Disaster Strikes! GDPS to the rescue!

Steven Cook

GDPS Software Development

Client Technical Advocate

IBM

cooksd@us.ibm.com

Abstract

Overview of GDPS
GDPS xDR solution (Synergy between GDPS and VM)

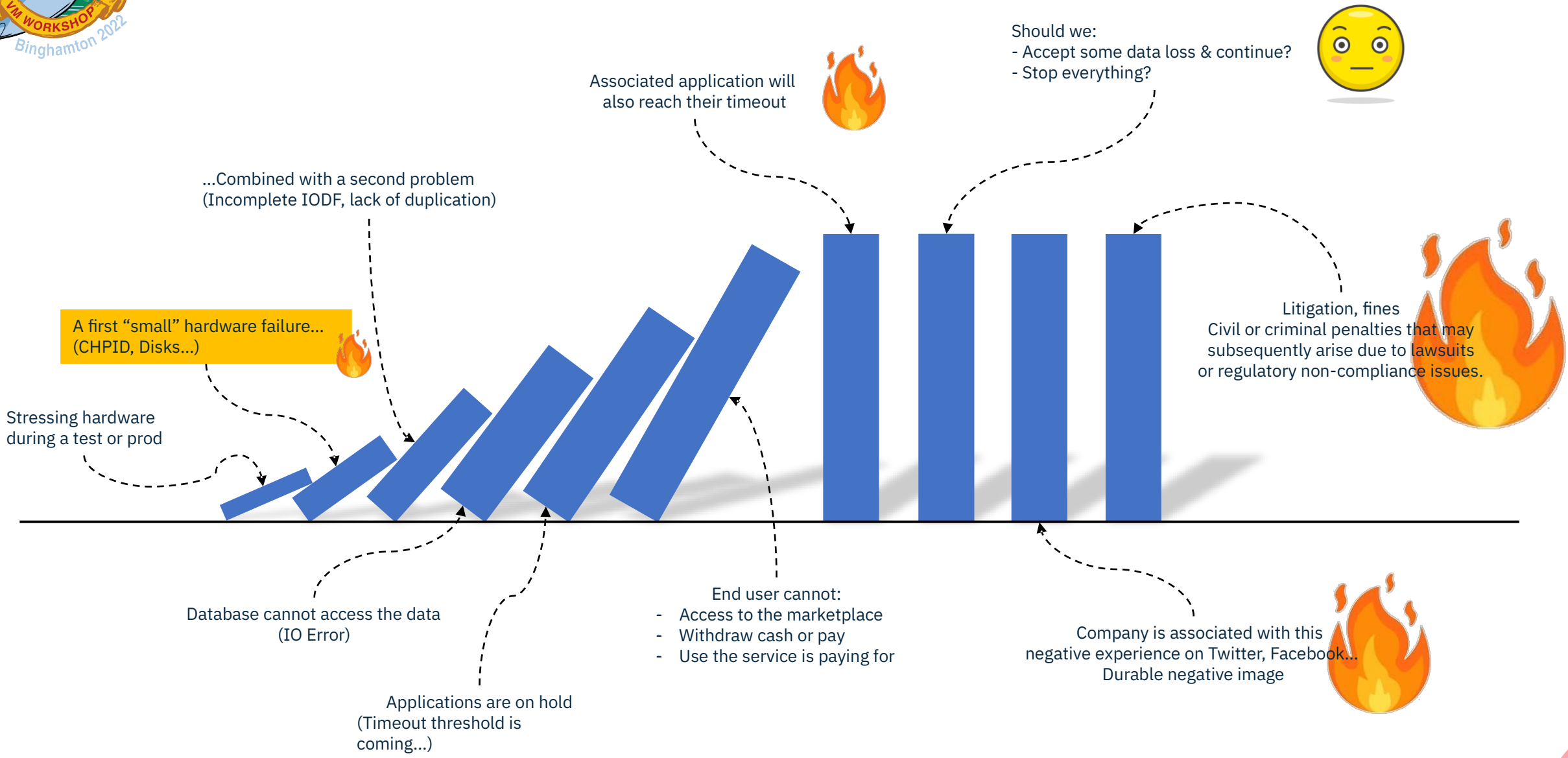
How to debug your VM GDPS environment with advanced log retrieval
How to save LinuxONE systems from an outage

GDPS LCP & Cyber Resiliency

Red Hat OpenShift Container Platform (RHOCP) and GDPS.

GDPS Overview

The “small hardware problem”



When do we need a CA/DR solution?

Global disaster

- Hurricane
- Earthquake
- Power plants failure..

Do we have safe backup?
Do we have system ready to start outside of the region?

Local disaster

- Fire
- Power supply problem
- Unplanned IT Failure

Could we avoid downtime and data loss?
Is there a procedure to restart systems?

Maintenance

- Hardware & software update.
- Switch to a new datacenter
- Test

Can we do that transparently?
How to reduce the risk of a rolling problem during a maintenance scenario?

Built for continuous availability and disaster recovery

Automation

- Automate actions
- React to events
- Synchronize operations

GDPS™
Providing world class protection

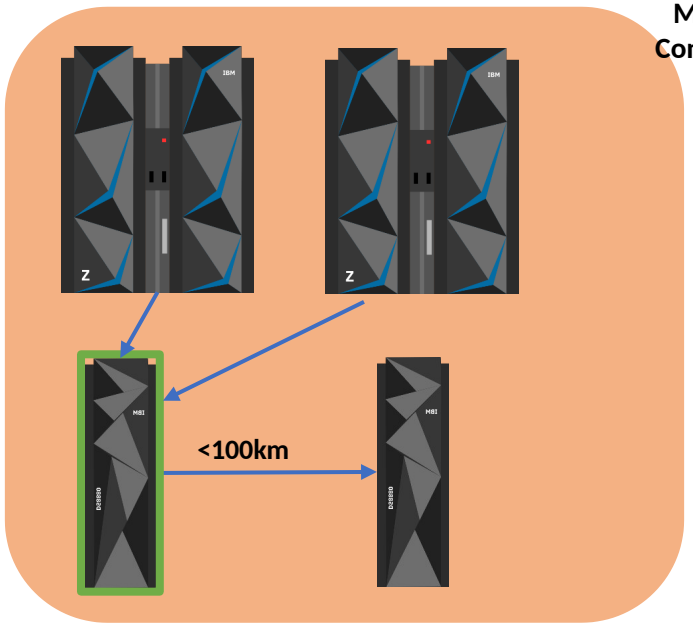
Single point of control

- Clear view of your systems and storages devices status
- Simply presents faults and warnings

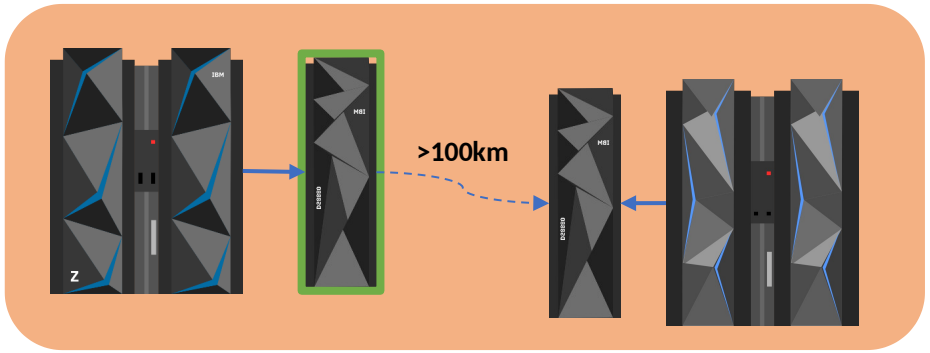
Heterogeneous type of storage (IBM DS8K, Hitachi, EMC disk...)

Heterogeneous platform (z/OS, KVM, zVM, Linux, SSC, zCX)

Metro configuration
Continuous Availability



Global configuration
Disaster Recovery



Handling complex situation

- Most of the time, problems strike us from multiple side at the same time
  - Data replication
  - Sysplex outage
  - Data corruption

- Metro Mirror = synchronous – Near CA solution
- Global Mirror = asynchronous - DR
- Both solutions can be combined to reach the highest level of resilience.

- GDPS has built-in function to handle this as automatically and simply as we want.
- Built-in function to start complex recovery procedure without having to manually do anything

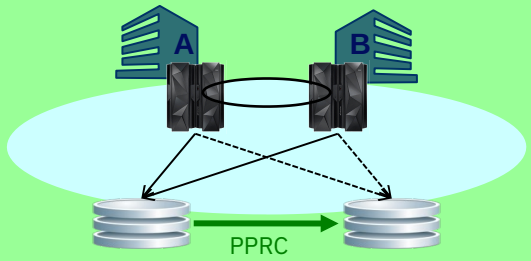
GDPS: a family of solutions designed to address different requirements and topologies

GDPS Metro

Near-continuous availability (CA) and disaster recovery (DR) within a metropolitan region

Two data centers

Systems can remain active
Multisite workloads can withstand site and storage failures



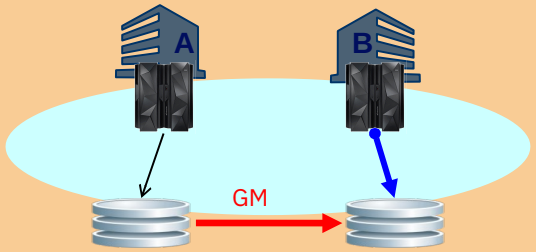
DR RPO equals 0 and RTO is less than 1 hour or
CA RPO equals 0 and RTO minutes

