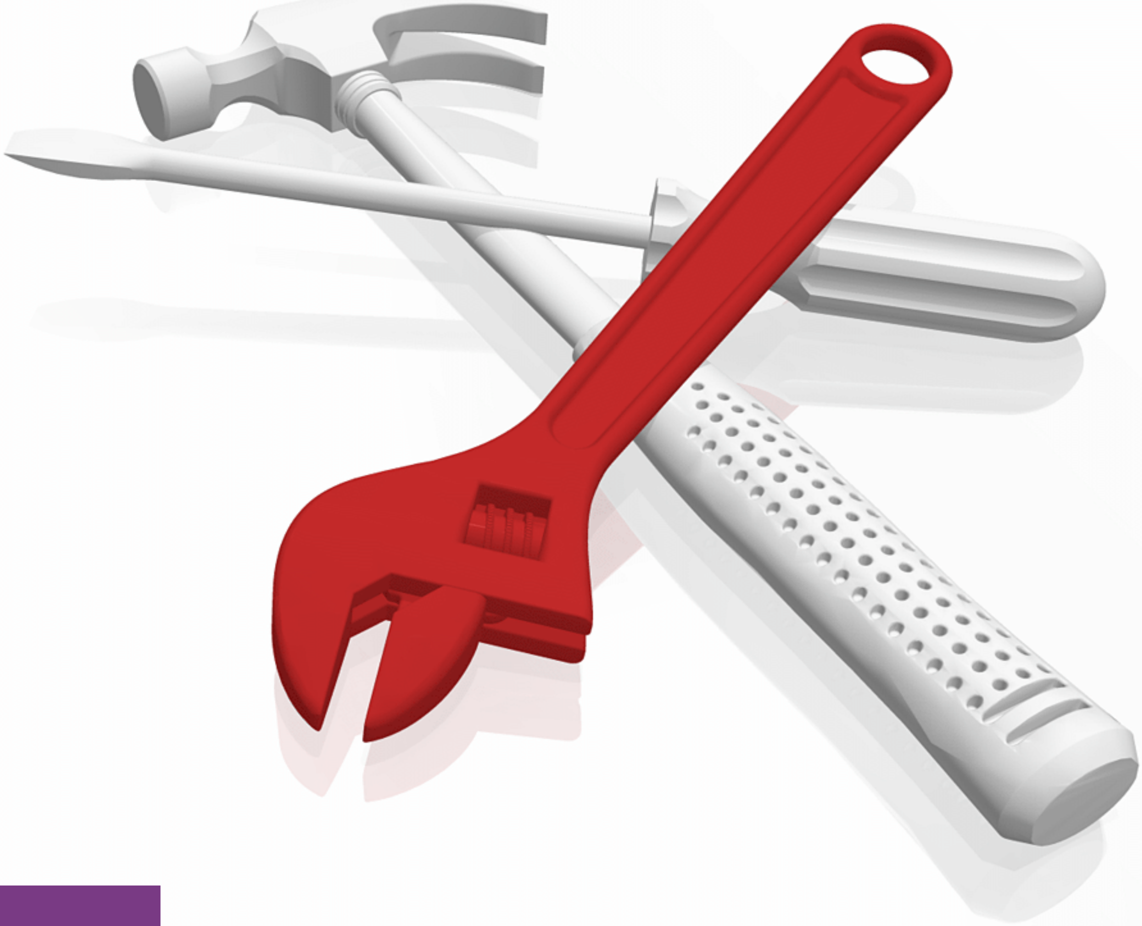
Redbooks
ibm.com/redbooks

IBM Virtual Machine Recovery Manager for IBM Power Cookbook

Dino Quintero
Tim Simon
Felipe Bessa
Shawn Bodily
Carlos Jorge Cabanas Aguero
Vera Cruz
Sachin P. Deshmukh
Dishant Doriwala
Alexander Ducut
Karim El Barkouky
Santhosh S Joshi
Youssef Largou
Juan Prada Diez
Vivek Shukla
Antony Steel
Yadong Yang



Power Systems

IBM
Redbooks

IBM Redbooks

IBM Virtual Machine Recovery Manager for IBM Power Cookbook

August 2023

SG24-8539-00

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

First Edition (August 2023)

This edition applies to the following products:

- Virtual Machine Recovery Manager (VMRM) 1.7
- AIX 7.2.2.1 for the KSYS partition
- AIX 7.3.0.1 for the KSYS partition

Contents

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®
Cognos®
Db2®
DS8000®
FlashCopy®
GDPS®
HyperSwap®
IBM®
IBM Cloud®
IBM FlashSystem®
IBM Spectrum®
IBM Z®
OS/400®
Parallel Sysplex®
POWER8®
POWER9™
PowerHA®
PowerVM®
Redbooks®
Redbooks (logo) ®
Storwize®
SystemMirror®
WebSphere®
XIV®

The following terms are trademarks of other companies:

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Red Hat, OpenShift, RHCSA, are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

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

This IBM Redbooks® publication is designed to give the reader a broad understanding of IBM Virtual Machine Recovery Manager (VMRM). VMRM is a family of solutions that provides high availability and disaster recovery (HADR) management solutions for users of IBM Power servers. The VMRM solutions include the following items:

- VMRM HA provides a single-site, high availability (HA) solution.
- VMRM DR provides a dual-site, disaster recovery (DR) solution.
- VMRM HADR and VMRM HADRHA combine HADR into a single management solution.

Because VMRM is based on virtual machine (VM) recovery, it is operating system-independent, and can provide a solution for any VM running an operating system that is supported by IBM Power.

The publication provides a high-level description of the VMRM solutions that are suitable for management looking for availability solutions for their infrastructure. In addition, it provides in-depth information into the installation, configuration, and management of the solutions, which is designed to help the system administrators that are involved in the installation and management of the solution.

Authors

This book was produced by a team of specialists from around the world working at IBM Redbooks, Austin Center.

Dino Quintero is a Systems Technology Architect with IBM Redbooks. He has 28 years of experience with IBM Power technologies and solutions. Dino shares his technical computing passion and expertise by leading teams developing technical content in the areas of enterprise continuous availability (CA), enterprise systems management, high-performance computing (HPC), cloud computing, artificial intelligence (including machine and deep learning), and cognitive solutions. He is a Certified Open Group Distinguished Technical Specialist. Dino is formerly from the province of Chiriqui in Panama. Dino holds a Master of Computing Information Systems degree and a Bachelor of Science degree in Computer Science from Marist College.

Tim Simon is an IBM Redbooks Project Leader in Tulsa, Oklahoma, US. He has over 40 years of experience with IBM®, primarily in a technical sales role working with customers to help them create IBM solutions to solve their business problems. He holds a Bachelor of Science degree in Math from Towson University in Maryland. He has worked with many IBM products, and has extensive experience creating customer solutions by using IBM Power, IBM Storage, and IBM Z® throughout his career.

Felipe Bessa is an IBM Brand Technical Specialist and Partner Technical Advocate for IBM Power. He works for IBM Technology in Brazil, and has over 25 years of experience in the areas of research, planning, implementation, and administration of IT Infrastructure Solutions. Before joining IBM, he was recognized as a Reference Client for the following solutions: IBM Power Technologies for SAP and SAP HANA, IBM PowerVC, IBM PowerSC, Monitoring and Security, IBM Storage, and Run SAP Like a Factory (SAP Solution Manager) Methodology. He has been elected as an IBM Champion for Power 2018 - 2021.

Shawn Bodily is seven-time IBM Champion for Power and a Senior IT Consultant for Clear Technologies in Dallas, Texas. He has 29 years of IBM AIX® experience, with the last 25 years as a specialist of HADR, primarily focused around IBM PowerHA®. He has written and presented extensively about HA and storage at technical conferences, webinars, and onsite with customers. He is an IBM Redbooks Platinum Author who has co-authored over a dozen IBM Redbooks publications and IBM Redpaper publications.

Carlos Jorge Cabanas Aguero has been a consultant with IBM Technology Lifecycle Services in Argentina for the last 11 years. Before joining IBM, he worked in various roles in the IT industry by supporting AIX and other UNIX solutions. He has extensive experience with supporting AIX and Linux on IBM Power, including HADR solutions and performance tuning.

Vera Cruz is a consultant for IBM Power at IBM ASEAN Technology Lifecycle Services. She has 28 years of IT experience with implementation, performance management, HA and risk assessment, and security assessment for IBM AIX and IBM Power across diverse industries, including banking, manufacturing, retail, and government institutions. She has been with IBM for 8 years. Before joining IBM, she worked for various IBM Business Partners in the Philippines and Singapore by working as a Tech Support Specialist and Systems Engineer for IBM AIX and IBM Power. She holds a degree in computer engineering at the Cebu Institute of Technology University in Cebu, Philippines.

Sachin P. Deshmukh is the Global Power and AIX Platform Lead for Kyndryl, who is based in the US. His area of expertise includes AIX operating system provisioning and support, IBM PowerHA, virtualization, and the IBM Cloud® platform. He provides guidance, oversight, and assistance to global delivery teams supporting Kyndryl accounts. As a member of the Critical Response Team, he works on major incidents and high severity issues. He participates in proactive Technical Health Checks and Service Management Reviews. He interacts with automation, design, procurement, architecture, and support teams for setting delivery standards and creating various best practices documentation. He creates and maintains the AIX Security Technical Specifications for Kyndryl. He is certified on various other platforms, such as Amazon Web Services (AWS) Solutions Architect (Associate), AWS Cloud Practitioner, and Red Hat Certified System Administrator (RHCSA). Before his transition to Kyndryl in 2021, he had been with IBM since 1999. He has been closely associated with IBM AIX and the Power platform for close to 30 years.

Dishant Doriwala is a Senior Staff Software engineer and Test Lead for the VMRM for HADR product. He works in IBM Systems Development Labs (ISDL), Hyderabad, India, and has 10 years of experience in the industry, with expertise in testing HADR products. He has experience on working various HADR solutions, such as IBM PowerHA System Mirror, Reliable Scalable Cluster Technology (RSCT), VMRM, and IBM Geographic Logical Volume Manager (GLVM). He has expertise in enterprise storage, such as IBM SAN Volume Controller and IBM Storwize®, Hitachi, Dell EMC Symmetrix Remote Data Facility (SRDF), and IBM XIV®. He has written white papers, IBM Redpaper publications, and technical articles about HADR. He holds a master's degree in Software Technologies from the International Institute of Information Technology, Pune, and a Bachelor in Electronics and Communications degree from VTU, Bangalore.

Alexander Ducut has been with IBM for 26 years in roles like Brand Technical Specialist, Technical Support, Client Technical Architect, Services Delivery Manager, and Client Technical Manager. He has designed and implemented several complex projects involving IBM servers and IBM Storage with HADR across different industries. He has co-authored three IBM Redbooks publications. He helps clients address their digital transformation initiatives with infrastructure, cloud, and application modernization by using IBM Power solutions.

Karim El Barkouky is a Senior IT Management Consultant who works at MEA - Technology Services- Lab Services. He worked in IBM Systems as L2 remote support as a global PowerHA subject matter expert in Cairo, Egypt. He has 8 years of experience in the IT industry, with expertise in several implementations and consultancy tasks for various HA solutions, such as IBM PowerHA System Mirror, IBM Spectrum Scale, IBM Cluster Aware AIX (CAA), RSCT, GLVM, VMRM, SUSE Linux Enterprise Server - SUSE/HA extension, and container orchestrators like Red Hat OpenShift. He is a recognized trainer that has delivered various IBM AIX and HA training sessions across the MEA Region. He has experience with IBM Power Servers and IBM PowerVM®, PowerVC, PowerSC, and Linux on Power.

Santosh S Joshi is a Senior Staff Software Engineer at the IBM India Systems Development Lab, IBM India. He has over 18 years of experience in the IT field. He works for the IBM PowerVM Live Partition Mobility (LPM) development team. He has worked for IBM VMRM HADR for Power solution development. He holds a Bachelor of Engineering degree in Electronics and Communication from Visvesvaraya Technological University, Belagavi India. His areas of expertise include PowerVM virtualization, HADR solutions, clustering technologies, and storage area networks (SAN)**.**

Youssef Largou is the founding director of PowerM, a Platinum IBM Business Partner in Morocco. He has 21 years of experience in systems, HPC, middleware, and hybrid clouds, including IBM Power, IBM Storage, IBM Spectrum®, IBM WebSphere®, IBM Db2®, IBM Cognos®, IBM WebSphere Portal, IBM MQ, Enterprise Service Bus (ESB), IBM Cloud Paks, and Red Hat OpenShift. He has worked within numerous industries with many technologies. Youssef is an IBM Champion for 2020 - 2022, an IBM Redbooks Gold Author, and designed many reference architectures. He has been an IBM Beacon Award Finalist in Storage, Software-Defined Storage and LinuxONE five times. He holds an engineer degree in Computer Science from the Ecole Nationale Supérieure des Mines de Rabat, and an Excecutif MBA from EMLyon.

Juan Prada is an IBM i Senior System Administrator in Madrid, Spain. He has over 18 years of experience IBM i and its predecessors, IBM Power, IBM OS/400®, IBM i5/OS, and IBM i administration. He has experience with PowerVM Solutions and IBM Storage (IBM DS8000® family, Storwize, IBM SAN Volume Controller, and IBM FlashSystem®). He has worked for IBM Business Partners and customers in the financial and retail sectors.

Vivek Shukla is a Presales Consultant for cloud, AI, and cognitive offerings in India. He is an IBM Certified L2 (Expert) Brand Technical Specialist. He has over 20 years of IT experience in Infrastructure Consulting, AIX, and IBM Power servers and IBM Storage implementations. He has hands-on experience with IBM Power servers, AIX, and system software installations; RFP understandings; statement of work (SOW) preparations; sizing; performance tuning; root cause analysis; DR; and mitigation planning. He has written several IBM Power FAQs, and is the Worldwide Focal for Techline FAQs Flash. He holds a master's degree in Information Technology from IASE University, and a bachelor's degree (BTech) in Electronics & Telecommunication Engineering from IETE, New Delhi. His areas of expertise include Power Enterprise Pools, Red Hat OpenShift, Cloud Paks, and hybrid cloud.

Anthony Steel is a senior technical staff member working with IBM Australia. A research chemist by training, he brings a unique experience and perspective with over 30 years of experience in the IT industry as a programmer, customer, and IBM Business Partner. He spent over 20 years with IBM Australia and IBM Singapore as a Senior Managing Consultant and Advanced Technical Support. Antony’s customers include users, senior management, and other key stakeholders in many industries, including some of the largest financial and business institutions and government departments in Australia, New Zealand, and the Asia Pacific region. He is an IBM Champion who has helped with preparing HA and AIX certification exams.

Yadong Yang is an IBM IT Management Consultant for IBM Power. He works for IBM Technology Services (formerly IBM STG Lab Services) in the US. He has worked for IBM for about 20 years. His expertise includes IBM PowerVM, IBM PowerHA SystemMirror®, VMRM, AIX System Administration, AIX Performance, Linux on Power, IT Infrastructure Architecture, and SAN storage. He has more than 26 years of experience in AIX. He has a Ph. D. degree in Mathematics from North Carolina State University.

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

Srikanth Thannerru, Advisory Software Engineer
VMRM IBM India System Development Labs

Adhish Kapoor, VMRM Developer
IBM India System Development Labs

Jes Kiran Chittigala, HADR Architect for Power VMRM and Master Inventor
IBM India System Development Labs

Abhilash Kadivendi, IBM VMRM
Development Partner, India

Pandi Jai Sree, IBM VMRM
Development Partner, India

Now you can become a published author, too!

Here is 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 LinkedIn:

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

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

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

- Stay current on recent Redbooks publications with RSS Feeds:

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

1

Introducing high availability and disaster recovery

This chapter describes high availability and disaster recovery (HADR), including technologies that are used with clusters to restart the servers. In addition, this chapter introduces the IBM Virtual Machine Recovery Manager (VMRM) for HADR.

The following topics are described in this chapter:

- High availability and disaster recovery overview
- Restart technologies and clustering methods
- Comparing solutions

1.1 High availability and disaster recovery overview

This section provides a high-level overview of HADR topics. It defines the terminology that is used throughout this publication. These definitions might differ from what information that you find on the internet. Generally, the definitions that we present here are commonly accepted.

Availability
The ability of a service component to perform its required function at any instant or over a stated period. It is expressed as the availability ratio, for example, the proportion of time that the service is available for use by the customers within the agreed service hours.

Continuous availability (CA)
The attribute of a system to deliver nondisruptive service to the user 365 days a year, 24 hours a day (assuming no planned or unplanned outages occur).

> **Note:** Usually, high availability (HA) usually means CA.

Figure 1-1 shows the concept of CA as a combination of high availability (HA) and continuous operations.

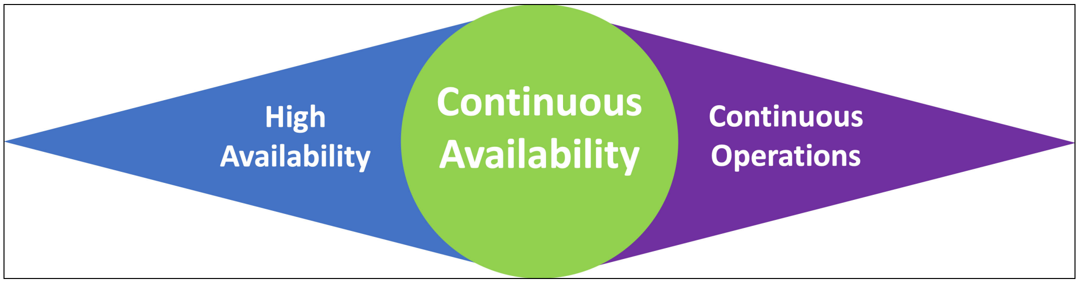


Figure 1-1 Continuous availability (HA and continuous operations)

Continuous operations (CO)
The ability of a system to continuously operate and mask planned outages from users. It uses redundant hardware and software components (often clustering) along with nondisruptive maintenance and change management procedures.

High availability
The ability of a system to provide access to applications regardless of local failures, whether these failures are in the business processes, the physical facilities, or the IT hardware or software. The aim is to mask unplanned outages from users.

Disaster recovery (DR)
The ability to continue processing, with a minimal loss of integrity, of a data center at a different site if a disaster destroys the primary site or otherwise renders it inoperable. A DR solution resumes processing at another site.

Recovery Time Objective (RTO)
Refers to the targeted duration of time between a failure and the point when operations resume.

Recovery Point Objective (RPO) The point at which data is restored if there is a failure or disaster. There might be data loss depending on the data protection or recovery solution that is implemented.

Business Recovery Objective (BRO) The time within which business processes must be recovered, along with the minimum staff, assets, and services that are required within this time.

Network Recovery Objective (NRO) Refers to the maximum time that the network operations can be down for a business.

1.1.1 General concepts

From a service perspective, three concepts exist:

Active/inactive (cold standby) The service is running on one system. One or more physical backup systems exist. Backup systems are not powered on or virtual system definitions are not defined. Only a physical connection to the data exists.

Active/passive (warm standby) The service is running on one system at a time, and one or more backup systems can take over the service. An active OS is running on the backup systems.

Active/active (load-balanced) The same service is running concurrent in multiple systems. The application has simultaneous access to the same data on all systems. In a system failure, all new requests are directed only to the remaining online systems.

An active/active solution requires that the application is aware of the redundant components, but active/passive and active/inactive solutions are exempt from this requirement.

From an operating system or system perspective, two concepts also exist:

Internally managed Commonly called *application-based HA* or *application-based DR*.

Externally managed Commonly called *virtual machine (VM)-based HA* or *VM-based DR*.

Figure 1-2 illustrates these two concepts. Detailed differences are described in the following sections.

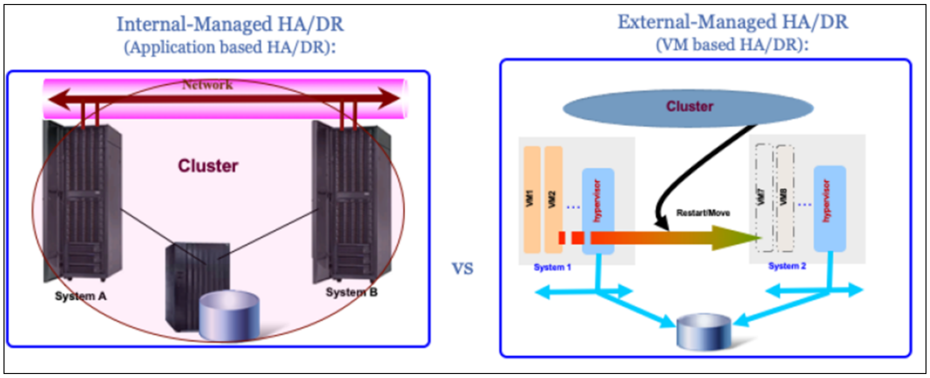


Figure 1-2 Internally and externally managed HADR

Internally managed environment

In an internally managed environment, the operating system or the application has information that it is part of a cluster. Usually, HA components are installed that check whether the cluster partners, hardware, and software components are reachable and available.

Highlights of this environment include the following items:

- Can be used on physical or virtual systems.
- Has a hot-standby topology.
- Is based on independent operating systems.
- The cluster logic is part of the OS or application.
- Rolling migration is possible.
- Supports active/passive and active/active architectures within the cluster.

Externally managed

In an externally managed environment, the operating system is unaware if it is part of a cluster.

Highlights of this environment include the following items:

- Requires a virtual system.
- Has a cold-standby topology.
- Is based on a single operating system.
- The cluster logic is outside of the OS or application.
- Supports only an active/inactive architecture within the cluster.
- Offers reduced license costs.

1.1.2 Outage-related differences

Independent of the selected architecture (internally managed or externally managed), there are two main forms of outages: planned and unplanned.

Planned outages occur when you can schedule an outage for things such as hardware or software maintenance. Sometimes, your availability requirements for an application may allow you to do changes during a regularly scheduled outage period for that application. In other cases, your availability requirements may require you to minimize or remove planned downtime.

Unplanned outages occur when some component in the environment fails and interrupts service to your users, such as hardware failures in the network, servers, or storage devices. Loss of service through an external network also can cause an unplanned outage, so having multiple connections to external networks can minimize this possibility. Other causes might be loss of electrical service, fire, flooding, or other storm damage.

In this section, we describe the differences between internally and externally managed architectures in how they handle planned and unplanned outages.

Planned outages

For planned hardware outages, both internally managed and externally managed environments can limit the time that an application is unavailable for a planned outage.

For hardware maintenance and firmware (FW), both internally managed and externally managed environments can minimize or eliminate outage time. As shown in Figure 1-3 on page 5, an update or upgrade of the underlying hardware or FW can be hidden from the user.

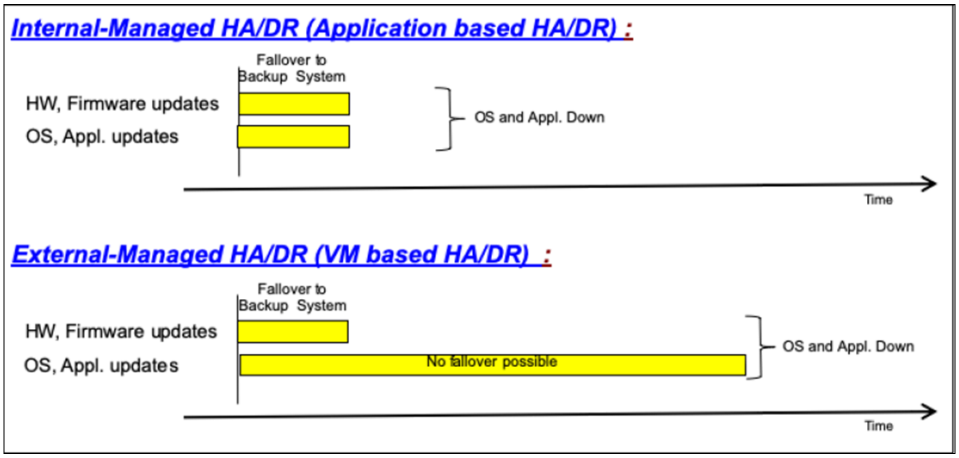

Internal-Managed HA/DR (Application based HA/DR) :
Fallover to Backup System
HW, Firmware updates
OS, Appl. updates
OS and Appl. Down
Time
External-Managed HA/DR (VM based HA/DR) :
Fallover to Backup System
HW, Firmware updates
OS, Appl. updates
No fallover possible
OS and Appl. Down
Time

Figure 1-3 Software and hardware maintenance-dependent action times

The *outage period* is the time that it takes to move to a new hardware environment. You can make the changes on the backup hardware while the application is still running on the production environment. On completion, you can move the production system services to the backup server. Then, you can make the same hardware and FW changes on the production environment, and then move the services back to the original production system.

From a planning point of view, you need two short outages to move services away and back to the production environment, as opposed to a single long outage. Often, when you are using IBM Power servers, it is possible to nondisruptively move the workload between servers by using Live Partition Mobility (LPM), and you can do planned hardware and FW maintenance without an outage. LPM is described in 1.2.1, “Live Partition Mobility” on page 10.

There is a difference between internally managed and externally managed environments when you are doing operating system and application updates.

In an externally managed environment, you need a longer downtime to do an update to the operating systems or application because you have only one operating system and one installation of the application. You cannot hide the whole time that is needed to make the updates from the user, as shown in Figure 1-3.

However, in an internally managed environment, the update of the operating system and application can be hidden from the user like you hid the hardware update from the user because you have multiple, independent installations. The update can be made on the backup system while the application is still running on the current environment, as shown in Figure 1-3, and then the application services can be moved to the backup system while the production system is updated.

Unplanned outages

As shown in Figure 1-4, the unexpected outage of hardware, operating system, or applications can be covered in a similar way for both internally managed and externally managed architectures. This situation is true when the outage is due to a hardware component, an operating system failure, or an application outage.

In an internally managed environment, failure of the operating system or the application code can be partly hidden from the user because there is a standby system with its own operating system where the application can be moved to. What is visible is the fallover time that is needed to restart the application on the backup system, as shown in Figure 1-4.

In an externally managed environment, if the failure of the operating system or the application is the result of corruption of the operating system image or application code, then a simple restart cannot fix the problem. Instead, you must restore your operating system, application code, or both, which might result in a longer outage for your users, as shown in Figure 1-4.

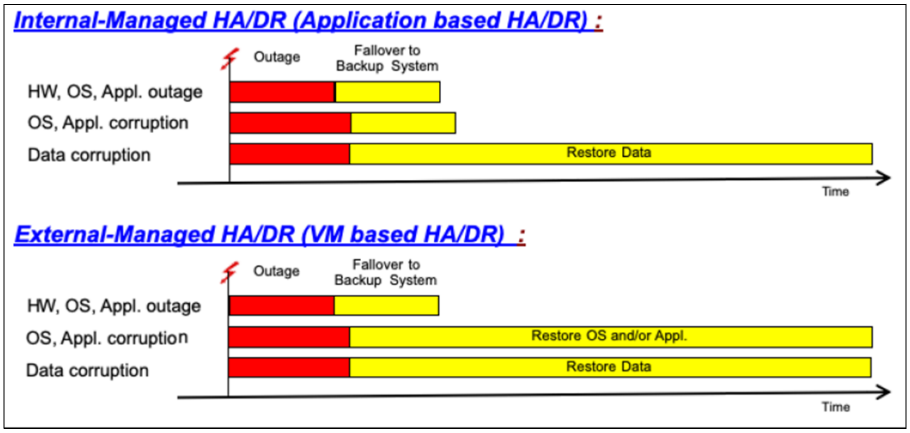


Figure 1-4 Failure-dependent action times

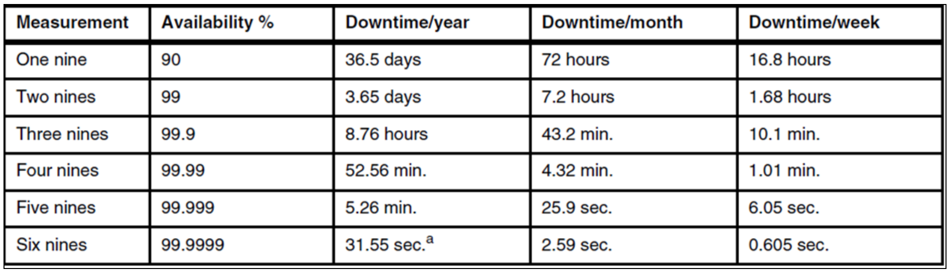
However, if the outage occurs because of, or results in, data corruption, the outage cannot be masked from the user and often the recovery outage is lengthy. This scenario is the worst case because it requires a restore of your data from your backup media. This restoration time can be lengthy, and depending on your backup policies, the recovery point may be old. In this case, the outage time is the same for both internally managed and externally managed environments.

1.1.3 High availability and continuous availability

Usually, when the topic is about HA, it is really about CA. As shown in Figure 1-1 on page 2, CA is the combination of HA and continuous operations. In this section, all references to HA are about CA.

Measuring availability

Often, people measure availability by percentage (%). You might find comments about “three or four 9s” of availability. Figure 1-5 on page 7 shows what these percentage values mean in hours or minutes of downtime.



Measurement	Availability %	Downtime/year	Downtime/month	Downtime/week
One nine	90	36.5 days	72 hours	16.8 hours
Two nines	99	3.65 days	7.2 hours	1.68 hours
Three nines	99.9	8.76 hours	43.2 min.	10.1 min.
Four nines	99.99	52.56 min.	4.32 min.	1.01 min.
Five nines	99.999	5.26 min.	25.9 sec.	6.05 sec.
Six nines	99.9999	31.55 sec.[a]	2.59 sec.	0.605 sec.

Figure 1-5 Availability targets

Although these 9s of availability can provide information about the availability of your environment, they can be misleading. Here is a hypothetical situation in which a customer has the following guidelines:

1. It is acceptable if the system goes offline for 1 hour every day.
2. If the system is down for 8 hours continuously, the company goes bankrupt.

What does this mean in terms of the annual availability percentages?

- For guideline 1, in the worst case scenario, you might have up to 365 hours of outage that the business survives and customers tolerate, even though the annual availability percentage can be as low as 95.833%.
- For guideline 2, you can have an availability level of three nines (99.909%), but if you have a single outage extending to and beyond 8 hours, then the company might still go out of business.

Planning for availability

The two most important items to consider when planning for HADR solutions include RTO and RPO.

RPO How much data may be lost in a failure that is tolerable to the business and can be restored.

RTO Calculated from the time the failure is detected and adds the switch over time to the backup or failover system to the time that is required for the applications to restart and are available for use.

Outage How long until the outage is recognized.

Prepare to repair How long until a decision is made whether a DR situation must be declared.

Repair or failover How long until the original system is repaired or reinstalled, or how long until failover to the backup system is complete.

Minimum service How long until full service is available on the same or different hardware.

Figure 1-6 shows a summary of the major components that are involved in determining what your RPO and RTO will be.

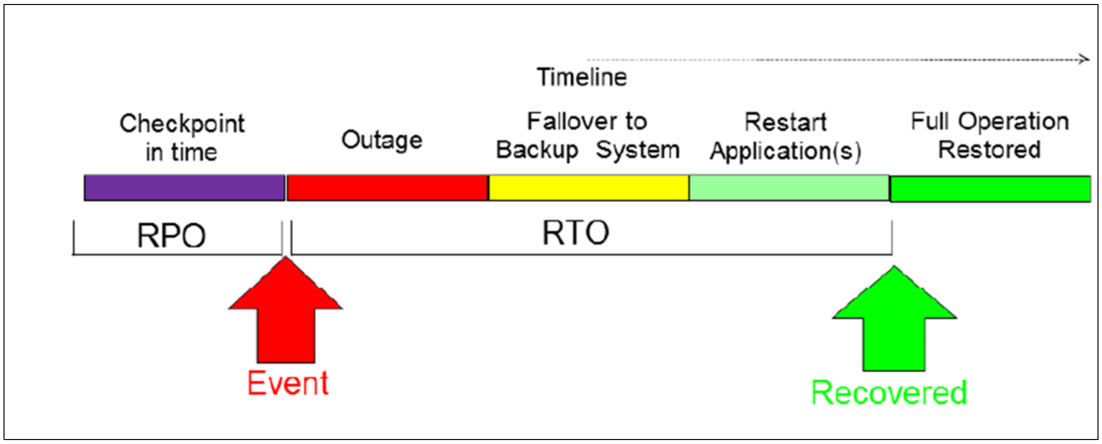


Figure 1-6 Major RPO and RTO components

Here are some other items to consider:

Outage time The amount of time until the outage is detected.

Switch over to backup or failover time The duration of the switchover to the backup or failover system.

Production ready The time to restart the application and services to render the system ready for production.

Depending on the selected solution and the application that you use, these values differ. Choose the solution that meets your business requirements in these areas.

Other considerations for high availability

Several extra items must be considered when planning for a HA environment, as shown in Figure 1-7.

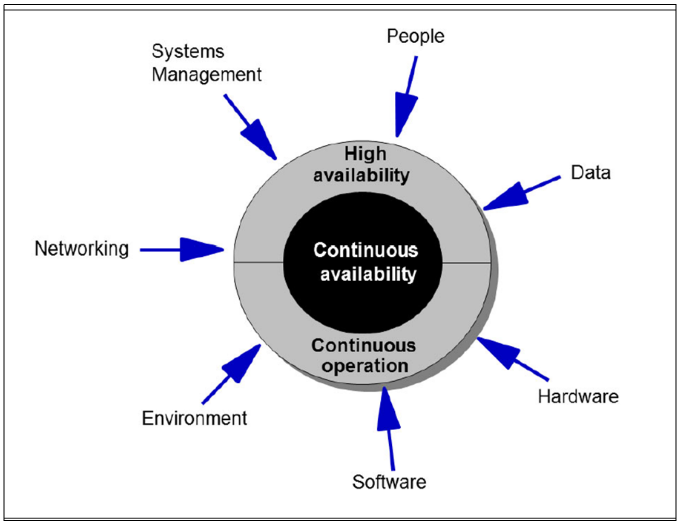


Figure 1-7 Other considerations for continuous availability

Here are the components that are shown in Figure 1-7 on page 8:

People The knowledge and experience of the system administrators managing the environment is important to the overall stability and usability of the availability solution. Recovering operations in a disaster requires people with the correct skills and documentation.

Data An important aspect is that critical data must be redundant (by using a RAID 1, 5, or 6 setup) and backups must exist. If you need to recover quickly in a backup site from a site failure at your primary data center, consider replicating the data to the backup site.

Hardware The hardware must have redundant components and be capable of handling the expected workload. A slow responding system is almost as bad as a downed one.

Software The software (application) must be able to automatically recover after a system crash.

Environment The location of your data center is important. Certain external environmental factors like being close to the coastline or a river implies a risk of flooding. Also, electrical power support must be redundant.

Networking Also important is configuring an internal redundant network that is combined with a redundant internet connection.

Systems management Systems management, especially good change management control, is important. You also must have organized incident and problem management.

1.1.4 Disaster recovery

This section describes some components of DR from an IT perspective. The main purpose of DR is to have a defined and possibly automated procedure for recovery from a major business outage, such as an entire data center outage as the result of a power problem, earthquake, flooding, storm, or other similar uncontrollable circumstances.

Planning for disaster recovery

From a risk assessment perspective, you have the same challenges that are described in “Measuring availability” on page 6.

The RTO and RPO that are achievable for DR are normally different from the RPO and RTO values that you can achieve for HA.

Depending on the selected solution and the application that you use, these values differ.

Other considerations for disaster recovery

A DR solution must consider the items that are described in “Other considerations for high availability” on page 8. In addition, the distance between your data centers is important because it can dictate, or further reduce, the options that are available for DR.

Natural disasters spread across several, even hundreds of kilometers. Therefore, planning for the distance between sites should consider the potential of both sites being impacted by the same catastrophe. The DR site should be selected while considering external environmental factors that can impact its availability.

1.2 Restart technologies and clustering methods

Many technologies and solutions are available for IBM Power to increase logical partition (LPAR) and application availability. In this section, we cover many of these options and highlight which solution is best suited to which environment.

1.2.1 Live Partition Mobility

LPM is a component of the PowerVM Enterprise Edition hardware feature that can move AIX, IBM i, and Linux LPARs from one physical system to another one. The mobility process transfers the entire system environment, which includes the processor state, memory, attached virtual devices, and connected users.

Active partition mobility moves AIX, IBM i, and Linux LPARs that are running, including the operating system and applications, from one system to another one. The LPAR and its applications do not need to be shut down, so there is no outage time.

Inactive partition mobility moves a powered-off AIX, IBM i, or Linux LPAR from one physical system to another one.

Partition mobility provides systems management flexibility, and it is designed to improve system availability. For example:

- You can avoid planned outages for hardware or FW maintenance by migrating LPARs to another server. Partition mobility can help because you can use it to work around scheduled maintenance activities.
- You can avoid downtime for a server upgrade by migrating LPARs to another server and then performing the upgrade.
- If a server indicates a potential failure, you can migrate its LPARs to another server before the failure occurs. Partition mobility can help avoid unplanned downtime if the error is caught soon enough.
- You can consolidate workloads running on several small servers onto a single, larger server.
- You can move workloads from server to server to optimize resource utilization and workload performance within your computing environment. With active partition mobility, you can manage workloads with minimal downtime.
- For some systems, applications can be moved from one server to an upgraded server by using IBM PowerVM Editions LPM or the AIX Live Application Mobility software without affecting the availability of the applications.

However, although partition mobility provides many benefits, it does not provide the following functions:

- Automatic workload balancing.
- A bridge to new functions. Often, LPARs must be restarted and possibly reinstalled to leverage new features.

When an LPAR is moved by using LPM, a profile is automatically created on the target server that matches the profile on the source server. Then, the partition's memory is copied asynchronously from the source system to the target server, which creates a clone of a running partition. Memory pages that changed on the partition (“dirty” pages) are recopied. When a threshold is reached that indicates that enough memory pages were successfully copied to the target server, the LPAR on that target server becomes active, and any remaining memory pages are copied synchronously. Then, the original source LPAR is automatically removed.

Because the Hardware Management Console (HMC) always migrates the last activated profile, an inactive LPAR that has never been activated cannot be migrated. For inactive partition mobility, you can either select the partition state that is defined in the hypervisor or select the configuration data that is defined in the last activated profile on the source server.

There are many prerequisites that must be met before an LPAR can be classified as LPM ready. The source and destination systems must be configured correctly so that you can successfully migrate the mobile partition from the source system to the destination system. Verify the configuration of the source and destination servers, the HMC, the Virtual I/O Server (VIOS) LPARs, the mobile partition, the virtual storage configuration, and the virtual network configuration.

For more information about preparing for partition mobility, see Preparing for mobile partitions.

In addition to the minimum required FW, HMC versions, and VIOS versions, the high-level prerequisites for LPM include the following items:

- The LPAR to be moved can be in an active or inactive state.
- The source and target systems must be in an active state.
- The source and target systems VIOSs that provide the I/O for the LPAR must be active.
- The source and the target systems must have a VIOS that is marked as the mover service partition (MSP).
- The source and target MSPs must be active.
- Resource Monitoring and Control (RMC) network communication must exist between the mobile partitions, service processor, and the MSPs.
- The logical memory block (LMB) size must be the same on the source and the target systems.
- The target system must have enough resources (processors and memory) to host the partition.
- The target system VIOSs must provide the same networks that are used by the LPAR.
- The source and the target system VIOSs must both be able to see all the LPARs’ storage logical unit numbers (LUNs).
- If there are physical I/O devices that are attached to the partition, they must be removed from the partition before it can be moved.
- For IBM i partitions, the restricted I/O partition cannot be set.

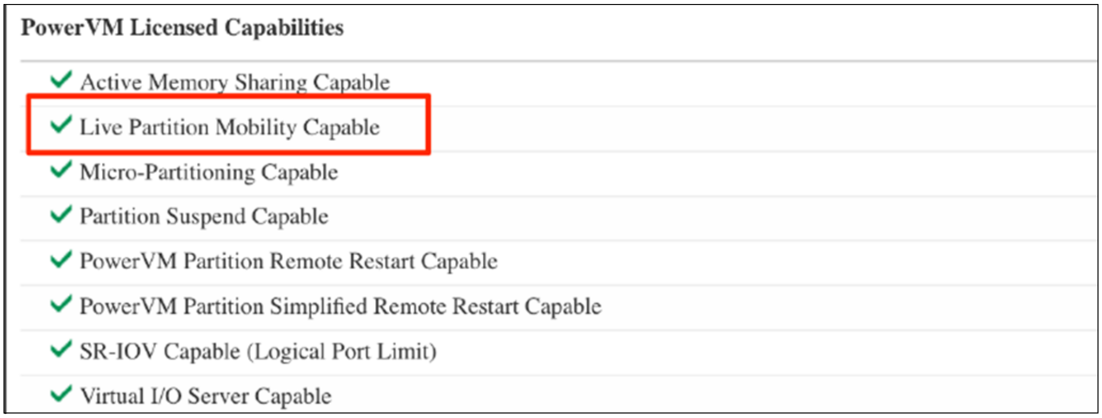
You can use the HMC command **`miglpar`** or the GUI to validate whether an LPAR is LPM-capable without performing the actual migration. For more information, see Configuration validation for partitions.

Initiating LPM can be performed by using the HMC GUI, the HMC command-line interface (CLI), IBM Power Virtualization Center (IBM PowerVC), IBM Lab Services LPM Automation Toolkit, or the VMRM. However, there are some restrictions:

- The HMC GUI can initiate only a single LPM migration at a time.
- The HMC CLI can initiate only a single LPM migration at a time, unless scripted.
- IBM PowerVC can initiate only a single LPM migration at a time, unless frame evacuation is used.
- IBM PowerVC cannot migrate inactive LPARs.

You can confirm whether an IBM Power server is licensed for LPM by going to the HMC and selecting **Resources** → **All Systems System Name** → **Licensed Capabilities**.

Figure 1-8 shows a Power server that is LPM-capable.



PowerVM Licensed Capabilities

✓ Active Memory Sharing Capable
✓ Live Partition Mobility Capable
✓ Micro-Partitioning Capable
✓ Partition Suspend Capable
✓ PowerVM Partition Remote Restart Capable
✓ PowerVM Partition Simplified Remote Restart Capable
✓ SR-IOV Capable (Logical Port Limit)
✓ Virtual I/O Server Capable

Figure 1-8 PowerVM Live Partition Mobility Capable

1.2.2 Simplified Remote Restart

Simplified Remote Restart (SRR) is a component of the PowerVM Enterprise Edition hardware feature that can restart AIX, IBM i, and Linux LPARs on a different physical server if the original server is no longer active. If the original physical server (source) has an error that causes an outage, you can restart the LPARs on another (target) server.

If the source server has a physical fault that requires fixing, then you can use SRR to recover the key LPARs more quickly. After a failure, you can use SRR for fast reprovisioning of the partition, which might take less time than waiting for the original server to restart and then restarting the partition.

SRR is available starting with any IBM POWER8® or later Power processor-based systems that use FW level 8.2.0 or later and HMC 8.2.0 or later. Compared to previous options, SRR removes the need to use a reserved storage device that is assigned to each partition. It is a best practice to use SRR where possible.

Here are the characteristics of SRR:

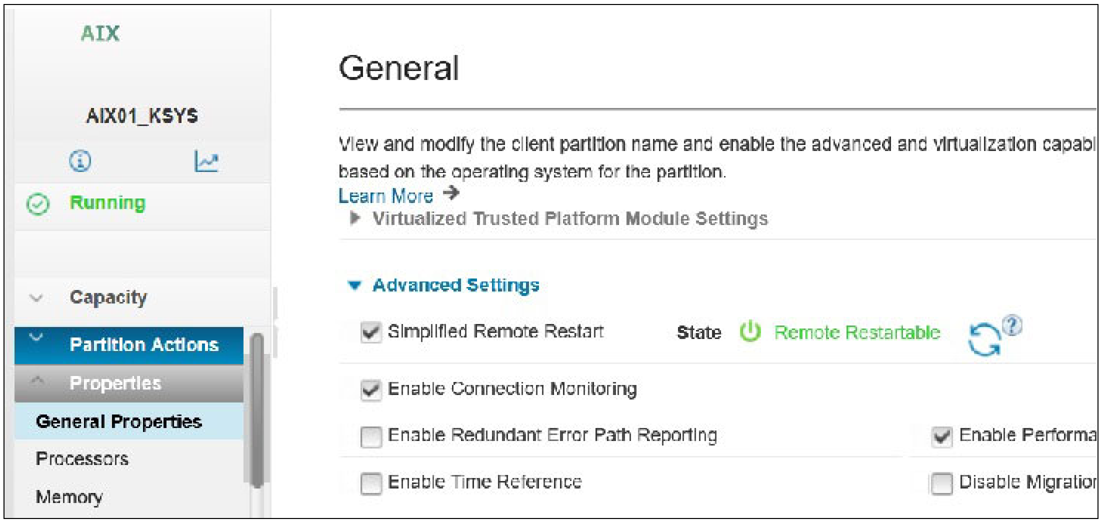
- SRR is not a suspend and resume or migration operation of the partition that preserves the active running state of the partition. It is a restart operation, and during the remote restart operation, the LPAR is shut down and then restarted on the target system.
- SRR preserves the resource configuration of the partition. If processors, memory, or I/O are added or removed while the partition is running, the remote restart operation activates the partition with the most recent configuration.
- When an LPAR is restarted by using SRR, a new profile is automatically created on the target server that matches the profile on the source server. Then, that new profile is mapped to the storage LUNs that were being used by the original partition (the partition is inactive). Then, the new profile on the target server is activated, and the partition is again active.

As with LPM, there are some prerequisites that must be met for SRR to work. However, if a partition is LPM-capable, then it is SRR-capable.

Other than the minimum required FW, HMC versions, and VIOS versions, the high-level SRR prerequisites include the following items:

- The source system must be in a state of Initializing, Power Off, Powering Off, No connection, Error, or Error - Dump in progress.
- The source systems VIOSs that provide the I/O for the LPAR must be inactive.
- The target system must be in an active state.
- The target systems VIOSs that provide the I/O for the LPAR must be active.
- The LPAR that is restarted must be in an inactive state.
- The LMB size is the same on the source and the target systems.
- The target system must have enough resources (processors and memory) to host the partition.
- The target system VIOSs must provide the networks that are required for the LPAR.
- The source and the target systems VIOSs must both see all the LPARs' storage LUNs.
- All physical I/O devices must be removed from the partition before it can be moved.
- For IBM i partitions, the restricted I/O partition cannot be set.

For an LPAR to perform a remote restart operation, you must set a flag against it by using the HMC. It is possible to view and set this flag dynamically by using the HMC by selecting **LPAR General Properties** → **Advanced Settings** → **Simplified Remote Restart**, as shown in Figure 1-9.



General

View and modify the client partition name and enable the advanced and virtualization capabl
based on the operating system for the partition.

Learn More →

▸ Virtualized Trusted Platform Module Settings

▾ Advanced Settings

☑ Simplified Remote Restart State Remote Restartable

☑ Enable Connection Monitoring

□ Enable Redundant Error Path Reporting ☑ Enable Performa

□ Enable Time Reference □ Disable Migratior

Figure 1-9 SRR option setting

HMC 9.1.910.0 enhancements

In HMC V9 R1.910.0, many SRR enhancements were announced:

- Remote restart a partition with reduced or minimum CPU or memory on the target system.

  When a system outage occurs and you want to restart all the partitions on another system, the target system might not have enough capacity to host all the partitions. If some specific partitions such as development or test workloads can be run with reduced resources, then it is now possible to restart partitions on the target system with fewer memory and processor resources than were available on the original host system.

- Remote restart by choosing a different virtual switch on the target system.

  You can validate or perform the remote restart operation for an LPAR when you want to start the LPAR with a different virtual switch on the target server than the virtual switch assigned on the source server.

- Remote restart the partition without powering on the partition on the target system.

  With this option, you can prevent an LPAR from being started during the remote restart operation. You can use this option in cases where you want to check the configuration on the target system before powering on the partition. All other steps are performed during a remote restart operation except for powering on the partition.

- Remote restart the partition for test purposes when the source-managed system is in the Operating or Standby state.

  Remote restart is supported when a system has failed. If you want to validate whether a remote restart operation works in a system failure, you can use the validate option. However, if you want to go one step further and test restarting the partition on another system, use the test option. The source partition must be in the shutdown state to use the test option for remote restart.

- Display the partition configuration information.

  HMC collects and persists the configuration data that is required for restarting a partition. You can use the **`lsrrstartlpar`** command to view the persisted configuration information of all the LPARs that support SRR.

- Remote restart by using the Representational State Transfer (REST) application programming interface (API).

  You also can perform the remote restart operation by using the REST API. The REST API can be reached at the following URL:

  ```
  https://<<HMCIP>>:12443/rest/api/uom/ManagedSystem/<ManagedSystem_UUID>LogicalPartition/<<PARTITION_UUID>>/do/RemoteRestart
  ```

  `<<HMCIP>>` is the IP address of your HMC.

  All options and overrides are added to the REST API.

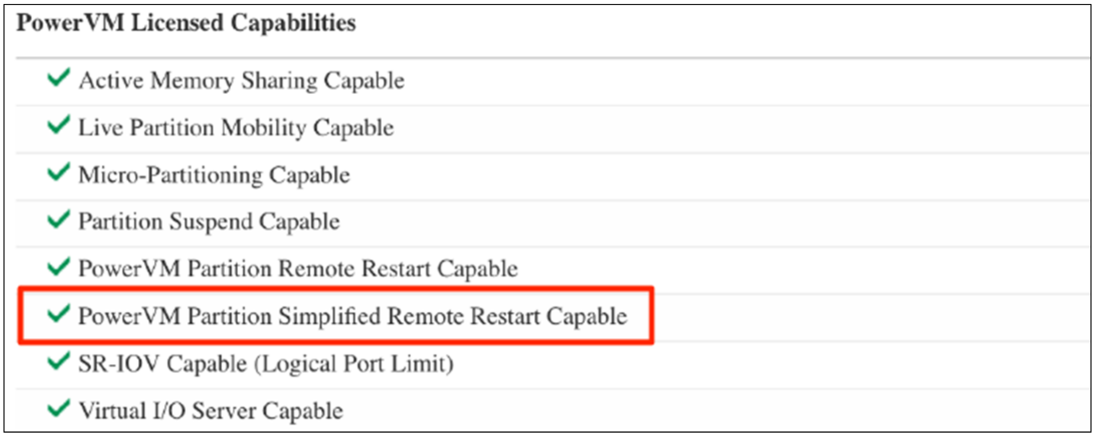
Controlling Simplified Remote Restart

You can initiate SRR by using the HMC CLI, REST APIs, IBM PowerVC, IBM Lab Services LPM and SRR Automation Toolkit, or VMRM. However, there are limitations:

- The HMC GUI cannot be used to initiate partition restarts with SRR.
- The HMC CLI (**`rrstartlpar`**) can initiate only a single partition restart with SRR.
- Only up to 32 concurrent SRR operations can occur for a destination server (including concurrent **`rrstartlpar`** commands).
- IBM PowerVC can initiate a single partition restart or an entire frame restart, but not a subset of SRR-capable partitions.
- IBM PowerVC can optionally be configured to automatically start SRR for all SRR capable partitions on a failed server.

You can confirm whether an IBM Power server is licensed for SRR by opening the HMC and selecting **Resources** → **All Systems** → **System Name** → **Licensed Capabilities**, as shown in Figure 1-10.

For more information, see Remotely restarting a logical partition.



PowerVM Licensed Capabilities

✓ Active Memory Sharing Capable
✓ Live Partition Mobility Capable
✓ Micro-Partitioning Capable
✓ Partition Suspend Capable
✓ PowerVM Partition Remote Restart Capable
✓ PowerVM Partition Simplified Remote Restart Capable
✓ SR-IOV Capable (Logical Port Limit)
✓ Virtual I/O Server Capable

Figure 1-10 PowerVM Simplified Remote Restart capability

1.2.3 VMRM

VMRM is an automated solution that implements recovery of your partitions by using restart technology. VMRM relies on an out-of-band monitoring and management component that restarts the VMs on another server when the host infrastructure fails. The requirements for moving partitions with VMRM are similar to what is required for SRR.

There are multiple deployment options that are provided by VMRM. Depending on your requirements, VMRM can provide a HA solution within a single site or two sites within metro distances by using VMRM HA. To support your DR requirements across sites that are farther apart, VMRM DR provides a solution for managing workloads between your production or primary site and your secondary (backup) or DR site. For customers that want more flexibility on where the workloads are recovered, two more options are supported: HADR and HADRHA. These options are introduced in this section. For more information, see Chapter 2, “IBM VMRM architecture and components” on page 21.

As with the other partition restart technologies that we have described in this chapter, VMRM should be differentiated from a clustering technology that deploys redundant hardware and software components for a near real-time failover operation when a component fails. The full clustering solution for IBM Power solutions is IBM PowerHA SystemMirror, which is described briefly in 1.2.4, “IBM PowerHA SystemMirror” on page 17.

The VMRM HA solution is ideal to ensure HA for many VMs, and if it meets your RPO requirements, it is simpler to manage than cluster environments because it does not have the complexities of clustering. Because VMRM HA is based on SRR technology, it is OS-independent and can be used with IBM AIX, IBM i, or Linux. This simplified management capability is extended to a second site for DR solutions by using VMRM DR. The additional options of VMRM HADR and VMRM HADRHA are extensions and combinations of the VMRM HA and VMRM DR solutions to provide integrated HADR capabilities.

VMRM HA

HA management is a critical feature of business continuity plans. Any downtime to the software stack can result in loss of revenues and disruption of services. VMRM HA for Power is a HA solution that is easy to deploy, and provides an automated solution to recover the VMs, also known as LPARs.

The VMRM HA solution implements recovery of the VMs based on the VM restart technology (SRR). The VM restart technology relies on an out-of-band monitoring and management component that restarts the VMs on another server when the host infrastructure fails. The VM restart technology is different from the conventional cluster-based technology that deploys redundant hardware and software components for a near real-time failover operation when a component fails.

The VMRM HA solution is ideal to ensure HA for many VMs. Also, the VMRM HA solution is easier to manage because it does not have clustering complexities.

