the number of consecutive minutes during which the `PATH_THRESHOLD` value must be met to cause IOS to remove the path. So, a `PATH_INTERVAL` value of more than one minute makes it less likely that path removal will occur. Even with path recovery options, the system will never take the last path to a device offline.

The path recovery options are described in more detail in IBM Knowledge Center for z/OS, *MVS Initialization and Tuning Reference*:

https://www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.ieae200/ieae200359.htm

The **DISPLAY IOS,RECOVERY** MVS command displays the recovery option settings, as shown in Example 6-16.

Example 6-16 D IOS,RECOVERY example

```
D IOS,RECOVERY
IOS103I 11.40.45 RECOVERY OPTIONS 367
LIMITED RECOVERY TIME IS 2 SECONDS
LIMITED RECOVERY IS REQUESTED FOR DASD
PATH RECOVERY SCOPE IS BY DEVICE
DCCF IS SET TO MESSAGE
```

By enabling IOS path recovery options, the system can act more operatively to remove a failing path sooner. The limited recovery time option can also aid in triggering an unplanned HyperSwap faster.

6.2.8 Enable I/O timeouts to trigger a HyperSwap

The I/O timing facility can be enabled to trigger a HyperSwap when an I/O timeout occurs for a device that is monitored for HyperSwap. This timeout can occur based on soft errors or due to performance issues. For more details, see IBM Knowledge Center for z/OS, *MVS Initialization and Tuning Reference*:

https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.ieae200/iot.htm

You can configure the timeout trigger in the **SYSx.PARMLIB** member **IECIOsx**

- ▶ The I/O timing facility can be configured with the `IOTIMING` parameter based upon user defined I/O timing thresholds. It is important to set the `IOTIMING` to a higher value than the highest PPRC Task Timeout value (defaults to 30 seconds).
- ▶ To enable a HyperSwap trigger upon I/O timeout, modify the `IOTHSWAP` and `IOTTERM` parameters. To enable an I/O timeout to trigger HyperSwap, specify `IOTHSWAP=YES`. If you want to allow that timed out I/O can continue to swapped devices, specify also `IOTTERM=N0`.

Optionally, to modifying the **IECIO\$xx** member in **SYSx.PARMLIB**, the MVS **SETIOS** command can be used to temporarily and dynamically modify the I/O Timing values.

With **IOTIMING** specified and **IOTHSWAP=YES**, an I/O timing condition for a configured device may trigger a HyperSwap. Example 6-17 shows the logged message if such a timeout occurs.

Example 6-17 Timeout message example

```
IOS080I devn,chpid,[jobname], I/O TIMEOUT INTERVAL HAS BEEN EXCEEDED FOR {AN  
ACTIVE | A QUEUED} REQUEST. [DATASET NAME=dsname]
```

You can use the MVS **DISPLAY IOS,MIH** command to show the configured timeouts and the **DISPLAY IOS,MIH,IOTHSWAP** command to check the I/O Timing trigger setting. Example 6-18 shows the command output when the I/O Timing trigger for HyperSwap is disabled (default).

Example 6-18 MIH IO Timing trigger configuration display

```
COMMAND INPUT ==> /D IOS,MIH,IOTHSWAP  
RESPONSE=MCECEBC  
IOS086I 12.06.53 IOT HSWAP OPTIONS 529  
IO TIMING TRIGGER      : DISABLED
```

6.2.9 Couple Data Set considerations

With one exception, the Sysplex Couple Data Sets (CDSs) must be allocated on volumes that are not HyperSwap managed. This also means that they are not protected by HyperSwap. The z/OS built in high availability (HA) functionality for CDSs is used to protect them against disk failures. Manual switching is required in case of a planned HyperSwap.

The exception to this rule is the System Logger CDS (LOGR). The system logger is a z/OS component that provides a logging facility for applications running in a Sysplex. When using PPRC for disaster recovery (DR) or HyperSwap, the LOGR CDS and log streams must be allocated on volumes that are mirrored and therefore configured in the HyperSwap session.

The LOGR CDS is the only CDS that is updated more frequently, and if the system logger log streams use coupling facility (CF) structures, both must be kept consistent after a Freeze or HyperSwap. Otherwise a restart (IPL) of the system might fail.

For more considerations about Couple Data Sets, see IBM Knowledge Center for z/OS, z/OS *MVS Setting Up a Sysplex* on chapter *Planning the couple data sets*:

https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.ieaf100/cds.htm

In the following sections, we describe some HyperSwap topologies and some CDS placement approaches. In all cases, we explain how the z/OS built-in HA functionality protects continued access to the CDSs. However, HA might be compromised afterwards. You might have to change the CDS configuration manually to restore HA.

In cases where the automatic HA is not triggered, like during a planned HyperSwap, or an unplanned HyperSwap without loss of access to the primary CDSs, the CDS access will remain unchanged. But CDS HA might also be compromised and manual reconfiguration required.

CDS placement for a two site Metro Mirror configuration

To optimize Sysplex availability, place the Sysplex CDSs (except the LOGR) according to the following rules:

- ▶ Allocate primary CDSs on volumes of the primary disk system.
- ▶ Allocate alternate CDSs on volumes of the secondary disk system.
- ▶ Do not replicate the CDS volumes and have them excluded from the HyperSwap configuration.
- ▶ Allocate at least one spare CDS for each type on the primary and secondary disk system to be able to quickly create new alternate CDSs in case one site is unavailable.

Place the LOGR CDS according to these rules:

- ▶ Allocate the primary and alternate LOGR CDS on different volumes at same site (PPRC primaries).
- ▶ Mirror primary and alternate LOGR CDS volumes and include them in the HyperSwap configuration.
- ▶ To increase failure tolerance, use volumes from different LCUs or even storage systems if possible.

Note: In the past, the recommendations for placing the LOGR CDSs have been different. To reflect the current status, the z/OS Health Checker component has been updated to tolerate both LOGR CDS on the same storage subsystem for HyperSwap environments.

Figure 6-1 illustrates an example placement of CDS in a two-site replication environment. The blue strings show LCUs with devices that are part of the HyperSwap configuration. The green strings show LCUs with simplex devices, which are excluded from PPRC and HyperSwap.

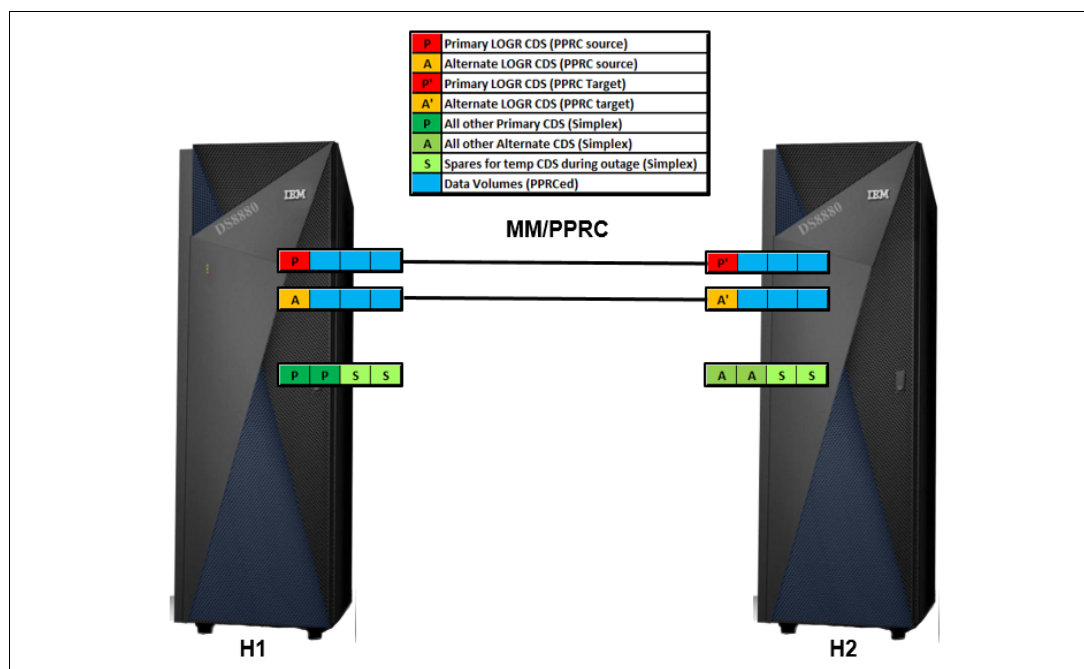


Figure 6-1 Placement of CDS in a two site replication topology

In this configuration, non-mirrored CDSs are protected against a disk failure by the automatic fail over capability to the alternate CDSs. The LOGR CDS is protected by HyperSwap.

CDS placement in a three site multiple target MM-MM configuration

In a multi-target MM-MM replication environment, you can have two target sites for storage HA, but z/OS supports only one target site for CDS availability. Therefore you must consider alignment of defined HyperSwap priorities with your Sysplex CDS placement.

We introduce two approaches in the following sections. Use the examples to develop the best configuration for your environment. We are discussing the non-replicated CDSs only. The replicated ones (LOGR) are protected by HyperSwap.

Primary CDSs in local site, alternate in remote site

The following configuration describes a common multiple target setup:

- ▶ H1 and H2 close to each other in a local campus, to protect against a single system failure.
- ▶ H3 in a remote site to protect against a site failure and for DR.

If you place the primary CDSs on either H1 or H2, and the alternate ones on H3, your CDSs are protected against a complete outage of the local campus (H1 and H2).

Figure 6-2 illustrates such an example. Again, the blue strings show LCUs with devices that are part of the HyperSwap configuration and the green ones show LCUs with simplex devices. In this case, the primary CDSs are allocated on H1 disks, the alternates on H3 and the spare CDSs on H2.

Note: If you place the primary CDS on H1 and the alternate on H2, the H1-H2 campus itself could be a single point of failure for the CDSs. If the whole site fails, both CDSs would be lost, causing a sysplex-wide outage.

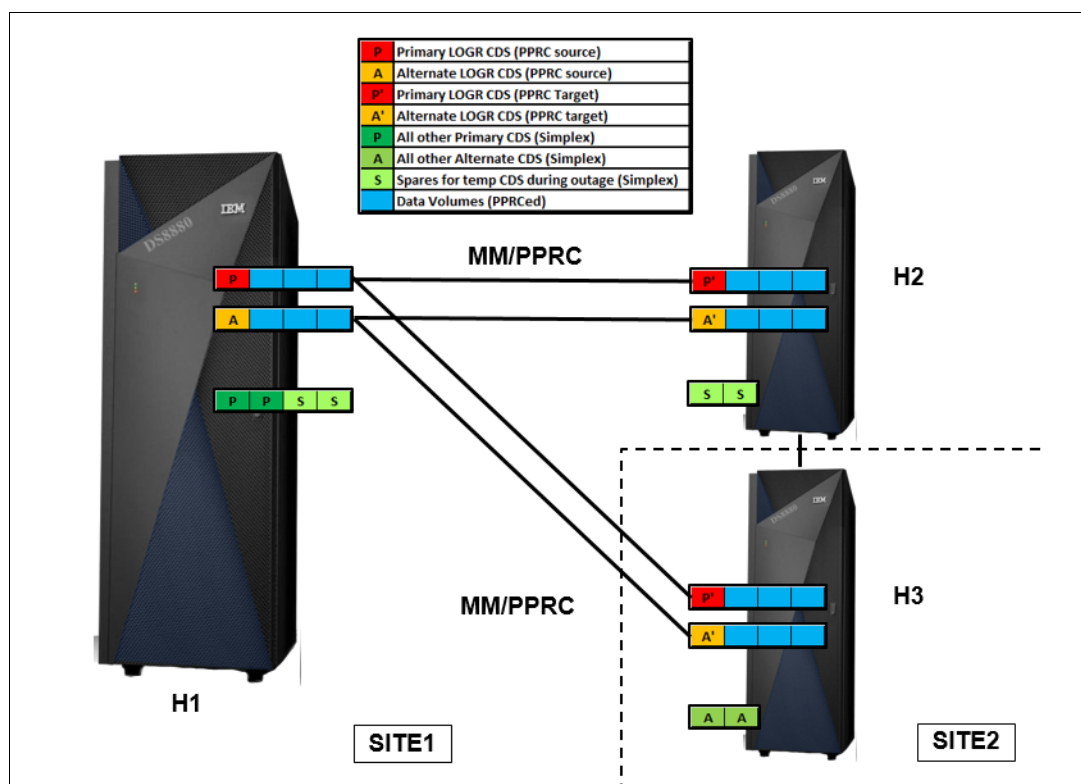


Figure 6-2 Placement option of CDS in a multi target MM/MM PPRC configuration

Assuming production I/O is running against the H1 disks, in case of a failure in H1 a HyperSwap can happen in two directions:

- ▶ Swap from H1 to H2. Regular I/O continues in H2, CDSs in H1 are unavailable, and z/OS will automatically switch to the alternate CDSs in H3:
 - Your regular I/O and the CDS access take place against different storage systems in different locations. If this situation is undesirable, consider prioritizing the swap to H3.
 - In order to return to CDS HA, you have to change the spare CDSs in H2 to alternates as soon as possible after the HyperSwap.
 - Consider switching the roles of the H2 and the H3 CDS, to return to your normal protected state: make the H2 CDS primary and the H3 CDSs the alternates.
 - If H3 is unavailable for some reason during or after the swap, no alternate CDSs will be available. This can cause a Sysplex outage and force you to manually recover CDS in H2 for an IPL from the H2 disks.
- ▶ Swap from H1 to H3. Regular I/O continues in H3, CDSs in H1 are unavailable, and z/OS will automatically switch to the alternate CDSs in H3:
 - Regular I/O and CDS access take place against the H3 disks, which is further away from the host system. This situation may lead to increased I/O response times. If this situation is undesirable, consider prioritizing the swap to H2.
 - In order to return to CDS HA, you have to change the spare CDSs in H2 to alternates as soon as possible after the HyperSwap.
 - If H3 is unavailable for some reason when the swap is attempted, HyperSwap will try to swap to H2. In this case, no alternate CDSs will be available. This can cause a Sysplex outage and force you to manually recover CDS in H2 for an IPL from the H2 disks.

Primary CDSs in remote site, alternate in remote site

An alternative way is to place the non-mirrored primary and alternate CDSs on the two secondary disk systems.

Figure 6-3 on page 113 illustrates such an example. Again, the blue strings show LCUs with devices that are part of the HyperSwap configuration and the green ones show LCUs with simplex devices. In this case, the primary CDSs are allocated on H3 disks, the alternates on H2 and the spare CDSs on H1.

Note: In this configuration, your regular I/O and the CDS access take place against different storage systems in different locations, CDS access even over the longer distance to H3. You have to determine whether the increased response time for the CDS access is tolerable in your environment.

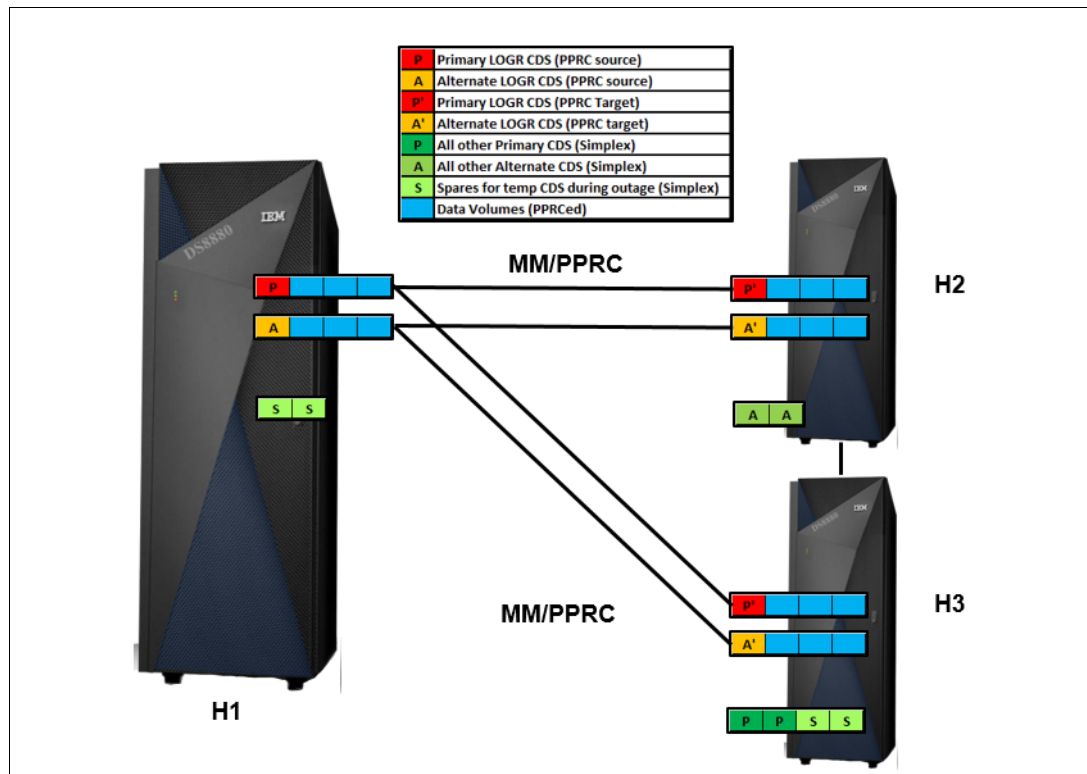


Figure 6-3 Primary CDS is allocated in H3 disk, all other storage access (I/O) are made in H1 disk

Again, assuming production I/O is running against the H1 disks, in case of a failure in H1, a HyperSwap can happen in two directions:

- ▶ Swap from H1 to H2. Regular I/O continues in H2, and CDS access stays in H3:
 - CDS HA remains intact, because the alternates in H2 are still available.
 - If H2 is unavailable for some reason during or after the swap, HyperSwap will attempt to swap to H3. CDS access will also remain on H3.
- ▶ Swap from H1 to H3. Regular I/O continues in H3, and CDS access stays in H3:
 - CDS HA remains intact, because the alternates in H2 are still available.
 - If H3 is unavailable for some reason during or after the swap, HyperSwap will attempt to swap to H2. The primary CDSs in H3 also become unavailable, and CDS access will automatically switch to the alternates in H2.

Manual Couple Data Set switching

After a HyperSwap or site switch you must ensure that HA for all CDS is restored. This may require switching a set of alternate CDSs to primaries, creating new alternates from former primaries or spares, or creating new spares.

As an example we explain the steps required after a planned HyperSwap in the 2-site scenario we describe in “CDS placement for a two site Metro Mirror configuration” on page 110.

After a planned HyperSwap from H1 to H2, the regular I/O continues on H2, whereas CDS access remains on H1. In order to move CDS access to H2, you switch the alternate CDSs on H2 to primaries, using the **SETXCF COUPLE** command with the **PSWITCH** parameter.

Example 6-19 shows the command syntax. The **TYPE** parameter is optional. If omitted, all active primary CDSs are switched.

Example 6-19 Switching PRIMARY Couple Data Set command

SETXCF COUPLE{,TYPE=xxx},PSWITCH

Now both, regular I/O and CDS access is on H2. But there still is no CDS HA at this time, because there are no alternate CDSs. To redefine alternate CDSs, use the **SETXCF COUPLE** command with the **ACOUPLE** parameter. Example 6-20 shows the command syntax. You must specify the CDS type and the name of an existing spare CDS that you want to turn into the new alternate.

Example 6-20 Configuring (spare) CDS as ALTERNATE CDS command

SETXCF COUPLE,TYPE=xxx,ACOUPLE=(spare_CDS)

There are two options, depending on whether the old primary H1 is available or not:

- ▶ H1 is available and ready for use: run the **ACOUPLE** command against the former primary CDSs on H1.
- ▶ H1 is unavailable or should not be used at this time: run the **ACOUPLE** command against the existing spare CDSs on H2.

To display the actual CDS configuration, use the MVS **DISPLAY XCF,COUPLE** command. Example 6-21 shows the output of such a command.

Example 6-21 DISPLAY XCF,COUPLE example

D XCF,COUPLE,TYPE=LOGR
RESPONSE=MCECEBC
IXC358I 13.22.32 DISPLAY XCF 732
LOGR COUPLE DATA SETS
PRIMARY DSN: SYS1.CEBCPLEX.LOG.CDS01
VOLSER: COUPL5 DEVN: 1808
...
ALTERNATE DSN: SYS1.CEBCPLEX.LOG.CDS02
VOLSER: COUPL6 DEVN: 1809
...
LOGR IN USE BY ALL SYSTEMS

6.2.10 IPL considerations

After a HyperSwap, all the z/OS LPARs in the Sysplex are using the secondary disks as their primary devices (and all of their primary disks as their secondary devices). Any IPL that is needed after the HyperSwap must be done using the secondary disks instead of the primary disks. You must create IPL profiles in the Hardware Management Console (HMC) and procedures to be used when you need to start a z/OS LPAR using the secondary disks.

The mirroring of primary to secondary disks means that the secondaries have the same VOLSER (name) as their primary partners. While the HyperSwap target volumes are PPRC secondaries, you have no read or write access to them and therefore cannot accidentally start from the wrong set of disks. However, immediately after a HyperSwap occurs, the primary and secondary disks are both in a PPRC primary suspended state, and before you restart mirroring in the reverse direction, both sets of devices may be read from and written to.

If you start a z/OS LPAR at this time using your secondary disks, and you still have I/O capability to the primary disks, a lot of Duplicate Volser messages will be produced that must be replied to. Replying to each of these messages will drastically increase the time to perform a z/OS image IPL, and wrong replies can result in data integrity exposures.

Note: If you find yourself in such a situation, you can also disable the FICON paths to the old primaries instead of replying to each message individually. This action could be done for instance by disabling corresponding switch ports, or by setting the FICON I/O ports on the primary storage controller into FCP mode, so that the z/OS image that is loaded can no longer access the old primary disks.

To reduce the likelihood of performing an IPL off of the wrong devices, and to avoid these Duplicate Volser messages, follow one of the directions described in the following sections.

Note: HyperSwap will try to Soft Fence the old primary disks after a HyperSwap occurred. If Soft Fence is supported by the storage system, it prohibits I/O to the old primary disks. This also reduces the likelihood to IPL from the wrong devices after a HyperSwap.

Alternate Subchannel Sets

The preferred option to reduce the risk of IPLing with the wrong disks is to use alternate subchannel sets. With alternate subchannel sets, your primary devices are in one subchannel set (typically 0), and the secondary devices in another one (typically 1 or 2). All of the primary devices must be in one subchannel set, and all of the secondary devices must be in one other subchannel set.

The device numbers of the primary and secondary devices must be the same within each subchannel set. For example, device 4500 would be device 04500 in subchannel set 0, and 14500 in subchannel set 1.

When you perform an IPL, the LOADPARM information entered on the HMC contains the name of the **LOADxx** member in **SYSx.PARMLIB**. Table 6-1 shows the LOADPARM information.

Table 6-1 LOADPARM information on hardware console

IODF ccuu	LOADxx	IMSI	Alt Nuc
1 - 4	5 - 6	7	8

The LOADPARM information specifies the **LOADxx** member in **SYSx.PARMLIB** (digit 5-6) that is used for the IPL. In the **LOADxx** member, you specify the subchannel set that you want to use. Example 6-22 explains the IPL load parameters of the **LOADxx** member:

Example 6-22 LOADxx member information

* IODF Suffix *					
* IODF-HLQ *					
* OS-Config *					
* Subchannel Set *					
* *					
* V V V V *					
.*-+---1---+---2---+---3---+---4---+---5---+---6---+---					
IODF 88 R17FTDIO CONFIG01 00 Y 0					

When you IPL specifying a subchannel set of 1, it tells the system to use the devices in subchannel set 1 if they exist. If devices are defined only in subchannel set 0 (for example, devices that are not mirrored), the devices defined in subchannel set 0 are used as default.

Starting with IBM System z196 (GA2), you can specify in the HMC a five digit IPL volume that contains the subchannel set and device number. In this case, you have the option of setting the subchannel set number in **LOADxx** to a value of *, which means that you will be using the subchannel set based on what you specified as the current IPL volume. For example, if you IPL from device 04500, z/OS will use subchannel set 0, and if you IPL from device 14500, subchannel set 1 will be used.

Valid values for subchannel set are 0, 1, 2, *, and blank. If the subchannel set is blank, you will be prompted to enter the subchannel set that you want to use.

In other words, by specifying the correct IPL volume and the correct **LOADPARM**, you can avoid duplicate Volser messages and accidentally using the wrong disks.

Maintaining separate I/O definitions

If you do not have a processor that supports alternate subchannel sets, or if you are unable to use them, another method is to maintain two separate I/O configurations. One is used for IPL using the primary disks, and the other for IPL using the secondary disks.

You have to create two separate IODFs, for example using HCD, distribute them to all LPARs in the Sysplex and also load them into two IOCDS slots in the HCD. Furthermore you must have two different **LOADxx** members in **SYS1.PARMLIB**. Depending on which IO definition you want to use, you choose the IOCDS slot and the load member to use, when you enter the IPL information in the HMC.

The disk definition of both configurations is as follows:

- ▶ I/O configuration for IPL from primary disks:
 - Primary disks defined as **ONLINE** at IPL
 - Secondary disks defined as **OFFLINE** at IPL
- ▶ I/O configuration for IPL from secondary disks:
 - Primary disks defined as **OFFLINE** at IPL
 - Secondary disks defined as **ONLINE** at IPL

Table 6-2 provides detailed rules to create two I/O configurations.

Table 6-2 HCD configuration

IPL using	primary addresses		secondary addresses	
	primary disks	secondary disks	primary disks	secondary disks
HyperSwap volumes	ONLINE	OFFLINE	OFFLINE	ONLINE
CDS volumes (except the LOGR)	ONLINE	ONLINE	ONLINE	ONLINE
non HyperSwap volumes	as required	as requires	as required	as required

6.2.11 Allocation and esoteric names

Esoteric definitions such as SYSDA must specify both primary and secondary devices for allocations to succeed, regardless of which set of disks is currently considered primary.