GDPS Global

Disaster recovery at extended distance

Two data centers

More rapid systems disaster recovery with "seconds" of data loss
Disaster recovery for out-of-region interruptions



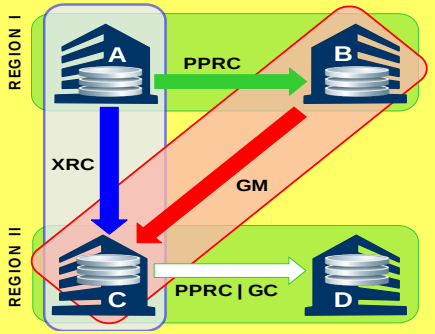
RPO seconds and RTO less than 1 hour

GDPS Metro Global 3 or 4-site

Near-continuous availability (CA) regionally and disaster recovery (DR) at extended distance from either region

Three or Four data centers

Near-continuous availability (CA) and Disaster recovery (DR) when running from any site



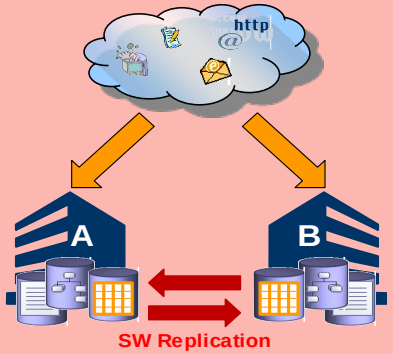
Designed for near-continuous availability within either region and RPO seconds and RTO less then one hour for unplanned region fail-over

GDPS Continuous Availability

Near-continuous availability, disaster recovery, and cross-site workload balancing at extended distance

Two or more data centers

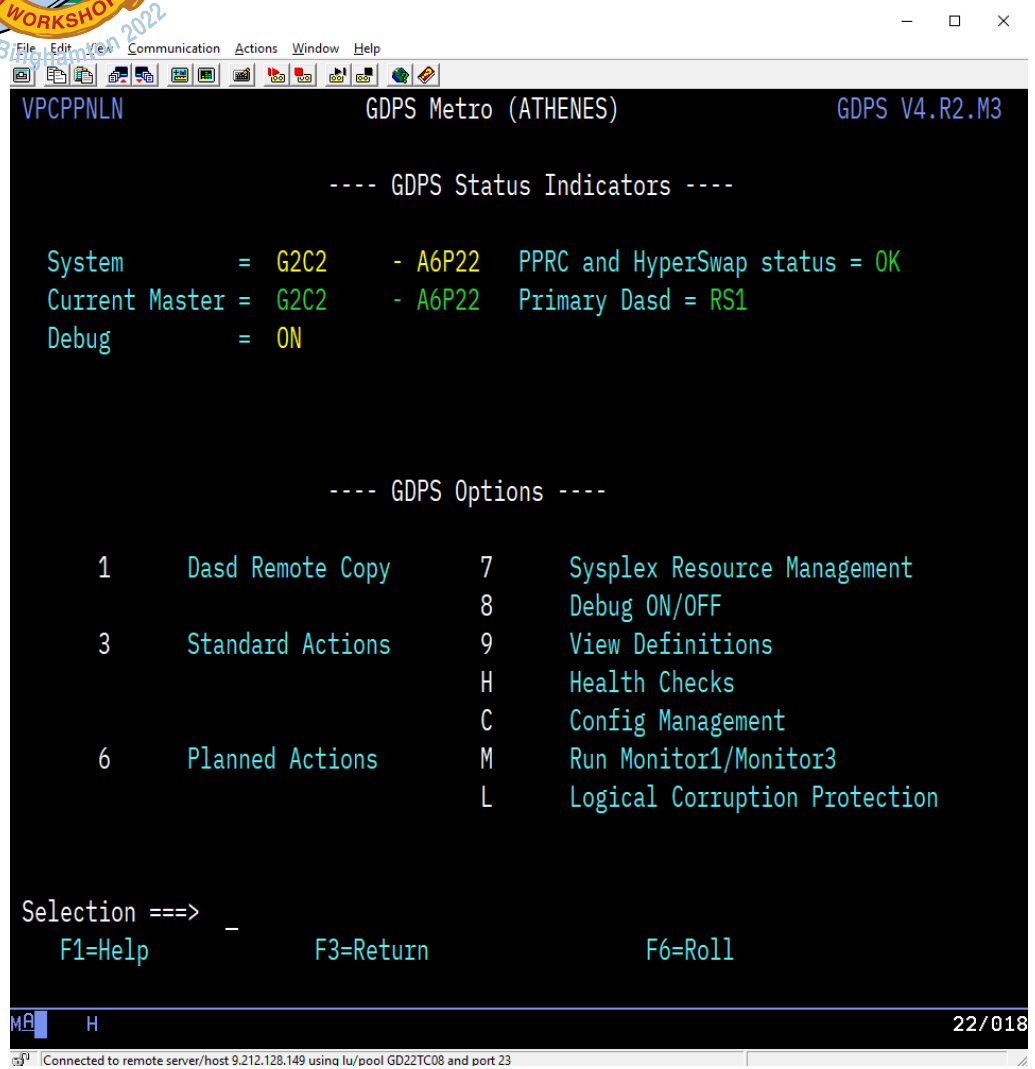
Disaster recovery for out-of -region interruptions
All sites active