VMRM DR

DR of applications and services is a key component to provide continuous business services. The VMRM DR for Power solution is a DR solution that is simple to deploy and provides automated operations to recover the production site. The VMRM DR solution is based on the IBM Geographically Dispersed Parallel Sysplex® (IBM GDPS®) offering concept that optimizes the usage of resources. This solution does not require the deployment of backup VMs for DR, so the VMRM DR solution reduces the software license and administrative costs.

The VMRM DR solution is based on the VM restart technology across two sites. The VM restart-based HADR solution relies on an out-of-band monitoring and management component (provided by VMRM DR) that restarts the VMs on other hardware when the host infrastructure fails.

VMRM HADR

VMRM HADR provides more HA features in addition to the VMRM DR solution. This solution provides more flexibility about where your applications can run after a failure recovery by supporting the recovery of your applications at your primary and secondary sites.

The important HA features of the HADR type of deployment of the VMRM DR solution include the following ones:

- LPM support within a site
- Support for VM failure and host failure within a site
- Application failover support within a site
- Fibre Channel (FC) adapter failure within a site
- Network adapter failure within a site
- Monitoring CPU and memory usage within a site
- Move operation and failover rehearsal operation across sites and within a site
- DR support from one site to another site

VMRM HADRHA

The VMRM HADRHA solution adds extra HA features to the VMRM DR solution and the VMRM HADRR solution. The HADRHA solution allows recovery of your applications within the same site at both the primary site and the secondary site.

The important HA features of the HADR type of deployment of the VMRM DR solution includes the following ones:

- LPM support within a site
- Support for VM failure and host failure within a site
- Application failover support within a site
- FC adapter failure within a site
- Network adapter failure within a site
- Monitoring CPU and memory usage within a site
- Move operation and failover rehearsal operation across sites and within a site
- DR support from one site to another site

1.2.4 IBM PowerHA SystemMirror

IBM PowerHA SystemMirror for AIX and IBM i are separate, licensed products that provide HA clusters on IBM Power servers. There was also an edition for Linux, but it has been withdrawn.

A PowerHA cluster must contain a minimum of two LPARs (called nodes) that communicate with each other by using heartbeats and keepalive packets. The cluster contains many resources, such as IP addresses, shared storage, and application scripts, which are grouped to form a resource group.

If PowerHA detects an event within the cluster, it automatically acts to ensure that the resource group is placed on the most appropriate node in the cluster to ensure availability. A correctly configured PowerHA cluster after setup requires no manual intervention to protect against a single point of failure. These failures include:

- Physical servers
- Nodes
- Applications
- Adapters
- Cables
- Ports
- Network switches
- Storage area network (SAN) switches

The cluster can be controlled manually if the resource groups must be balanced across the clusters or moved for planned outages.

PowerHA Enterprise Edition also provides cross-site clustering where shared storage is unavailable but data replication, either SAN or IP-based, is available. In this environment, PowerHA uses the remote copy facilities of the storage controllers to ensure that the nodes at each site have access to the same data, but on different storage devices. It is possible to combine both local and remote nodes within a PowerHA cluster to provide local HA along with cross-site DR.

Clusters within PowerHA can be configured in many ways:

Active/Passive: One node in the cluster runs the resource group, and its partners are in standby mode waiting to take on the resources when required. The passive nodes in the cluster must be running for them to participate in the cluster. Although the standby nodes do not have to have the full processor and memory allocation when in passive mode, they must still be active.

Active/Active: All nodes in the cluster are running a resource group, but also are the standby node for another resource group in the cluster. Many resources groups can be configured within a cluster, so how they are spread out across the nodes and in which order they move is highly configurable. This configuration is also referred to as *mutual takeover*.

Concurrent: All nodes in the cluster run the same resource group.

For more information about IBM PowerHA SystemMirror for AIX, see *IBM PowerHA SystemMirror for AIX Cookbook*, SG24-7739. For more information about IBM PowerHA SystemMirror for i, see *IBM PowerHA SystemMirror for i: Preparation (Volume 1 of 4)*, SG24-8400.

1.3 Comparing solutions

In 1.2, “Restart technologies and clustering methods” on page 10, we described LPM, SRR, VMRM, and PowerHA, which are all different solutions that each have their own advantages and disadvantages. In this section, we show where each solution fits in terms of providing HA or DR for applications running on your IBM Power servers. We also highlight where solutions are not appropriate for your environment.

Ease of use

Both LPM and SRR are relatively simple to configure and use. Although this book does not describe how to enable a VM to be LPM- and SRR-ready, this task can be performed in a few simple steps and your success verified online. Both LPM and SRR are included in IBM PowerVM Enterprise Edition, so no extra software licenses or costs are required.

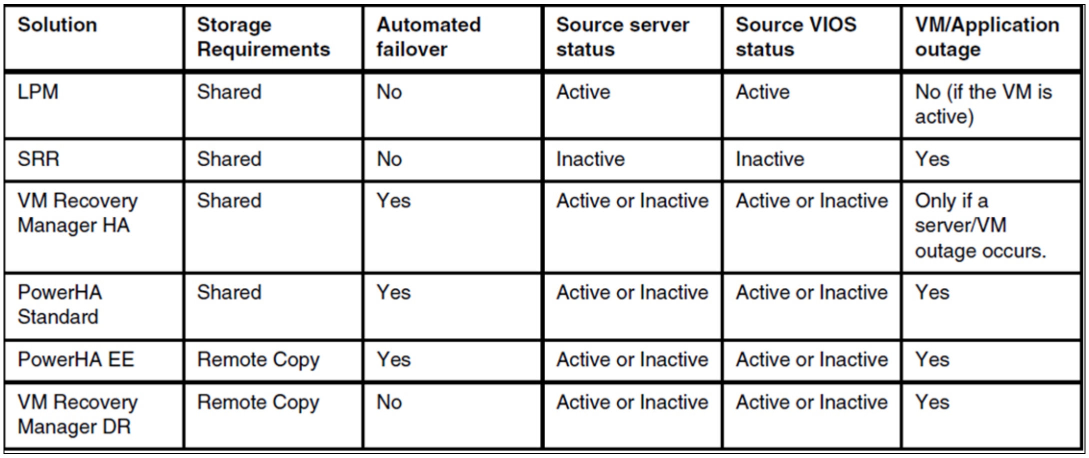
IBM PowerHA is a more complex product to set up because it requires a license and you must install the cluster code on all nodes in the cluster. It also requires an experienced IBM PowerHA consultant to design, implement, and maintain a successful cluster.

VMRM HA is simpler to configure than IBM PowerHA, but relies on LPM and SRR being configured to function correctly.

Availability, recovery times, and recovery points

LPM, SRR, VMRM HA, and standard PowerHA must have connectivity to the same shared storage to work successfully. In all these cases, the recovery points must be the same. For VMRM DR and cross-site PowerHA Enterprise Edition, storage replication is needed, and the recovery point depends on how storage replication is configured.

The key differentiators in this section are availability and recovery times, as shown in Figure 1-11. You can see how each product differs in terms of storage requirements, automation, server status, and outages.



Solution	Storage Requirements	Automated failover	Source server status	Source VIOS status	VM/Application outage
LPM	Shared	No	Active	Active	No (if the VM is active)
SRR	Shared	No	Inactive	Inactive	Yes
VM Recovery Manager HA	Shared	Yes	Active or Inactive	Active or Inactive	Only if a server/VM outage occurs.
PowerHA Standard	Shared	Yes	Active or Inactive	Active or Inactive	Yes
PowerHA EE	Remote Copy	Yes	Active or Inactive	Active or Inactive	Yes
VM Recovery Manager DR	Remote Copy	No	Active or Inactive	Active or Inactive	Yes

Figure 1-11 Solutions comparison matrix

For example, if you start with LPM, the source and targets servers (and their VIOSs) must be running and active. Although the VM that you want to move can be offline, the server it is hosted on must be online. If this criterion is met, then using LPM on an active VM does not result in any downtime. If that VM crashes, LPM does not automatically restart the VM or migrate it to another server because manual intervention is required. Therefore, for applications and VMs where a basic form of planned HA is required, using only LPM might be sufficient. However, it is not sufficient when automatic mobility is required or recovery from an offline source server.

As with LPM, SRR requires the destination server to see the same shared storage as the source server to rebuild the VM. The key difference between SRR and LPM is that the source server must be offline so that the rebuild is successful when using SRR. Although SRR is not a fully automated product, it can be automated by using PowerVC, and it is possible that you can build automation around the product by using the REST API capability too.

VMRM is a fully automated management system that is based around the SRR and LPM functions. It provides options for HA in one site and HADR in two sites by using VMRM DR, VMRM HADR, and VMRM HADRHA.

PowerHA SystemMirror is a fully functional automated clustered solution that can provide more availability by automatically recovering workloads by using available redundant components. Also, PowerHA SystemMirror recovers workloads quicker when they are moved between server nodes in the cluster because the OS is active, so all you need to do is activate the application components.

It is possible to run a mixture of these technologies within the same environment to customize your HADR solution to the requirements of each of your applications.

2

IBM VMRM architecture and components

This chapter describes the various IBM Virtual Machine Recovery Manager (VMRM) clustering options, components, and architecture.

VMRM for Power can be deployed across existing PowerVM virtualized environments. VMRM provides an automated solution for high availability (HA) of virtual machines (VMs) and applications running under VMRM. It also provides disaster recovery (DR) capability for VMs from a production site to a backup site. Disasters can be natural calamities, hardware failure, or a power failure in data centers.

The VMRM solution supports four types of clusters:

- HA
- DR
- High availability and disaster recovery (HADR)
- HADRHA

The following topics are described in this chapter:

- VMRM family
- IBM VMRM GUI

2.1 VMRM family

VMRM is a family of products that provides HADR capabilities for your IBM Power environment. VMRM HA implements recovery of the VMs based on the VM restart technology.

The VM restart technology relies on an out-of-band monitoring and management component that restarts the VMs on another server when the host infrastructure fails. The VM restart technology is different from the other cluster-based technologies that deploy redundant hardware and software components for a near real-time failover operation when a component fails. VMRM HA is ideal to ensure HA for many VMs, and is simpler to manage because it does not have the complexity of many other clustering solutions.

The products have many components in common, and these components are combined into different solutions to meet your specific requirements.

Here are the different family solutions:

- VMRM HA

  VMRM HA provides a single-site, HA solution to manage the availability of your applications at that single site. VMRM HA also supports two or more data centers in a campus environment, with the requirement that all the servers must have access to the shared storage that is used to store your data. Distance between the different campus sites is limited by the additional latency that the distance adds to your data access times.

- VMRM DR

  VMRM DR provides a 2-site DR solution that manages the availability of your applications across a primary site and a remote backup site. The product uses and controls storage replication between the two sites. Multiple storage vendor products are supported.

- VMRM HADR

  VMRM HADR combines the HA features of VMRM HA with the DR capabilities of VMRM DR. You can move workloads within a single data center for local failures while retaining the ability to move your workload to the backup site in a site failure. This solution provides HA support at the primary site only.

- VMRM HADRHA

  VMRM HADRHA builds on the capabilities of VMRM HADR and adds the ability to manage local failures at both the production site and the backup site. This approach is the most flexible of the availability management options for your applications, and provides local HA in both the primary and backup site along with DR between the sites.

VMRM HA is available as a stand-alone product or as an integrated component in AIX Enterprise Edition. VMRM DR (including HADR and HADRHA) is available as a stand-alone product or as an integrated component of the IBM Private Cloud Edition or IBM Private Cloud Edition with AIX.

2.1.1 Common components

The four solutions are based on the following common components that are used in each solution:

- Controlling system (KSYS)
- GUI
- Hardware Management Console
- Virtual I/O Server

Controlling system (KSYS)

Each of the solutions requires a management and monitoring capability to determine the health of the environment and direct the movement of workloads to the different servers across the sites in an outage, whether planned or unplanned. The *KSYS system* provides that capability for all the VMRM solutions. KSYS is the primary component in VMRM solutions. It provides a single point of control for the entire environment.

The KSYS subsystem runs in an AIX logical partition (LPAR). You can customize the security level for the KSYS LPAR according to the AIX security requirements of your organization. The KSYS cannot be affected by errors that can cause an outage in the production systems. Therefore, the KSYS must be self-contained and share a minimum number of resources with the production system.

The KSYS subsystem must remain operational even if the site fails. Ensure that you periodically receive KSYS health reports. You can check the KSYS subsystem health in the VMRM HA GUI dashboard.

The KSYS LPAR can be protected from failure by using other products, such as PowerHA SystemMirror for AIX. Starting with VMRM 1.7, HA support for the KSYS is integrated into VMRM. VMRM uses AIX Reliable Scalable Cluster Technology (RSCT) for cluster management functions. HA for the KSYS system is documented in Chapter 8, “KSYS high availability” on page 217.

Figure 2-1 shows the logical interactions between KSYS and other physical components of the VMRM DR solution.

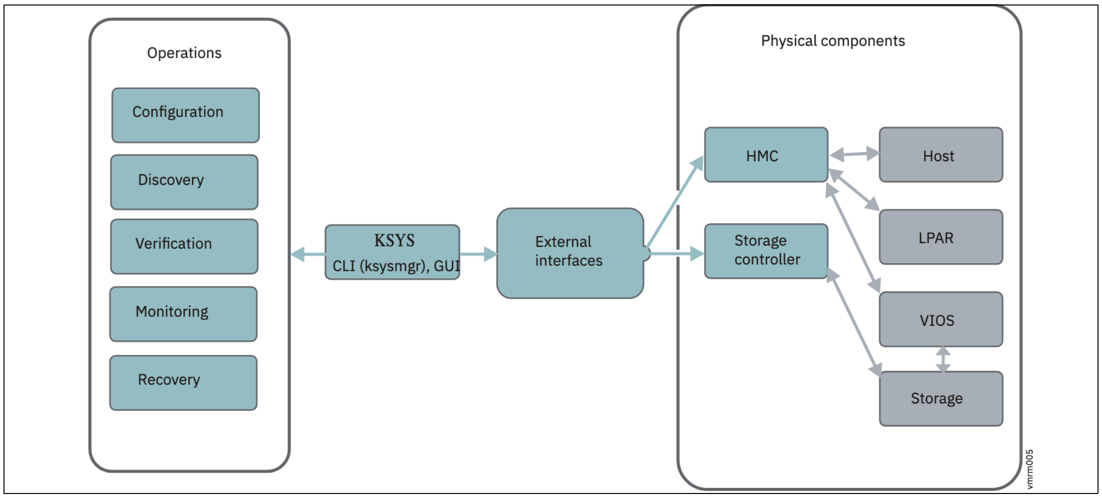


Figure 2-1 Logical interaction between KSYS and other components

The KSYS constantly monitors the production environment for any unplanned outage that affects the production site or the disk subsystems. If an unplanned outage occurs, KSYS analyzes the situation to determine the status of the production environment. When a site fails, the KSYS notifies the administrator about the failure. If the failure is severe, the administrator can initiate a site takeover. The KSYS pauses the processing of the data replication to ensure backup data consistency and process the site takeover.

The KSYS handles discovery, verification, monitoring, notification, and recovery operations to support DR for the VMRM DR solution. The KSYS interacts with the Hardware Management Console (HMC) to collect configuration information of the managed systems. The KSYS interacts with the Virtual I/O Server (VIOS) through the HMC to obtain storage configuration information of the VMs. The KSYS also provides storage replication management and Capacity on Demand (CoD) management for processors and memory.

You can configure the KSYS by using the **ksysmgr** command. The **ksysmgr** command has the following format:

```
ksysmgr ACTION CLASS [NAME] [ATTRIBUTES...]
```

Security implementation for the KSYS subsystem

The KSYS subsystem runs in an AIX LPAR. You can customize the security settings on this LPAR based on the AIX security requirements of your organization. The KSYS management is enabled only for the root user in the KSYS LPAR. The KSYS subsystem does not communicate to any external systems except the HMCs, storage subsystems, and **ksysmgr**.

The KSYS subsystem uses Representational State Transfer (REST) application programming interfaces (APIs) to communicate to the HMCs. HTTP Secure (HTTPS) must be enabled for REST API communication. The KSYS subsystem communicates with the storage subsystems by using the APIs that are provided by the storage vendors. For any specific security requirements of these APIs, see the storage vendor documentation. The **ksysmgr** command provides a command-line interface (CLI) capability that communicates to the KSYS subsystem. You can configure and view the status of the KSYS subsystem and its resources by using the **ksysmgr** CLI or the GUI.

GUI

You can manage the VMRM environment by using CLI commands, but you can use a GUI to monitor and manage the VMRM solution. The GUI is described in 2.2, “IBM VMRM GUI” on page 41. Deployment of the GUI is documented in Chapter 9, “IBM VMRM GUI deployment” on page 237.

Hardware Management Console

VMRM is based on a VM restart technology. To monitor and manage the environment, VMRM uses the HMC to communicate with and control your IBM Power servers. An HMC must be connected to each of the hosts (servers) that are managed.

The HMC is a virtual or a physical appliance that manages the IBM Power servers (hosts), VIOSs, and LPARs that are managed by the KSYS LPAR. The HMC provides REST APIs that are used by the KSYS subsystem. These REST API calls are used by the KSYS LPAR to perform various configuration and operational tasks.

The KSYS subsystem collects the details about the managed systems, VIOSs, and VMs from the HMC by using REST API queries. The KSYS subsystem also collects detailed information about system processor allocations, system memory allocation, hardware health, network connectivity, and the worldwide port names (WWPNs) of the physical Fibre Channel (FC) adapters from the HMC.

The KSYS subsystem performs the following operations by using the HMC:

- Checks the system capability for each operation.
- Periodically collects state information about the host, LPAR, and VIOS. It also gathers the IP addresses of the host, VIOS, and LPAR that the KSYS subsystem can use for subsequent monitoring.
- Provides the disk-mapping information to the VIOS in the backup site.
- Validates the backup site by checking whether the destination hosts can do a remote restart operation.
- Provides appropriate return codes to KSYS so that KSYS can perform the required recovery actions.
- Cleans up disk-mapping information in VIOS when the mapping information is no longer required.

To ensure enhanced availability, you can configure dual HMCs. In this case, if one HMC is down or unreachable, the KSYS can use another configured HMC to collect the required information and control any recovery actions.

> **Note:** Ensure that port 12443 on HMC is excluded from the firewall so that the KSYS subsystem can communicate with the HMC by using the HMC Rest API.

For more information, see HMC REST APIs.

Virtual I/O Server

In the IBM Power servers, virtualization support is provided by using the VIOS. The VIOS is required to provide connectivity to the networks and the storage across all the sites. Each host server requires VIOS servers to be configured to support the VMRM solution.

2.1.2 VMRM HA

VMRM HA supports a HA cluster within a data center or across data centers in a campus environment. Like all the VMRM solutions, the HA solution is an automated solution that is simple to deploy. This section describes the capabilities of VMRM HA along with its architecture and a description of the components that are involved in the solution.

VMRM HA overview

HA management is a critical feature of business continuity plans. Any downtime to the software stack can result in a loss of revenue and disruption of services. VMRM HA monitors and manages multiple servers in a single site. If a failure occurs on one of the servers, the LPARs that are running on that server are restarted on the remaining operational servers automatically so that you can recover from the failure more quickly and minimize downtime.

Key features of VMRM HA

The VMRM HA solution provides the following capabilities:

- Host health monitoring
- VM and application health monitoring
- Management of unplanned outages
- Management of planned outages
- Support for advanced placement policies
- GUI and command-line based management

Host health monitoring

VMRM HA monitors hosts for any failures. If a host fails, the VMs in the failed host are automatically restarted on other hosts. VMRM HA uses the host monitor (HM) module of the VIOS partition in a host to monitor the health of hosts.

VM and application health monitoring

VMRM HA monitors VMs, registered applications, and hosts for any failures. If a VM or a critical application fails, the corresponding VMs are restarted automatically on other hosts. VMRM HA uses the VM monitor (VMM) agent that must be installed in each VM to monitor the health of VMs and registered applications.

Management of unplanned outages

When VMRM HA detects a failure in the environment during an unplanned outage, the VMs are restarted automatically on other hosts. If you need tighter control of the recovery process, you can change the auto-restart policy to advisory mode. In advisory mode, the failed VMs are not relocated automatically; instead, email or text messages are sent to the administrator, who can choose to manually restart the VMs by using the tool's interfaces.

Management of planned outages

For a planned outage when maintenance is required (either firmware (FW) updates or hardware maintenance), VMRM HA uses Live Partition Mobility (LPM) to nondisruptively migrate the VMs on the affected server to the remaining hosts in the group. When the maintenance completes, VMRM HA can restore the VMs to their original host in a single operation.

Support for advanced placement policies

VMRM HA provides advanced policies to define relationships between VMs so that you can define whether VMs can be collocated with other VMs or whether they should be run on different servers. You can define the priority of each VM to manage which VMs are restarted first. You can define the CPU and memory configuration that is used during failover operations in a case where the available hardware is less than what the LPAR is currently using.

GUI and command-line based management

You can use a GUI or a CLI to manage the resources in VMRM HA. To use the GUI, install the UI server and use your web browser to manage the resources. Alternatively, the **`ksysmgr`** command and the **`ksysvmmgr`** command on the KSYS LPAR provide end-to-end HA management for all resources.

Architecture and components of VMRM HA

VMRM HA is the HA solution of the VMRM family. Figure 2-2 on page 27 shows the architecture of VMRM HA. As a HA solution, VMRM HA uses shared storage within a site (or campus). Access to that storage is provided by the VIOS in each host server. The VMRM HA solution can support any storage systems that are certified with the VIOS, except for internet Small Computer Systems Interface (iSCSI) storage devices. Storage disks that are related to VMs must be accessible across all the hosts within the host group so that VM can be moved from a host to any other host within the host group.

A set of hosts is grouped to provide a pool of resources that is used for your workloads. For a planned outage, VMRM HA uses LPM to move VMs off the host that needs maintenance, and can move them back when the maintenance completes.

When a failure is detected, VMRM HA can automatically relocate and restart the affected VMs on other healthy hosts within the group.

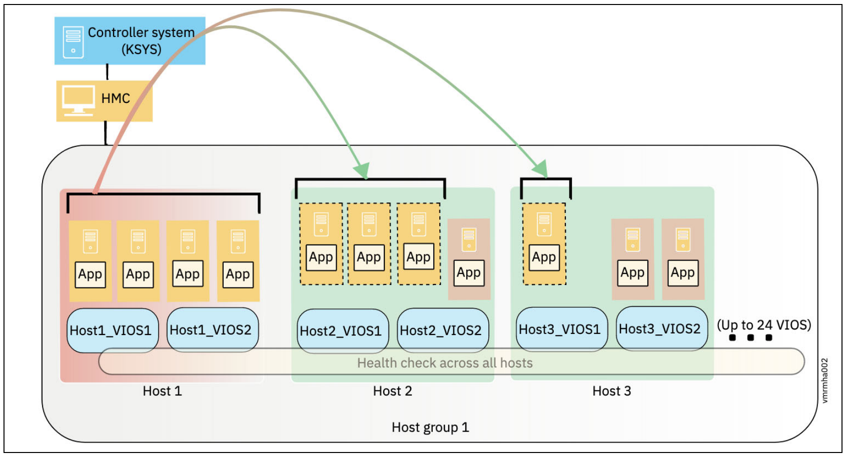


Figure 2-2 VMRM HA solution architecture

VMRM HA uses the components that are shown in Figure 2-3.

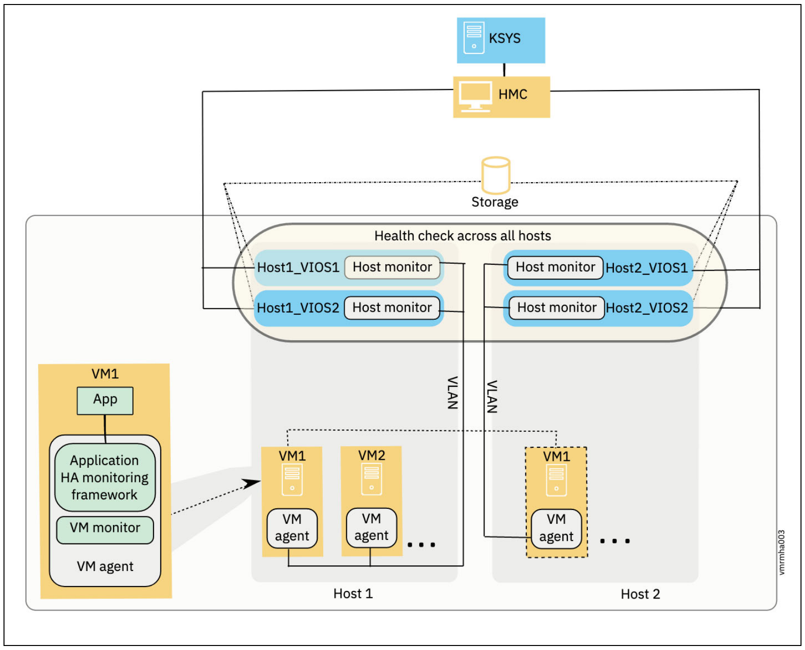


Figure 2-3 VMRM HA solution components

Controller system (KSYS)

The controlling system, also called KSYS, is a fundamental component that monitors the production environment for any unplanned outage. This component is the same monitoring LPAR that is used in all the VMRM solutions. If an unplanned outage occurs, the KSYS analyzes the situation, notifies the administrator about the failure, and can automatically move the failed VMs to another host in the host group. The KSYS interacts with the HMC to collect configuration information about managed systems. The KSYS subsystem also collects VIOS health information through the HMC.

Host group

Hosts are grouped to provide backup for each other. When failures in any hosts are detected, VMs in the failed host are relocated and restarted on other healthy hosts within the group of hosts. This group of hosts is called a *host group*.

Host monitor

The HM daemon is included with the VIOS and deployed during the VIOS installation. When you initialize the KSYS subsystem for the HA feature, the HM module becomes active. The KSYS subsystem communicates with the HM daemon through the HMC to monitor the hosts for HA.

VM agent

You can optionally install the VM agent file sets, which are included with the KSYS file sets in the guest VMs. The VM agent subsystem provides a HA feature at the VM and application levels. The VM agent monitors the following issues in the production environment:

- VM failures: If the operating system of a VM is not working correctly, or if the VM stopped working because of an error, the VM restarts on another host within the host group. The KSYS subsystem uses the VMM module to monitor the heartbeat from the VM to the HM subsystem in a VIOS.
- Application failures: There is an option to register applications in the VM agent by using application monitoring. The VM agent uses the Application HA monitoring framework to monitor the health of the application by periodically running application-specific monitor scripts, which can identify whether the application failed, and restart the VM in the same host or another host. This framework can manage the sequence in which applications are started and stopped within a VM.

Note: The VM agent is supported on AIX and Linux (Red Hat Enterprise Linux (RHEL) and SUSE Linux Enterprise Server) guest VMs only. Currently, the VM agent subsystem is not supported for the IBM i and Ubuntu VMs. Therefore, IBM i and Ubuntu VMs are relocated from one host to another host within the host group only after a host failure.

2.1.3 VMRM DR

DR of applications and services is a key component to provide continuous business services. The VMRM DR for Power solution is a DR solution that is simple to deploy and provides automated operations to recover the production site. The VMRM DR solution is based on the IBM Geographically Dispersed Parallel Sysplex (IBM GDPS) offering concept that optimizes the usage of resources. This solution does not require the deployment of backup VMs for DR, which reduces the software license and administrative costs for your environment. VMRM DR now supports Single-Root I/O Virtualization (SR-IOV) and Virtual Network Interface Controller (vNIC) features.

The VM restart-based VMRM DR solution relies on an out-of-band monitoring and management component that restarts the VMs on other hardware when the host infrastructure fails.

Figure 2-4 on page 29 illustrates the VMRM DR solution. The KSYS is the LPAR that manages the complete VMRM environment.

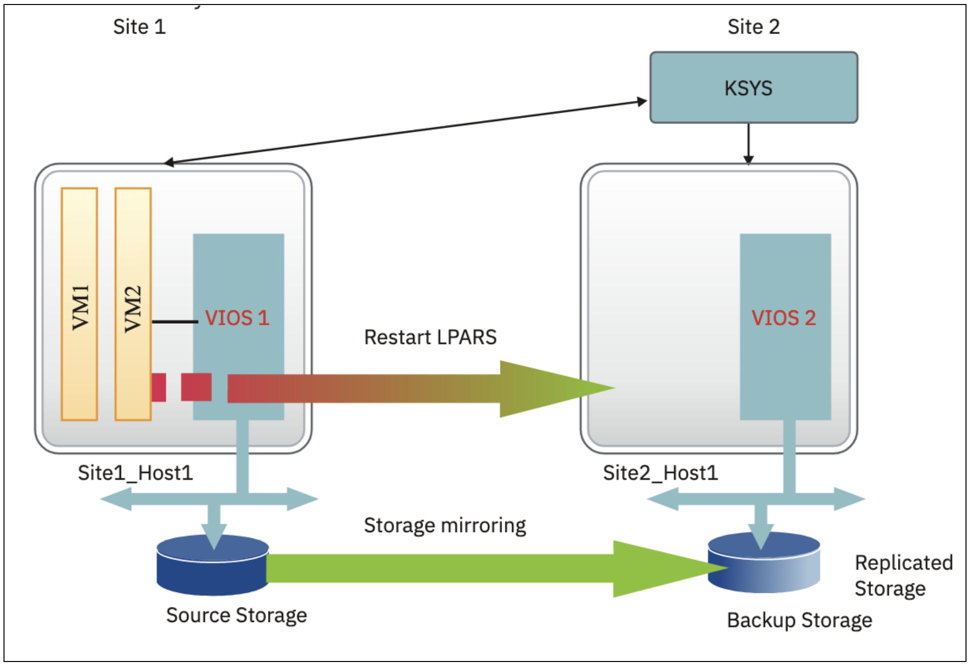


Figure 2-4 VM restart-based disaster recovery model for VMRM

Overview of VMRM DR for Power

Using a set of scripts and manual processes at a site level to manage your environment and restore service at another site takes more time than using automated procedures. The VMRM DR solution provides automated operations to automatically recover a production site in case of failures. This solution provides a simple deployment model that uses a controller system (KSYS) to monitor the entire VM environment. This solution also provides flexible failover policies and storage replication management.

VMRM DR for Power offers the following benefits:

- Simplified DR management
- Cost savings by eliminating the need for hardware and software resources on the backup or DR site
- Reduced license costs
- Reduced administration costs
- Ability to test the DR environment without affecting the production environment

VMRM for Power uses VM restart technology to restart VMs in a backup site if there is a disaster or planned system maintenance. The main difference between VMRM DR for Power and a traditional DR environment such as IBM PowerHA SystemMirror is that VMRM DR for Power does not require resources (VM or LPARs) to be running on the backup site for failover. A key benefit of the VMRM for Power configuration is that it reduces licensing costs and administration requirements.

VMRM for Power is managed by a single control system LPAR that is called KSYS, which stands for (K)controller system LPAR. With KSYS, the administrator can perform move operations and DR tests. KSYS handles all the complexity of the communication between the different components of the VMRM for Power environment to perform the necessary tasks.

Features of the VMRM DR solution

VMRM DR for Power provides many user-centric features to help with DR in a traditional 2-site configuration. The following list shows some of the important features and capabilities of a VMRM DR solution:

- Support for IBM Power servers running on POWER7 processor-based servers and later.
  - Supports all operating systems that are supported on IBM Power, such as:
    - AIX.
    - IBM i.
    - Linux (RHEL, SUSE Enterprise Linux, and Ubuntu).
  - Boot device management for POWER8 (or later) processor-based servers.
  - 1000 VMs or LPARs are supported (the GUI supports only 200).
- Storage replication support for the following systems:
  - Dell EMC Symmetrix Remote Data Facility (SRDF) (VMAX) and Dell EMC Unity.
  - IBM SAN Volume Controller based storage, including IBM FlashSystem and Storwize.
  - IBM XIV.
  - Hitachi.
  - IBM DS8000.
- Ease of use and ease of management:
  - Simple to deploy and manage by using either the **`ksysmgr`** utility or the GUI.
  - Simple migration from older releases to the new release of VMRM DR.
  - Prompt event notification mechanism.
  - HMC Nova link coexistence support.
- Capacity management:
  - Shared processor pool support.
  - Supports one-to-one mapping for a host or one-to-many mappings for a host. M to N server pairing is supported across sites. Administrators can deploy and manage a DR environment where M number of servers on the home site are configured to failover to N servers at the backup site. For example, administrators can deploy six servers at the primary site and two servers at the backup site.
  - Enterprise pool support with the ability for flexible capacity management.
  - Elastic On/OFF CoD support.
  - Priority-based capacity adjustment support during a recovery.
- Customizable configuration options, such as:
  - Group support allows management of objects as a group as opposed to one at a time for the following groups:
    - Host group, which manages groups of servers.
    - Workgroup, which supports a group of VMs.
  - Customization framework that supports plug-in scripts for the following items:
    - Perform custom checks daily.
    - Custom responses to events.
  - Customize the minimum required paths for VMs to move to the remote site.

  - Customize the minimum number of virtual Fibre Channel (vFC) adapters that the VIOS requires for the VM during a DR operation so that you can perform a recovery when there are fewer vFC adapters that are available in the DR environment.
  - Custom consistency group (CG) name for storage subsystem.
  - Priority-based restart of VMs on DR.
  - LAN and VSWITCH configuration that is supported at system level, host group level, workgroup level, and host level. Virtual LAN (VLAN) and vSwitch customization per site.
  - SR-IOV/VNIC support, including the ability to override if there is a mismatch in the SR-IOV configuration in the source and the target sites.
- Built-in support of HA for the KSYS node by using a multi-node KSYS cluster, which does not require IBM PowerHA SystemMirror.
- DR Rehearsal support supports the ability to test DR processes without interrupting production site VMs. Multiboot disk is supported for the DR rehearsal operation.

Architecture and components of VMRM DR

The VMRM DR solution provides a DR environment by identifying a set of resources that are required for processing the VMs in a server during disaster situations. Figure 2-5 shows the architecture for VMRM DR solution.

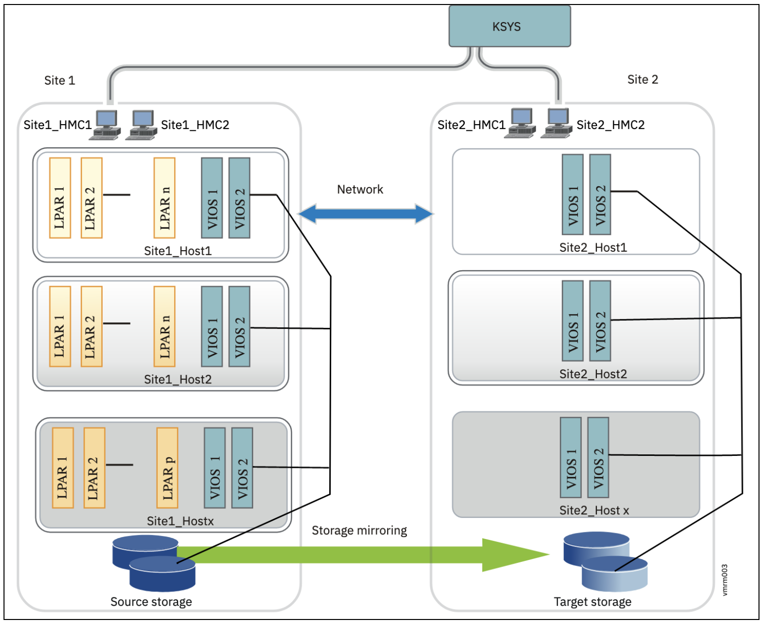


Figure 2-5 VMRM DR solution architecture

VMRM DR is a 2-site solution where the data for the workload must be replicated from the primary site to the backup site. The data is replicated by using the storage replication options that are provided by the storage vendor. In the primary site, there is sufficient available hardware to allow the workloads to be restarted in the backup site.

The KSYS LPAR is running in the backup site and controls the movement of the workload when an event occurs. This movement involves first controlling the storage replication through the standard APIs that are provided by the storage vendor and making the storage volumes available to be activated at the backup site. Then, the LPARs that were impacted are restarted on the servers at the backup site.

VMRM DR supports CoD and Power Enterprise Pool to help you optimize the resource utilizations in your environment. You can use these technologies to reduce the active resources during normal operations at your backup site. When the workloads must be moved from the production site due to either a planned or unplanned outage, VMRM DR can activate any resources that are required to support your environment.

As described in “Features of the VMRM DR solution” on page 30, VMRM DR can move workloads between sites when the processor and memory configurations are not the same.

VMRM consists of many different components. These components are monitored by KSYS controller machines. The VMRM DR solution uses the following components:

- Controller system (KSYS)
- Site
- Host
- VMs or LPARs
- Storage
- Network
- HMC
- VIOS
- Host group
- Workgroup

Figure 2-6 shows the VMRM DR components. These components are described in the following sections.

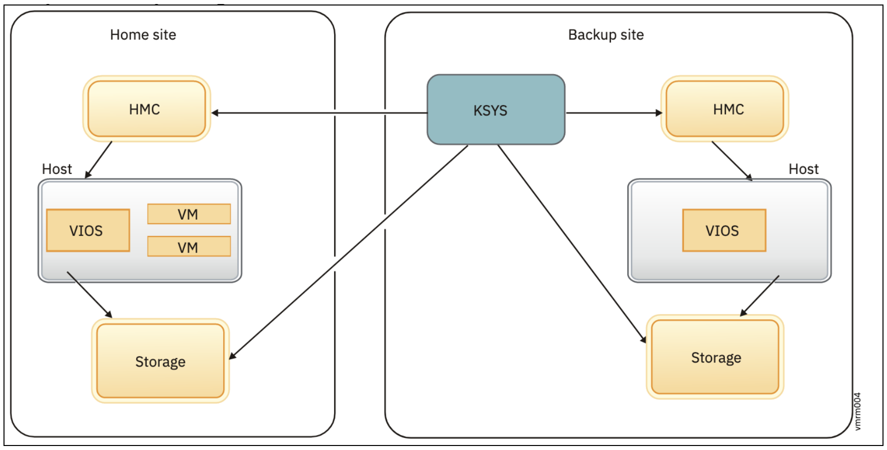


Figure 2-6 Components of VMRM DR solution

Controller system (KSYS)

The KSYS is an important component in the VMRM solution. For VMRM DR, ensure that you deploy the KSYS in the backup site so that the KSYS is isolated from any issues or failure in the active site. The KSYS is responsible for performing the recovery actions in a planned or unplanned disaster. Therefore, the availability of KSYS is an absolute requirement of the solution. The KSYS *cannot* be deployed at the primary site, and is usually at the backup site because the KSYS must remain operational even if the active site fails or if the disks at the active site fail. Technically, KSYS may be deployed at a neutral location if it has access to the HMC, VIOS, and storage at both sites. A third-site deployment is not recommended because it adds more complexity.

Hardware Management Console

The KSYS LPAR interacts with the HMCs for processes that involve host, VIOS, and disk subsystem resources. These processes include discovery, monitoring, recovery, and cleanup.

Sites

Sites are logical names that are created at the KSYS level. All the HMCs, hosts, VIOSs, and storage devices are mapped to one of the two sites.

Only two sites can be configured: home site and backup site. A workgroup or a host group can be active on any of the two sites. You can query the details about a site, what host groups are active on the site, and what active workgroups are on the site by using the **ksysmgr** command.

Sites can be of the following types:

Home Site (primary site): Indicates the site where the workloads primarily run. The **ksysmgr** command can display and configure the current attributes of the active site.

Backup Site (DR site): Indicates the site that acts as a backup for the workload at a specific time. During a disaster or a potential disaster, workloads are moved to the backup site.

Sites can be created by using the **ksysmgr** command.

Figure 2-7 shows the site attributes.

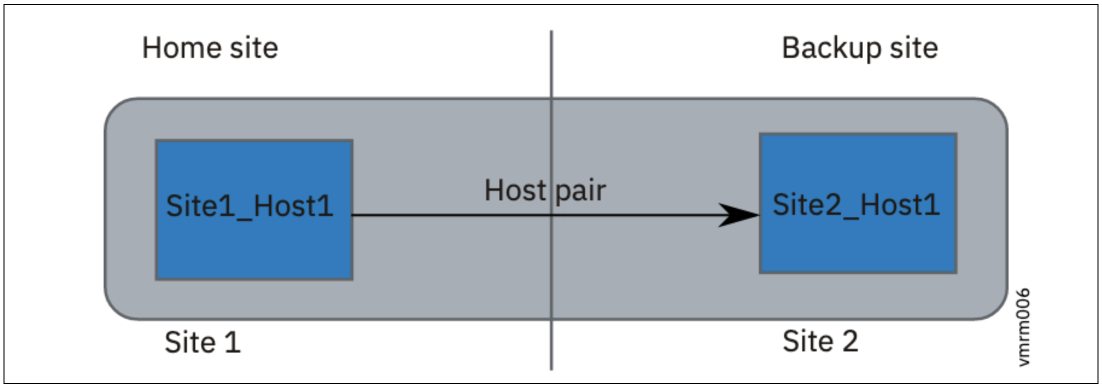


Figure 2-7 Site attribute

In this example, the Site1 and Site2 sites can switch back and forth as active and backup sites, depending on where the LPARs are. Site1 is assigned and configured as the active site for the LPARs on the Host1 host. More applications can be assigned to Site2 with failover to Site1 if required.

Hosts

A *host* is a managed system that runs the VMs and their workloads. A host is sometimes called a *server*, or a Central Processor Complex. Hosts are managed by an HMC and are identified by their Universally Unique Identifier (UUID), which is tracked in the HMC.

The VMRM DR solution uses the following host-specific terms:

Host pair: Indicates the set of hosts that are paired across the sites for HADR.

Each host in the host pair must meet all the resource requirements (for example, CPU, memory, and VIOS-based virtual I/O aspects) to run the same workload in a disaster or a potential disaster.

Host group: Indicates a group of hosts that are logically chosen and named by the administrator.

A set of hosts can be grouped according to the business requirements. Each host must belong to a host group. For example, group hosts that run similar workloads, or group the most important hosts so that the monitoring and recovery operations can be performed on that set of host both quickly and concurrently. By grouping the most important hosts in their own group, the entire host group can be moved to the backup site in a disaster.

Discovery, verification, move, and recovery operations can be performed at the host group level. These operations can be run at a site level, where all the host groups are included in the operation. If a host group already was moved to the backup site and a site-level move operation is started from the home site, that host group is skipped for the operation and continues to run at the backup site.

Figure 2-8 shows the host-related configuration across sites.

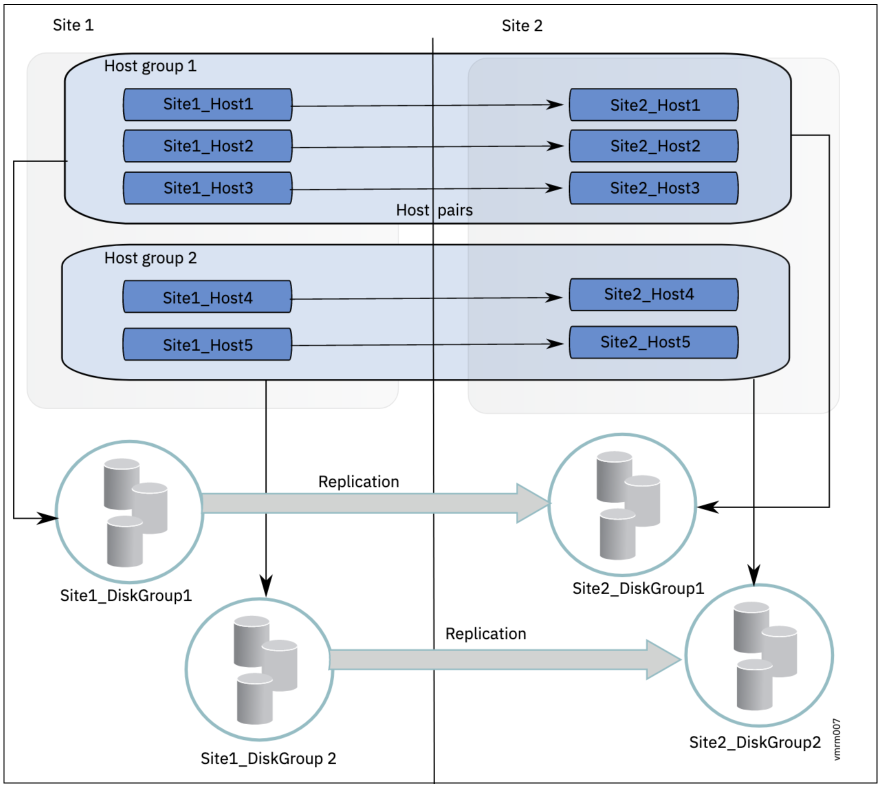


Figure 2-8 Host and host group configuration

The VMRM DR solution supports an environment in which M number of hosts on the home site are configured to failover with N number of hosts on the backup site. This configuration is referred as M host-to-N host (MxN) pairing. A host group with the one-to-many paring is called an *asymmetric* host group. Host pairing is not required in an asymmetric host group configuration.

Workgroup

One or more workgroups can be created within a host group, and you can add VMs to each workgroup. When a command runs on a workgroup, the command operation takes effect on all the VMs in that workgroup. All operations and commands that are run for host group can be run for a workgroup.

A default workgroup is created automatically when a host group is created. If a workgroup is not created with VMs in a host group, all the VMs are added to the default workgroup. If a discovery, verify, move, or DR test operations that are run at a host group level, the operations also have the same effect on the workgroups within the host group. You can create a host group without workgroup support by setting the **`workgroup`** attribute to `no` in the command that you run to create a host group.

Note: The HADR and HADRHA types of deployment do *not* support workgroups.

Figure 2-9 shows the host group, workgroup, and VM configuration.

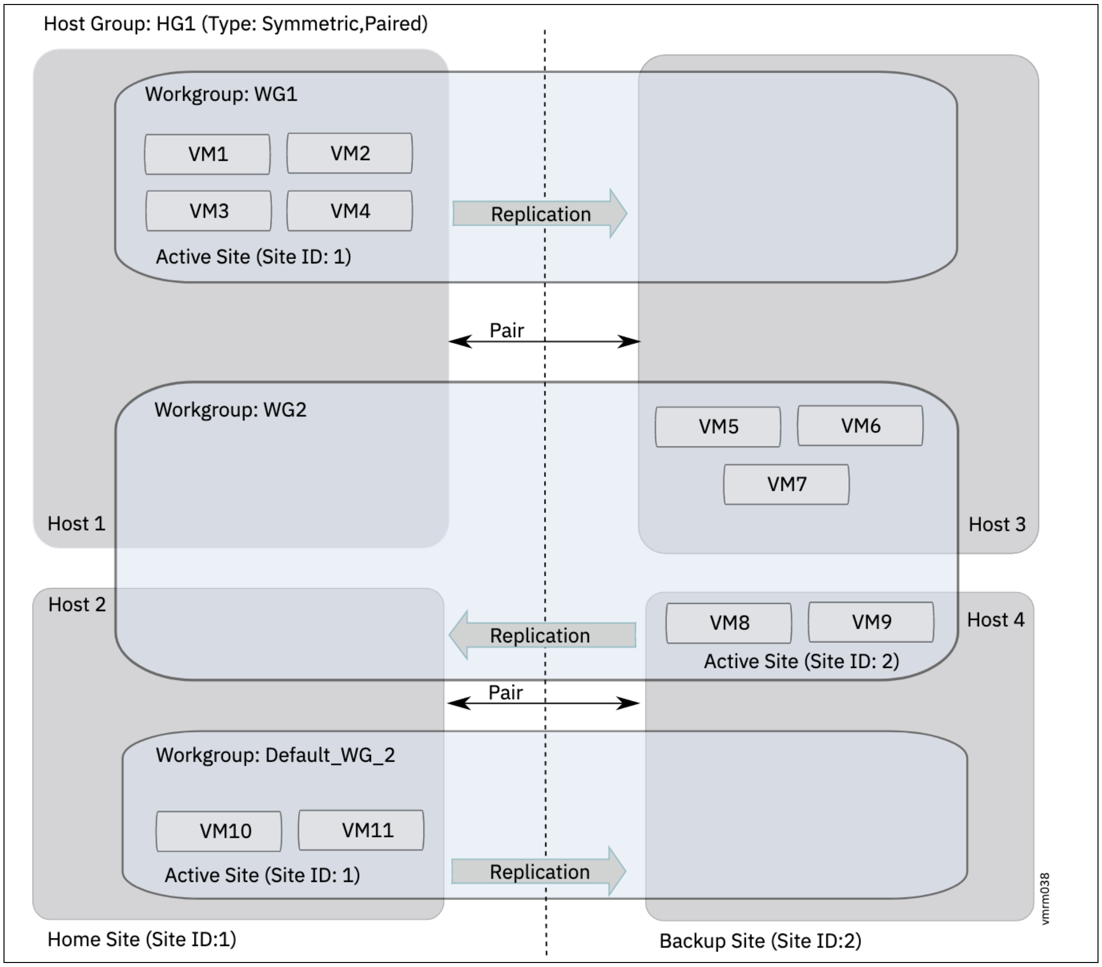


Figure 2-9 Host group, workgroup, and VM configuration

Four hosts are added in this symmetric host group configuration. Host1 and Host2 belong to the home site, and Host3 and Host4 belong to the backup site. Host1 and Host2 in the primary site are paired to Host3 and Host4, which are in the backup site. The VMs of the host groups are added to the two different workgroups. If a workgroup is not created and you add VMs to your host group, those VMs are added to the default workgroup.

Virtual machines

VMs, also known as LPARs, are associated with specific VIOS partitions to map the virtualized storage to run a workload. A host can contain multiple VMs, as shown in Figure 2-10.

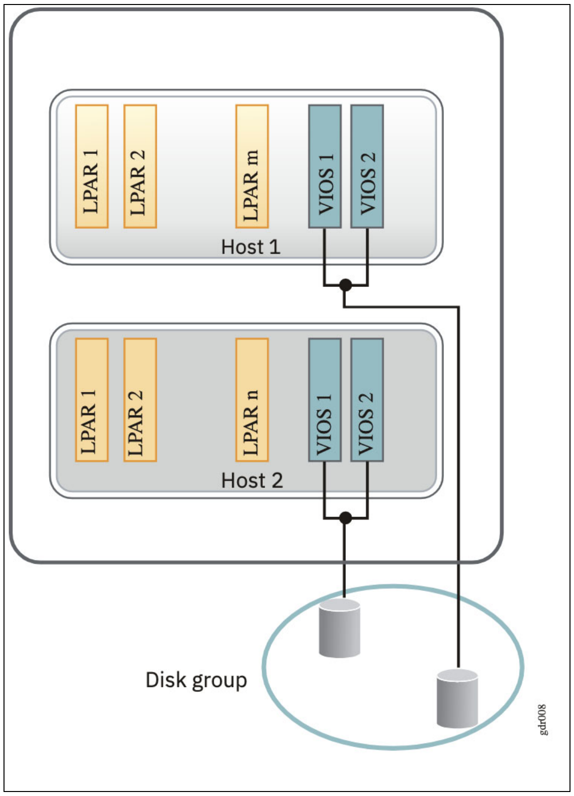


Figure 2-10 Virtual machines configuration

Virtual I/O Server

The KSYS receives information about the storage configuration of the VMs from the VIOS. The storage area network (SAN) zoning and logical unit number (LUN) masking must be performed so that the VIOS can access the disks' information. The KSYS interacts with the VIOS to obtain information about the disks that are provisioned to the client partitions. During the validation process, the data that is collected from the active site is used on the backup site to validate whether VMs can be moved to the backup site during disaster situations.

The KSYS interacts with the VIOS to get information about the LPAR storage. The KSYS also interacts with the VIOS when the KSYS activates the various VMs during the DR operations. Therefore, the VIOS must have sufficient processing power and memory to handle requests from the KSYS along with handling the regular I/O activities that are in progress on the VIOS. If there are multiple VMs that are clients of the VIOS pairs, it is a best practice to dedicate some extra capacity during the DR operation. For example, you can add at least 0.1 CPU and 1 GB of memory to the planned capacity for the VIOS.

To back up and restore the virtual and logical configuration, use the **viosbr** command on the VIOS partitions. It is also possible to collect, apply, and verify device settings in a VIOS runtime environment by using the VIOS rules management. The VIOS rules support consistent device settings across multiple VIOS partitions and improve usability of the VIOS.

For more information, see viosbr command and VIOS rules management.

Storage agents

A DR solution requires an organized storage management process because storage is a vital entity in any data center. The VMRM DR solution relies on data replication, which is managed by the storage system, from the active site to the backup site.

In the VMRM DR solution, the data is replicated from the active site to the backup site by using *storage replication*. Depending on the exact type of storage devices that is used, the initial storage configuration *might* require the installation of storage controller software to perform replication operations. The general storage management tasks include starting, stopping, suspending, reversing, resyncing, pausing, and resuming the replication. For more information about the installation of storage controller software, see the documentation from the storage vendor.

Figure 2-11 shows an example of mapping storage devices across the active site and the backup site.

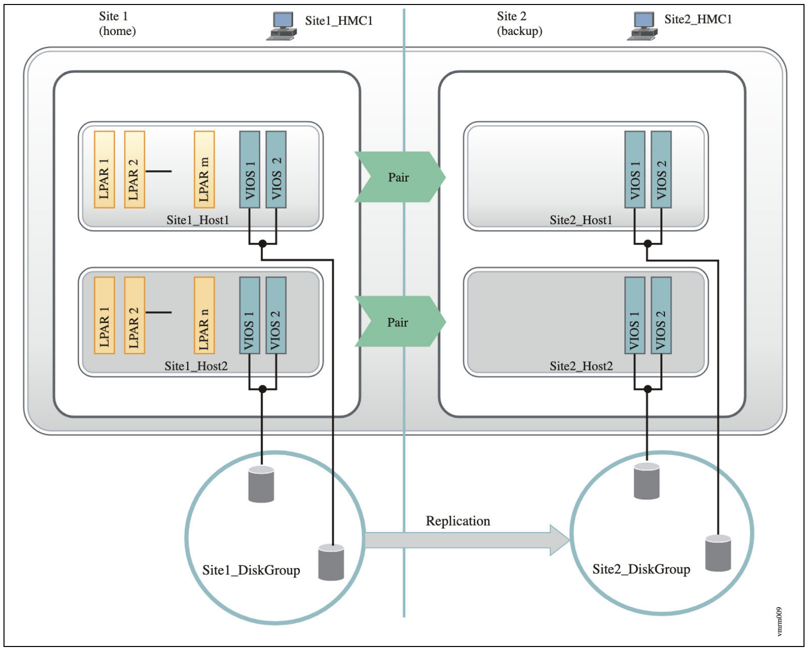


Figure 2-11 Storage replication across sites for VMRM DR

After the initial storage setup, the storage agent must be added to the KSYS configuration that interacts with the storage subsystem. When using storage controller software, the storage agents interact with the storage controller to perform storage-specific operations in the disks.