6.2.12 JES3 considerations

z/OS HyperSwap supports JES3, including JES3 managed devices. When a new HyperSwap configuration is loaded (and during each monitor interval), HyperSwap checks all device pairs. Both devices in any given pair must either be JES3 managed, or both must be non-JES3 managed. In addition, the secondary device must be offline and not in use.

You can determine if a device is JES3 managed with the JES3 ***INQUIRY,D,D=dddd** command. Example 6-23 shows the output when the device is JES3 managed (offline and online devices).

Example 6-23 JES3 Display command examples for managed devices

```
*I,D,D=9607
IAT8572 9607 (AV ) SC64
IAT8572 9607 (AV ) SC70
IAT8572 9607 (OFF) SC65
NOT OPR
IAT8500 INQUIRY ON DEVICES COMPLETE

*I,D,D=9E07
IAT8572 9E07 (AV ) SC64 ML9E07,JES=P,OS=P
IAT8572 9E07 (AV ) SC70 ML9E07,JES=P,OS=P
IAT8572 9E07 (AV ) SC65 ML9E07,JES=P,OS=P
MOUNTED
IAT8500 INQUIRY ON DEVICES COMPLETE
```

Example 6-24 shows an output example for a device that is not JES3 managed. You can see a Device Not Found message:

Example 6-24 JES3 Display command example for unmanaged devices

```
*I,D,D=0001
IAT8570 DEVICE=0001 NOT FOUND
IAT8500 INQUIRY ON DEVICES COMPLETE
```

For a complete command syntax of the JES3 **INQUIRY** command, see IBM Knowledge Center for z/OS, *JES3 Command Reference*, on the *Displaying RJP status and device status *INQUIRY,D* page:

https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.iatb300/inqd.htm

6.2.13 JES2 considerations

During a HyperSwap operation, depending on the HyperSwap policies, it is possible that one or more z/OS LPARs will be partitioned out of the Sysplex if they fail to complete the HyperSwap. If an LPAR that was taken out of the Sysplex was holding the JES2 checkpoint data set lock at that time, it may result in a damaged checkpoint record, and the message \$HASP265 will appear in the z/OS syslog, as shown in Example 6-25 on page 118.

Example 6-25 JES2 checkpoint damage record detected message

```
$HASP265 JES2 CKPT1 Data Set - Damaged Record Detected
$HASP285 JES2 Checkpoint Reconfiguration Starting
$HASP275 Member xxxx - JES2 CKPT1 Data Set - I/O Error - Reason Code 00000090
```

To avoid the need to manually reconfigure new JES2 checkpoint data sets, always have a valid NEWCKPT1 and NEWCKPT2 definition in-place. Also make sure that OPVERIFY=NO is specified in the checkpoint definitions, to avoid operator involvement during automated checkpoint reconfiguration. This setup can be verified by using the JES2 command **\$DCKPTDEF**. Example 6-26 shows a corresponding JES2 checkpoint data set configuration.

Example 6-26 JES2 Checkpoint data set configuration output

```
COMMAND INPUT ==> /$DCKPTDEF
RESPONSE=MCECEBC
$HASP829 CKPTDEF
...
$HASP829      INUSE=YES,VOLATILE=NO),
$HASP829      NEWCKPT1=(DSNAME=SYS1.HASPCPK2,VOLSER=CEB2C1),
$HASP829      NEWCKPT2=(DSNAME=SYS1.HASPCPK4,VOLSER=CEB2D1),
$HASP829      MODE=DUPLEX,DUPLEX=ON,LOGSIZE=2,
...
$HASP829      RECONFIG=NO,VOLATILE=(ONECKPT=WTOR,
$HASP829      ALLCKPT=WTOR),OPVERIFY=NO
```

6.2.14 Enhanced Catalog Sharing considerations

z/OS catalogs can be enabled for the Enhanced Catalog Sharing (ECS) protocol to improve performance of catalog sharing across multiple LPARs in a Sysplex. When a catalog is enabled and active for ECS, all entries describing changes to a shared catalog are stored in the Coupling Facility. The volume I/O penalty required for the default VSAM Volume Data Set (VVDS) shared catalog protocol is eliminated, which results in better Sysplex-wide performance.

In order to identify individual catalog entries in the ECS cache structure, a catalog identifier is composed by the Node Element Descriptor (NED) address of the volume along with a relative offset number of the catalog in the VVDS. This identifier in the cache structure becomes invalid after a HyperSwap and needs to be reestablished for each ECS catalog by removing and adding the catalog back to ECS.

ECS listens and reacts automatically on ENF signals issued by a Unit Control Block (UCB) swap to determine when an active ECS catalog needs to be removed from the cache structure. You will see an IEC378I message in the syslog after a catalog has been removed from ECS, as illustrated in Example 6-27.

Example 6-27 Removed catalog from ECS message

```
IEC378I catname REMOVED FROM ECS DUE TO DDR SWAP
```

However, there is no coordinated automation in place to reactivate ECS for the catalog. This is because the catalog must first be removed from ECS by all LPARs sharing this catalog, which is an asynchronous operation in the Sysplex.

Note: If you use ECS on HyperSwap managed volumes, you need to re-enable ECS manually after a HyperSwap has occurred.

You can re-enable ECS for all eligible catalogs on all Sysplex LPARs with the MVS **MODIFY CATALOG,EC SHR(ENABLEALL)** command. It can be routed to all LPARs, as shown in Example 6-28.

Example 6-28 Enabling eligible ECS catalogs command on all Sysplex LPARs

RO *ALL,F CATALOG,EC SHR(ENABLEALL)

Optionally, you can also automate this command to be performed some time after the HyperSwap IOSHM0414I completion message has been logged, as shown in Example 6-29.

Example 6-29 Hyperswap completion message

IOSHM0414I hh:mm:ss.nn reason HyperSwap Completed

You have to consider some delay after the HyperSwap completion to allow the asynchronous ECS removal on all LPARs to complete before you re-enable ECS. HyperSwap tests can give you an indication for the required time until all IEC378I messages from all LPARs have been logged.

You might consider converting your ECS configuration to the new Record Level Sharing (RLS) catalog sharing protocol when using z/OS 2.1 or later on all LPARs in the Sysplex. The RLS sharing protocol provides not only more granular locking through the use of a Coupling Facility lock structure, but also provides greater buffering and caching through the use of the **SMSVSAM** address space and its associated buffer pools.

A catalog in RLS mode completely eliminates the use of the SYSIGGV2 BCS reserve/enqueue, ISC, VLF, and ECS for that catalog, and the responsibility of locking, buffering and caching falls onto the **SMSVSAM** address space. As such, it provides better performance compared to ECS protocol and does not require special handling in a HyperSwap managed environment.

For more details about z/OS catalog sharing and available protocols, see IBM Knowledge Center for z/OS, *DFSMS Managing Catalogs*, on the *Sharing Catalogs Among Systems* page:

https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.idac100/sharcat.htm

6.2.15 Cache fast write avoidance

Cache Fast Write (CFW) is a disk storage system feature that allows exploiters of this function to write temporary data to the storage system cache, but not down to disk. Applications that may exploit Cache Fast Write include **DFSORT** and **SyncSort**.

If Cache Fast Write is enabled on a PPRC primary device, it is executed as a DASD Fast Write (DFW). When an I/O is received that specifies CFW, it comes with an identifier, the CFwid. This CFwid is compared to the one stored by the storage system. If it does not match, the storage system rejects the I/O and the sort job fails. This mechanism is designed to ensure that if the cache contents are lost, the job knows it.

So if one of the CECs in the storage system fails, and it fails over to the other, the sort jobs will fail because the cache contents has been lost. Similarly, if there is a HyperSwap to a different storage system, the CFWDID will not match and the job will fail. In that case, there has not been any loss of data, but the job still fails. This is why CFW should be disabled in a PPRC environment.

Disabling CFW does not change performance because CFW I/O to PPRC primaries is run as DFW I/O by the storage system. Instead, avoiding CFW allows the sort job to survive a HyperSwap or storage system CEC fail over.

Note: It is a good practice to eliminate any use of Cache Fast Write in a HyperSwap configuration.

You can use the MVS **DEVSERV PATHS,dddd** command to determine the CFW setting of a device, as shown in Example 6-30.

Example 6-30 DEVSERV PATHS command to determine CFW status

```
DEVSERV PATHS,D000
IEE459I 13.50.26 DEVSERV PATHS 922
  UNIT DTYPE MD CNT VOLSER CHPID=PATH STATUS
    RTYPE SSID CFW TC DFW PIN DC-STATE CCA DDC CYL CU-TYPE
OD000,33903 ,F ,000, ,9C=+ A6=+ AE=+ AF=+
    2107 D001 Y YY. YY. N PPRIMARY 00 00 1113 3990-6
***** SYMBOL DEFINITIONS *****
F = OFFLINE + = PATH AVAILABLE
```

To disable CFW, you use the DFSMS **SETCACHE CACHEFASTWRITE OFF** command. You specify a z/OS device number in the command and the setting is applied to the complete LCU that the device is attached to. Therefore, you need one such command for each LCU that is participating in the HyperSwap configuration. It changes the behavior of the storage system hardware, and therefore you have to run it only on one LPAR in the Sysplex. Example 6-31 shows sample JCL code calling the IDCAMS program with the required parameters.

Example 6-31 Disable Cache Fast Write sample code

```
...
//STEP0 EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
    SETCACHE UNITNUMBER(D000) CFW OFF
/*
```

You can have more than one **SETCACHE** instruction in the same **IDCAMS** call. Example 6-32 shows the output of the **DEVSERV PATHS** command after the change.

Example 6-32 DEVSERV PATHS with CFW disabled

```
DS PATHS,D000,8
IEE459I 14.16.11 DEVSERV PATHS 096
  UNIT DTYPE MD CNT VOLSER CHPID=PATH STATUS
    RTYPE SSID CFW TC DFW PIN DC-STATE CCA DDC CYL CU-TYPE
OD000,33903 ,O ,000,ATD000,9C=+ A6=+ AE=+ AF=+
    2107 D001 N YY. YY. N MT-D1POS0 00 00 1113 2107
OD001,33903 ,F ,000, ,9C=+ A6=+ AE=+ AF=+
    2107 D001 N YY. YY. N MT-D1POS0 01 01 1113 2107
```

```
0D002,33903 ,F ,000,      ,9C=+ A6=+ AE=+ AF=+  
2107 D001 N YY. YY. N MT-D1POS0 02 02      1113 2107  
...
```

As you can see, CFW was disabled for all devices in the LCU. For more details, see IBM Knowledge Center for z/OS, *z/OS DFSMS Access Method Services Commands*, in the *SETCACHE* section:

https://www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.idai200/dgt3i249.htm

6.2.16 Concurrent Copy avoidance

Concurrent Copy is a DFSMS copy function that allows you to obtain Point In Time (PIT) copies of your data concurrent with your normal processing. It is normally invoked by DFDSS Dump or Copy jobs for backup purposes.

Concurrent Copy relies on information that is stored in a sidefile in the primary disk storage system cache. This information is not mirrored to the secondary disk storage system. If a HyperSwap occurs when a Concurrent Copy job is running, this job is terminated and will have to be restarted after the HyperSwap operation completes.

Note: It is a good practice to eliminate any Concurrent Copy usage in a HyperSwap configuration.

6.2.17 Z Global Mirror (XRC) interactions

zGM (XRC) uses the z/OS System Data Mover (SDM) to asynchronously copy primary devices to a remote storage system. After a HyperSwap, SDM suspends the XRC sessions and the XRC target devices will still be recoverable to the point in time of the HyperSwap operation. Although GDPS Metro Global - XRC (GDPS MzGM) with HyperSwap supports an incremental XRC resynchronization from the new primary devices, this capability is not available with z/OS HyperSwap.

Note: After a z/OS HyperSwap, all XRC data in the storage system cache will be lost and a full initialization of all XRC volumes must be done from the new primary devices to avoid data loss, data integrity or cross volume data consistency issues.

6.2.18 FlashCopy usage in a HyperSwap environment

FlashCopy is often used to create backups or point-in-time copies of a certain range of volumes. Certain mainframe operating systems, such as z/OS, can also use FlashCopy on a data set level. FlashCopy operations are run by the storage system that hosts the FlashCopy source and target volumes.

Managing FlashCopy before and after a HyperSwap

Depending on the interface that you use to control the FlashCopy tasks, there might be a fixed association to the source and target disk device of the FlashCopy relation. This condition usually implies an association to the storage system that performs the FlashCopy. If any of the FlashCopy volumes is part of a HyperSwap configuration, the association will change after a HyperSwap. This can invalidate the procedures that you used to control the FlashCopy operations, such as TSO scripts, batch jobs, or DSCSI commands.

If your FlashCopy control interface uses a fixed storage system device association, you must ensure that it is able to address the correct devices even after a HyperSwap. For example, if you use scripted commands to operate FlashCopy for the primary volumes, you might consider maintaining two sets of scripts, one for the primaries, and another one for the secondaries, which you use after a HyperSwap.

Important: Additional care must be taken if FlashCopy target volumes are used in the HyperSwap configuration. See the following sections for additional details.

FlashCopy targets in a HyperSwap configuration

If FlashCopy target volumes are part of the HyperSwap configuration, you have to use the *Remote Pair FlashCopy with Preserve Mirror* (RPFC) capability to prevent HyperSwap from becoming disabled during FlashCopy operations. When a FlashCopy is initiated between the PPRC primary devices, the RPFC function of the primary storage system performs a synchronized remote FlashCopy between the secondary devices, and thus keeps the MM replication synchronized.

Without this functionality, a FlashCopy to a primary PPRC device in the HyperSwap configuration would cause MM to go into DUPLEX PENDING mode and HyperSwap to be disabled, until the MM pair has completed the full resynchronization and returns into FULL DUPLEX mode.

On DS8000 storage systems, use of RPFC in a HyperSwap environment requires the FlashCopy options Allow FC to PPRC Primary and Allow Targets to be online. Additionally, it is good practice to use the Preserve Mirror Required option to prevent an unexpected PPRC status change on the FlashCopy target PPRC pair.

Note: The DS8880 storage systems do not support the *Preserve Mirror Preferred* option anymore. The goal of this policy has been incorporated into the modified behavior of the *Preserve Mirror Required* option. The consolidated goal of the *Required* option is now to take the FlashCopy whenever possible, but only if it does not cause a PPRC state change. It means, depending on the PPRC state either a RPFC or a normal FlashCopy is taken. For more details on the latest Remote Pair FlashCopy behavior, see the Redbooks publication *DS8000 Copy Services*, SG24-8367, in the section about *Remote Pair FlashCopy implementation and usage*.

While local FlashCopy targets are normally in an OFFLINE state when a FlashCopy is initiated (except for data set level FlashCopy), HyperSwap will place all secondary PPRC devices in a *pathgrouped* state upon activation of the HyperSwap configuration. In MVS the device state will be shown as F-SYS (offline, in use by system) instead of OFFLINE. However, a storage controller can only use the pathgroup state to distinguish if a device is online or offline.

Therefore, all HyperSwap secondary devices are considered as online by the DS8000 storage system. For this reason, the **Allow target online** parameter is required to ensure that the remote FlashCopy can be established without error.

Example 6.2.19 shows the required parameters to prevent an unexpected PPRC state change in a HyperSwap environment for the TSO **FCESTABL** command.

Example 6-33 FCESTABL parameters for HyperSwap managed FlashCopy target devices

```
TGTPPRIM(YES) PRESERVEMIRROR(REQUIRED) ONLINTGT(YES)
```

Important: If you don't allow online targets, a FlashCopy might be successful for the primary volumes (if the FlashCopy target devices are offline), but fail for the secondaries because of the F-SYS (pathgrouped) state. This situation causes the FlashCopy target PPRC relations to suspend and HyperSwap to be disabled.

Additionally, the suspension is a Freeze trigger for the HyperSwap Manager. If you defined a Freeze&Stop policy for the HyperSwap session, no more write I/O will be possible for the duration of the configured Extended Long Busy (ELB) timeout. As such, a FlashCopy operation with improper parameter usage might cause a production I/O impact in a HyperSwap environment.

For more information about Remote Pair FlashCopy, see the IBM Redbooks publication *DS8000 Copy Services*, SG24-8367:

<http://www.redbooks.ibm.com/abstracts/sg248367.html>

Remote Pair FlashCopy usage with Multiple Target Peer-to-Peer Remote Copy

In a Multiple Target Peer-to-Peer Remote Copy (MT-PPRC) configuration, Remote Pair FlashCopy synchronization is supported only for one of the two PPRC relations, even if both are in FULL DUPLEX state. To define which of the PPRC relations is enabled to support RPFC, you can use the DSCLI `chpprc` command, as shown in Example 6-34.

Example 6-34 Control Remote Pair FlashCopy capability for Multi Target relations

```
chpprc -action enable -ctrl pmir source_volume_ID:target_volume_ID
chpprc -action disable -ctrl pmir source_volume_ID:target_volume_ID
```

For more details, see IBM Knowledge Center for DS8880 on the `chpprc` page:

https://www.ibm.com/support/knowledgecenter/en/ST5GLJ_8.5.0/com.ibm.storage.ssic.help.doc/f2c_clchpprc_6lvfam.html

For the CSM 3-site Multi Target-MM-MM session type, this specific RPFC capability was not initially supported as a CSM session or role pair property. Starting with CSM 6.2.0, a new server property has been implemented to enable users to specify which of the role pairs should enable the RPFC capability. To make this specification, you can add a property to the CSM `rmserver.properties` server properties file, as shown in Example 6-35.

Example 6-35 Remote Pair FlashCopy property for Multi Target PPRC sessions

```
com.ibm.csm.<sessionName>.<rolepair>.userpfc=true
```

Note: You can specify only one of the two MM role pairs in this property.

When CSM establishes the MM session pairs, the pair marked with this property is enabled to support RPFC. Be aware of following restrictions when using this property:

- ▶ This property is set to `false` by default. It must be set to `true` to enable RPFC for a specific role pair in a session.
- ▶ The RPFC property is only used when CSM is establishing the corresponding relationships. If the relationships are already established on the DS8000, the corresponding role pair in the session needs to be suspended and restarted to activate the RPFC capability. Alternatively, the DS8000 DSCLI can be used to enable the RPFC capability on existing PPRC pairs.

- ▶ Currently CSM does not support removing the RPFC capability on existing PPRC pairs. If there is a requirement to switch RPFC capability between the legs of a Multi Target MM relationship, use the DS8000 DSCLI to disable the capability concurrently on the current pairs before you change the CSM property to enable RPFC on the other role pair.

Alternatively, you can use CSM to terminate the current MM role pair with the RPFC capability, which removes the PPRC relationships completely on the DS8000. However, this requires a full resynchronization of the terminated role pair when it will be restarted.

- ▶ If the CSM server property is modified through the CSM GUI **Settings** → **Server Properties** menu, the change is effective immediately after saving the properties. If the change is made manually in the `rmserver.properties` file, allow up to 2 minutes for the CSM server to pick up the change.
- ▶ CSM server properties are not replicated between active and standby servers. If you modify the RPFC property, ensure to make this change also on the standby CSM server to allow proper session management after a **Takeover** on the CSM standby server.

For more details, see IBM Knowledge Center for CSM, on the *Preserve Mirror option* page:

https://www.ibm.com/support/knowledgecenter/SSESK4_6.2.3/com.ibm.storage.csm.help.doc/frg_c_preserve_mirror_recs.html

Note: DS8000 Remote Pair FlashCopy is not supported together with asynchronous replication. Therefore, it cannot be used in three-site or four-site CSM sessions that contain Global Mirror (GM) relations.

There is a workaround, if you do not need the FlashCopy targets at the remote end of the long distance replication (DR location), using the CSM *Consistency Group* functionality. For example, if you run a three-site MT-MM-GM session and need to create FlashCopies where the targets are part of the HyperSwap configuration, you can combine the MM leg of the three site session, containing the FlashCopy sources, with a separate MM session, containing the FlashCopy targets, in a single HyperSwap configuration. See 7.3.5, “HyperSwap management for asymmetrical replication topologies” on page 152 for details.

6.2.19 Coexistence with other products that use UCB swaps

Products like *IBM Transparent Data Migration Facility* (IBM TDMF) or *Innovation FDR Plug and Swap* (FDR/PAS) logically move (migrate) volumes concurrently by swapping UCB pointers. Both IBM TDMF and FDR/PAS support z/OS HyperSwap by temporarily preventing a HyperSwap from occurring. While they perform their UCB swap, they programmatically block the z/OS HyperSwap function.

If you use such products, make sure that you are running a version that supports z/OS HyperSwap. The following product levels are required as a minimum:

- ▶ IBM TDMF v5.2 or above
- ▶ FDRPAS V 5.4/76 or above

z/OS support for IBM TDMF and FDR/PAS was provided in APAR OA26509 for z/OS releases 1.9 and above.

6.2.20 Special HyperSwap considerations for use with other applications

Consider the following suggestions for using HyperSwap with other applications.

SAP/DB2 and z/OS HyperSwap

The preferred method of SAP Backup is to do a FlashCopy of the DB tables followed by the DB logs. This method is available with IBM DB2® 9, which uses DFSMSHsm Fast Replication (**FRBACKUP**) to flash the volumes to an SMS Copy Pool. DFSMSHsm supports the Remote Pair FlashCopy (RPFC) capability to avoid that Flash might change the PPRC state of the FlashCopy target volume. For details about using RPFC and Flash to PPRC primary with DFSMSHsm Fast Replication, see IBM Knowledge Center for z/OS MVS *Using MM primary volume during fast replication backup* page:

https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.arcf000/fcpremir.htm

zCDP for DB2 (DB2 System Backup & Restore) utilities in conjunction with DFSMSHsm Fast Replication can eliminate DB2 backup windows. More and more customers require a copy of their backups at both sites, which is still available after a HyperSwap. Proper implementation of the RPFC option can ensure that it has no impact to HyperSwap readiness while taking synchronized FlashCopy on local and remote storage subsystems. See 6.2.18, “FlashCopy usage in a HyperSwap environment” on page 121 for more details.

Note: DFSMSHsm Fast Replication requires that source and target FlashCopy volumes be online. Therefore it implicitly uses the DS8000 FlashCopy to online target option, which is also required if the FlashCopy target device is a HyperSwap enabled PPRC pair with RPFC capability.

IMS/DB2 and z/OS HyperSwap

Both DB2 and IMS™ Full Function and Fast Path provide the ability for software duplication of various key data sets, for example DB logs, DB table spaces, and so on. Typically these are read across multiple storage systems to handle situations where HyperSwap provides an alternative solution today. Rethinking the most appropriate duplication method with these applications might be required if HyperSwap is being implemented.

Additionally, the DB2 and IMS Lock timeout values must be configured to be higher than the Planned & Unplanned HyperSwap time.

Computer Associates MIM and z/OS HyperSwap

In order to prevent Computer Associates MIM from taking a page fault during HyperSwap processing, both Computer Associates and IBM recommend to add MIM to the list of Critical Paging address spaces:

CRITICALPAGING for PGM=MIMDRRM

Computer Associates also has other recommendations for Multi Image Integrity (MII) and to ensure that RESERVEs are converted to Global ENQs when running in a HyperSwap enabled environment. For more details, see the Computer Associates manual *CA MII Data Sharing for z/OS - CA MII Programming Guide* chapter about *Utilities and other Interfaces / GDPS/PPRC HyperSwap Support*:

https://support.ca.com/cadocs/0/CA%20MIM%20Resource%20Sharing%20for%20z%20S%2011%209-z%20S-ENU/Bookshelf_Files/PDF/MIMVS_MIIProgGd_enu.pdf

Note: z/OS HyperSwap does *not* support the described Computer Associates Rexx interfaces. However, you need to ensure that RESERVEs are converted to Global ENQs.

6.2.21 SMF Recording

When z/OS HyperSwap is active, there is no SMF interval recording for either the HSIB or HSIBAPI address spaces, or for the **XCFAS** address spaces. The reason for this design is to avoid potential hangs during HyperSwap processing due to access to disk storage by SMF. If you have existing SMF processes that depend on SMF interval records for **XCFAS**, review and revise these procedures accordingly.



Part 3

Management and Operations

This part is an overview of how to manage and operate various aspects of z/OS HyperSwap, IBM Copy Services Manager (CSM) sessions and the z/OS IP host connection. It describes CSM session configuration options for Hardened Freeze and HyperSwap management, as well as HyperSwap testing, logging, alerting, and troubleshooting capabilities.



Managing z/OS HyperSwap with IBM Copy Services Manager

This chapter describes how to set up and manage z/OS HyperSwap with IBM Copy Services Manager (CSM). First it explains the required steps, available options, and HyperSwap related session actions with the help of a two-site Metro Mirror (MM) Failover/Failback example session. Then it discusses additional options and considerations that come with other session types that support z/OS HyperSwap:

- ▶ Basic HyperSwap session
- ▶ Three-site sessions with long-distance replication
- ▶ Three-site sessions with two synchronous replication legs
- ▶ Four-site session with long-distance replication and regional HyperSwap support

7.1 Prepare session and enable HyperSwap

In this section, we describe how to associate a z/OS Sysplex to a CSM session and how to enable HyperSwap for this session. We also describe the various HyperSwap configuration options.

7.1.1 Assign discovered Sysplex to CSM session

As explained in 2.1, “CSM connection type overview” on page 20, you must connect CSM to the z/OS HyperSwap Manager address space in order to enable and manage HyperSwap. You can have either one or more z/OS IP host connections or a z/OS native Host Connection.

Before you can enable z/OS HyperSwap in a CSM session, you have to associate the session with the Sysplex that is supposed to manage HyperSwap for the session. This step is required because you can manage more than one Sysplex with a single CSM server using separate sessions, each associated with its own Sysplex.

CSM lists every Sysplex it is connected to in the session properties dialog. Pick the Sysplex you want to manage with your session. Figure 7-1 shows the drop-down menu to select a Sysplex name. CSM does not allow you to enable HyperSwap until the session is associated with a Sysplex.