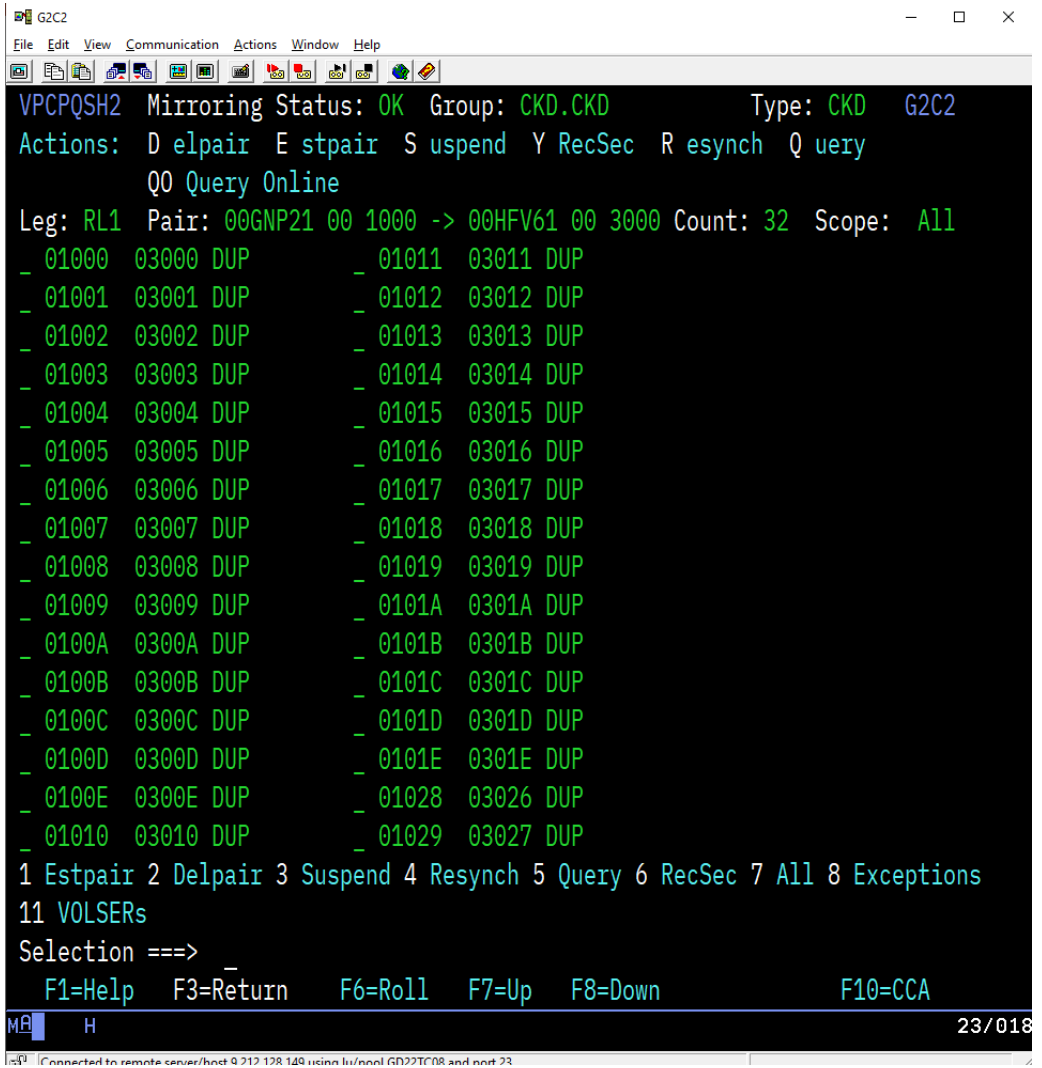


RPO zero or seconds and RTO seconds

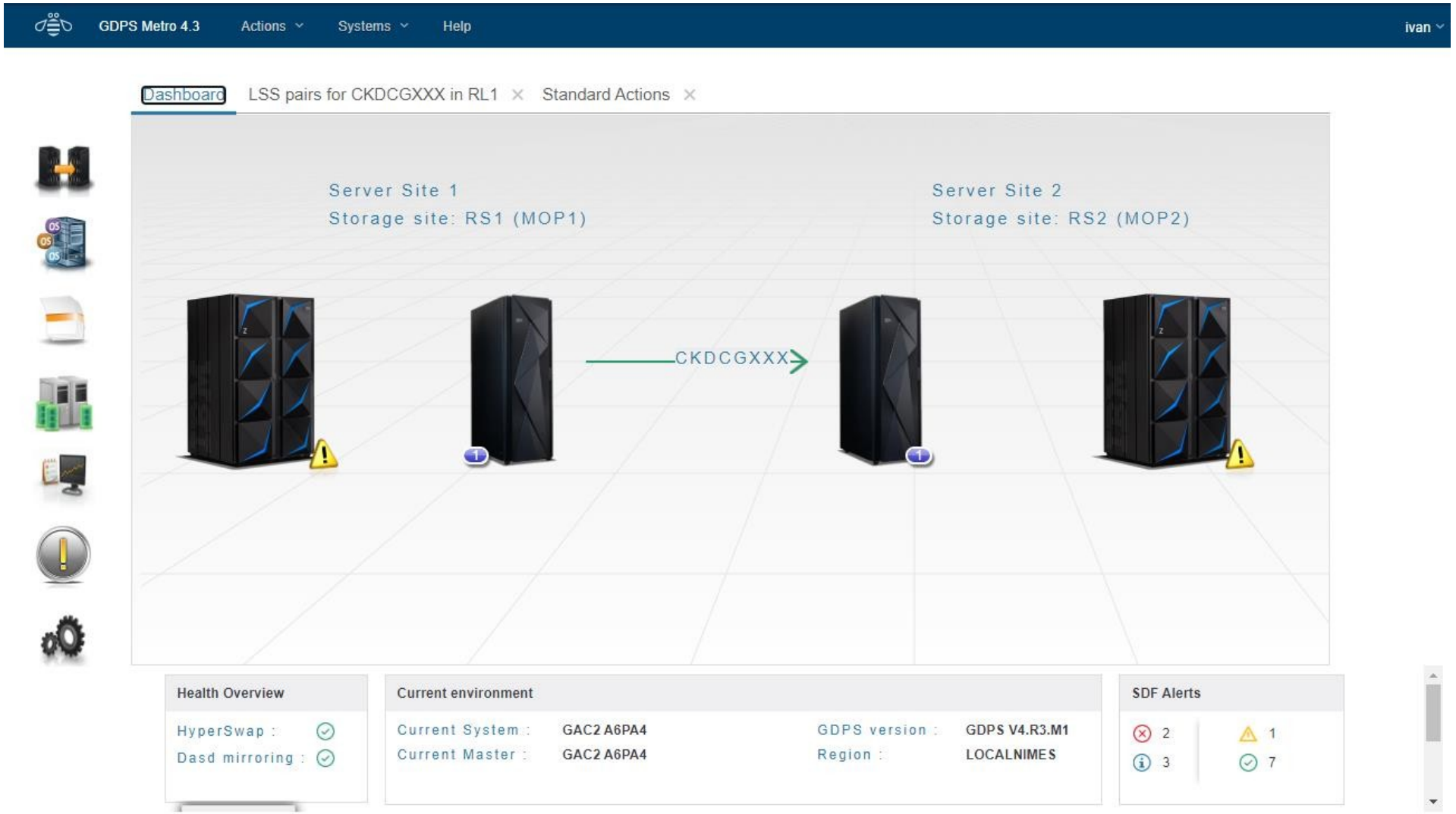
(c) Copyright IBM 2022

3270 interface

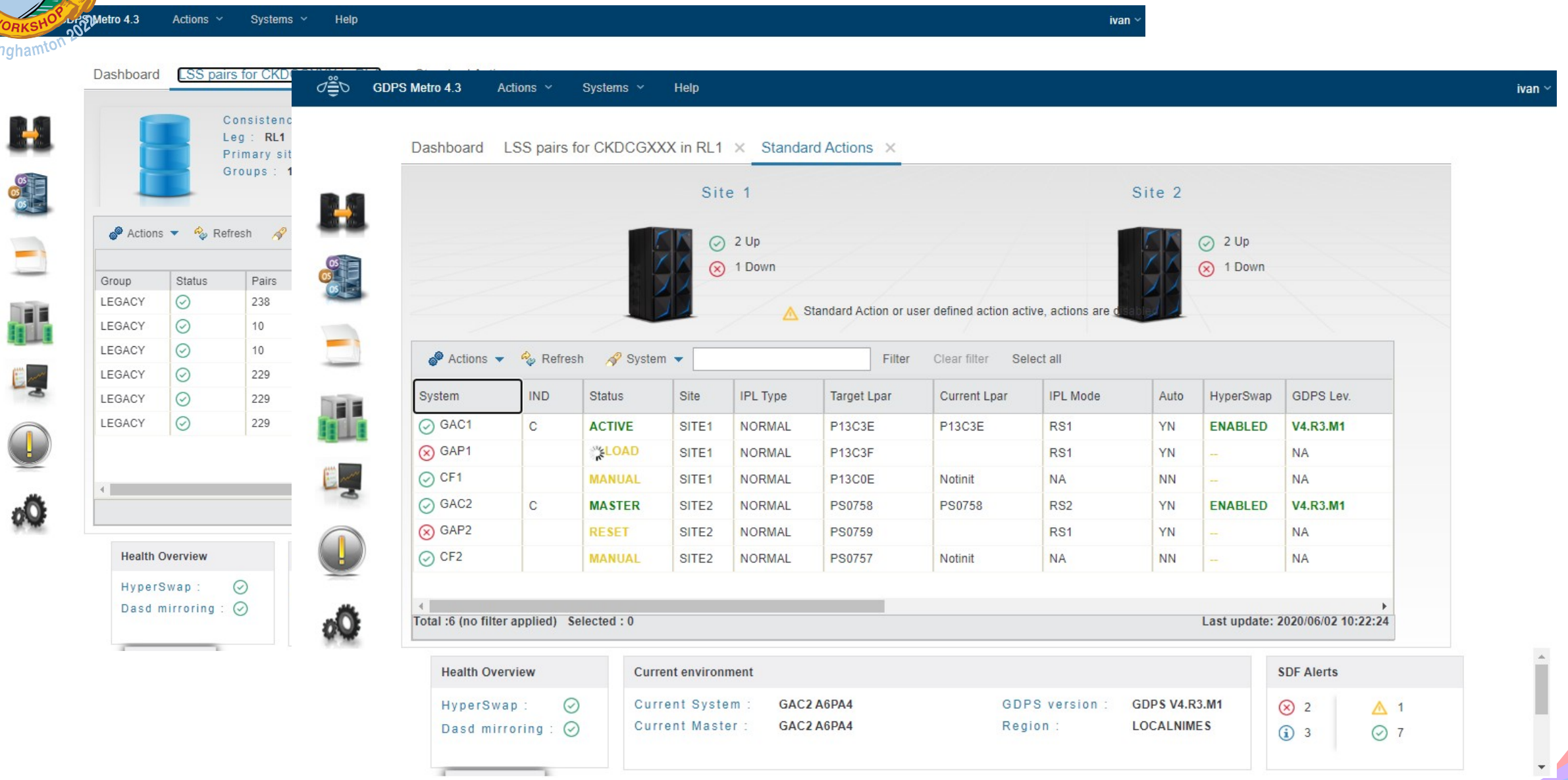




Web Interface

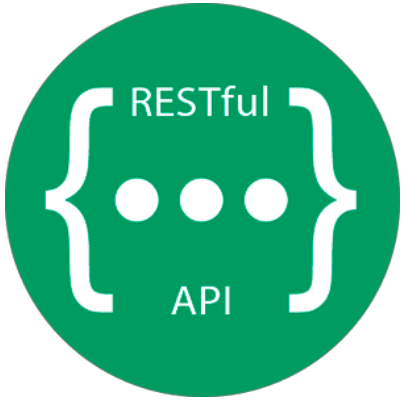


Systems, Storage, Alerts, and more...



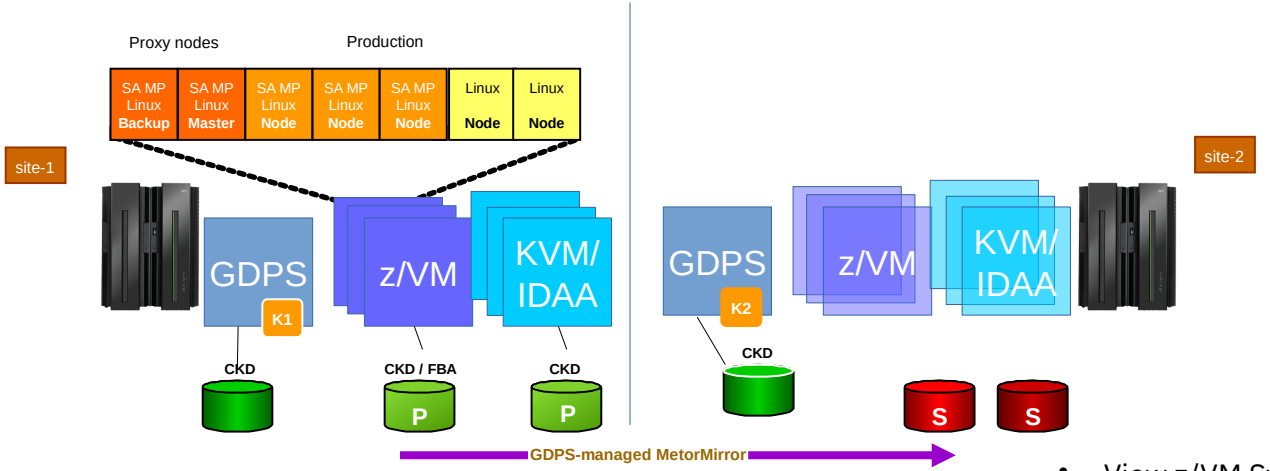
Restful API

- Most of the functions are now available thru a Restful API
- Encourage synergy between GDPS and other solutions
- Design your own interface to fit your requirements