The storage subsystem uses the following components for configuration and recovery operations:

Storage controller A node that contains the software to manage the interaction between the disks and the hosts that are connected to the storage.

Disk group Indicates a group of disks within a site.

Consistency group Indicates a group of storage devices from multiple storage arrays. This group of storage devices maintain the consistency of data.

Disk pair Indicates the set of disks or disk groups that are paired across the sites for DR.

Here are the storage systems that are supported by VMRM DR solutions:

- IBM SAN Volume Controller based storage (Storwize and IBM FlashSystem)
- IBM DS8000 Storage System
- IBM XIV Storage System
- Hitachi storage system
- Dell EMC unity storage system
- Dell EMC SRDF (VMAX) system

For more information about SAN storage and SAN fabric support for a VMRM configuration, see 10.2, “SAN storage general considerations for the VMRM DR environment” on page 265 and 10.3, “SAN fabric setup for the IBM VMRM DR environment” on page 266.

For more information about the various supported storage subsystems, see 10.4, “Storage components in the IBM VMRM DR solution” on page 268.

Network

The network must be configured for the existing resources, which include hosts, HMCs, VIOSs, and storage devices. For the VMRM DR solution to work, the KSYS node must be directly connected to the HMCs and the storage controllers in both sites. The KSYS uses the HMC to interact with the hosts and VIOSs, and the KSYS uses the storage controller to interact with the storage subsystem. The KSYS system properties can be modified to enable or disable the network-mapping function globally across the sites. By using the network mapping function, you can create VLAN ID or virtual switch mapping policies that contain a mapping of VLAN IDs or virtual switches that are assigned to the VMs when the VMs are moved from the active site to the backup site.

2.1.4 VMRM HADR

Although VMRM DR provides a 2-site solution for DR, and VMRM HA provides a single-site HA solution, many customers need a solution that provides both options.

VMRM HADR overview

VMRM HADR for Power supports HA within the primary site and provides DR options to a backup site. Within the primary site, failures can occur at the application level, the VM level, or a host level. If there are failures within the primary site, the VMRM HADR automatically migrates the VMs to the remaining hosts at that site. If the failure is across sites, which includes planned and unplanned move operations at the site level and the host group level, you must initiate a move operation manually.

VMRM HADR uses a Shared Storage Pool (SSP) cluster that is formed with all the source site's VIOS instances for VM and host monitoring to provide the HA solution.

The important features of the VMRM HADR include all the essential and advanced features of DR and HA features, such as LPM, support for VM failure and host failure recovery, and application failover support within a home site; FC adapter failure; network adapter failure; monitoring CPU and memory usage; move operation and failover rehearsal operation across the site; and other DR features.

An example VMR HADR configuration overview is shown in Figure 2-12.

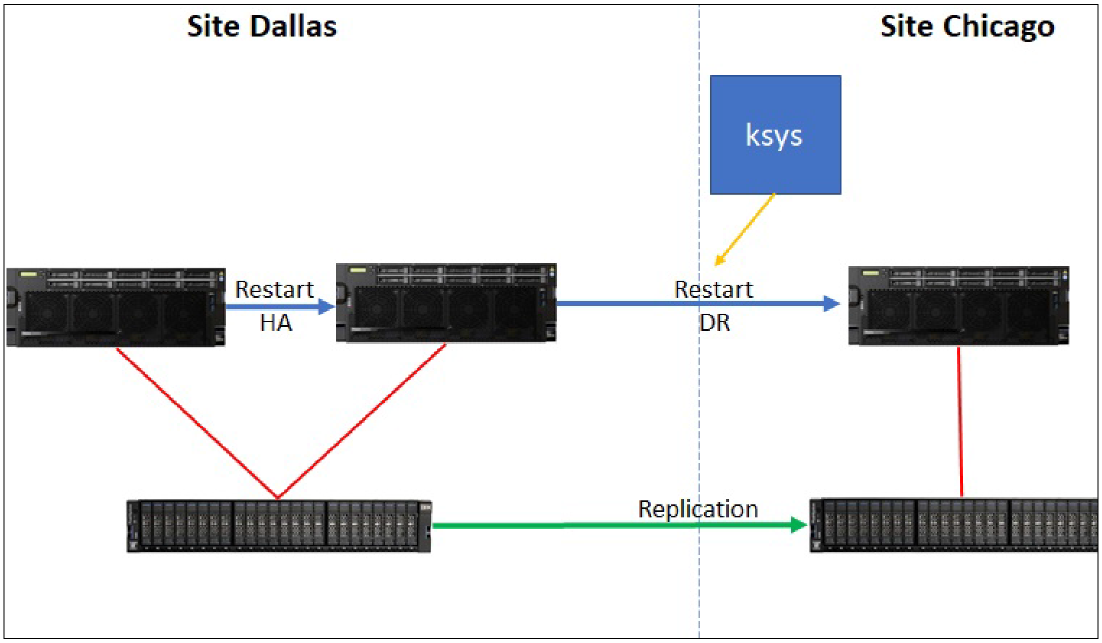


Figure 2-12 VMRM HADR solution overview

Key features of VMRM HADR

The key features are a combination of “Key features of VMRM HA” on page 25 and “Features of the VMRM DR solution” on page 30. In addition, consider these important features:

- LPM support within a site
- Support for VM failure and host failure within a site
- Application failover support within a site
- FC adapter failure within a site
- Network adapter failure within a site
- Monitoring CPU and memory usage within a site
- Move operation and failover rehearsal operation across sites and within a site
- DR support from one site to another site

Architecture and components of VMRM HADR

The solution components that are used is a combination of all components in both HADR options. However, there are specific requirements and limitations:

- For a HADR cluster, you should have at least two hosts on the home site and a minimum of one host on the backup site.
- Home site hosts should have a minimum of two VIOS instances.

- Home site VIOS instances should have at least two shared disks between them for an SSP cluster and a Cluster Aware AIX (CAA) volume group for the repository. The size of the shared disks must be greater than or equal to 10 GB.
- All managed VMs should have disks on the source and target storage, and replication should exist between the disks.
- The workgroup feature is not supported for the HADR type of deployment.
- When you shut down or restart a VM manually, the dependent applications are not affected. The recovery of dependent applications is considered only when failure has occurred with the parent application, the VM, or the host.
- Remove the default host group (`Default_HG`) before configuring the HADR types of deployment with PowerHA SystemMirror. To remove the default host group from the KSYS subsystem, run the following command:

```
rmrsrc -s "Name='Default_HG'" IBM.VMR_HG
```

- Disable the quick discovery feature before running the LPM and the restart operations on the VMs.

2.1.5 IBM VMRM HADRHA

As the name implies, this configuration involves DR capabilities between two sites *and* HA within each site.

Overview of VMRM HADRHA

An example VMRM HADRHA configuration is shown in Figure 2-13.

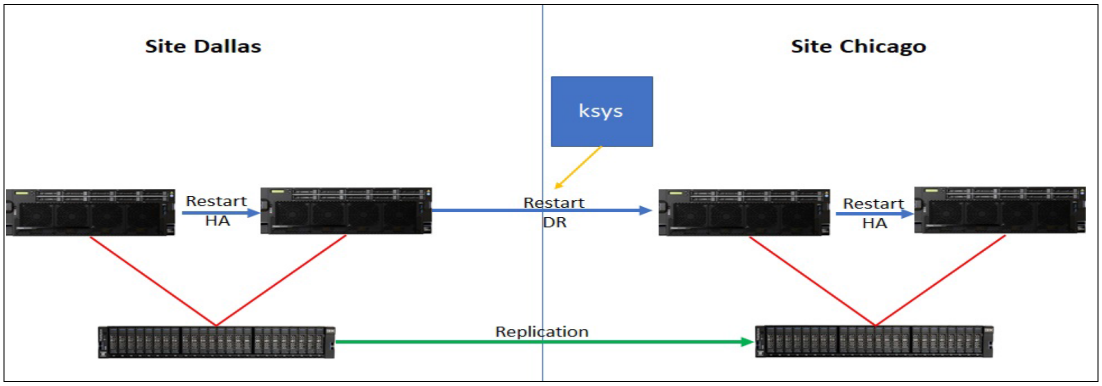


Figure 2-13 VMR HADRHA configuration overview

Key features of VMRM HADRHA

The key features are a combination of “Key features of VMRM HA” on page 25 and “Features of the VMRM DR solution” on page 30. Specific important HA features of the HADRHA type of deployment of the VMRM DR solution include the following features:

- LPM support at both the home site and the backup site
- Support for VM failure and host failure in both the home site and the backup site
- Application failover support in both the home site and the backup site
- FC adapter failure within a site
- Network adapter failure within a site
- Monitoring CPU and memory usage within a site

- Move operation and failover rehearsal operation across the sites
- DR support from one site to another site

Architecture and components of VMRM HADRHA

The solution components that are used are a combination of all components in both HADR options. However, there are specific limitations:

- The workgroup feature is not supported for the HADRHA type of deployment.
- When you shut down or restart a VM manually, the dependent applications are not affected. The recovery of dependent applications is considered only when failure occurs with the parent application, the VM, or the host.
- Remove the default host group (`Default_HG`) before configuring the HADRHA types of deployment with PowerHA SystemMirror. To remove the default host group from the KSYS subsystem, run the following command:

  ```
  rmrsrc -s "Name='Default_HG'" IBM.VMR_HG
  ```
- Disable the quick discovery feature before running the LPM and the restart operations on the VMs.

2.2 IBM VMRM GUI

Although VMRM can be configured from the KSYS CLI, you can use a GUI interface. Although every option that is available in the CLI might not exist in the GUI, most operations can be performed with the GUI.

2.2.1 Overview

The GUI was enhanced to support administrative functions and display the topology of the DR, HADR, and HADRHA KSYS configuration. The deployment wizard provides a simple way to deploy the VMRM DR solution. With the VMRM DR GUI, you can do workgroup management, and there is workgroup support for a DR cluster and asymmetric deployment support for a DR or HADR type KSYS cluster. The VMRM DR GUI supports cluster creation from the KSYS registration page for DR and HADR KSYS clusters. The VMRM DR GUI supports host group deployment for DR and HADR KSYS clusters. A user can check previous failover reports from the GUI dashboard. Other enhancements include managed and unmanaged VMs' bifurcation in topology, VM status display in topology, and support for policies such as flex capacity, network mappings, and others.

2.2.2 GUI agents

The GUI primarily consists of and depends on the following agents:

- `ksys.ui.agent`: The GUI agent file set that must be installed on the KSYS nodes.
- `ksys.ui.server`: A GUI server file set that must be installed on the system that manages the KSYS nodes. This file set can be installed on a KSYS node.
- `ksys.ui.common`: A GUI common file set that must be installed along with both of the above server and agent file sets.

For more information about installing and configuring the GUI, see Chapter 9, “IBM VMRM GUI deployment” on page 237.

3

Planning and deploying IBM VMRM HA

This chapter describes the planning, installation, and configuration of IBM Virtual Machine Recovery Manager High Availability (VMRM HA) for IBM Power.

To implement the VMRM HA solution, you must review your current high availability (HA) recovery plan and consider how the VMRM HA solution can be integrated into your current environment.

The following topics are described in this chapter:

- VMRM HA requirements
- VMRM HA file sets and structure
- Installing VMRM HA
- Configuring VMRM HA
- Setting up HA policies
- Uninstalling VMRM HA

3.1 VMRM HA requirements

Before you plan the implementation of the VMRM HA solution, you must understand the other entities and resources that the VMRM HA solution requires for providing HA service for your environment.

Meet the following requirements before you install the VMRM HA solution:

- Software requirements
- Firmware (FW) requirements
- Installation and configuration requirements
- Hardware Management Console (HMC) requirements
- Host group requirements
- Networks requirements
- GUI requirements

3.1.1 Software requirements

Table 3-1 shows the software requirements for VMRM HA.

Table 3-1 VMRM HA software component requirements

Component	Requirement
KSYS controller	IBM AIX 7.2 with Technology Level 2 or later. Install the latest version of OpenSSL software for the AIX operating system by going to AIX Web Download Pack Programs[a].
HMC	HMC 9.9.1.0 or later.
Virtual I/O Server (VIOS)	For VMRM 1.7: VIOS 3.1.2.40 or later.
Logical partition (LPAR)	Each host must have one of the following operating systems: ▶ AIX 6.1 or later. ▶ Red Hat Enterprise Linux (RHEL) (Little Endian) Version 7.4 or later (kernel version 3.10.0-693). ▶ SUSE Linux Enterprise Server (Little Endian) Version 12.3 or later (kernel version 4.4.126-94.22). ▶ Ubuntu Linux distribution Version 16.04. ▶ IBM i 7.1 or later.
Virtual machine (VM) Agent	The VM Agent is used to monitor the VM and applications to restart the VM if the applications fail. The agent can be installed only on the following operating systems currently: ▶ AIX 6.1 and later. ▶ RHEL (Little Endian) Version 7.4 or later (kernel version 3.10.0-693). ▶ SUSE Linux Enterprise Server (Little Endian) Version 12.3 or later (kernel version 4.4.126-94.22).

[a] The latest version of the OpenSSL software is included in the AIX base media.

3.1.2 Firmware requirements

This section describes the FW requirements for VMRM HA:

- The VMRM HA solution requires that PowerVM Enterprise Edition is deployed in each of the hosts.
- The VMRM HA solution supports the following minimal levels of Power servers:
  - IBM POWER7+ processor-based servers that have the following FW levels:
    - FW770.90 and later
    - FW780.70 or later except for MMB systems (9117-MMB models)
    - FW783.50 and later
  - IBM POWER8 processor-based servers that have the following FW levels:
    - FW840.60 and later
    - FW860.30 and later
  - IBM POWER9™ processor-based servers with FW910 or later.
  - IBM Power10 processor-based servers with FW1020 or later.

3.1.3 Installation and configuration requirements

This section describes the installation and configuration requirements for the VMRM HA:

- You must have root authority to perform any installation tasks.
- The KSYS LPAR must have at least one core CPU and 8 GB of memory. More CPU and memory might be required for large environments with more than 100 LPARs that are managed.
- The VIOS must have enough available space in the / (root), `/var`, and `/usr` file systems. Running VMRM HA requires that extra CPU and memory resources be defined for each VIOS that is managed by VMRM HA. Add at least one 1-core CPU and 4 GB of memory above the VIOS sizing that is recommended for your production environment without VMRM HA. As you scale your environment, you should add at least one 1-core CPU and 10 GB of memory.
- Ensure that you have enough space in the KSYS LPAR so that the KSYS file sets can be installed successfully. You must have 30 MB of disk space in the `/opt` directory and 200 MB of disk space in the `/var` directory.
- Before you start the installation, you must check whether the KSYS software is installed by running the **`ksysmgr q cl`** command. If the KSYS software is installed, you must uninstall the software before proceeding.
- If you are installing VM Agents, ensure that each VM meets the following disk space requirements:
  - At least 100 MB of disk space in the `/usr` directory to install the VM Agent file sets
  - At least 1 GB of disk space in the `/var` directory for log files
- For a production environment, you must have two VIOSs per host. There is a maximum of 24 VIOSs in a single host group. If more than two VIOSs are running in a host, you can exclude specific VIOSs from VMRM HA management when you configure the KSYS configuration settings.

3.1.4 Host group requirements

A *host group* is a logical grouping of different servers (hosts) that are used to run your environment. VMs that are running in the host group are moved to other hosts in the same host group if a failure occurs. You can have more than one host group within your VMRM HA environment if you want to segment your applications into logical groups.

The following section describes the host group requirements for the VMRM HA:

- The host group can be named with a logical name that can be up to 64 characters.
- For each host group, the KSYS subsystem requires two disks for cluster health management. A disk of at least 10 GB, which is called the *repository disk*, is used for health monitoring of the hosts, and another disk of at least 10 GB, which is called the *HA disk*, is used for health data tracking for each host group. These disks must be accessible to all the VIOSs on each of the hosts on the host group, as shown in Figure 3-1. These disks are used to build a Shared Storage Pool (SSP) for the host group. The SSP is automatically built when the KSYS system is configured.
- At the time of writing, an SSP supports a maximum of 24 VIOSs per SSP cluster, which is why a host group can contain a maximum of 12 hosts with 24 VIOSs.
- All the hosts in the host group must be configured for network and storage so that any VM from any host can be migrated to any other host within the host group.
- A single KSYS LPAR can manage up to four host groups.

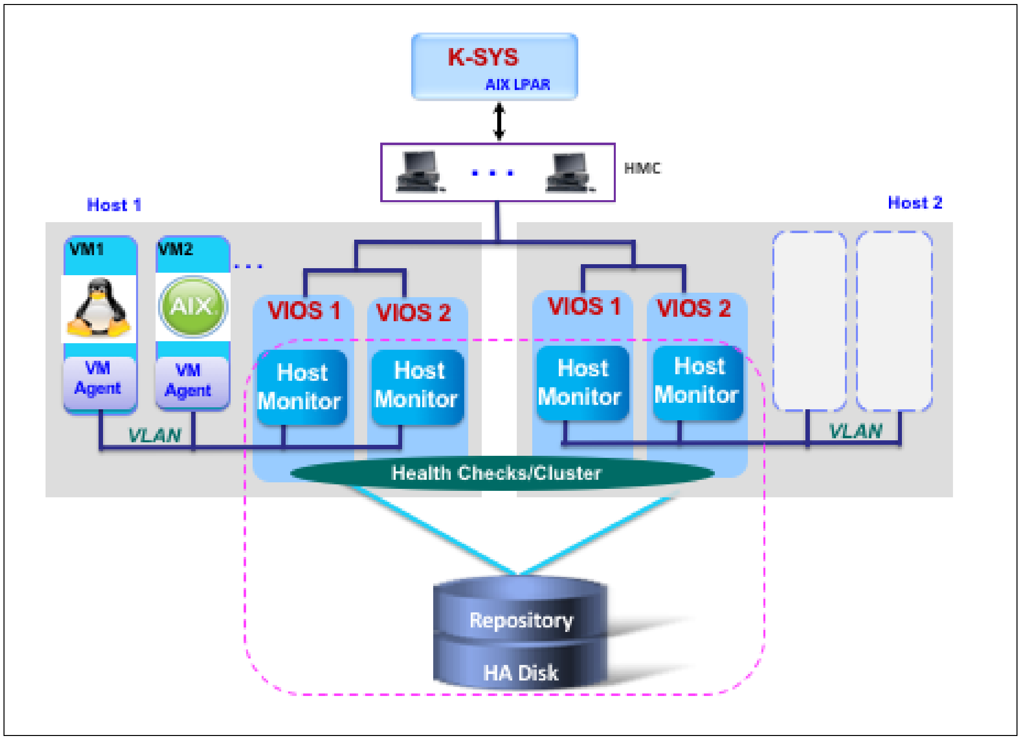
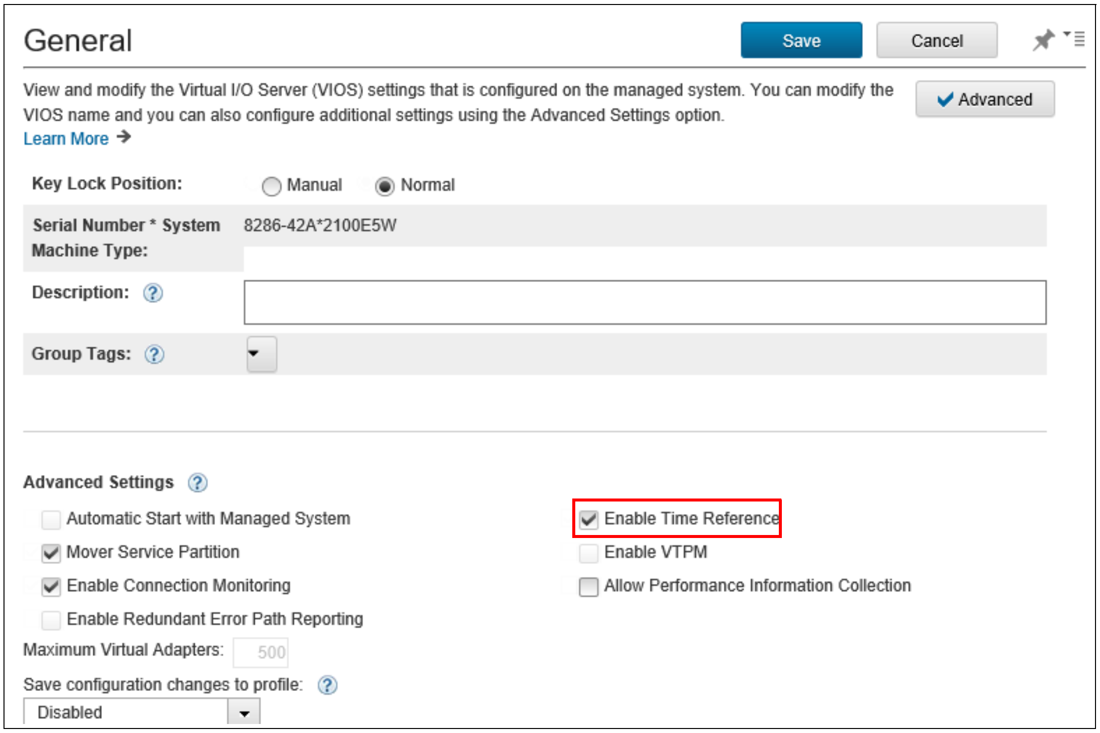


Figure 3-1 KSYS disk health cluster management

3.1.5 HMC requirements

The following section describes the HMC requirements for the VMRM HA:

- The VMRM HA solution requires HMC 9.9.1.0 or later. HMC 9 can manage POWER9, POWER8, and POWER7+ processor-based servers. To manage Power10 processor-based servers, you must have HMC 10. HMC 10 can manage Power10, POWER9, and POWER8 processor-based servers. A host group cannot have both Power10 and POWER7+ processor-based servers in the host group, but they can be managed in different host groups by using different HMCs. It is a best practice to have each host managed by two HMCs.
- Ensure that you can perform a Live Partition Mobility (LPM) operation on the VMs among the hosts that you want to be part of VMRM HA management. You can use HMC-based LPM validation to ensure that the VMs can move from a host to any other host in the host group.
- There are cases where the time-of-day clock might not be correctly updated when moving VMs from one host to another host, such as when the VM is running on POWER7+ processor-based servers or later and the Simplified Remote Restart (SRR) attribute is not set for that VM in the HMC. To retain the correct time-of-day clock for a VM across these hosts, you must set the VIOS partition profile on both the source host and destination host as the time reference partition. To do so, select **Time Reference Partition** in the HMC, as shown in Figure 3-2.



View and modify the Virtual I/O Server (VIOS) settings that is configured on the managed system. You can modify the VIOS name and you can also configure additional settings using the Advanced Settings option.

Key Lock Position: ○ Manual ● Normal

Serial Number * System Machine Type: 8286-42A*2100E5W

Description:

Group Tags:

Advanced Settings

□ Automatic Start with Managed System
☑ Mover Service Partition
☑ Enable Connection Monitoring
□ Enable Redundant Error Path Reporting
☑ Enable Time Reference
□ Enable VTPM
□ Allow Performance Information Collection

Maximum Virtual Adapters: 500

Save configuration changes to profile: Disabled

Figure 3-2 VIO partition properties: Selecting Enable Time Reference

- To migrate an IBM i VM from a source host to the destination host, verify that the **Restricted I/O Partition** checkbox for the IBM i LPAR is selected in the HMC. For more information about the steps to verify the restricted I/O mode, see IBM Documentation.
- Ensure that the `automatic reboot` attribute is not set for any VM in the HMC. The KSYS validates this attribute and prompts you to disable this attribute. Setting this attribute can lead to unpredictable results, such as a VM restart on two hosts simultaneously.
- When you add a host or manage a VM that is co-managed by the HMC and PowerVM NovaLink, set the HMC as the master mode. Otherwise, the discovery operation fails, and the VMs on the host will not be monitored for HA.

  When you are using PowerVM NovaLink to configure and monitor your VMs, you can register scripts to be plugged into VMRM HA. These scripts set the HMC to master mode for a brief period so that the KSYS subsystem can connect through the HMC to monitor the environment for HA. Sample scripts are provided which can be customized for your environment.

3.1.6 Network requirements

The following section describes the network requirements for VMRM HA:

- All VMs that are managed by the VMRM HA solution must use virtual I/O resources through the VIOS. The VMs must not be connected to any dedicated physical network adapter or have any dedicated devices.
- Storage area network (SAN) connectivity and zoning must be configured so that all the VIOSs can access the disks that are accessed by the hosts.
- Ensure that the KSYS LPAR has HTTP Secure (HTTPS) connectivity to all the HMCs that can manage the hosts in the host group.
- The same virtual LAN (VLAN) must be configured across the managed hosts.
- Ensure that a proper Resource Monitoring and Control (RMC) connection exists between the VMs and HMC. If the RMC connection between the VMs and the HMC has issues, the Partition Load Manager (PLM) cannot work and the VMs cannot be discovered.
- Ensure that redundant connections are established from the KSYS LPAR to the HMC and from the HMC to each VIOS LPAR, as shown in Figure 3-3 on page 49. Any connectivity issues between KSYS, the HMC, and the VIOS LPARs can lead to disruption in the regular data collection activity and HA actions.

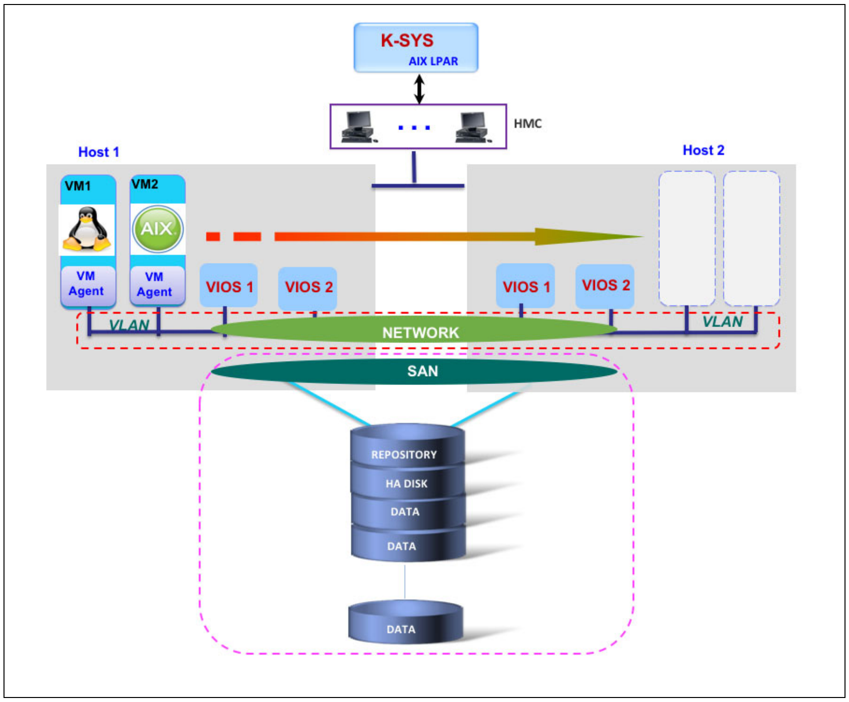


Figure 3-3 VMRM HA for network requirements

3.1.7 VMRM HA limitations

Consider the following restrictions for the VMRM HA solution:

- KSYS limitations
- KSYS LPM limitations
- VM agent limitations
- GUI limitations

KSYS limitations

- VMRM HA does not work if the LPM feature is disabled at the FW level.
- The following commands can be run without considering any policies:

  ```
  ksysmgr verify host_group <host_group_name>
  ksysmgr lpm host <host_name> action=validation
  ```

  Successful completion of the verification and validation operations does not mean that the VMs can be relocated successfully.
- The KSYS automatically builds an SSP for each host group when it is initialized (by using the two required disks per host group). The KSYS subsystem uses the format `KSYS_<peer domain>_<HG_ID>` to name an HA SSP. The KSYS subsystem uses this format to differentiate between an HA-defined SSP and a user-defined SSP. Therefore, you must not use this format for any user-defined SSPs.
- The KSYS subsystem supports the SSP cluster's HA disk only when the SSP is created from the KSYS subsystem. The KSYS subsystem does not display the HA disk in any query when you use a user-defined SSP cluster.
- You cannot modify a KSYS subsystem's HA disk after creating the SSP cluster from the KSYS node.

- When you remove the KSYS cluster, the KSYS subsystem sometimes fails to delete HA-specific VM and VIOS adapters. Delete the VIOS adapters manually to avoid inconsistencies across the VIOSs. If you create the KSYS cluster again, the KSYS subsystem can reuse the previous HA-specific adapters.
- To remove the KSYS cluster, run the following command:

  ```
  ksysmgr -f remove ksyscluster <ksyscluster_name>
  ```

- To remove the SSP cluster, from the padmin shell, run the following command in one of the VIOSs of the SSP cluster:

  ```
  cluster -remove
  ```

- To check whether the `hsmon` daemon is stopped in all VIOSs, run the following command:

  ```
  lssrc -s ksys_hsmon
  ```

- To stop the `hsmon` daemon in the VIOS, run the following command in all VIOSs:

  ```
  stopsrc -s ksys_hsmon -c
  ```

- After configuring a KSYS cluster and applications on that cluster, if you shut down a VM or an LPAR of the cluster, the KSYS subsystem does not change the status of the VM or LPAR to red. The status remains green. However, if you shut down the same VM or LPAR from the HMC, the KSYS subsystem changes the status of the VM or LPAR to red.
- A maximum of 10 scripts can be added in the KSYS subsystem for the **`add notify`** command.
- On VIOS nodes, if the disks of an SSP are not accessible after the system is reactivated due to a shutdown or restart, the disk state remains down. This situation impacts the start of the pool, and requires a quorum to come back online. As a workaround, choose one of the following options.

  If you do not want to restart your VIOS, use workaround option 1.

  – Workaround option 1: Complete the following procedure:

    i. Restore the disk connectivity.

    ii. Run the **`cfgmgr`** command as a root user to make the system aware of the disks.

    iii. Run the following command as `padmin`:

    ```
    clstartstop -stop -m <node>
    ```

    iv. Run the following command as `padmin`:

    ```
    clstartstop -start -m <node>
    ```

  – Workaround option 2: Complete the following procedure:

    i. Restore the disk connectivity.

    ii. Restart the VIOS node.

- Sometimes, the cleanup operation fails in the local database mode when a VM is configured with a virtual Small Computer System Interface (vSCSI) disk.

  Workaround: Bring the SSP cluster back to the global mode.

- If a VM has been shut down manually and a dependent application is part of the VM, the KSYS subsystem does not always handle the application dependency correctly.

- If a current repository disk is down, an automatic replacement does not occur by using a previously used repository disk that has the same cluster signature. In this case, the automatic replacement operation fails because a backup repository disk might not be available.

  Workaround: Run the following command to clear the previous cluster signatures:

  ```
  cleandisk -r <diskname>
  ```

- If there are many VMs spread across the hosts of a host group, then when the LPM verification operation is run on the host group, more requests might be sent to a host than the maximum number of requests that the host can handle. If so, the verification operation might fail with following error:

  ```
  HSCLB401 The maximum number of partition migration commands allowed are already
  in progress.
  ```

- If you upgrade the AIX operating system in the KSYS LPAR after upgrading the KSYS software, a few class IDs might be missing in the `/usr/sbin/rsct/cfg/ct_class_ids` file, and the KSYS daemon might stop working.

  Workaround: Run the following command to check whether the class IDs are reserved:

  ```
  cat /usr/sbin/rsct/cfg/ct_class_ids
  IBM.VMR_HMC 510
  IBM.VMR_CEC 511
  IBM.VMR_LPAR 512
  IBM.VMR_VIOS 513
  IBM.VMR_SSP 514
  IBM.VMR_SITE 515
  IBM.VMR_SA 516
  IBM.VMR_DP 517
  IBM.VMR_DG 518
  IBM.VMR_KNODE 519
  IBM.VMR_KCLUSTER 520
  IBM.VMR_HG 521
  IBM.VMR_APP 522
  IBM.VMR_CLOUD 523
  IBM.VMR_DP_CLD 524
  IBM.VMR_SA_CLD 525
  IBM.VMR_LPAR_CLD 526
  IBM.VMR_SITE_CLD 527
  IBM.VMR_VMG_CLD 528
  ```

  If any of the class IDs that are displayed in the preceding list are missing in your output, add the missing entries in the `/usr/sbin/rsct/cfg/ct_class_ids` file to restart the VMR services.

KSYS LPM limitations

- You cannot run an LPM operation simultaneously on multiple hosts by using multiple **ksysmgr** commands. Instead, you use a single **ksysmgr** command and provide a list of VMs (in a comma-separated list) to the command. This command works only if all the VMs in the list are present in the same host.
- The flexible capacity policy is applicable only on CPU and memory resources. It is not applied to I/O resources. Ensure that enough I/O resources are available in the target host.
- The flexible capacity policy is applicable only for VM failover operations. The flexible capacity function does not work when VMs are migrated by using the LPM operation.

- If a VM is migrated from host1 to host2 due to a failure, then when the applications in the VM become stable, an entry is made in the FailedHostList list of that application. If at a later point the application must be migrated due to an application failure when running on host2, host1 will not be considered as a backup for the application failure migration because the VM previously failed on host1.

  If host1 must be considered as a backup for future application failure, use the following workaround:

  Workaround: After the VM is stable on the host2, clear the FailedHostList list of the VM.

  Run the command **`chrsrc -s 'Name="VMName"' IBM.VMR_LPAR VmRestartFailedCecs='{""}'`** to clear the FailedHostList list for the VM.

- A discovery operation or a KSYS restart operation automatically starts dependency applications that were stopped by the user if they were stopped before the discovery or the restart of the KSYS subsystem.

  Workaround: Consider the following options:

  - Do not perform the discovery operation after stopping the dependency application.
  - Disable the auto discover and the quick discovery features.
  - Do not perform the KSYS subsystem restart.

VM agent limitations

- The **`ksysvmmgr start|stop app`** command supports only one application at a time.
- The **`ksysvmmgr suspend|resume`** command is not supported for the applications that are configured in an application dependency setup.
- For all applications that are installed on the non-rootvg disks, you must enable the *automatic varyon* option for volume groups and the *auto mount* option for file systems after the VM is restarted on the AIX operating system.
- If the application is in any of the failure states `NOT_STOPPABLE`, `NOT_STARTABLE`, `ABNORMAL`, or `FAILURE`, you must fix the failure issue, and then run the **`ksysvmmgr start|resume application`** command to start and monitor the application.
- If the KSYS cluster is deleted or if a VM is not included for the HA management, the VM agent daemon becomes inoperative. Manually restart the VM agent daemon in the VM to bring the VM agent daemon to an operative state.
- For the VMs running on the Linux VM agent, the restart operation might take longer than expected, and the rediscovery operation might fail and display the following message:

  ```
  Rediscovery has encountered error for VM VM_Name
  ```

  Workaround: Run the discovery operation after the VM is in the active state.

GUI limitations

- The VMRM HA GUI does not support multiple sessions that are originating from the same computer.
- The VMRM HA GUI does not support duplicate names for host group, HMC, host, VIOS, and VMs. If a duplicate name exists in the KSYS configuration, the GUI might have issues during host group creation or in displaying the dashboard data.
- The VMRM HA GUI refreshes automatically after each topology change (for example, VM migration operation and host migration operation). After the refresh operation is complete, the default KSYS dashboard is displayed. Expand the topology to view the log information in the Activity window for a specific entity.
- Any operation that is performed by a user from the command-line interface (CLI) of VMRM HA is not displayed in the activity window of the VMRM HA GUI.

Miscellaneous

- The VMRM HA solution does not support the internet Small Computer Systems Interface (iSCSI) disk type. Only NPIV and vSCSI disk types are supported.
- If you are using a user-defined SSP cluster and you want to add a host or VIOS to the environment, you must add it to the SSP cluster first. Then, you can add the host or VIOS to the KSYS cluster. Also, if you want to remove a host or VIOS from the environment, you must first remove it from the KSYS cluster and then remove it from the SSP cluster.
- VMRM HA supports only detailed-type snapshot.
- After each **`manage`** VIOS operation and **`unmanage`** VIOS operation, you must perform a **`discovery`** operation.

Errors that the KSYS subsystem cannot handle

The KSYS subsystem automatically restarts the VMs only when the KSYS subsystem is certain of the failures. If the KSYS subsystem is unsure, it sends an alert message to the administrator to review the issue and to manually restart VMs if required.

Sometimes, the KSYS subsystem cannot identify whether the host failure is real or if the host failure is because of a partitioned network. The KSYS subsystem does not automatically restart VMs in the following example scenarios:

- When the KSYS subsystem cannot connect to the HMC to quiesce the failed VM (fencing operation) on the source host before restarting the VM on the target host. The fencing operation is required to ensure that the VM is not running on two hosts simultaneously.
- The host monitor (HM) module and the VIOS can monitor their own network and storage. Sometimes, network and storage errors are reported by the VIOS, and these error events notifications are sent to the administrator through email and text messages. In these cases, the KSYS subsystem does not move the VMs automatically to avoid false relocation.
- When a host group is spread across two buildings with storage subsystem technologies such as IBM SAN Volume Controller HyperSwap, where HMCs, hosts and other required resources exist in each building and the KSYS LPAR is deployed on the backup building, the following scenarios cannot be automatically handled:
  - Power failure in the main building: The KSYS subsystem cannot connect to the HMCs and hosts in the primary site. The KSYS subsystem detects the host failure and notifies the administrator.
  - Issues in network and storage partitioning between the buildings: The KSYS subsystem cannot connect to the HMCs, and notifies the administrator about the host failure. The administrator must review the environment and decide whether to move the VMs. The VMs might be operating correctly on the main host. The administrator can rectify the network links between the hosts, and the KSYS subsystem will start operating in normal mode.

3.1.8 GUI requirements

The following section describes the GUI requirements for the VMRM HA:

- The LPAR in which you want to install the GUI file sets must be running AIX 7.2 with Technology Level 2 Service Pack 1 (7200-02-01) or later. You can choose to install the GUI server file set on one of the KSYS nodes.
- The LPAR in which you are installing the GUI server must run in an Enhanced Korn shell that uses the **`/usr/bin/ksh93`** shell script.

- The LPAR in which you are installing the GUI server file set must have at least one 1-core CPU and 8 GB of memory. If you are installing the GUI server file set on the KSYS node, ensure that the required resources are available on the KSYS node to accommodate the GUI.
- Google Chrome and Mozilla Firefox web browsers support access to the GUI for the VMRM HA solution.

Installation and usage of the GUI is described in Chapter 9, “IBM VMRM GUI deployment” on page 237.

3.2 VMRM HA file sets and structure

The VMRM HA package consists of file sets for the installation of KSYS, VM Agent, and GUI.

The following sections describe the key components of the VMRM HA solution.

KSYS

KSYS is the base product software that must be installed on an AIX LPAR. It provides the technical foundation of VMRM HA and command-line-based administration by using the **`ksysmgr`** and **`ksysrppmgr`** commands.

Here are the KSYS file sets:

- `ksys.ha.license`
- `ksys.main.cmds`
- `ksys.main.msg.en_US.cmds`
- `ksys.main.rte`
- `ksys.hautils.rte`

The following file sets are the specific language command files for languages other than English:

- `ksys.main.msg.en_US.cmds`
- `ksys.main.msg.DE_DE.cmds`
- `ksys.main.msg.ES_ES.cmds`
- `ksys.main.msg.FR_FR.cmds`
- `ksys.main.msg.IT_IT.cmds`
- `ksys.main.msg.JA_JP.cmds`
- `ksys.main.msg.PT_BR.cmds`
- `ksys.main.msg.ZH_CN.cmds`
- `ksys.main.msg.ZH_TW.cmds`

VM Agent

The VM Agent is an optional file set that can be installed on the managed VMs that are running either AIX or Linux operating systems. If you install the VM Agent, you can monitor the individual VMs and the applications that are running in the VM. Otherwise, only host level monitoring is supported.

- AIX VM Agent file set:

  `ksys.vmmon.rte`

- RHEL VM Agent package:

  `vmagent-1.7.0-1.0.el7.ppc64le`

- SUSE Linux Enterprise Server package:

  `vmagent-1.7.0-1.0.suse123.ppc64le`

GUI

An optional file set that can be installed on an AIX LPAR for accessing the VMRM HA solution by using a GUI. You can install the GUI in the KSYS LPAR, but you should consider LPAR resources like CPU and memory allocation. The GUI can be installed on a different LPAR in your environment.

- `ksys.ui.agent`: The GUI agent file set that must be installed on the KSYS nodes.
- `ksys.ui.server`: A GUI server file set that must be installed on the system that manages the KSYS nodes. This file set can be installed on one of the KSYS nodes.
- `ksys.ui.common`: A GUI common file set that must be installed along with both the `ksys.ui.server` (GUI server) file set and the `ksys.ui.agent` (GUI agent) file set.

3.3 Installing VMRM HA

The VMRM HA solution provides HA management for IBM Power servers with PowerVM virtualization. After you plan the implementation of VMRM HA, you can install the VMRM HA software. The VMRM HA uses other components such as HMCs and VIOSs that must be in your production environment.

The KSYS software requires AIX 7.2 TL2 SP1 or later for the OS running on the LPAR that it is installed in. In addition, the following software must be installed:

- VIOS 3.1.2.40 or later must be installed on all VIOS partitions that are part of the host group. HM, which is a key component of the VMRM HA solution, is installed on the VIOS by default. The HM component is enabled and used when you install the VMRM HA file sets. VMRM HA requires two VIOSs per host.
- HMC 9.9.1.0 or later must be used to manage all hosts that are part of the cluster. If IBM Power10 hosts are in the cluster, the HMC must be Version 10 to manage those hosts. In this case, only IBM POWER8, IBM POWER9, and IBM Power10 processor-based hosts are allowed in the host group.

Figure 3-4 shows the components of VMRM HA.

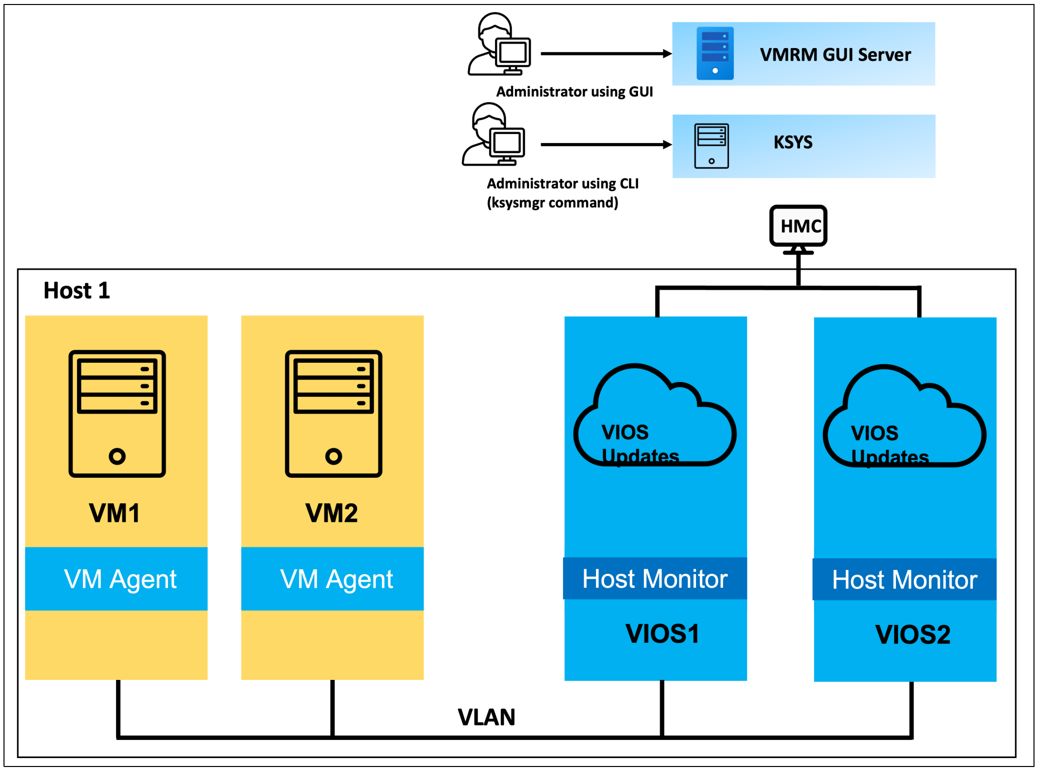


Figure 3-4 Components of VMRM HA

To install the VMRM HA solution, you must first install the KSYS file sets. After the KSYS software is installed and the cluster is configured, the KSYS subsystem automatically monitors the health of hosts by enabling the HMs in the VIOS partitions of each host that is part of the VMRM HA management.

If you intend to have VM- and application-level monitoring for AIX or Linux VMs, install the VM Agents into those LPARs. To manage the environment with a GUI, install the GUI server on an AIX LPAR in your environment. You connect to the GUI server by using your browser.

Complete the following procedures to install the VMRM HA solution:

1. Install the VIOS interim fix if you run a VIOS level less than 3.1.1.
2. Install the KSYS software.
3. Optional: Install VM Agents into the VMs.
4. Optional: Install the GUI server.

3.3.1 Installing the VIOS interim fix

Table 3-2 on page 57 shows the required interim fix for the level of VIOS that you are running. Download the interim fix and install it before installing VMRM HA for Power 1.7. The interim fix should be installed in each VIOS before you initialize the KSYS subsystem. The installation process is shown in this section.

Table 3-2 VIOS interim fix by VIOS

VIOS level	Interim fix	Download location
Version 3.1.4.10	IJ44264	https://aix.software.ibm.com/aix/ifixes/ij44264/IJ44263m5a.221124.epkg.Z
Version 3.1.3.21	IJ44264	https://aix.software.ibm.com/aix/ifixes/ij44264/IJ44275m4a.221115.epkg.Z
Version 3.1.2.40	IJ44264	https://aix.software.ibm.com/aix/ifixes/ij44264/IJ44277m4a.221115.epkg.Z

Important: Install the interim fix before you initialize the KSYS subsystem.

If you have a shared pool that is configured in your environment, ensure that there are no active cluster services. Stop any active cluster services by running the following command:

```
clstartstop -stop -n clustername -m hostname
```

Run the command in each of the managed VIOS instances, as shown in Example 3-1.

Example 3-1 Installing the VIOS interim fix

```
$ updateios -install -dev /home/padmin/vios_fix -accept

*******************************************************************************
EFIX MANAGER PREVIEW START
*******************************************************************************


+-----------------------------------------------------------------------------+
Efix Manager Initialization
+-----------------------------------------------------------------------------+
Initializing log /var/adm/ras/emgr.log ...

+-----------------------------------------------------------------------------+
Processing Efix Package 1 of 1.
```

Example 3-2 shows the continuation of the installation of the VIOS interim fix.

Example 3-2 Accepting the installation of the VIOS interim fixes

```
+-----------------------------------------------------------------------------+
Efix package file is: /home/padmin/vios_fix/IJ10896m2a.181102.epkg.Z
MD5 generating command is /usr/bin/csum
MD5 checksum is 961dcf33ab5bcbd2d8b0adefcbc57f10
Accessing efix metadata ...
Processing efix label "IJ10896m2a" ...
Verifying efix control file ...
*******************************************************************************
EFIX MANAGER PREVIEW END
*******************************************************************************


+-----------------------------------------------------------------------------+
Operation Summary
+-----------------------------------------------------------------------------+
Log file is /var/adm/ras/emgr.log

EPKG NUMBER       LABEL               OPERATION              RESULT
===========       ==============      =================      ==============
1                 IJ10896m2a          INSTALL PREVIEW        SUCCESS

ATTENTION: system reboot will be required by the actual (not preview) operation.
Please see the "Reboot Processing" sections in the output above or in the
/var/adm/ras/emgr.log file.

Return Status = SUCCESS

Continue the installation [y|n]?Y
```

Example 3-3 shows the summary of the installation of the VIOS interim fix.

Example 3-3 Summary of the installation of VIOS interim fix

```
+------------------------------------------------------------------------------+
Operation Summary
+------------------------------------------------------------------------------+
Log file is /var/adm/ras/emgr.log

EPKG NUMBER       LABEL               OPERATION              RESULT
===========       ==============      =================      ==============
1                 IJ10896m2a          INSTALL                SUCCESS

ATTENTION: system reboot is required. Please see the "Reboot Processing"
sections in the output above or in the /var/adm/ras/emgr.log file.

Return Status = SUCCESS

File /etc/inittab has been modified.

One or more of the files listed in /etc/check_config.files have changed.
        See /var/adm/ras/config.diff for details.
$
```

Note: The installation output of the VIOS interim fix was truncated to save space.

Verify whether the installation of the interim fix is successful by running **lssw**, as shown in Example 3-4.

Example 3-4 Final output of the lssw command

```
ID  STATE LABEL      INSTALL TIME      UPDATED BY ABSTRACT
=== ===== ========== ================= ========== ==============================
1    S    IJ10896m2a 04/01/23 15:56:38       Fixes to support VM Recover Manager

STATE codes:
S = STABLE
```

Important: After the installation successfully completes, a system restart is required.

If the cluster services were stopped, start the cluster services by running the following command:

```
clstartstop -start -n clustername -m hostname
```

3.3.2 Installing the KSYS software

You can use either smitty or the **installp** command in the AIX LPAR to install KSYS file sets that are included in the package.

To install the KSYS software, complete the following steps:

1. Ensure that all the prerequisites that are specified in 3.1, “VMRM HA requirements” on page 44 are complete.
2. Go to the directory that contains the images that you want to install and run the command that is shown in Example 3-5.

Example 3-5 Installing the KSYS software

```
# installp -acFXYd . -V2 ksys.hautils.rte ksys.ha.license ksys.main.cmds
ksys.main.msg.en_US.cmds ksys.main.rte ksys.ui.agent ksys.ui.common
```

3. Verify whether the installation of file sets is successful by running the command that is shown in Example 3-6.

Example 3-6 Listing the file sets that are installed at the KSYS node

```
# lslpp -l ksys.ha.license ksys.hautils.rte ksys.main.cmds ksys.main.msg.en_US.cmds
ksys.main.rte
  File set                      Level  State      Description
  ----------------------------------------------------------------------------
Path: /usr/lib/objrepos
  ksys.ha.license            1.7.0.0  COMMITTED  Base Server Runtime
  ksys.hautils.rte           1.7.0.0  COMMITTED  Base Server Runtime
  ksys.main.cmds             1.7.0.0  COMMITTED  Base Server Runtime
  ksys.main.msg.en_US.cmds   1.7.0.0  COMMITTED  Base Server Runtime
  ksys.main.rte              1.7.0.0  COMMITTED  Base Server Runtime

Path: /etc/objrepos
  ksys.hautils.rte           1.7.0.0  COMMITTED  Base Server Runtime
  ksys.main.cmds             1.7.0.0  COMMITTED  Base Server Runtime
  ksys.main.rte              1.7.0.0  COMMITTED  Base Server Runtime
```

4. To check the command-line utility of the KSYS subsystem, run the **/opt/IBM/ksys/ksysmgr** command, as shown in Example 3-7. The KSYS subsystem might take a few minutes to run the command for the first time. You can add the `/opt/IBM/ksys` directory to your PATH environment variable so that you can access the **ksysmgr** command easily.

Example 3-7 Checking the ksysmgr command

```
# /opt/IBM/ksys/ksysmgr
No command arguments found
ksysmgr [-v] [-f] [-i] [-t] [-l {low|med|max}]
       [-a {<ATTR>,<ATTR#2>,...}] <ACTION> <CLASS> [<NAME>]
       [-h | <ATTR>=<VALUE> <ATTR#2>=<VALUE#2> ...]

ksysmgr [-v] [-f] [-t] [-l {low|med|high|max}]
       [-a {<ATTR>,<ATTR#2>,...}] <ACTION> <CLASS>"
       [<NAME>] [<ATTR>=<VALUE> <ATTR#2>=<VALUE#2> ...]
.
      ACTION={add|modify|delete|query|manage|unmanage|...}
       CLASS={ksyscluster|hmc|host|...}
```

```
ksysmgr {-h|-?} [-v] [<ACTION>[ <CLASS>]]
ksysmgr [-v] help

Here is a list of available actions for ksysmgr:
Available actions
         add
         delete
         discover
         help
         manage
         unmanage
         modify
         query
         recover
         restore
         restart
         report
         cleanup
         sync
         verify
         lpm
         refresh
         start
         stop
         trace
```

5. After you have successfully installed the KSYS file sets, check whether the class IDs that are shown in Example 3-8 by running the command that is shown in the example.

Example 3-8 Checking the ID class

```
# cat /usr/sbin/rsct/cfg/ct_class_ids | grep IBM.VMR
IBM.VMR_HMC                                      510
IBM.VMR_CEC                                      511
IBM.VMR_LPAR                                     512
IBM.VMR_VIOS                                     513
IBM.VMR_SSP                                      514
IBM.VMR_SITE                                     515
IBM.VMR_SA                                       516
IBM.VMR_DP                                       517
IBM.VMR_DG                                       518
IBM.VMR_KNODE                                    519
IBM.VMR_KCLUSTER                                 520
IBM.VMR_HG                                       521
IBM.VMR_APP                                      522
IBM.VMR_CLOUD                                    523
IBM.VMR_DP_CLD                                   524
IBM.VMR_SA_CLD                                   525
IBM.VMR_LPAR_CLD                                 526
IBM.VMR_SITE_CLD                                 527
IBM.VMR_VMG_CLD                                  528
IBM.VMR_APP_CLD                                  529
```

6. If the `IBM.VMR_APP` class is not available in the output, manually add the `IBM.VMR_APP 522` entry into the `/usr/sbin/rsct/cfg/ct_class_ids` file and refresh the Reliable Scalable Cluster Technology (RSCT) subsystem by running the command that is shown in Example 3-9 on page 61.