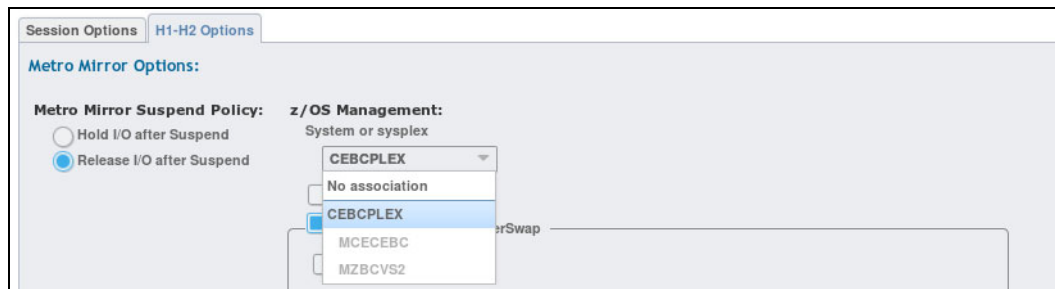


Figure 7-1 Associate Sysplex to session

The drop-down field only shows the z/OS system names for the logical partitions (LPARs) that CSM is connected to.

Note: The z/OS system name shown by CSM is the name as it appears, for example, in the output of the MVS command **DISPLAY XCF, SYSPLEX**.

When you define a Sysplex association for a session, you cannot change it as long as it is in Prepared state. You must at least **Suspend** the session in order to change the Sysplex association.

7.1.2 Enable HyperSwap for a session

After you have associated a Sysplex to the session, you can enable HyperSwap in the session properties dialog, as shown in Figure 7-2.

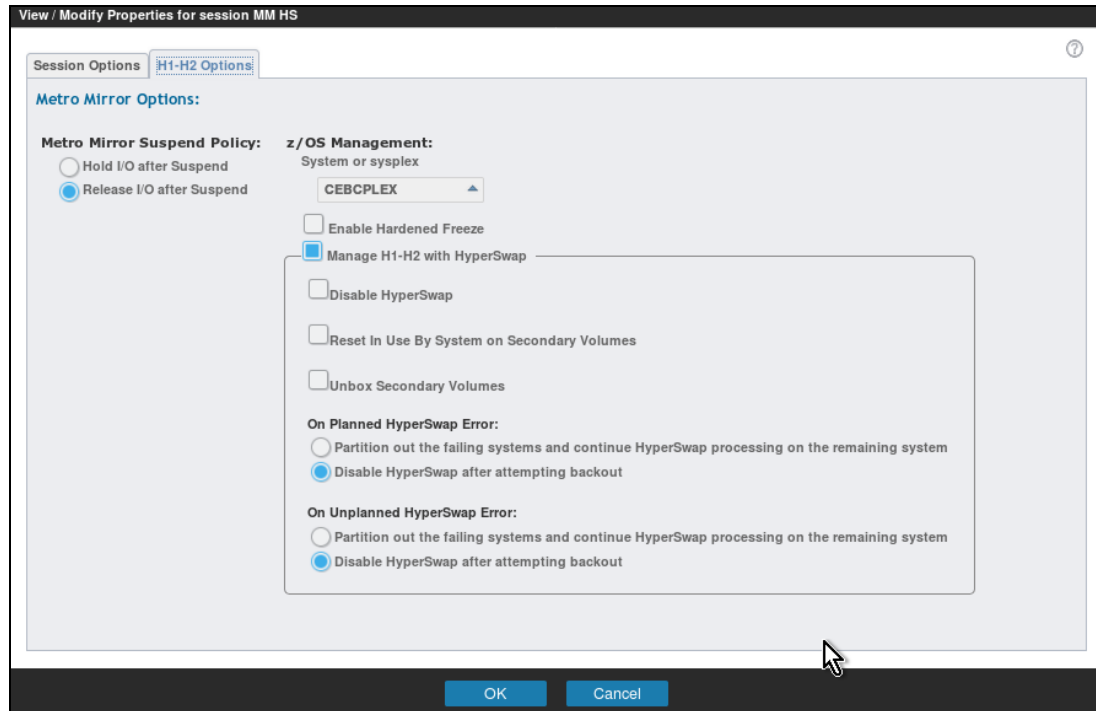


Figure 7-2 Manage H1-H2 with HyperSwap

Note: For certain session types, HyperSwap management can be activated for different role pairs in a session on different tabs of the session properties dialog. We explain these options later in this chapter.

After HyperSwap management is activated in the session properties, CSM communicates to the HyperSwap management address space of the associated Sysplex, depending on the session state and the actions that are being performed:

- ▶ Session is inactive: No z/OS communication is necessary.
- ▶ Session is started or restarted: Make initial HyperSwap load test to all pairs in the session before (re-)starting PPRC.
- ▶ Session is Prepared with all MM pairs in Full Duplex: Load the HyperSwap configuration and start monitoring the z/OS HyperSwap state.
- ▶ HyperSwap is disabled while HyperSwap configuration is loaded: Disable HyperSwap for active configuration per operator command.
- ▶ HyperSwap is re-enabled while HyperSwap configuration is loaded: Enable HyperSwap for active configuration per operator command.
- ▶ HyperSwap management is being removed while the session is active: Purge the HyperSwap configuration if loaded and stop HyperSwap state monitoring.
- ▶ HyperSwap management is being added while the session is active: Load the HyperSwap configuration if the session is Prepared and start HyperSwap state monitoring.

7.1.3 HyperSwap configuration settings

The session properties dialog page for HyperSwap management offers some settings that you can use to influence the behavior of the HyperSwap function in certain situations.

Disable HyperSwap

If a HyperSwap configuration is loaded and the **Disable HyperSwap** option is selected, the HyperSwap status will go to `Disabled by Operator`. The option corresponds to the z/OS **SETHS DISABLE** command and has the same effect on the session. Clearing this property corresponds to a **SETHS ENABLE** command and enables HyperSwap again for the loaded configuration. For more **SETHS** command details see 6.2, “IBM z/OS configuration for HyperSwap” on page 99.

Reset or unbox secondary volumes

Since CSM 6.2.2, two options are available that can be applied to recover a HyperSwap configuration load failure:

- **Reset in Use by System on Secondary Volumes**

During the load, a secondary device that is `OFFLINE` but has a state of `IN USE BY SYSTEM` or `F-SYS`, which indicates that the `UCBNALOC` bit is enabled for other system access to the device, will be tolerated.

- **Unbox Secondary Volumes**

During the load, a boxed secondary device will automatically be unboxed

These options are disabled by default and you should only enable them temporarily if a normal configuration load fails. This situation can happen if a secondary device is `BOXED` in z/OS or detected as being `IN USE BY SYSTEM`. If you see such an error, first investigate what the root cause could be.

If you are sure that the configuration is correct and the devices can be used in the HyperSwap configuration, activate the corresponding load option and try to start the CSM session again. This action triggers a HyperSwap configuration reload with the selected recovery option. When the load is successful and the session goes into the `Prepared` state with HyperSwap enabled, deactivate the selected load option again.

For additional details about how to detect and recover `BOXED` or `IN USE BY SYSTEM` devices, see 8.5, “Troubleshooting” on page 174.

Note: These new HyperSwap load options are only applicable after z/OS APAR OA53082 is applied to all LPARs in the HyperSwap managed Sysplex.

Recovery in case of a HyperSwap failure

There are options to influence the recovery actions if a HyperSwap error occurs, either during a planned or an unplanned HyperSwap trigger. You can select one of the following actions for both cases independently:

- **Partition out the failing systems and continue HyperSwap processing on the remaining systems**

If this option is set and a HyperSwap failure occurs, the z/OS LPARs where the HyperSwap failed will be quiesced and partitioned out of the Sysplex. The HyperSwap continues for the remaining LPARs. This is the default option for unplanned HyperSwap failures.

► **Disable HyperSwap after attempting bailout**

If this option is set and a HyperSwap failure occurs, the HyperSwap Manager address spaces on all z/OS LPARs attempts to reverse all HyperSwap related activities and restore the pre-HyperSwap state. Depending on how far the swap had already progressed, the reversal may not be successful and can result in a partially swapped Sysplex. This is the default option for planned HyperSwap failures.

Note: Consider your organization availability requirements and policies to choose the best HyperSwap failure policy settings for both HyperSwap types.

Hardened Freeze

You can use the **Enable Hardened Freeze** setting to provide a more robust way to maintain data consistency for disaster recovery (DR). With Hardened Freeze, the HyperSwap infrastructure is used to perform the freeze and release function that is used to make the MM secondary device consistent in case of a replication problem.

To use Hardened Freeze, you need a CSM host connection and the HyperSwap address spaces running. You can use Hardened Freeze without enabling HyperSwap. It is implicitly used when HyperSwap is activated, regardless of the Hardened Freeze setting in the session properties. If Hardened Freeze is enabled without HyperSwap, CSM loads the session as MM configuration to the z/OS HyperSwap Manager. When HyperSwap is enabled, the session is loaded as a HyperSwap configuration, which implicitly uses the Hardened Freeze functionality.

WARNING: Without Hardened Freeze functionality, in a CSM server running on a z/OS LPAR with the underlying CSM server file system volumes configured in a MM relation, the volumes could become inoperable when entering the freeze (Extended Long Busy (ELB) condition) required for data consistency. Subsequently, the CSM server will be unable to perform the unfreeze (release ELB condition).

This can lead to a complete Sysplex halt until the storage system itself releases the freeze after the configured ELB timeout (default 2 minutes). With the Hardened Freeze functionality, the freeze and release operations are performed by the HyperSwap address spaces, which reside in z/OS main memory and don't depend on the ability to perform I/O to primary volumes.

If a CSM server is running on a z/OS LPAR with the underlying CSM server fleshiest volumes configured in a MM relation, it is good practice to have the Hardened Freeze capability always enabled in the corresponding CSM session, even if HyperSwap is also activated for the session. This ensures that when HyperSwap is removed, for example during a maintenance activity, CSM will reload the session as MM configuration to the HyperSwap Manager and Hardened Freeze functionality remains enabled for the session.

Details about how to maintain data consistency for DR purposes is beyond the scope of this publication. For more information about how CSM and the DS8880 storage systems manage consistency, see the IBM Redbooks publications *IBM Copy Services Manager Implementation Guide*, SG24-8375 and *DS8000 Copy Services*, SG24-8367:

- <http://www.redbooks.ibm.com/abstracts/sg248375.html>
- <http://www.redbooks.ibm.com/abstracts/sg248367.html>

7.1.4 HyperSwap active

When HyperSwap is activated successfully for a session, CSM indicates it by adding the HyperSwap symbol, a circular arrow, to the session pictogram, as shown in Figure 7-3. It also adds a HyperSwap and z/OS Association field to the textual description.

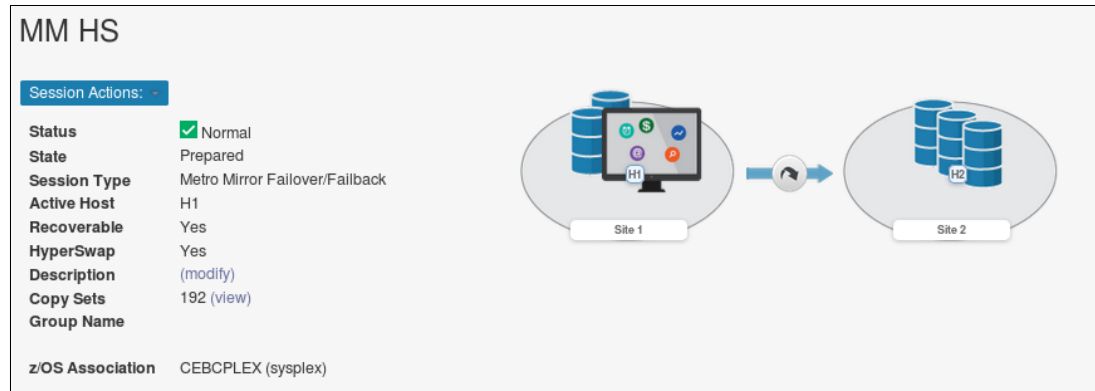


Figure 7-3 Session with HyperSwap enabled

The CSM session overview panel also contains columns which indicate whether HyperSwap or Hardened Freeze is enabled for a session, as you can see in Figure 7-4.

Name	Group Name	Status	State	Type	Active...	Active Site	Recov...	Progress	Hyper...	Hard...
MM HS		Normal	Prepared	MM	H1	Site 1	Yes	H1 → H2 10	Yes	
AW_MM_TCT_Demo		Normal	Prepared	MM	H1	ACA91	Yes	H1 → H2 10		

Figure 7-4 CSM session overview with HyperSwap enabled session

If you enabled HyperSwap management for an inactive or suspended session, the session state will not change directly. Only after you run a **Start** command for the session and the synchronization or resynchronization of the pairs is completed (Prepared state), will the HyperSwap configuration be loaded and enabled.

Note: If you enable HyperSwap for an inactive or suspended session, an additional z/OS HyperSwap load test is performed by CSM before MM is started or restarted. This z/OS HyperSwap load test fails if not at least one device from the HyperSwap configuration is online to each LPAR in the Sysplex. In this case CSM does not (re-)start the session and will set it to a Severe status.

A possible workaround for such a situation is to skip the z/OS HyperSwap load test. This can be accomplished by removing the HyperSwap management property from the session before you issue the **Start** command. After the session reaches a Prepared state, you can activate the HyperSwap management property again and CSM will pass the HyperSwap configuration directly without load test.

7.1.5 Check HyperSwap status in z/OS

You can also check the HyperSwap configuration and status information in z/OS, using the z/OS **DISPLAY HS** command, as shown in Example 7-1.

Example 7-1 DISPLAY HS command examples

DISPLAY HS,CONFIG

IOSHM0304I Active Configurations 943

Session Name	Session Type	Priority	Status	Systems Impacted
MM_HS_____H1H2	HyperSwap	1	HyperSwap Ready	0

DISPLAY HS,STATUS

IOSHM0303I HyperSwap Status 958

Number of configurations: 1

Replication Session: MM_HS_____H1H2

Socket Port: 5858

HyperSwap enabled

Swap Highest Priority: No

Disallow Non-MultiTarget System: No

New member configuration load failed: Disable

Planned swap recovery: Disable

Unplanned swap recovery: Disable

FreezeAll: Yes

Stop: No

The settings marked **blue** are the ones that can be changed in the CSM session properties. Table 7-1 shows how you can map the HyperSwap console status configuration options to the CSM session properties:

Table 7-1 Mapping of HyperSwap z/OS console status information to CSM session properties

z/OS console status	CSM session HyperSwap property
Number of configurations: 1 or 2 Can be 2 only in a Multi Target MM - MM session with 2 active HyperSwap configurations	<ul style="list-style-type: none">▶ 1: Single MM role pair of a CSM session has HyperSwap activated▶ 2: Two MM role pairs of a CSM multi target session have HyperSwap active at same time
Replication Session: <ul style="list-style-type: none">▶ <i>Name_____HxHy</i>: the CSM session name (long names are truncated with ... in the middle) and the corresponding role pair▶ <i><CSM Consistency Group Name></i>	Without set Consistency Group Name: <ul style="list-style-type: none">▶ CSM session name▶ Role pair which uses this HyperSwap settings With set Consistency Group Name: <ul style="list-style-type: none">▶ Customized CSM Consistency Group Name
HyperSwap status: <ul style="list-style-type: none">▶ Enabled▶ Degraded▶ Disabled	Session status: <ul style="list-style-type: none">▶ Session is HyperSwap Prepared, Normal, Green▶ Session is HyperSwap Prepared, Warning, Yellow▶ Session is in HyperSwap mode, Severe, Red

z/OS console status	CSM session HyperSwap property
Swap Highest Priority: <ul style="list-style-type: none"> ▶ No ▶ Yes (Will swap the active HyperSwap configuration with the highest priority) 	HyperSwap Site selection and Priority: <ul style="list-style-type: none"> ▶ Allow HyperSwap Manager to determine the HyperSwap site ▶ Determine the HyperSwap site by specified priorities: Hx, Hy, Hz
New member configuration load failed: <ul style="list-style-type: none"> ▶ Disable ▶ Partition 	On Configuration Load error: <ul style="list-style-type: none"> ▶ Disable HyperSwap (new default, not changeable since CSM 6.2.2) ▶ Partition out failing systems
Planned swap recovery: <ul style="list-style-type: none"> ▶ Disable ▶ Partition Unplanned swap recovery: <ul style="list-style-type: none"> ▶ Disable ▶ Partition 	On Planned HyperSwap Error: <ul style="list-style-type: none"> ▶ Disable HyperSwap (default) ▶ Partition out failing systems On Unplanned HyperSwap Error: <ul style="list-style-type: none"> ▶ Disable HyperSwap ▶ Partition out failing systems (Default)
FreezeAll:(Use of Hardened Freeze) <ul style="list-style-type: none"> ▶ No ▶ Yes 	Session Type: <ul style="list-style-type: none"> ▶ Basic HyperSwap session only ▶ All other sessions with enabled HyperSwap
Stop: <ul style="list-style-type: none"> ▶ No ▶ Yes 	MM Suspend Policy: <ul style="list-style-type: none"> ▶ Release I/O after Suspend ▶ Hold I/O after Suspend

For more details and other HyperSwap related z/OS commands, see 6.2, “IBM z/OS configuration for HyperSwap” on page 99.

7.2 HyperSwap usage scenarios

The following sections provide details about most common HyperSwap usage scenarios. For a general understanding, we also provide some basic information about CSM session management. However, this publication is not intended to be a complete CSM guide. If you need more detailed information, see IBM Knowledge Center for CSM:

https://www.ibm.com/support/knowledgecenter/SSESK4/csm_kcwelcome.html

In addition, see *IBM Copy Services Manager Implementation Guide*, SG24-8375:

<http://www.redbooks.ibm.com/abstracts/sg248375.html>

7.2.1 General remarks about CSM session management

CSM allows you to perform certain actions on the defined session. Actions are allowed, based on the current state of a session. CSM helps you to take the best possible action by allowing only the ones that make sense in a given situation. Figure 7-5 on page 137 shows an example of a session action menu.

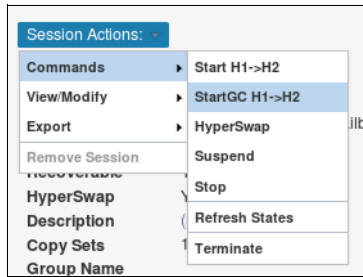


Figure 7-5 Session actions example

Session actions can also be directly performed from the session overview panel. A few session actions can even be performed when multiple sessions are selected, like defining a common consistency group name.

Whenever you perform an action command on a session, CSM shows a confirmation dialog that describes the consequences of the selected action. We show an example for a **Start H1->H2** command in Figure 7-6.

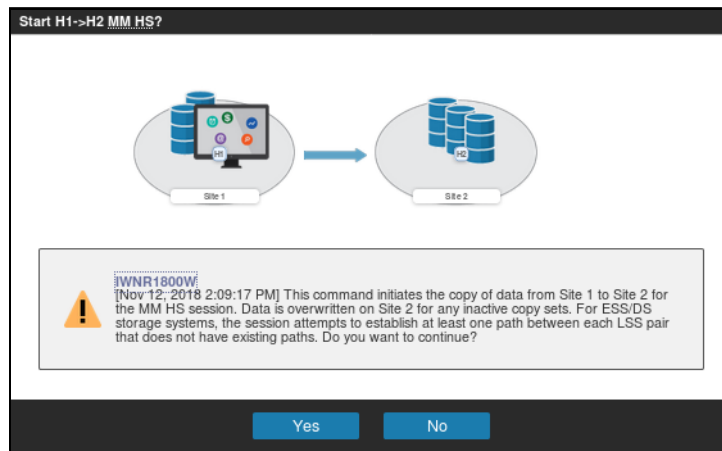


Figure 7-6 Confirm session command

Always read the description carefully and make sure you have chosen the correct command with the desired consequences. After you click the **Yes** button, CSM performs the command without any further confirmation.

After a session command is run, CSM indicates it in a status line at top of the GUI window, as shown in Figure 7-7.

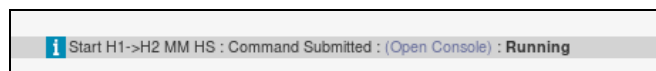


Figure 7-7 Session command status

The status indicator in the line changes from Running to Completed after the command has completed. It may also change to Error if the command did not complete successfully. In this case, CSM shows an error message. You can click the message to get more information about the error.

CSM also logs session state changes and errors in the CSM Console panel. For more information about error logging and alerting, see 8.1, “CSM monitoring, logging and alerting” on page 156.

7.2.2 Starting a HyperSwap session

After you define a HyperSwap capable MM session and populate it with Copy Sets, you can start it, using the **Session Actions** drop-down menu, as shown in Figure 7-8.

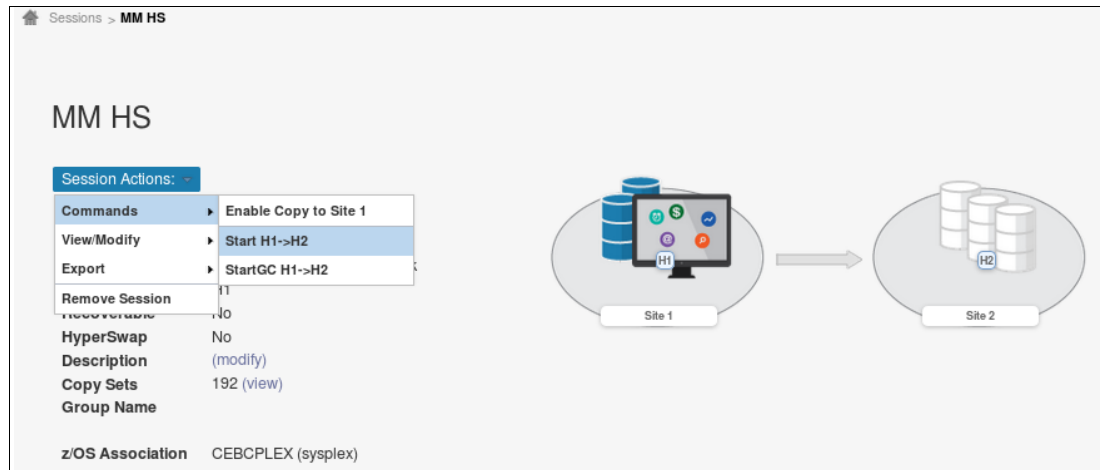


Figure 7-8 Start a HyperSwap session

CSM starts the MM replication for all Copy Sets in the session. As shown in Figure 7-9, the session enters a Preparing state and Warning status without HyperSwap capability, until all Copy Sets are synchronized. CSM also shows the initial copy progress of the replication in the session pictogram on the session details panel, as well as on the session overview panel for each participating role pair of the session.

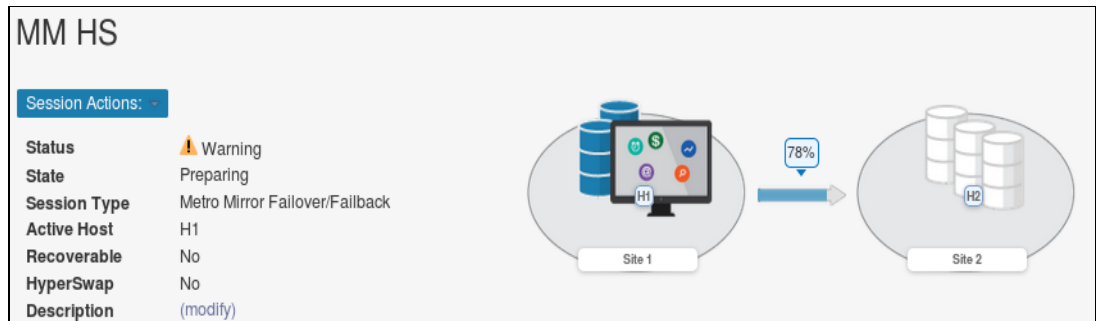


Figure 7-9 HyperSwap session in Preparing State

After all Copy Sets are synchronized (Prepared), and CSM has been able to load the HyperSwap configuration to z/OS, the session enters a Normal status and Prepared state. HyperSwap is also shown as enabled, as seen in Figure 7-3 on page 134.

7.2.3 Planned HyperSwap

You can use the **HyperSwap** command in the session actions menu, as shown in Figure 7-10, to perform a planned HyperSwap. This action swaps the application I/O from the H1 to the H2 volumes in the session without application impact.

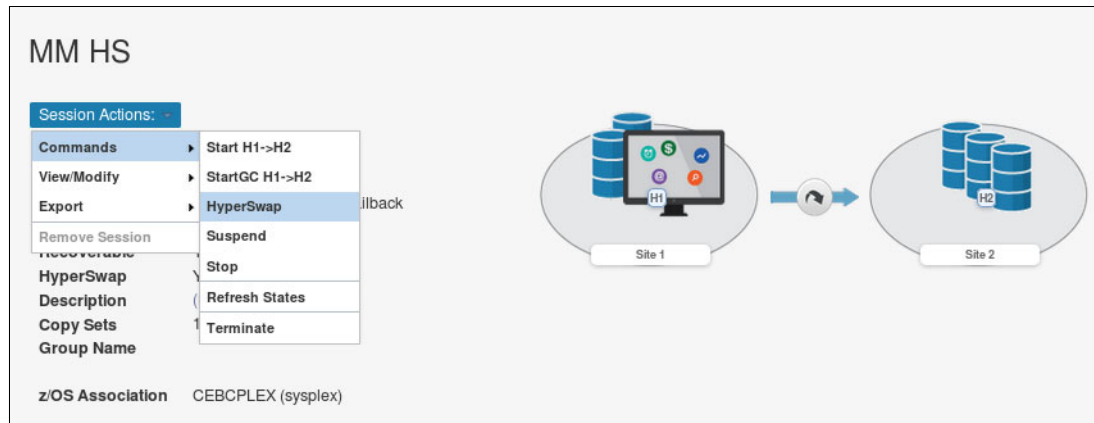


Figure 7-10 Perform planned HyperSwap

After you confirm the command in the warning dialog, the HyperSwap is performed by the z/OS HyperSwap address spaces. When it completes, all application I/O is then running against the H2 volumes and data replication is suspended. Figure 7-11 shows the session view after the HyperSwap completed.