GDPS xDR solution (Synergy between GDPS and VM)

GDPS xDR: z/VM Linux Guests



- Coordinated HyperSwap – z/OS, z/VM with its guests
- Graceful shutdown and startup (re-IPL in place) of Linux clusters or nodes
- Coordinated takeover – recovery from a Linux node or cluster failure
- Multiple Linux clusters are supported, as are multiple z/VM systems & Linux LPARs
- All members of a SA MP cluster must run under same z/VM system or SSI

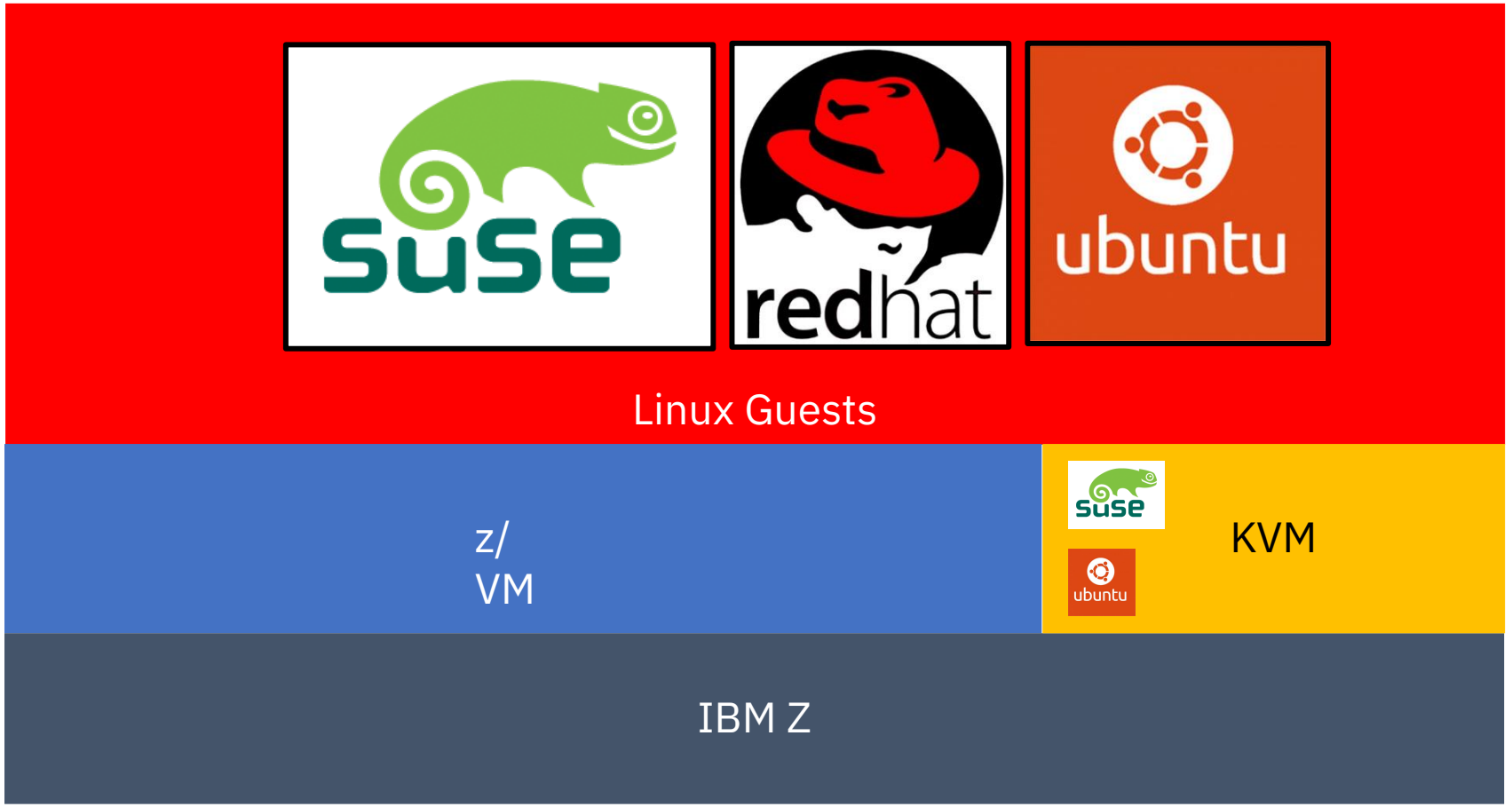
- View z/VM System and xDR Proxy
- HyperSwap planned/unplanned
- Site Switch planned/unplanned
- Freeze planned/unplanned
- Start/Stop z/VM image
- Live Guest Relocation

- SSC (vIDAA) in a Metro, MGM 3-site and 4-site configuration

- RESTful API provided for GDPS

Coordinated recovery for planned and unplanned events

Integration of distros of Linux guests (xDR and GVA)



Note:
For z/VM, xDR proxies are located in the Linux Guest (Suse or Redhat)
For KVM, xDR proxies are located in KVM

How to debug your VM GDPS environment with advanced log retrieval

Problem determination

GDPS provides a number of aids for problem determination:

- xDR Configuration Verification Programs
- xDR Monitor alerts can be found in the NetView log and can additionally be sent to a z/VM operator
- The GDPS xDR Status panel. (The last signal GDPS received about that node, or the last command GDPS sent to the node is also displayed and useful)
- GDPS Debug with the option of verbose tracing to a dataset
- Tracing of SA MP xDR components
- The **xdrstatus** command
- The **xdrgetlogs** command
- First Failure Data Capture (FFDC) messages can be found in the NetView log of the GDPS Master system (written to the Netview log using operator AUTLXX2, which you can filter on)

```
STATMON.BROWSE     ACTS  NETWORK LOG FOR 02/12/21 (21043) COLS 045 174  07:53
                                          DOMAIN: DSS3O   SCROLL ==> CSR
+----5----+----6----+----7----+----8----+----9----+---10----+---11----+---12----+---13----+---14----+---15----+---16----+
AUTLXX2  DSS3O SBBENGT-VPCLDCAP: 'VPCLDISP HSPROC XDRCSE3 VMproxycluster3 vmproxy3'
AUTLXX2  DSS3O SBBENGT-VPCLDCAP: XDRCSE3 Error report Cluster VMproxycluster3 node vmproxy3
AUTLXX2  DSS3O SBBENGT-VPCLDCAP: XDRCSE3 *received command Ä40.7802 xdr.hyperswap -v 1 -V -c VMproxycluster3 -n vmproxy3
AUTLXX2  DSS3O SBBENGT-VPCLDCAP: XDRCSE3 *Error: non-zero CP response for command 'HYPERSWAP ENABLE 012A1.15 01501.239':
AUTLXX2  DSS3O SBBENGT-VPCLDCAP: XDRCSE3 *
AUTLXX2  DSS3O SBBENGT-VPCLDCAP: XDRCSE3 HCPIOJ6412E 01520 is not a valid DASD type.
AUTLXX2  DSS3O SBBENGT-VPCLDCAP: XDRCSE3 HCPIOJ6412E 01521 is not a valid DASD type. Enable processing completed
AUTLXX2  DSS3O SBBENGT-VPCLDCAP: XDRCSE3 *16
AUTLXX2  DSS3O SBBENGT-VPCLDCAP: XDRCSE3 1
```

Output from the xdrstatus command

```
vmproxy2:~ # xdrstatus
xDR proxy master node
monitored state: erpd is online
erpd is up and running
cmdreceiver is up and running
xdrheartbeat is up and running
xDR maintenance mode is OFF
GDPS #1: (ConfigFile=/etc/Tivoli/tec/xdr1.conf, site=1, 10.20.30.11:5529, socket=6,
time=0)
GDPS #2: (ConfigFile=/etc/Tivoli/tec/xdr2.conf, site=2, 10.20.30.12:5529, socket=4,
time=0)
master K-system site: 2
erpd internal state: prepared
config received: mtmm: 12 gm: fc:
xdrlevel: 4.1.0.7 interim fix XDRFP71
package installed:
xdr-4.1.0.7-22075.s390x
xdrsl10-4.1.0.7-22075.s390x
```

Collecting xDR logs

The retrieval of z/VM, KVM, and IDAA proxy logs from GDPS is enhanced to allow administrators to collect Proxy-related data directly from GDPS panel without the need to involve administrators of distributed systems.

All the collected data is put in a tar file. You can either trigger collecting logs from xDR nodes by using the CL action on the xDR panel, which will also allow you to transfer the created tar file to Controlling system, or call xdrgetlogs on the node.

```
xdrgetlogs
--------------
collecting logs for xDR...
--------------
The collected debug data is available as /tmp/xdrlogs-2022-06-15-22.12.tar
```

How to save LinuxONE systems from an outage

GDPS Virtual Appliance

- Brings High Availability and disaster recovery capabilities of IBM Z to Linux-only enterprises and Linux-only systems

- No z/OS skills required!