Example 3-9 Refreshing the RSCT subsystem

```
# rmcctrl -z
#
# rmcctrl -s
0513-059 The ctrmc Subsystem has been started. Subsystem PID is 19661060.
#
```

3.4 Configuring VMRM HA

After the VMRM HA solution is installed, you must complete some mandatory configuration steps before you use the HA feature of the VMRM HA solution.

You can use the **ksysmgr** command or the VMRM HA GUI to interact with the KSYS daemon to manage the entire environment for HA. For an example of configuring VMRM HA by using the GUI, see 9.4, “Configuring VMRM HA by using the GUI” on page 245.

The VMRM HA solution monitors the hosts and the VMs when you add information about your environment to the KSYS. To set up the KSYS subsystem, complete the following steps:

1. Initialize the KSYS cluster.
2. Add HMCs.
3. Add hosts.
4. Create host groups.
5. Configure VIOSs.
6. Configure VMs.
7. Set contacts for event notification.
8. Enable the HA monitoring.
9. Discover and verify the KSYS configuration.
10. Optional: Back up the configuration data.

The ksysmgr command

In the following sections, the **ksysmgr** command is used to start adding resources to the KSYS node configuration. You notice that the **ksysmgr** command accepts aliases, for example, using the **ksysmgr create cluster** command has the same effect as using the **ksysmgr add ksyscluster** command:

```
ksysmgr add ksyscluster [<ksysclustername>] type=<HA>
      ksysnodes=<ksysnode1,ksysnode2>
      [sync=<yes|no>]
    add => ad*, cr*, make, mk
    ksyscluster => ksyscl*, cl*
```

To find the syntax and aliases of every action or parameter that is accepted by the **ksysmgr** command, use the **-h** option, as shown in Example 3-10.

Example 3-10 Finding the syntax and every option that is accepted by ksysmgr

```
# ksysmgr -h
No command arguments found

ksysmgr [-v] [-f] [-i] [-t] [-l {low|med|max}]
[-a {<ATTR>,<ATTR#2>,...}] <ACTION> <CLASS> [<NAME>]
[-h | <ATTR>=<VALUE> <ATTR#2>=<VALUE#2> ...]

ksysmgr [-v] [-f] [-t] [-l {low|med|high|max}]
```

```
[-a {<ATTR>,<ATTR#2>,...}] <ACTION> <CLASS>"
[<NAME>] [<ATTR>=<VALUE> <ATTR#2>=<VALUE#2> ...].
ACTION={add|modify|delete|query|manage|unmanage|...}
CLASS={ksyscluster|hmc|host|...}

ksysmgr {-h|-?} [-v] [<ACTION>[ <CLASS>]]
ksysmgr [-v] help


Here is a list of available actions for ksysmgr:
Available actions
         add
         delete
         discover
         help
         manage
         unmanage
         modify
         query
         recover
         restore
         restart
         report
         cleanup
         sync
         verify
         lpm
         refresh
         start
         stop
         trace
```

3.4.1 Initializing the KSYS cluster

The KSYS environment relies on RSCT, which is a built-in component in AIX to create its cluster on the KSYS LPAR. After you create the KSYS cluster, various daemons of RSCT and KSYS are activated. Then, the KSYS node can process the commands that you specify in the CLI. This section describes how to create a single node KSYS cluster.

Starting with VMRM 1.7, you can create a multi-node cluster for HA without external clustering products, such as IBM PowerHA SystemMirror. HA KSYS clusters are described in Chapter 8, “KSYS high availability” on page 217.

Important: Be sure to populate the `/etc/hosts` file on all KSYS LPARs by adding the IP address or name resolution of all KSYS LPARs, HMCs, VIOSs, IP addresses, and storage.

To create and initialize a KSYS cluster, complete the following steps in your KSYS LPARs:

1. Configure a single node cluster and add the KSYS node to the cluster by running the command that is shown in Example 3-11.

Example 3-11 Creating a cluster and adding a KYSYS node to the cluster

```
# ksysmgr add ksyscluster <ksysclustername> ksysnodes=$(uname -n) type=HA
Adding node to current cluster configuration
Ksyscluster has been created, please run: "ksysmgr verify ksyscluster
<ksysclustername>"
```

2. Verify the KSYS cluster configuration by running the command that is shown in Example 3-12.

Example 3-12 Verifying the cluster configuration

```
# ksysmgr verify ksyscluster <ksysclustername>
Verified, Please run: "ksysmgr sync ksyscluster <ksysclustername>"
```

3. Deploy the KSYS cluster by running the command that is shown in Example 3-13.

Example 3-13 Deploying the KSYS cluster

```
# ksysmgr sync ksyscluster <ksysclustername>
Starting KSYS subsystem ...
   Waiting for KSYS subsystem to start ...
KSYS subsystem has started, you can begin adding HMCs, Hosts, etc
```

Steps 1 - 3 can be done by using a single command, as shown in Example 3-14.

Example 3-14 Creating and deploying a KSYS cluster

```
# ksysmgr add ksyscluster <ksysclustername> ksysnodes=$(uname -n) type=HA sync=yes
Adding node to current cluster configuration
Ksyscluster has been created, running verify now
Ksyscluster has been verified, running sync now
Starting KSYS subsystem ...
   Waiting for KSYS subsystem to start ...
KSYS subsystem has started, you can begin adding HMCs, Hosts, etc
```

4. Verify that the KSYS cluster is created successfully by running one of the commands that are shown in Example 3-15.

Example 3-15 Verifying the KSYS cluster

```
# ksysmgr query ksyscluster
Name:                ha-test
State:               Online
Type:                HA
Ksysnodes:           VMR_cluster:1:Online

# lsrpdomain
Name    OpState RSCTActiveVersion MixedVersions TSPort GSPort
ha-test Online  3.2.6.4           No            12347  12348

# lssrc -s IBM.VMR
Subsystem        Group           PID          Status
 IBM.VMR         rsct_rm         12124460     active
```

Important: The output message must display the state of the KSYS cluster as `Online`.

Adding more nodes to your existing single node KSYS cluster is described in 8.2, “Creating a 2-node or multi-node KSYS cluster” on page 223.

If you are building a KSYS environment, it is possible to create a two node KSYS cluster by running a single command:

```
ksysmgr add ksyscluster cluster_name ksysnodes=ksys_nodename1,ksys_nodename2
type=HA
```

3.4.2 Adding HMCs

The KSYS interacts with the HMC for discovery, verification, monitoring, recovery, LPM, and cleanup operations. HMCs provide details about the hosts and VIOS partitions that are managed by the HMCs. The VMRM HA solution cannot be implemented without configuring the HMCs.

Note: The HMC user, whose username and password details are provided to the KSYS, must have at least `hmcsuperadmin` privileges and remote access. The KSYS subsystem uses the Representational State Transfer (REST) application programming interface (API) to communicate with the HMCs in the environment. Therefore, ensure that your environment allows HTTPS communication between the KSYS and HMC subsystems.

To add the HMCs to the KSYS configuration setting, complete the following steps in the KSYS LPAR:

1. Add the HMC by using the **`ksysmgr add hmc`** command. Example 3-16 shows adding two HMCs, one with username `powervc` and password `P@ssw0rd` and the other with username `hscroot` and password `xyz123`.

Example 3-16 Adding the HMC

```
# ksysmgr add hmc prdthmc01 login=powervc password=P@ssw0rd ip=172.25.33.41
HMC prdthmc01 added successfully

# ksysmgr add hmc prdthmc02 login=hscroot password=abc123 ip=172.25.33.42
HMC prdthmc02 added successfully
```

2. Repeat step 1 to add more HMCs.
3. Verify the HMCs that you added by running the command that is shown in Example 3-17.

Example 3-17 Listing the HMC that is added to the KSYS

```
# ksysmgr query hmc
Name:                prdthmc01
Ip:                  172.25.33.41
Login:               powervc

                        Managed Host List:

Hostname                               UUID
=========                               ====
SN0287333-1080hex1                30e536a4-34f5-3d6c-b461-401bbbbbbbbb
```

```
SN0286bbb-1080hex2                48ea164e-e539-32a5-bbdb-7a1bbbbbbbbb
============================================================================
Name:                prdthmc02
Ip:                  172.25.33.42
Login:               hscroot

                        Managed Host List:
Hostname                               UUID
=========                               ====
e52m3-8408-E8D-21DD71T                  e17e3ddc-71cc-327f-884b-4fa6a411bbb9
e60m2-8408-E8D-21DD4DT                  2d8b3d3a-ca43-3147-9d02-fd999bfc7ff4
e46m4-8247-22L-2123D7A                  5f322ea0-00dd-3615-acbb-a958add020b2
rt13-8286-42A-21E0B2V                   4462c37c-65c6-3614-b02a-aa09d752c2ee
e52m2-8408-E8D-21DD44T                  ac43f075-3a03-3509-864a-cfd979139cb0
rt11-8286-42A-0607585                   d04d8a4a-99fa-3e4b-80bc-c9d9716bd8f8
e46m5-8247-22L-212A71A                  c13ac0ed-f458-3b2e-be92-bf61b0e88933
e60m3-8408-E8D-21DD4BT                  a71b1e42-4f08-360d-910a-7689b17eb09b
============================================================================
```

This output shows all managed hosts for each HMC.

3.4.3 Adding hosts

After the HMCs are added to the KSYS subsystem, you can review the list of hosts that are managed by each HMC, as shown in Example 3-17 on page 64, and then identify the hosts that you want to add to the KSYS for HA.

To add hosts to the KSYS configuration, complete the following steps in the KSYS LPAR:

1. Add the managed hosts `SN0287333-1080hex1` and `SN0286bbb-1080hex2` to the KSYS by running the command that is shown in Example 3-18.

Example 3-18 Adding hosts to the KSYS

```
# ksysmgr add host SN0287333-1080hex1
Host SN0287333-1080hex1 added successfully

# ksysmgr add host SN0286bbb-1080hex2
Host SN0286bbb-1080hex2 added successfully
```

Tip: If the host is connected to more than one HMC, you must specify the Universally Unique Identifier (UUID) of the host.

2. Repeat step 1 for all hosts that you want to add to the KSYS subsystem.
3. Verify the hosts that you added by running the command that is shown in Example 3-19.

Example 3-19 Verifying hosts that are added to the KSYS

```
# ksysmgr q host
Name:                SN028bbbb-1080hex2
UUID:                48ea164e-e539-32a5-bbdb-7abbbbbbb
FspIp: Must run discovery first to populate
Host_group: No host_group defined
VIOS:                E10802VIOS2
                     E10802VIOS1
```

```
HMCs:                prdthmc01
Proactiveha:         disable
Lpm_support:         None
VM_failure_detection_speed:    fast
MachineSerial:       028bbbb
ProcPools:           DefaultPool

Name:                SN0287333-1080hex1
UUID:                30e536a4-34f5-3d6c-b461-40abbbbbbb
FspIp: Must run discovery first to populate
Host_group: No host_group defined
VIOS:                E10801VIOS2
                     E10801VIOS1
HMCs:                plgiephmc
Proactiveha:         disable
Lpm_support:         None
VM_failure_detection_speed:    normal
MachineSerial:       028bbbb
ProcPools:           DefaultPool
```

3.4.4 Creating host groups

You can group a set of hosts depending on your business requirements. Each host in the KSYS subsystem must be a part of a host group.

The KSYS subsystem creates an SSP cluster across the VIOSs that are part of the host group for monitoring the health of the environment. The cluster monitors the health of all VIOSs across the cluster and retains the health data that is available to the KSYS subsystem by using a VIOS on the host group. The SSP cluster is used only by the KSYS. Do not use this SSP cluster for any other purpose.

You can continue to use vSCSI or NPIV modes of the cluster. However, if an SSP cluster exists in your environment, the KSYS subsystem does not deploy new SSP clusters, but instead uses the existing SSP cluster for health management. However, if an existing SSP cluster is used, the KSYS subsystem might not support VIOS management.

The KSYS subsystem requires two disks to create the health monitoring SSP cluster across the VIOSs on the host group. A disk of at least 10 GB is required to monitor VIOS heartbeat across all hosts, which called as repository disk, and another disk of at least 10 GB is required to track health data, which is called a HA disk, for each host group. These disks must be accessible to all the managed VIOSs on each of the hosts on the host group. Specify the disk details when you create the host group or before you run the first discovery operation. You cannot modify the disks after the discovery operation runs successfully. If you want to modify the disks, you must delete the host group and re-create the host group with the disk details.

To create a host group in the KSYS subsystem, complete the following steps in the KSYS LPAR:

1. Identify all VIOSs that are managed by KSYS, as shown in Example 3-20.

Example 3-20 Listing all VIOSs that are managed by KSYS

```
# ksysmgr query vios
Name:                E10802VIOS1
UUID:                37D77A24-932B-4ECA-947D-47C546CD2E94
Host:                SN028bbbb-1080hex2
Version:             VIOS 3.1.4.10
State:               MANAGED
HMstate:             Yes
Last_response:       1 seconds
MAC_address:         4A9EF9B69513
HM_versions:         2.00
                     2.01
                     2.02

Name:                E10802VIOS2
UUID:                2E2170D2-3D7A-4289-A540-9331B398A473
Host:                SN028bbbb-1080hex2
Version:             VIOS 3.1.4.10
State:               MANAGED
HMstate:             Yes
Last_response:       1 seconds
MAC_address:         4A9EF7CA820C
HM_versions:         2.00
                     2.01
                     2.02

Name:                E10801VIOS1
UUID:                2F995825-EE49-409C-A74E-C3FDE4EC808A
Host:                SN028bbbb-1080hex1
Version:             VIOS 3.1.4.10
State:               MANAGED
HMstate:             Yes
Last_response:       0 seconds
MAC_address:         C2D843DAA40D
HM_versions:         2.00
                     2.01
                     2.02

Name:                E10801VIOS2
UUID:                51D72581-1A2A-426B-A4D2-613C302CC066
Host:                SN028bbbb-1080hex1
Version:             VIOS 3.1.4.10
State:               MANAGED
HMstate:             Yes
Last_response:       1 seconds
MAC_address:         C2D8468B6F0E
HM_versions:         2.00
                     2.01
                     2.02

Name:                TEST-old_vios
```

```
UUID:                 55F05794-AF34-45E2-83DF-4DE40A7D6B7E
Host:                 rN028bbbb-1080hex1
Version:              VIOS 3.1.0.00
State:                MANAGED
HM_versions:          Unknown
```

2. To identify all the available shared disks by VIOS so that you can designate the repository disk and the HA disk for the SSP cluster, run the commands that are shown in Example 3-21.

Example 3-21 Identifying all available shared disks by VIOS

```
# ksysmgr query viodisk vios=rt12v1,rt12v2,rt11v1,rt11v2

Looking for free shared disks in these VIOSs:
E10802VIOS2
        E10801VIOS1
        E10802VIOS1
        E10801VIOS2

This can take a few minutes

These are the shared free disks which appear on all VIOS in the list provided:
DiskNames are as they appear on VIOS E10801VIOS1

DiskName         Size             ViodiskID
---------------------------------------------------------------------------------
hdisk0           20480
01M0lCTTIxNDUxMjQ2MDA1MDc2ODAyODEwNDI2ODgwMDAwMDAwMDAwMDExMA==
hdisk2           20480
01M0lCTTIxNDUxMjQ2MDA1MDc2ODAyODEwNDI2ODgwMDAwMDAwMDAwMDExMQ==
hdisk3           20480
01M0lCTTIxNDUxMjQ2MDA1MDc2ODAyODEwNDI2ODgwMDAwMDAwMDAwMDExMg==
hdisk4           20480
01M0lCTTIxNDUxMjQ2MDA1MDc2ODAyODEwNDI2ODgwMDAwMDAwMDAwMDExRA==
```

It also is possible to identify all available shared disks by host, as shown in Example 3-22.

Example 3-22 Identifying all available shared disks by hosts

```
# ksysmgr query viodisk hosts=rt12-8286-42A-2100E5W,rt11-8286-42A-0607585

Looking for free shared disks in these VIOSs:
E10802VIOS2
        E10801VIOS1
        E10802VIOS1
        E10801VIOS2

This can take a few minutes

These are the shared free disks which appear on all VIOS in the list provided:
DiskNames are as they appear on VIOS E10801VIOS1

DiskName         Size             ViodiskID
--------------------------------------------------------------------------------
hdisk0           20480
01M0lCTTIxNDUxMjQ2MDA1MDc2ODAyODEwNDI2ODgwMDAwMDAwMDAwMDExMA==
hdisk2           20480
01M0lCTTIxNDUxMjQ2MDA1MDc2ODAyODEwNDI2ODgwMDAwMDAwMDAwMDExMQ==
hdisk3           20480
01M0lCTTIxNDUxMjQ2MDA1MDc2ODAyODEwNDI2ODgwMDAwMDAwMDAwMDExMg==
hdisk4           20480
01M0lCTTIxNDUxMjQ2MDA1MDc2ODAyODEwNDI2ODgwMDAwMDAwMDAwMDExRA==
```

3. Create a host group and add the hosts and disks (by using `ViodiskID` information) that you want in this host group by running the command that is shown in Example 3-23.

Example 3-23 Creating a host group

```
ksysmgr add host_group HEX2_PRD_HG  hosts=SN028bbbb-1080hex1,SN028bbbb-1080hex2
repo_disk=01M0lCTTIxNDUxMjQ2MDA1MDc2ODAyODEwNDI2ODgwMDAwMDAwMDAwMDExMA==
ha_disk=01M0lCTTIxNDUxMjQ2MDA1MDc2ODAyODEwNDI2ODgwMDAwMDAwMDAwMDExMQ==
Host_group ITSO_HG added successfully
Run discover command to proceed further
```

4. Repeat step 1 on page 65 for all host groups that you want to create in the KSYS subsystem.

5. Verify the host groups that you created by running the command that is shown in Example 3-24.

Example 3-24 Listing host groups

```
# ksysmgr query host_group */or #ksysmgr q hg
Name:                 HEX2_PRD
Hosts:                SN028bbbb-1080hex1
                      SN028bbbb-1080hex2
Memory_capacity:      Priority-Based Settings
                      low:100
                      medium:100
                      high:100
CPU_capacity:         Priority-Based Settings
                      low:100
                      medium:100
                      high:100
Skip_power_on:        None
Sriov_override:       No
HA_monitor:           enable
Lpm_support:          None
Proactiveha:          enable
Restart_policy:       auto
VM_failure_detection_speed:    normal
Host_failure_detection_time:   90

SSP Cluster Attributes (will be populated after discovery)
Sspname:              KSYS_ha-test_1
Ssp_version:          VIOS 3.1.4.10
VIOS:                 E10801VIOS2
                      E10802VIOS1
                      E10801VIOS1
                      E10802VIOS2
Repo_disk:
01M0lCTTIxNDUxMjQ2MDA1MDc2ODAyODEwNDI2ODgwMDAwMDAwMDAwMDExMA==
HA_disk:
01M0lCTTIxNDUxMjQ2MDA1MDc2ODAyODEwNDI2ODgwMDAwMDAwMDAwMDExMQ==
```

Enable HA monitoring for the KSYS subsystem to start monitoring the environment. To check whether HA monitoring is active, run the **ksysmgr query system** command. If HA monitoring is active, then `HA_monitor` shows `enable`, as shown in Example 3-25.

Example 3-25 Listing system-wide persistent attributes

```
# ksysmgr query system
System-Wide Persistent Attributes
auto_discovery_time:         00:00 hours
notification_level:          low
dup_event_processing:        yes
HA_monitor:                  enable
host_failure_detection_time: 90 seconds
vm_failure_detection_time:   normal
proactiveha:                 enable
network_isolation:           none
quick_discovery_interval:    60 minutes
quick_discovery:             enable
deep_discovery:              enable
vm_auto_discovery:           enable
custom_script_timeout:       none
trace_file_size:             not set
memory_capacity:     Priority-Based settings
                             low:100
                             medium:100
                             high:100
cpu_capacity:        Priority-Based settings
                             low:100
                             medium:100
                             high:100
ping:                        enable
lpm_support:                 enable
port_validation:             disable
min_redundancy_paths:        disable
cleanup_files_interval:      7 days
ksys_lang:
optimise_put_storage:        disable
connection_timeout:          75 seconds (default)
hmc_ping_timer:              0 seconds
sa_ping_timer:               0 seconds
User Scripts for Host Group: None

User Scripts for VM: None
```

If you need to enable HA monitoring, run the command that is shown in Example 3-26.

Example 3-26 Enabling HA monitoring

```
# ksysmgr modify system ha_monitor=enable
KSYS ha_monitor has been updated
```

Then, you can validate the setting by using the command that is shown in Example 3-25.

3.4.5 Discovering and verifying the KSYS configuration

After adding various resources (HMCs, hosts, and host groups) to the KSYS subsystem, you must run the discovery operation. During the initial discovery operation, the KSYS subsystem creates the required HA setup to monitor the VMs and hosts. The KSYS subsystem creates an SSP cluster based on the information that is specified in the configuration steps. During any subsequent discovery operations, the KSYS subsystem scans the environment for any changes to the environment and adapts to the modified environment.

For example, when you add a host or when you run the LPM operation from one host to another host that is outside of the current KSYS subsystem, the KSYS configuration settings are updated in the next discovery operation.

By default, the KSYS subsystem automatically rediscovers sites once every 24 hours at midnight. You can change this period by modifying the **`auto_discover_time`** system attribute.

After the KSYS subsystem discovers the resources, a verification is required to ensure that the VMs can be restarted on another host without any errors during a failover operation. The first discovery operation can take a few minutes because the SSP health cluster is deployed during the first discovery operation.

To discover and verify the configuration for a specific host group, complete the following steps:

1. Discover the resources by running the following command:

   ```
   ksysmgr discover host_group hg_name
   ```

2. Verify the resources by running the following command:

   ```
   ksysmgr verify host_group hg_name3
   ```

Important: Run the discovery and verification commands each time that you modify the resources in the KSYS subsystem.

To perform both the discovery and verification operations, run the command that is shown in Example 3-27.

Example 3-27 Running discovery and verification of the KSYS configuration

```
# ksysmgr -t discover hg HEX2_PRD verify=yes
06:12:22  Running discovery on Host Group HEX2_PRD, this may take a few minutes...
        Existing HA trunk adapter found for VIOS E10801VIOS1
        Creating HA trunk adapter for VIOS E10801VIOS1
        Finished creating HA trunk adapter for VIOS E10801VIOS1
        Creating HA trunk adapter for VIOS E10801VIOS2
        Finished creating HA trunk adapter for VIOS E10801VIOS2
        Creating HA trunk adapter for VIOS E10802VIOS1
        Finished creating HA trunk adapter for VIOS E10802VIOS1
        SSP creation started for Host_group HEX2_PRD
        SSP creation completed for Host_group HEX2_PRD
        Preparing VIOS in SN028bbbb-1080hex1 for HA management
        VIOS in SN028bbbb-1080hex1 prepared for HA management
        Preparing VIOS in SN028bbbb-1080hex2 for HA management
        VIOS in SN028bbbb-1080hex2 prepared for HA management
        Discovery has started for VM rt11002
        Configuration information retrieval started for VM rt11002
        Discovery has started for VM rt12005
        Configuration information retrieval started for VM rt12005
        Discovery has started for VM rt11009
        Configuration information retrieval started for VM rt11009
```

```
        Discovery has started for VM rt11005
        Configuration information retrieval started for VM rt11005
        Discovery has started for VM rt11001
        Configuration information retrieval started for VM rt11001
        Discovery has started for VM rt12004
        Configuration information retrieval started for VM rt12004
        Discovery has started for VM rt12003
        Configuration information retrieval started for VM rt12003
        Discovery has started for VM rt12002
        Configuration information retrieval started for VM rt12002
        Discovery has started for VM rt12001
        Configuration information retrieval started for VM rt12001
        Discovery has started for VM rt11004
        Configuration information retrieval started for VM rt11004
        Discovery has started for VM rt11007
        Configuration information retrieval started for VM rt11007
        Discovery has started for VM rt11003
        Configuration information retrieval started for VM rt11003
        Discovery has started for VM rt11010
        Configuration information retrieval started for VM rt11010
        Discovery has started for VM rt11008
        Configuration information retrieval started for VM rt11008
        Discovery has started for VM rt11006
        Configuration information retrieval started for VM rt11006
        Configuration information retrieval completed for VM rt11002
        Discovery for VM rt11002 is complete
        Configuration information retrieval completed for VM rt12005
        Discovery for VM rt12005 is complete
        Configuration information retrieval completed for VM rt11009
        Discovery for VM rt11009 is complete
        Configuration information retrieval completed for VM rt11005
        Discovery for VM rt11005 is complete
        Configuration information retrieval completed for VM rt11001
        Discovery for VM rt11001 is complete
        Configuration information retrieval completed for VM rt12004
        Discovery for VM rt12004 is complete
        Configuration information retrieval completed for VM rt12003
        Discovery for VM rt12003 is complete
        Configuration information retrieval completed for VM rt12002
        Discovery for VM rt12002 is complete
        Configuration information retrieval completed for VM rt12001
        Discovery for VM rt12001 is complete
        Configuration information retrieval completed for VM rt11004
        Discovery for VM rt11004 is complete
        Configuration information retrieval completed for VM rt11007
        Discovery for VM rt11007 is complete
        Configuration information retrieval completed for VM rt11003
        Discovery for VM rt11003 is complete
        Configuration information retrieval completed for VM rt11010
        Discovery for VM rt11010 is complete
        Configuration information retrieval completed for VM rt11008
        Discovery for VM rt11008 is complete
        Configuration information retrieval completed for VM rt11006
        Discovery for VM rt11006 is complete
Discovery has finished for ITSO_HG
15 out of 15 managed VMs have been successfully discovered

Host_group verification started for ITSO_HG
        rt11002 verification has started
        rt12005 verification has started
        rt11009 verification has started
        rt11005 verification has started
        rt11001 verification has started
        rt12004 verification has started
        rt12003 verification has started
        rt12002 verification has started
        rt12001 verification has started
        rt11004 verification has started
        rt11007 verification has started
        rt11003 verification has started
        rt11010 verification has started
        rt11008 verification has started
        rt11006 verification has started
        rt11002 verification has completed
        rt11010 verification has completed
        rt11009 verification has completed
        rt12001 verification has completed
        rt11008 verification has completed
        rt12005 verification has completed
        rt11004 verification has completed
        rt11003 verification has completed
        rt11005 verification has completed
        rt12002 verification has completed
        rt11001 verification has completed
        rt12003 verification has completed
        rt12004 verification has completed
        ERROR: Verify has encountered an error for VM rt11007
        ERROR: Verify has encountered an error for VM rt11006
Verification has finished for ITSO_HG
13 out of 15 VMs have been successfully verified
Unverified VMs:
        rt11007
        rt11006

Following error is returned for VM rt11007:
Errors:\nHSCL2957 Either there is currently no RMC connection between the management
console and the partition rt11007 (9*8286-42A*0607585) or the partition does not support
dynamic partitioning operations. Verify the network setup on the management console and the
partition and ensure that any firewall authentication between the management console and
the partition has occurred. Run the management console diagrmc command to identify problems
that might be causing no RMC connection.\n\nDetails:\nHSCL2957 Either there is currently no
RMC connection between the management console and the partition rt11007
(9*8286-42A*0607585) or the partition does not support dynamic partitioning operations.
Verify the network setup on the management console and the partition and ensure that any
firewall authentication between the management console and the partition has occurred. Run
the management console diagrmc command to identify problems that might be causing no RMC
connection.\n\nJob execution on HMC failed with status <COMPLETED_WITH_ERROR>. Message:
<Errors:\nHSCL2957 Either there is currently no RMC connection between the management
console and the partition rt11007 (9*8286-42A*0607585) or the partition does not support
dynamic partitioning operations. Verify the network setup on the management console and the
partition and ensure that any firewall authentication between the management console and
the partition has occurred. Run the management console diagrmc command to identify problems
that might be causing no RMC connection.\n\nDetails:\nHSCL2957 Either there is currently no
RMC connection between the management console and the partition rt11007
(9*8286-42A*0607585) or the partition does not support dynamic partitioning operations.
Verify the network setup on the management console and the partition and ensure that any
firewall authentication between the management console and the partition has occurred. Run
the management console diagrmc command to identify problems that might be causing no RMC
connection.\n>.
```

```
Following error is returned for VM rt11006:
Errors:\nHSCL2957 Either there is currently no RMC connection between the management
console and the partition rt11006 (6*8286-42A*2100E5W) or the partition does not support
dynamic partitioning operations. Verify the network setup on the management console and the
partition and ensure that any firewall authentication between the management console and
the partition has occurred. Run the management console diagrmc command to identify problems
that might be causing no RMC connection.\n\nDetails:\nHSCL2957 Either there is currently no
RMC connection between the management console and the partition rt11006
(6*8286-42A*2100E5W) or the partition does not support dynamic partitioning operations.
Verify the network setup on the management console and the partition and ensure that any
firewall authentication between the management console and the partition has occurred. Run
the management console diagrmc command to identify problems that might be causing no RMC
connection.\n\nJob execution on HMC failed with status <COMPLETED_WITH_ERROR>. Message:
<Errors:\nHSCL2957 Either there is currently no RMC connection between the management
console and the partition rt11006 (6*8286-42A*2100E5W) or the partition does not support
dynamic partitioning operations. Verify the network setup on the management console and the
partition and ensure that any firewall authentication between the management console and
the partition has occurred. Run the management console diagrmc command to identify problems
that might be causing no RMC connection.\n\nDetails:\nHSCL2957 Either there is currently no
RMC connection between the management console and the partition rt11006
(6*8286-42A*2100E5W) or the partition does not support dynamic partitioning operations.
Verify the network setup on the management console and the partition and ensure that any
firewall authentication between the management console and the partition has occurred. Run
the management console diagrmc command to identify problems that might be causing no RMC
connection.\n>.

Please review the error(s) and take any corrective actions
```

Note: Example 3-27 on page 71 shows that the VMs `rt11006` and `rt11007` have errors because they have RMC connection problems.

Configuring VIOSs

When you add hosts to the KSYS subsystem, all the VIOSs on the hosts are added to the KSYS subsystem. The VMRM HA solution monitors the hosts and VMs by using the VIOSs on the host.

The VMRM HA solution requires at least two VIOSs per host. You can have a maximum of 24 VIOSs across different hosts in a single host group. If a host has more than two VIOSs, you can exclude specific VIOS partitions from HA management.

To exclude specific VIOS partitions from HA management, run the following command:

```
ksysmgr unmanage vios viosname
```

Configuring virtual machines

When a host is added to the KSYS subsystem, all the VMs on the host are included by default in the HA management. If you do not want HA for any of the VMs, you can exclude specific VMs from the HA management by running the following command with the appropriate flags:

```
ksysmgr unmanage vm name=vmname host=hostname | uuid=lparuuid |
                    ALL host=hostname | ALL host_group=hg_name
```

In Example 3-28, the VMs `rt11006`, `rt11007`, `rt11008`, `rt1009`, and `rt11010` were unmanaged.

Example 3-28 Unmanaging VMs

```
# ksysmgr unmanage vm name=rt11006,rt11007,rt11008,rt11009,rt11010
VM rt11006 was successfully unmanaged. Please run discovery to apply changes
VM rt11007 was successfully unmanaged. Please run discovery to apply changes
VM rt11008 was successfully unmanaged. Please run discovery to apply changes
VM rt11009 was successfully unmanaged. Please run discovery to apply changes
VM rt11010 was successfully unmanaged. Please run discovery to apply changes
```

To list all VMs and query all managed and unmanaged VMs, run the **`ksysmgr query vm`** command, as shown in Example 3-29.

Example 3-29 Querying VMs

```
# ksysmgr query vm
Managed VMs:
        rt11002
        rt12005
        rt11005
        rt11001
        rt12004
        rt12003
        rt12002
        rt12001
        rt11004
        rt11003

Unmanaged VMs:
        rt11009
        rt11007
        rt11010
        rt11008
        rt11006
```

After you change the host group `ITSO_HG`, perform discovery and verification, as shown in Example 3-30.

Example 3-30 Performing discovery and verification after unmanaging VMs

```
# ksysmgr discover  host_group HEX2_PRD verify=yes
Running discovery on Host_group ITSO_HG, this may take few minutes...
.
.
.
Discovery has finished for ITSO_HG
10 out of 10 managed VMs have been successfully discovered
.
.
.
Verification has finished for ITSO_HG
10 out of 10 VMs have been successfully verified
```

Enabling HA monitoring at the VM and application level

At this moment, you have HA monitoring only at the host level. To enable HA monitoring at the VM and application levels, you must install the VM Agent for HA monitoring, which is described in 7.2, “Setting up the VM Agent” on page 202.

After installing the VM Agent for HA monitoring, you start the daemon agent by running the **ksysvmmgr start** command in each VM.

Example 3-31 shows how to start VM monitor (VMM) on AIX VMs.

Example 3-31 Starting VMM on AIX VMs

```
# ksysvmmgr status
Subsystem         Group            PID          Status
 ksys_vmm                                       inoperative

(0) root @ rt11001: /
# ksysvmmgr start
0513-059 The ksys_vmm Subsystem has been started. Subsystem PID is 17957374.

(0) root @ rt11001: /
# ksysvmmgr status
Subsystem         Group            PID          Status
 ksys_vmm                          17957374     active
```

Example 3-32 shows how to start VMM on Red Hat VMs.

Example 3-32 Starting VMM on Red Hat VMs

```
# ksysvmmgr status
ksys_vmm daemon is currently inoperative.

(0) root @ rt11004: /root
# ksysvmmgr start
ksys_vmm has been started.

(0) root @ rt11004: /root
# ksysvmmgr status
ksys_vmm daemon is active.
```

Example 3-33 shows how to start VMM on SUSE VMs.

Example 3-33 Starting VMM on SUSE VMs

```
# ksysvmmgr status
ksys_vmm daemon is currently inoperative.

(0) root @ rt11005: /root
# ksysvmmgr start
ksys_vmm has been started.

(0) root @ rt11005: /root
# ksysvmmgr status
ksys_vmm daemon is active.
```

Now that VMM is enabled on the VMs, you must enable KSYS HA monitoring at the VM level for each VM by running the following command:

```
ksysmgr modify vm vm1[,vm2,...] ha_monitor=enable
```

In Example 3-34, the VMs rt11001, rt11002, rt11003, rt11004, rt11005, rt12001, rt12002, rt12003, rt12004, and rt12005 were changed to enable the ha_monitor.

Example 3-34 Enabling the HA VM monitoring level on KSYS

```
# ksysmgr modify vm
rt11001,rt11002,rt11003,rt11004,rt11005,rt12001,rt12002,rt12003,rt12004,rt12005
ha_monitor=enable
For VM rt11002 attribute(s) 'ha_monitor' was successfully modified.
For VM rt12005 attribute(s) 'ha_monitor' was successfully modified.
For VM rt11005 attribute(s) 'ha_monitor' was successfully modified.
For VM rt11001 attribute(s) 'ha_monitor' was successfully modified.
For VM rt12004 attribute(s) 'ha_monitor' was successfully modified.
For VM rt12003 attribute(s) 'ha_monitor' was successfully modified.
For VM rt12002 attribute(s) 'ha_monitor' was successfully modified.
For VM rt12001 attribute(s) 'ha_monitor' was successfully modified.
For VM rt11004 attribute(s) 'ha_monitor' was successfully modified.
For VM rt11003 attribute(s) 'ha_monitor' was successfully modified.
```

Run discovery and verification after VMM is enabled, as shown in Example 3-35.

Example 3-35 Performing discovery and verification after enabling VMM

```
# ksysmgr discover  host_group ITSO_HG verify=yes
Running discovery on Host_group ITSO_HG, this may take few minutes...
.
.
.
        Creating first HA client adapter for VM rt12001
        Finished creating first HA client adapter for VM rt12001
        Creating first HA client adapter for VM rt12005
        Creating second HA trunk client for VM rt12001
        Finished creating second HA client adapter for VM rt12001
        Finished creating first HA client adapter for VM rt12005
        Creating second HA trunk client for VM rt12005
        Finished creating second HA client adapter for VM rt12005
        Creating first HA client adapter for VM rt12003
        Finished creating first HA client adapter for VM rt12003
        Creating second HA trunk client for VM rt12003
        Finished creating second HA client adapter for VM rt12003
.
.
.
        Starting HA monitoring for VM rt12001
        Starting HA monitoring for VM rt12005
        HA monitoring for VM rt12001 started successfully
        HA monitoring for VM rt12005 started successfully
        Starting HA monitoring for VM rt12003
        HA monitoring for VM rt12003 started successfully
        Starting HA monitoring for VM rt12002
        Starting HA monitoring for VM rt12004
        HA monitoring for VM rt12002 started successfully
        Starting HA monitoring for VM rt11001
        HA monitoring for VM rt12004 started successfully
        HA monitoring for VM rt11001 started successfully
        Starting HA monitoring for VM rt11004
.
.
.
```

```
        VM monitor state has moved to 'STARTED' for VM rt11002
        VM monitor state has moved to 'STARTED' for VM rt12005
        VM monitor state has moved to 'STARTED' for VM rt11005
        VM monitor state has moved to 'STARTED' for VM rt11001
        VM monitor state has moved to 'STARTED' for VM rt12004
        VM monitor state has moved to 'STARTED' for VM rt12003
        VM monitor state has moved to 'STARTED' for VM rt12002
        VM monitor state has moved to 'STARTED' for VM rt12001
        VM monitor state has moved to 'STARTED' for VM rt11004
        VM monitor state has moved to 'STARTED' for VM rt11003
.
.
Verification has finished for ITSO_HG
10 out of 10 VMs have been successfully verified
```

3.5 Setting up HA policies

After you set up the KSYS subsystem successfully, set up recovery policies to customize the default configuration settings to suit your HA preferences.

This section describes the VMRM HA solution options that you can customize.

Note: Run the discovery and verification command after you set any policy.

3.5.1 HA monitoring policies

An HA monitoring policy turns on or off HA monitoring for the associated entity. The specified policy at the lowest resource level is considered first for HA monitoring. If you do not specify this policy for a resource, the policy of the parent resource is applied to the resource. For example, if you enable HA monitoring for the host group, HA monitoring is enabled for all the hosts within the host group unless you disable HA monitoring for specific hosts.

You can enable HA monitoring for VMs only after you install the VM Agent on each VM and start the VM Agent successfully. If you do not set up the VM Agent, the KSYS subsystem returns error messages for HA monitoring at the VM level.

To set the HA monitoring, run the following command:

```
ksysmgr modify system|host_group|host|vm name ha_monitor=enable|disable
```

Example 3-36 shows the **ksysmgr query system** command that checks the HA monitoring for the KSYS.

Example 3-36 Checking HA monitoring for the KSYS

```
# ksysmgr query system
System-Wide Persistent Attributes
auto_discovery_time:        00:00 hours
notification_level:         low
dup_event_processing:       yes
ha_monitor:                 enable
host_failure_detection_time: 90 seconds
vm_failure_detection_speed:  normal
User Scripts for Host Group:
```

To check HA monitoring for the host group, run the **ksysmgr query host_group** command that is shown in Example 3-37.

Example 3-37 Checking HA monitoring for the host group

```
# ksysmgr query host_group
Name:                ITSO_HG
Hosts:               rt12-8286-42A-2100E5W
                     rt11-8286-42A-0607585
Memory_capacity:     Priority-Based Settings
                     high:100
                     medium:100
                     low:100
CPU_capacity:        Priority-Based Settings
                     high:100
                     medium:100
                     low:100
Skip_power_on:       No
HA_monitor:          enable
Restart_policy:      auto
VM_failure_detection_speed:    normal
Host_failure_detection_time:   90
```

To check the HA monitoring for the VM rt11001, run the **ksysmgr query vm** command that is shown in Example 3-38.

Example 3-38 Checking the HA monitoring for the VM rt11001

```
# ksysmgr query vm rt11001
Name:                rt11001
UUID:                3BF44186-0679-4032-BF4C-95B24901822A
State:               READY_TO_MOVE
Host:                rt12-8286-42A-2100E5W
Priority:            Medium
VM_failure_detection_speed:    normal
HA_monitor:          enable
Homehost:            rt12-8286-42A-2100E5W
VM_status:           NO_OPERATION_IN_PROGRESS
Version_conflict:    No
```

3.5.2 Environment-level policies

This section describes the environment-level policies.

Restart policy

The *restart policy* notifies the KSYS subsystem to restart the VMs automatically during a failure. This attribute can have the following values:

auto If you set this attribute to `auto`, the KSYS subsystem automatically restarts the VMs on the destination hosts. The KSYS subsystem identifies the most suitable host based on available CPUs, memory, and other specified policies. In this case, the KSYS subsystem also notifies the registered contacts about the host or VM failure and the restart operations. This value is the default value of the **restart_policy** attribute.

advisory_mode If you set this attribute to `advisory_mode`, the VMs are not restarted automatically after host or VM failures. In this case, the KSYS subsystem notifies the registered contacts about the host or VM failures. The administrator must review the failure and manually restart the VMs on other hosts by using the **ksysmgr** commands.

To set the restart policy, run the following command:

```
ksysmgr modify host_group name restart_policy=auto|advisory_mode
```

For example, to check the restart policy of the host group `ITSO_HG`, we run the command **ksysmgr query host_group**, as shown in Example 3-39.

Example 3-39 Checking the restart_policy of the host group ITSO_HG

```
# ksysmgr query host_group
Name:                ITSO_HG
Hosts:               rt12-8286-42A-2100E5W
                     rt11-8286-42A-0607585
Memory_capacity:     Priority-Based Settings
                     high:100
                     medium:100
                     low:100
CPU_capacity:        Priority-Based Settings
                     high:100
                     medium:100
                     low:100
Skip_power_on:       No
HA_monitor:          enable
Restart_policy:      auto
VM_failure_detection_speed:    normal
Host_failure_detection_time:   90
```

Host failure detection time

The *host failure detection time policy* indicates the time that the KSYS waits on a nonresponsive host before the KSYS declares the host to be in an inactive state. This value is measured in seconds. The KSYS subsystem uses the specified time to ensure the health of the host and attempts to connect to the host before the KSYS declares the failure. After this duration, the VMs are restarted on another host that is within the host group. The value of this attribute can be 90 – 600 seconds. The default value is 90 seconds.

To set the host failure detection time, run the following command:

```
ksysmgr modify system|host_group name host_failure_detection_time=time_in_seconds
```

To check the KSYS host failure detection time, we run the command **ksysmgr query system**, as shown in Example 3-40.

Example 3-40 Checking the KSYS host failure detection time

```
# ksysmgr query system
System-Wide Persistent Attributes
auto_discovery_time:         00:00 hours
notification_level:          low
dup_event_processing:        yes
ha_monitor:                  enable
host_failure_detection_time: 90 seconds
vm_failure_detection_speed:  normal
```

To check the host group failure detection time, we use the **ksysmgr query host_group** command, as shown in Example 3-41.

Example 3-41 Checking the host group host failure detection time

```
# ksysmgr query host_group
Name:                ITSO_HG
Hosts:               rt12-8286-42A-2100E5W
                     rt11-8286-42A-0607585
Memory_capacity:     Priority-Based Settings
                     high:100
                     medium:100
                     low:100
CPU_capacity:        Priority-Based Settings
                     high:100
                     medium:100
                     low:100
Skip_power_on:       No
HA_monitor:          enable
Restart_policy:      auto
VM_failure_detection_speed:    normal
Host_failure_detection_time:   90
```

Flexible capacity policy

The *flexible capacity policy* modifies the allocation of memory and CPU resources of a VM when a VM is moved from its home host to another host on the host group. You can set flexible capacity values based on the priority of a VM. You can set different flexible capacity values for various priorities of VMs: high, medium, and low. Specify the flexible capacity values in percentage.

For example, you can define the following flexible capacity values at the host group level: 100% CPU and 100% memory for high priority VMs; 70% CPU and 80% memory for medium priority VMs; and 60% CPU and 75% memory for low-priority VMs. When a medium priority VM is migrated from its home host to another host on the host group, its capacity is adjusted to 70% CPU and 80% memory. If the VM is restored back to its home host, the VM is restored with 100% resources.

The flexible capacity policy does not consider I/O slots, adapters, and resources that are available on the hosts. Ensure that all the I/O virtualization requirements of the VMs are met within the host group environment. Also, the flexible capacity policy is applicable only to VM relocation that is based on restart operations. LPM operations do not follow the flexible capacity policy.

To set the flexible capacity policy, run the following command:

```
ksysmgr modify host_group
     [memory_capacity=(1-100) | minimum | current_desired | none]
[priority=low|medium|high]
     [cpu_capacity=(1-100) | minimum | current_desired | none]
[priority=low|medium|high]
```

Example 3-42 shows the default settings of the flexible capacity policy for the host group `ITSO_HG`.

Example 3-42 Listing the flexible capacity policies of the host group ITSO_HG

```
# ksysmgr query  host_group
Name:               ITSO_HG
Hosts:              rt12-8286-42A-2100E5W
                    rt11-8286-42A-0607585
Memory_capacity:    Priority-Based Settings
                    high:100
                    medium:100
                    low:100
CPU_capacity:       Priority-Based Settings
                    high:100
                    medium:100
                    low:100
```

In Example 3-43, the flexible capacity policies were set as follows:

- Memory capacity to 60% for medium-priority VMs
- CPU capacity to 70% for medium-priority VMs
- Memory capacity to 50% for low-priority VMs
- CPU capacity to 50% for low-priority VMs

Example 3-43 Changing the flexible capacity policies

```
# ksysmgr modify host_group ITSO_HG options memory_capacity=60 priority=medium
For Host_group ITSO_HG attribute(s) 'memory_capacity', 'priority' was successfully modified

# ksysmgr modify host_group ITSO_HG options cpu_capacity=70 priority=medium
For Host_group ITSO_HG attribute(s) 'cpu_capacity', 'priority' was successfully modified

# ksysmgr modify host_group ITSO_HG options memory_capacity=50 priority=low
For Host_group ITSO_HG attribute(s) 'memory_capacity', 'priority' was successfully
modified.

# ksysmgr modify host_group ITSO_HG options cpu_capacity=50 priority=low
For Host_group ITSO_HG attribute(s) 'cpu_capacity', 'priority' was successfully modified
```

Example 3-44 shows the host group ITSO_HG after changing its flexible capacity policies.

Example 3-44 Checking the flexible capacity policies after changing them for ITSO_HG

```
# ksysmgr query  host_group
Name:                    ITSO_HG
Hosts:                   rt12-8286-42A-2100E5W
                         rt11-8286-42A-0607585
Memory_capacity:         Priority-Based Settings
                         high:100
                         medium:60
                         low:50
CPU_capacity:            Priority-Based Settings
                         high:100
                         medium:70
                         low:50
```

Affinity policies

An *affinity policy* specifies affinity rules for a set of VMs that defines how the VMs must be placed within a host group during a relocation. The following affinity policies are supported if all VMs in an affinity group have the same priority.

Collocation

A *collocation policy* indicates that the set of VMs must always be placed on the same host after relocation, as shown in Figure 3-5.

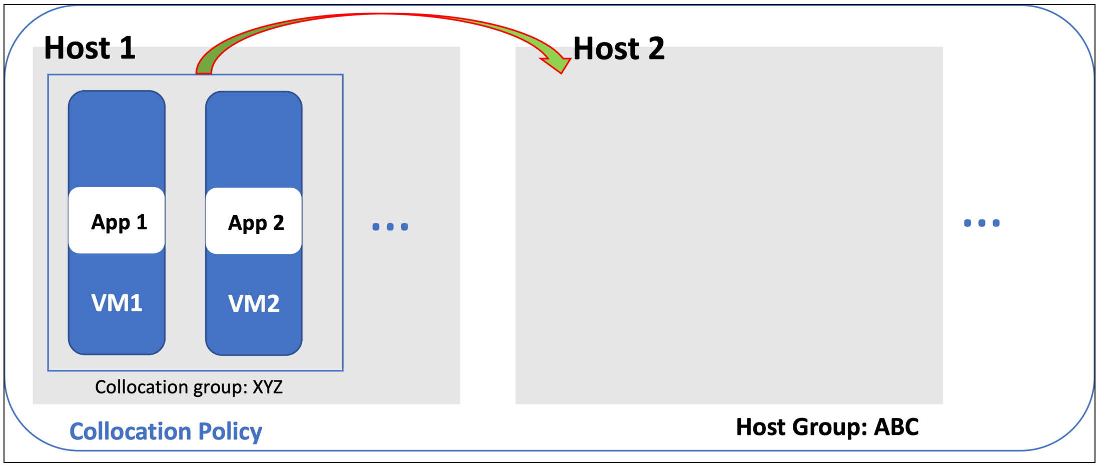


Figure 3-5 Collocation policy

To set this policy, run the following commands:

```
ksysmgr add collocation name vm=vmname1[,...]>
ksysmgr modify collocation name policy=add|delete vm=vm1[,...]
```

Example 3-45 shows the collocation policy policy_1 for the VMs rt12001, r12002, and 12003.

Example 3-45 Creating a collocation policy

```
# ksysmgr add collocation policy_1 vm=rt12001,rt12002,rt12003
Collocation group policy_1 was created
```

To list the collocation policies that are available, run the command **ksysmgr query collocation**, as shown in Example 3-46.

Example 3-46 Listing the collocation policies

```
# ksysmgr query collocation
Name:                    policy_1
Type:                    Collocation
VMs:                     rt12003
                         rt12002
                         rt12001
```

Example 3-47 shows how to delete a collocation policy.

Example 3-47 Deleting a collocation policy

```
# ksysmgr delete collocation policy_1
Collocation group policy_1 was removed
```

Anticollocation

An *anticollocation policy* indicates that the set of VMs must never be placed on the same host after relocation. In Figure 3-6, when Host 1 fails, VM3 and VM4 are set to anticollocation with VM1 and VM2 so that they restart on different hosts.

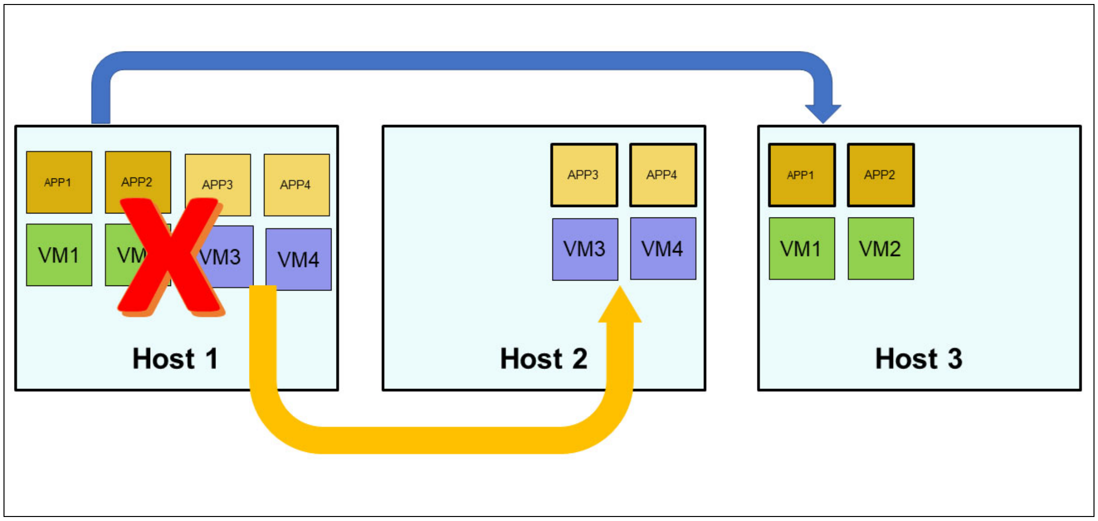


Figure 3-6 Anticollocation policy

To set this policy, run the following commands:

```
ksysmgr add anticollocation name vm=vmname1[,...]>
ksysmgr modify anticollocation name policy=add|delete vm=vm1[,...]
```

Example 3-48 shows the anticollocation policy `policy_2` with the VMs `rt12001` and `rt12002`.

Example 3-48 Creating an anticollocation policy

```
# ksysmgr add anticollocation policy_2 vm=rt12001,rt11001
Anticollocation group policy_2 was created
```

To list the anticollocation policies that are available, run the command **ksysmgr query anticollocation**, as shown in Example 3-49.

Example 3-49 Listing the anticollocation policies

```
# ksysmgr query anticollocation
Name:                policy_2
Type:                anticollocation
VMs:                 rt11001
                     rt12001
```

Example 3-50 shows how to delete an anticollocation policy.

Example 3-50 Deleting an anticollocation policy

```
# ksysmgr delete anticollocation policy_2
Anticollocation group policy_2 was removed
```

Workgroup

A *workgroup policy* indicates that the set of VMs must be prioritized within the assigned priority.

To set this option, run the following commands:

```
ksysmgr add workgroup name vm=vmname1[,...]
ksysmgr modify workgroup name policy=add|delete vm=vm1[,...]
```

Example 3-51 shows the creation of a workgroup policy with the VMs `rt11001`, `rt11002`, and `rt11003`.

Example 3-51 Creating a workgroup policy

```
# ksysmgr add workgroup dev_itso vm=rt11001,rt11002,rt11003
Workgroup group dev_itso was created
```

To list the workgroup policies that are available, run the **ksysmgr query workgroup** command, as shown in Example 3-52.

Example 3-52 Listing the workgroup policies

```
# ksysmgr query workgroup
Name:                dev_itso
Type:                workgroup
VMs:                 rt11002
                     rt11001
                     rt11003
```

Example 3-53 shows how to delete the workgroup policy.

Example 3-53 Deleting the workgroup policy

```
# ksysmgr delete workgroup dev_itso
Workgroup group dev_itso was removed
```

> **Note:** When you set affinity policies, ensure that the host group has sufficient capacity for the policies to be implemented during host failure, VM failure, or application failure. For example, if the host group contains only two hosts, you cannot set an anticollocation policy on VMs of a specific host because the host group does not contain multiple target hosts to restart the VMs.

3.5.3 VM-level policies

This section describes the VM-level policies for relocating VMs during failover operations.