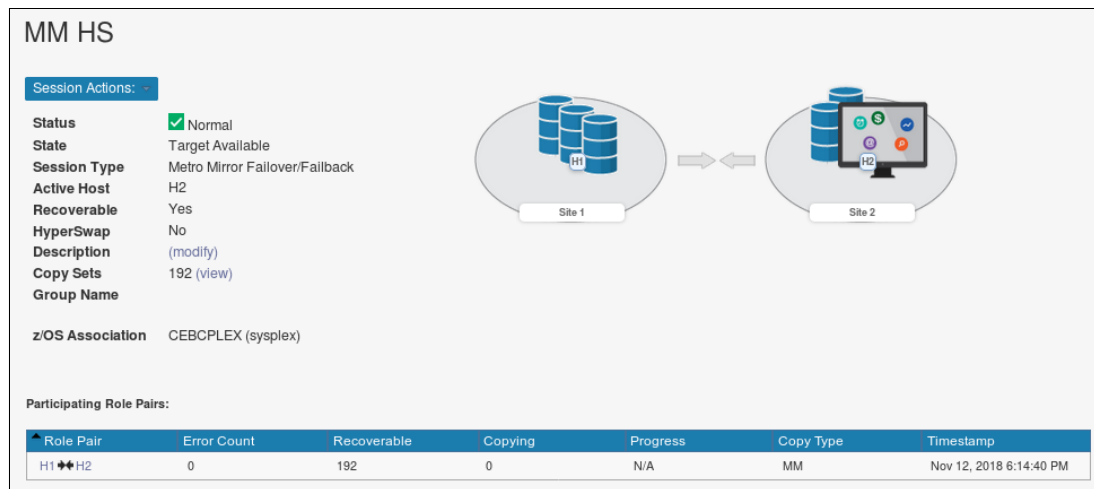


Figure 7-11 Session view after planned HyperSwap

The session reflects the new state as Target Available, the current Active Host as H2, and the missing HyperSwap capability. The role pair overview table shows a time stamp, which is set to the time of the HyperSwap.

7.2.4 Resynchronizing replication after a HyperSwap

When you are ready to start data replication back to the H1 volumes, you run the **Start H2->H1** session command, as shown in Figure 7-12.

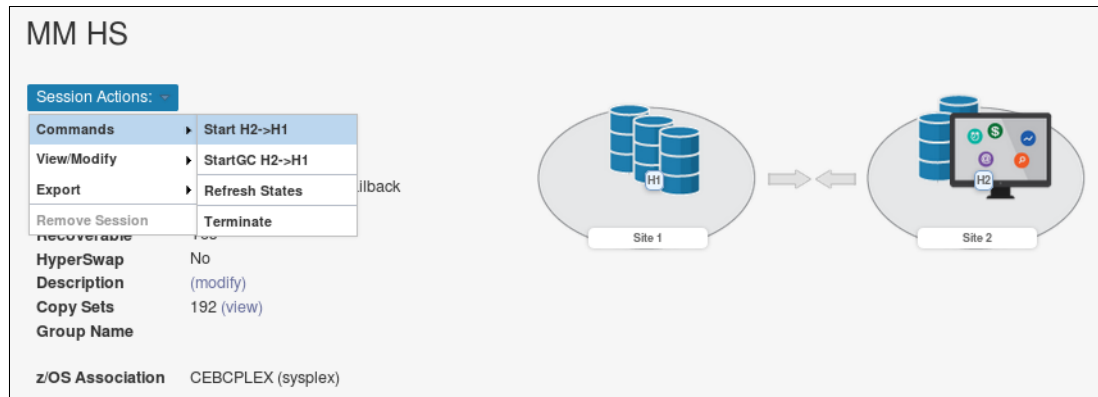


Figure 7-12 Resync after HyperSwap: Start H2 -> H1

CSM reverses the replication direction to H2 -> H1 and restarts the replication. Only data that was changed on H2 between the HyperSwap and the resynchronization will be replicated. The session details panel shows the replication progress in the reversed direction, as shown in Figure 7-13.

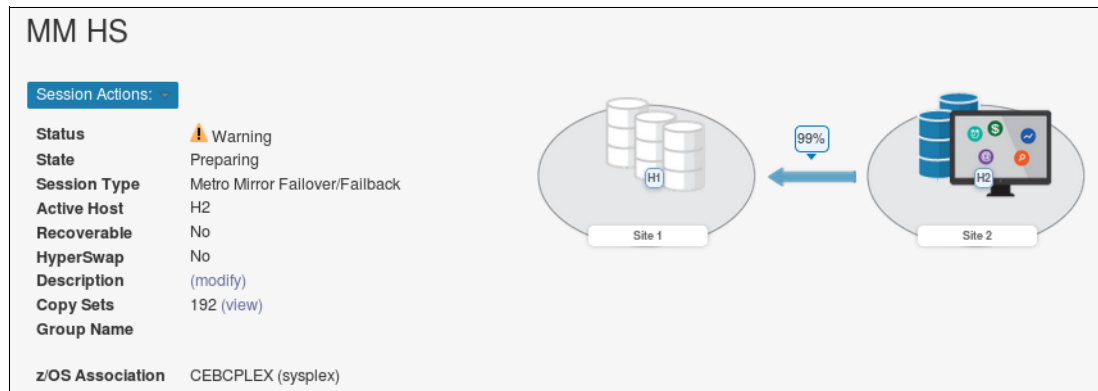


Figure 7-13 Resync after HyperSwap in progress

When the resynchronization is complete, CSM automatically re-enables the HyperSwap capability. The session view, in Figure 7-14 on page 141, shows the HyperSwap symbol and the respective information in the text fields. Host I/O is still against the H2 volumes, and the replication direction from H2 to H1.

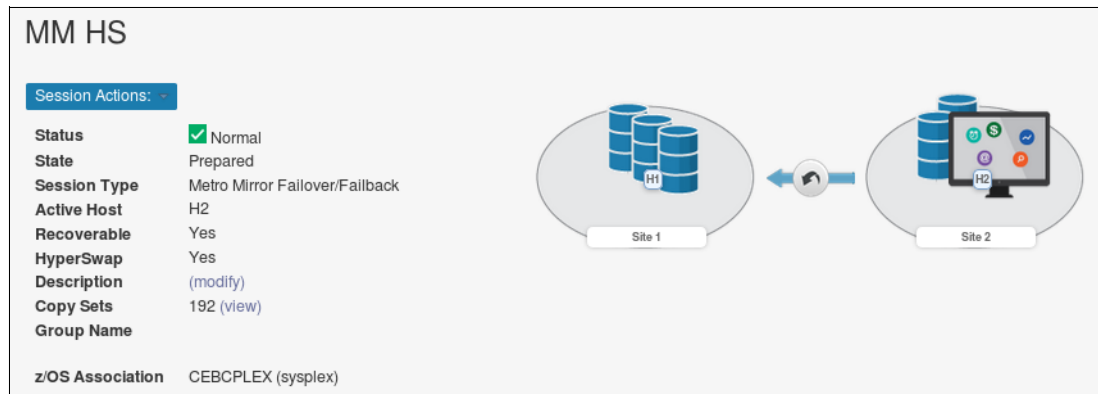


Figure 7-14 Basic HyperSwap session - Start H2->H1 Completed

The next HyperSwap will swap application I/O from H2 back to H1. The sequence of events is exactly as described above, just in the opposite direction.

7.2.5 Further considerations

This section describes other circumstances you might encounter.

Pausing replication in a HyperSwap session

There are two ways to pause replication in a MM session:

- The **Suspend** command pauses replication in a way to ensure that a consistent set of data can be provided on the target site for recovery. For a MM role pair, it performs a Freeze operation to pause the replication, and therefore makes the secondaries consistent, such that they could be used for recovery. HyperSwap is disabled and the session remains recoverable.
- The **Stop** command pauses replication without guaranteeing a consistent set of data on the target site. For a MM role pair it performs a pause of the replication relationship for each individual pair and therefore leaves the secondaries in an inconsistent state. HyperSwap is disabled and the session is marked as unrecoverable.

In both cases the replication relations remain active and change recording bitmaps are maintained by the storage systems. Use the known session **Start** command to restart replication. Only changed data will need to be replicated.

Terminating a HyperSwap session

The **Terminate** command withdraws the MM relationships between the H1 and H2 volumes, thus terminating data replication. If you want to start a HyperSwap session after it has been terminated, a full copy will take place from H1 to H2. The **Terminate** command on its own does not maintain consistency, because it removes the replication relationships without a Freeze operation.

Note: How to maintain data consistency for DR purposes is beyond the scope of this publication. For more information about how CSM and the DS8880 storage systems manage consistency, see *IBM Copy Services Manager Implementation Guide*, SG24-8375 and *DS8000 Copy Services*, SG24-8367.

PPRC Cascaded flag

With one exception, all DS8000 CSM replication session types use the Cascaded flag when PPRC pairs are established. The exception is the Basic HyperSwap session type, as explained in 7.3.1, “Basic HyperSwap session” on page 142. Using the Cascaded flag does not harm the PPRC management, even if cascading is not used. The benefit however, is that it provides flexibility to manage more complex topologies, if PPRC needs to be cascaded at a later time.

If any of these session types is used with third-party storage systems, such as Hitachi Virtual Storage Platform (VSP), you might have to take extra steps to configure the storage system to allow cascaded PPRC.

7.3 Characteristics of different HyperSwap capable session types

In this section, we explain how HyperSwap management of various other CSM session types differs from the ordinary MM session we used as example in the previous sections. We cover only the HyperSwap related aspects of the session. See *IBM Copy Services Manager Implementation Guide*, SG24-8375 and IBM Knowledge Center for CSM for all other session management aspects.

7.3.1 Basic HyperSwap session

The session type *Basic HyperSwap* is intended only for storage system high availability (HA) at low cost. It is the only replication session type available in *IBM Copy Services Manager for z/OS Basic Edition*, which you can run in z/OS without additional license charges. The session cannot be used for DR because it does not maintain data consistency of the secondary devices in case of a replication problem or rolling disaster.

The *Basic HyperSwap* session implicitly has HyperSwap management enabled and does not offer the DR-related options. Except for that, all other HyperSwap related configuration options are available, as you can see in Figure 7-15.

The screenshot shows the 'Session Options' tab with the 'H1-H2 Options' sub-tab selected. Under 'Metro Mirror Options:', there is a 'z/OS Management:' section with a dropdown menu set to 'CEBCPLEX'. Below this are three unchecked checkboxes: 'Disable HyperSwap', 'Reset In Use By System on Secondary Volumes', and 'Unbox Secondary Volumes'. There are two sections for error handling: 'On Planned HyperSwap Error:' and 'On Unplanned HyperSwap Error:'. Each section has two radio button options: 'Partition out the failing systems and continue HyperSwap processing on the remaining system' and 'Disable HyperSwap after attempting backout'. In both sections, the 'Disable HyperSwap after attempting backout' option is selected.

Figure 7-15 HyperSwap related options of a Basic HyperSwap session

Because Basic HyperSwap is not intended for DR, it also does not provide the implicit Hardened Freeze capability. This is indicated in the z/OS console HyperSwap status FreezeAll:No, as shown in Example 7-2.

Example 7-2 No disaster recovery support in Basic HyperSwap session

```
DISPALY HS,STATUS
...
FreezeAll: No
Stop: No
```

This condition means that neither z/OS nor CSM will react with a freeze processing on corresponding triggers such as suspended primary devices due to link errors. The z/OS HyperSwap Manager will monitor primary PPRC devices of a Basic HyperSwap configuration for suspending states. Once detected, it reacts with immediate release I/O processing (Unfreeze) of the affected logical control unit (LCU) pairs to avoid that I/O may be impacted by any ELB condition on the suspended primary devices.

The Basic HyperSwap configuration will remain loaded, but HyperSwap will be disabled after the first suspended PPRC pair. The HyperSwap Manager continues to monitor for subsequent suspended primaries to release I/O and avoid subsequent ELB impacts until the session will be purged by other CSM activities.

This behavior of the Basic HyperSwap session is significantly different to the Hardened Freeze behavior used in the other HyperSwap enabled sessions. Therefore Basic HyperSwap sessions cannot be used to ensure DR on the secondary site, but only to ensure storage HA of a single site or campus configuration, where replication errors are less likely to occur.

The Basic HyperSwap session also does not provide a **Suspend** command, to stop MM with consistent secondaries.

Note: With a Basic HyperSwap session, CSM does not use the Cascaded flag when establishing MM relations, since the session is not intended to be flexible for allowing cascaded topologies. If this session type is used with 3rd party storage subsystems such as Hitachi VSP, you don't have to set a specific storage system option mode to allow cascaded PPRC.

7.3.2 Three-site session types with remote replication for disaster recovery

In this section we explain the HyperSwap related specifics of the two types of three-site sessions with remote replication for DR. We do not cover other topics, such as long-distance replication, recovery objectives, and DR procedures. See *IBM Copy Services Manager Implementation Guide*, SG24-8375 for details about these topics.

Multi Target MM - GM session

In this session type, you have a synchronous MM and an asynchronous Global Mirror (GM) replication leg from the same set of primary volumes. Figure 7-16 shows the topology of an active session. There also is a variant of this session type that uses an additional practice volume on the DR site (H3).

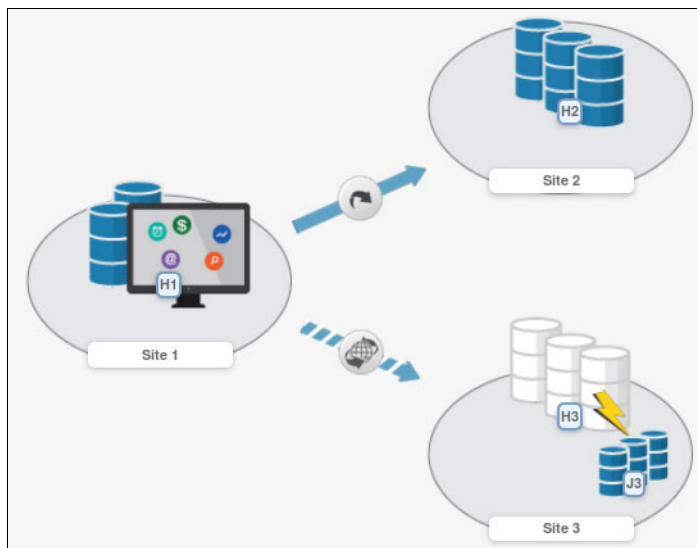


Figure 7-16 Topology of a Multi Target MM - GM session with HyperSwap

You have HyperSwap capability on the MM leg H1-H2. The session properties offer the same HyperSwap related configuration settings as for the two-site MM session described in 7.1, “Prepare session and enable HyperSwap” on page 130.

If a HyperSwap occurs, either planned or unplanned, host I/O is swapped to H2. After the swap, both replication legs are suspended, as shown in Figure 7-17.

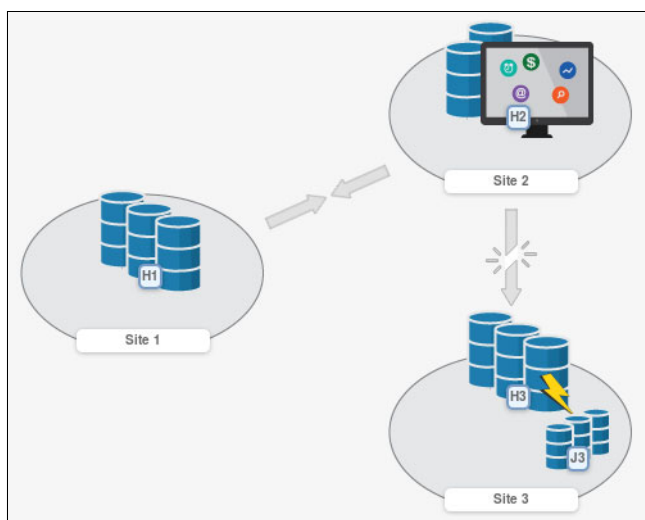


Figure 7-17 MT-MM-GM session after HyperSwap to H2

H2 acts as the new primary and can replicate in two ways:

- ▶ Synchronously to H1 (MM)
- ▶ Asynchronously to H3/J3 (GM)

By default, you must restart both replication legs manually. CSM offers to start both at the same time or individually, depending on the state of your infrastructure. After the resynchronization between H2 and H1 is complete, CSM automatically enables HyperSwap.

Due to the *Multi Target Incremental Resynchronization* (MTIR) capability, only data that has been changed after the HyperSwap is replicated (if the infrastructure and the replication relations remain in place). See *IBM DS8870 Multiple Target Peer-to-Peer Remote Copy*, REDP-5151 for more details about the incremental resynchronization capabilities with Multiple Target Peer-to-Peer Remote Copy (MT-PPRC).

Note: Starting with CSM 6.2.1, CSM can be configured to restart the replication between the former multi target sites automatically after a HyperSwap. This option is not exposed in the GUI. You must enter a new CSM property in the Server Properties file:

csm.auto.restart.after.swap=true

See IBM Knowledge Center for CSM, on the *rmserver.properties* file page for details about changing the CSM server properties file:

https://www.ibm.com/support/knowledgecenter/en/SSESK4_6.2.3/com.ibm.storage.csm.help.doc/frg_r_rmserver_properties_file.html

Three-site cascaded Metro Global Mirror session

In a cascaded Metro GM session, MM is also replicating from H1 to H2, but the GM asynchronous leg is replicating from H2 to H3/J3, as shown in Figure 7-18. There also is a variant of this session type that uses an additional practice volume on the DR site (H3).

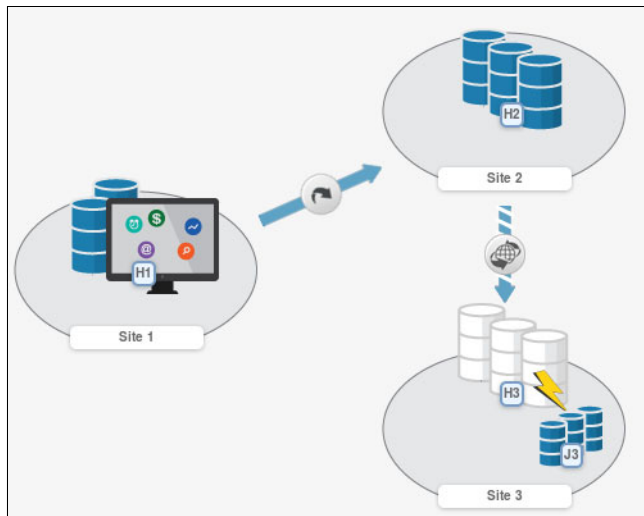


Figure 7-18 Topology of a Metro Global Mirror session with HyperSwap

You have HyperSwap capability on the MM leg H1-H2. The session properties offer the same HyperSwap related configuration settings as for the two-site MM session described in 7.1, “Prepare session and enable HyperSwap” on page 130.

If a HyperSwap occurs, either planned or unplanned, host I/O is swapped to H2. After the swap, the MM synchronous replication is suspended, whereas the GM asynchronous replication is still active, as shown in Figure 7-19.

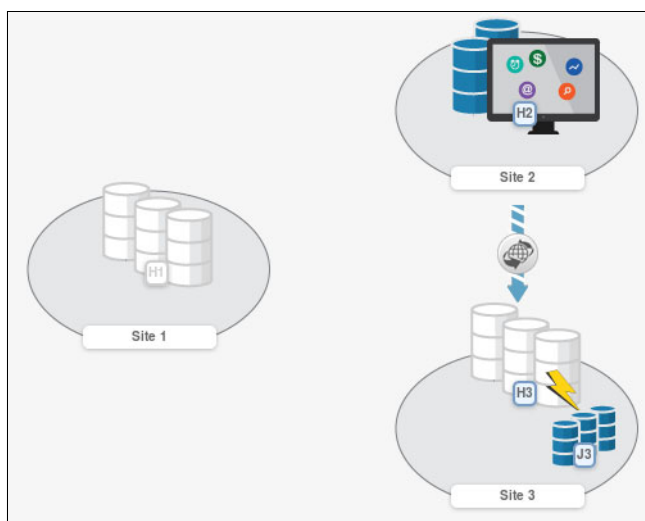


Figure 7-19 Metro Global Mirror session after HyperSwap

Returning to a tree-site configuration after a HyperSwap implies a reversal of the cascaded replication direction. You can do this using the CSM session command **Start H2->H1->H3**. Only data that has been changed after the HyperSwap is replicated (as long as the infrastructure and the replication relations remain in place). This session type does not use MT-PPRC and its MTIR capabilities. Therefore, CSM performs the resynchronization in several steps, utilizing the *Metro Global Mirror (MGM) Incremental Resynchronization* capabilities, as illustrated in Figure 7-20.

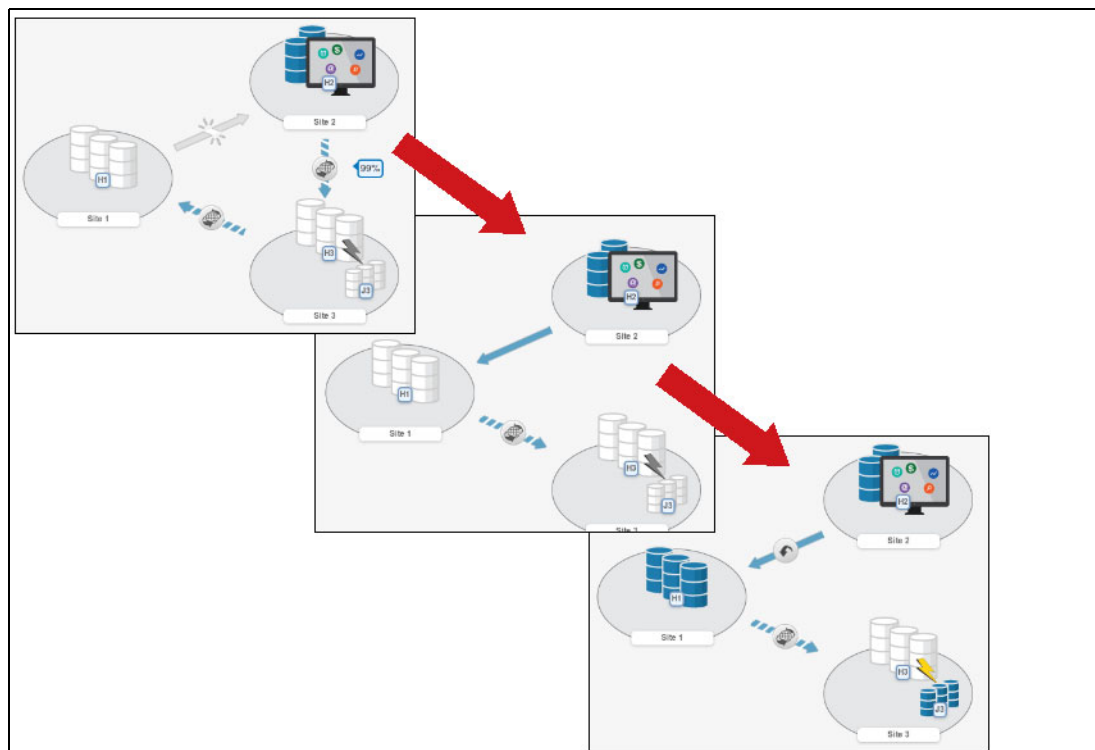


Figure 7-20 Sequence of steps for an MGM session to return to 3-site configuration

The resynchronization of the changed data happens over the remote distance link between H3 and H1. See *IBM Copy Services Manager Implementation Guide*, SG24-8375 and *DS8000 Copy Services*, SG24-8367 for more details about the cascaded incremental resynchronization process.

Note: The MGM replication topology and session type were introduced long before the DS8000 MT-PPRC capabilities. For backward capability in existing client configurations, the session type, its procedures and capabilities are not enhanced with Multi Target capabilities.

A major advantage of the MGM replication topology is that it does not require manual intervention when the primary site fails. I/O can HyperSwap to the secondary site while GM remains active with the remote site for continuous DR protection. However, manual intervention is required if the secondary site fails in order to start incremental resynchronization between the primary and remote sites to reestablish DR protection.

Starting with CSM 6.2.1, this major advantage has been met by supporting an automatic resynchronization capability between the target sites of a Multi Target Session after a HyperSwap occurred to any of the target sites. For this and following other reasons, today the Multi Target MM - GM session type is more convenient in most situations:

- ▶ Its internal recovery procedures are much simpler, thus faster and more robust
- ▶ Incremental resynchronization can be used between any site in various failover and failback scenarios
- ▶ No manual intervention is required to restore protection if any of the target site fails, because the surviving leg will continuously be used to replicate data
- ▶ Data of the MM relation after a HyperSwap is resynchronized over the local MM links
- ▶ Each replication leg can be managed individually in CSM, thus providing more operational flexibility

7.3.3 Three-site Multiple Target MM - MM session

In a *Multiple Target MM - MM* (MT MM-MM) session, you have two synchronous MM replication legs from the same set of primary volumes. Figure 7-21 on page 148 shows the topology of an active session.

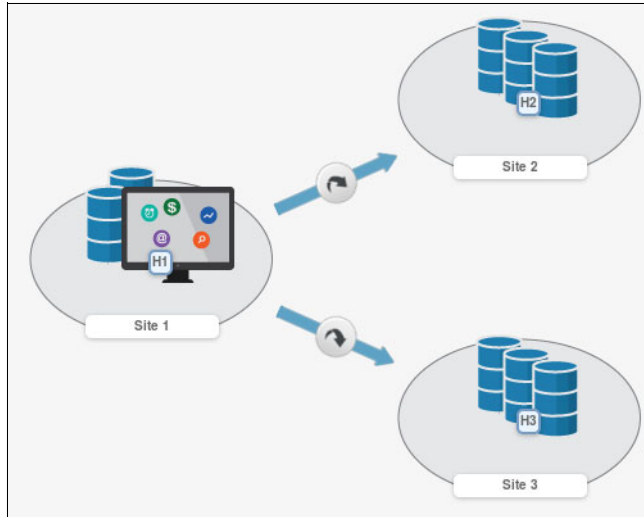


Figure 7-21 Topology of an MT MM-MM session

You can have HyperSwap capability on both MM legs. After a HyperSwap was performed, either to H2 or H3, you have the choice to start MM replication and enable HyperSwap between H2 and H3, too. Therefore the session properties offer additional tabs to configure HyperSwap and enable it for each leg individually. Figure 7-22 shows the first tab, which contains general session settings, such as the z/OS Sysplex association.