- Years of Intellectual Capital invested in GDPS logic available providing
  - Ability to avoid impact cause by primary disk outage (planned or not)
  - Scripted automation

- Monitoring and central point of control provided thru the GDPS interface

GDPS Virtual Appliance

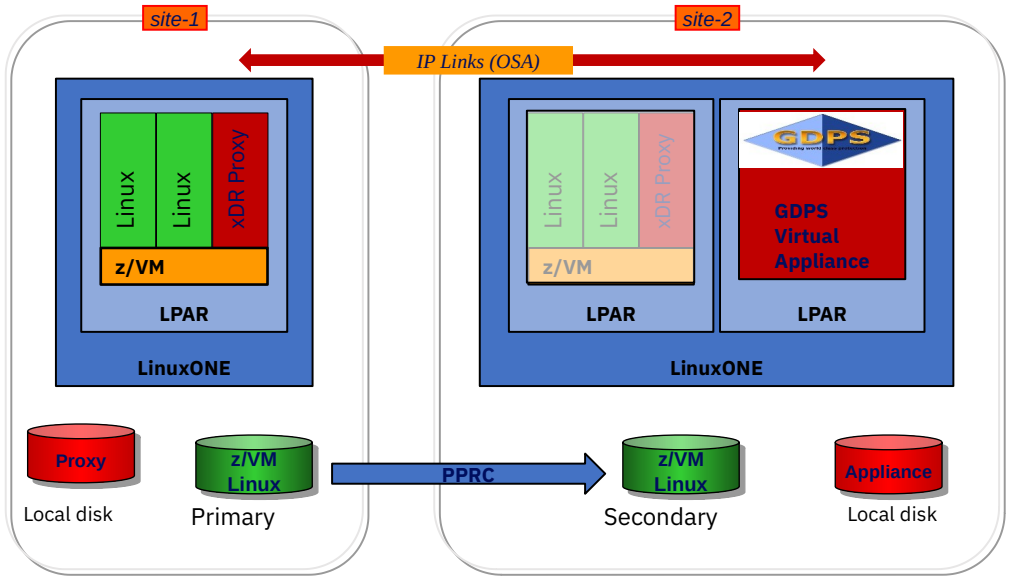
Operate GDPS using the GDPS web GUI

- View z/VM System and xDR Proxy
- HyperSwap planned/unplanned
- Site Switch planned/unplanned
- Freeze planned/unplanned
- Start/Stop z/VM image
- Start/Stop z/VM guest(s)
- Manage Linux clusters
- Live Guest Relocation

Provides non-z/OS customers the same benefits of high availability and D/R which were only available to z/OS customers

Provides additional benefit for moving workloads to Linux on IBM Z

GDPS Virtual Appliance: GDPS/Metro xDR capabilities for z/VM & Linux on z Systems clients who do not use z/OS



A comprehensive continuous availability and disaster recovery solution for z/VM clients

- **Monitors and manages**
  - PPRC replication management
  - Secondary data consistency
  - Planned and unplanned HyperSwap
- **System and Hardware management capabilities**
- Intuitive graphical user interface
- Simple scripting capability

GDPS LCP & Cyber Resilience

The question is not IF you will be attacked but WHEN

$170 B

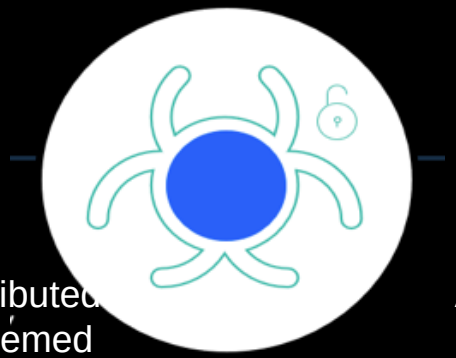
Predicted global ransomware demands WW forecast [6]

2000%

Explosive growth of attacks on enterprise operations 2019 compared to 2018 [1]

$8 Billion

Estimated global cost of WannaCry attack [3]



+ 50+

Unique malware distributed in various Covid-19 themed campaigns [4]

67%

Average increase in ransomware destructive attacks in 2019 [1]

$111K

Average ransomware cost up from 6700 in 2018 [2]

$230 Million

GDPR fine for one data breach [5]

© 2021 IBM Corporation

1. X- force intelligence index report 2020
2. Forbes Aug 18,2020
3 ReInsurance news May 23 2017
4,XF IRIS internal data analysis IBM 2020
5 Compliance Week July 8, 2019
6. MSSP Alert Feb 13,2020

SolarWinds Orion: More US government agencies hacked

solarwinds

BBC NEWS

HONDA

Honda Hackers May Have Used Tools Favored by Countries

The New York Times

REUTERS

'Payment sent' - travel giant CWT pays $4.5 million ransom to cyber criminals

GARMIN

The Garmin Hack Was a Warning

As ransomware groups turn their attention to bigger game, expect more high-profile targets to fall.

WIRED

The Register

Major bank-logic bomber jailed for eight years

Real-life BOFH ordered to pay $3.1m restitution

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

GDPS with Logical Corruption Protection

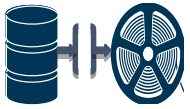
1. GDPS now includes Logical Corruption Protection support to protect against cyber attacks and more.
2. A licensed offering that can be deployed in a range of different GDPS solutions.
   - LCP-Manager(MM) and LCP-Manager(GM)
3. Provides the ability to secure Point-In-Time captures of critical data using either FlashCopy or Safeguarded Copy.
4. These Point-In-Time captures can be used for a variety of purposes

Catastrophic
Recover the entire environment back to the point in time of the copy as this is the only recovery option

Forensic
Recover the copy and use the copy to investigate the problem and determine what final recovery action is required.

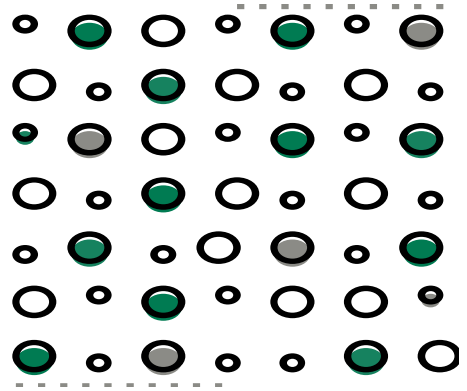
Surgical
Extract data from the copy and logically restore back to the production environment

Validation
Regular analytics on the copy to provide early detection of a problem or reassurance that the copy is a good copy prior to a further action

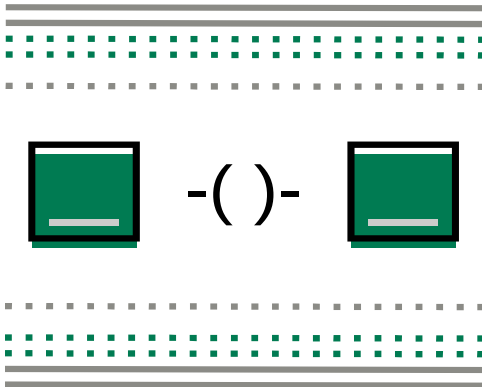


Offline Backup
Backup the copy of the environment to offline media to provide a second layer of protection

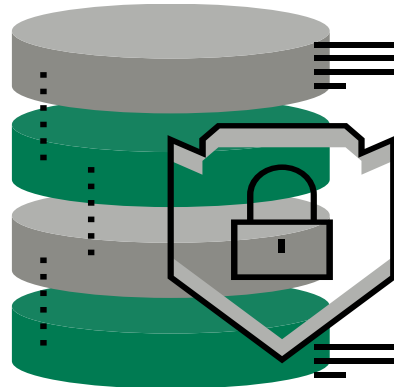
Required Characteristics for Protection Copies



Granularity
LCP must be able to create multiple secure copies to minimize data loss in the event of a corruption incident



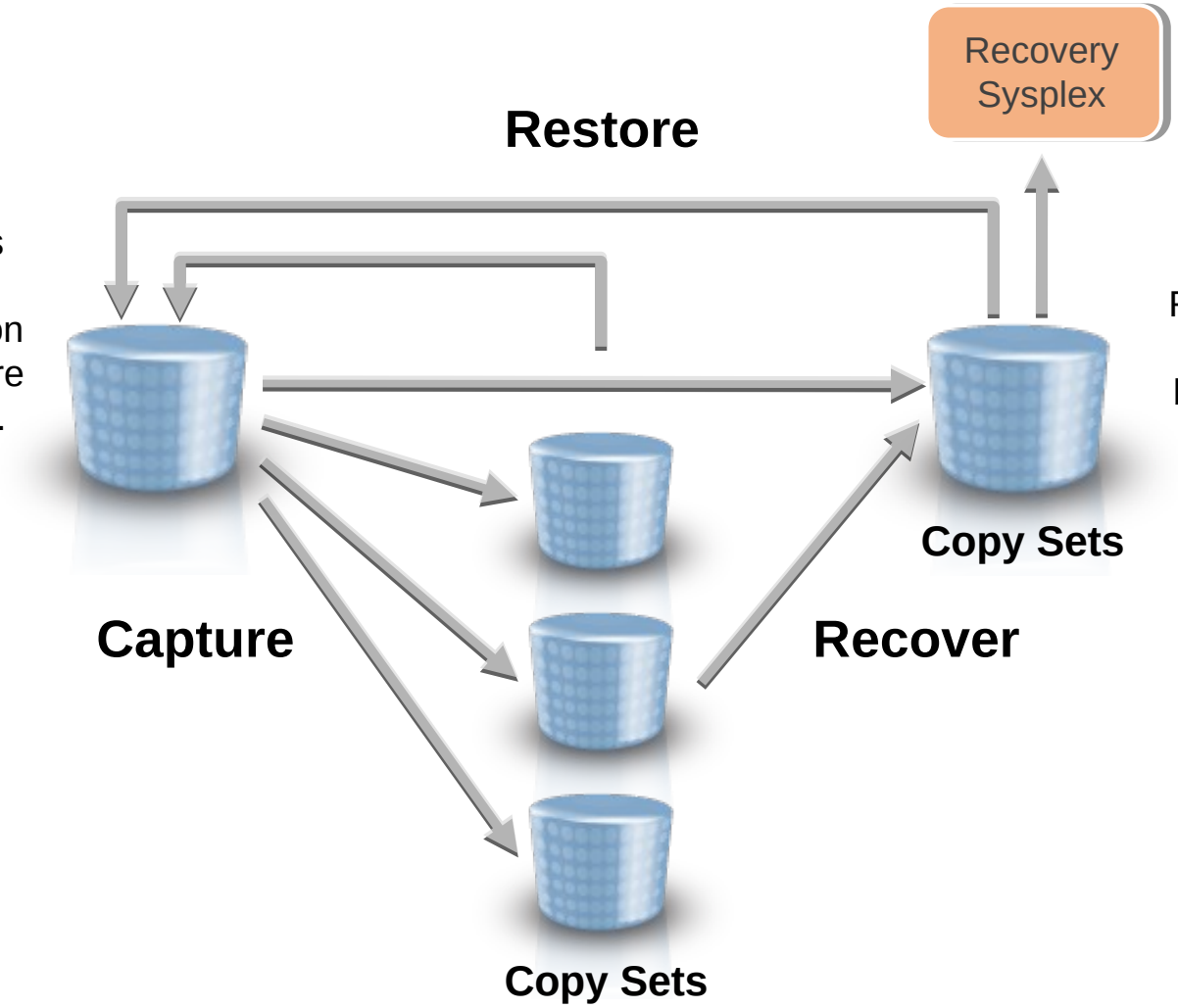
Isolation
The secure copies must be isolated from the active production data so that it cannot be corrupted by a compromised host system. This is also known as an Air Gap solution