Host blocklist

The *host blocklist* policy specifies the list of hosts that must not be used for relocating a specific VM during a failover operation. For a VM, you can add hosts within the host group to the blocklist based on performance and licensing preferences, as shown in Figure 3-7.

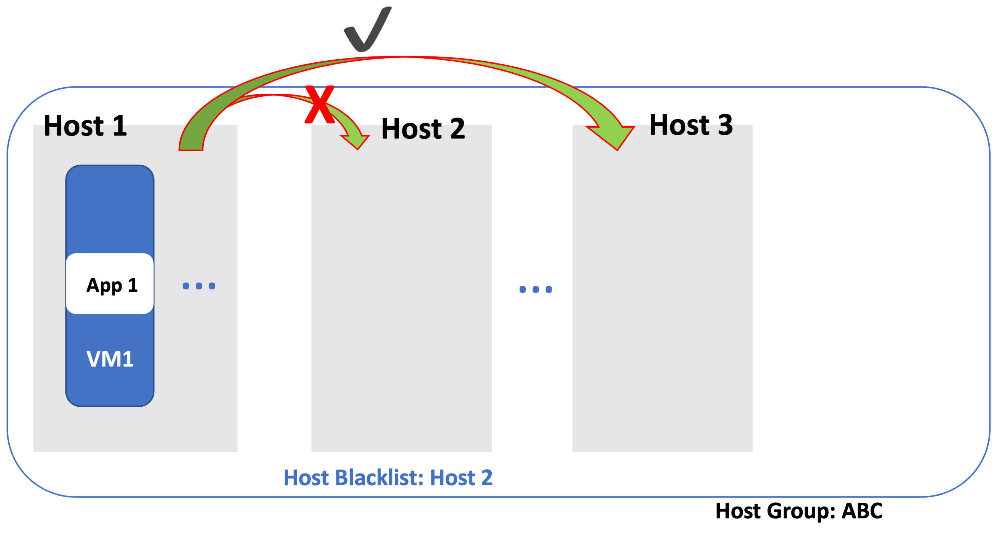


Figure 3-7 Host blocklist policy

To set this option, run the following command:

```
ksysmgr modify vm vmname
   blacklist_hosts=hostname[,...] policy=add|delete
```

Example 3-54 shows that VM `rt11004` does not have a blocklist policy.

Example 3-54 Checking the blocklist policy

```
# ksysmgr query vm rt11004
Name:                    rt11004
UUID:                    4FCD724B-8407-4945-A973-C25C4CA69A94
State:                   READY_TO_MOVE
Host:                    rt11-8286-42A-0607585
Priority:                Medium
VM_failure_detection_speed:    normal
HA_monitor:              enable
Homehost:                rt11-8286-42A-0607585
VM_status:               NO_OPERATION_IN_PROGRESS
Version_conflict:        No
```

Example 3-55 shows that host `rt12-8286-42A-2100E5W` in VM `rt1004` was set as the host blocklist.

Example 3-55 Setting the blocklist policy on VM rt11004

```
# ksysmgr modify vm rt11004 blacklist_hosts=rt12-8286-42A-2100E5W
WARNING: No backup host will be left for this VM rt11004.
For VM rt11004 attribute(s) 'blacklist_hosts' was successfully modified.
```

> **Note:** The warning appeared only because this test environment is composed only of two hosts on the host group.

To list the blocklist host that is configured on VM rt11004, run the command **`ksysmgr query vm rt11004`**, as shown in Example 3-56.

Example 3-56 Checking the blocklist policy on VM rt11004

```
#  ksysmgr query vm rt11004
Name:                rt11004
UUID:                4FCD724B-8407-4945-A973-C25C4CA69A94
State:               INIT
Host:                rt11-8286-42A-0607585
Priority:            Medium
VM_failure_detection_speed:    normal
HA_monitor:          enable
Homehost:            rt11-8286-42A-0607585
Blacklist_hosts:     rt12-8286-42A-2100E5W
VM_status:           NO_OPERATION_IN_PROGRESS
Version_conflict:    No
```

Example 3-57 shows how to delete the blocklist policy from VM rt11004.

Example 3-57 Deleting the blocklist host from VM rt11004

```
#  ksysmgr modify vm rt11004 blacklist_hosts=rt12-8286-42A-2100E5W policy=delete
For VM rt11004 attribute(s) 'blacklist_hosts', 'policy' was successfully modified.
```

Failover priority

The *failover priority* policy specifies the order of processing multiple VMs restart operations. For example, if a host fails and all the VMs must be relocated to other hosts on the host group, the priority of the VM determines which VM is processed first. The supported values for this attribute are `High`, `Medium`, or `Low`. This attribute is set at the VM level. Specify the UUID of the VM if you have two or more VMs with the same name. By default, all VMs in the host group have a priority of `Medium`.

To set the failover priority, run the following command:

```
ksysmgr modify vm name1[,name2,...] | filepath=filepath priority=high|medium|low
```

In Example 3-58, the VM rt11001 is set to the `High` priority.

Example 3-58 Setting the VM rt11001 to the High priority

```
# ksysmgr modify vm rt11001 priority=High
For VM rt11001 attribute(s) 'priority' was successfully modified.
```

To check the priority of the VM rt11001, run the command **ksysmgr query vm rt11001**, as shown n Example 3-59.

Example 3-59 Checking the priority policy of the VM rt11001

```
# ksysmgr query vm rt11001
Name:               rt11001
UUID:               3BF44186-0679-4032-BF4C-95B24901822A
State:              READY_TO_MOVE
Host:               rt11-8286-42A-0607585
Priority:           High
VM_failure_detection_speed:    normal
HA_monitor:         enable
Homehost:           rt12-8286-42A-2100E5W
VM_status:          NO_OPERATION_IN_PROGRESS
Version_conflict:   No
```

Example 3-60 shows that how to set the priority on all the VMs on the host `rt12-8286-42A-2100E5W`. In this example, they were set to the `High` priority.

Example 3-60 Setting all VMs on the host rt12-8286-42A-2100E5W to the High priority

```
# ksysmgr modify vm ALL  host=rt12-8286-42A-2100E5W priority=High
For VM rt12005 attribute(s) 'host', 'priority' was successfully modified.
For VM rt12004 attribute(s) 'host', 'priority' was successfully modified.
For VM rt12003 attribute(s) 'host', 'priority' was successfully modified.
For VM rt12002 attribute(s) 'host', 'priority' was successfully modified.
For VM rt12001 attribute(s) 'host', 'priority' was successfully modified.
```

Home host

The *home host* policy specifies the home host of the VM. By default, the KSYS subsystem sets this value initially to the host where the VM was first discovered. You can change the home host value of a VM even when the VM is running on another host. If so, the specified home host is used for all future operations. This attribute is useful when you get a host repaired after failure and you want to restart the VMs in its home host.

To set the home host value, run the following command:

```
ksysmgr modify vm name1[,name2...] homehost=hostname
```

To check that the VM `rt11001` is with the home host `rt12-8286-42A-2100E5W`, run the **ksysmgr query vm** command, as shown in Example 3-61.

Example 3-61 Checking the home host of the VM rt11001

```
# ksysmgr query vm rt11001
Name:               rt11001
UUID:               3BF44186-0679-4032-BF4C-95B24901822A
State:              READY_TO_MOVE
Host:               rt11-8286-42A-0607585
Priority:           High
VM_failure_detection_speed:    normal
HA_monitor:         enable
Homehost:           rt12-8286-42A-2100E5W
VM_status:          NO_OPERATION_IN_PROGRESS
Version_conflict:   No
```

In Example 3-62, there is a request to change the home host of the VM rt11001 to `rt11-8286-42A-0607585`.

Example 3-62 Changing the home host of the VM rt11001

```
# ksysmgr modify vm rt11001 homehost=rt11-8286-42A-0607585
```

In Example 3-63, you check that VM rt11001 has the home host `rt11-8286-42A-0607585`.

Example 3-63 Checking the home host of the VM 11001

```
# ksysmgr query vm rt11001
Name:                rt11001
UUID:                3BF44186-0679-4032-BF4C-95B24901822A
State:               READY_TO_MOVE
Host:                rt11-8286-42A-0607585
Priority:            High
VM_failure_detection_speed:    normal
HA_monitor:          enable
Homehost:            rt11-8286-42A-0607585
VM_status:           NO_OPERATION_IN_PROGRESS
Version_conflict:    No
```

Relocation mapper flow diagram

When a failure occurs in an environment that is managed by VMRM HA, the KSYS evaluates the error and determines the list of VMs that need to be relocated. The KSYS then creates a relocation map that it uses to recover the VMs in an affected host group. The relocation map accounts for all the relocation settings and the system settings to create an action plan.

Figure 3-8 shows the relocation mapper flow diagram for the policies for VMs in IBM Recovery Manager HA for IBM Power.

The steps in the diagram are as follows:

1. Create an empty map table.
2. Check the VM level priority: `High`, `Medium`, or `Low`.
3. Check the collocation priority.
4. Check the anticollocation priority.
5. Check for Best Fit: Available CPU and memory.
6. Check the Priority List: Flex capacity.
7. Check for auto mode: *Yes* starts a recovery restart, and *No* sends a notification.

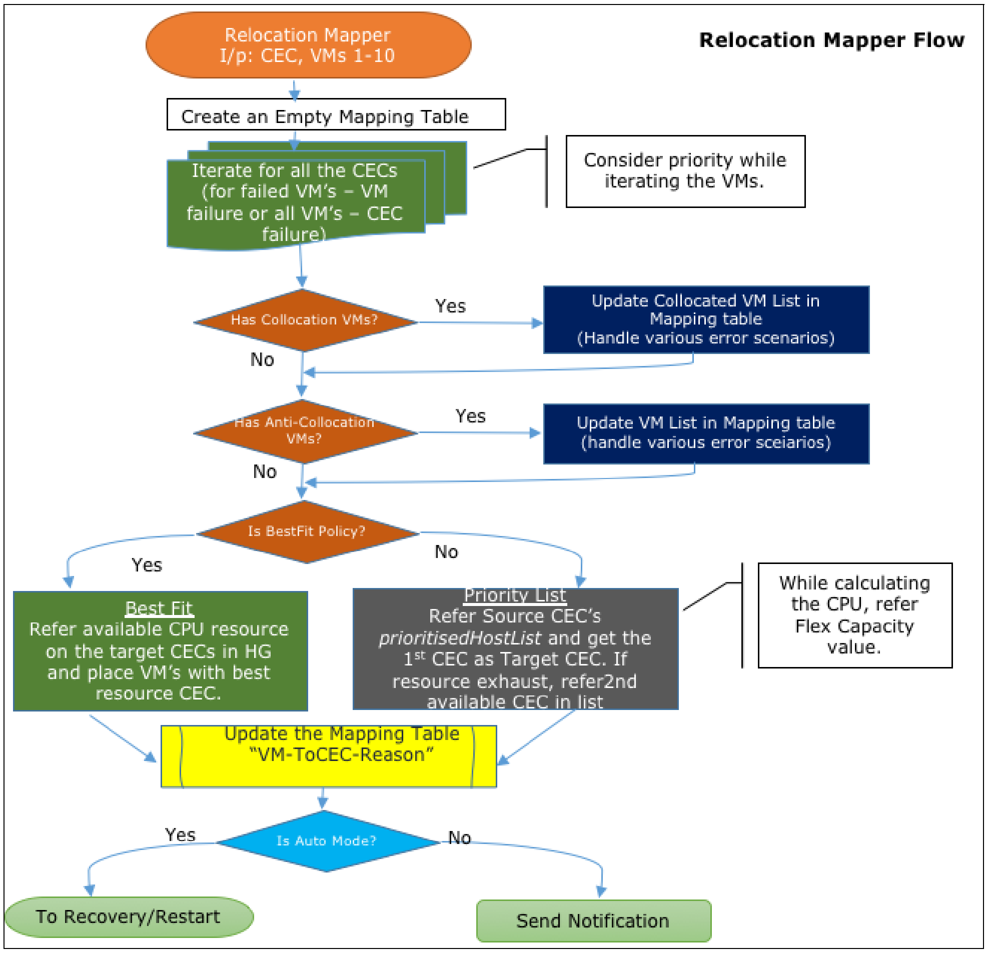

Relocation Mapper Flow
Relocation Mapper
I/p: CEC, VMs 1-10
Create an Empty Mapping Table
Iterate for all the CECs (for failed VM's – VM failure or all VM's – CEC failure)
Consider priority while iterating the VMs.
Has Collocation VMs?
Yes
Update Collocated VM List in Mapping table (Handle various error scenarios)
No
Has Anti-Collocation VMs?
Yes
Update VM List in Mapping table (handle various error sceiarios)
No
Is BestFit Policy?
Yes
No
Best Fit
Refer available CPU resource on the target CECs in HG and place VM's with best resource CEC.
Priority List
Refer Source CEC's prioritisedHostList and get the 1st CEC as Target CEC. If resource exhaust, refer2nd available CEC in list
While calculating the CPU, refer Flex Capacity value.
Update the Mapping Table "VM-ToCEC-Reason"
Is Auto Mode?
Yes
No
To Recovery/Restart
Send Notification

Figure 3-8 Relocation Mapper Flow

3.6 Uninstalling VMRM HA

To uninstall the VMRM HA solution, use the CLI to uninstall all the installed VMRM HA file sets by running the **`installp -u`** command.

To uninstall the VMRM HA solution, complete the following procedures:

1. Uninstalling the KSYS software
2. Uninstalling VM Agents

> **Note:** You must have root authority to perform any uninstallation tasks.

3.6.1 Uninstalling the KSYS software

If you must uninstall the KSYS file sets from the KSYS node, remove the cluster before uninstalling the file sets. Otherwise, the RSCT Peer Domain remains in the node. Example 3-64 shows the command that is used to perform the cluster removal.

Example 3-64 Removing the KSYS cluster before removing the KSYS file sets

```
# ksysmgr remove ksyscluster ITSO_HA
WARNING: This action will remove all configuration and destroy the KSYS setup, its
recommended to create a backup "ksysmgr add snapshot -h"
Do you want to a backup to be created now ? [y|n]
y
Created: /var/ksys/snapshots/oldclust_BASIC_2018-11-27_15:23:46.xml.tar.gz
Successfully created a configuration snapshot:
/var/ksys/snapshots/oldclust_BASIC_2018-11-27_15:23:46.xml.tar.gz
Do you wish to proceed? [y|n]
y
This may take a few minutes to safely remove the ksyscluster
Virtual client adapters have been deleted
Host_groups have been deleted
Trunk adapters have been deleted
IBM.VMR process stopped successfully
Peer domain stopped successfully
Peer domain was removed successfully
```

> **Tip:** If you reinstall the file sets and re-create the environment later, consider creating a snapshot before removing the cluster so that you can restore the snapshot after reinstalling the file sets.

Example 3-65 shows how to uninstall the KSYS file sets.

Example 3-65 Uninstalling the KYS file sets

```
# installp -ug ksys.*
.
.
.
Installation Summary
--------------------
Name                        Level           Part        Event       Result
-------------------------------------------------------------------------------
ksys.ha.license             1.3.0.0         USR         DEINSTALL   SUCCESS
ksys.hautils.rte            1.3.0.0         ROOT        DEINSTALL   SUCCESS
ksys.hautils.rte            1.3.0.0         USR         DEINSTALL   SUCCESS
ksys.main.msg.en_US.cmds    1.3.0.0         USR         DEINSTALL   SUCCESS
ksys.ui.agent               1.3.0.0         ROOT        DEINSTALL   SUCCESS
ksys.ui.agent               1.3.0.0         USR         DEINSTALL   SUCCESS
ksys.ui.common              1.3.0.0         USR         DEINSTALL   SUCCESS
ksys.main.cmds              1.3.0.0         ROOT        DEINSTALL   SUCCESS
ksys.main.cmds              1.3.0.0         USR         DEINSTALL   SUCCESS
ksys.main.rte               1.3.0.0         ROOT        DEINSTALL   SUCCESS
ksys.main.rte               1.3.0.0         USR         DEINSTALL   SUCCESS
```

4

Planning and deploying IBM VMRM DR

This chapter describes planning and deploying an installation of the IBM Virtual Machine Recovery Manager DR (VMRM DR) environment. It also provides information about the configuration and management functions that help with a successful VMRM DR environment.

The following topics are described in this chapter:

- Requirements
- Prerequisites for implementing VMRM DR
- Installing VMRM DR
- Configuration overview for VMRM DR
- Configuring VMRM DR
- Moving virtual machines across sites
- Managing and administering VMRM DR
- Troubleshooting in VMRM DR

4.1 Requirements

Before you plan the implementation of the VMRM DR solution, it is important to understand the other components and resources that the VMRM DR solution requires for disaster recovery (DR) operations.

To implement the VMRM DR solution, review the current DR plan and consider how the VMRM DR solution can be integrated into your environment. The VMRM DR solution can coexist with some of the existing product offerings with a few exceptions. Therefore, planning the implementation prevents issues in the configuration and DR operations.

The following sections list the requirements before installing the VMRM DR solution. This list is current at the time of writing. To validate whether there are more requirements, see the Requirements for the VM Recovery Manager DR solution.

4.1.1 Software requirements

This section lists the software requirements for the various components of IBM VMRM DR for Power:

- The KSYS logical partition (LPAR) must be running IBM AIX 7.2 with Technology Level 1 Service Pack 1 (7200-01-01) or later.
- The latest version of OpenSSL software for the AIX operating system, which can be downloaded from AIX Web Download Pack Programs.
- Each LPAR on the host must have one of the following operating systems:
  - AIX 6.1 or later
  - PowerLinux:
    - Red Hat Enterprise Linux (RHEL) (Little Endian, Big Endian) Version 7.2 or later
    - SUSE Linux Enterprise Server Version 12.1 or later
    - Ubuntu Linux distribution Version 16.04 or later
  - IBM i 7.1 or later

Table 4-1 describes the minimum version of dependent products that VMRM DR supports for each feature. For more information about the supported versions, see the respective products' software page.

Table 4-1 Dependent products requirements

Feature or component	Virtual I/O Server (VIOS) version	Storage version	Storage models	Supported replication modes of data mirroring	KSYS version	Firmware level	HMC version
Dell EMC Unity - Async	3.1.2.21	Firmware (FW) Version 5.1 or later	Dell EMC Unity storage system Version 5.1 or later	Async	1.5.0.1		HMC 9.9.1.0
Dell EMC Unity - Sync	3.1.2.21	FW Version 5.1 or later	Dell EMC Unity Storage System Version 5.1 or later.	Sync Async	1.6.0.0		HMC 9.9.1.0

Feature or component	Virtual I/O Server (VIOS) version	Storage version	Storage models	Supported replication modes of data mirroring	KSYS version	Firmware level	HMC version
IBM XIV Storage System	3.1.0.21	XIV Storage System Command-Line Interface (XCLI) 4.8.0.6 or later.	XIV Storage System and IBM FlashSystem A9000	Sync Async	1.3.0.2		HMC 9.9.1.0
Unmanaged disk	3.1.1.21				1.5.0.1 (1.5.0.0 with replication)		HMC 9.9.1.0
DR	2.2.5.10				1.1.0.0		HMC 9.9.1.0
High availability (HA)	3.1.0.11				1.3.0.0		HMC 9.9.1.0
High availability and disaster recovery (HADR)	3.1.1.0				1.4.0.0		HMC 9.9.1.0
HADRHA	3.1.2.10				1.5.0.0		HMC 9.9.1.0
Multiboot-DR	2.2.5.10				1.1.0.1	IBM POWER8 with FW 8.6.0	
Hitachi Storage System	2.2.6.00	Command Control Interface (CCI) Version 01-39-03/04 with model RAID-Manager/AIX	Hitachi Virtual Storage Platform (VSP) G200 Hitachi VSP G400 Hitachi VSP G600 Hitachi VSP G800 Hitachi VSP G1000	TrueCopy (Sync2) Universal Replication (Async1)	1.2.0.0		HMC 9.9.1.0

Feature or component	Virtual I/O Server (VIOS) version	Storage version	Storage models	Supported replication modes of data mirroring	KSYS version	Firmware level	HMC version
IBM DS8000 Storage System	2.2.5.20	DS8000 Series Command-Line Interface (DSCLI) 7.7.51.48 or later	IBM System Storage DS8000 Series Storage System	Global Mirror	1.1.0.1		HMC 8.8.6.0 Service Pack 1
IBM SAN Volume Controller and IBM Storwize Storage System	2.2.5.20	SAN Volume Controller 6.1.0 or later Storwize 7.1.0 or later	SAN Volume Controller 6.1.0 or later Storwize 7.1.0 or later	Metro Mirror (Sync) Global Mirror (Async) Global Mirror with Change Volumes	1.1.0.1		HMC 8.8.6.0 Service Pack 1
Dell EMC Symmetrix Remote Data Facility (SRDF) Storage System	2.2.5.10	Solution Enabler SE 8.1.0.0, SE 8.4.0.7, SE 9.4.0.0	SRDF-capable storage subsystems of the Dell EMC VMAX family	SRDF /S- Sync2 (1.0.0.1) SRDF /A- Async1 (1.0.0.0)	1.1.0.0		HMC 9.9.1.0
Dell EMC Unity - Sync	3.1.2.21	FW Version 5.1 or later	Dell EMC Unity Storage System Version 5.1 or later	Sync Async	1.6.0.0		HMC 9.9.1.0
DR Rehearsal	2.2.5.10				1.2.0.0		HMC 9.9.1.0
Shared mode DR	2.2.6.0				1.2.0.0		HMC 9.9.1.0
Previously saved virtual machine (VM) profile to retry the recovery operation	2.2.5.10				1.2.0.0		HMC 9.9.1.0
Auto logical unit number (LUN) masking	2.2.6.0		Dell EMC SRDF / SAN Volume Controller Storage Systems		1.6.0.0		HMC 9.9.1.0
Auto LUN masking			Hitachi Storage Systems		1.7.0.0		

Feature or component	Virtual I/O Server (VIOS) version	Storage version	Storage models	Supported replication modes of data mirroring	KSYS version	Firmware level	HMC version
Integrated KSYS HA clustering	3.1.4.10				1.7.0.0		HMC 9.9.1.0
PowerHA SystemMirror based KSYS HA management (HADR)	3.1.1.0				1.3.0.2		HMC 9.9.1.0
Live Partition Mobility (LPM) progress indication (HA)	3.1.0.11				1.3.0.2		HMC 9.9.1.0
DR support for VM with Hybrid Network Virtualization (SR-IOV migratable)	2.2.5.10				1.6.0.0	IBM POWER9 processor -based servers with FW level FW940.10	HMC 9.2.9.5.1
Reduced path support VM	3.1.3.10				1.6.0.0		HMC 9.9.1.0
Multi-boot DR Test	2.2.5.10				1.6.0.0	IBM POWER8 processor -based servers with FW 8.6.0	HMC 9.9.1.0
Multi-boot HA	3.1.0.11				1.5.0.0	POWER8 processor -based servers with FW 8.6.0	HMC 9.9.1.0
IBM i	2.2.5.10				1.1.0.1		HMC 9.9.1.0
Linux	2.2.5.10				1.1.0.1		HMC 9.9.1.0
VM agent	3.1.0.11				1.3.0.0		HMC 9.9.1.0
Diskview	3.1.4.10				1.7.0.0		HMC 9.9.1.0

- Install the mandatory APAR fixes and VIOS fixes with VMRM DR. For more information about interim fixes downloads, see Installing VIOS and KSYS interim fixes.
- For a multi-node KSYS, VMRM 1.7 or later is required on all the KSYS nodes. For more information about KSYS HA, see Chapter 8, “KSYS high availability” on page 217.
- This list is current at the time of writing. To validate whether there are more requirements, see Software Requirements.

4.1.2 Configuration requirements

- VMRM DR supports two sites: a home site and a backup site. There is no limit to the distance between the sites. It is possible to have applications running on both sites that are backed up by the other site.
- Historically, there was support for only one KSYS LPAR to manage the VMRM environment. Customers could use clustering solutions such as PowerHA SystemMirror to provide HA for the management LPAR. Starting with VMRM 1.7.0.0, it is possible to create a multi-node KSYS cluster natively within the VMRM solution.

  For VMRM DR, the KSYS system should be at the backup site so that it can run recovery options if the home site suffers a complete outage.
- The KSYS LPAR must have at least one 1-core CPU and 8 GB of memory. These requirements can be higher if you have a large environment with more than 100 LPARs in the data center.
- The managed VMs must run on POWER7 processor-based servers or later, run PowerVM, and managed by an HMC.

  If you use HADR or HADRHA solutions, the managed hosts must run on POWER7+ processor-based servers or later.
- To support virtual LAN (VLAN) and vSwitch at the workgroup level, create the required Shared Ethernet Adapter (SEA) on all VIOS that are based on the VM group.
- The VMRM DR solution supports the following storage devices:
  - Dell EMC storage system

    The VMRM DR solution supports storage devices for the Dell EMC VMAX family (VMAX1, VMAX2, and VMAX3). The Dell EMC storage devices must be SRDF-capable. The Dell EMC storage must have Solutions Enabler SRDF family Version 8.1.0.0 or later installed. Both SRDF/S (Synchronous) and SRDF/A (Asynchronous) replication modes are supported. The Symmetrix Command-Line Interface (SYMCLI) interface on the KSYS node must be the same version or later as the version of the SYMCLI interface on the storage agent.
  - Dell EMC Unity Storage System

    The VMRM DR supports Dell EMC Unity storage system Version 5.0.6.0.6.252 or later. Both synchronous and asynchronous modes of data replication are supported across sites.
  - IBM SAN Volume Controller and Storwize Storage Systems

    The VMRM DR solution supports IBM SAN Volume Controller 6.1.0 or later, and IBM Storwize V7000 7.1.0 or later. Both Metro Mirror (synchronous) and Global Mirror (asynchronous) modes of data replication are supported across sites.

- IBM System Storage DS8000 series

  The VMRM DR solution supports DS8700 or later and DS8000 Storage Systems with DSCLI 7.7.51.48 or later. Only the Global Mirror (asynchronous) mode of data replication is supported across sites.

- Hitachi storage systems

  The VMRM DR solution supports the Hitachi VSP G1000 and Hitachi VSP G400 with CCI Version 01-39-03/04 and model RAID-Manager/AIX. Both synchronous and asynchronous modes of data replication are supported across sites.

- IBM XIV Storage System and IBM FlashSystem A9000

  The VMRM DR solution supports IBM XIV Storage System and IBM FlashSystem A9000. Both Metro Mirror (synchronous) and Global Mirror (asynchronous) modes of data replication are supported across sites.

Note: For the required supported levels of each storage agent, see Table 4-1 on page 94.

Important: When multiple target VIOS VMs are used during the DR move operation, each VIOS must have enough NPIV ports to host all the adapters of the VMs that will be moved to the host. If each target VIOS must serve different VMs, then update the storage area network (SAN) zoning so that VMs are distributed across the target VIOS partitions during the DR move operation.

4.1.3 Network requirements

- All VMs that are managed by the VMRM DR solution must use virtual I/O resources through VIOS. The VMs must not be connected to any physical network adapter or have any dedicated devices.
- When using a SEA, the configuration must be set to bridge to the same Ethernet network between all the hosts at the same site.
- The same VLAN is assumed to be configured across the sites. If a different VLAN is required in the target site, you must update the KSYS configuration to use the new VLAN ID in the backup site.
- Ensure that redundant connections exist between the KSYS to the HMCs and from the HMCs to the VIOS LPARs. Any connectivity issues between KSYS, HMC, and VIOS LPARs can lead to disruption in the regular data collection activity and failures during DR operations.

4.1.4 Administrative requirements

Ensure that the following prerequisites are met before implementing VMRM DR:

- The KSYS must have HTTP Secure (HTTPS) connectivity to all the HMCs across both sites.
- All the VIOS partitions and disk pairs must be defined and deployed correctly across both sites.
- Each VIOS in the target site must have the same number of virtual Fibre Channel (vFC) adapters that are assigned to the VMs in the source host.
- The source and destination hosts must have at least one logical memory block (LMB) of available space. This available space is used by the `drstartlpar` command during the move operation.

- Storage replication must be set up correctly for any disks that are used in the VMRM DR-managed environment.
- SAN connectivity and zoning must be configured so that VIOS can access the disks that are relevant to the hosts across the host pairs. For example, a disk D1 that is connected to the VIOS of a host must have a mirror disk D1_M that is connected to the VIOS of the paired host in the backup site. Any connectivity issues can cause the VMRM DR verification to fail.
- SAN connectivity must be designed so that the SAN fabrics connecting VIOS to the storage on a host pair do not connect to each other.

Mapping N_Port ID Virtualization for VMRM DR

To map the N_Port ID Virtualization (NPIV) setting for VMRM DR, complete the following steps:

1. Create a SAN zone in a switch that consists of the NPIV worldwide port number (WWPN) of the VM and the WWPN of the source SAN subsystem.
2. In the source SAN subsystem, mask both the LUNs and the WWPN of the NPIV client.
3. Create a SAN zone in a switch that contains both the NPIV WWPN and the WWPN of the target SAN.
4. In the target SAN subsystem, mask both the mirrored LUNs and the WWPN of the NPIV client.

Mapping the virtual Small Computer System Interface for VMRM DR

To map the virtual Small Computer System Interface (vSCSI) addresses for VMRM DR, complete the following steps:

1. Create a SAN zone in a switch that contains both the source VIOS WWPN and the WWPN of the source SAN.
2. In the source SAN subsystem, ensure that the LUN is masked with the WWPN of the source VIOS.
3. Create a SAN zone in a switch that contains both the target VIOS WWPN and the WWPN of the target SAN.
4. In the target SAN subsystem, ensure that the mirrored LUN is masked with the WWPN of the target VIOS.

4.1.5 Storage requirements

- Ensure that all the prerequisite software is installed on the same LPAR in which the KSYS software is installed. The prerequisite software includes any storage controller software that must be installed on the KSYS LPAR so that the KSYS can send commands to the storage to manage storage-specific operations.
- Regardless of the type of storage, the disk size in the active and backup sites must be same.
- Ensure that all the disks that belong to the VMs in each host have mirror relationships with the corresponding disks in the other site.
- Verify that the disks that are used for the VMs and managed by the VMRM DR solution are not being managed by any other DR solutions.
- For vSCSI disk mapping, ensure that you do not use Logical Volume Manager (LVM)-based disk partition management from the VIOS.

For more information about SAN terminology and other SAN-related requirement details, see Introduction to Storage Area Networks and What is a storage area network?

4.1.6 GUI requirements

Here is a list of requirements for installing and using the VMRM GUI:

- The LPAR, in which you want to install the GUI file sets, must be running IBM AIX 7.2 with Technology Level 2 Service Pack 1 (7200-02-01) or later. You can choose to install the GUI server file set on one of the KSYS nodes.
- The GUI server must run in an Enhanced Korn shell that uses the `/usr/bin/ksh93` shell script.
- The GUI server must have at least one 1-core CPU and 8 GB of memory.
- Google Chrome Version 63 or later, and Mozilla Firefox Version 57 or later web browsers are supported to access the GUI for the VMRM solution.

Installation and usage of the GUI is documented in Chapter 9, “IBM VMRM GUI deployment” on page 237.

4.1.7 Licensing considerations

Here is a list of licensing considerations when using VMRM:

- With the VMRM DR solution, the VMs that are replicated or managed by the solution are hosted on the production system processors. The licensing requirements are not determined by the number of VMs that is managed, but by the number of process cores that is defined to the VMs. License the number of processing cores that is assigned to the VMs (rounded up to the next whole number) that are being managed by the VMRM DR solution.
- The VMRM DR licenses are installed on an AIX partition that is the partition that is running the KSYS orchestrator. The VMRM DR license enables the KSYS orchestrator.
- The KSYS LPAR can be running on any system that has the appropriate connectivity to the HMCs, VIOS partitions, and storage controllers. For VMRM DR, it is a best practice that the KSYS is in the backup site so that it can manage a disaster failover if the primary site loses power.
- The VMRM DR solution conforms to the active/inactive technology, which includes LPM in your HA configuration. Because all the VMs restart on the recovery hosts, you do not need extra application-specific licenses. Some applications are sensitive to the serial number of the host on which they are running. Ensure that each application and LPAR can be run on the intended backup host.
- VMRM DR product requires PowerVM Enterprise Edition is installed on all the hosts that are configured for DR management.

4.1.8 Known interim fixes

Here are the known interim fixes:

- VIOS interim fixes
- KSYS interim fixes
- GUI interim fixes

VIOS interim fixes

Table 4-2 provides information about the corresponding interim fixes that you must install with the VIOS version that you are using.

Table 4-2 VIOS interim fixes

VIOS version	APARS	Download URL
3.1.4.10	IJ44263, IJ44264, IJ44265, IJ44391, and IJ44392	https://aix.software.ibm.com/aix/ifixes/ij44264/IJ44263m5a.221124.epkg.Z
3.1.3.21	IJ44275 and IJ44276	https://aix.software.ibm.com/aix/ifixes/ij44264/IJ44275m4a.221115.epkg.Z
3.1.3.10	IJ35732	https://aix.software.ibm.com/aix/efixes/IJ35732/IJ35732m3b.211201.epkg.Z
3.1.2.40	IJ44277, IJ44278, and IJ44279	https://aix.software.ibm.com/aix/ifixes/ij44264/IJ44277m4a.221115.epkg.Z
3.1.2.20	IJ33042, IJ33043, IJ33041, IJ33044, IJ33034, and IJ33045	https://aix.software.ibm.com/aix/ifixes/ij33034/IJ33034m2a.210607.epkg.Z
3.1.2.10	IJ28933 IJ28934, IJ28935, and IJ28937	https://aix.software.ibm.com/aix/efixes/IJ28933/IJ28933m1a.201106.epkg.Z
3.1.1.30	IJ25171	https://aix.software.ibm.com/aix/ifixes/IJ25171/IJ25171s3a.210709.epkg.Z
3.1.1.25	IJ25175, IJ25173, IJ25171, IJ25170, IJ25169, IJ25168, IJ27427, IJ25166, IJ25174, and IJ25165	http://aix.software.ibm.com/aix/efixes/ij25165/IJ25165m2c.200727.epkg.Z
3.1.1.21	IJ33050 (only for Unity Storage)	https://aix.software.ibm.com/aix/ifixes/ij33050/
3.1.1.21	IJ25175, IJ25173, IJ25171, IJ25170, IJ25169, IJ25168, IJ27427, IJ25166, IJ25174, and IJ25165	http://aix.software.ibm.com/aix/efixes/ij25165/IJ25165m2c.200727.epkg.Z

VIOS version	APARS	Download URL
3.1.1.10	IJ21043 and IJ22767	http://aix.software.ibm.com/aix/ifixes/IJ21043/IJ21043m1b.200218.epkg.Z
3.1.1.0	IJ21043 and IJ22767	http://aix.software.ibm.com/aix/ifixes/IJ21043/IJ21043m1b.200218.epkg.Z

KSYS interim fixes

Example 4-1 provides information about the corresponding interim fixes that you must install for the VMRM version that you are using.

Example 4-1 KSYS interim fixes

KSYS Version	APAR	Download APAR
1.6.0.0	IJ36417	https://aix.software.ibm.com/aix/efixes/IJ36417m0a/IJ36417m0a.211208.epkg.Z
1.5.0.0	IJ29125	http://aix.software.ibm.com/aix/efixes/IJ29125m/IJ29125m0a.201110.epkg.Z

GUI interim fixes

Table 4-3 provides information about the corresponding GUI interim fixes for the appropriate version of VMRM.

Table 4-3 GUI interim fixes

GUI Version	APAR	Download APAR
1.7.0.0	IJ45264	https://aix.software.ibm.com/aix/efixes/IJ45264/IJ45264.230208_1.7.epkg.Z
1.6.0.0	IJ45264	https://aix.software.ibm.com/aix/efixes/IJ45264/IJ45264.230207_1.6.epkg.Z

4.1.9 VMRM DR limitations

Here is a list of the limitations when you use VMRM DR:

- The status of a host must be consistent across the HMCs that are added to the host when it is added to the KSYS configuration.
- While adding a host to the KSYS configuration, the Resource Monitoring and Control (RMC) connection between the configured HMCs of the host and the VMs must be in the active state.
- Any VIOSs in the cluster that are in an unhealthy state must be unmanaged.
- If the serial number or Universally Unique Identifier (UUID) of an installed storage agent must change, it cannot be changed directly. Instead, you must remove the storage agent from KSYS subsystem and then add the storage agent back again for those changes to take effect.

- The VMRM DR does not support sharing a managed disk or unmanaged disk between VMs of two different workgroups or host groups.
- The site-level cleanup operation might not show proper results when the previous move operation failed because the KSYS daemon or the KSYS subsystem restarting.

  Workaround: Run the cleanup operation on the host group.
- Removing a consistency group (CG) in the Hitachi storage system can take a long time, which can impact the amount of time that it takes to delete a KSYS cluster. The time also is affected by the number of workgroups that are defined in the KSYS.
- Do not perform the LPM operation *across* host groups. All LPM operations must be performed *within* a host group. If the LPM operation is initiated across host groups and the VM is part of a workgroup, the site-level discovery operation might not complete because of an error.
- On VIOS nodes, if the disks of a Shared Storage Pool (SSP) are not accessible after the system is reactivated because it was shut down or restarted, the state of the disks remains down. The SPP does not start correctly because it requires a quorum to come back online. Choose one of the following workaround options:
  - Workaround option 1: If you do not want to restart the VIOS, complete the following procedure:
    1. Restore the disk connectivity.
    2. To make the disks available to the system, run the **cfgmgr** command as `root`.
    3. Run the following commands:

       ```
       padmin: clstartstop -stop -m <node>
       padmin: clstartstop -start -m <node>
       ```
  - Workaround option 2: If you want to restart the VIOS, complete the following procedure:
    1. Restore the disk connectivity.
    2. Restart the VIOS node.
- If a VM is migrated from host1 to host2 due to a failure, then when the applications in the VM become stable, an entry is made in the FailedHostList list of that application. If at a later point the application must be migrated due to an application failure when running on host2, host1 is not considered as a backup for the application failure migration because the VM had previously failed on host1.

  If host1 must be considered as a backup for a future application failure, use the following workaround.

  Workaround: After the VM is stable on the host2, clear the FailedHostList list of the VM. Run the **chrsrc -s 'Name="VMName"' IBM.VMR_LPAR VmRestartFailedCecs='{""}'** command to clear the FailedHostList list for the VM.
- If you want the system to ignore the unmanaged VIOSs in the HMC during a discovery operation, disable the SAN zones from the selected VIOS before performing the DR operation.
- The cleanup operation on a VM with vSCSI disk fails in the local database mode.

  Workaround: Bring the SSP cluster back to the global mode.
- The **ksysmgr** command fails to start or stop applications that belong to an application dependency setup if VIOSs are in the local database mode.

- The discovery operation or the KSYS restart operation automatically starts the dependent applications that are part of an application dependency setup and that were stopped manually.

  Workaround: Consider one of the following workaround options:

  – Do not perform the discovery operation after stopping the dependent application.

  – Disable the auto-discover and the quick discovery features.

  – Do not restart the KSYS subsystem after you stopped the dependent application.

- The restart operation of the VMs that are running on the Linux VM agent might take a longer time than expected, and the discovery operation might fail and display the following message:

  ```
  Restart has encountered error for VM <vm_name>.
  ```

  Workaround: Rerun the discovery operation.

- The VMRM DR solution cannot be used if the LPM features are disabled at the FW level.

- When temporary I/O errors occur at the VIOS cluster level, the migration process of the VMs after the host failure is not triggered automatically.

  Workaround: Initiate the host-level restart operation by using the GUI or command-line interface (CLI). To initiate the host-level restart operation, run the following command:

  ```
  ksysmgr restart host <host_name>
  ```

- If a VM is migrated across host groups, you must run the discovery operation on the source host group and the target host group. After running the discovery operation on both host groups, the KSYSNODE node reflects the migration status of the VM.

- The backup and restore LPAR control blob (LCB) feature is not supported for VMs that are part of an asymmetric host-group configuration.

- If a VM profile exists on multiple hosts, the command **ksysmgr query vm host=<hostname>** might not display the VM details properly.

  Workaround: Run the command with another host that has the same VM profiles.

- If a current repository disk is down, automatic replacement does not occur on a previously used repository disk that has the same cluster signature. If no other backup repository disk is available, the automatic replacement operation fails.

  Workaround: Run the following command to clear the previous cluster signatures:

  ```
  cleandisk -r <diskname>
  ```

- As part of the HA verification operation, the KSYS subsystem verifies the configuration of each VM against all backup hosts within a site. In a scalable environment, when the KSYS subsystem sends parallel verification requests and the HMC is busy with previously received requests, the new request can lead to exceeding the maximum supported requests, and then the verification operation fails with the following error:

  ```
  HSCLB401 The maximum number of partition migration commands allowed is already
  in progress.
  ```

  Workaround: Rerun the verify operation on the host group.

- The move operation fails when all NPIV ports of a physical Fibre Channel (FC) port are used by VMs, and none of the NPIV ports on the FC adapters are available.

  Workaround: Keep at least 20% of NPIV ports available on each FC port.

- The discovery operation at the site level fails and the VM is not recoverable after a VM is migrated from one host group to another host group by using LPM from the Hardware Management Console (HMC).

  Workaround: Run the discovery operation on the source host group, and then run the discovery operation on the target host group.

  > **Note:** If the scheduled site-level auto discovery operation is run before performing the above mentioned workaround and the discovery operation on the source host group fails while adding the migrated VM's disks to the existing CG, you must perform the following workaround.
  >
  > Workaround: Manually delete the VM's disks from the CG of the source host group.

- The VMR daemon fails if you remove the HMC from the KSYS configuration when the discovery or migration operation is in progress. Do not make any changes in the KSYS configuration when the discover or migration operation is in progress.
- The Dell EMC Unity Representational State Transfer (REST) application programming interface (API) call might not send the complete information about disks of the replication session to the KSYS subsystem. The **`ksysmgr`** displays the member exception error while running the DR operations.

  Workaround: Run the same operation again for which the **`ksysmgr`** displayed the member exception error.
- The storage agent password must not contain any special characters.
- For DR, HADR, and HADRHA cluster types, use unique names for each cluster if you are using the same storage for more than one cluster. If you use same cluster name for more than one cluster, creating a disk group might result in an error.
- For a multi-node KSYS setup, while adding clusters, it is a best practice that the operating system version and the Reliable Scalable Cluster Technology (RSCT) version are the same on all nodes. If the operating system that is running on a node is on an earlier version than the other node, you must specify the node that is running the earlier version of the operating system before the node that is running the later version of the operating system when you run a command to add nodes to the cluster.
- For a multi-node KSYS cluster that is using a Hitachi storage agent, the Hitachi Open Remote Copy Manager (HORCM) configuration file on the nongroup leader (non-GL node) is not updated automatically. To update the HORCM file, configure the **`vmrm_horcm_sync.py`** script at the `/opt/IBM/ksys/samples/utils/vmrm_horcm_sync.py` location by using the **`ksysmgr add scripts`** command.
- In the KSYS LPAR, if you upgrade the AIX operating system after upgrading the KSYS software, a few class IDs might be missing in the `/usr/sbin/rsct/cfg/ct_class_ids` file, and the KSYS daemon might stop working. For a workaround, see Planning Limitations.

GUI limitations

Here is a list of limitations when using VMRM GUI:

- The VMRM DR GUI does not support multiple sessions that originate from the same computer.
- The VMRM DR GUI does not support duplicate names for the host group, HMC, host, VIOS, VMs, site, workgroup, and storage agent. If a duplicate name exists in the KSYS configuration, the GUI might encounter an error during the host group creation or while displaying the dashboard data.

- The VMRM DR GUI refreshes automatically after each topology change (for example, VM migration operation and host migration operation). After the refresh operation of VMRM DR GUI completes, the default KSYS dashboard is displayed. Expand the topology view in the Activity window to view the log information for a specific entity.
- Any operation that is performed by a user from the CLI of VMRM DR is not displayed in the activity window of the VMRM DR GUI.
- The VMRM DR GUI does not support failover rehearsal for IBM XIV vSCSI disks. Failover rehearsal for IBM XIV vSCSI disks can be performed only by using the CLI of the VMRM DR for Power solution.
- GUI reports show only details about operations that are triggered from GUI. The operations that are triggered from the CLI are not displayed in the GUI reports.

Small Computer System Interface reservations

If the VMs in the active site are using Small Computer System Interface (SCSI)-2 or SCSI-3 persistent reservations to control access to a shared storage device (for example, if the value of the **`reserve_policy`** attribute is set to `PR_shared` in the AIX operating system), and a VM is moved to the backup site, all the reservations are lost, and policies are set to default reservation policies according to the storage and operating system that is associated with the VM. This action occurs because the storage subsystems do not transfer reservations across the mirror copies of data. In addition, the host or storage adapter identities, which are part of reservation management, also change across the active site and the backup site during the DR move operation.

Example: A PowerHA SystemMirror cluster is established across a set of VMs and disk fencing is enabled on the active site. In this case, PowerHA SystemMirror performs disk fencing by using SCSI-3 persistent reservations. Therefore, in the active site, each VM must have stored its own key for disk fencing. When the VMRM DR solution moves these VMs to the backup site, all these VMs start in the backup site, a cluster is established, reservation is enabled, and the keys are stored back into the storage subsystem.

Date and time of virtual machines

When VMs are moved from the active site to the backup site, the date and time in the VMs depend on the backup site environment in the following ways:

- For POWER7 and POWER8 processor-based systems:

  If a time reference is set up for the system (for example, you set the reference of all VMs on the host based on a single source like a VIOS) and the move operation is performed, the VMs acquire time and date information from the reference VIOS on the target host.
- For POWER8 processor-based systems:

  If the Simplified Remote Restart (SRR) option is enabled for a VM and the VM is moved to a target POWER8 processor-based system, the VM retains its original time and date value from the active site.

Changing the disk names and disk queue depth values

After the DR operation, the disk names are not sustained on the backup site. In the case of replicated disks, the disk identifier changes when the VMs are started on the backup site and the disks are renamed based on the disk identifiers. Therefore, disk names are not sustained across sites. However, you can create customized scripts to be run after the DR operation and the disks can be renamed based on predefined information.

Similarly, as the disk identifier changes during the DR operation, the disks are added to the backup sites as new disks are plugged in. Therefore, custom queue depth values change on the backup site. The AIX operating system provides a tunable parameter in the **chdef** command to manage the queue depth as a global policy that works only for Dell EMC storage systems and DS8000 series of storage systems. By using the **chdef** command, you can set the value of a predefined attribute for the entire AIX environment. Any new disks that are added after you run this command can inherit the value from the specified global policy. For more information about the **chdef** command, see the **chdef** command in IBM Documentation.

Dependency on the VMR daemon

If you stop the VMR daemon (IBM.VMR subsystem) forcefully and then start it again, the VMR daemon might take up to 2 minutes to become stable and perform any operations, depending on the number of hosts and VMs that are defined in the KSYS configuration settings.

Miscellaneous

- If a specific VM profile exists on the target site, then during the DR restart operation, the KSYS subsystem does not restart the specific VM on the target site.
- The *skip power on* feature is supported only for the move operation from the home site to the backup site.
- After each manage or unmanage VIOS operation, you must run the discovery operation.
- The flex capacity policy for host is ignored.
- You cannot add more than 10 scripts to the **ksysmgr add notify** command.

4.2 Prerequisites for implementing VMRM DR

Before implementing the VMRM DR solution, properly plan the resources and corresponding details for your production and backup sites. Identify the following information and have it available when you plan for the VMRM DR implementation.

KSYS node

Identify the host and the LPAR in which you plan to create the KSYS node. The host preferably should be in the backup site during the normal (non-disaster) conditions. The host that it is running on should not be managed by the KSYS subsystem. The LPAR running the KSYS must be running IBM AIX 7.2 with Technology Level 1 Service Pack 1 (7200-01-01) or later.

The KSYS node must be able to communicate to all HMCs at both sites by using the HTTPS protocol. In addition, the KSYS node must be able to communicate to the storage subsystems at both sites by using the connections that are supported by the storage vendor.

KSYS cluster

Identify a name for your 1-node KSYS cluster.

Sites

Identify names for your active and backup sites.

HMC

Identify the HMCs that you want to add in your active and backup sites. For better reliability, use a dual-HMC configuration in your sites to ensure enhanced availability if one of the HMCs is down or unreachable.

For each HMC that you plan to include in the configuration, you need the following information:

- HMC name or IP address
- Username
- Password

When a host is managed by both PowerVM NovaLink and the HMC, ensure that the HMC is the master while you are doing the configuration.

Hosts

Identify all hosts that you want to manage in the primary site. Make sure that the HMCs that are managing those hosts are included the list of HMCs that you are managing. Identify the hosts in the backup site that will be used to recover the LPARs if there is a failure. By default, VMRM DR assumes symmetric pairing where all hosts in the primary site are paired with one host in the secondary site. VMRM DR supports asymmetric host groups where hosts in the primary site can be grouped with multiple hosts in the backup site. Asymmetric pairing is enabled by setting the **`mxn_pairing`** parameter to `yes`. You must have either the name of the host or the UUID of the host available for each host that you are planning to include in the VMRM DR implementation.

LPAR

Identify the LPARs that you want to include in the VMRM DR implementation and install your applications as required. You can exclude any LPARs that you do not want to include in the VMRM DR solution. You must have the LPAR name available for each LPAR that you are planning to include in the VMRM DR implementation.

Note: The VMs must not be scheduled to restart automatically if the VM is included in the VMRM DR management.

Virtual I/O Server

The VIOS configuration in the active site host should match the configuration of the VIOS running in the backup site host that is included in the host pairing.

Note: If you have multiple VIOS configurations that use vSCSI disk mapping, ensure that the VIOSs do not have any back-end disk reservations.

During the verification phase, the VMRM DR solution displays a warning message about any VIOS issues. For example, if any of the VIOS partitions are down, a warning message is displayed. The VMRM DR solution skips this check if you use the **`lose_vios_redundancy`** attribute persistently. For more information about this option, see “Managing the system attributes” on page 155.

Even after you use this option, the source VMs can be moved to the backup host only when the VIOS in the target host can accommodate all the virtual adapters of the VM.

Problems might occur during the DR operation if one of the VIOSs or FC adapters is down.

Note: The VMRM DR for Power solution requires VIOS 3.1.1.21 or later with all the subsequent patches for the unmanage disk function.

Storage

- Allocate the primary storage based on the current storage requirements.
- Map primary storage LUNs to the appropriate VMs and VIOS as required (vSCSI or NPIV).
- Allocate backup or mirror LUNs at the backup site.
- Identify the storage agent count and storage agent names based on the current storage configuration. The storage controller software that interacts with the storage subsystem must be installed on the KSYS node.
- Configure the physical connectivity and zoning of backup storage LUNs to the appropriate adapters to ensure storage availability when the VMs start in the backup site.
- Set up replication relationships between primary storage LUNs and backup storage LUNs. Include VM operating system LUNs in the replication. You do not need to set up CGs. The KSYS subsystem performs those operations.
- Have the storage administrative information ready to specify in the KSYS configuration settings (for example, storage agent count and name, username, password, serial number of the storage disks, and IP address of the storage controller server).
- For Dell EMC storage, review the existing SRDF composite groups. Verify that the storage disks, which will be included in the VMRM DR implementation, are not part of any existing composite groups.

FC port limitation

Figure 4-1 shows an NPIV-based VIOS configuration in which the source host contains two VIOS partitions that use 2-port FC adapters. If the target host does not contain a dual-VIOS configuration or if one of the VIOSs in the target host is not functioning, the VM can be moved from the source host to the target host only when the VIOS in the target host uses a 4-port FC adapter.

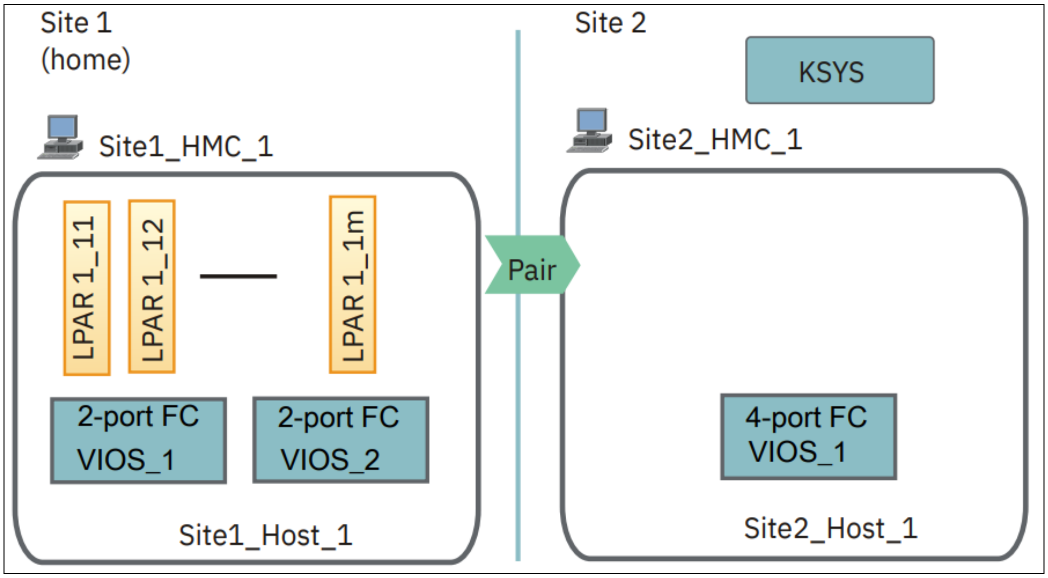


Figure 4-1 VIOS configuration during disaster recovery

Email or contacts for notification

Identify the contacts that must receive the notification if any failures or disaster occurs. You can have the following type of notifications:

- Email
- System Management Services (SMS)

4.2.1 Prerequisites for virtual machines running a Linux operating system

When an LPAR runs a Linux operating system, the Linux operating system uses the SCSI ID as the device ID for some file systems during installation. However, the SCSI ID might change when you recover the VM from the active site to the backup site. In this case, the VM cannot start in the backup site because of the change in SCSI ID. Therefore, you must replace the SCSI ID with the UUID in the `/etc/fstab` file and the Boot loader option after you install the Linux operating system in the VM.