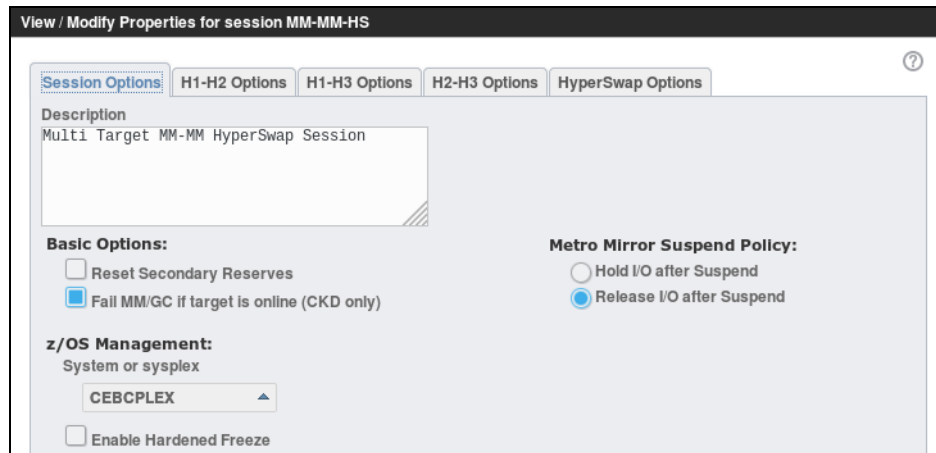


Figure 7-22 General session settings for a MT MM-MM session

Figure 7-23 shows the second tab, which you use to enable HyperSwap for the H1-H2 replication leg. You see equivalent tabs for the other replication legs H1-H2 and H2-H3.

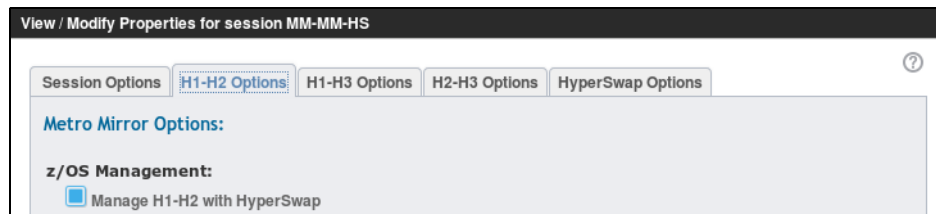


Figure 7-23 Enable HyperSwap for individual legs in a MT MM-MM session

You can configure the common HyperSwap settings in the last tab. They are the same for all three potential legs, as shown in Figure 7-24.

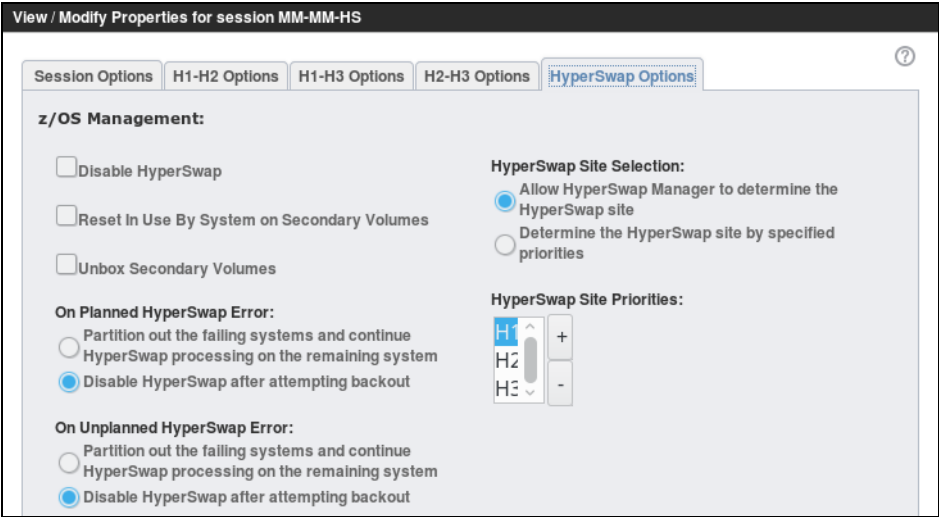


Figure 7-24 Common HyperSwap settings in a MT MM-MM session

In addition to the settings you already know from other session types, you can also select whether the HyperSwap Manager address spaces should determine the target for an unplanned HyperSwap autonomously, or whether you want to define a HyperSwap priority. The session command to initiate a planned HyperSwap lets you choose either option.

Note: A reason to choose a HyperSwap site priority could be a significant difference in replication distances between sites. If, for example, H1-H2 is much farther than H1-H3, you could consider to prioritize the swap from H1 to H3, instead of leaving the decision to the software.

z/OS HyperSwap supports only one active HyperSwap session. For a MT MM-MM session it can consist of two HyperSwap configurations, so that HyperSwap can swap to any of the two target sites, depending on the defined swap priorities. The z/OS command **DISPLAY HS,CONFIG** reflects this fact, as shown in Example 7-3.

Example 7-3 z/OS *DISPLAY HS,CONFIG* command for MT MM-MM session

```
DISPLAY HS,CONFIG
RESPONSE=MCECEBC
IOSHM0304I Active Configurations
```

Session Name	Session Type	Priority	Status	Systems Impacted
MM-MM-HS___H1H2	HyperSwap	2	HyperSwap Ready	0
MM-MM-HS___H1H3	HyperSwap	3	HyperSwap Ready	0

If a HyperSwap occurs, either planned or unplanned, host I/O is swapped to one of the secondary sites and both replication legs are suspended. Figure 7-25 on page 150 shows the situation after a swap to H2.

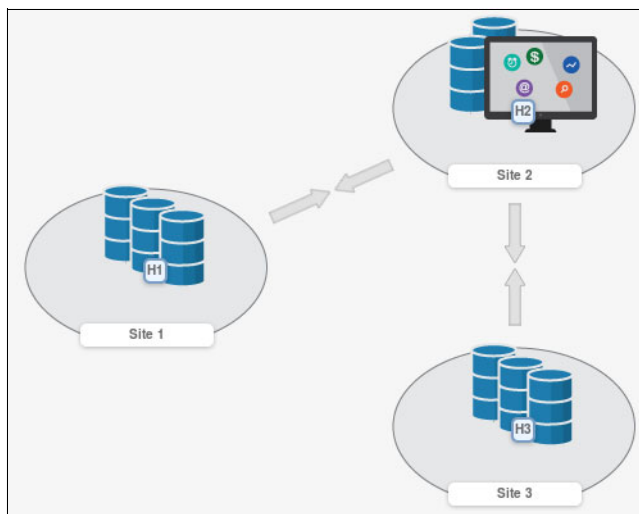


Figure 7-25 MT MM-MM session after HyperSwap to H2

To return to a protected configuration, you must restart the replication manually. The DS8000 MT-PPRC Incremental Resynchronization capability allows to resynchronize replication from H2 to H1, H2 to H3, or both directions. If you configured the session to turn on HyperSwap on the H2-H3 leg as well, HyperSwap will be enabled for both legs after the resynchronization is complete, as shown in Figure 7-26.

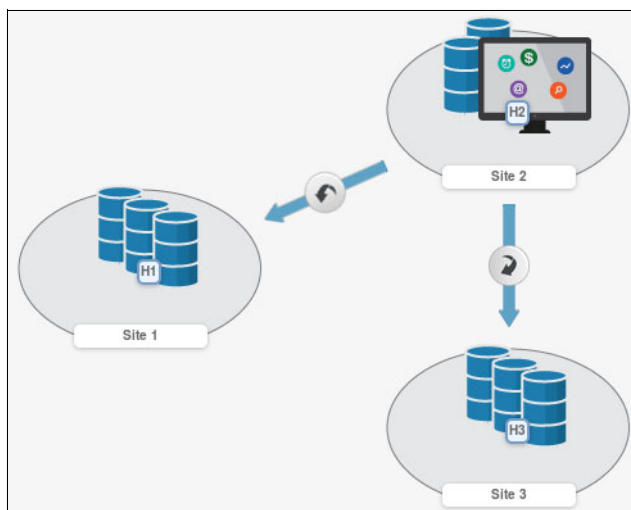


Figure 7-26 HyperSwap options after resynchronization in a MT MM-MM session

Note: Starting with CSM 6.2.1, CSM can be configured to restart the replication between the former multi target sites automatically after a HyperSwap. This option is not exposed in the GUI. You must enter a new property to the CSM server properties file:

csm.auto.restart.after.swap=true

See IBM Knowledge Center for CSM *rmserver.properties* file page for details about changing the CSM server properties file:

https://www.ibm.com/support/knowledgecenter/en/SSESK4_6.2.3/com.ibm.storage.csm.help.doc/frg_r_rmserver_properties_file.html

If you enable HyperSwap between the original multi target secondary sites (H2-H3) and automatic restart after a HyperSwap, CSM will also enable HyperSwap automatically when the automatic resynchronization has completed.

7.3.4 Four-site session MM - GM w/ Site 4 Replication

Since version 6.2.3, CSM supports a four-site session type *MM - GM w/ Site 4 Replication*. This session manages a symmetrical two-region configuration. In the current active region (where production I/O is running), you can have HA and local DR with synchronous MM replication and HyperSwap.

The data is also replicated via GM to the remote region. There again, local HA and DR is prepared for quick use with an additional cascaded Global Copy replication leg. In this publication, we provide only a high-level overview of this very powerful session type.

Figure 7-27 shows the topology of the CSM four-site session, with production running in region A at H1. HyperSwap is enabled for the synchronous replication H1-H2. After a region switch, you can quickly synchronize the Global Copy between H3 and H4, and enable HyperSwap for region B.

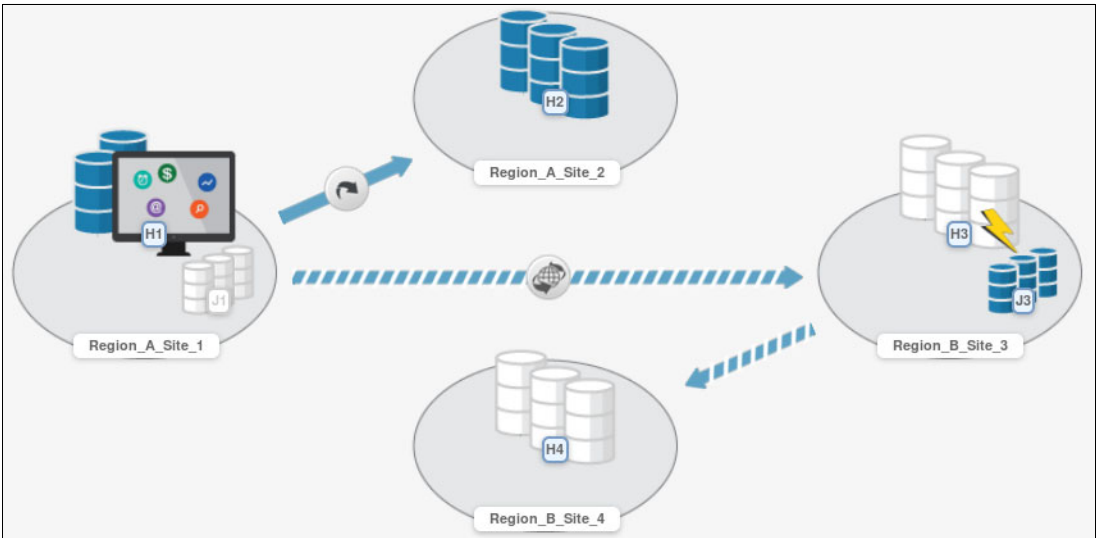


Figure 7-27 CSM 4-site session

There are two role pairs that can support HyperSwap. Therefore the session properties dialog has two tabs to enable the feature, H1-H2, and H3-H4 options, as shown in Figure 7-28. Each of the HyperSwap configurations belongs to its own region, and can have its own Sysplex association.



Figure 7-28 Session properties for a 4-site session

The general HyperSwap configuration is the same as with most other session types. You can change them using the HyperSwap Options tab. The other tabs are for GM management and are not discussed here.

After a local HyperSwap to H2, you can resynchronize the remote replication to H3, using the DS8000 MT-PPRC Incremental Resynchronization capabilities. Only data that was changed since the HyperSwap must be replicated.

Note: Starting with CSM 6.2.1, CSM can be configured to restart the replication between the former multi target sites automatically after a HyperSwap. This option is not exposed in the GUI. You must enter a new property to the CSM server properties file:

csm.auto.restart.after.swap=true

See IBM Knowledge Center for CSM *rmserver.properties* file page for details about changing the CSM server properties file:

https://www.ibm.com/support/knowledgecenter/en/SSESK4_6.2.3/com.ibm.storage.csm.help.doc/frg_r_rmserver_properties_file.html

A switch to the remote region (region B) is a DR action, and therefore disruptive. After recovering the GM secondary volumes H3, you can quickly re-establish local HA and DR by synchronizing the Global Copy replication between H3 and H4 to MM.

As long as the infrastructure and replication relations are intact, for example after a planned site switch, you can also quickly re-establish remote DR capability by resynchronizing the GM in the opposite direction, from H3 to H1, and then the cascaded Global Copy from H1 to H2. This finally leads to the topology shown in Figure 7-29.

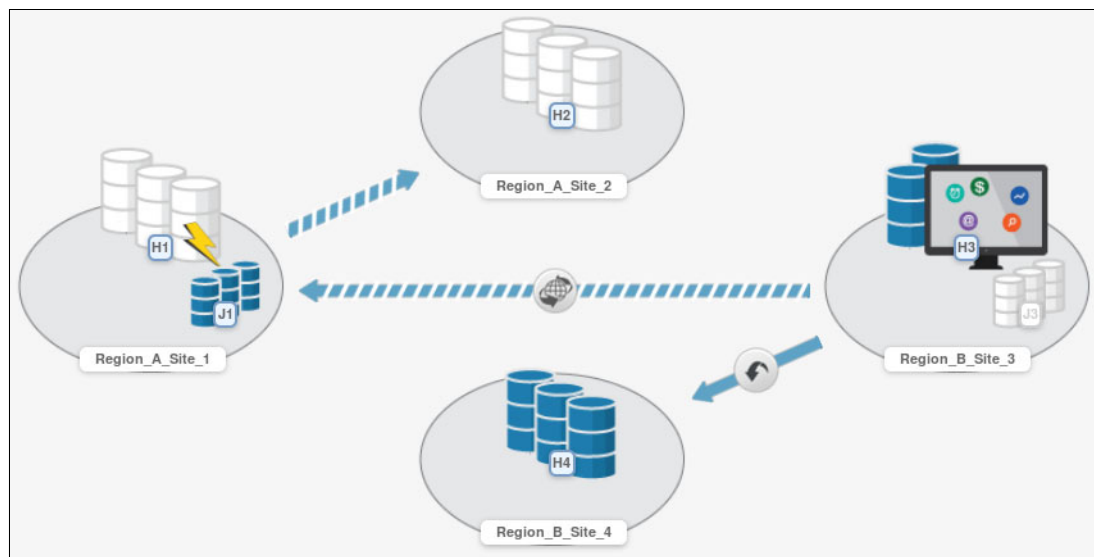


Figure 7-29

7.3.5 HyperSwap management for asymmetrical replication topologies

Starting with version 6.2.0, CSM also supports asymmetrical HyperSwap configurations. This topology can be used, for instance, in three site replication topologies, where HyperSwap should protect all volumes for HA, but only a subset of them must be replicated via GM for DR. CSM does not provide session types with asymmetrical volume configurations, but enables you to merge the HyperSwap configuration of more than one CSM session.

In the previously mentioned situation, you can merge the HyperSwap management of all pairs in a two-site MM session with all MM pairs of second session, for instance a three-site MM - GM or MGM session. The combined MM pairs of both sessions are used to load a common, merged HyperSwap configuration to the associated Sysplex.

To utilize this capability, you associate the same Sysplex to all sessions that you want to merge in a single HyperSwap configuration. Then you define a common *Consistency Group Name* for all affected MM role pairs. You can do that by using the CSM GUI **Actions** → **View/Modify** → **Set Consistency Group Name**. Figure 7-30 shows how to set Consistency Group Names.

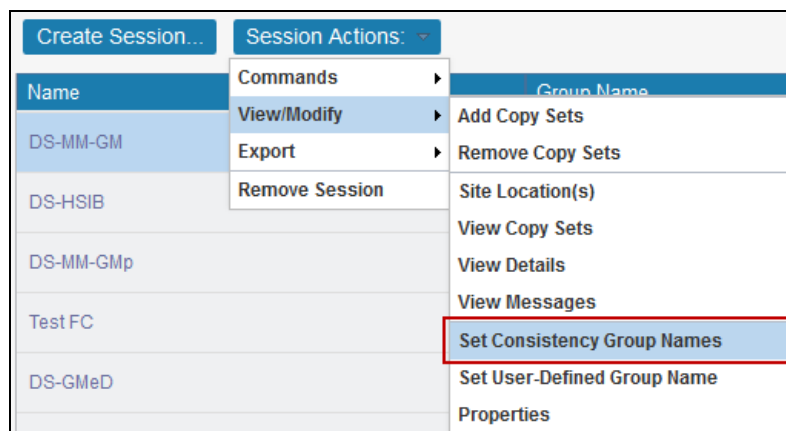


Figure 7-30 Set Consistency Group Names

Figure 7-31 shows how to enter a Consistency Group Name for the H1-H2 role pair.

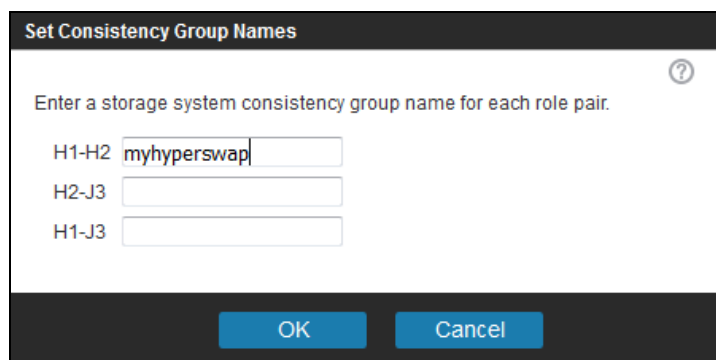


Figure 7-31 Storage System Consistency Group Name

Make sure that you assign the same name to all MM role pairs of the affected sessions that you want to HyperSwap together. When all sessions that should merge the HyperSwap configuration have the same Consistency Group Name and have all their MM pairs in a Prepared state, CSM merges the MM volume pair definition and loads a consolidated HyperSwap configuration.

Note: If more than one role pair uses the same Consistency Group Name, the HyperSwap configuration is not loaded until all pairs assigned with the same Consistency Group Name are in a Prepared state. If one session reaches Prepared first, it displays a warning message indicating that a load has not yet been done because it is waiting for other sessions to reach Prepared. It is assumed that if sessions are grouped together, HyperSwap should be enabled only with the merged configuration.

Figure 7-32 shows two sessions that use a consolidated HyperSwap configuration. You see the defined Consistency Group Names in the session panels.

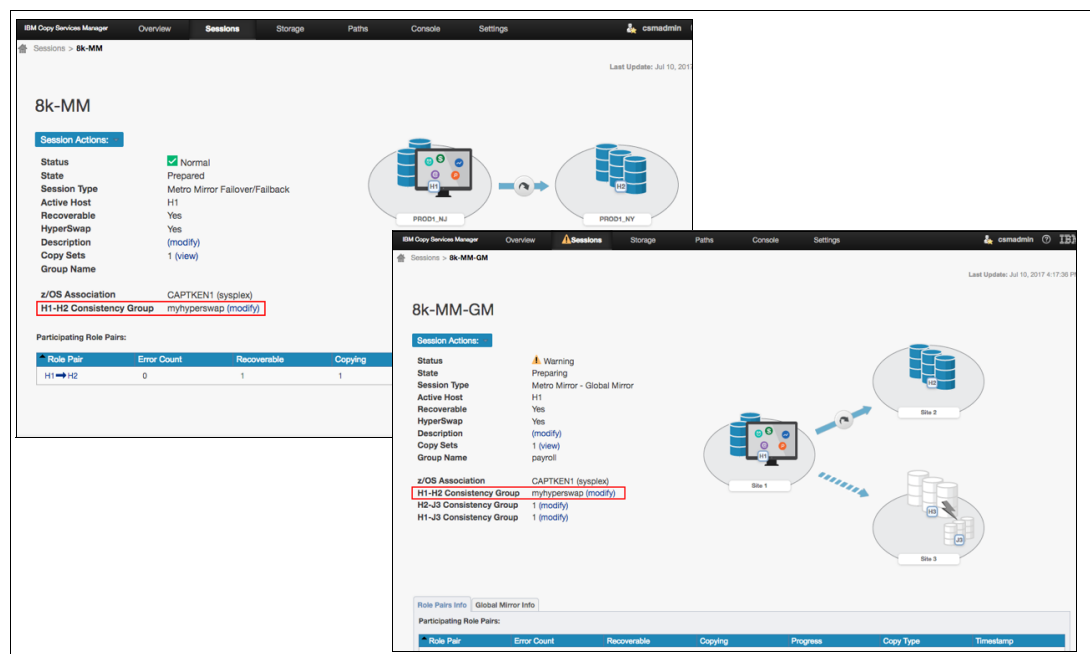



Figure 7-32 Two sessions combined for a common HyperSwap configuration

Note: The *Consistency Group Name* cannot be changed while the session already manages an active HyperSwap or Hardened Freeze configuration.

If a Consistency Group Name is defined, it is used as the z/OS configuration name when loading the HyperSwap or Hardened Freeze configuration. When such a consolidated HyperSwap configuration is active, any HyperSwap event or command will cause all of the shared CSM sessions to HyperSwap.

Note: The *Session Group Name* is a different alias definition than the *Consistency Group Names*. The Session Group Names are simply used to manually group various CSM sessions for simplified filtering on the Session Overview Panel. A session can have only one Session Group Name, but can have different Consistency Group Names (one for each role pair that supports consistency management across multiple CSM sessions).

The Consistency Group Name definition can also be used to define multiple sessions to Freeze their MM pairs consistently. CSM will freeze across all sessions with the same Consistency Group Name before releasing I/O again (Unfreeze) in any of these sessions.



Additional operational considerations

This chapter covers operational considerations, such as monitoring and logging HyperSwap related events, as well as configuring alerts, both in IBM Copy Services Manager (CSM) and z/OS. Then it describes the HyperSwap related z/OS MVS system commands. It also explains different ways to test an HyperSwap configuration, gives guidelines on how to reconfigure storage devices, and finally provides methods to resolve some potential situations that can prevent your HyperSwap configuration from being enabled.

8.1 CSM monitoring, logging and alerting

This section provides an overview of the monitoring, logging, and alerting options of CSM. We show some examples and go into detail only for HyperSwap related items. If you need information about all CSM capabilities, see IBM Knowledge Center or *IBM Copy Services Manager Implementation Guide*, SG24-8375.

8.1.1 CSM monitoring

CSM shows the health status of all components on its dashboard, the page that you see when you log in. It displays a summary of the status for the active sessions, storage connections, host connections and, if configured, CSM server high availability (HA). Figure 8-1 shows an example of the dashboard, with a warning displayed for the Storage Systems connection category.

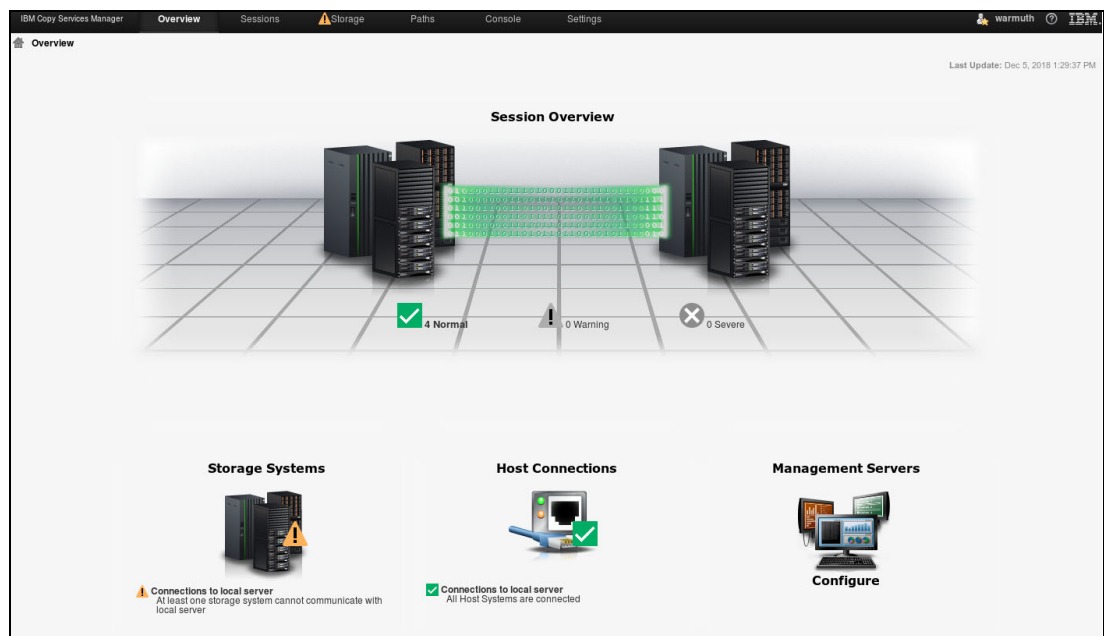


Figure 8-1 CSM dashboard

CSM indicates the health of a certain component or category by small icons, as shown in Table 8-1.