Immutability
The secure copies must be protected against unauthorized manipulation .

The Anatomy of LCP

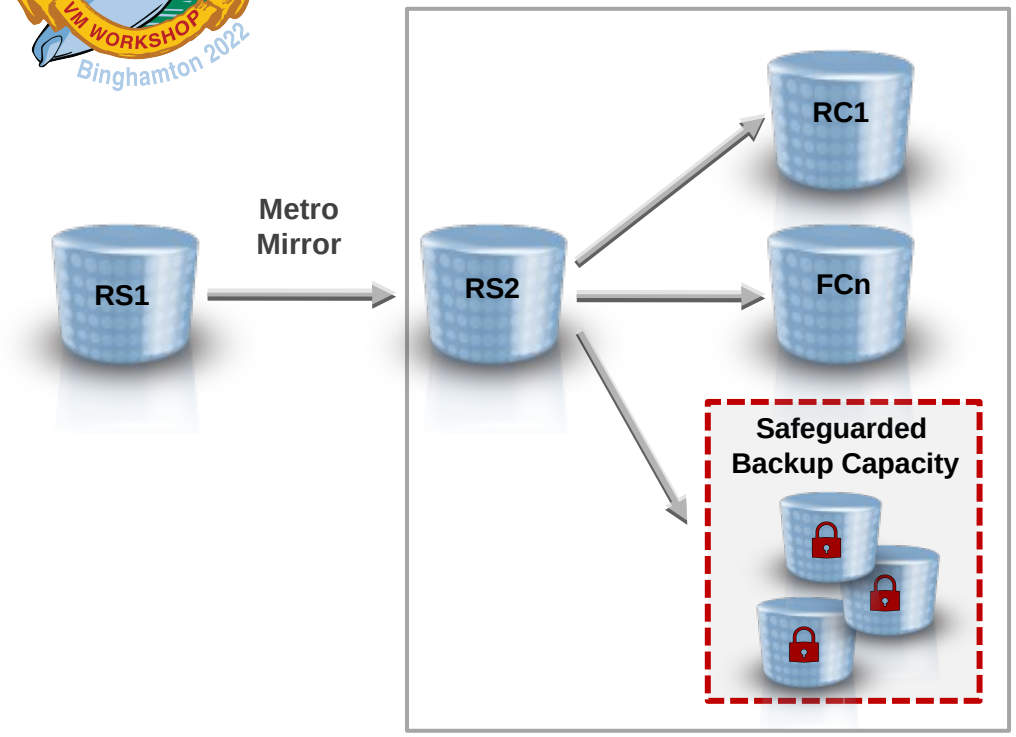
Source devices are where the copies are taken from. These could be production volumes in a virtual isolation environment or a staging volume where the environment is physically isolated. The source volumes inherit the security/protection provided by the production environment policies and capabilities.

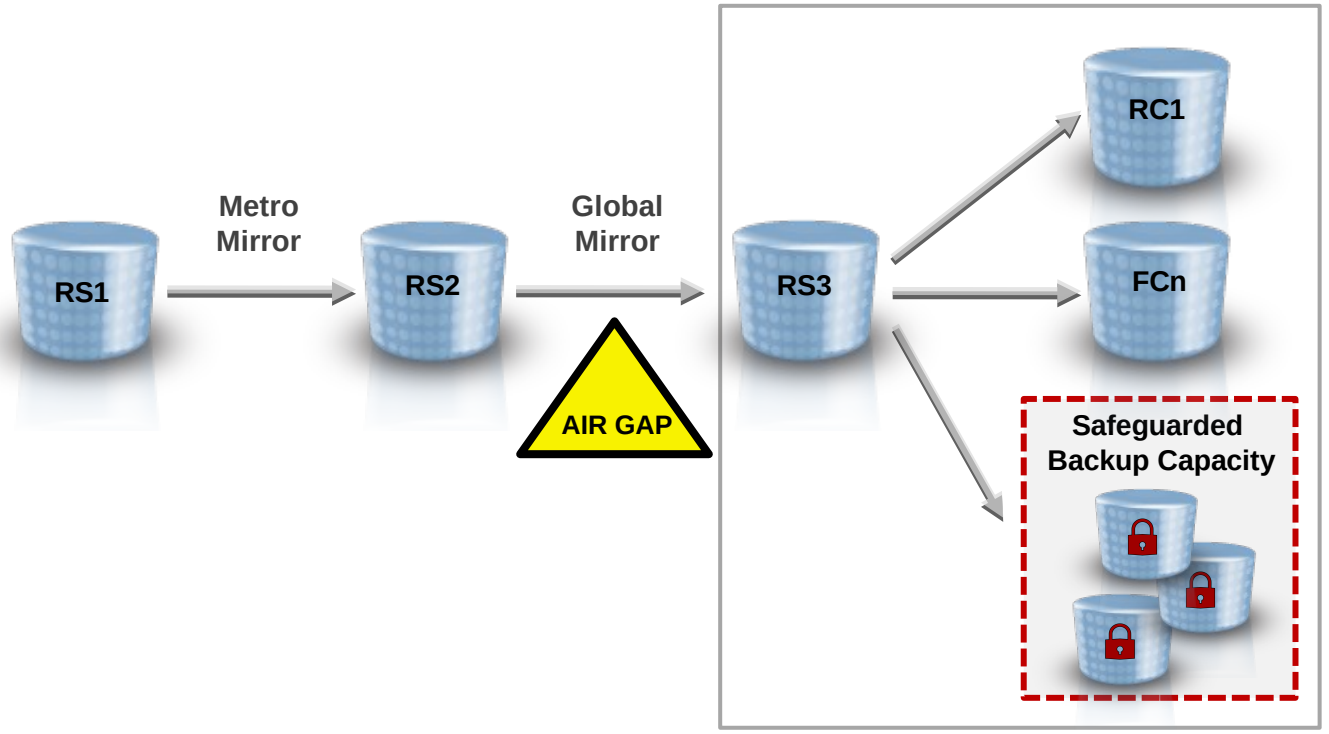


Recovery devices enable the IPL of systems for data validation of the backup copy, forensic analysis of a potential corruption event or other recovery purposes.

Protection/Backup capacity provides one or more logical protection Point-In-Time copies which are not accessible by any systems. Additional security measures aim to protect these from inadvertent or malicious actions.