To replace the SCSI ID with UUID in the Linux VM after installing the operating system, complete the following steps:

1. Identify the UUID of the required disk by running the following commands:

   a. Identify the disk that contains the Linux operating system by running the following command:

   ```
   linux:/usr/bin # fdisk -l
   ```

   Example 4-2 shows the output.

Example 4-2 Identifying the Linux disk

```
Disk /dev/sda: 107.4 GB, 107375493120 bytes
255 heads, 63 sectors/track, 13054 cylinders, total 209717760 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xbac70600
 Device Boot Start End Blocks Id System
/dev/sda1 * 2048 2854 403+ 41 PPC PReP Boot
/dev/sda2 417792 4626431 2104320 82 Linux swap / Solaris
/dev/sda3 4626432 209717247 102545408 83 Linux
Disk /dev/sdb: 107.4 GB, 107375493120 bytes
255 heads, 63 sectors/track, 13054 cylinders, total 209717760 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xbac70600
 Device Boot Start End Blocks Id System
/dev/sdb1 * 2048 2854 403+ 41 PPC PReP Boot
/dev/sdb2 417792 4626431 2104320 82 Linux swap / Solaris
/dev/sdb3 4626432 209717247 102545408 83 Linux
Disk /dev/mapper/360000970000196800508533033323741: 107.4 GB, 107375493120 bytes
255 heads, 63 sectors/track, 13054 cylinders, total 209717760 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xbac70600
 Device Boot Start End Blocks Id System
```

```
/dev/mapper/360000970000196800508533033323741_part1 * 2048 2854 403+ 41 PPC PReP
Boot
/dev/mapper/360000970000196800508533033323741_part2 417792 4626431 2104320 82
Linux swap / Solaris
/dev/mapper/360000970000196800508533033323741_part3 4626432 209717247 102545408 83
Linux
```

In this example, the `/dev/sda3` boot device is the disk that contains the Linux operating system.

b. List the corresponding UUID of the disks by running the following command:

```
linux:/dev/disk/by-id # blkid
```

Example 4-3 shows the output.

Example 4-3 Listing the UUID

```
/dev/sda2: UUID="2d6e8edb-cc0e-4db1-9125-7d4ec8faf58d" TYPE="swap"
/dev/sda3: UUID="6187ca4a-1589-4f57-8c3e-33a4043450b8" TYPE="ext3"
/dev/sdb2: UUID="2d6e8edb-cc0e-4db1-9125-7d4ec8faf58d" TYPE="swap"
/dev/sdb3: UUID="6187ca4a-1589-4f57-8c3e-33a4043450b8" TYPE="ext3"
/dev/mapper/360000970000196800508533033323741_part2:
UUID="2d6e8edb-cc0e-4db1-9125-7d4ec8faf58d" TYPE="swap"
```

In this example, you can identify the UUID of the `/dev/sdb3` disk.

2. Open and edit the `/etc/fstab` file to replace the SCSI ID of the disk with the UUID of the disk, as shown in Example 4-4.

Example 4-4 Editing /etc/fstab

```
linux:~ # cat /etc/fstab
/dev/mapper/360000970000196800508533033323741_part2 swap swap defaults 0 0
#/dev/disk/by-id/scsi-360000970000196800508533033323741-part3 / ext3
acl,user_xattr 1 1
/dev/disk/by-uuid/6187ca4a-1589-4f57-8c3e-33a4043450b8 /boot ext3 acl,user_xattr 1
1 ====> Replace SCSI ID with UUID
proc /proc proc defaults 0 0
sysfs /sys sysfs noauto 0 0
debugfs /sys/kernel/debug debugfs noauto 0 0
devpts /dev/pts devpts mode=0620,gid=5 0 0
```

3. Change the Boot loader option in the Linux VM by using the Linux operating system setup and configuration tool YaST. Select **YaST** → **System** → **Boot loader**. Edit the root device and replace the SCSI ID with the UUID of the disk.

4.3 Installing VMRM DR

After you finish the planning process for your VMRM DR implementation, install the VMRM DR software. The VMRM DR software contains the KSYS package that should be installed on an LPAR in the backup site to manage the DR environment. The VMRM DR solution uses other components such as HMCs, VIOSs, and storage controllers to manage the DR failover. These components were identified during your planning. The VMRM DR DR is enabled by using the following components.

KSYS or controller system

The KSYS software is installed in an AIX LPAR. The KSYS monitors the entire environment and enables DR operations, if required.

HMCs

HMCs in the active site and the backup site manage the IBM Power servers.

VIOS partitions

Various VIOS partitions within hosts of the active site and the backup site virtualize and manage storage resources for the hosts' VMs.

Storage controllers

Storage systems in the active site and the backup site enable storage for the various VMs and the replication between the sites.

4.3.1, “Installation” on page 113 explains the packaging information and installation for the KSYS software. The KSYS software can be installed in any AIX LPAR.

There must be an LPAR in the identified host that has IBM AIX 7.2 with Technology Level 1 Service Pack 1 (7200-01-01) or later installed.

When you install the KSYS software on an LPAR, the LPAR is referred to as the KSYS node. This LPAR controls the entire environment for DR. To support DR for the VMRM DR solution, the KSYS handles discovery, monitoring, notification, recovery, and verification aspects that are associated with DR operations.

4.3.1 Installation

The KSYS file sets must be installed on the identified LPAR, which is preferably at the backup site. You can run the **`installp`** command or use the System Management Interface Tool (SMIT) panel to install the file sets on the LPAR.

Before you install the file sets, ensure that the following prerequisites are met:

- You must have root authority to perform the installation tasks.
- Identify the host that you use to create the KSYS node. The host must be preferably at the backup site during the normal (non-disaster) conditions.
- You must have created an LPAR in the identified host that has IBM AIX 7.2 with Technology Level 1 Service Pack 1 (7200-01-01) or later installed.

- Ensure that you have enough space in this LPAR so that KSYS file sets can be installed successfully. You might want to have 30 MB of disk space in the `/opt` directory and 200 MB of disk space in the `/var` directory.
- Before you install or upgrade VM monitor (VMM) file sets, ensure that you set the VM that you are upgrading to unmanaged in the KSYS and run a discovery operation. Then, you can install or upgrade the VMM file sets on that partition. When complete, set the unmanaged VM back to managed, depending on your requirement. Run the discovery operation again after you change the VM from unmanaged to managed.

KSYS package

The KSYS software consists of file sets that can be installed on any AIX LPAR. The KSYS package consists of the following file sets:

- `ksys.main.rte`
- `ksys.main.cmds`
- `ksys.license`
- `ksys.ha.license`
- `ksys.hautils.rte`
- `ksys.ui.agent`
- `ksys.ui.common`
- `ksys.ui.server`
- `ksys.drutils.rte`
- `ksys.main.msg.en_US.cmds`
- `ksys.main.msg.DE_DE.cmds`
- `ksys.main.msg.ES_ES.cmds`
- `ksys.main.msg.FR_FR.cmds`
- `ksys.main.msg.IT_IT.cmds`
- `ksys.main.msg.JA_JP.cmds`
- `ksys.main.msg.PT_BR.cmds`
- `ksys.main.msg.ZH_CN.cmds`
- `ksys.main.msg.ZH_TW.cmds`

The following file sets are the storage agents. For more information, see 4.5.7, “Adding storage agents to the KSYS” on page 130. For more information and considerations for storage, see Chapter 10, “Advanced topics” on page 261.

- `ksys.mirror.emc.rte`
- `ksys.mirror.svc.rte`
- `ksys.mirror.ds8k.rte`
- `ksys.mirror.hitachi.rte`
- `ksys.mirror.xiv.rte`
- `ksys.mirror.unity.rte`

The following file sets are the VM monitoring agents. Do not install them in the KSYS LPAR. Install them into the managed VMs (AIX or Linux). The installation of the agents is documented in 7.1, “Installing VM Agents” on page 200.

- `ksys.vmmon.rte (for AIX)`
- `./RPMS/linux/vmagent-1.7.0-1.0.el7.ppc64le.rpm (for RHEL)`
- `./RPMS/linux/vmagent-1.7.0-1.0.suse123.ppc64le.rpm (for SUSE Enterprise Linux)`

Installation directories

When installing the KSYS file sets, all the necessary configuration and binary files are installed in the designated directories. Some of the important files and corresponding directories are listed in Table 4-4.

Table 4-4 Directories used during installation of VMRM DR

Type of file	File name	Directory where the files are installed
KSYS administration command: **ksysmgr** binary file	ksysmgr	/opt/IBM/ksys
CPU and memory capacity management command: **ksysrppmgr** binary file	ksysrppmgr	/opt/IBM/ksys
Storage scripts	Multiple storage scripts	/opt/IBM/ksys/storages/EMC/ /opt/IBM/ksys/storages/SVC/ /opt/IBM/ksys/storages/ds8k/ /opt/IBM/ksys/storages/Hitachi/ /opt/IBM/ksys/storages/XIV/ /opt/IBM/ksys/storages/Unity
Samples files for configuration	data_collection setup_dr setup_dr_HBAs setup_dr_ethernet setup_dr_hadiskhbs setup_dr_hostname_ip setup_dr_vgs failover_config.cfg README setup_dr_hostname_ip_via_config_file	/opt/IBM/ksys/samples/site_specific_nw/AIX/
Samples files for configuration	postscript prescript PostHGOffline PostHGOnline PostHGVerify PreHGOffline PreHGOnline PreHGVerify postSiteOffline postSiteOnline postscript preSiteOffline preSiteOnline prescript	/opt/IBM/ksys/samples/custom_validation
Samples files for configuration	event_script_template	/opt/IBM/ksys/samples/event_handler
Snap script directory	vmsnap	/usr/lib/ras/snapscripts/

Type of file	File name	Directory where the files are installed
Log directory	`events.log` `opevents.log`	`/var/keys`

Log directory	`ksysmgr.log`
	`ksysmgr.oplog`
	`ksys_srdf.log`
	`ksys_svc.log`
	`ksys_ccl.log`
	`ksys_xiv.log`
	`ds8k.log`
	`ksys_unity.log`
		`/var/keys/log`

Package size requirement

Most of the KSYS software is installed in the `/opt` file system. However, the KSYS creates multiple log files and trace files as part of first failure data capture (FFDC) information. The minimum disk space that is required for various file systems and directories is listed in Table 4-5 and Table 4-6.

Table 4-5 Preinstallation or update

File system or directory	Required disk space
`/opt`	30 MB

Table 4-6 Postinstallation or update

File system or directory	Required disk space
`/var`	200 MB

Note: The administrator must monitor and maintain the space that is required for the pre-installation and postinstallation requirements.

4.3.2 Installing the KSYS and GUI file sets

To install the KSYS file sets in the identified LPAR, complete the following steps:

1. Ensure that all the prerequisites that are specified in 4.1.1, “Software requirements” on page 94 are complete.
2. Download the VMRM DR software components from Entitled Systems Support (ESS).
3. Copy the file sets to a location that can be used to install the file sets.
4. Decompress the file sets according to the guidelines that are provided with the package.

5. Install the file sets by running the following command:

   ```
   installp -acFXYd fileset_location -V2 [-e filename.log] ksys.!(*vmmon*)
   ```

   The **-V2** flag enables the verbose mode of installation. This command installs all `ksys.*` file sets except for the `ksys.vmmon.rte` file set. Alternatively, you can use the **smit installp** command with the **all_latest** option to install all file sets in the directory.

   – This command also installs all GUI file sets, which include GUI server file sets and GUI agent file sets.

   – The `ksys.vmmon.rte` file is an optional file set that should be installed on VMs. For more information, see 7.1, "Installing VM Agents" on page 200.

6. Verify whether the installation of a file set is successful by running the following command:

   ```
   lslpp -l ksys.*
   ```

7. Run the **/opt/IBM/ksys/ksysmgr** command to check the CLI utility of the KSYS subsystem. The KSYS subsystem might take a few minutes to run the command for the first time. You can add the `/opt/IBM/ksys` directory to the PATH environment variable to access quickly the **ksysmgr** command.

8. After successful installation of the KSYS file sets, enter the following command to check whether the class IDs are reserved:

   ```
   # cat  /opt/rsct/cfg/ct_class_ids | grep IBM.VMR
   IBM.VMR_HMC                                    510
   IBM.VMR_CEC                                    511
   IBM.VMR_LPAR                                   512
   IBM.VMR_VIOS                                   513
   IBM.VMR_SSP                                    514
   IBM.VMR_SITE                                   515
   IBM.VMR_SA                                     516
   IBM.VMR_DP                                     517
   IBM.VMR_DG                                     518
   IBM.VMR_KNODE                                  519
   IBM.VMR_KCLUSTER                               520
   IBM.VMR_HG                                     521
   IBM.VMR_APP                                    522
   IBM.VMR_CLOUD                                  523
   IBM.VMR_DP_CLD                                 524
   IBM.VMR_SA_CLD                                 525
   IBM.VMR_LPAR_CLD                               526
   IBM.VMR_SITE_CLD                               527
   IBM.VMR_VMG_CLD                                528
   ```

If any of the class IDs that are displayed in the preceding screen are missing in your output, add the missing entries into the `/usr/sbin/rsct/cfg/ct_class_ids` file before configuring the KSYS cluster.

4.3.3 Installing GUI file sets

To use the VMRM DR and to manage KSYS nodes by using the GUI, you must install the GUI server and GUI agent file sets on a system. The LPAR in which you want to install the GUI file sets must be running IBM AIX 7.2 with Technology Level 2 Service Pack 1 (7200-02-01) or later. You can choose to install the GUI server and GUI agent file sets on one of the KSYS nodes. For more information about installing the GUI, see Chapter 9, "IBM VMRM GUI deployment" on page 237.

4.4 Configuration overview for VMRM DR

After the KSYS file sets are installed, the VMRM DR solution can be configured. The configuration steps involve adding resources to the KSYS configuration.

The flow chart that is shown in Figure 4-2 provides a summary of the configuration steps for a DR type deployment with a symmetric type of host group and without configuring the workgroups.

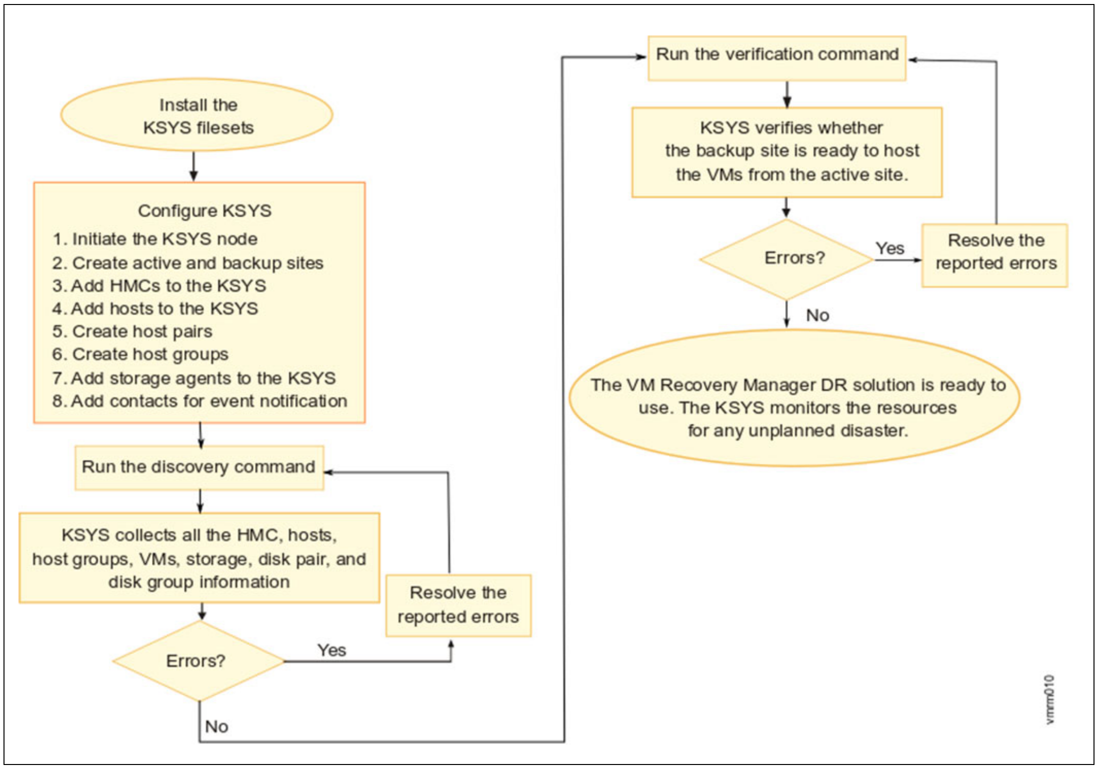

Install the KSYS filesets
Configure KSYS
1. Initiate the KSYS node
2. Create active and backup sites
3. Add HMCs to the KSYS
4. Add hosts to the KSYS
5. Create host pairs
6. Create host groups
7. Add storage agents to the KSYS
8. Add contacts for event notification
Run the discovery command
KSYS collects all the HMC, hosts, host groups, VMs, storage, disk pair, and disk group information
Errors?
Yes
Resolve the reported errors
No
Run the verification command
KSYS verifies whether the backup site is ready to host the VMs from the active site.
Errors?
Yes
Resolve the reported errors
No
The VM Recovery Manager DR solution is ready to use. The KSYS monitors the resources for any unplanned disaster.
vmrm010

Figure 4-2 VMRM DR solution: Installation, configuration, and administration

After the VMRM DR software is installed, setting up the KSYS subsystem is required. Here are the configuration steps to start using the DR feature of the VMRM DR solution.

Note: In later sections of this chapter, we provide detailed instructions and show commands for configuring each resource.

1. Initiating the KSYS node

   After the VMRM DR software is installed on the KSYS LPAR, the KSYS environment must be initiated before configuring the DR environment. The KSYS environment relies on RSCT to create its cluster.

2. Creating sites

   Sites must be created that are used to map the location for all the HMCs, hosts, and storage devices. There is an active site, also referred as the home site, where the workloads are running, and a backup site that acts as a backup for the workloads during a disaster or a potential disaster situation.

3. Adding HMCs to the KSYS

   The KSYS interacts with the HMC for discovery, verification, monitoring, recovery, and cleanup operations. HMCs that are configured in both the active and backup sites provide details about the hosts and VIOS partitions that are managed by the HMCs in each site. The VMRM DR solution cannot be implemented without configuring the HMCs. Therefore, HMC details must be provided to the KSYS.

4. Adding hosts to the KSYS

   The KSYS monitors and manages the DR operations across sites. The KSYS requires that each host must be paired to one or more hosts in the other site. This type of pairing allows the VMs to move from one host to another host across sites. Plan the host pairing across sites in advance, and then implement the pairing.

5. Creating host pairs

   After the hosts are added to the KSYS, identify the hosts that must be paired across the active site and the backup site. Each backup host in the host pair must meet all the resource requirements so that the backup host can run the same workload in a disaster or a potential disaster situation. If you use asymmetric (`mxn_pairing`) pairing, you do not need to create host pairs.

6. Creating host groups

   You can group a set of hosts based on your business requirements. For example, you can group the hosts that run similar type of workloads. You can also group important hosts together so that the monitoring and recovery operations can be performed for the set of hosts together and quickly. In disaster situations, you can move a host group separately to the backup site.

7. Adding storage agents to the KSYS

   In the VMRM DR solution, data is replicated from the active site to the backup site by using storage replication. The KSYS manages the storage subsystems for data mirroring as a part of the DR operations. To manage the storage subsystems, the KSYS uses the APIs that are provided by the storage subsystem. The various storage devices must be registered in all sites with the KSYS as storage agents so that KSYS can monitor and manage the data replication across sites. The storage agents interact with the storage devices or the storage controller software in each site depending on the type of storage in your environment.

8. Setting up contacts for event notification

   The KSYS tracks various events that occur in the environment, analyzes the situation, and notifies you about any issues or potential disaster through the registered contacts. The contact details must be provided to the KSYS so that you can receive notifications about any situation that might need your action.

9. Configuring VIOS

   When you add hosts to the KSYS subsystem, all VIOSs on the hosts are added to the KSYS subsystem. The VMRM DR solution monitors the hosts and VMs by using VIOSs on the host.

10. Customizing consistency group name

    The CG name of the storage subsystems can be customized.

11. Configuring the site-specific IP address

    If the home site and the backup site have different network configuration, the KSYS subsystem uses sample scripts to configure the network configuration that is provided by the user at the backup site.

12. Configuring the Single-Root I/O Virtualization (SR-IOV) override feature

    The SR-IOV override feature can be enabled at the host group level and the site level. The SR-IOV override feature is used during the restart operation. By default, the status of SR-IOV override feature is not set for the site, and the status is disabled for the host group.

4.5 Configuring VMRM DR

This section provides details about the steps that are involved in configuring VMRM DR.

4.5.1 Initializing the KSYS node

After the VMRM DR software is installed on the KSYS LPAR, you must initiate and set up the KSYS environment before you configure the DR environment. The KSYS environment relies on RSCT to create its cluster.

After you create the KSYS cluster, various daemons of RSCT and KSYS are activated. Then, the KSYS LPAR can process the commands that are required to configure the DR environment.

Note: In VMRM DR, the KSYS operates with either a single-node and multi-node cluster. Version 1.7 introduced the multi-node cluster feature, which supports two nodes in a cluster. For more information about how to configure a multi-node KSYS cluster, see Chapter 8, “KSYS high availability” on page 217. For more information, see *Multi-node cluster for KSYS nodes high availability in IBM VM Recovery Manager: Configuring a multi-node cluster and creating the cluster snapshot*.

To create and initiate a single-node or multi-node cluster, complete the following steps:

1. Create a cluster and add the KSYS node to the cluster by running following command, which creates a cluster, adds the KSYS nodes to the cluster, and starts the VMR daemon:

   ```
   ksysmgr add ksyscluster cluster_name ksysnodes=ksys_nodename type=DR sync=yes
   ```

2. Verify the KSYS cluster that was created by running the following command:

   ```
   ksysmgr query ksyscluster
   ```

The output is shown in Example 4-5.

Example 4-5 Querying ksyscluster results

```
Name:                   test_cluster
State:                  Online
Type:                   DR
Ksysnodes:              ksys216.ausprv.stglabs.ibm.com:1:Online
```

When the KSYS cluster is initialized, add the resources that will be managed so that the KSYS is aware of those resources, including the HMCs, hosts, and storage agents.

4.5.2 Creating sites

For a VMRM DR cluster, you must create two sites. All the HMCs, hosts, and storage devices are mapped to a site. Create an active site, also referred as the home site, where the workloads are running, and a backup site that acts as a backup for the workloads during a disaster or a potential disaster situation.

Sites are logical names that represent the physical locations or data centers. A site name can be any American Standard Code for Information Interchange (ASCII) string, but the name is limited to 64 characters. A site name cannot contain any special characters or spaces. Only two sites can be configured. By default, the active site is the home site. When the sites are created, the replication type of the site is set to asynchronous by default. After the sites are created, the type of storage replication can be changed to synchronous. This setting should match the replication type of the storage agents.

To create sites for the VMRM DR solution, complete the following steps in the KSYS LPAR (KSYS controller node):

1. Create an active or home site (Site1) by running the following command:

   ```
   ksysmgr add site Site1 sitetype=home
   ```

2. Create a backup site (Site2) by running the following command:

   ```
   ksysmgr add site Site2 sitetype=backup
   ```

3. Verify the sites that were created by running following command:

   ```
   ksysmgr query site
   ```

The output of **query site** is displayed in Example 4-6.

Example 4-6 Output of query site

```
Name:                Site2
            Sitetype:           BACKUP
            Active Host_groups: None
            Active Workgroups:  None

            Name:               Site1
            Sitetype:           HOME
            Active Host_groups: None
            Active Workgroups:  None
```

4. If the storage replication is synchronous, the KSYS **replication_type** should be modified because it was configured as asynchronous by default. If the configuration uses a shared storage configuration for DR replication, then the **replication_type** should be set to `shared`.

   To modify the replication type, run the following command:

   ```
   ksysmgr modify system replication_type=sync sites=Site1,Site2
   ```

   The **replication_type** attribute supports the following values: `sync`, `shared`, and `async` (default).

4.5.3 Adding HMCs to the KSYS

The KSYS interacts with the HMC for discovery, verification, monitoring, recovery, and cleanup operations. HMCs that are configured in both the active and backup sites provide details about the hosts and VIOS partitions that are managed by the HMCs in each site. The VMRM DR solution cannot be implemented without configuring the HMCs.

> **Note:** The HMC user, whose username and password details are provided to the KSYS, must have `hmcsuperadmin` privileges with remote access enabled.

To add the HMCs to a specific site, complete the following steps on the KSYS LPAR:

1. Add the HMC that manages the host or hosts in the active site (Site1) by running the following command:

   ```
   ksysmgr add hmc Site1_HMC1 login=hscroot password=xyz123
   hostname=Site1_HMC1.testlab.ibm.com site=Site1
   ```

   > **Note:** To avoid entering the password on the CLI, the **`password`** value can be omitted. In this case, the **`ksysmgr`** command prompts for the password later.

2. Add the HMC that manages the host or hosts in the backup site (Site2) by running the following command:

   ```
   ksysmgr add hmc Site2_HMC1 login=hscroot password=xyz123
   hostname=Site2_HMC1.testlab.ibm.com site=Site2
   ```

3. Repeat steps 1 and 2 for all the HMCs that you want to add to the KSYS.
4. Verify the HMCs that are added by running the following command:

   ```
   ksysmgr query hmc
   ```

   The output for this query is shown in Example 4-7.

Example 4-7 Query HMC command output

```
Name:              Site2_HMC1
Site:              Site2
Ip:                9.xx.yy.zz
Login:             hscroot

                        Managed Host List:

Hostname                               UUID
=========                               ====
Host1_Site2                             82e8fe16-5a9f-3e32-8eac-1ab6cdcd5bcf
Host2_Site2                             74931f30-e852-3d47-b564-bd263b68f1b1
Host3_Site2                             c15e9b0c-c822-398a-b0a1-6180872c8518
Host4_Site2                             f6cbcbda-8fec-3b6e-a487-160ca75b2b84
Host5_Site2                             4ce17206-4fde-3d5a-a955-dbf222865a77
Host6_Site2                             346f184d-bace-36f5-97b5-3955c62a6929
Host7_Site2                             a977d52e-fd3a-325d-bd02-124663066cac
Host8_Site2                             ae115482-3a50-32f3-935a-7ff9be433e33
Host9_Site2                             b3880199-3b8b-3ade-b360-f76146c2d7f3
Host10_Site2                            26c7c48e-3b81-363b-85d0-e110ebc43b15
============================================================================
```

```
Name:              Site1_HMC1
Site:              Site1
Ip:                9.xx.yy.zz
Login:             hscroot


                        Managed Host List:

Hostname                               UUID
=========                               ====
Host1_Site1                             caffee0a-4206-3ee7-bfc2-f9d2bd3e866f
Host2_Site1                             6ce366c5-f05d-3a12-94f8-94a3fdfc1319
Host3_Site1                             67ff62ec-ecb5-3ad4-9b35-0a2c75bb7fe4
============================================================================
```

Note: If the HMC password contains any special characters, then use the following command to define the HMC:

```
ksysmgr add hmc HMC1 login=hscroot site=Site1
```

Because the password was not specified, **ksysmgr** prompts you to enter the password.

4.5.4 Adding hosts to the KSYS

After the HMCs are added to the KSYS, review the list of managed hosts by each HMC, and then identify the required hosts to add to the KSYS for DR.

Important: Do not use the same HMC to connect to hosts across the sites. If you connect the source hosts and target hosts to the same HMC, it leads to an invalid configuration in the KSYS subsystem, which can cause failures in DR operations.

When a host is added to a host group, all the VMs on the host are included as managed by default. If you plan to exclude a set of VMs that were defined as a result of adding hosts, you can unmanage those VMs before running the discovery and verification operations.

Priority types of high, medium, or low can be set for the VMs. You can prioritize your VMs either within a single host or among multiple hosts. Higher-priority VMs that run your more important workloads are considered first for a move operation. When running a move operation, the **ksysmgr** command initiates the operation for the VMs that have the highest priority first.

You can obtain the hostname by querying the HMC. The hostname can be copied and used in the command execution.

To add the hosts to the KSYS configuration, complete the following steps in the KSYS LPAR:

1. Add the managed host that is running the workload in site1 by running the following command:

   ```
   ksysmgr add host Site1_host1 site=Site1
   ```

   The Site1_host1 host, which is a managed host for the Site1_HMC1 HMC, is added in the active site.

2. Add the backup host at site2 that acts as a backup host to the KSYS by running the following command:

   ```
   ksysmgr add host Site2_host1 site=Site2
   ```

3. Repeat steps 1 on page 123 and 2 for all hosts that will be added to the KSYS.
4. Verify that the hosts are added by running the following command:

   ```
   ksysmgr query host
   ```

   The results for the query host look like Example 4-8.

Example 4-8 Query host command results

```
Name:            Site2_host1
                UUID:            c15e9b0c-c822-398a-b0a1-6180872c8518
                FspIp:
                Host_group:      No host_group defined
                Pair:            None
                Vswitchmap:      Not currently set
                Vlanmap:         Not currently set
                DrVswitchmap:    Not currently set
                DrVlanmap:       Not currently set
                Skip_power_on:   No
                Site:            Site2
                VIOS:            Site2_VIOS1
                                 Site2_VIOS2
                HMCs:            Site2_HMC1
                MachineSerial:   xyz
                ProcPools:       DefaultPool

                Name:            Site1_host1
                UUID:            67ff62ec-ecb5-3ad4-9b35-0a2c75bb7fe4
                FspIp:
                Host_group:      No host_group defined
                Pair:            None
                Vswitchmap:      Not currently set
                Vlanmap:         Not currently set
                DrVswitchmap:    Not currently set
                DrVlanmap:       Not currently set
                Skip_power_on:   No
                Site:            Site1
                VIOS:            Site1_VIOS1
                                 Site1_VIOS2
                HMCs:            Site1_HMC1
                MachineSerial:   xyz
                ProcPools:       DefaultPool
```

5. To exclude any VMs from being managed, run the following command for each VM:

   ```
   ksysmgr unmanage vm name=vmname host=hostname | uuid=lparuuid | ALL
   host=hostname | ALL host_group=hg_name
   ```

   To place a VM under KSYS management again, run the following command:

   ```
   ksysmgr manage vm vmname|lparuuid
   ```

6. To specify a priority for specific VMs for the move operation, run the following command:

   ```
   ksysmgr modify VM name1[,name2,name3,...] | file=filepath [uuid=uuid_value
   [host=hostname] [priority=low|medium|high]
   ```

Note: The **`file`** parameter is an XML file that contains a list of VM references.

4.5.5 Creating host pairs

The KSYS monitors and manages the DR operations across sites. With the KSYS, each host must be paired to another host across sites in a symmetric host group configuration. This type of pairing enables the VMs to move from one host to another host across sites. Carefully plan the host pairing across sites in advance, and then implement the pairing. After the hosts are added to the KSYS, identify the hosts that must be paired across the active site and the backup site. Each backup host in the host pair must meet all the resource requirements so that the backup host can run the same workload in a disaster or a potential disaster situation.

Note: If asymmetric host group configuration is being used, do not pair the hosts.

Host pairing guidelines

Each host in a pair must belong to different sites:

- The paired host in the backup site always must have enough resources to host the managed VMs from the active site.

  For example, if the active site is Site_1 and the Host_1 host in that site is running 55 VMs that require 100 cores of CPU and 512 GB of memory, you can pair the Host_1 host from the active site with the Host_2 host on the backup site only when the Host_2 host contains at least 100 cores of CPU and 512 GB of memory. If the capacity is not sufficient in the backup host, a warning is issued during the validation process.
- If you are using Enterprise Pools, Host_2 can borrow required resources from the Enterprise Pool before the VMs are moved.
- You can pair different generations of Power servers. For example, you can pair a POWER8 server with a POWER9 server. However, the target server should have enough resources to host the production VMs.

To pair the hosts across the sites in the VMRM DR solution, complete the following steps in the KSYS LPAR:

1. Pair the identified host (for example, hostname: Site1_host1) in the active site to the identified host (for example, hostname: Site2_host1) in the backup site by running the following command:

   ```
   ksysmgr pair host Site1_host1 pair=Site2_host1
   ```
2. Repeat step 1 for all the host pairs that you create.
3. Verify the host pair that you created by running the following command:

   ```
   ksysmgr query host
   ```

   The output of query host shows the paired hosts, as shown in Example 4-9.

Example 4-9 query host output

```
Name:            Site2_host1
                UUID:           c15e9b0c-c822-398a-b0a1-6180872c8518
                FspIp:
                Host_group:     No host_group defined
                Pair:           Site1_host1
                Vswitchmap:     Not currently set
                Vlanmap:        Not currently set
```

```
DrVswitchmap:    Not currently set
DrVlanmap:       Not currently set
Skip_power_on:   No
Site:            Site2
VIOS:            Site2_VIOS1
                 Site2_VIOS2
HMCs:            Site2_HMC1
MachineSerial:   xyz
ProcPools:       DefaultPool

Name:            Site1_host1
UUID:            67ff62ec-ecb5-3ad4-9b35-0a2c75bb7fe4
FspIp:
Host_group:      No host_group defined
Pair:            Site2_host1
Vswitchmap:      Not currently set
Vlanmap:         Not currently set
DrVswitchmap:    Not currently set
DrVlanmap:       Not currently set
Skip_power_on:   No
Site:            Site1
VIOS:            Site1_VIOS1
                 Site1_VIOS2
HMCs:            Site1_HMC1
MachineSerial:   xyz
ProcPools:       DefaultPool
```

4. If you must unpair the existing host, first remove the host from the host group, and then run the following command:

```
ksysmgr pair host Site1_host1 pair=none
```

4.5.6 Creating host groups

There are two types of host groups within VMRM DR: symmetric and asymmetric. A symmetric host group consists of several hosts in a one-to-one pairing where all hosts in the primary site that are included in a symmetric host group must be paired with a host in the backup site. An asymmetric host group enables a many-to-many grouping between the hosts at the primary site and those hosts at the backup site.

Symmetric host group

It is possible to group a set of hosts based on your business requirements. For example, it is possible to group the hosts that run similar type of workloads. Also, important hosts can be grouped so that the monitoring and recovery operations can be performed for the set of hosts together and quickly. In disaster situations, a host group can be moved separately to the backup site.

Guidelines to manage host groups

- When creating a symmetric host group, each host already must be added to the KSYS configuration settings and that host must be paired with a backup host in the backup site.
- Each host in a site must be a part of a host group. If a paired host is not added to any host groups, the host is automatically added to the Default_HG host group during the discovery operation.

- If you add or remove hosts from a host group, you must run a discovery operation to manage or unmanage all the VMs from the recovery management. The modified host group displays the correct list of managed VMs only after a discovery operation.
- The corresponding hosts in the backup site that are paired with the active site hosts are grouped logically within the same host group. For example, if host1 in the active site is paired with host2 in the backup site and you create a host group hg1 with host1, then host2 is added automatically to the host group hg1.
- Each host group is associated with a separate disk group. The disks in the disk group must not be shared among different host groups. The disk groups are named in the following format:

  ```
  VMRDG_{peer_domain_name}_{site_name}_{host_group_ID}
  ```

  The disk group name must not exceed the maximum number of characters that is supported for a CG at the storage controller.

To add hosts groups to the KSYS configuration, complete the following steps in the KSYS LPAR:

1. To create a host group and add the existing hosts that you want to include in this host group, run the following command:

   ```
   ksysmgr add host_group hg1 [site=<Site_1>] hosts=Host_11,Host_12,Host_13
   [mxn_pairing=<yes>] [workgroup_support=<no>]
   ```

   – By default, the **mxn_pairing** attribute is set to `no`. Hosts must be paired before adding the hosts to the host group. When one host in the host pair is added to a host group, the other host of the host pair automatically is added to the respective host group in the other site. These hosts form a symmetric host group, which contains one-to-one paired hosts.

   – To create an asymmetric host group, which contains one-to-many paired hosts, set the **mxn_pairing** attribute to `yes`. In this case, hosts should not paired before adding the hosts to the host group. Host and host-group pairing of all hosts must be performed manually.

   – All the hosts in the backup site that are paired with the specified hosts are also added to the host group.

   – By default, the **workgroup_support** attribute is set to `yes`. A host group is automatically created with the workgroup. To disable the workgroup support for a host group, set the **workgroup_support** attribute to `no` when adding the host group.

   – Any VMs running in the backup site on the hosts in a host group are no longer managed after a host group is created.

   – By default, the KSYS subsystem considers VMs of the home site to create a host group. To create a host group and add VMs at the backup site to the host group, use the **site** option in the **ksysmgr** command.

2. Repeat step 1 to create all host groups in the KSYS subsystem.
3. To verify that the host groups exist, run the following command:

   ```
   ksysmgr query host_group hgname
   ```

The output from running this command is shown in Example 4-10.

Example 4-10 ksysmgr query host_group

```
Name:              hg1
Home Site Hosts:   Host_11
                   Host_12
                   Host_13
Backup Site Hosts: Host_21
                   Host_22
                   Host_23
Workgroups:        none
Memory_capacity:   Priority-Based Settings
                   low:100
                   medium:100
                   high:100
CPU_capacity:      Priority-Based Settings
                   low:100
                   medium:100
                   high:100
skip_power_on:     No
sriov_override:    No
Site:              Site1
Vswitchmap:        Not currently set
Vlanmap:           Not currently set
DrVswitchmap:      Not currently set
DrVlanmap:         Not currently set
Type:              symmetric
Custom CG Name:
Backup Site CG Name:
```

4. To add or remove hosts from the existing host groups, run the following command:

   ```
   ksysmgr modify host_group hg_name add | remove hosts=host1,host2... |
   file=filepath
   ```

   The **file** parameter is an XML file that contains a list of hosts. An example of the XML file is shown in Example 4-11.

Example 4-11 XML file format for adding or removing hosts

```
<KSYSMGR><HOST><NAME>host1</NAME></HOST></KSYSMGR>
<KSYSMGR><HOST><NAME>host2</NAME></HOST></KSYSMGR>
<KSYSMGR><HOST><NAME>host3</NAME></HOST></KSYSMGR>
```

5. To modify the capacity-related attributes for all the hosts in a host group, run the following command:

   ```
   ksysmgr modify host_group hg_name options
   [memory_capacity=<(1-100) | minimum | current_desired | none | default>
   priority=<low | medium | high>]
   [cpu_capacity=<(1-100) | minimum | current_desired | none | default>
   priority=<low | medium | high>]
   [skip_power_on=<yes|no>]
   ```

For more information about setting flexible capacity policies. see 4.7.2, “Configuring the flexible capacity policies” on page 146 and Configuring the flexible capacity policies.

Asymmetric host group

The VMRM DR solution can manage an environment in which *M* number of hosts on the home site are configured to failover to *N* number of hosts on the backup site. This mode is known as *one-to-many pairing*.

When you create a host group, provide a custom name of the storage composite group (CG) that is defined in the storage controller. This parameter is specific to the type of storage that is used in the cluster. For example:

- For a Dell EMC storage agent, the composite group name of the source storage agent and the composite group name of the target storage agent can be different. While creating a host group, you can specify a custom name for the composite group that will be created. For Dell EMC storage agents, two different attributes, **customcgname** and **bsitecgname**, are used for the source storage agent and the target storage agents.
- For storage systems other than Dell EMC storage systems, the composite group name of the source storage agent and the composite group name of the target storage agent must be the same.

To create an asymmetric host group with Dell EMC storage systems, run the command that is shown in Example 4-12.

Example 4-12 The ksysmgr add host_group command syntax

```
ksysmgr add host_group <host_group_name>
hosts=<host1[,host2,...]> | file=filepath
[ha_disk=<ViodiskID>]
[repo_disk=<ViodiskID>]
[backup_repo_disk=<ViodiskID[,ViodiskID2...]> |  backup_repo_disk=none]
[mxn_pairing=<yes>][customcgname=<CgName>] [bsitecgname=<CgName>]
add => ad*, cr*, make, mk
host_group => hg, host_g*
```

For example:

```
ksysmgr add host_group <name> hosts=<host1,host2,.. hostn> mxn_pairing=yes
customcgname=<source_cg_name> bsitecgname=<target_site_cgname>
```

> **Note:** If the storage subsystem in a cluster is not a Dell EMC, **bsitecgname** is not required.

While creating an *asymmetric* host group, the hostnames must be provided from both sites and the specified hosts cannot be paired. By default, the host group type is *symmetric*. To create an *asymmetric* host group, set the value of the **mxn_pairing** attribute to `yes`. Similarly, if you want to use a workgroup, set the **workgroup_support** attribute to `yes`.

In an asymmetric host group configuration, the KSYS subsystem dynamically determines the target host for a VM. This mapping is determined based on the resource availability on the target site during the discovery operation. You can query a VM to view the target host of the VM.

Run the following command to query the VM:

```
ksysmgr q vm
```

Running this command produces the output that is shown in Example 4-13.

Example 4-13 The ksysmgr query vm output

```
ksysmgr query vm vm1

Name:                vm1
UUID:                1D001C62-3E50-4E8D-9A89-FE22F089401F
State:               READY
Dr Test State:       READY
Host:                Site1_host1
Priority:            Medium
Skip_power_on:       None
Homehost:            Site1_host1
DrTargetHost:        Site1_host2
Active Pool:         DefaultPool
PoolMap:             None
```

The `DrTargetHost` field displays the name of the host where a VM will be moved during the move operation.

To manually specify the target host of a VM, put the target host in the `DrTargetHost` field and run the **`ksysmgr modify vm`** command. Otherwise, the KSYS subsystem updates this attribute automatically during the discovery operation. If you want to change the target host of a VM, specify `None` as the value for the `DrTargetHost` field to allow the KSYS subsystem to automatically determine the target host of the VM.

Run the following command to set a target host for a VM in an asymmetric host group setting:

```
ksysmgr modify vm <vm_name> DrTargetHost=<host_name>
```

Note: The `DrTargetHost` field should be used only for asymmetric host group VMs.

Important: The type, symmetric or asymmetric, that is set as you are adding the host_group cannot be modified later.

4.5.7 Adding storage agents to the KSYS

In the VMRM DR solution, data is replicated from the active site to the backup site by using storage replication. The KSYS manages the storage subsystems for data mirroring as a part of the DR operations. To manage the storage subsystems, the KSYS uses the APIs that are provided by the storage subsystem's manufacturer. Register the various storage devices in all sites with the KSYS as storage agents so that KSYS can monitor and manage the data replication across sites. The storage agents interact with the storage devices or the storage controller software in each site depending on the type of storage in your environment.

Important: All the prerequisite software must be installed on the same LPAR in which the KSYS software is installed.

If the storage subsystem uses a storage controller software, the storage controller software also must be installed on the KSYS LPAR.

The storage controller is the software component that you receive from the storage vendor that enables KSYS to contact storage devices and perform replication operations.

The VMRM DR solution supports the following storage agents:

- Dell EMC SRDF storage systems
- SAN Volume Controller and Storwize devices
- DS8000 series storage devices
- Hitachi storage devices
- IBM XIV Storage Systems
- Dell EMC Unity

Dell EMC storage

For Dell EMC storage, the storage agent uses the Symmetrix Application Program Interface (SYMAPI) commands that interact with the Dell EMC Solution Enabler software to manage the Dell EMC storage devices. You can use the SYMAPI commands (for example, **`symcfg list`**) to determine the 12-digit serial number and the IP address of the storage device. For more information, see the IBM Systems Technical white paper *Dell EMC SRDF storage agent configuration for IBM Virtual Machine Recovery Manager*.

SAN Volume Controller and Storwize storage devices

For IBM SAN Volume Controller Storage Systems and other IBM Storage Systems that are based on the SAN Volume Controller code, such as Storwize or IBM FlashSystem Storage Systems, the storage agent uses specific storage scripts and their corresponding interfaces to interact with the storage devices. When you add an IBM SAN Volume Controller based storage agent to the KSYS subsystem, you must specify the cluster ID, storage login username, and the IP address of the storage subsystem.

D8000 series storage devices

For a DS8000 Series Storage System, the storage agent uses specific storage scripts and their corresponding interfaces to interact with the storage devices. When you add a storage agent for the DS8000 Storage System, you must specify the serial number or the storage controller, storage login username, password, and the IP address of the storage subsystem.

Hitachi storage devices

For Hitachi storage systems, the storage agents use the CCI to interact with the CCI server to manage the storage devices.

IBM XIV Storage Systems

Specify the serial number of the storage system, login username and password of the storage, and the IP address of the storage system when adding IBM XIV Storage Systems.

Dell EMC Unity storage devices

Beginning with VMRM DR 1.5 Service Pack 1, VMRM DR supports the Dell EMC Unity storage agent for storage management.

> **Note:** For more detailed instructions about defining storage, see 10.4, “Storage components in the IBM VMRM DR solution” on page 268.

To add storage agents to KSYS node, use the command that is shown in Example 4-14.

Example 4-14 The add storage agent command

```
# ksysmgr add storage_agent -?
      ksysmgr add storage_agent <storage_agent_name>
         hostname | ip =<hostname[,hostname2,hostname3] | ip[,ip2,ip3]>
         site=<sitename>
         storagetype=<type>
         serialnumber=<number> | clusterid=<number> | instance=<instance_number>
         [login=<username>]
         [password=<password>]
         [drinstance=<drinstance_number>]
       add => ad*, cr*, make, mk
       storage_agent => storage*, sta
```

Here are some additional notes for storage agents:

- A login and password might be needed for some storage devices.
- An instance number is required only for Hitachi storage.
- A DrInstance number is required only for Hitachi when performing a DR test.
- XIV storage devices can have up to three IP addresses.

Here are example syntaxes for various storage types:

- SAN Volume Controller storage:

  ```
  ksysmgr add storage_agent <storage_agent_name>
     hostname | ip =<hostname | ip>
     site=<sitename>
     storagetype=svc
     clusterid=<number>
  login=<username>
  ```

- Dell EMC/SRDF storage:

  ```
  ksysmgr add storage_agent <storage_agent_name>
     hostname | ip =<hostname | ip>
     site=<sitename>
     storagetype=srdf
     serialnumber=<number>
  ```

- DS8000 storage:

  ```
  ksysmgr add storage_agent <storage_agent_name>
     hostname | ip =<hostname | ip>
     site=<sitename>
     storagetype=ds8k
     serialnumber=<number>
     login=<username>
     password=<password>
  ```

- Hitachi storage:

```
ksysmgr add storage_agent <storage_agent_name>
   hostname | ip =<hostname | ip>
   site=<sitename>
   storagetype=hitachi
   serialnumber=<number>
   instance=<instance_number>
   [drinstance=<drinstance_number>]
   login=<username>
   password=<password>
```

- XIV storage:

```
ksysmgr add storage_agent <storage_agent_name>
   hostname | ip =<hostname[,hostname2,hostname3] | ip[,ip2,ip3]>
   site=<sitename>
   storagetype=xiv
   serialnumber=<number>
   login=<username>
   [password=<password>]
```

- Unity storage:

```
ksysmgr add storage_agent <storage_agent_name>
   hostname | ip =<hostname | ip>
   site=<sitename>
   storagetype=unity
   serialnumber=<number>
   login=<username>
   [password=<password>]
```

4.5.8 Creating a workgroup

A *workgroup* is a logical grouping of a subset of hosts within your host group. One or more workgroups can be created within a host group, and you can add VMs to the workgroups. A workgroup can simplify operations by providing a single point of control for all VMs in the workgroup. All operations and commands that are run for host group also can run for a workgroup.

A default workgroup is created automatically when a host group is created. If a workgroup has not been created and you add any VMs to the host group, all the VMs are added to the default workgroup.

When running a command on a workgroup, the command operation takes effect on all the VMs that are defined in the workgroup. When running a discovery or verifying, moving, or running DR test operations at a host group level, the operations also take the same effect on the workgroups within the host group.

Note: If you do not want workgroup support, create the host group with the workgroup attribute set to `no`.

Figure 4-3 shows the host group, workgroup, and VM configuration.

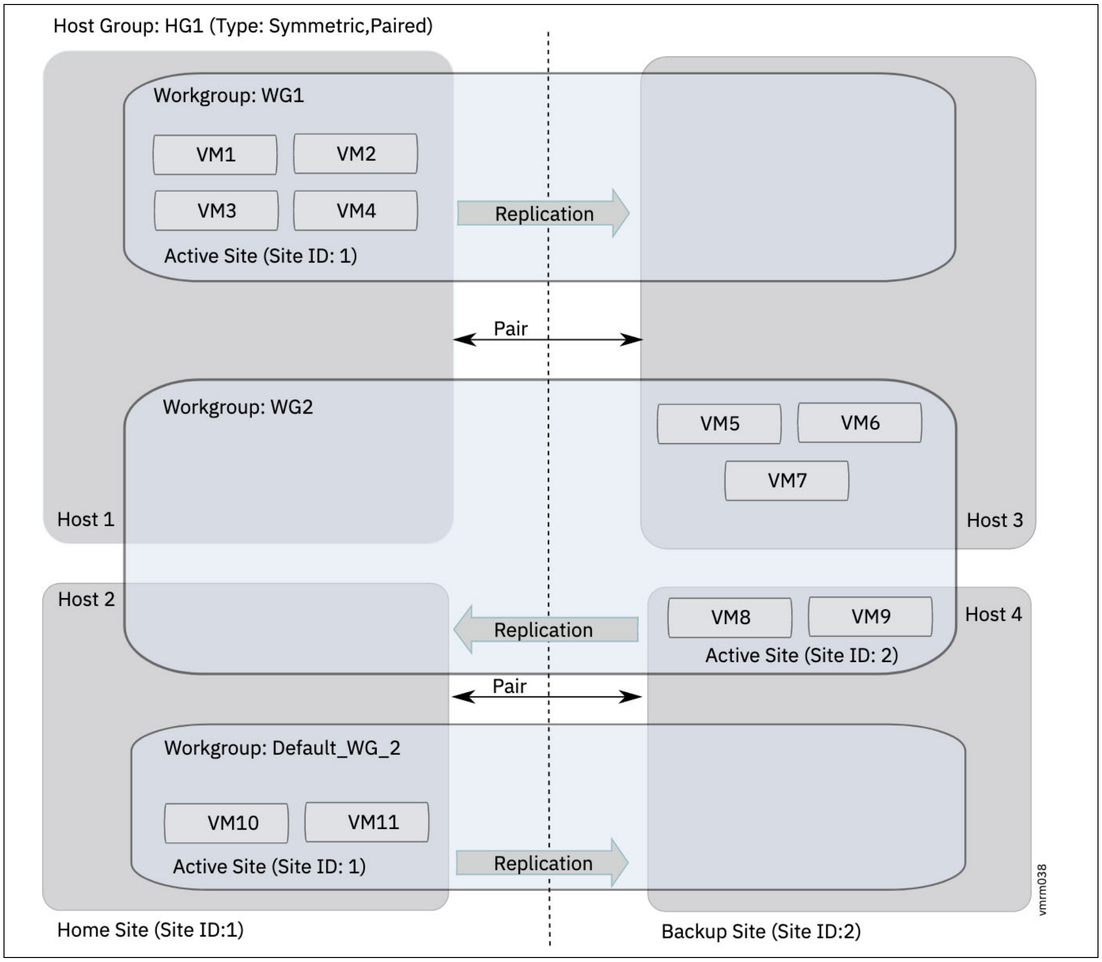


Figure 4-3 Host group, workgroup, and VM configuration

In Figure 4-3, four host groups are added to a symmetric host group configuration. Host1 and Host2 belong to the home site. Host3 and Host4 belong to the backup site. The hosts from home site, Host1 and Host2, are paired to the hosts in the backup site, Host3 and Host4. The VMs of the host groups are added to the two different workgroups. If a workgroup is not created and you add VMs to the host group, all the VMs are added to the default workgroup.

4.5.9 Discovering DR configurations

After adding the various HMCs, hosts, host groups, and storage subsystems to the KSYS subsystem for DR management, run the **ksysmgr discover** command to discover all the hosts that are managed by the HMCs in both the home and the backup sites. During the discovery process, the KSYS subsystem captures the configuration information of the home site and its relationship with the backup site and prepares the backup site to perform DR operations when needed later.

During the initial discovery operation, the KSYS subsystem uses its configuration information to gather the list of VMs from all the host groups across the sites and the corresponding disks for DR management. During any subsequent discovery operations, the KSYS subsystem scans the environment for any changes to the environment (for example, the addition of a new VM, the addition of a disk to VM, or the LPM movement of a VM from one host to another host) and adapts to the modified environment.

The KSYS subsystem interacts with the HMC to retrieve the details about the disks of each VM and check whether the VMs are set up with mirrored storage devices. If the disks are not set up properly for mirroring, the KSYS subsystem notifies you about any volume groups that are not mirrored. All volume groups of a VM must be mirrored. Disks can be accessed over NPIV, vSCSI, or a combination of both of these modes.

The KSYS subsystem identifies and stores the UUID of the boot disk for each VM during the discovery operation. The KSYS subsystem also stores the information about the corresponding replicated boot disks in the backup site. When you initiate a DR operation, the KSYS subsystem uses this information to start the VMs with the corresponding boot disks on the paired host in the backup site. For example, if a VM in the home site has multiple bootable disks, the KSYS subsystem restarts the VM by using the corresponding boot disk in the backup site.

Important: The VMRM DR identifies and stores the boot disk information for POWER8, and later processor-based servers. The VMRM DR solution requires HMC 8.8.6.0 Service Pack 1 or later to support this feature. If your production environment contains an older version of the host or HMC, the KSYS subsystem cannot store the boot disk information, and the VMs restart in the backup site by using the first disk in the SMS menu.

- If the configuration is modified, for example, an LPAR or a storage device is added, the KSYS subsystem rediscovers the home site, identifies the changes in the configuration, and marks the changes in its registries. The KSYS subsystem monitors this new environment for any disaster situations.
- For Dell EMC storage subsystem, the Gatekeeper and Access Control Logix (ACLX) devices are ignored by the KSYS node during the discovery operation. Similarly for Hitachi, command devices are ignored by the KSYS node during the discovery operation.