Table 8-1 CSM status icons

Icon	Meaning
✓	Healthy: everything is as expected
⚠	Warning: something is not as expected, but without immediate impact on the protection
✗	Error: something is not as expected with impact on the protection

If there is anything unexpected with any of these components, you can click the affected component's pictogram to get a more detailed view, as shown in Figure 8-2 for the storage connections. In this example, the panel identifies which storage connection is degraded.

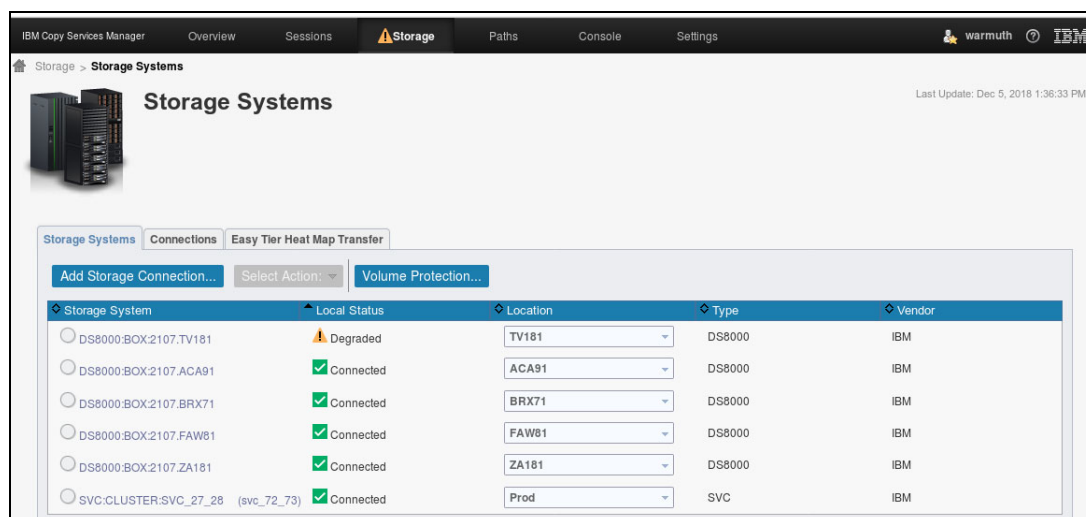


Figure 8-2 CSM list of connected storage systems

You can click the degraded storage connection to get more details about it. Other component overview panels provide similar options.

The CSM sessions overview panel displays the state and health of all defined sessions, as shown in Figure 8-3.

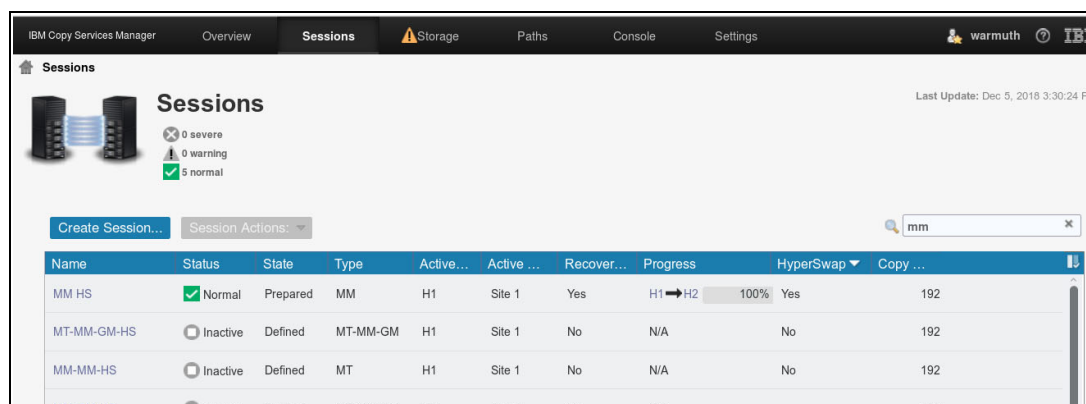


Figure 8-3 CSM Sessions overview

You get a quick overview of the status and state of your sessions. There are columns available to indicate various session aspects:

- ▶ The session type
- ▶ The replication progress
- ▶ The HyperSwap capability and whether the feature is enabled or disabled
- ▶ The Hardened Freeze capability and whether the feature is enabled or disabled

The view is very flexible. You can define the columns you want CSM to show and also filter for patterns in the session names. If you select a session, you get a menu of available session actions to invoke directly. If you click a session name, CSM takes you to the session's main panel.

8.1.2 CSM logging

CSM displays all messages for all active sessions in the CSM console. You can open it by clicking the **Console** button in the CSM main menu. Figure 8-4 shows an example of this log, listing a few HyperSwap related informational messages.

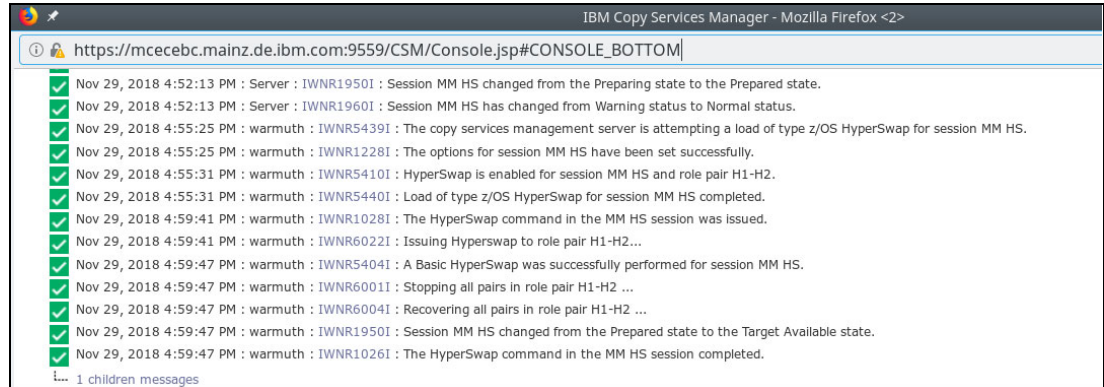


Figure 8-4 The CSM Console

CSM creates console entries for all significant events, including the following examples:

- ▶ Configuration changes
- ▶ Session state changes
- ▶ Session status notifications
- ▶ Communication failures
- ▶ Management-server state changes

The console entries contain message codes that are also hot links to a more detailed description of the entry, including the explanations of error and reason codes that may be provided.

Some entries contain other messages, which are called *Children Messages*. They are related to the parent and usually report events that were leading to the parent message. Figure 8-5 shows an example of a parent and its children messages that were caused by an (artificial) hardware failure.

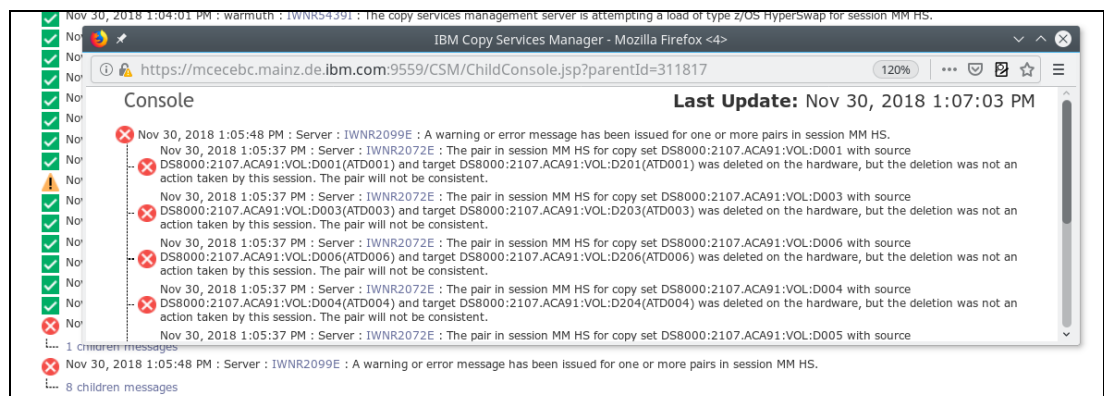


Figure 8-5 CSM console with children messages

Some messages may contain a hardware-related error code, which is also marked as a hot link. To get a more detailed description, click the link to open the code explanation help page in another browser window.

8.1.3 CSM alerting

CSM provides two ways to notify you when problems or unexpected events occur:

- ▶ E-Mail notification
- ▶ SNMP traps

You can enable each of the notification methods individually, or both. You get to the configuration panels by opening the **Settings** menu on the CSM main menu, then clicking **Alert Notification**.

Note: CSM does not trigger a notification for a HyperSwap event itself. However, during a HyperSwap, the session transitions to a different state, which triggers an alert.

Alert filtering is not possible in CSM, and must be implemented on the SNMP trap or e-Mail receiving systems. For more information about CSM alerting, see IBM Knowledge Center for CSM:

https://www.ibm.com/support/knowledgecenter/en/SSESK4_6.2.3/com.ibm.storage.csm.htmlp.doc/csm_r_alerts.html

E-Mail notification

CSM sends E-Mail notifications for the following general events:

- ▶ Session-state change
- ▶ Configuration change
- ▶ Session-status notification
- ▶ Communication failure
- ▶ Management-server state change

SNMP traps

CSM sends SNMP traps for the following general events:

- ▶ Session state change
- ▶ Configuration change
- ▶ Suspending-event notification
- ▶ Communication failure
- ▶ Management Server state change
- ▶ Scheduled Task notification

8.2 Operational considerations for z/OS

This section discusses some operational considerations for the z/OS environment.

8.2.1 z/OS HyperSwap commands

z/OS provides a couple of MVS system commands to display HyperSwap information and perform certain HyperSwap related actions. In the following sections we provide a summary of the available commands and the most common use cases.

Summary of HyperSwap related commands

Table 8-2 on page 160 provides a list and summary of the HyperSwap related commands to query and display HyperSwap related information.

Table 8-2 z/OS HyperSwap related query and display commands

Command	Result
D HS,STATUS	Displays the status of a HyperSwap session. This command also displays any reasons why HyperSwap might be disabled, and the policies for the HyperSwap session.
D HS,CONFIG(DETAIL,ALL)	Displays the most detailed configuration for the HyperSwap session. The volumes and status of all pairs in the HyperSwap configuration are listed. If ALL is omitted, only the first couple of volumes are listed)
F HSIB,D	Displays status of the HSIB address space on the logical partition (LPAR). It also shows which LPAR is running the HyperSwap Master, which logs all detailed HSIB messages.
D M=DEV(nnnnn)	Displays device related configuration information, including whether the device is being monitored by HyperSwap and whether the device has been swapped by HyperSwap.
DS QD,nnnnn	Query actual device information from the storage controller. It will show whether a device is fenced.

Table 8-3 lists the MVS commands to manage HyperSwap:

Table 8-3 z/OS HyperSwap management commands

Command	Result
SETHS SWAP[,NAME(session_name)]	Initiates a planned HyperSwap for the active HyperSwap session.
SETHS DISABLE	Disable HyperSwap by operator command. This command prevents a HyperSwap from occurring, either by command or automatically. The HyperSwap configuration remains loaded.
SETHS ENABLE	Enable HyperSwap by operator command. This command allows a HyperSwap to be performed, either by command or automatically (if a HyperSwap session is not disabled for other reasons).
SETHS RESUMEIO	Resumes normal I/O activity to devices after a suspended HyperSwap or Hardened Freeze action because the Hold I/O after Suspend option was used.
SETHS UNFENCE	Unconditional removal of the Soft Fence condition for all DASD devices.
SETHS UNBLOCK	Unconditional reset of the HyperSwap inhibited by programmatic blocking condition.
SETIOS HYPERSWAP	New SETIOS command option to trigger an unplanned HyperSwap by command via an ENF63 signal.

For a detailed explanation of the **SETHS** command syntax and its parameters, see IBM Knowledge Center for z/OS MVS on the following page:

https://www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.ieag100/iea3g1_Syntax48.htm

Note: The **DISPLAY HS**, the **SETHS**, and the **SETIOS** commands require sufficient command authorization for TSO users that monitor/manage HyperSwap:

- ▶ **SETHS ENABLE/DISABLE/SWAP** requires UPDATE authority to profile MVS.SETHS in the OPERCMDS class.
- ▶ **DISPLAY HS** requires READ authority to profile MVS.DISPLAY.HS in OPERCMDS class.
- ▶ **SETIOS HYPERSWAP** requires UPDATE authority to profile MVS.SETIOS.IOS in the OPERCMDS class.

DISPLAY HS command

You can use the **DISPLAY HS** command to get information about the current HyperSwap configuration. If you use the **CONFIG** option, you get a summary and status information, as shown in Example 8-1.

Example 8-1 DISPLAY HS,CONFIG command output

DISPLAY HS,CONFIG

IOSHM0304I Active Configurations 309

Session Name	Session Type	Priority	Status	Systems Impacted
MM_HS_____H1H2	HyperSwap	1	HyperSwap Ready	0

If you use the **STATUS** option, you get some more detail about the configuration(s) and the settings of the HyperSwap session. Example 8-2 shows an example of the command output.

Example 8-2 DISPLAY HS,STATUS command output

DISPLAY HS,STATUS

IOSHM0303I HyperSwap Status 311

Number of configurations: 1

Replication Session: MM_HS_____H1H2

Socket Port: 5858

HyperSwap enabled

Swap Highest Priority: No

Disallow Non-MultiTarget System: Yes

New member configuration load failed: Disable

Planned swap recovery: Disable

Unplanned swap recovery: Disable

FreezeAll: Yes

Stop: No

See 7.1.3, “HyperSwap configuration settings” on page 132 for an explanation of the settings and a comparison of CSM and z/OS nomenclature.

You can also display the device pairs of a HyperSwap configuration. With the **CONFIG(DETAIL,ALL)** option, you get a list of all device pairs in the configuration. Without the **ALL** parameter, the command only shows a partial list, as shown in Example 8-3.

Example 8-3 DISPLAY HS,CONFIG(DETAIL) command output

DISPLAY HS,CONFIG(DETAIL)

IOSHM0304I HyperSwap Configuration 502

Replication Session: MM_HS_____H1H2

Prim. SSID	UA	DEV#	VOLSER	Sec. SSID	UA	DEV#	Status
D0	AA	0D0AA		D2	AA	0D2AA	

D0	56	0D056		D2	56	0D256
D0	9B	0D09B		D2	9B	0D29B
D0	3B	0D03B		D2	3B	0D23B
D0	00	0D000	ATD000	D2	00	0D200
D0	8A	0D08A		D2	8A	0D28A
...						
D0	34	0D034		D2	34	0D234
D0	6E	0D06E		D2	6E	0D26E
D0	9F	0D09F		D2	9F	0D29F

A0 Device(s) not displayed

With the **CONFIG(EXCEPTION, ALL)** option, you get a list of all device pairs in the configuration with abnormal status. Example 8-4 shows the output for the case that no exception exists.

Example 8-4 DISPLAY HS,CONFIG(EXCEPTION,ALL) command output

```

DISPLAY HS,CONFIG(EXCEPTION)
IOSHM0304I HyperSwap Configuration
Replication Session: MM_HS_____H1H2
All Duplex

```

See z/OS MVS Knowledge Center for a complete description of the **DISPLAY HS** command:

https://www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.ieag100/displayhs.htm

SETHS command

You can use the **SETHS** command to trigger certain HyperSwap related actions.

Enable and disable HyperSwap

If you issue the **SETHS DISABLE** command while a HyperSwap configuration is active, HyperSwap becomes disabled, but the HyperSwap configuration remains loaded. Example 8-5 shows the command and its consequences to the HyperSwap status.

Example 8-5 SETHS DISABLE command

```

SETHS DISABLE
IOSHM0306I HyperSwap disallowed by operator
IOSHM0302I HyperSwap disable request complete

```

```

DISPLAY HS,STATUS
IOSHM0303I HyperSwap Status 549
Number of configurations: 1
Replication Session: MM_HS_____H1H2
Socket Port: 5858
HyperSwap disabled:
  By operator
...

```

CSM also reflects this state in the session configuration panel, as shown in Figure 8-6.

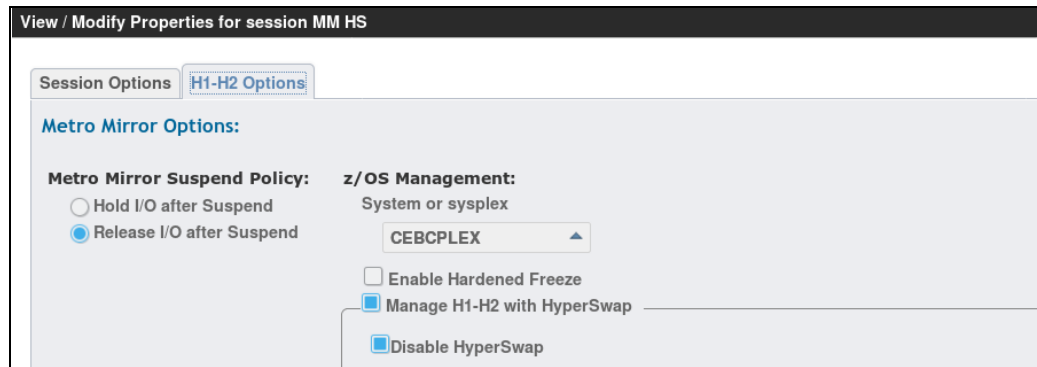


Figure 8-6 HyperSwap disabled after *SETHS DISABLE* command

You can re-enable HyperSwap either by unchecking the *Disable HyperSwap* option in the CSM session properties panel, or by issuing the **SETHS ENABLE** command (Example 8-6).

Example 8-6 SETHS ENABLE command

SETHS ENABLE

```
IOSHM0305I HyperSwap allowed by operator
IOSHM0300I HyperSwap function enabled for all PPRC pairs
IOSHM0302I HyperSwap enable request complete
IOSHM0805I HyperSwap Enabled
```

D HS,STATUS

```
IOSHM0303I HyperSwap Status 595
Number of configurations: 1
Replication Session: MM_HS_____H1H2
Socket Port: 5858
HyperSwap enabled
```

Note: You can also issue **SETHS DISABLE** without active HyperSwap configuration. z/OS then reports that HyperSwap is disabled. However, this is of little consequence, because this state is overridden by a HyperSwap configuration load.

Planned HyperSwap

Using the **SETHS SWAP** command, you can trigger a planned HyperSwap, as shown in Example 8-7.

Example 8-7 Planned HyperSwap with SETHS SWAP

SETHS SWAP

```
IOSHM0400I 15:56:10.37 HyperSwap requested
...
```

We show the full sequence of messages related to a planned HyperSwap in 8.2.4, “HyperSwap sequence logging example” on page 165.

After a HyperSwap, either planned or unplanned, HyperSwap is disabled and no configuration is loaded in z/OS. In order to be protected again, you have to restart the data replication in the reverse direction, and re-enable HyperSwap. You have to do this within CSM. There are no z/OS commands available.

Other SETHS command options

There are a few more options available for the **SETHS** command:

- ▶ **UNFENCE**
- ▶ **RESUMEIO**
- ▶ **UNBLOCK**

These options are mainly used to resolve abnormal situations. Therefore, we describe them with their use cases in 8.5, “Troubleshooting” on page 174.

8.2.2 z/OS messages related to HyperSwap

There are three types of messages in the z/OS system logs that are important in a HyperSwap configuration:

- ▶ HyperSwap messages
- ▶ Messages that are related to the data replication (Metro Mirror (MM))
- ▶ IO error messages that may trigger a HyperSwap

HyperSwap messages are posted whenever a HyperSwap related event occurs. This can be a successful configuration load, a load failure, a HyperSwap itself, planned or unplanned, or a HyperSwap enable or disable event. The HyperSwap messages in the z/OS system log have the following ID convention:

- ▶ **IOSH**: The first four characters indicate that the message comes from HyperSwap subcomponent of Input/Output Supervisor (IOS).
- ▶ The fifth character indicates which of the two address spaces initiated the message.
 - **S**: HyperSwap application programming interface (API) Service address space.
 - **M**: HyperSwap Management address space.
- ▶ **nnnn**: The next four characters are the four-digit message number.
- ▶ The last character is the message type identifier (for example, **I** for informational or **E** for an event).

See IBM Knowledge Center for z/OS for a complete list and more detail about the HyperSwap related messages:

https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.iam900/idg68675.htm

The most relevant replication related and I/O error messages are:

- ▶ **IEA491E** indicates a PPRC (MM) suspend event. This event will cause an unplanned HyperSwap if the error reason is **PRIMARY DEVICE WRITE FAILURE**. For all other error reasons, HyperSwap will be disabled.
- ▶ The following messages always cause an unplanned HyperSwap, if HyperSwap is enabled:
 - **IEA497I**: error on a PPRC primary device after excessive recovery.
 - **IOS107I**: boxed device processing was deferred to allow further recovery.
 - **IOS078I**: I/O operation time out.

Without HyperSwap enabled, errors that would cause an unplanned HyperSwap result in a permanent I/O error.

Other PPRC related messages with no immediate effect on HyperSwap are:

- ▶ IEA498I: One or more paths between peer subsystems are removed or established for any reason other than online execution of Establish Peer-to-Peer Remote Copy Paths order or Remove Peer-to-Peer Remote Copy Paths order.
- ▶ IEA075I: PPRC Summary notification. This message summarizes the PPRC state for all the devices in a control unit.
- ▶ IEA494I: The state of the PPRC pair has changed.

Note: Even if IEA075I or IEA494I are not related to a HyperSwap, they may be logged along a Freeze trigger. If HyperSwap is enabled, the Hardened Freeze sequence may be processed for a consistent split of the MM secondary devices. The HyperSwap configuration will be purged afterwards and your environment is no longer protected for HA or disaster recovery (DR), since replication was stopped.

8.2.3 HyperSwap alerting

In order to get notifications when a Freeze or HyperSwap occurs, you can configure the z/OS alert system to act when the z/OS syslog message displays, as shown in Example 8-8.

Example 8-8 Syslog message indicating the start of a HyperSwap

```
IOSHM0400I <timestamp> HyperSwap requested
```

8.2.4 HyperSwap sequence logging example

As discussed in 1.3.4, “HyperSwap sequence” on page 11, a HyperSwap sequence consists of multiple steps, called phases. Example 8-9 shows a z/OS console log extract from a planned HyperSwap sequence as it appears on the LPAR which acts as the HyperSwap master. To make the example readable, we removed repeated status messages from the individual LPARs.

Example 8-9 HyperSwap sequence logging example

```
13:10:34.32 IOSHM0400I 13:10:34.32 HyperSwap requested
13:10:34.33 IOSHM0401I 13:10:34.33 Planned HyperSwap started - UserExit 226
                                Configuration: MM_HS_____H1H2
13:10:34.33 IOSHM0402I 13:10:34.33 HyperSwap phase - Validation of I/O
connectivity starting
13:10:34.37 IOSHM0403I 13:10:34.37 HyperSwap phase - Validation of I/O
connectivity completed
13:10:34.37 IOSHM0404I 13:10:34.37 HyperSwap phase - Freeze and quiesce DASD I/O
starting
13:10:34.39 IEA075I PPRC SUMMARY,SSID=D201, 241
DEVICE NED=2107.980.IBM.75.0000000ACA91.D200,
SECSSID=D001(D0B1 P000 S00F),
SUSPENDED=00F,PPRC=0C0,TOTAL=0C0,
REASON=SUSPEND(0A),FREEZE
13:10:34.40 IOSHM0405I 13:10:34.40 HyperSwap phase - Freeze and quiesce DASD I/O
completed
13:10:34.40 IOSHM0406I 13:10:34.40 HyperSwap phase - Failover PPRC volumes
starting 13:10:34.41 IEA075I PPRC SUMMARY,SSID=D201, 249
DEVICE NED=2107.980.IBM.75.0000000ACA91.D20F,
SECSSID=D001(D000 P000 S0C0),
```

```

SUSPENDED=OC0,PPRC=OC0,TOTAL=OC0,
REASON=SUSPEND(OA),FREEZE
13:10:34.53 IOSHM0407I 13:10:34.53 HyperSwap phase - Failover PPRC volumes
completed
13:10:34.53 IOSHM0408I 13:10:34.53 HyperSwap phase - Swap UCBs starting
13:10:34.55 IOSHM0409I 13:10:34.55 HyperSwap phase - Swap UCBs completed
13:10:34.55 IOSHM0410I 13:10:34.55 HyperSwap phase - Resume DASD I/O starting
13:10:34.67 IOSHM0411I 13:10:34.67 HyperSwap phase - Resume DASD I/O completed
13:10:34.67 IOSHM0433I 13:10:34.67 HyperSwap phase - Soft Fence starting
13:10:34.77 IOSHM0434I 13:10:34.77 HyperSwap phase - Soft Fence completed
13:10:34.79 IOSHM0429I 13:10:34.79 HyperSwap processing issued an UnFreeze
13:10:34.79 IOSHM0412I 13:10:34.79 HyperSwap phase - Cleanup starting
13:10:36.69 IOSHM0413I 13:10:36.69 HyperSwap phase - Cleanup completed
13:10:36.69 IOSHM0414I 13:10:36.69 Planned HyperSwap completed
13:10:36.69 IOSHM0809I HyperSwap Configuration Monitoring stopped
13:10:36.72 *IOSHM0803E HyperSwap enabled with limited capability
13:10:36.72 *IOSHM0803E HyperSwap Disabled
13:10:36.73 IOSHM0200I HyperSwap Configuration Purge complete

```

Note: Example 8-9 on page 165 also shows that the PPRCSUM feature is activated, which logs only a single IEA075I PPRC summary message per logical control unit (LCU) rather than an individual IEA494I message per device.

You can determine the impact on the host I/O by subtracting the timestamp of the start of *Freeze and quiesce DASD I/O* phase from that of the end of *Resume DASD I/O* phase, as illustrated in Example 8-10. The HyperSwap configuration used here contains 192 devices in a single LCU. The impact on host I/O operations was 0.3 seconds.