Virtual versus Physical Isolation

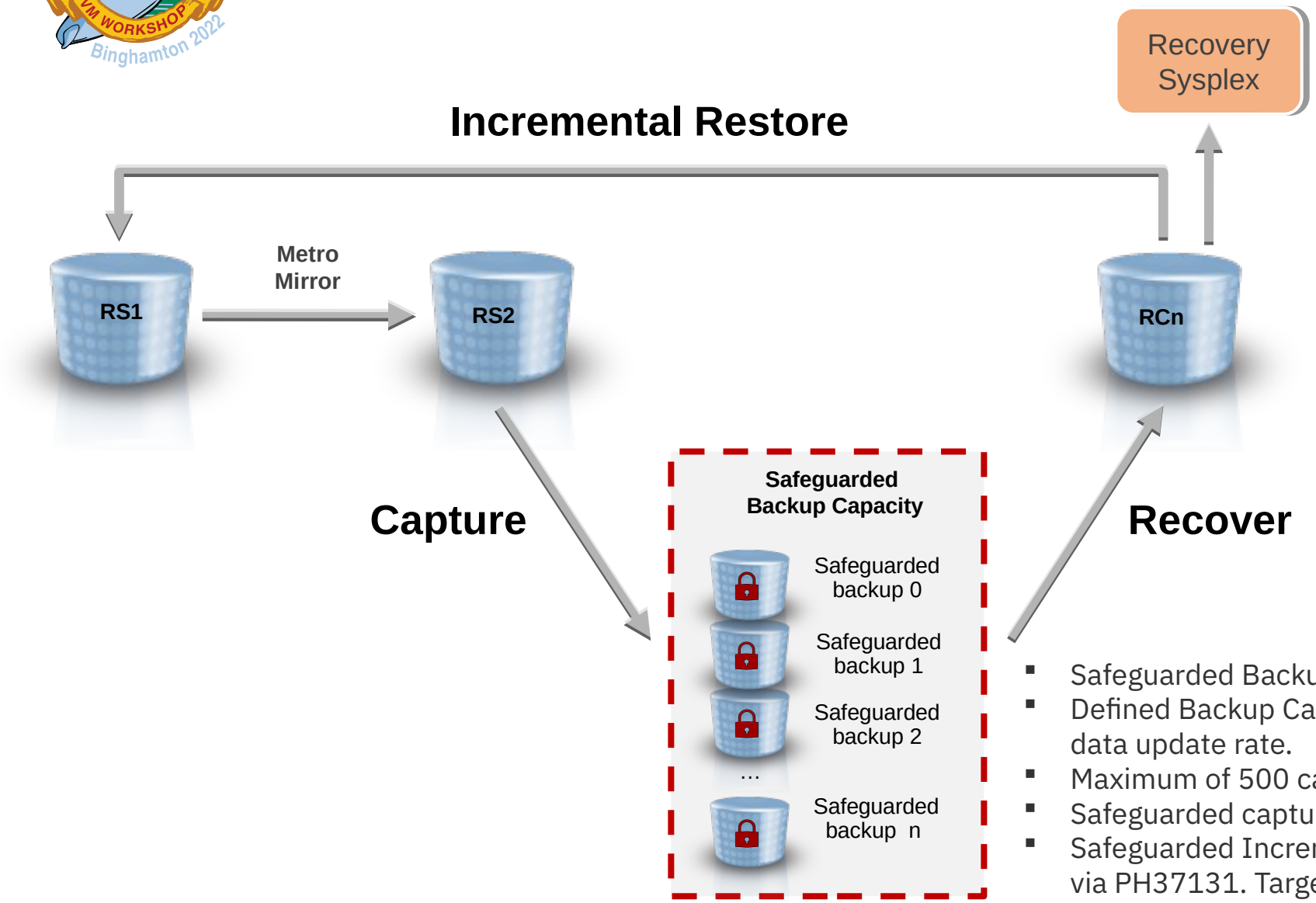




- The protection copies are created in one or more storage systems in the existing HA and DR topology.
- The storage systems typically reside in the same SAN and TCP/IP network as the production environment.
- **Potential performance impact during the capture process.**

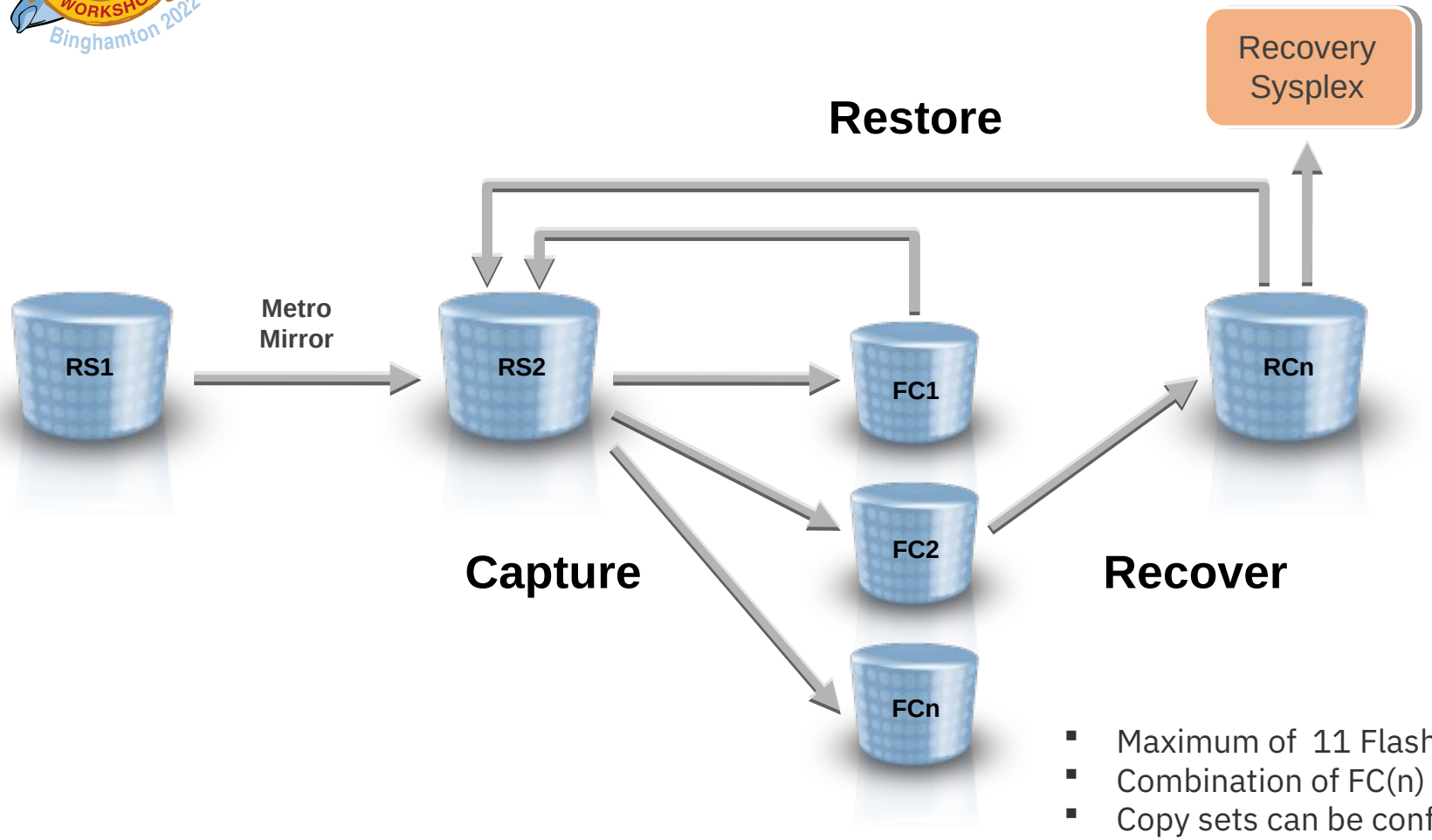
- Additional storage systems are used for the protection copies.
- The storage systems do not typically reside in the same SAN or TCP/IP network as the production environment.
- The storage systems have restricted access and even different administrators to provide separation of duties.
- **No performance impact during the capture process.**

Safeguarded Copy Sets



- Safeguarded Backup Capacity must first be configured on DS8000.
- Defined Backup Capacity should be based on retention period and data update rate.
- Maximum of 500 captures supported.
- Safeguarded captures can be recovered.
- Safeguarded Incremental Restore to Production will be supported via PH37131. Target date November 2021

FlashCopy Copy Sets



- Maximum of 11 FlashCopy sets supported
- Combination of FC(n) and RC(n)
- Copy sets can be configured and captured in both replication sites
- FlashCopy captures can be recovered and restored

Modify a Management Profile

```
VPCPMPMS                Logical Corruption Protection                AZK1

You have requested the modification of an LCP Management profile

Management Profile: GOLD_SGC_RS2          Profile name
 Consistency Group: PRODUCTI              Consistency Group name
  Replication Site: 2                     Replication site number

      Capture Type: SAFEGUARD             SafeGuard capture profile
  Retention Period: MINUTE(1)             Retention period for all captures
  Minimum Interval: MINUTE(1)             Minimum interval between captures
         Copy Set: 1                      Copy set assigned to this profile
  Reservation Time: 0600                  Maximum Reservation Scan elapsed time
     Check In Time: 010                   Maximum Check In elapsed time



Enter NO to cancel or YES to proceed with the profile modification

Selection ===>  yes_

F1=Help  F3=Return
```

Manage Profile name, consistency group, and replication site

Safeguarded Copy or FlashCopy profile

Retention period of LCP captures, days, hours, minutes

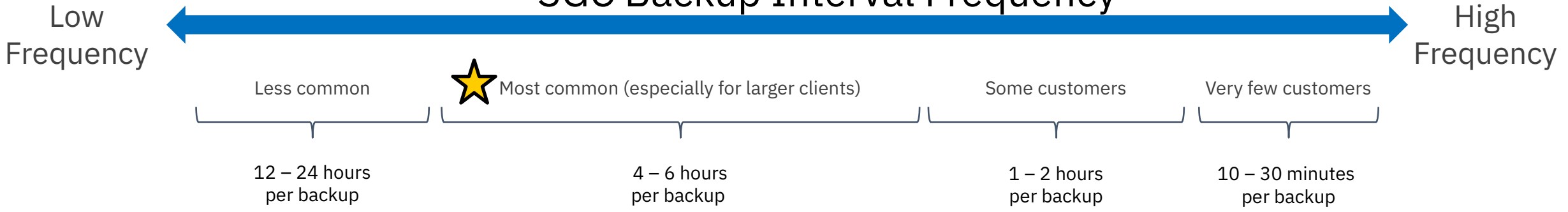
Minimum elapsed time between successive LCP captures

Maximum permissible time for the reservation scan before the LCP Capture is aborted