By default, the KSYS subsystem automatically rediscovers sites once every 24 hours. This frequency can be changed by modifying the **`auto_discover_time`** attribute. However, if the configuration was modified by adding or removing any resource and you want the KSYS subsystem to rediscover the resources immediately, you can manually run the **`ksysmgr discover`** command. When running a discovery operation for a site, the KSYS subsystem might take a few minutes to discover all the VMs in all the host groups across both sites and to display the output. If you want a quicker result, run the discovery operation only for the specific host group that was modified.

After a VM is migrated within a site or across the sites, and multiple disk systems are used, you should run the discovery operation manually to update the KSYS configuration. However, if you do not run the discovery operation manually, the periodic discovery discovers the changes automatically when it runs.

To discover resources in the KSYS configuration settings, complete one of the following steps in the KSYS LPAR:

- To discover all the resources across both sites, run the following command:

  ```
  ksysmgr discover site site_name
  ```

  The KSYS subsystem discovers all the hosts and VMs from all the host groups across both sites. Therefore, it might take a few minutes to discover all the hosts and display the output.

- To discover all the hosts in a specific host group, run the following command:

  ```
  ksysmgr discover host_group hg_name
  ```

- To discover all VMs in a specific workgroup, run the following command:

  ```
  ksysmgr discover workgroup workgroup_name
  ```

VM auto discovery

VM auto discovery is controlled by a system-level property (**`vm_auto_discovery`**), which you can set as `disabled` or `enabled`. By default, this property is enabled.

The KSYS subsystem manages all VMs automatically by default. Setting the VM auto-discovery property defines whether the KSYS subsystem automatically manages newly created VMs and undiscovered VMs when they are discovered.

If the **`vm_auto_discovery`** property is `enabled`, all VMs are managed automatically. If it is `disabled`, any newly created VMs on the KSYS-managed hosts and any undiscovered VMs will *not* be managed by the KSYS subsystem.

To check whether the **`vm_auto_discovery`** property is enabled or disabled, run the following command:

```
# ksysmgr -a vm_auto_discovery query system

System-Wide Persistent Attributes
vm_auto_discovery:           enable
```

To enable or disable the attribute, run following relevant command:

- **`ksysmgr modify system vm_auto_discovery=enable`**
- **`ksysmgr modify system vm_auto_discovery=disable`**

4.5.10 Verifying a DR configuration

After the KSYS subsystem discovers the resources, it monitors the entire environment for any disaster situations and verifies whether the configuration setting is valid for both sites. This verification is required to ensure that the backup site is ready to host the workloads of the VMs from the home site during a site switch for DR operation. If you set a priority to specific VMs, the verification operation is initiated for the VMs that have the highest priority.

To validate the configuration setting in both sites, complete one of the following actions in the KSYS node:

- To validate the configuration in the home site, run the following command:

  ```
  ksysmgr verify site home_site_name
  ```

  The KSYS subsystem validates the configuration settings on all the hosts and VMs from all the host groups across both sites. You can perform both the discovery and verification operations by running the following command:

  ```
  ksysmgr discover site site_name verify=yes
  ```

- To validate the configuration for a specific host group, run one of the following commands:
  - **`ksysmgr verify host_group hg_name`**
  - **`ksysmgr discover host_group hg_name verify=yes`**
- To validate the configuration for a specific workgroup, run one of the following commands:
  - **`ksysmgr verify workgroup workgroup_name`**
  - **`ksysmgr discover workgroup workgroup_name verify=yes`**

If an error occurs during the verify operation, the **`ksysmgr`** CLI displays it.

The **`ksysmgr query system status`** command can be used to view the status of the VM. If the verification process is successfully done, the state of the VM will be in the `READY_TO_MOVE` state. This state ensures that the configuration is good for the planned DR operation.

Daily checks by KSYS

The KSYS subsystem checks the active site in the VMRM DR environment daily to ensure that any change in the configuration setting or resources is discovered and verified by the KSYS subsystem. The daily verification checks ensure that the workloads are always ready to be moved to the backup site if any disaster occurs.

Daily checks that KSYS performs can be disabled as needed. By default, daily KSYS checks are enabled.

```
# ksysmgr -a quick_discovery query system

   System-Wide Persistent Attributes
   quick_discovery:             enable
```

To disable the checks, run the following command:

```
# ksysmgr modify system quick_discovery=disable

   KSYS quick_discovery has been updated
```

Now, the query results are as follows:

```
# ksysmgr -a quick_discovery query system

   System-Wide Persistent Attributes
   quick_discovery:             disable
```

4.6 Moving virtual machines across sites

After the verification phase, the KSYS continues to monitor the active site for any failures or issues in any resources at the site. When any planned or unplanned outages occur, if the situation requires DR, the recovery or move must be manually initiated by using the **ksysmgr** command, which moves the VMs to the backup site. The flowchart that is shown in Figure 4-4 shows the recovery process for a VMRM DR solution.

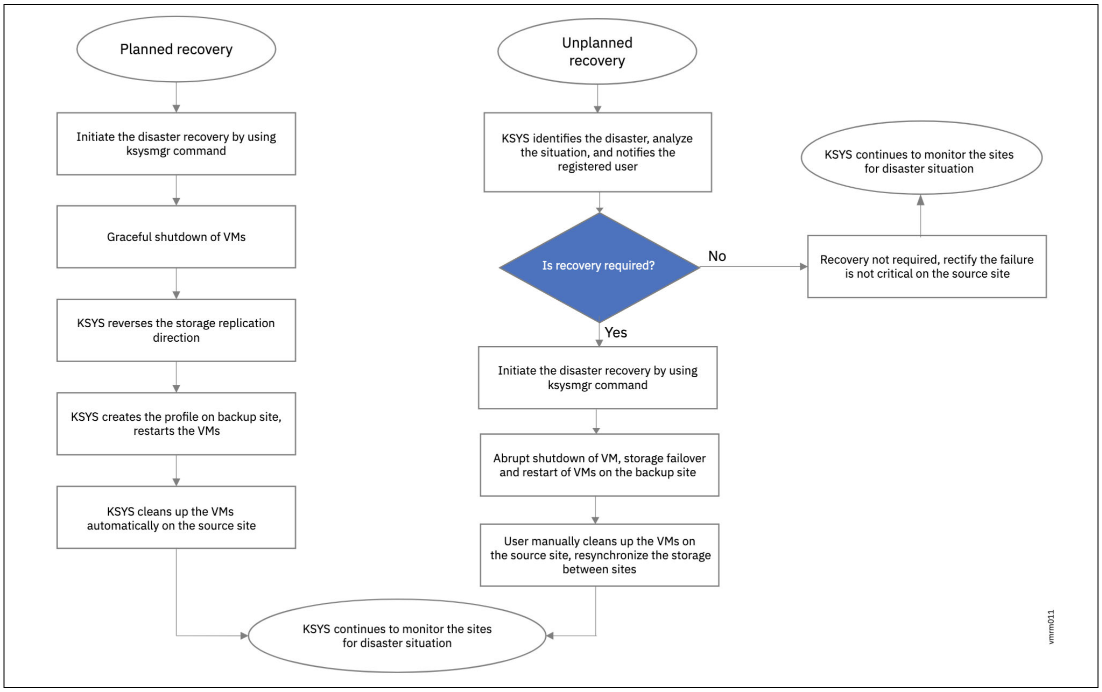

Planned recovery
Initiate the disaster recovery by using ksysmgr command
Graceful shutdown of VMs
KSYS reverses the storage replication direction
KSYS creates the profile on backup site, restarts the VMs
KSYS cleans up the VMs automatically on the source site
Unplanned recovery
KSYS identifies the disaster, analyze the situation, and notifies the registered user
Is recovery required?
No
Recovery not required, rectify the failure is not critical on the source site
KSYS continues to monitor the sites for disaster situation
Yes
Initiate the disaster recovery by using ksysmgr command
Abrupt shutdown of VM, storage failover and restart of VMs on the backup site
User manually cleans up the VMs on the source site, resynchronize the storage between sites
KSYS continues to monitor the sites for disaster situation
vmrm011

Figure 4-4 VMRM disaster recovery process

4.6.1 Initiating a disaster recovery

In a planned recovery, you can initiate a site switch by using the **ksysmgr** command. In an unplanned outage, the KSYS subsystem analyzes the situation and notifies you about the disaster or potential disaster. Based on the information about the disaster, you can determine whether a site switch is required.

When issues occur in the replication of storage subsystem, the KSYS preserves the storage consistency information and notifies you about the issue by using the specified notification method, such as email or text message. The health of the system can be assessed by using the KSYS information, HMCs, and applicable storage vendor tools to determine whether the situation requires a true DR.

If the situation requires DR, manually initiate the recovery operation by running the **move** command by using the CLI or GUI. After the **move** operation completes, the VMs or the LPARs are restarted automatically on the corresponding target hosts.

For a planned recovery, the storage replication direction is reversed from the current active site to the earlier active site. After the site switch completes, the KSYS automatically cleans the source site from where the switch was initiated. For an unplanned recovery, the storage is not replicated back to the previously active storage. Therefore, after the problems in the previously active site are resolved, the storage must be manually resynchronized. A resynchronization is necessary for any subsequent planned **move** operation.

Also, the source site must be manually cleaned from where the switch was initiated after the HMC and hosts become operational.

If the VMs, which are moved from the active site to the backup site within the paired hosts, have multiple boot disks, the KSYS subsystem uses the stored information about the boot disk list during the discovery operation to start the VMs by using the corresponding boot disks in the backup site. Before initiating a DR operation, ensure that the boot disks in the active site are replicated to corresponding disks in the backup site, and the KSYS subsystem contains HMC 8.8.6.0 Service Pack 1 or later. This feature is supported only for POWER8 or later processor-based servers. If your production environment contains an older version of host or HMC, the KSYS subsystem cannot store boot disk information, and the VMs restart in the backup site by using the first disk in the SMS menu.

To recover the VMs, complete the following steps in the KSYS node:

1. Optional: Verify whether a disk pair and disk group exist before you initiate the recovery:

   a. To determine the relationship of the disks between the active site and the backup site, run the following command:

      ```
      ksysmgr query disk_pair
      ```

   b. To verify that the composite disk group exists in both the active site and the backup site, run the following command:

      ```
      ksysmgr query disk_group
      ```

2. Switch the site from the active site (Site1) to the backup site (Site2) for planned or unplanned recovery by running the following command:

   ```
   # ksysmgr move site -?
   ```

   The **move site** command is shown in Example 4-15.

Example 4-15 The move site -command syntax

```
ksysmgr [-f] move site
      from=<sitename>
      to=<sitename>
      [force=<true|false>]
      [lose_vios_redundancy=<yes|no>]
      [dr_type=<planned|unplanned>]
      [dr_test=<yes|no>]
      [cleanup=<yes|no>]
      [skip_shutdown=<yes|no>]
    move => mov*, mv, swi*
    site => sit*
```

Notes:

- **skip_shutdown** is valid only for unplanned moves.
- When **dr_test=yes**, do not specify the **dr_type** attribute

When the **dr_type** attribute is not specified, the **ksysmgr** command starts a planned recovery by default. The LPARs automatically restart in the backup site.

In a *planned* recovery, the KSYS automatically cleans the source site from where the switch was initiated. In an *unplanned* recovery, you must manually clean the source site after the HMC and hosts become operational. However, if you specify the **cleanup=no** attribute during a planned recovery, the VMs are not cleaned up from the source site.

For unplanned move operations, you can set the `skip_shutdown` attribute to *yes* to indicate that the source site is not operational and therefore, the KSYS subsystem does not attempt operations such as shutting down the VMs on the source site.

> **Important:** The source site must *not* be operational when you use the **`}skip_shutdown`** attribute.
>
> **Note:** If you start a move operation for a specific host group or workgroup and the move operation fails, the state of the host group or workgroup becomes `RECOVERY_VM_ONLINE`. In this case, you cannot start the move operation for the entire site unless the failed host group or workgroup is recovered completely.
>
> Recover the failed host groups and workgroups in a host group before you attempt a move operation for the entire site.
>
> The command to recover host group or workgroup is one of the following commands:
>
> - **`"ksysmgr recover host_group <hg_name>`**
> - **`"ksysmgr recover workgroup <wg_name>"`**
>
> Otherwise, you can continue to move the other host groups and workgroups to the backup site individually.

3. After an unplanned recovery, a clean-up of VMs at the source site is required. Depending on the situation, a clean-up can be done manually by using one of the following commands:

   – **`ksysmgr cleanup site Site1`**

   – **`ksysmgr cleanup host_group <hg_name>`**

   – **`ksysmgr cleanup workgroup <wg_name>`**

4. For an unplanned recovery, resynchronize the storage data from the active site to the backup site by running one of the following commands:

   – **`ksysmgr resync site active_site_name`**

   – **`ksysmgr resync host_group active_hg_name`**

   – **`ksysmgr resync workgroup active_workgroup_name`**

   If the unplanned move operation was at the site level, you must run the **`ksysmgr resync`** command at the site level. Similarly, if a VM was moved to the backup site in an unplanned move operation at the host group level or the workgroup level, run the **`ksysmgr resync`** command at the host group level or workgroup level.

4.6.2 Recovering failed VMs

After the site switch operation is complete, if some VMs were not moved successfully, you can use the **`ksysmgr recover`** command to move the failed VMs to the new active site.

When you run the **`ksysmgr recover`** command for a specific host group or a workgroup, the KSYS subsystem attempts to move all the failed VMs of that host group or workgroup from the current site to the target site.

Note: The **ksysmgr recover** command can be used only when the reverse replication of storage is successful and the VM is in the RECOVERY_VM_ONLINE state.

To check the state of a VM, use the **ksysmgr query vm** command. The state of the VM is displayed.

You can use this command only at the host group or workgroup level. The **ksysmgr recover** command is not supported at the site level.

When performing the recovery operation after the move operation of a VM fails, the KSYS subsystem provides an option to use the current or previously saved LPAR or VM profile to retry the recovery operation. The LPAR profiles of VMs are backed up regularly based on the configuration settings. Also, each time the administrator changes the configuration settings for an LPAR and runs the discovery operation, a backup of the LPAR profile file is created with the relevant timestamp at the /var/ksys/tmp location.

When you run the **ksysmgr recover** command, the KSYS subsystem attempts to recover the VMs by using the latest available LPAR profiles. If the VM recovery fails, you are prompted to choose whether you want to recover the VM to the backup site by using an LPAR profile from the backup profiles list. If you want to restart the VM with a previously backed up LPAR profile, select yes, and then the CLI prompts you to select the LPAR profile file based on the timestamp. The KSYS subsystem fetches the backup profile and uses the configuration settings that are specified in the selected LPAR profile to restart the VM. If you select no as the response for the CLI prompt, the VM restarts on the backup host with the existing configuration settings of the LPAR.

After the site switch operation completes, if the storage is successfully switched to the backup site, the failed VMs in the previously active site are not linked to the most recent disks. Therefore, the **ksysmgr recover** command moves the VM configuration without affecting the storage because the storage already was moved.

To recover the failed VMs after the move operation completes, enter the following command:

```
ksysmgr recover host_group host_group_name
```

To recover the failed VMs of specific workgroup, enter the following command:

```
ksysmgr recover workgroup workgroup_name
```

In an asymmetric host group configuration, when the recovery operation is initiated, the target host for a VM is considered according to the DRMapTable that is created in the previous failed move operation.

For example, Consider a host group that has two hosts that are named Host1 and Host2 on the home site and a host that is named Host3 on the backup site. A VM named VM1 is part of Host1. The host already was moved to the backup site. In the home site, Host1 is down and only Host2 is available. When you initiate a move operation from the backup site to the home site, the policy manager discovers Host2 as the target host for VM1. In the DRMapTable, Host2 is updated as the target host for VM1.

Now, if Host2 does not have the required capacity, the move operation for the VM1 fails.

To recover the VMs during a disaster after the failed move operation, complete the following steps:

1. Start Host1 and upgrade the Host2 resources.
2. Run the recovery operation again because the move operation failed.

During the recovery operation, VM1 is moved to Host2 in the home site instead of Host1. The recovery operation refers to the DRMapTable that is created in the previous move operation.

4.6.3 Options for moving virtual machines

The **ksysmgr** CLI provides multiple options for moving VMs between sites. The **move site** command options are shown in Example 4-16.

Example 4-16 The move site command

```
# ksysmgr move site -?
ksysmgr [-f] move site
      from=<sitename>
      to=<sitename>
      [force=<true|false>]
      [lose_vios_redundancy=<yes|no>]
      [dr_type=<planned|unplanned>]
      [dr_test=<yes|no>]
      [cleanup=<yes|no>]
      [skip_shutdown=<yes|no>]
    move => mov*, mv, swi*
    site => sit
```

Note:

- **skip_shutdown** is valid only for unplanned moves.
- When dr_test=yes, do not specify the **dr_type** attribute

Some examples of these options are shown in the following sections.

Moving the virtual machines by using the force option

In some scenarios, when you modify the KSYS configuration, the KSYS subsystem might discover the configuration change as part of its daily check. However, the resources might not be verified to check whether the VMs can be moved to the backup site.

To move the VMs to the backup site by using the **force** option, run the following command:

```
ksysmgr move from=site1 to=site2 force=true
```

This command also can be used for an unplanned move.

Moving virtual machines without cleanup

During a planned move operation, the KSYS subsystem removes the VM from the source site. If you do not want to remove the VM from the source site or clean up the VM from the source site, set the **cleanup** attribute to no.

To move a VM without cleanup on a source site, run the following command:

```
ksysmgr -f move from=site1 to=site2  cleanup=no dr_type=planned
```

Moving the virtual machines with the skip shutdown option

You can skip the shutdown of VMs because you are moving a VM from a site that is down. If you cannot shut down the VMs because the complete site is down and unreachable, set the **skip_shutdown** attribute to yes to skip the shutdown of the VMs. Use this attribute only when the VMs are not active. To move a VM with the **skip_shutdown** option, run the following command:

```
ksysmgr -f move from=site1 to=site2  skip_shutdown=yes dr_type=unplanned
```

Note: This option is supported only for an unplanned move operation.

Relocation plan for virtual machines

In an asymmetric host group configuration, the relocation plan shows the target host, where the VMs will be relocated after migration.

To determine the relocation plan of a VM, run the following command:

```
# ksysmgr report system  relocation_plan -?

ksysmgr [-v] report system
ksysmgr report system relocation_plan
vm=<vmname[,vmname2...]> | host=<hostname> | host_group=<host_group_name> |
site=<sitename>
    report => rep*
    system => sys*
```

Note: UUIDs may be used rather than names for VMs or hosts.

An example of the output of relocation plan is shown in Example 4-17.

Example 4-17 The ksysmgr relocation plan output

```
# ksysmgr report system relocation_plan vm=jrainier102
DR Relocation Plan Results:
VM jrainier102 will relocate to Host jrainier2-9105-42A_783DDB1
```

The output displays the details about the relocation plan of the VM on the target host based on the attribute values that are specified in the command. To display the relocation plan of a specific VM, use the **vm** attribute. To display the relocation plan of all VMs in a host, use the **host** attribute. Similarity, use the **host_group** attribute and the **site** attribute to know the relocation plan of all VMs in the host group and the site. However, this process might differ during migration because the KSYS subsystem dynamically obtains the target hosts based on the resource availability unless you specified the target host.

4.7 Managing and administering VMRM DR

This section provides a list of the tasks that you can perform to maintain and monitor the resources in the IBM VMRM DR for Power solution.

4.7.1 Generating the KSYS system report

After you add all the required resources to the KSYS configuration, you can generate the KSYS system report that summarizes the entire KSYS environment.

Instead of running different commands to query each resource, a consolidated report can be generated to view all the added resources in the KSYS configuration by running the following command:

```
ksysmgr report system
```

The resulting output is shown in Example 4-18.

Example 4-18 KSYS system report

```
This is the latest KSYS configurations, run discover to capture any changes

KSYS is ready to be issued a command
Ksysmgr version: 1.7.0.0
Ksys version:    1.7.0.0
Status:
Current environment:
====================
Number of sites:2
Number of storage agents:2
Number of HMCs:2
Number of hosts:4
Number of host_groups:1
Number of VIOS:8
Number of VMs:34
Total managed processors: 8.00
Total managed memory: 40960.00 MB
```

The system report also can be generated with the **verbose** option, which displays details of sites, the corresponding HMCs, hosts, host group, managed VMs, and other items.

```
# ksysmgr -v report system
```

The resulting output is shown in Example 4-19.

Example 4-19 Verbose KSYS system report

```
This is the latest KSYS configuration, run discover to capture any changes

Status: KSYS is ready to be issued a command
Ksysmgr version: 1.7.0.0
Ksys version: 1.7.0.0
Current environment:
====================

Backup Site: INDIA
```

```
    HOST: jrainier2-9105-42A_783DDB1
         HMC:
               e17vhmc17
         VIOS:
              jrainier2v1
              jrainier2v2
         Paired Host:
              jrainier1-9105-42A_783C431

         Number of Managed VMs:  0
         Configurable Processors: 48.00
         Configurable Memory: 524288.00 MB

    Storage Agent:
              sw6_local

    Total configurable Processors: 48.000000
    Total configurable Memory: 524288.000000 MB

Home Site:  US

    Host_Group: Default_HG
         Active Hosts: jrainier2-9105-42A_783DDB1
         Backup Hosts: jrainier1-9105-42A_783C431

    HOST: jrainier1-9105-42A_783C431
         HMC:
               e17vhmc2
         VIOS:
              jrainier1v1
              jrainier1v2
         Paired Host:
              jrainier2-9105-42A_783DDB1

         Number of Managed VMs:  3
         Configurable Processors: 48.00
         Configurable Memory: 524288.00 MB

    Storage Agent:
              sw3_remote

    Total configurable Processors: 48.000000
    Total configurable Memory: 524288.000000 MB
```

4.7.2 Configuring the flexible capacity policies

By using the flexible capacity policies, you can configure the memory and processor resources so that you can move the VMs from the source host to the target host even when the target host does not have the same quantity of memory and processor resources as the source host. You can set the flexible capacity policies for the backup site.

You can use the flexible capacity option to start VMs on the backup site with a different capacity as compared to the active site. The active site resources are used as a reference to calculate the percentage of resources that must be assigned during the recovery of VMs on the backup site.

You can set the flexible capacity policies at the host group or site level, and they can be used in the following cases:

- To perform the DR operations with a different amount of resources at the backup site.
- To test the DR operation by using the failover rehearsal function with either fewer resources or more resources at the backup site.
- To pair hosts across the active site and the backup site even when the available resources for both hosts differ.

When you create an LPAR in the HMC, a profile is created for the LPAR that includes the resource limits such as minimum, desired, and maximum memory and processors that you want to allocate for that LPAR. If flexible capacity policies are not specified, by default the desired value of resources are used by KSYS.

The allocation of memory and CPU capacity for a VM must be more than or equal to the memory and CPU capacity of the VM that is allocated at the backup site.

Figure 4-5 shows the various flexible capacity policies.

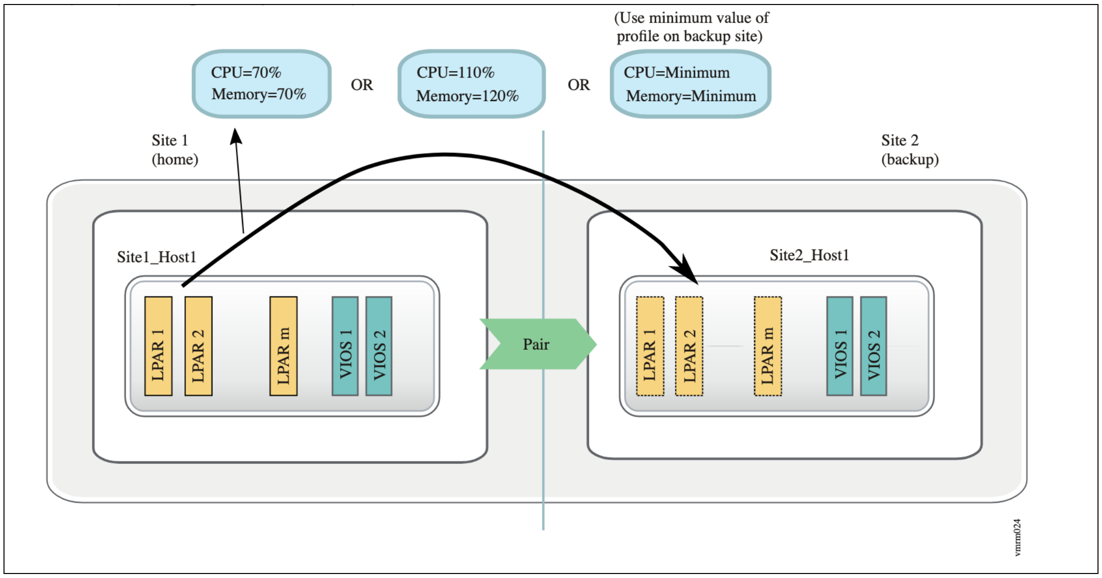


Figure 4-5 Flex capacity management

Percentage of the existing capacity value

This policy specifies the percentage of resources that must be allocated to the VM after recovery on the backup site as compared to the active site.

The following example describes the percentage-based resource allocation:

If a VM is running on the active site with 10 GB of memory and two dedicated processors, and if you specify the flexible capacity policy with 50% CPU resources and 70% memory resources, then after the recovery of that VM on the backup site, the VM will be running with one processor and 7 GB of memory.

Memory is calculated and rounded off to the nearest multiples of memory region size on the target host. If dedicated processors are allocated to a VM, the calculated values are rounded off to the closest decimal. Similarly, we can configure the flexible capacity values at host group level and site level. If the flexible capacity policy is configured at the host group level, the flexible capacity policy applies to all the managed VMs of the host group. Likewise, if the flexible capacity policy is configured at the site level, the flexible capacity policy applies to all VMs of all host groups at the site level. The percentage value that you specify in this policy must always be greater than 1.

Minimum value

This value sets the resource value of the backup site LPAR (when the LPAR is started on the backup site during the recovery operation) to the minimum value that is defined in the LPAR profile on the active site.

Current desired

This value sets the resource value of backup site LPAR (when the LPAR is started on the backup site during the recovery operation) to the desired value that is defined in the LPAR profile on the active site.

None

This value resets the existing value. When you set the value to `none`, VM capacity management does not use flexible capacity management. CPU and memory resources across the active site and backup site match the values that are defined in the LPAR profile.

Using the reduced capacity function might result in a decrease of the performance of the VMs at the backup site, but the VMs can be restarted in the target host with the reduced capacity. You can use the reduced capacity function during planned outages, where the VMs are temporarily moved to the target host and then moved back to the source host after a system maintenance or upgrade operation completes. When the VMs are moved back to the home site, the original capacity settings of the VM are retrieved and the VMs are run with the initial performance.

If you do not want the HMC to check and compare the resource capacity between the source host and the target host during the verify operation, you can set the **`skip_resource_check`** parameter to `yes`.

If you do not want the VMs to start automatically after they are moved to the target host, you can set the **`skip_power_on`** parameter to `no`.

Host group level configuration

To configure reduced capacity settings for all the hosts in a host group, enter the following command in the KSYS LPAR:

```
ksysmgr modify host_group hgname[,hgname2,...]
      [memory_capacity=<(1-1000) | minimum | current_desired  | none>
        priority=<low | medium | high>]
      [cpu_capacity=<(1-1000) | minimum | current_desired | none>
        priority=<low | medium | high>]
      [skip_power_on=yes|no]
```

For example:

```
ksysmgr modify host_group Site1_HG1,Site1_HG2 options memory_capacity=50
cpu_capacity=50 skip_power_on=yes priority=medium
```

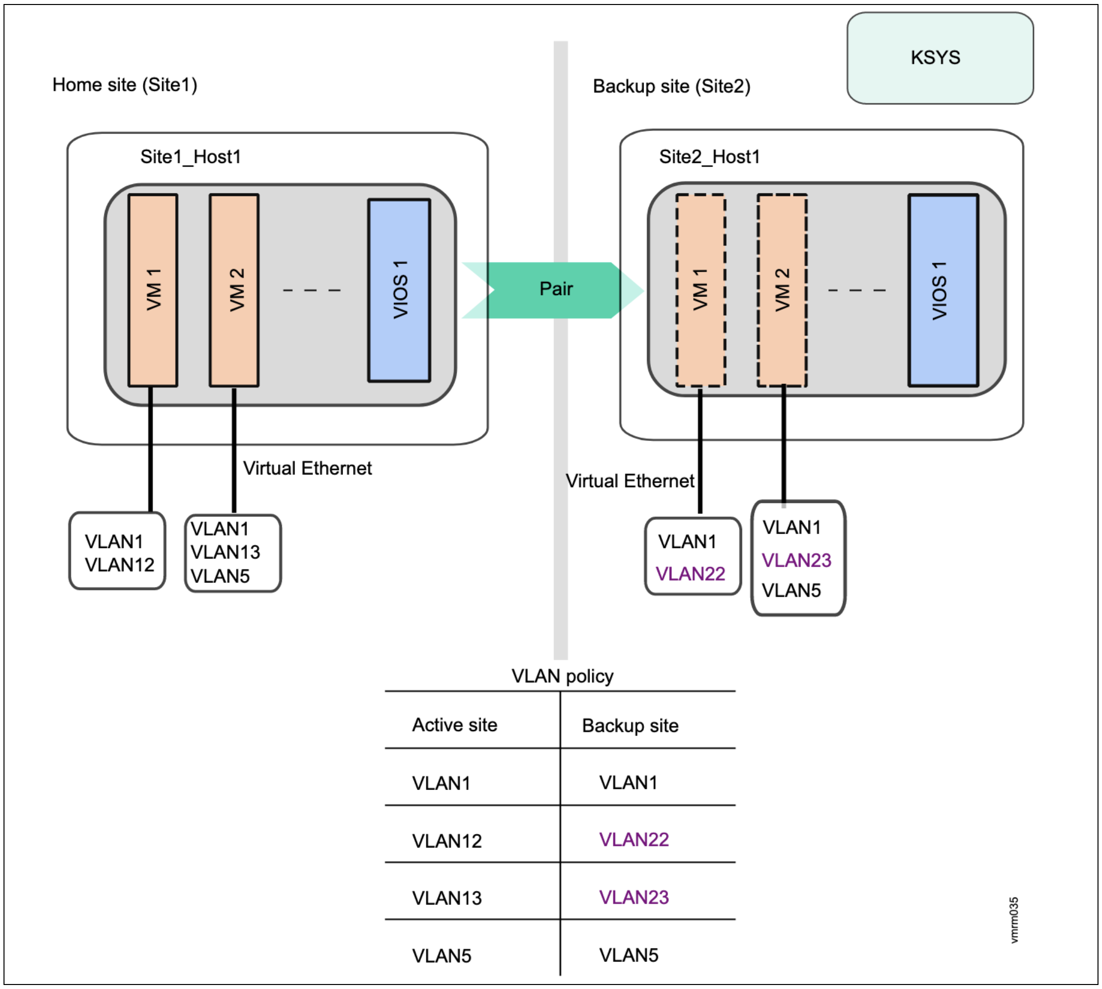
Flexible capacity setting also can be use at the system level.

4.7.3 Configuring the network mapping policy

A VLAN is created by assigning artificial LAN identifiers (VLAN IDs) to the datagrams that are exchanged through the physical network. Hosts that are on the same VLAN represent a subset of the hosts that are on the physical network. Hosts that belong to the same subnet can communicate without any routing device. The subnets are separated when the hosts in a subnet have different VLAN IDs.

When a virtual Ethernet adapter is created in an HMC, a virtual Ethernet switch port is configured simultaneously. The VMs within a host, which must communicate with other VMs for workload operations, are configured with the same VLAN IDs. Similarly, some VMs in your host environment might be isolated from other VMs through a private network and might have different VLAN IDs.

For example, consider a host in the active site that contains two VMs that use the following VLAN IDs: VLAN1, VLAN12, VLAN13, and VLAN5. If you want these VMs to start in the backup site with VLAN IDs VLAN1, VLAN22, VLAN23, and VLAN5, you can set a VLAN policy that modifies the VLAN ID from VLAN12 to VLAN22, and from VLAN13 to VLAN23 when VMs are moved from the active site to the backup site. Therefore, when you move the VMs across sites, the VMs are restarted in the target site with the assigned VLAN IDs, as shown in Figure 4-6 on page 149.



VLAN policy

Active site	Backup site
VLAN1	VLAN1
VLAN12	VLAN22
VLAN13	VLAN23
VLAN5	VLAN5

Figure 4-6 Network mapping configuration

Network mapping policy for an asymmetric host group

To enable the network mapping policy in an asymmetric host group, you must set a policy at the host group level or at a higher level, such as site level or system level. All the hosts in the respective site must have a similar network mapping configuration.

For example, HG1 is an asymmetric host group that has Host1 and Host2 in the home site and Host3, Host4, and Host5 in the backup site. Ensure that all VLAN or vSwitch values set by **ksysmgr** are available on the hosts of the home site, that is, Host1 and Host2 in this example. Similarly, all VLAN or vSwitch values that are set by **ksysmgr** must be available on the hosts of the backup site, which are Host3, Host4 and Host5 in this example.

System-level network mapping policy

To enable the network mapping policy and create network mapping policy for all hosts and host groups across the active site and the backup site, enter the following command in the KSYS LPAR:

```
ksysmgr modify system network_mapping=<enable | disable>
network=<vlanmap | vswitchmap> sites=<siteA,siteB>
       siteA=<#,[#,...]> siteB=<#,[#,...]>]
```

For example:

```
ksysmgr modify system network_mapping=enable network=vlanmap sites=siteA,siteB
siteA=1,12,13,5 siteB=1,22,23,5
```

Site-level network mapping policy

To enable the network mapping policy and create network mapping policy for all hosts and host groups in a specific site, enter the following command in the KSYS LPAR:

```
ksysmgr modify site <sitename[,sitename2,...]> | file=<filepath> [network=<vlanmap
| vswitchmap> backupsite=siteB sitename=<#[,#,...] || all> siteB=<#[,#,...] ||
all> [dr_test=<yes|no>]
```

For example:

```
ksysmgr modify site site1 network=vlanmap backupsite=site2 site1=1,2,3 site2=4,5,6
```

Host group-level network mapping policy

To create a mapping policy of VLAN ID or virtual switches for all the hosts in a host group across sites, enter the following command in the KSYS LPAR:

```
ksysmgr modify host_group <name> options
      network=<vlanmap | vswitchmap>  sites=<siteA,siteB>
       siteA=<#,[#,...]> siteB=<#,[#,...]>
```

Host-level network mapping policy

To create a VLAN ID mapping policy for all VMs in a host across sites, enter the following command in the KSYS LPAR:

```
ksysmgr modify host <hostname[,hostname2,...]> | file=<filepath>
     network=<vlanmap | vswitchmap>  sites=<siteA,siteB>
       siteA=<#,[#,...]> siteB=<#,[#,...]>
```

A warning message is displayed when LAN ID or vSwitch values are not the same as the discovered VLAN ID or vSwitch values. However, the command sets the VLAN ID or vSwitch values with the values that are provided in the command after displaying the warning message.

4.7.4 Modifying the KSYS configuration

Growing business requirements might require changes in your current configuration, for example, adding a specific VM, adding an entire host to your environment, adding an HMC, or adding a disk in the VM. After the VMRM DR solution is implemented, the KSYS subsystem continues to monitor any changes in the KSYS configuration. To modify the current configuration, use the **ksysmgr discover** command to discover and validate the changes in the KSYS configuration immediately.

Unmanaging a disk

A non-replicated disk that is associated with a VM can be excluded during the DR operation. The excluded disk is referred to as an *unmanaged disk*, which can be from a source site only, and it will not be considered for DR management. The excluded or unmanaged disks are not available on the DR site during the DR operations. When a disk that is in the local host is unmanaged and the disk is replicated, the replicated disk of the unmanaged disk is ignored at the target host during the verification operation and move operation. Also, an unmanaged disk will not be added to any CG. Only a disk in the home site can be unmanaged.

Prerequisites

Consider the following additional requirements when using the unmanage disk feature:

- Ensure that the unmanaged disk pair's secondary disk is not accessible from the backup site, and also ensure that the primary disk is accessible from the home site. The KSYS subsystem does not explicitly verify whether the primary disk can be accessed from the home site.
- Ensure that the vFC of a VM contains both managed and unmanaged disks. The DR failover rehearsal operation is not supported if the vFC contains only unmanaged disks.
- Specify the worldwide name (WWN) of a disk when unmanaging a disk. You can get the WWN of a disk by running the following command:

  ```
  lsmpio -q -l hdisk1
  ```

Commands

- To unmanage disk, run the following command:

  ```
  ksysmgr unmanage disk diskid=<diskid1[,...]>
  ```

- To manage a disk, run the following command:

  ```
  ksysmgr manage disk diskid=<diskid1[,...]>
  ```

Note: A discovery operation must run after you unmanage or manage disks.

Limitations

- The DR failover rehearsal operation from the backup site to the home site is not supported if the operation involves unmanaged disks. The DR failover rehearsal operation is supported only from the home site to the backup site with unmanaged disks.
- VMRM DR does not support sharing a managed disk or unmanaged disk between VMs of two different workgroups or host groups.
- When unmanaging a disk, which is replicated at the KSYS subsystem level, use the disk identifier that is assigned to the disk in the home site.
- The unmanage disk feature is not supported if multiple DS8000 series storage agents are configured in a site.

Managing and unmanaging virtual machines

If you want to exclude some VMs during a DR operation, run the following command for each VM:

```
ksysmgr unmanage vm
      name=<vmname> host=<hostname> | uuid=<lparuuid> | ALL host=<hostname> | ALL
host_group=<host_group_name>
```

If you want to unmanage all VMs in a host, run the following command:

```
ksysmgr unmanage ALL host=xyz
```

If you want to unmanage all VMs in a host group. run the following command:

```
ksysmgr unmanage ALL host_group=HG1
```

This command unmanages all VMs in all hosts in the host group HG1.

If you want to include some VMs during a DR operation, run the following command for each VM:

```
ksysmgr unmanage vm
      name=<vmname> host=<hostname> | uuid=<lparuuid> | ALL host=<hostname> | ALL
host_group=<host_group_name>
```

Modifying the attributes of the added resources

In addition to adding new resources, you can modify the attributes of an existing resource in the KSYS configuration:

- To update the HMC login credentials or IP address, use the following syntax:

  ```
  ksysmgr modify hmc hmcname
  [login=new_username]
  [password=new_password]
  [hostname|ip=new_hostname|new_ip]
  ```

- To change the storage agent details, use the following syntax:

  ```
  ksysmgr modify storage_agent <storage_agent_name>
  [storage_agent_name=<new_storage_agent_name>]
  [hostname=<hostname[,hostname2,hostname3]>]
  [ip=<ip[,ip2,ip3]>]
  [login=<username>]
  [password=<password>]
  [drinstance=<drinstance_number>]
  modify => mod*, ch*, set
  storage_agent => storage*, sta
  ```

- To update the contact details for the KSYS notification, use the following syntax:

  – **ksysmgr modify notify oldcontact=old_username newcontact=new_username**

  – **ksysmgr modify notify oldcontact=old_email_address**

  newcontact=new_email_address

- To update the priority of VMs, use the following syntax:

  ```
  ksysmgr modify VM name1[,name2,name3,...] | file=filepath
  [uuid=uuid_value]
  [host=hostname]
  [priority=low|medium|high]
  ```

- To update the target host of a VM for the DR operation for a VM that belongs to an asymmetric host group, run the following command:

  ```
  ksysmgr modify vm <vm_name> DrTargetHost=<hostname|none>]
  ```

If **DrTargetHost** is set to none, on the next discovery, KSYS selects the most suitable target host based on the capacity and availability of resources.

Removing resources from the KSYS configuration

If a specific resource does not need to be covered when you use the VMRM DR solution, you can remove the resource and the associated resources from the KSYS configuration.

Removing virtual machines from a workgroup

When you remove a host from the KSYS configuration, all the VMs are removed. Therefore, if you want to remove a specific VM, instead of removing the host from the KSYS configuration, you must exclude the VM from the KSYS configuration so that the VM is not moved to the backup site during a DR operation. You can exclude a specific VM by running the **`ksysmgr unmanage vm_name`** command.

If the VM is defined in a workgroup, another option to remove that VM from management is to remove it from the workgroup by running the following command:

```
ksysmgr modify workgroup workgroup_name policy=delete vm=vmname
```

The KSYS subsystem automatically unmanages a VM after the VM is removed from a workgroup.

Removing a workgroup

Before removing a workgroup, you must first remove the associated VMs from the workgroup by using the **`ksysmgr modify wg`** command that is shown in “Removing virtual machines from a workgroup” on page 153.

To remove a workgroup, run the following command:

```
ksysmgr delete workgroup workgroup_name
```

Removing a host

To remove a host, you must first remove the host from the host group, and then break the associated host pair by running the following command:

```
ksysmgr modify host_group hg_name remove hosts=host1
```

After the host pair is broken, run the following command to remove the hosts in both the active site and the backup site:

```
ksysmgr delete host hostname
```

All the VMs that are running on the host are removed from the KSYS configuration. Also, remove the host in the opposite site that was paired to the removed host. If you add or remove hosts from a host group, you must run a discovery operation to manage or *unmanage* all the VMs from recovery management. The modified host group displays the correct list of managed VMs only after a discovery operation.

After an LPM operation on a VM or an HA restart of a VM, you must initiate the explicit discovery operation to update the disk mapping for a DR operation. Without an explicit discovery operation, if you remove a host from host group, the KSYS subsystem removes all disks from the source host.

Removing a host group

To remove a host group, first remove all the hosts from the host group (see “Removing a host” on page 153), and then delete the host group by running the following command:

```
ksysmgr delete host_group hg_name
```

Removing an HMC

If an HMC that is included in the KSYS configuration is not managing any hosts in the KSYS configuration, you can remove the HMC from the KSYS configuration by using the following syntax:

```
ksysmgr delete hmc hmcname
```

Removing a storage agent

If you remove an entire storage array from a site, you must remove the host group, and then remove the storage agent that is associated with that storage array. Remove the CG of the storage agent before deleting the storage agent. To delete a storage agent, run the following command:

```
ksysmgr delete storage_agent storage_agent_name
```

Managing the KSYS notifications

After you add the contact details to the KSYS configuration for the first time, you can modify the contact details later depending on the changing requirements:

- To modify the contact information, run the following commands:
  - **ksysmgr modify notify oldcontact=old_username newcontact=new_username**
  - **ksysmgr modify notify oldcontact=old_email_address newcontact=new_email_address**
- To delete all the contact information for a specific user, run the following command:

  ```
  ksysmgr delete notify user=username
  ```

- To query all the registered contact details, run the following command:

  ```
  # ksysmgr query notify -?
  ksysmgr query notify [ contact | script ]
        [ user=<username> | contact=<contact> ]
        [ script=<full path script> ]
      query => q*, ls, get, sh*
      notify => rn, remote_not*, noti*
  ```

The output of the query looks like Example 4-20.

Example 4-20 The ksysmgr query notify output

```
User:            abc
Contact:       abc@ibm.com

User:            xyz
Contact:       xyz@ibm.com
```

4.7.5 Running scripts for specific events

You can create scripts for specific events. When an event occurs, you can enable the script to run as part of the event. By using scripts, you are notified about a specific event, and you can collect details about the event, take corrective actions, and handle the processes after the event completion. For more information about scripts, see the event script samples that are in the `/opt/IBM/ksys/samples/event_handler/event_script_template` file on the ksys node. Specify the full path of the script to add a script for notification configuration. When the event occurs, the KSYS subsystem validates the existence and the authorization of the scripts.

- To add a script, run the following command:

  ```
  ksysmgr add notify script=script_file_path_name event=event_name
  ```

  For example:

  ```
  ksysmgr add notify script=/tmp/script.sh event=HMC_UNREACHABLE
  ```

- To modify a script, run the following command:

  ```
  ksysmgr modify notify oldscript=old_script_file_path_name
  newscript=new_script_file_path_name
  ```

  For example:

  ```
  ksysmgr modify notify oldscript=/tmp/script.sh newscript=/tmp/newscript.sh
  ```

- To remove a script, run the following command:

  ```
  ksysmgr delete notify script=script_file_path_name
  ```

- To query a script, run the following command:

  ```
  ksysmgr query notify script
  ```

Notification message

Even if you set the KSYS configuration to not receive any event notifications, the messages are logged in the `/var/ksys/events.log` notification log file. Example 4-21 shows an example of the notification message.

Example 4-21 Notification example

```
HMC_DOWN event has occurred. Details are as follows:
     Event:              HMC_DOWN
     Type:               Critical Error Event
     Time:               Tue Jul 19 00:35:32 CDT 2016
     Entity Affected:    HMC
     Resource Affected:  vmhmc1
     Description:        0000-132 Error - HMC x.x.x.x is down.
     Suggestion:         Please try to restart.
```

Managing the system attributes

After you synchronize the KSYS cluster by running the **`ksysmgr sync ksyscluster`** command, the KSYS subsystem sets up the default, system-wide persistent attributes. The KSYS subsystem uses these system-wide persistent attributes for activities such as automatic rediscovery of the resources, notification of critical events, and removal of duplicate notifications.

By default, the KSYS subsystem sets up the following system attributes:

- **auto_discovery_time**

  Specifies the time for daily discovery at which the KSYS subsystem rediscovers the environment automatically for any new or modified resources. By default, the value of this attribute is 00:00, which means the KSYS subsystem discovers the resources and updates its database about the VMs every 24 hours at 00:00.

  The HMC and VIOS are involved in the rediscovery process to update information about the VMs. Therefore, if your environment is large (for example, hundreds of LPARs in the data center), you might want to set the time to a time with a minimal load on the HMC, VIOS, and the underlying I/O subsystems. Any configuration changes to the hosts, VMs, disks, and any other entities (for example, adding new disks to a VM) are captured when the rediscovery occurs. This attribute also specifies the time during which any changes in the configuration setting can be lost if a disaster occurs before the rediscovery.

- **lose_vios_redundancy**

  Specifies starting the VMs at another site without a dual-VIOS setup in the target host. By default, this attribute is set to no, which means that the dual-VIOS setup is maintained during the DR operation. If your currently active site, which has a dual-VIOS configuration, fails, and one of the VIOS in the target host of the backup site is not functioning, you might want to recover the VMs with only one VIOS on the backup site and continue the workloads that are running in the active site. In this case, you can set this attribute to yes. However, if the VMs start with a single-VIOS configuration on the backup site and you want to move the VMs back to the previous site that has a dual-VIOS configuration, you must manually add the second VIOS to the configuration. For more information, see Configuring VIOS partitions for a dual setup.

- **notification_level**

  Enables or disables the notification for different types of events. This parameter supports the following values:

  - low (default)

    Only critical error events are sent.

  - medium

    Critical and warning error events are sent.

  - high

    All events, which include informational events, are sent.

  - disable

    None of the events are sent.

Note: The KSYS subsystem sends site event notifications without considering the value of the **notification_level** system attribute. For more information, see 4.7.4, “Modifying the KSYS configuration” on page 150.

- **dup_event_processing**

  Reduces duplicate event notifications. The email and script notifications that are related to the duplicate events are also disabled. This parameter can have the following values:

  – `yes` (default)

    Sends notices about only those events that have not repeated in the last 24 hours.

  – `no`

    Sends notices about all the messages.

- **replication_type**

  Specifies the storage replication mode across the sites. This parameter can have the following values:

  – `async`

    Specifies the asynchronous replication mode in which data is transferred across sites in predefined timed cycles or in delta sets.

  – `sync`

    Specifies the synchronous replication mode in which the storage subsystem acknowledges to the host that it has received and checked the data.

  – `shared`

    Specifies a shared mode in which a single storage system is connected to multiple sites.

  Specify the source and the target sites that are associated with the storage replication operation.

- **network_mapping**

  Enables or disables the network mapping policies for all hosts and host groups across the active site and the backup site.

- **network**

  Creates network mapping policy for all hosts and host groups. This attribute can be specified only when the **network_mapping** attribute is set to `enable`. Either a VLAN mapping policy or a virtual switch mapping policy can be created.

- Quick discovery

  You can enable or disable the quick discovery property.

- Quick discover interval

  You can set time interval in minutes for a quick discovery operation.

- Customer script timeout

  You can configure the timeout duration for a custom script. If the custom script cannot complete the run within the configured timeout duration, the KSYS subsystem terminates the run of the custom script and proceeds with the next execution.

- Ping

  You can enable or disable the **ping** attribute at the system level through this tunable. The KSYS subsystem performs a scheduled health checkup on the HMC and storage systems. The KSYS subsystem informs you about the health state of the HMC and storage systems through the **ping** attribute. If the **ping** attribute is disabled, the KSYS subsystem does not provide the health state notification about the HMC and storage systems. Also, when the **ping** attribute is disabled, the `HMC_UNREACHABLE` event and the `STG_UNREACHABLE` event are not triggered. By default, the **ping** attribute is enabled.

- **deep_discovery**

  The **deep_discovery** attribute can be enabled or disabled at the system level through this tunable. The deep discovery process is similar to the discovery operation, except that the deep discovery process runs automatically every 24 hours by default. During the deep discovery process, the KSYS subsystem collects all information that is collected during the quick discovery process and information about the storage systems. You can update the deep discovery process period by using the **auto_discovery_time** attribute. By default, the **deep_discovery** attribute is enabled. When disabled, the KSYS subsystem does not discover the environment automatically for any new or modified resources.

- **ksys_lang**

  To get the output of **ksysmgr** and VMRM in other languages than English, you can set the **ksys_lang** attribute to set the support language. By default, **ksys_lang** is set to `en_US`.

- **trace_file_size**

  By default, the trace file size will be 50 MB, but it is a best practice to change it to 25 MB if HA of the KSYS node is configured.

Command syntax to modify the system attribute

The syntax of **ksysmgr modify system** is shown in Example 4-22.

Example 4-22 The modify system command

```
# ksysmgr modify system -?

ksysmgr modify system
      [auto_discovery_time=<hh:mm>]
        hh - hour:   00 to 23
        mm - minute: 00 to 59
      [quick_discovery_interval=<mm>]
        mm - minute: 5 to 480
      [custom_script_timeout=<sec>]
        sec - seconds: Any positive integer
      [quick_discovery=<enable | disable>]
      [deep_discovery=<enable | disable>]
      [trace_file_size=<MB>]
        MB - Megabyte: Between 1 and 50 for single node KSYS cluster
                       Between 1 and 25 for Multiple node KSYS cluster
      [lose_vios_redundancy=<yes | no>]
      [notification_level=<low | medium | high | disable>]
      [dup_event_processing=<yes | no>]
      [replication_type=<async | sync | shared>   sites=<A,B>]
      [network_mapping=<enable | disable>]
      [vm_auto_discovery=<enable | disable>]
      [ping=<enable | disable>]
      [optimise_put_storage=<enable | disable>]
      [min_redundancy_paths=< no.of paths - for enable | 0 - for disable>]
      [hmc_ping_timer=<(10-30) time in seconds>]
      [sa_ping_timer=<(10-30) time in seconds>]
      [cleanup_files_interval=<disable | (1-30) days>]
      [memory_capacity=<(1-1000) | minimum | current_desired | none | default>
        priority=<low | medium | high>]
      [cpu_capacity=<(1-1000) | minimum | current_desired | none | default>
        priority=<low | medium | high>]
      [network=<vlanmap | vswitchmap>  sites=<siteA,siteB>
      siteA=<#[,#,...] || all> siteB=<#[,#,...] || all> [dr_test=<yes|no>]
```

```
    [policy=delete]]
    [ksys_lang=<language>]
    [connection_timeout=<default | (1-600) time in seconds>]
  modify => mod*, ch*, set
  system => sys*
```

The following restrictions apply when using the **`modify system`** option of the **`ksysmgr`** command:

- Do not change **`quick_discovery_interval`** to a value less than 60 minutes.
- If the **`custom_script_timeout`** value is set to `0`, no timeout is set, and the system waits indefinitely for the script to run.
- **`trace_file_size`** limit check errors can be overridden with the **`-f`** flag for only a single-node KSYS cluster.
- **`trace_file_size`** can be set to maximum of 25 MB in a multi-node KSYS cluster.
- Supported locales for **`ksys_lang`** are `DE_DE`, `FR_FR`, `JA_JP`, `PT_BR`, `ZH_TW`, `ES_ES`, `IT_IT`, `ZH_CN`, and `en_US`.
- The default language is `en_US`.

Managing a shared storage configuration

The VMRM DR solution manages DR across two sites based on storage replication across the sites. However, the VMRM DR solution also supports a mode of deployment in which disks are shared across sites. In this case, the KSYS subsystem does not manage any storage subsystems. The disks can be shared across sites that are separated by short distances (0 - 100 km). The storage technologies (for example, IBM HyperSwap®) perform *synchronous* mirroring across sites and abstract the mirroring from the hosts. These storage technologies provide a shared disk type of deployment for hosts across sites.

Restrictions:

- Because the storage is shared, the NPIV and other similar ports are visible to VIOS on both sites. It might cause problems that are related to SAN login and disk validations. Therefore, HMC and VIOS-related checks are not performed in the shared deployment mode, so the administrator must set up the sites while considering storage, network, and so on, and must maintain the configuration settings. Any misconfiguration might result in errors during a DR.
- The DR failover rehearsal operation is not supported for shared storage deployments.

Shared storage without replication management

When the storage device is a single storage system that is split or separated by distance in two different sites as stretched systems, the storage replication management is hidden from the hosts and VIOS partitions. The storage subsystem is displayed as a single, shared storage across the two sites. In this case, the storage recovery and replication are performed entirely by the storage platform, so the storage agents in the KSYS subsystem interact with the storage devices. Therefore, there is no need to consider the disk pair and disk group mappings for the shared storage configuration.

When moving VMs from the active site to the backup site, the KSYS subsystem considers the storage subsystem as unmirrored shared storage and starts the VMs on the backup site. If the DR operation is unplanned, the storage subsystem performs the entire storage recovery.

Note:

- The VMRM DR solution supports this type of shared storage only for sites that are spanned across short distances. Also, the storage subsystem must provide shared storage characteristics.
- The VMRM DR solution does not support heterogeneous storage systems for this type of shared mode configuration. Deploy the same type of storage systems across the sites in your environment.

Figure 4-7 shows an example of a shared storage configuration that uses a HyperSwap stretched, cluster-based technology.