Example 8-10 Determine I/O impact of a planned HyperSwap

```

13:10:34.37 IOSHM0404I 13:10:34.37 HyperSwap phase - Freeze and quiesce DASD I/O
starting
...
13:10:34.67 IOSHM0411I 13:10:34.67 HyperSwap phase - Resume DASD I/O completed

```

Note: I/O impact times vary depending on the size of the configuration and the storage controller performance for processing the Freeze operation. For an unplanned HyperSwap, you also have to add potential I/O impact time while z/OS or PPRC are trying to recover I/O errors until a real I/O or path error is declared for a device, which finally triggers the unplanned HyperSwap sequence. To reduce z/OS I/O recovery times, see 6.2.7, “Reduce delays of HyperSwap triggers” on page 107.

8.2.5 HyperSwap failures

HyperSwap processing prevents a HyperSwap from occurring if certain conditions are not satisfied prior to beginning of the swap. HyperSwap only initiates a swap if it can expect that the swap will complete successfully. If there are problems beforehand that it cannot handle, HyperSwap tries not to make the situation worse by performing a swap that cannot succeed.

If a failure occurs part way through a HyperSwap operation, and one or more systems in the Sysplex cannot complete the swap, subsequent actions depend on when and where the failure occurred, and what the settings for the HyperSwap session are:

- ▶ If the swap policy is set to **Disable** HyperSwap, which is the default for planned HyperSwaps, HyperSwap backs out of the operation. Afterwards, the situation will be as if HyperSwap had not been available. You have to perform manual recovery for the problem that caused the HyperSwap attempt, in order to continue normal operations.
- ▶ If the swap policy is set to **Partition** out the failing systems, which is the default for unplanned HyperSwaps, the LPARs that cannot swap are partitioned out of the Sysplex, and the swap continues on the LPARs that are able to proceed. You have to IPL the LPARs that were partitioned out on the site the Sysplex was swapped to.

In both cases, you have to analyze the reason that caused the HyperSwap failure, in order to re-enable HyperSwap and avoid such a situation in the future. Involve IBM support to help analyze and address the issue.

8.3 Testing unplanned HyperSwap

A good practice is to establish a small test environment and thoroughly test your HyperSwap setup before deploying the feature on your production systems. A test environment enables you to exercise all of your parameters and operational procedures and to become familiar with the HyperSwap behavior.

After you have set up HyperSwap on your production systems, always test HyperSwap there too, to make sure that it works the way you expect it. Test environments usually do not have the size and complexity of production environments, and sometimes there are important attributes of the production environment that have not been exposed there. This way, you can find and fix any problems before you need HyperSwap in a real recovery situation.

You can perform planned HyperSwap testing through one of the following options:

- ▶ Issue **HyperSwap Hx-Hy** command to the CSM session, as described in 7.2.3, “Planned HyperSwap” on page 139.
- ▶ Issue the z/OS MVS command **SETHS SWAP**, as described in 8.2.1, “z/OS HyperSwap commands” on page 159.

Unplanned HyperSwap testing that is based on a HyperSwap trigger, for example an ENF63 signal, requires an I/O error to a managed primary device. This can be accomplished by using one of the following methods:

- ▶ Physically disturb the FICON communication paths to a managed hardware device, for example by disabling switch ports, unplugging FICON cables, or even switching off storage or connection devices.
- ▶ Logically disable the communication to a device, for example by forcing paths or devices to be varied offline. We explain this method in “Forcing an IO error to trigger an unplanned HyperSwap” on page 168.
- ▶ With z/OS new functions APAR OA53082, a command was introduced to trigger an unplanned HyperSwap. See “z/OS initiated unplanned HyperSwap” on page 168 for details.

In general, you must prepare unplanned HyperSwap tests carefully. Make sure that you do not affect resources other than those that are supposed to be part of the test.

Physical error injection can be difficult in shared environments, where only a subset of resources can be used for the test. Logical path or device error injection might be more suitable for testing in such environments. However, it usually leads to boxed devices, which you must recover before you can return your setup to normal operation. See “Resolving fenced devices” on page 177.

8.3.1 z/OS initiated unplanned HyperSwap

z/OS new functions APAR OA53082 introduced a method to force an unplanned HyperSwap through an ENF63 signal by command. The following link takes you to the description of this APAR:

<https://www-01.ibm.com/support/docview.wss?rs=63&uid=isg1OA53082>

Note: Besides the support for triggering an unplanned HyperSwap by command, the APAR is also required to support the new HyperSwap load options that were introduced with CSM version 6.2.2, which we describe in 7.1.3, “HyperSwap configuration settings” on page 132.

You can use the **SETIOS HYPERSWAP** command option to request an unplanned HyperSwap without altering the current state of any HyperSwap managed device. As such, it helps to prevent boxed devices in unplanned HyperSwap test scenarios. Example 8-11 shows the messages z/OS logs if you trigger an unplanned HyperSwap by command.

Example 8-11 Unplanned HyperSwap triggered with SETIOS HYPERSWAP command

```
13:07:33.36 WARMUTH 00000280 SETIOS HYPERSWAP
13:07:33.38          00000080 IOS060I SETIOS HYPERSWAP COMMAND ACCEPTED
13:07:33.39 STC04920 00000080 IOSHM0400I 13:07:33.39 HyperSwap requested
...
```

Note: The unplanned HyperSwap occurs asynchronously to the completion of the command as long as there is a HyperSwap Manager active, such as GDPS or z/OS HyperSwap.

8.3.2 Forcing an IO error to trigger an unplanned HyperSwap

You can force a PPRC primary device offline, even if it is in use by the system, to trigger an unplanned HyperSwap. To that goal, you have to use the MVS system command **VARY** with the **FORCE** option. You also have to confirm this action by replying to a WTOR. The test will result in a boxed condition on the old primary device that you must remove later to return to normal operation. Example 8-12 shows the log entries for such a test action.

Example 8-12 Unplanned HyperSwap with VARY OFFLINE FORCE

```
18:23:40.20 WARMUTH 00000280 VARY D000,OFFLINE,FORCE
18:23:40.21          00000080 *13 IEE800D CONFIRM VARY FORCE FOR D000 - REPLY NO
OR YES
18:23:59.25 WARMUTH 00000280 REPLY 13,YES
18:23:59.25 WARMUTH 00000080 IEE600I REPLY TO 13 IS;YES
18:23:59.25 WARMUTH 00000080 IEE846I D000 PENDING OFFLINE AND PENDING BOXED
18:23:59.25          00000090 IOS107I DEVICE D000 BOX PROCESSING DEFERRED
18:23:59.26 STC04920 00000080 IOSHM0400I 18:23:59.26 HyperSwap requested
...
```

If you have a dedicated storage system available for testing, you can also test the loss of all connections to the device or even loss of the complete device. You can trigger a no paths condition by configuring all channel paths (CHPs) to the device offline to z/OS. For the last CHP you have to use the **FORCE** option.

As a consequence of forcing paths or devices offline to trigger an unplanned HyperSwap, the affected devices (primaries before the HyperSwap) will be placed in a Boxed state by the operating system. If you want to restart mirroring, these boxed devices will become MM secondaries, and MM cannot write to a device as long as it is boxed. Also, a HyperSwap configuration load test will fail on an LPAR, if any secondary devices are offline but boxed or marked as being Used by a system (UCBNALOC is on).

You have to remove the boxed state before you can restart the CSM session and reactivate HyperSwap. Without unboxing, the CSM command to start the replication will fail. See 8.5.1, “Recovering boxed devices” on page 174 for more detail on boxed devices and ways to recover the situation. You can also refer to this IBM Knowledge Base document for help with unplanned HyperSwap testing and cleanup of boxed devices:

<https://www-01.ibm.com/support/docview.wss?uid=isg1II14654>

8.4 Reconfigure replicated Count Key Data storage devices

In this section, we provide general guidelines for various reconfiguration tasks of replicated storage devices. Some of the listed steps may be optional for a specific reconfiguration task, but should be considered when performing the corresponding reconfiguration.

8.4.1 Relabel existing replication devices

Relabeling a device might be required if you free up a volume and want to relabel it as a spare volume without removing it from the replication environment. Alternatively, you might want to relabel a replicated spare device to a new VOLSER for application use. Relabeling can be performed with the **ICKDSF** program using the **INIT** command. For more details, see the *Device Support Facilities (ICKDSF) User's Guide and Reference, INIT command*:

https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.ickug00/ick40239.htm

Device relabeling does not require you to stop replication because it will only change the logical content (VTOC) of the device, which is replicated to the secondary device peer. The VOLSER label will be shown in CSM as device username for Count Key Data (CKD) volumes.

Note: VOLSER label changes may take some time until they are refreshed in various CSM GUI panels, since most of the panels use local browser cache that is updated asynchronously from the CSM server.

Before relabeling a device with a new VOLSER, it is good practice to take the primary device offline on all LPARs. Otherwise, the VOLSER label change is not recognized automatically by the LPARs that have the device still online. To avoid stale VOLSER information, the **ICKDSF INIT** program by default verifies that the device is offline to other systems, if this feature is supported by the storage system firmware prior performing the command.

For more details, see *Device Support Facilities (ICKDSF) User's Guide and Reference*, **INIT** command, **VERIFYOFFLINE** parameter:

https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.ickug00/verifyoff.htm

The following steps should be considered when you relabel replicated devices.

- ▶ Vary primary device offline on all LPARs
This action will ensure that there are no LPARs with stale VOLSER label information after the device was re-initialized with a new label.
- ▶ Re-initialize the primary device with new label
Use the **ICKDSF** program with the **INIT** command to re-initialize the device with a new label if the device content must also be cleaned up. The **INIT** command will also ensure that the allocated tracks of the device are released. If it is a space efficient device, it will also ensure that the allocated extends on the storage system will be released for this device. Depending on the DS8000 firmware, this space release will also be replicated for MM as well as Global Mirror (GM) relations.
- ▶ Vary primary device online on all required LPARs
This action will enable use of the relabeled device and ensure each LPAR has updated VOLSER label information.

Note: There is another command option for the **ICKDSF**: The **REFORMAT** command supports relabeling only a device. It will not change any other data on the device and requires that the device is online.

8.4.2 Create new replication devices

Consider the following steps when creating new storage devices in your managed replication environment.

- ▶ Create new base devices on storage systems.
This is required on each storage system that will participate in the replication of the new devices. The created base devices for a replication pair must be of same type and size.
- ▶ Create new alias devices on storage systems.
This is only necessary, if your alias device (PAV) configuration must be adapted on the logical control unit (LCU or LSS) which holds the new devices. For performance reasons, the alias device configuration on each storage system should be symmetrical for the replicated LCUs. If the used LCUs have already sufficient alias devices configured and HyperPAV or SuperPAV is in use, this step is not required.
- ▶ Update the z/OS I/O configuration of all LPARs to access the new devices.
This is required if the existing I/O configuration of the LPARs does not yet include the Unit Control Block (UCB) ranges with the new base and alias devices. Changes can usually be processed dynamically. Verify that you have logical and physical path definitions in place for the new devices. The MVS commands **DEVSERV QDASD,dddd** and the **DEVSERV PATH,dddd** can be used to query actual device and path status for the new devices.
- ▶ Verify that CSM recognized the new storage devices.
You can review the volume information of each storage system in CSM. Usually device changes on DS8000 storage systems trigger CSM to refresh the storage configuration automatically if CSM is connected to the DS8000 Hardware Management Console (HMC).

However, if CSM is only connected via a z/OS FICON connection, this automatic refresh will not be triggered. CSM refreshes a storage configuration at an hourly interval. If the new devices have not been recognized yet by CSM, you can also trigger a manual storage system configuration refresh in CSM.

Note: Alias devices are not listed in the CSM volume information because they cannot be used for any kind of Copy Services.

► Add new storage devices to your CSM session:

- Adding devices to a new or inactive CSM session.

You can create a new CSM session, add new copy sets with the new devices, and start the replication of the session afterwards with a corresponding **Start** command. This option may require specific consideration when a role pair of the inactive session is initially enabled for HyperSwap or Hardened Freeze management. In that case, CSM will perform an initial load test to the HyperSwap Manager prior starting the replication.

This test will fail if not at least one device is online on each LPAR. Because it is good practice to establish the replication prior to starting potential work on new devices, HyperSwap or Hardened Freeze management can be temporarily removed from the Session prior initial start, and added back later on once the devices are initialized and online to the LPAR(s).

- Adding devices to an active CSM session.

When the session is already active while you add the copy sets with the new devices, there are several steps processed by CSM during this task. CSM will ensure to minimize the impact on the active consistency group used by the session while adding devices. The synchronization of added devices is processed first, before they are afterwards added to the consistency group.

Therefore, the session will change from a Prepared state into a Preparing state while the synchronization is being processed. For HyperSwap or Hardened Freeze managed MM role pairs, the new devices will be added to the HyperSwap/Hardened Freeze configuration just after they have all reached a Prepared state (Full Duplex on DS8000). CSM will process a purge of the active HyperSwap/Hardened Freeze configuration and reload a new configuration to the HyperSwap Manager, including the added devices.

For GM role pairs, the new devices will be added to the GM Master session after they have processed their Global Copy first pass completion. This process will minimize the RPO impact until the GM Master can form the next consistency group including the added devices.

► Initialize the new devices.

You need to initialize the new devices with a VOLSER label before you can take them online on any LPAR. This is usually performed with the **ICKDSF** program using the **INIT** command. For more details please refer to the *Device Support Facilities (ICKDSF) User's Guide and Reference, INIT command*:

https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.ickug00/ick40239.htm

The CKD VOLSER label will be shown in CSM as device username.

Note: VOLSER label changes can take some time until they are refreshed in various CSM GUI panels, because most of the panels use local browser cache, which is updated asynchronously from the CSM server.

- Vary the devices online.

When the desired replication state is reached, and the new devices are participating in the CSM session consistency group (session is *Prepared*), you can vary the new devices online where needed and start using them.

8.4.3 Delete existing replication devices

The following steps should be considered when deleting storage devices from your managed replication environment. This can go as far as deleting the base device from the storage system and freeing up the UCBs on the LPARs of the managed Sysplex.

- Vary the devices offline on all LPARs.

This step is required if you reinitialize or delete the devices from the storage system completely. It can be skipped if you still use the devices in your LPARs and only remove them from the replication configuration.

- Remove devices from active CSM session by removing copy sets from the active session.

CSM will process the necessary tasks to remove the volumes from the active consistency group mechanism. For HyperSwap or Hardened Freeze managed role pairs, it will purge the active configuration in HyperSwap Manager. For GM managed role pairs, it will pause the GM Master session and remove the volumes from the GM Master configuration. Then, it will terminate all replication relationships for the removed copy sets. After that is completed, the active consistency group mechanism will be restarted.

For HyperSwap/Hardened Freeze managed role pairs, it will reload the new configuration to the HyperSwap Manager. For GM role pairs, the GM Master session will be restarted to continue forming consistency groups. All devices of the removed copy sets will be in a SIMPLEX state on the DS8000.

Note: If there are multiple copy sets to be removed, it is good practice to use the GUI. It allows to remove multiple copy sets at once from the active consistency group used by the session. Using the GUI is faster and with less impact to the active consistency group than using the CSMCLI command `rmcpset`.

- Delete base devices on storage systems.

If you do not plan to reuse the simplex devices as spare devices, you may want to delete the base devices completely. Before you delete a base device, you need to check if the base device was configured with alias devices on the DS8000 storage system. Although all alias devices can be dynamically used for any base device in the LCU with the HyperPAV feature, the DS8000 associates each alias device to a single base device. Often, alias devices are associated with the first base device in the LCU, but the association can also be distributed across multiple base devices.

Attention: If you delete a base device from a DS8000, all associated alias devices are deleted with it. If that is the case, recreate alias devices that you still need in the LCU and associate them to another base device.

- Update the z/OS I/O configuration of all LPARs to remove the old devices.

Update your z/OS I/O configuration if you want to free up the UCB addresses of the removed device. If the configured UCBs will be reused by new devices from the same storage control unit, this step is not required.

8.4.4 Resize existing replication devices

The DS8000 supports dynamic volume resizing, but only for devices in SIMPLEX state. Therefore, you have to terminate replication for the affected volumes, resize all volumes that make up the copy sets, and finally restart replication. Additionally, you might also have to refresh the device configuration in z/OS IOS and logically expand the VTOC on the devices to allow z/OS to use the additional capacity.

The following steps should be considered when you want to resize replicated devices:

- Vary primary devices offline (optional).

The primary devices can be dynamically resized even if they remain online and in use by z/OS LPARs. However, because replication must be terminated for the resize process, it may cause a HA and/or DR capability impact if the primary devices remain in use. To avoid this, it is good practice to stop using the primary devices to be resized. This can be ensured by taking them offline on all LPARs.

- Terminate replication for devices to be resized.

This task is processed by removing copy sets from the active CSM session.

CSM will process the necessary tasks to remove the volumes from the active consistency group mechanism. For HyperSwap or Hardened Freeze managed role pairs, it will purge the active configuration in HyperSwap Manager. For GM managed role pairs, it will pause the GM Master session and remove the volumes from the GM Master configuration. Then, it will terminate all replication relationships for the removed copy sets.

When that is completed, the active consistency group mechanism will be restarted. For HyperSwap/Hardened Freeze managed role pairs, it will reload the new configuration to the HyperSwap Manager. For GM role pairs, the GM Master session will be restarted to continue forming consistency groups. All devices of the removed copy sets will be in a SIMPLEX state on the DS8000.

Note: If there are multiple copy sets to be removed, it is good practice to use the GUI. It enables you to remove multiple copy sets at once from the active consistency group used by the session. Using the GUI is faster and with less impact to the active consistency group than using the CSMCLI command **rmcpset**.

- Resize the CKD volumes on the DS8000 storage systems

You can expand existing CKD volumes in SIMPLEX state via the DS8000 Storage System GUI or the DSCLI command **chckdvol**. For detailed use of the command, refer to IBM Knowledge Center for DS8880 page *chckdvol*:

https://www.ibm.com/support/knowledgecenter/ST5GLJ_8.5.1/com.ibm.storage.ssic.help.doc/f2c_clchckdvol_1kyvr8.html

After the change, all volumes of a copy set must again be of the same type and size.

Note: The DS8000 storage system does not support the function to reduce the capacity of a volume.

- Verify that CSM recognized the storage device changes.

You can review the volume information of each storage system in CSM. Usually device changes in DS8000 storage systems trigger CSM to refresh the storage configuration automatically if CSM is connected to the DS8000 HMC. However, if CSM is only connected via a z/OS FICON connection, this automatic refresh will not be triggered.

CSM refreshes a storage configuration at an hourly interval. If the changed devices have not been recognized yet by CSM, you can also trigger a manual storage system configuration refresh in CSM.

- Adding devices back into active CSM session.

Add the copy sets back into the CSM session after CSM recognized the device changes on all affected storage systems. CSM will minimize the impact to the active consistency group used by the session while adding the changed devices. The synchronization of added devices is processed, before they are added to the consistency group.

Therefore, the session will change from a *Prepared* state into a *Preparing* state while the synchronization is processed. For HyperSwap or Hardened Freeze managed MM role pairs, the new devices will be added to the HyperSwap/Hardened Freeze configuration just after they have all reached a *Prepared* state (Full Duplex on DS8000). CSM will process a purge of the active HyperSwap/Hardened Freeze configuration and reload a new configuration to the HyperSwap Manager including the added devices.

For GM role pairs, the new devices will be added to the GM Master session after they have processed their Global Copy first pass completion. This process minimizes the RPO impact until the GM Master can form the next consistency group including the added devices.

- Reformat VTOC information for changed primary devices.

This may be required to allow z/OS to use the additional capacity of the expanded devices. In order to use the **ICKDSF** program with the **REFORMAT** command, the device must be varied online to one LPAR first. Use the **REFORMAT** parameter **REFVTOC** to rebuild the VTOC in its current location, using the same track size. For more details on the **REFVTOC** parameter, see the *Device Support Facilities (ICKDSF) User's Guide and Reference*, **REFORMAT** command:

https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.ickug00/ick40560.htm

- Vary primary devices with updated VTOC online on other LPARs,

This will ensure that each LPAR using the devices has the actual VTOC and device information. LPARs which keep the changed devices offline can also be refreshed with the changed device information. The MVS command **MODIFY ANTAS000,REDISCOVER** will trigger an offline device discovery through the System Data Mover (SDM) and update the IOS device tables with latest device information found on the storage controller.

8.5 Troubleshooting

In this section, we explain some issues that can occur and prevent you from enabling HyperSwap, together with methods to correct the situation. We conclude with instructions to generate support data if you have to involve IBM support to resolve an issue.

8.5.1 Recovering boxed devices

There may be situations where a swap has been performed successfully, but errors occurred that must be cleared manually. The most common of these situations is that of a Boxed old primary device, as a consequence of the I/O error that initially led to the HyperSwap.

Messages in the z/OS system log, such as the one shown in Example 8-13, indicate that devices have been boxed. The message ID defines the reason for z/OS to place the device in boxed status.

Example 8-13 Syslog message for a boxed device

```
IOS451I devn, BOXED, NO ONLINE OPERATIONAL PATHS
```

After resolving the problem that led to the HyperSwap itself, you also have to clear the boxed state. The boxed device (primary before the HyperSwap) is now becoming a MM secondary, and MM cannot write to device as long as it is boxed. Also, a HyperSwap configuration load test will fail on an LPAR, if any secondary devices are offline but *boxed* or marked as being *Used by a system* (UCBNALOC is on). Without unboxing, the CSM command to start the replication will fail.

Note: Boxed devices are a typical result of triggering an unplanned HyperSwap artificially using a z/OS **VARY OFFLINE, FORCE** command.

You can use the **DISPLAY U** or **DISPLAY M=DEV** commands to determine if any and which devices in your configuration are boxed, as shown in Example 8-14.

Example 8-14 Determine boxed devices

```
19:21:35.47 WARMUTH 00000280 DISPLAY U,,D000
19:21:35.48 WARMUTH 00000080 IEE457I 19.21.35 UNIT STATUS 579
                    579 00000080 UNIT TYPE STATUS          VOLSER      VOLSTATE      SS
                    579 00000080 D000 3390 F-BOX                      /RSDNT      0
                    579 00000080 D001 3390 OFFLINE                      /RSDNT      0
...

19:23:14.41 WARMUTH 00000280 DISPLAY M=DEV(D000)
19:23:14.42 WARMUTH 00000090 IEE174I 19.23.14 DISPLAY M 581
                    581 00000090 DEVICE OD000 STATUS=DEVICE IS BOXED: RESIDUAL..
                    581 00000090 CHP                      9C  A6  AE  AF
                    581 00000090 ENTRY LINK ADDRESS    00  00  08  08
                    581 00000090 DEST LINK ADDRESS    01  01  09  09
                    581 00000090 PATH ONLINE          Y   Y   Y   Y
                    581 00000090 PATH OPERATIONAL      Y   Y   Y   Y
                    581 00000090 MANAGED               N   N   N   N
                    581 00000090 CU NUMBER             D001 D001 D001 D001
                    581 00000090 INTERFACE ID          0240 0242 0312 0310
                    581 00000090 MAXIMUM MANAGED CHPID(S) ALLOWED: 0
                    581 00000090 DESTINATION CU LOGICAL ADDRESS = D0
...

```

CSM version 6.2.2 and later have the capability built in to perform the unboxing during the load operation.

You can use the **Unbox Secondary Volumes** option in the session properties panel when you restart the session after the unplanned HyperSwap, as shown in Figure 8-7.

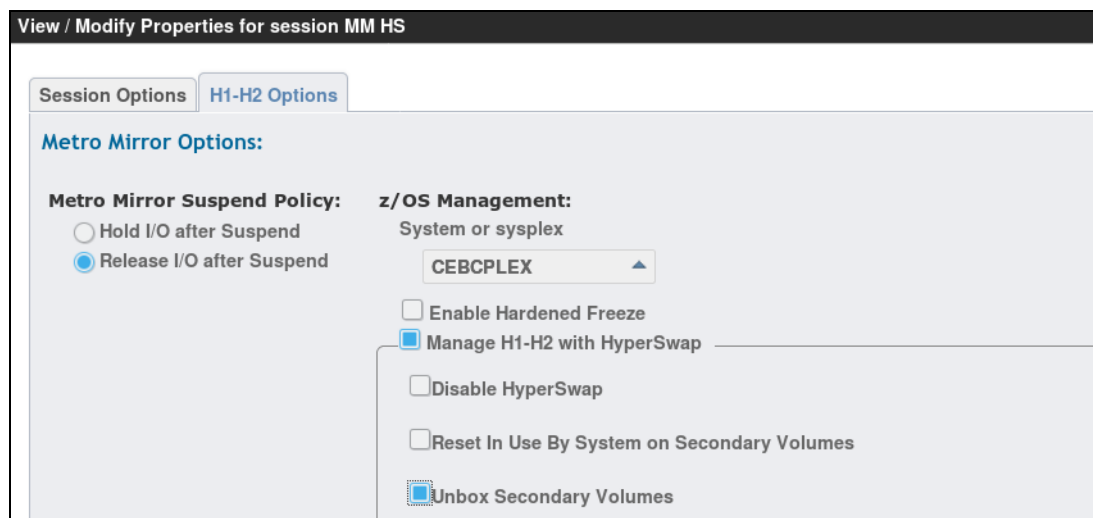


Figure 8-7 CSM option to unbox secondary volumes

See 7.1.3, “HyperSwap configuration settings” on page 132 for a more detailed explanation of the HyperSwap options.

Note: z/OS APAR OA53082 must be applied to all LPARs in the HyperSwap managed Sysplex to use the **Unbox Secondary Volumes** option.

If this feature is not available in your environment, or did not work as expected, you can use manual methods to remove the boxed status. See this Knowledge Base document for help with unplanned HyperSwap testing and cleanup of boxed devices:

<https://www-01.ibm.com/support/docview.wss?uid=isg1II14654>

After unboxing a former primary device, it may happen that the DS8000 storage still has the volume in a grouped state from the time when the volume was boxed. A volume in a grouped state indicates that the volume is potentially online on an LPAR. If your CSM session has the property enabled to *Fail MM/GC if target is online (CKD only)*, a start of the session may fail on the pairs with hardware error code 0F60 as shown in following error message:

```
Message: IWNR2108E: A command was run for the pair in session session_name that
resulted in a hardware error for copy set copy_set_id with source source_volume
and target target_volume in role pair role_pair. The hardware returned an error
code of 0f60.
```

x0F60 error code explanation:

The secondary volume for an establish PPRC pair command or the target volume for an establish FlashCopy command is in a grouped state which implies the volume is on-line to a host.