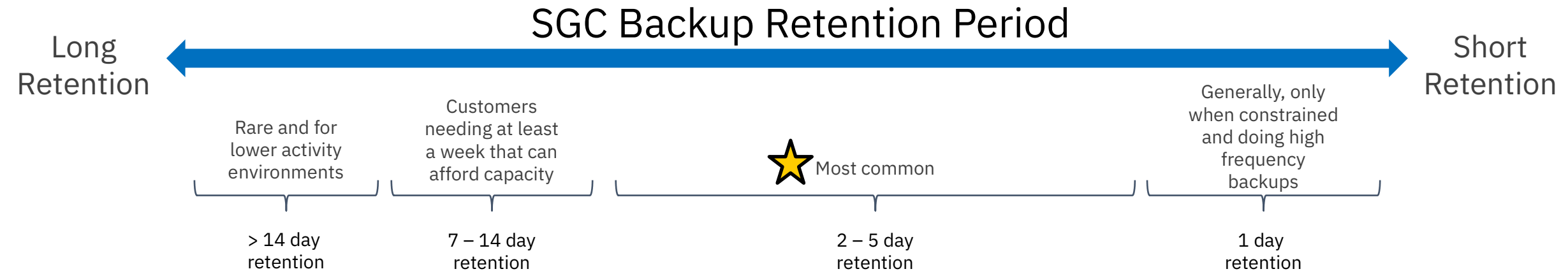
Maximum permissible time for Check In before the LCP Capture is aborted

LCP Capture Frequency

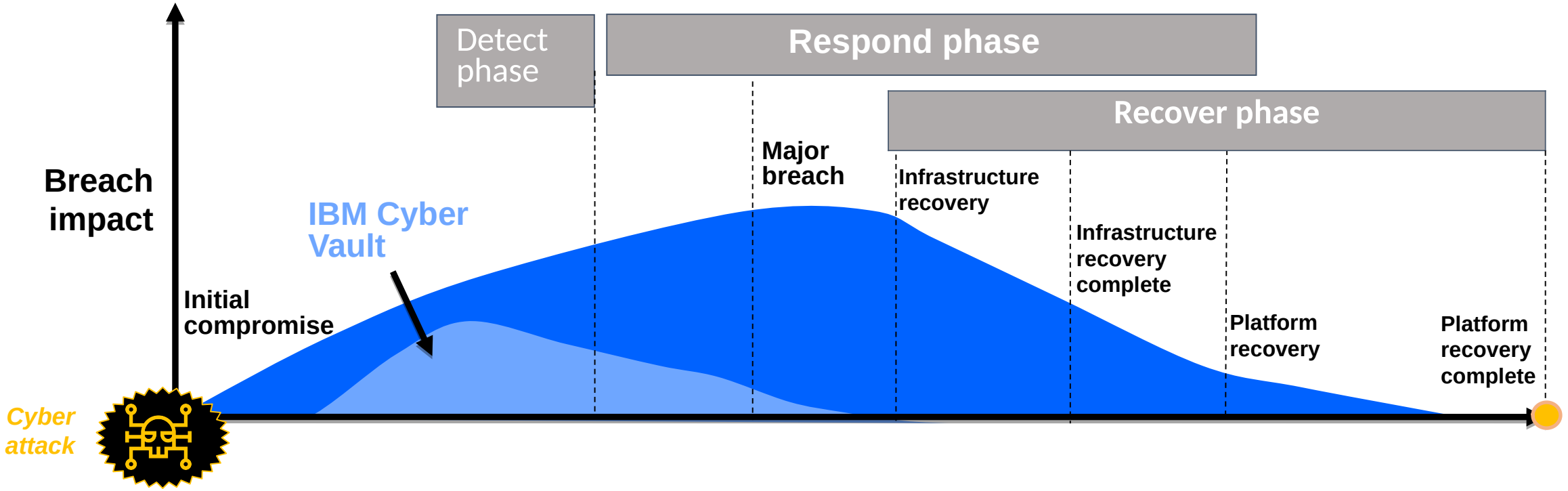
SGC Backup Interval Frequency



SGC Backup Retention Period



Speed recovery to significantly reduce the impact of breaches



Due to the Cyber Vault environment and the use of SafeGuarded Copy technology, data is continuously checked and corruption is found and can be corrected fast. Leading to a shorter impact time.

(c) Copyright IBM 2022

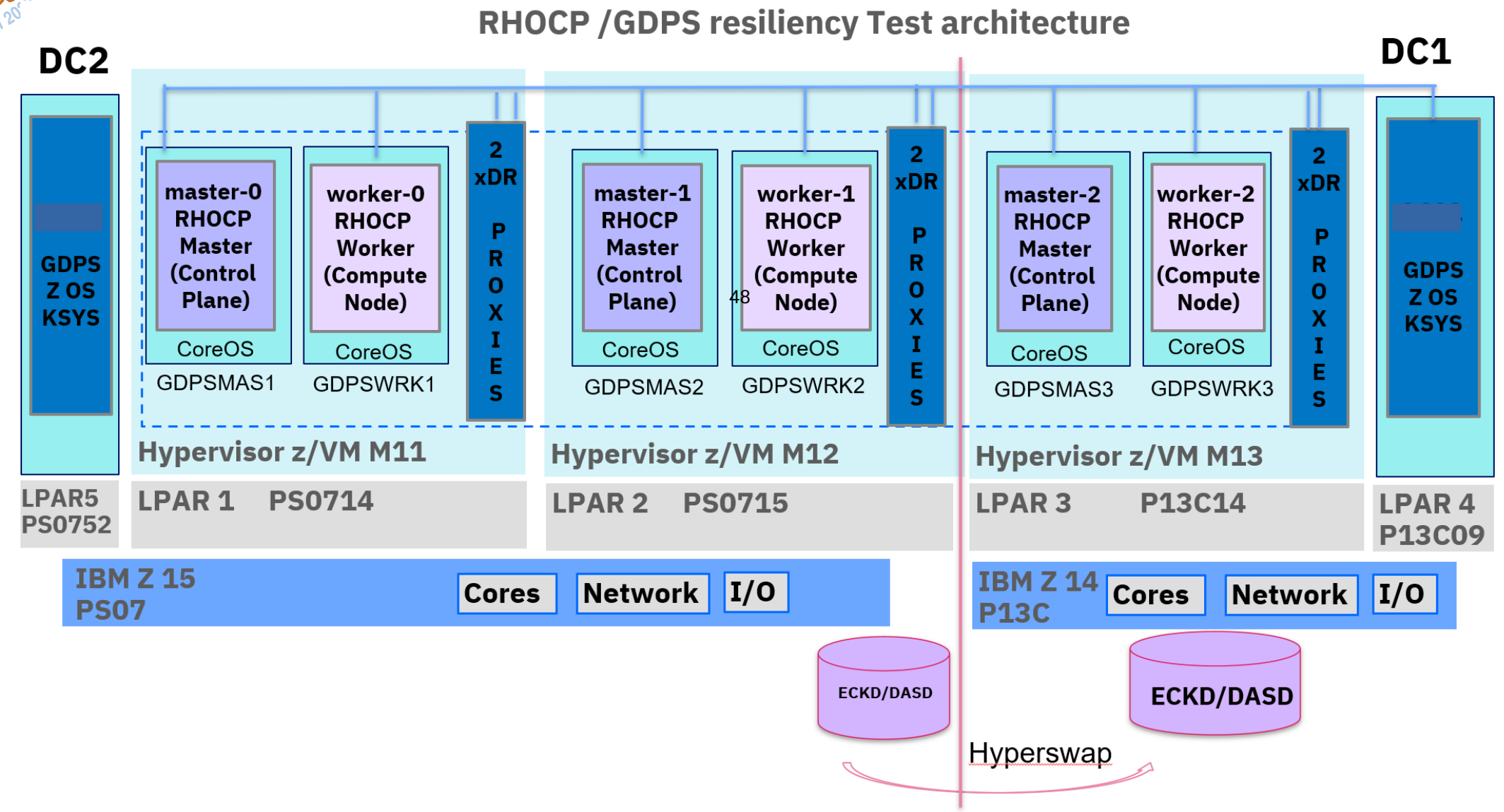
Red Hat OpenShift Container Platform (RHOCP) and GDPS

Red Hat Open Container Platform (RHOCP)

GDPS supports Red Hat OpenShift Container Platform (RHOCP) application environment (Master and Worker nodes) like any z/VM LPAR based application workload.

- **Mirroring of the RHOCP master and worker nodes DASD devices(Metro Mirror)**
- **Stop of a z/VM hosting a master and worker nodes**
- **Re Load of a z/VM hosting a master and worker nodes**
- **Stop of all z/VM hosting the complete RHOCP masters and workers nodes**
- **Live guest relocation of master and worker nodes on another z/VM member (planned maintenance)**
- **Coordinated planned HyperSwap**
- **Coordinated unplanned HyperSwap**
- **Coordinated takeover: unplanned Site failure**
- **Coordinated takeover: planned Site failure**

RHOCP configuration

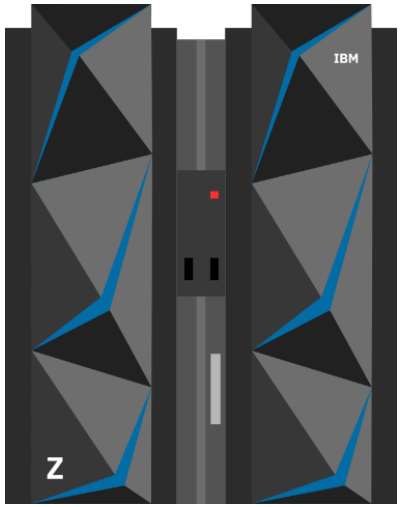


Questions and thank you

Additional information

Web sites:

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



GDPS Web site resources

- GDPS: The Enterprise Continuous Availability / Disaster Recovery Solution white paper
- GDPS pre-requisite information
- GDPS training schedule
- GDPS hardware qualification letters

- e-mail: gdps@us.ibm.com

GDPS™
Providing world class protection