If you get this hardware error code for a pair, verify that the affected devices which will become the new secondaries are no longer online to any LPAR in the Sysplex. If they are offline but still report to be in a grouped state, you can temporarily disable the session property *Fail MM/GC if target is online (CKD only)* and restart the session again. The DS8000 storage controller will then ignore the grouped state and the copy relation will be resynchronized.

8.5.2 Resolving fenced devices

HyperSwap uses a Soft Fence to protect old primary devices from further I/O after a HyperSwap, to prevent data integrity exposures:

- ▶ If a device is shared with LPARs external to the Sysplex where the HyperSwap occurred
- ▶ If an IPL occurs after a HyperSwap on a LPAR within the Sysplex, but the LPAR has primary and secondary devices defined as ONLINE

If a device is soft fenced, the DS8000 does not allow any further I/O to the device, nor can it become a secondary PPRC device. A Soft Fence is usually cleared by CSM once the replication is started again, or when the CSM session is terminated completely to avoid leftover fenced devices.

Note: The DS8000 supports the Soft Fence function since the following firmware levels:

- ▶ DS8800 - R6.3 SP6 Bundle 86.31.95.0 LMC 7.6.31.1150
- ▶ DS8700 - R6.3 SP6 Bundle 76.31.79.0 LMC 6.6.31.670
- ▶ DS8870 - R7.1.7 bundle 87.10.133.0 LMC 7.7.10.354

Verify Soft Fence state

There are various methods to verify if a device is fenced. In z/OS, you can use the **DEVSERV QDASD** and the **DEVSERV PATH** commands. Example 8-15 shows the output of a **DEVSERV QDASD**. The value **SOF** indicates that the device is in a soft fenced state.

Example 8-15 DEVSERV QDASD command output

DEVSERV QDASD,D200

```
IEE459I 16.19.55 DEVSERV QDASD 366
UNIT VOLSER SCUTYPE DEVTYPE      CYL  SSID SCU-SERIAL DEV-SERIAL EFC
OD200 ----- 2107980 2107900      1113 D201 0175-ACA91 0175-ACA91 SOF
****          1 DEVICE(S) MET THE SELECTION CRITERIA
****          1 DEVICE(S) FAILED EXTENDED FUNCTION CHECKING
```

Example 8-16 shows the output of a **DEVSERV PATH** command. Here the Soft Fence state is indicated literally.

Example 8-16 DEVSERV PATH command output

DEVSERV PATH,D200

```
IEE459I 16.22.02 DEVSERV PATHS 368
UNIT DTYPE MD CNT VOLSER CHPID=PATH STATUS
      RTYPE SSID CFW TC  DFW PIN DC-STATE CCA DDC      CYL CU-TYPE
OD200,33903 ,F ,000,      ,9C=+ A6=+ AE=+ AF=+
      2107 D201 Y YY. YY. N MT-D0POS1 00 00      1113 2107
** FENCED SOFT      D8FFFF00 D0FFFF00 D0FFFF00 D0FFFF00
      00000000 00000000
***** SYMBOL DEFINITIONS *****
F = OFFLINE      + = PATH AVAILABLE
```

With the DS8000 DSCLI, you can use the **showlcu -sfstate** command, as shown in Example 8-17. The Soft Fence state of all devices in the specified LCU is displayed as Enabled or Disabled.

Example 8-17 showlcu -sfstate DSCLI command

```
dsccli> showlcu -sfstate d2
ID                D2
...
=====Soft Fence State=====
Name              ID    Sfstate
=====
ckd_p0_D200 D200 Enabled
ckd_p0_D201 D201 Enabled
ckd_p0_D202 D202 Enabled
...
```

Remove Soft Fence state

Normally, no intervention is required to clean up a Soft Fence state. HyperSwap enables Soft Fence to protect the old primaries from accidental access, and CSM disables the state again when you request to restart the HyperSwap session. If this automated process should fail, or if for some reason you need access to the old primary devices after a HyperSwap, you can remove the Soft Fence state manually.

In z/OS the MVS system command **SETHS UNFENCE** removes the Soft Fence state unconditionally from all devices that are defined to the Sysplex as shown in Example 8-18.

Example 8-18 MVS system command SETHS UNFENCE

```
IOSHM0504I Function Code failed on device pair = 0C62C,00000 RC = 4,
Rsn = 0, Step# = 2000
IOSHM0316I SETHS UNFENCE has completed 036
          Member: MZBCVS2  Devices Processed: 7680  Reason: 0
          Member: MZBCGDP  Devices Processed: 7680  Reason: 0
          Member: MCECEBC  Devices Processed: 7680  Reason: 0
```

If you have a need to remove the Soft Fence state of an individual device, you can use the **CONTROL** command of the Device Support Facilities (ICKDSF). Example 8-19 shows a JCL sample for ICKDSF to remove Soft Fence state from a single device.

Example 8-19 ICKDSF example to remove Soft Fence

```
//RMSF      EXEC PGM=ICKDSF,PARM='NOREPLYU'
//SYSPRINT DD SYSOUT=*
//SYSIN     DD *
CONTROL CLEARFENCE SOFT UNIT(D000) -
SERIAL(ACA91) -
SCOPE(DEV)
/*
```

Specify the parameters as follows:

- ▶ **UNIT**: the z/OS device number that you want to unfence.
- ▶ **SCOPE**: determines whether you want to unfence a single device ('DEV') or a complete LSS ('LSS'). If you specify LSS, the whole LSS of the device specified with UNIT is unfenced.
- ▶ **SERIAL**: the last five digits of the Storage Image ID of the storage system the devices are located on.

Note: You can determine the Storage Image ID using a **DEVSERV QDASD** command. The field **DEV-SERIAL** provides the required information (see Example 8-15 on page 177).

8.5.3 Recovering from Secondary In Use By System

The MetroMirror secondary volumes that are part of a HyperSwap configuration have a special device state in z/OS: Offline, in Use by System (F-SYS). If the HyperSwap configuration is purged, or HyperSwap is disabled, z/OS returns the device to the normal Offline state.

There may be situations, where a device is in F-SYS state, although no HyperSwap configuration is loaded. In this case, a HyperSwap load test that includes this device will fail. You can determine if a device is in F-SYS state using the **DISPLAY U** or **DISPLAY M=DEV** commands, as shown in Example 8-20.

Example 8-20 Determine F-SYS state

DISPLAY U,,D200

```
IEE457I 15.52.18 UNIT STATUS 297
UNIT TYPE STATUS      VOLSER      V
D200 3390 F-SYS
D201 3390 F-SYS
...
```

DISPLAY M=DEV(D200)

```
IEE174I 15.54.18 DISPLAY M 341
DEVICE 0D200 STATUS=OFFLINE, IN USE BY SYSTEM
CHP          9C  A6  AE  AF
...
```

CSM version 6.2.2 and later have the capability built in to indicate to the HyperSwap Manager to tolerate an F-SYS state during the load of a HyperSwap configuration. You can use the **Reset In Use By System on Secondary Volumes** option in the session properties panel when you restart the session, as shown in Figure 8-8.

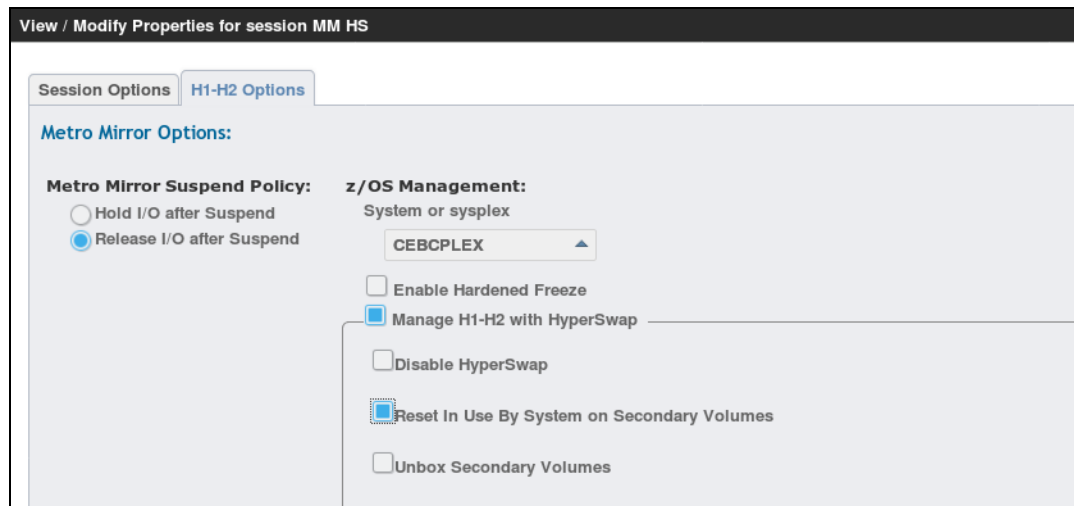


Figure 8-8 Recover from In Use By System state

Refer to 7.1.3, “HyperSwap configuration settings” on page 132 for a more detailed explanation of the HyperSwap options.

Note: z/OS APAR OA53082 must be applied to all LPARs in the HyperSwap managed Sysplex to use the Reset In Use By System on Secondary Volumes option.

If this feature is not available in your environment, the only way to reset F-SYS state is to IPL the affected LPARs.

8.5.4 Recovering from missing or stale NED

The *Device Node Element Descriptor* (NED) tells the operating system on which physical storage system the device is located. It must be available and consistent across all paths to a individual device. If the NED is missing, stale (does not match the currently attached hardware), or inconsistent, a HyperSwap configuration load will fail.

Note: Stale NEDs can occur, for example if storage hardware is replaced, but the z/OS and CSM configurations are not updated accordingly.

The NED is stored in certain z/OS device control blocks and device tables that must be refreshed in order to reflect the real configuration. You can use either of two methods to force this refresh.

The first method is based on the DFSMS System Data Mover (SDM). You can involve it using the **MODIFY** command, as shown in Example 8-21.

Example 8-21 The MODIFY command

```
MODIFY ANTAS000,REDISCOVER  
ANTB8002I OFFLINE DEVICE DISCOVERY COMPLETE; RC=4 REAS=2
```

In our example, the SDM address space ANTAS000 returned a return code of 4 with reason code 2, which means that *some offline devices were not processed*. If you see such a result, and the HyperSwap configuration load still fails, retry the recovery with the second method described here. Also resort to the second method if SDM is not active in your environment.

If you have multiple LPARs in the Sysplex where any of them could be affected by missing or stale NEDs, you can also route the command to all LPARs, as shown in Example 8-22.

Example 8-22 Route command to all LPARs in Sysplex

```
ROUTE *ALL,MODIFY ANTAS000,REDISCOVER
```

You should allow up to one minute for the LPARs to complete the rediscovery.

For the second method, you use the **DEVSERV QDASD** command. It provides options to delete and revalidate the affected data structures. In Example 8-23 we show how to perform this refresh for an entire LCU, defined by its SSID. You can also use any other device definition methods provided by **DEVSERV**.

Example 8-23 Refresh device tables using DEVSERV

```
DEVSERV QDASD,SSID=D001,DELETE  
IEE459I 13.18.35DEVSERV QDASD- 190  
SSID
```

```
D001
  DEVICE TABLE FOR THIS SSID IS CLEARED
```

DEVSERV QDASD,SSID=D001,VALIDATE

```
IEE459I 13.19.04 DEVSERV QDASD 192
  UNIT VOLSER SCUTYPE DEVTYPE      CYL  SSID SCU-SERIAL DEV-SERIAL EFC
OD000 ATD000 2107980 2107900      1113 D001 0175-ACA91 0175-ACA91 *OK
OD001 ATD001 2107980 2107900      1113 D001 0175-ACA91 0175-ACA91 *OK
...
```

8.5.5 Additional hints and tips

This section describes other tips you may find helpful.

Find HyperSwap master

Sometimes you may need to know, on which z/OS system in your Sysplex the HyperSwap Manager master address space is running. The LPAR with master address space provides all detailed HyperSwap log messages. You can use the MVS system **MODIFY** command, as shown in Example 8-24. The LPAR with master address space provides all detailed HyperSwap log messages.

Example 8-24 Get HyperSwap master

MODIFY HSIB,DISPLAY

```
IOSHMOPR Master System = MZBCVS2
IOSHM0424I Master status = 00000000 00000000 0000002600000000
...
```

The first parameter after the command is the name of the HyperSwap Manager address space. It can be different from that in the example.

Note: The **MODIFY** command can be abbreviated as **F**, the **DISPLAY** parameter as **D**. The abbreviated command example is **F HSIB,D**.

Resuming I/O in case of Hold I/O after Suspend

If you are using the CSM MM Suspend Policy Hold I/O after Suspend, all write I/O operations will be stopped for the configured Extended Long Busy (ELB) timeout if MM is suspended for any reason. You can resume write I/O by issuing the **SETHS RESUMEIO** command. Optionally, you can issue the **Release I/O** command in the CSM session.

Restoring HyperSwap in case of programmatic blocking condition

Some programs that also use the UCB swap capability of z/OS, such as IBM Transparent Data Migration Facility (IBM TDMF), can disable or block HyperSwap for the periods of time where they want to perform UCB swaps themselves. Normally, they reset their block after they are done. Should a program fail to do this and leave the programmatic blocking condition in place (IOSHM0311I), you can reset it manually by issuing the **SETHS UNBLOCK** command.

8.5.6 Creating support information

For any abnormal situation that points to a defect in hardware, software, or your configuration, you will most likely involve IBM support for help and problem resolution. The IBM support

representative will ask you to provide support information. CSM allows you to generate support packages for CSM itself, and also for the attached DS8000 storage systems.

To create a CSM support package, you select **Settings** → **Advanced Tools** from the CSM main menu. As shown in Figure 8-9, in the first section of the Advanced Tools panel, you find a button to create a PE data package, and a link leading to another panel where you can download existing packages.

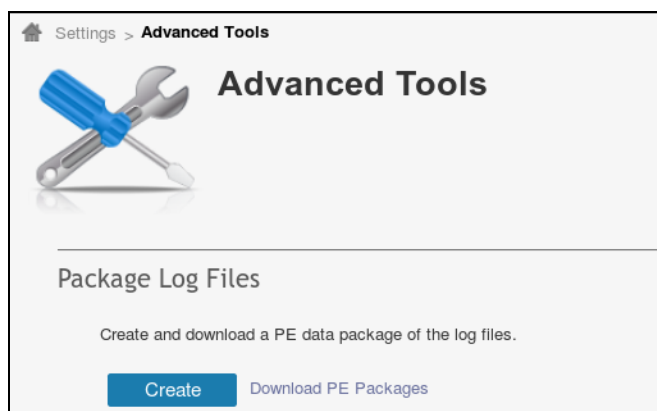


Figure 8-9 Create a CSM support package

To create a DS8000 storage system support package, you first go to the list of attached storage systems, by selecting **Storage** → **Storage Systems** from the CSM main menu. In this list, you select the storage system that you want to create the support data for. Use the **Select Actions** button to get a list of actions and select **Create Systems Diagnostics**, as shown in Figure 8-10.



Figure 8-10 Create DS8000 support package

Note: The DS8000 must be connected to the CSM server with a user that has an admin role, otherwise the CSM server is not authorized to perform diagnostic commands on the storage system.



A

Checklists

This appendix contains checklists you can use to plan and track the implementation of various components of the IBM Copy Services Manager (CSM) and z/OS HyperSwap solutions that are discussed in this IBM Redbooks publication.

Checklist for implementation planning

Table A-1 lists the high level tasks to consider when planning for the proper solution.

Table A-1 Implementation planning checklist

Task description	Owner	Status
Define the overall solution requirements	Client	
Review solution components to get an understanding of their capabilities and limitations	Client, Solution architect	
Review implementation scenarios to determine the preferred implementation topology for storage replication and optional HyperSwap management	Client, Solution architect	
Review the CSM license types to determine the preferred CSM licensing option and ensure it covers the selected implementation topology	Client, Sales Rep, Solution architect	
Review the pre-requisites for implementation of the required solution components and ensure they can be achieved	Client, Solution architect	

Checklist for CSM installation on z/OS

Table A-2 lists the high level tasks for an installation of CSM on a z/OS logical partition (LPAR).

Table A-2 CSM installation on z/OS checklist

Task description	Owner	Status
Review the TCP/IP communication requirements and define ports to be used for the installation	System Admin, Security Admin	
Make sure the used ports are open in network firewalls as well as CSM Server operating system firewalls	System Admin, Security Admin	
Obtain installation images from Shopz	System Admin, Sales Rep	
Review Program Directory and perform SMPE installation of CSM	System Admin	
Create required user accounts	Security Admin	
Create and mount the CSM file system	System Admin, Storage Admin	
Perform CSM installation in UNIX System Services	System Admin	
Create started tasks for required CSM server address spaces	System Admin	
Launch CSM server and verify accessibility and functionality	System Admin, CSM Admin	

Task description	Owner	Status
If the CSM server file system volumes will be part of a managed Metro Mirror (MM) configuration: Make sure to enable either Hardened Freeze or HyperSwap for this session to prevent that the CSM server may freeze its own release I/O processing. Otherwise this can result in a Sysplex halt for the configured Extended Long Busy (ELB) timeout (2 minutes)	CSM Admin	

Checklist for z/OS IP host connection setup

Table A-3 lists the high level tasks to implement a z/OS IP host connection between a CSM server and a z/OS LPAR.

Table A-3 z/OS IP host connection setup checklist

Task description	Owner	Status
Review the z/OS IP host connection requirements and define the socket ports to be used for the connections	System Admin, Security Admin	
Make sure the used ports are open in network firewalls as well as CSM Server operating system firewalls	System Admin, Security Admin	
Create required user accounts for HyperSwap and IP Socket Connection started tasks and authentication	System Admin, Security Admin	
Configure HyperSwap tasks on all LPARs that should connect to the CSM servers. Use the SOCKPORT parameter with the defined port	System Admin	
Create self signed certificates or obtain certificates from trusted Certificate Authority	Security Admin	
Create keyring with the certificate	Security Admin	
Export the certificate to a file for use by the CSM servers	Security Admin	
Configure Application Transparent Transport Layer Security (AT-TLS) policy rules for encryption of the HyperSwap socket port traffic	Network Admin, Security Admin	
Configure the z/OS TCP/IP Policy agent (PAGENT) as started task and configure activation of the defined policy rules	Security Admin, Network Admin	
Only for CSM servers prior 6.1.5: Create Java keystore file, add exported certificate and replace default keystore file on CSM servers	System Admin, CSM Admin	
Create a host connection definition on the CSM servers. For CSM servers at 6.1.5 or later: Upload the exported certificate file during the IP host connection definition.	System Admin, CSM Admin	
Verify z/OS IP host connection capability from all required CSM servers to all required LPARs	System Admin, CSM Admin, Network Admin, Security Admin	
Optional: If VIPA is used for IP virtualization of the z/OS IP host connection: make sure each LPAR can be connected and automatic reconnection to another LPAR takes place once an LPAR disconnects	System Admin, CSM Admin, Network Admin, Security Admin	

Checklist for z/OS HyperSwap implementation

Table A-4 lists the high level tasks to prepare a z/OS HyperSwap implementation.

Table A-4 z/OS HyperSwap implementation preparation checklist

Task description	Owner	Status
Review HyperSwap functionality and dependencies	System Admin, Storage Admin, CSM Admin	
Review the z/OS HyperSwap pre-requirements and make sure they can all be met: <ul style="list-style-type: none"> ▶ All LPARs in Sysplex must participate HyperSwap and must have defined physical and logical access via FICON to HyperSwap devices ▶ If Monoplex is used: Ensure proper configuration in PARMLIB ▶ HyperSwap must be able to control all system and application related disk devices, with the exception of certain XCF Couple Data Sets that must be excluded ▶ Ensure symmetric Channel configuration to primary and secondary devices. Caution must be taken if zHyperLink attachment is used. ▶ Ensure symmetric MIDAW configuration ▶ Avoid sharing of HyperSwap managed devices with external LPARs not belonging to the managed Sysplex ▶ Avoid sharing of HyperSwap managed logical control unit (LCU) pairs with externally managed replication on same LCU pairs ▶ Ensure sufficient user permissions for HyperSwap related console commands 	System Admin, Security Admin, Storage Admin	
Review the DS8000 pre-requirements for HyperSwap usage and make sure they can all be met: <ul style="list-style-type: none"> ▶ Proper firmware levels are installed ▶ Copy Services licenses (MM) are activated ▶ Unique SSIDs are configured for primary and secondary LCUs ▶ If CSM runs on a DS8880 Hardware Management Console (HMC): Review and comply to related specific requirements 	System Admin, Storage Admin	
Ensure latest HyperSwap PTFs are installed on all Sysplex LPARs	System Admin	
Enable Critical Paging on all Sysplex LPARs: Activation requires an IPL	System Admin	
Avoid use of Hardware Reservations. Make sure Reservations are converted to Global ENQs	System Admin, Storage Admin	
Review HyperSwap related message control capabilities and implement desired message control options	System Admin	
Review options to reduce delays of HyperSwap triggers and configure them appropriately	System Admin, Storage Admin	
Review options to allow I/O timeouts to trigger a HyperSwap and configure them appropriately	System Admin, Storage Admin	
Review Couple Data Set considerations and plan proper placement for the selected solution	System Admin, Storage Admin	

Task description	Owner	Status
If Enhanced Catalog Sharing is used: Review considerations for ECS after a HyperSwap. Consider migration to RLS protocol for catalog sharing if applicable	System Admin	
Review IPL considerations and implement an adequate mechanism to prevent IPLs from the wrong devices after a HyperSwap	System Admin, Storage Admin	
Review allocation and esoteric name requirements and configure them appropriately	System Admin, Storage Admin	
Review JES3/JES2 applicable considerations for HyperSwap managed environments	System Admin	
Avoid use of Cache Fast Write	System Admin	
Avoid use of Concurrent Copy	System Admin	
For XRC only: Review XRC interactions with HyperSwap	System Admin, Storage Admin	
If FlashCopy volumes are part of the HyperSwap configuration: Review proper configuration options for the FlashCopy tasks to avoid HyperSwap or Freeze impacts during FlashCopy processing	System Admin, Storage Admin	
If you use other products that use Unit Control Block (UCB) swap, make sure they can coexist with z/OS HyperSwap	System Admin	
Review special HyperSwap related considerations for other applications if they are in use	System Admin	

Table A-5 lists the high level tasks to implement and activate HyperSwap for a Sysplex.

Table A-5 IBM z/OS HyperSwap implementation and activation checklist

Task description	Owner	Status
Configure and activate automated start of HyperSwap address spaces (HSIB and HSIBAPI) on each LPAR in the managed Sysplex	System Admin, Security Admin	
Establish connections from CSM to the z/OS HyperSwap address space and the managed storage systems: <ul style="list-style-type: none"> ► Create z/OS IP host connections if a CSM instance runs outside of the Sysplex ► Create z/OS Direct Connection (FICON) to allow CSM to manage devices via FICON ► Optional: Create DS8000 HMC connection for an additional communication path to manage storage devices 	System Admin, Storage Admin, CSM Admin	
Create or use existing CSM session and add device pairs to be managed with HyperSwap <ul style="list-style-type: none"> ► Consider use of a small test configuration for initial functional tests (no system related volumes) ► The final CSM session can be already prepared but will be activated just after completion of functional testing 	CSM Admin, Storage Admin	
Set a Sysplex association in the CSM session to enable HyperSwap management capabilities	CSM Admin	
Start the CSM session to create or assimilate existing MM pairs	CSM Admin, Storage Admin	

Task description	Owner	Status
If existing MM pairs are assimilated in the CSM session that is managed with HyperSwap: make sure the pairs do not use <i>Critical Mode</i> before you activate HyperSwap	CSM Admin, Storage Admin	
Once the session is <i>Prepared</i> , activate HyperSwap management in the CSM session properties to have the HyperSwap configuration loaded	CSM Admin, System Admin, Storage Admin	
Perform functional HyperSwap tests: <ul style="list-style-type: none"> ▶ Planned HyperSwap and resync ▶ Unplanned HyperSwap and resync 	CSM Admin, System Admin, Storage Admin	

Related publications

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

References

- ▶ IBM Copy Services Manager Knowledge Center
https://www.ibm.com/support/knowledgecenter/SSESK4/csm_kcwelcome.html
- ▶ z/OS Hot Topics Newsletter of August 2016, article on page 59: *Hurry up and HyperSwap, Making the best use of IOS recovery options in a HyperSwap environment*.
<https://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZS103027USEN&>
- ▶ IBM Knowledge Base document II14654: *How to TEST an UNPLANNED HYPERSWAP VIA the DEFERRED BOXING TRIGGER*:
<https://www.ibm.com/support/docview.wss?uid=isgl1II14654>
- ▶ White Paper: *Configuring z/OS to Ensure Successful DASD Swap Using the CRITICALPAGING Function*:
<http://www.ibm.com/support/docview.wss?uid=tsslwp101800>

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.

- ▶ *IBM Copy Services Manager Implementation Guide*, SG24-8375
<http://www.redbooks.ibm.com/abstracts/sg248375.html?Open>
- ▶ *IBM Tivoli Storage Productivity Center for Replication for System z*, SG24-7563
<http://www.redbooks.ibm.com/abstracts/sg247563.html?Open>
- ▶ *DS8000 Copy Services*, SG24-8367
<http://www.redbooks.ibm.com/abstracts/sg248367.html?Open>
- ▶ *IBM DS8880 Integrated Copy Services Manager and LDAP Client on the HMC*, REDP-5356
<http://www.redbooks.ibm.com/abstracts/redp5356.html?Open>
- ▶ *DS8000 Four-Site Replication with IBM Copy Services Manager*, REDP-5517
<http://www.redbooks.ibm.com/abstracts/redp5517.html?Open>

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

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services



SG24-8431-00

ISBN 0738457612

Printed in U.S.A.

Get connected