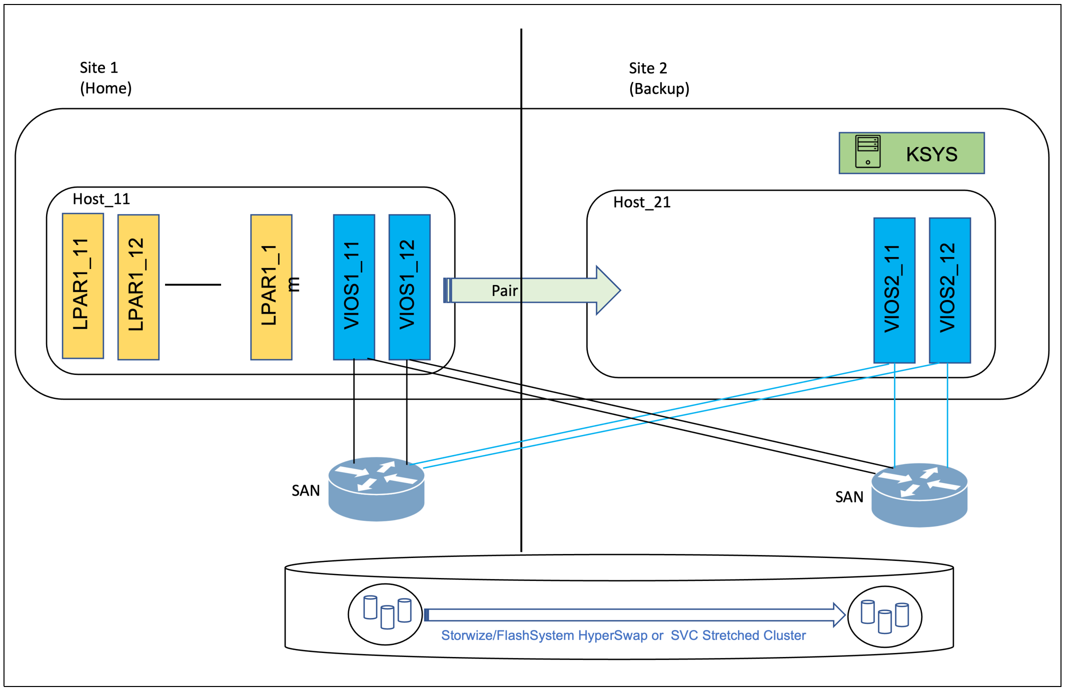


Figure 4-7 Shared storage without replication configuration

To set the shared mode replication, run the following command:

```
ksysmgr modify system replication_type=shared sites=<src_sitename>,
<backup_sitename>
```

Managing Capacity on Demand resources

When using capacity management solutions, you can use the VMRM DR solution to manage resource allocations during a DR failover operation. To manage resource allocations in a DR environment, the VMRM DR solution provides a resource pool provisioning (RPP) command that is called **ksysrppmgr**. The **ksysrppmgr** command optimizes available resources on the managed hosts. This command also minimizes your resource costs by optimizing the local consumption of pool resources. Before running the **ksysrppmgr** command to allocate resources to a managed host, run the **ksysrppmgr** command in check mode to simulate the execution and analyze the results.

The VMRM DR solution can manage resource allocation for the following capacity management solutions:

- Power Enterprise Pool
- Elastic (On/Off) Capacity-on-Demand

> **Note:** To use the **ksysrppmgr** command, you must authenticate to the HMCs by using the **hmcauth** command. The **ksysrppmgr** command communicates to the HMC through the REST APIs. Therefore, the APIs must be activated on the existing HMCs. At least one HMC is necessary to run resource requests. The **hmcauth** command is installed as part of the `bos.sysmgt.hmc` file set.

VMRM DR and Power Enterprise Pool

The Power Enterprise Pool feature provides flexibility to hosts that operate together as a pool of resources. Mobile activations can be assigned to any host in a predefined pool and the resources can be reassigned within a pool. When using Power Enterprise Pool for capacity management, review the following scenarios to determine how to manage the resource allocations by using the VMRM DR solution.

- Scenario 1: Using enterprise pools across sites

  In this scenario, the enterprise pool is shared across sites, as shown in Figure 4-8.

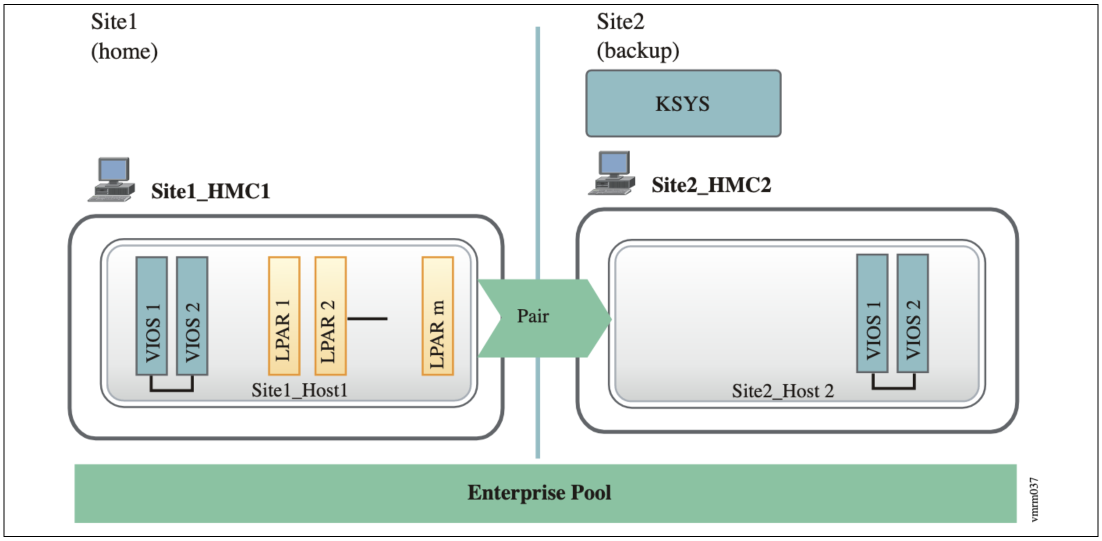


Figure 4-8 Power Enterprise Pool usage across the sites

When the active site fails, complete the following steps before you initiate the site-switch operation:

a. In the KSYS node, authenticate all the HMCs by running the **hmcauth** command:

```
hmcauth -u hmcuser -p password -a HMC_1_1
hmcauth -u hmcuser -p password -a HMC_2_1
```

b. Check whether the required number of processors and memory are available in the backup host that does not use Elastic (On/Off) Capacity on Demand (CoD) by running the following command:

```
ksysrppmgr -o check -h :HMC_1_1:hmcuser -h :HMC_2_1:hmcuser -m
Host_2_1:set:n:<memory_amount>:<no_of_processors> -r
```

If the return code of the command is `0`, all the requests can be fulfilled. If the return code is `1`, at least one request failed.

c. If the resource requests are not fulfilled, release the resources that are used by the VMs of Site_1, and return the resources to the enterprise pool either by using the HMC or by running the following command in the KSYS node:

```
ksysrppmgr -o execute -h :HMC_1_1:hmcuser -m Host_1_1:set:n:0:0
```

For more information about the steps to release or allocate resources by using the HMC, see Using Power Enterprise Pools.

d. Allocate the required amount of resources to the hosts in the Site_2 site by using the HMC or by running the following command in the KSYS node:

```
ksysrppmgr -o execute -h :HMC_2_1:hmcuser -m
Host_2_1:set:n:<memory_amount>:<no_of_processors> -r -v
```

The target host on the backup site now contains all the required resources to host the recovered VMs.

e. Verify whether the VMs can be moved to the backup site by running the following command:

```
ksysmgr verify site Site_2
```

> **Note:** If the backup site does not have sufficient processors or memory, the verify operation fails with a warning message. You can use the **force** (**-f**) option to move the VMs to the backup site with the existing configuration.

f. Initiate the DR by switching the site from Site_1 to Site_2 by running the following command in the KSYS node:

```
ksysmgr move from=Site_1 to=Site_2 dr_type=planned
```

- Scenario 2: Using enterprise pools within the backup site

  In this scenario, the enterprise pools are shared across hosts within the backup site. In the example shown in Figure 4-9, Host_1_1 in the active site is paired to Host_2_1 in the backup site. Host_2_2 is another host in the backup site that is running low-priority VMs. When the active site fails, you can allocate some resources from Host_2_2 to Host_2_1 to run the recovered VMs.

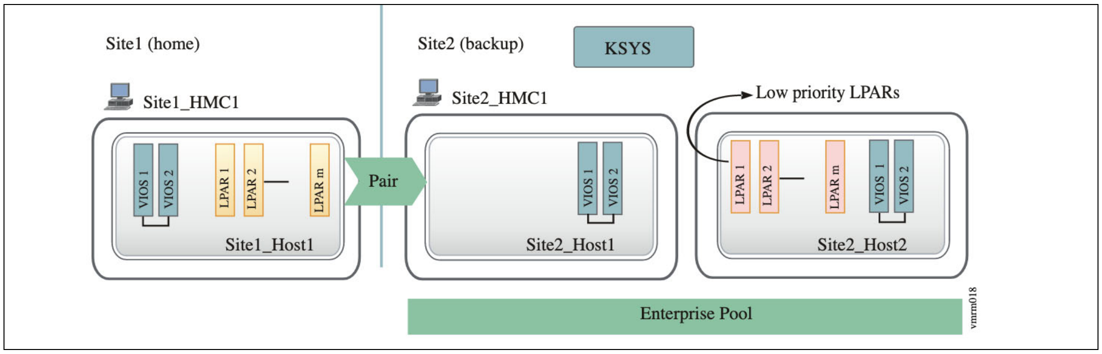


Figure 4-9 Power Enterprise Pool usage within the backup site

Before initiating a site-switch operation, complete the following steps:

a. In the KSYS node, authenticate all the HMCs by running the **hmcauth** command:

```
hmcauth -u hmcuser -p password -a HMC_1_1
hmcauth -u hmcuser -p password -a HMC_2_1
```

b. Check whether the required number of processors and memory are available in the backup host that does not use Elastic (On/Off) CoD by using the HMC or by running the following command in the KSYS node:

```
ksysrppmgr -o check -h :HMC_1_1:hmcuser -h :HMC_2_1:hmcuser -m
Host_2_1:set:n:<memory_amount>:<no_of_processors> -r -v
```

If the return code of the command is `0`, all the requests can be fulfilled. If the return code is `1`, at least one request failed. For more information about the steps to release or allocate resources by using the HMC, see Using Power Enterprise Pools.

c. If the output indicates that the request cannot be fulfilled, reduce the resources that are allocated to Host_2_2, which runs low-priority VMs, and return the resources to the enterprise pool either by using HMC or by running the following command in the KSYS node:

```
ksysrppmgr -o execute -h :HMC_2_1:hmcuser -m
Host_2_2:set:n:<memory_amount>:<no_of_processors>
```

d. Allocate the resources to the Host_2_1 host by running the following command:

```
ksysrppmgr -o execute -h :HMC_2_1:hmcuser -m
Host_2_1:set:n:<memory_amount>:<no_of_processors>
```

e. Verify whether the VMs can be moved to the backup site by running the following command:

```
ksysmgr verify site Site_2
```

> **Note:** If the backup site does not have sufficient processors and memory, the verify operation fails with a warning message. You can use the **force** (**-f**) option to move the VMs to the backup site with the existing configuration.

f. Initiate the DR by running the following command:

```
ksysmgr move from=Site_1 to=Site_2 dr_type=planned
```

VMRM DR and Elastic (On/Off) CoD

Elastic Capacity-on-Demand (formally known as On/Off CoD) provides a short-term CPU and memory activation capability for fluctuating peak processing requirements. If the resource requirements are not met even after you allocate the maximum number of resources from the enterprise pool, you can enable Elastic (On/Off) CoD to activate temporary resources for a specified number of days.

Figure 4-10 shows an example of Elastic (On/Off) CoD usage within a site.

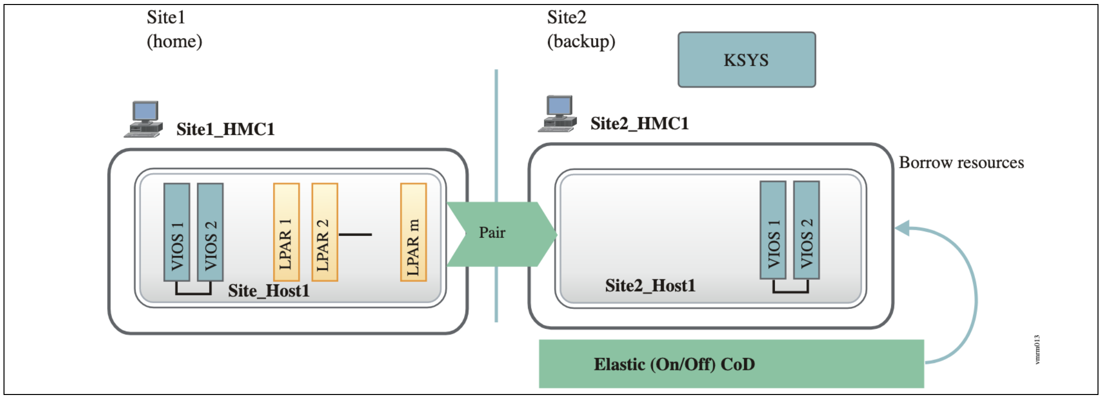


Figure 4-10 Elastic (On/Off) CoD usage for a host

When the active site fails, complete the following steps to enable Elastic (On/Off) CoD to manage the resources before you initiate a site-switch operation:

1. Authenticate all the HMCs by running the **hmcauth** command:

   ```
   hmcauth -u hmcuser -p password -a HMC_1_1
   hmcauth -u hmcuser -p password -a HMC_2_1
   ```

2. Identify the amount of available processor and memory units that are required by the backup hosts and determine whether you want to authorize the use of Elastic (On/Off) CoD to achieve the request. If the resource requests are not met by using enterprise pools, use Elastic (On/Off) CoD. For example, to request 2.5 CPUs and 10,500 MB of memory for the Host_2_1 host and use Elastic (On/Off) CoD for 5 days, enter the following command:

   ```
   ksysrppmgr -o execute -h :HMC_1_1:hmcuser -h :HMC_2_1:hmcuser -m
   Host_2_1:set:y5:10500:2.5 -r
   ```

1. Verify whether the VMs can be moved to the backup site by running the following command:

   ```
   ksysmgr verify site Site_2
   ```

   > **Note:** If the backup site does not have sufficient processors or memory, the verify operation fails with a warning message. You can use the **force** (**-f**) option to move the VMs to the backup site with the existing configuration.

2. Initiate the DR operation by running the following command in the KSYS node:

   ```
   ksysmgr move from=Site_1 to=Site_2 dr_type=planned
   ```

Running user-defined scripts for extra checks

When you need KSYS to perform some extra checks that are environment-specific, you can use scripts. Those scripts can be run before or after the discovery, verification, or DR operations.

For example, for enterprise pool resource management, a customized script can be added to update the backup host capacity and revert to older capacity values after the verification is complete. To monitor the workload that is running on the VMs for specific criteria, add scripts to check the workload before and after the verification. The scripts can run at site, host group, and VM levels.

Sample scripts are available in the `/opt/IBM/ksys/samples/custom_validation/` directory.

Running scripts before and after discovery and verification operations

The following attributes are available when adding any script for extra checks during verification operations:

- **`pre_verify`**

  When specifying a script with this attribute, the script runs before any discovery and verification operations. A **`pre_verify`** script can be added by entering the following command syntax:

  ```
  ksysmgr add script entity=site|host_group|vm pre_verify=script_path
  ```

- **`post_verify`**

  When specifying a script with this attribute, the script runs after any discovery and verification operations. A **`post_verify`** script can be added by entering the following command syntax:

  ```
  ksysmgr add script entity=site|host_group|vm post_verify=script_path
  ```

Running scripts before or after disaster recovery operations

You can use the following attributes to add a script for extra checks during DR operations:

- **`pre_offline`**

  When specifying a script with this attribute, the script runs before the VMs shut down at the primary site. A **`pre_offline`** script can be added by entering the following command syntax:

  ```
  ksysmgr add script entity=site|host_group|vm pre_offline=script_path
  ```

- **`post_offline`**

  When specifying a script with this attribute, the script runs after all the VMs shut down at the primary site. A **`post_offline`** script can be added by entering the following command syntax:

  ```
  ksysmgr add script entity=site|host_group|vm post_offline=script_path
  ```

- **`pre_online`**

  When specifying a script with this attribute, the script runs before the storage replication direction reverses and before the VMs restart on the target site. A **`pre_online`** script can be added by entering the following command syntax:

  ```
  ksysmgr add script entity=site|host_group|vm pre_online=script_path
  ```

- **`post_online`**

  When specifying a script with this attribute, the script runs after the VMs restart on the target site. A **`post_online`** script can be added by entering the following command syntax:

  ```
  ksysmgr add script entity=site|host_group|vm post_online=script_path
  ```

Registering scripts

When you register scripts, the KSYS subsystem passes the events arguments to the custom scripts that you registered. Values can be used to identify the operation that the KSYS subsystem is performing and determine at what stage of a specific operation to trigger the script by the KSYS subsystem.

Some of the events are listed here:

- `KSYS_MOVE_PLANNED_PRE_OFFLINE_SITE`
- `KSYS_MOVE_UNPLANNED_PRE_OFFLINE_SITE`

- KSYS_MOVE_PLANNED_POST_ONINE_SITE
- KSYS_MOVE_UNPLANNED_POST_ONLINE_SITE
- KSYS_PRE_DISCOVERVERIFY_QUICK_DISCOVERY_SITE
- KSYS_PRE_DISCOVERVERIFY_DETAIL_DISCOVERY_SITE
- KSYS_PRE_VERIFYONLY_QUICK_DISCOVERY_SITE
- KSYS_PRE_VERIFYONLY_DETAIL_DISCOVERY_SITE
- KSYS_PRE_DISCOVERONLY_QUICK_DISCOVERY_SITE

Configuring the timeout duration for custom scripts

The timeout duration for a custom script can be configured. If the custom script cannot complete the run within the configured timeout duration, the KSYS subsystem terminates the run of the custom script and proceeds with the next run. If the value `0` is set for the timeout duration, the system waits indefinitely for the custom script to complete the run before proceeding to the next run. Run the following command to configure the timeout duration for a custom script:

```
ksysmgr modify system [custom_script_timeout=<sec>]
```

The custom script timeout value that is set in this command is used at the site level, the host group level, and the VM level. The **sec** variable is the timeout duration in seconds for the custom script.

Running site-specific network scripts

During a DR event, when the LPARs move from the active site to the backup site, the IP addresses, subnet, and other network-related attributes change. If the backup environment will be the same as the source environment for the LPARs, DR scripts can be used that collect the information from the source LPARs and reconfigure the backup LPARs to match the system name, adapter configuration, network parameters, volume group information, and clustering configuration.

The DR scripts are custom scripts that are available in the KSYS package. Run these scripts in the VMs to collect required information about the source LPAR and use the collected information to re-create or import the environment in the recovered LPAR.

These scripts can be used for VMs that have AIX or Linux guest operating systems. Scripts consist of a readme file to ensure that users understand the configuration process. Scripts are available in the `/opt/IBM/ksys/samples/site_specfic_nw` file after KSYS software installation is done.

For more information about site-specific network configurations for Linux and AIX LPARs, see *Site-specific IP configurations in IBM Recovery Manager DR: Simplifying DR migration operation when the local and DR sites have different network configurations*.

4.8 Troubleshooting in VMRM DR

This section describes useful information if there are problems while you configure or use VMRM DR for Power. We describe some of the log files and traces that you can use for problem determination in an IBM Geographically Dispersed Resiliency for Power environment.

4.8.1 Notifications of KSYS events

The KSYS subsystem tracks various events that occur in the environment and saves the information in log files. The event log file is `/var/ksys/events.log` and operation event logs are at `/var/ksys/opevents.log`. The KSYS subsystem also sends emails and text notifications to the administrator if the contact information is registered on the KSYS configuration by using the **`ksysmgr add notify`** command.

You can run the **`ksysmgr query event`** command to list all the events that can be notified.

The events are categorized as critical errors, warning, and informational events. To query all events of a specific event type, run the following command:

```
ksysmgr query event type=error|warning|info
```

4.8.2 Analyzing the log files

When errors are encountered while running the **`ksysmgr`** command, log files can be analyzed to diagnose the issue. Determine the software component that is causing the problem by analyzing the log files. You can find the **`ksysmgr`** command log files in the `/var/ksys/log/` directory.

After a log file such as `host_monitor.log`, `host_monitor_crit.log`, or `host_monitor_hvncp.log` reaches a maximum size of 20 MB, the existing log file is backed up and a new log file is created. By default, network logging is not enabled. The spooling file that has the highest number in the file name becomes the oldest log file. By default, three spooling files are created for log collection. The number of spooling files can be configured by using the **`ksysmgr`** command. The maximum value is 10 spooling files.

When running the **`ksysmgr`** command, the following types of log files are created:

`ksysmgr.oplog`: Keeps a rolling record of all the **`ksysmgr`** operations that you ran for a specific period. All the commands that you entered are logged in this log file along with the date, time, and the transaction ID.

`ksysmgr.log`: Contains the detailed processing information about each function when you run a **`ksysmgr`** command. The `ksysmgr.log` file contains the detailed processing information only when you specify the **`-l max`** flag when you run the **`ksysmgr`** command.

`ksys_srdf.log`: Contains the detailed processing information about all the Dell EMC SRDF storage-specific functions along with the date and time.

`ksys_svc.log`: Contains the detailed processing information about all the SAN Volume Controller Storwize storage-specific functions along with the date and time.

`ksys_ccl.log`: Contains the detailed processing information about all the Hitachi storage-specific functions along with the date and time.

`ksys_ds8k.log`: Contains the detailed processing information about all the DS8000 series storage-specific functions along with the date and time.

`ksys_unity.log`: Contains the detailed processing information about all the Dell EMC Unity storage-specific functions along with the date and time.

Trace files contain details about processes that are running as part of the operations that are performed by the KSYS node. If you cannot identify the cause of an error by analyzing the log files, use the trace files for problem determination. Run the following command to convert trace files to a report:

```
ksysmgr trace log type=ksys|fde|fdelong|krest|krestlong|user|ALL > /test.out
```

The traces can be redirected to a file and viewed for debugging purposes.

The trace file can be extracted by using the RSCT **`rpttr`** command. Along with the log files, resource manager traces are useful during problem determination of issues with the KSYS node and the VMRM for Power environment. The configuration of the KSYS node is stored in RSCT resource classes under `/var/ct/<clustername>/registry/local_tree`. The RSCT daemon `IBM.VMR` also maintains traces that constantly run while you run **`ksysmgr`** operations. These traces are in the `/var/ct/<cluster_name>/log/mc/IBM.VMR` directory.

You can use the **`rpttr`** command to format the traces. The syntax is as follows:

```
# rpttr -f -o dict <trace file names>
```

Collecting log files for VMRM DR

To collect the log files of the KSYS subsystem, run the **`snap vmsnap`** command on the KSYS node. These log files can be used to debug issues that might occur while performing KSYS operations. To run the **`snap vmsnap`** command successfully, the `/tmp` folder must have 2 GB or more of space available. The log data is recorded in the `/tmp/ibmsupt/vmsnap/ksys.pax.Z` file.

The command to collect the log files for the KSYS subsystem is as follows:

```
snap vmsnap
```

An output of the **`vmsnap`** command is shown in Example 4-23.

Example 4-23 A vmsnap output

```
********Checking and initializing directory structure
Directory /tmp/ibmsupt/vmsnap already exists... skipping
Directory /tmp/ibmsupt/testcase already exists... skipping
Directory /tmp/ibmsupt/other already exists... skipping
********Finished setting up directory /tmp/ibmsupt

Checking Space requirement for vmsnap

Checking space requirements for my product...Checking for enough free space in
filesystem... done.

Gathering vmsnap data

Gathering VMRM product information...

Clearing the /tmp/ibmsupt/vmsnap of redundant files and directories...

Gathering VM/HM logs...

Collecting the VM logs for HG=0 (0 = ALL HGs)...
Collecting the HM logs for HG=0 (0 = ALL HGs)...
```

```
Successfully started VM/HM log collection...

To check the status of VM/HM log collection, run 'ksysmgr query system status monitor=yes'

Gathering RM traces and registry...

...................
Cleaning old temporary directory at
Log directory set to /tmp/ibmsupt/vmsnap/tmpstage.12124544
tar file set to /tmp/ibmsupt/vmsnap/tmpstage.12124544/ctsnap.ksys216.1106084226.tar
Gathering information......
Running gcore/gencore for active daemons...
............................
Completed running gcore/gencore for active daemons.
Preparing /var/ct on /tmp/ibmsupt/vmsnap/tmpstage.12124544/trclog//var/ct/

Gathering information......
...........................................................................................
.......Gathering trace spool files as follows:
lstrsp --node_name ksys216 --previous 1 --tar
./tmp/ibmsupt/vmsnap/tmpstage.12124544/ctsnap_out/TRACE_SPOOL.tar --no_usage --tar_ticks
Done gathering trace spool files

Starting tar/compress process......
copying files from /tmp/ibmsupt/vmsnap/tmpstage.12124544 to /tmp/ibmsupt/vmsnap
deleting temporary directory /tmp/ibmsupt/vmsnap/tmpstage.12124544
*******done*******
Successfully gathered RM traces and registry data...

Gathering storage and UIagent related data...

Successfully gathered storage and UIagent related data...

Gathering KSYS resource attributes...

Successfully gathered KSYS resource attributes...

Gathering KSYS class attributes...

Successfully gathered KSYS classes attributes...

Gathering General System information...

Successfully gathered general system information...

Removing existing redundant files if present in /tmp/ibmsupt/vmsnap.
Removing the extraneous files copied and compressed in the snap file ksys.pax.Z

VMRM snap data can be found in the file:/tmp/ibmsupt/vmsnap/ksys.pax.Z
VM and HM logs can be found in their corresponding VM's and HM's log location.
VM log location:/var/ksys/log/snap   HM log location:/tmp/ibmsupt/snap
```

4.8.3 Removing a KSYS cluster and uninstalling VMRM DR

If you must uninstall the KSYS file sets from the KSYS node, remove the cluster before uninstalling the file sets. Otherwise, the RSCT Peer Domain remains on the node. The command that is used to perform the cluster removal is as follows:

```
ksysmgr remove ksyscluster <cluster_name>
```

An example output from **ksysmgr remove ksyscluster** is shown in Example 4-24.

Example 4-24 A ksysmgr remove cluster output

```
# ksysmgr remove ksyscluster SMR_DR
WARNING: This action will remove all configuration and destroy the KSYS setup. It
iis recommended to create a backup with "ksysmgr add snapshot -h"
Do you want a backup to be created now ? [y|n]
N
Do you want to proceed? [y|n]
y
This might take a few minutes to remove the ksyscluster
06:09:55  Automatic deep discovery disabled
06:09:55  Automatic quick discovery disabled
06:53:34  Removed Workgroup VMs from workgroups
06:53:36  Workgroups have been deleted
07:04:53  Consistency group cleanup successful
07:05:47  IBM.VMR process stopped successfully
07:05:54  Peer domain was removed successfully
Removed tmp files successfully on ksys202gui.aus.stglabs.ibm.com node

If you want to have backup/snapshot before removing the cluster, give "Y" to the
prompt which shows "Do you want a backup to be created now ? [y|n]".
```

After you remove the cluster, the `ksys.*` file sets can be uninstalled by using the **smit remove** command or by using the **installp -ug ksys** command.

5

Planning and deploying IBM VMRM HADR

This chapter provides the procedure to configure IBM Virtual Machine Recovery Manager HADR (VMRM HADR).

The following topics are described in this chapter:

- Requirements
- Deployment
- Limitations for VMRM HADR
- Managing the VMRM HADR environment

5.1 Requirements

VMRM HADR is a combination of VMRM HA and VM Recovery DR. It has VMRM HA functions within the home site, and it plays the role of VMRM DR between the home and backup (disaster recovery (DR)) sites. Therefore, the requirements for both roles must be met before configuring VMRM HADR. Because the requirements for both VMRM HA and VMRM DR are covered in other chapters, we do not describe them here. For more information about the requirements for VMRM HA, see 3.1, “VMRM HA requirements” on page 44. For more information about the requirements for VMRM DR, see 4.1, “Requirements” on page 94.

Here are the hardware configuration prerequisites for a VMRM HADR cluster:

- Two or more hosts at the home site and one or more hosts at the backup site are required.
- Two Virtual I/O Server (VIOS) instances at the home site hosts are required.
- The home site VIOS instances must have at least two shared disks between them for a Shared Storage Pool (SSP) cluster, and a Cluster Aware AIX (CAA) volume group for the repository. The size of the shared disks must be 10 GB or more.
- The managed virtual machine (VMs) must have disks on the source storage and the target storage, and the replication process must run successfully between disks.

> **Note:** A new feature in VMRM 1.7 allows for more than one KSYS node in VMRM. This feature is especially useful in VMRM HADR and HADRHA environments. In these environments, one KSYS node on each site is a best practice. For more information about this new feature, see Chapter 8, “KSYS high availability” on page 217.

5.2 Deployment

Here is the procedure to deploy a VMRM HADR environment.

5.2.1 Installing the KSYS software

The VMRM DR installation media has all the file sets for VMRM HADR and HADRHA. Here are the file sets that are on the media:

```
ksys.drutils.rte
ksys.ha.license
ksys.hautils.rte
ksys.hsmon.rte
ksys.license
ksys.main.cmds
ksys.main.msg.DE_DE.cmds
ksys.main.msg.ES_ES.cmds
ksys.main.msg.FR_FR.cmds
ksys.main.msg.IT_IT.cmds
ksys.main.msg.JA_JP.cmds
ksys.main.msg.PT_BR.cmds
ksys.main.msg.ZH_CN.cmds
ksys.main.msg.ZH_TW.cmds
ksys.main.msg.en_US.cmds
ksys.main.rte
ksys.mirror.ds8k.rte
ksys.mirror.emc.rte
ksys.mirror.hitachi.rte
ksys.mirror.svc.rte
ksys.mirror.unity.rte
ksys.mirror.xiv.rte
ksys.ui.agent
ksys.ui.common
ksys.ui.server
ksys.vmmon.rte
vmagent-1.7.0-1.0.el7.ppc64le.rpm
vmagent-1.7.0-1.0.suse123.ppc64le.rpm
```

The last three items in the list must be installed on the managed VMs. The agents support the following operating systems:

- AIX (`ksys.vmmon.rte`)
- Red Hat (`vmagent-1.7.0-1.0.el7.ppc64le.rpm`)
- SUSE Linux (`vmagent-1.7.0-1.0.suse123.ppc64le.rpm`)

Do not install the file sets on the KSYS server. Only the required language file sets must be installed.

Likewise, there are file sets for each storage vendor that is supported. Install only the file set for your storage.

5.2.2 Creating the KSYS cluster

After the file sets for a high availability and disaster recovery (HADR) type of deployment of the VMRM solution is installed on the KSYS logical partitions (LPARs), create a VMRM cluster of HADR type.

To configure the HADR cluster type, specify **`type=HADR`** while configuring the cluster, as shown by the following command:

```
ksysmgr add ksyscluster <HADR_CLUSTER_NAME> type=HADR ksysnodes=<hostname>
sync=[yes|no]
```

For example:

```
ksysmgr add ksyscluster cluster_name ksysnodes=ksysnode1 type=HADR
```

5.2.3 Creating sites

Create sites that are used to map all the HMCs, hosts, and storage devices. Create an active site where the workloads are running and a backup site that acts as a backup for the workloads during a disaster or a potential disaster situation.

Site names are logical names that represent your sites. A site name can be any American Standard Code for Information Interchange (ASCII) string that is limited to 64 characters. A site name cannot contain any special characters or spaces.

By default, the active site is the home site. You can configure only two sites. When you create sites, the replication type of the site is asynchronous by default. After you create sites, you can change the type of storage replication to synchronous if needed.

To create sites for the HADR type of deployment of the VMRM solution, complete the following steps in the KSYS LPAR:

- Add the home site (Site1) by running the following command:

  ```
  ksysmgr add site <Site1> sitetype=home
  ```

- Add backup site (Site2) by running the following command:

  ```
  ksysmgr add site <Site2> sitetype=backup
  ```

5.2.4 Adding HMCs to the KSYS subsystem

The KSYS interacts with the HMC for discovery, verification, monitoring, recovery, and cleanup operations. HMCs that are configured in both the active and backup sites provide details about the hosts and VIOS partitions that are managed by the HMCs in each site. The HADR type of deployment of the VMRM solution cannot be implemented without configuring the HMCs. Therefore, you must provide the HMC details to the KSYS.

> **Note:** The HMC user, whose username and password details are provided to the KSYS, must have `hmcsuperadmin` privileges with remote access enabled.

To add the HMCs to a specific site, complete the following steps in the KSYS LPAR:

1. To add the HMC that manages the host or hosts in the active site (Site1), run the following command:

   ```
   ksysmgr add hmc <HMC1_name> ip=<HMC IP1> login=hscroot password=<abc123>
   site=<Site1>
   ```

2. Then, add the HMC that manages the host or hosts in the backup site (Site2) by running the following command:

   ```
   ksysmgr add hmc <HMC2_name> ip=<HMC IP2> login=hscroot password=<abc123>
   site=<Site2>
   ```

5.2.5 Adding hosts to the KSYS subsystem

The KSYS monitors and manages DR operations across sites. The KSYS requires that each host must be paired to another host across sites. This type of pairing enables the VMs to move from one host to another host across sites. Plan the host pairing across sites in advance, and then implement the pairing.

After the HMCs are added to the KSYS, you can review the list of managed hosts by each HMC, and then identify the hosts that you want to add to the KSYS for DR. Connect the source hosts and target hosts to different HMCs across sites. If you connect the source hosts and target hosts to the same HMC, it leads to an invalid configuration in the KSYS subsystem and can cause failures in DR operations.

When a host is added to a host group, all the VMs on the host are included by default in the DR management scope. However, DR management starts only after you configure the subsystems and run the discovery and verification operations. Therefore, if you plan to exclude a set of VMs after adding the hosts, you can unmanage those VMs and then run the discovery and verification operations.

To add the hosts to the KSYS configuration, complete the following steps in the KSYS LPAR:

1. Add the managed host (for example, hostname Host1, Host2), which is running the workload, to the KSYS subsystem by running the following commands:

   ```
   ksysmgr add host <Host1> site=<Site1>
   ksysmgr add host <Host2> site=<Site1>
   ```

2. Add the backup host (for example, hostname Host3), which acts as a backup host to the KSYS subsystem by running the following command:

   ```
    ksysmgr add host <Host3> site=<Site2>
   ```

5.2.6 Adding a storage agent

After adding hosts to the KSYS subsystem, you must add storage agents to the KSYS subsystem. For different type of storage systems, the parameters for adding a storage agent might be different. For more information about different storage types, see 9.4, “Configuring VMRM HA by using the GUI” on page 245.

To add a storage agent, run the following command:

```
ksysmgr add storage_agent <name> hostname|ip=<storage> login=<username>
password=<password> type=<type of storage> serialnumber=<storage_serialnumber>
site=<site_name>
```

5.2.7 Creating a host group

A *host group* is a group of hosts that are managed as a group. By using a host group, you can group a set of hosts based on your business requirements. For example, you can group the hosts that run similar type of workloads. You also can group important hosts together so that the monitoring and recovery operations can be performed quickly for that set of hosts as a unit. In disaster situations, you can move each host group separately to the backup site.

There are two types of host groups that can be defined in VMRM:

- Symmetric host groups are defined with a one-to-one mapping of the primary host and a backup host.
- Asymmetric host groups have a many-to many mapping of the hosts.

Here are the guidelines to manage host groups*:*

- Each host in a site must be a part of a host group. If a host is not added to any host groups, the host automatically is added to the Default_HG host group during the discovery operation.
- A host already must be added to the KSYS configuration settings, and if you use a symmetric host group, the host must be paired with a backup host in the backup site.
- The corresponding hosts in the backup site that are paired with the active site hosts are grouped logically within the same host group. For example, if host1 in the active site is paired with host2 in the backup site and you create a host group hg1 with host1, then host2 is automatically added to the host group hg1.

- Each host group must be associated with a separate disk group. The disks in the disk group must not be shared among different host groups. The disk groups are named with the following format:

  ```
  VMRDG_{peer_domain_name}_{site_name}_{host_group_ID}
  ```

  However, the disk group name must not exceed the maximum number of characters that is supported for a consistency group (CG) at the storage level.

  For IBM SAN Volume Controller and IBM DS8000 Storage Systems, host groups can span across a single type of storage. Multiple host groups can use the same type of storage disks, but the disks must not be shared among different host groups.
- After you add or remove hosts from a host group, you must run a discovery operation to manage or unmanage all the VMs. The modified host group displays the correct list of managed VMs only after a discovery operation.
- If you remove all hosts from Default_HG, the disk group corresponding to Default_HG is not removed. The disk groups are retained with the removed hosts.

To create a host group, identify the available disks that you can designate as the repository disk and the high availability (HA) disk for the SSP cluster by running the following command for the VIOSs that are part of the host group on the home site:

```
ksysmgr query viodisk vios=VIOS1,VIOS2,VIOS3,VIOS4
```

You can create a symmetric or asymmetric host group and add the existing hosts to it.

Symmetric host group

Before creating a symmetric host group, you must create host pairs. After the hosts are added to the KSYS subsystem, identify the hosts that must be paired across the active site and the backup site. Each backup host in the host pair must meet all the resource requirements so that the backup host can run the same workload in a disaster or a potential disaster situation. Pair the identified host (for example, hostname `Host1, Host3`) in the active site to the identified host (for example, hostname `Host2, Host4`) in the backup site by running the following commands:

```
ksysmgr pair host Host1 pair=Host2
ksysmgr pair host Host3 pair=Host4
```

Now, create a symmetric host group by running the following command:

```
ksysmgr add host_group Host_group1 hosts=Host1,Host3 ha_disk=SSP_disk1
repo_disk=SSP_disk2
```

> **Note:** After you add one host from the host-pair to a host group, the other host of the host-pair automatically is added to the respective host group in the other site. These hosts form a symmetric host group, which contains one-to-one paired hosts.

Asymmetric host group

To create an asymmetric host group and add the existing hosts to the asymmetric host group, run the following command:

```
ksysmgr add host_group Host_group1 hosts=Host1,Host2,Host3 mxn_pairing=yes
ha_disk=SSP_disk1 repo_disk=SSP_disk2
```

> **Note:** By default, the **`mxn_pairing`** attribute is set to `no`. To create an asymmetric host group, which contains one-to-many paired hosts, set the **`mxn_pairing`** attribute to `yes`. Do not pair the hosts before adding the hosts to the host group.

5.2.8 Unmanaging VMs

You might not want VMRM to manage all the VMs or VIOSs in your environment. You can unmanage VMs or VIOSs by running the following commands:

- To unmanage VIOSs, run the following command:

```
ksysmgr unmanage vios <viosname[,...]>
```

- To unmanage VMs, run the following command:

```
ksysmgr unmanage vm
      name=<vmname> host=<hostname> | uuid=<lparuuid> | ALL host=<hostname> |
ALL host_group=<host_group_name>
```

> **Note:** If you are planning for only a few of the VMs to be in the managed hosts, you can use the **ALL** option of the **unmanage** command. Then, after all the VMs are unmanaged, you can add the VMs that you want to be managed by using the **ksysmgr manage vm** command. The command syntax is as follows:
>
> ```
> ksysmgr manage vm
>       name=<vmname> host=<hostname> | uuid=<lparuuid> | ALL host=<hostname> |
> ALL host_group=<host_group_name>
> ```

5.2.9 Modifying any attributes

For VMRM HA or VMRM DR, some attributes or parameters might need to be changed for your environment. You can make the change now or later. If you choose to change these attributes later, run KSYS discovery and verify after any changes. The attributes that can be changed are documented in 3.5, “Setting up HA policies” on page 78 and 4.7, “Managing and administering VMRM DR” on page 144.

5.2.10 Discovering and verifying

Now, put everything together and activate the functions. Run discovery and verification again after you change the VMRM environment. You can run KSYS discovery and verification on a site or host group level.

- To perform the discovery and verify operations at the site level, run the following command:

```
ksysmgr discover site Austin verify=yes
```

- To perform the discovery and verify operations for a specific host group, run the following command:

```
ksysmgr discover host_group hg_name verify=yes
```

- To perform the discovery operation and DR-only verify operations for a specific host group, run the following command:

```
ksysmgr discover host_group hg_name verify=true option=DRonly
```

After the discovery and verify operations complete, you are done with configuring the VMRM HADR environment.

5.2.11 Installing virtual machine agents

To help manage AIX and Linux VMs, install agents in those VMs, as described in 7.1, “Installing VM Agents” on page 200.

5.2.12 Example configuration

Example 5-1 displays the commands that are used to create a VMRM HADR environment in our lab. This environment has the following components:

- One KSYS LPAR
- Two HMCs, one on each site
- Four hosts, two on each site
- Two IBM DS8000 Storage Systems, one on each site
- Four managed VMs

Example 5-1 Commands to deploy the VMRM HADR environment

```
ksysmgr add ksyscluster AB_HADR type=HADR ksysnodes=ksys910.aus.stglabs.ibm.com
ksysmgr add site HomeSite sitetype=home
ksysmgr add site BackupSite sitetype=backup
ksysmgr add hmc hahmc1 login=hscroot hostname=hahmc1.aus.stglabs.ibm.com
site=HomeSite
ksysmgr add hmc rthmc5 login=hscroot hostname=rthmc5.aus.stglabs.ibm.com
site=BackupSite
ksysmgr add host e52den-8247-22L-21339EA site=HomeSite
ksysmgr add host e52pen-8247-22L-2133AAA site=HomeSite
ksysmgr add host e50cat-8247-22L-2133A5A site=BackupSite
ksysmgr add host e10kacha-8284-22A-1073C6T site=BackupSite
ksysmgr pair host e52pen-8247-22L-2133AAA pair=e50cat-8247-22L-2133A5A
ksysmgr pair host e52den-8247-22L-21339EA pair=e10kacha-8284-22A-1073C6T
ksysmgr add storage_agent ds8k5 hostname=ds8k5hmc.aus.stglabs.ibm.com
site=HomeSite storagetype=ds8k login=fvtadmin
ksysmgr add storage_agent ds8k8 login=fvtadmin site=BackupSite storagetype=ds8k
ip=9.xxx.xxx.xxx
ksysmgr q viodisk vios=e52denv1,e52denv2,e52penv1,e52penv2

ksysmgr add hg HG1 hosts=e52den-8247-22L-21339EA,e52pen-8247-22L-2133AAA
ha_disk=01MOlCTTIxNDUxMjQ2MDA1MDc2ODAyODEwNDI2ODgwMDAwMDAwMDAwMEQONA==
repo_disk=01MOlCTTIxNDUxMjQ2MDA1MDc2ODAyODEwNDI2ODgwMDAwMDAwMDAwMERFQg==

ksysmgr unmanage vm ALL host_group=HG1
ksysmgr manage vm e52pen002
ksysmgr manage vm e52pen005
ksysmgr manage vm e52pen006
ksysmgr manage vm e52pen007
ksysmgr manage vm e52pen008
ksysmgr manage vm e52pen009
ksysmgr modify system ha_monitor=enable
ksysmgr discover site HomeSite verify=yes
```

The command in Example 5-2 on page 179 shows that the KSYS cluster type is HADR.

Example 5-2 HADR VMRM environment

```
# ksysmgr q cluster
Name:                AB_HADR
State:               Online
Type:                HADR
Ksysnodes:           ksys910.aus.stglabs.ibm.com:1:Online
```

Example 5-3 displays the host group information. It shows the SSP name, Repo_disk, and HA_disk.

Example 5-3 The host group information

```
Name:                HG1
Home Site Hosts:     e52den-8247-22L-21339EA
                     e52pen-8247-22L-2133AAA
Backup Site Hosts:   e10kacha-8284-22A-1073C6T
                     e50cat-8247-22L-2133A5A
Memory_capacity:     Priority-Based Settings
                     low:100
                     medium:100
                     high:100
CPU_capacity:        Priority-Based Settings
                     low:100
                     medium:100
                     high:100
Skip_power_on:       None
Sriov_override:      No
Site:                BackupSite
Vswitchmap:          Not currently set
Vlanmap:             Not currently set
DrVswitchmap:        Not currently set
DrVlanmap:           Not currently set
HA_monitor:          enable
Lpm_support:         None
Proactiveha:         disable
Restart_policy:      auto
VM_failure_detection_speed:    normal
Host_failure_detection_time:   90
Type:                symmetric
Custom CG Name:
Backup Site CG Name:

SSP Clusters Attributes
Sspname:             KSYS_AB_HADR_1_1
Sspstate:            UP
Ssp_version:         VIOS 3.1.3.21
VIOS:                e52denv2
                     e52denv1
                     e52penv2
                     e52penv1
Repo_disk:
01M0lCTTIxNDUxMjQ2MDA1MDc2ODAyODA4NEMxNDAwMDAwMDAwMDAwMTg0Qg==
HA_disk:
01M0lCTTIxNDUxMjQ2MDA1MDc2ODAyODA4NEMxNDAwMDAwMDAwMDAwMTg0QQ==
```

Example 5-4 displays the information of the VMs that are managed in the VMRM HADR environment.

Example 5-4 Managed VMs in the VMRM HADR environment

```
# ksysmgr q vm state=manage
Managed VMs:
        e52pen007
        e52pen005
        e52pen002
        e52pen009
        e52pen006
        e52pen008

All Managed VMs:
Name:                e52pen007
UUID:                0637A929-970D-4BC7-BCB2-658BEFD366F8
DRState:             READY_TO_MOVE
HAState:             READY_TO_MOVE
Dr Test State:       READY
Host:                e50cat-8247-22L-2133A5A
Priority:            Medium
Skip_power_on:       None
VM_failure_detection_speed:    normal
HA_monitor:          enable
Proactiveha:         disable
Homehost:            e52den-8247-22L-21339EA
BackupSiteHomehost:  e50cat-8247-22L-2133A5A
VM_status:           NO_OPERATION_IN_PROGRESS
Version_conflict:    No
DrTargetHost:        e52pen-8247-22L-2133AAA
AppMessaging:        enable
Active Pool:         DefaultPool
PoolMap:             None

Name:                e52pen006
UUID:                600A2B7C-F96E-4519-9B3B-97F30434375D
DRState:             READY_TO_MOVE
HAState:             READY_TO_MOVE
Dr Test State:       READY
Host:                e50cat-8247-22L-2133A5A
Priority:            Medium
Skip_power_on:       None
VM_failure_detection_speed:    normal
HA_monitor:          enable
Proactiveha:         disable
Homehost:            e52den-8247-22L-21339EA
BackupSiteHomehost:  e50cat-8247-22L-2133A5A
VM_status:           NO_OPERATION_IN_PROGRESS
Version_conflict:    No
DrTargetHost:        e52pen-8247-22L-2133AAA
AppMessaging:        enable
Active Pool:         DefaultPool
PoolMap:             None

Name:                e52pen009
```

```
UUID:                3C634ACA-5EA0-45CA-A09D-B653B9034CD9
DRState:             READY_TO_MOVE
HAState:             READY_TO_MOVE
Dr Test State:       READY
Host:                e50cat-8247-22L-2133A5A
Priority:            Medium
Skip_power_on:       None
VM_failure_detection_speed:    normal
HA_monitor:          enable
Proactiveha:         disable
Homehost:            e52den-8247-22L-21339EA
BackupSiteHomehost:  e50cat-8247-22L-2133A5A
VM_status:           NO_OPERATION_IN_PROGRESS
Version_conflict:    No
DrTargetHost:        e52pen-8247-22L-2133AAA
AppMessaging:        enable
Active Pool:         DefaultPool
PoolMap:             None

Name:                e52pen002
UUID:                1A844B48-2525-470F-AB9C-5645308C7BC9
DRState:             READY_TO_MOVE
HAState:             READY_TO_MOVE
Dr Test State:       READY
Host:                e50cat-8247-22L-2133A5A
Priority:            Medium
Skip_power_on:       None
VM_failure_detection_speed:    normal
HA_monitor:          enable
Proactiveha:         disable
Homehost:            e52den-8247-22L-21339EA
BackupSiteHomehost:  e50cat-8247-22L-2133A5A
VM_status:           NO_OPERATION_IN_PROGRESS
Version_conflict:    No
DrTargetHost:        e52pen-8247-22L-2133AAA
AppMessaging:        enable
Active Pool:         DefaultPool
PoolMap:             None

Name:                e52pen005
UUID:                0683B837-EF61-403C-8014-BDF657F62449
DRState:             READY_TO_MOVE
HAState:             READY_TO_MOVE
Dr Test State:       READY
Host:                e50cat-8247-22L-2133A5A
Priority:            Medium
Skip_power_on:       None
VM_failure_detection_speed:    normal
HA_monitor:          enable
Proactiveha:         disable
Homehost:            e52den-8247-22L-21339EA
BackupSiteHomehost:  e50cat-8247-22L-2133A5A
VM_status:           NO_OPERATION_IN_PROGRESS
Version_conflict:    No
DrTargetHost:        e52pen-8247-22L-2133AAA
```

```
AppMessaging:        enable
Active Pool:         DefaultPool
PoolMap:             None

Name:                e52pen008
UUID:                76A22ACD-97C6-4EB3-A420-758C553ACB2A
DRState:             READY_TO_MOVE
HAState:             READY_TO_MOVE
Dr Test State:       READY
Host:                e50cat-8247-22L-2133A5A
Priority:            Medium
Skip_power_on:       None
VM_failure_detection_speed:    normal
HA_monitor:          enable
Proactiveha:         disable
Homehost:            e52pen-8247-22L-2133AAA
BackupSiteHomehost:  e50cat-8247-22L-2133A5A
VM_status:           NO_OPERATION_IN_PROGRESS
Version_conflict:    No
DrTargetHost:        e52pen-8247-22L-2133AAA
AppMessaging:        enable
Active Pool:         DefaultPool
PoolMap:             None
```

5.3 Limitations for VMRM HADR

The following limitations apply when working with the HADR and HADRHA deployment types of VMRM:

- The workgroup option is not supported in the VMRM HADR or HADRHA configurations.
- When you manually shut down or restart a VM, the dependent applications are not affected. The recovery of dependent applications is considered only when failure occurred with the parent application, the VM, or the host.
- Remove the default host group (Default_HG) before configuring the HADR and HADRHA types of deployment with PowerHA SystemMirror. To remove the default host group from the KSYS subsystem, run the following command:

  ```
  rmrsrc -s "Name='Default_HG'" IBM.VMR_HG
  ```

- Disable the quick discovery feature before running the Live Partition Mobility (LPM) and the restart operations on VMs.

5.4 Managing the VMRM HADR environment

The management of the VMRM HADR environment is the same as what is documented in Chapter 3, “Planning and deploying IBM VMRM HA” on page 43 and Chapter 4, “Planning and deploying IBM VMRM DR” on page 93.

5.4.1 Installing GUI file sets

To use the VMRM DR and manage KSYS nodes by using the GUI, you must install the GUI server and GUI agent file sets on a system. The LPAR in which you want to install the GUI file sets must be running IBM AIX 7.2 with Technology Level 2 Service Pack 1 (7200-02-01) or later. You can choose to install the GUI server and GUI agent file sets on one of the KSYS nodes. For more information about installing the GUI, see Chapter 9, “IBM VMRM GUI deployment” on page 237.

6

Planning and deploying IBM VMRM HADRHA

This chapter provides the procedure to configure Virtual Machine Recovery Manager HADRHA (VMRM HADRHA) environments.

The following topics are described in this chapter:

- Requirements
- Deployment
- Limitations

6.1 Requirements

VMRM HADRHA is a combination of VMRM HA and VMRM DR. It has VMRM HA functions within the home site, and it plays the role of VMRM DR between the home and backup (disaster recovery (DR)) sites. If the virtual machines (VMs) are running in the backup site, VMRM HA functions are available at the backup site.

The requirements for both VMRM DR and VMRM HA must be met at both the home and backup sites before configuring VMRM HADRHA. The requirements for VMRM HA are described in 3.1, “VMRM HA requirements” on page 44. The requirements for VMRM DR are described in 4.1, “Requirements” on page 94.

Here are the hardware configuration prerequisites for a VMRM HADRHA cluster:

- Two or more hosts at the home site and one or more hosts at the backup site are required.
- Two Virtual I/O Server (VIOS) instances at the home site hosts are required.
- Home site VIOS instances must have at least two shared disks between them for a Shared Storage Pool (SSP) cluster, and a Cluster Aware AIX (CAA) volume group for a repository. The size of the shared disks must be 10 GB or more.
- Backup site VIOS instances must have at least two shared disks between them for an SSP cluster, and a CAA volume group for a repository. The size of the shared disks must be 10 GB or more.
- The managed VMs must have disks on the source storage and the target storage, and the replication process must run successfully between disks.

Note: A new feature in VMRM 1.7 enables more than one KSYS nodes in VMRM. This feature is especially useful in VMRM HADR and HADRHA environments. In these environments, one KSYS node on each site is a best practice. For more information about this new feature, see Chapter 7, “Common tasks across the IBM VMRM family” on page 199.

6.2 Deployment

Here is the procedure to deploy a VMRM HADRHA environment.

6.2.1 Installing the KSYS software

The file sets that are required for VMRM HADRHA are the same as for VMRM HADR, and the installation of the KSYS software for VMRM HADRHA are the same as for VMRM HADR. For more information about how to install the KSYS software, see 5.2, “Deployment” on page 172.

6.2.2 Creating the KSYS cluster

After the file sets for a HADRHA type of deployment of the VMRM solution are installed on the KSYS logical partitions (LPARs), create a VMRM cluster of HADRHA type.

To configure the HADRHA cluster type, specify `type=HADRHA` while configuring the cluster by running the following command:

```
ksysmgr add ksyscluster <HADR_CLUSTER_NAME> type=HADRHA ksysnodes=<hostname>
sync=[yes|no]
```

For example:

```
ksysmgr add ksyscluster HADRHA_TEST ksysnodes=ksys913.ausprv.stglabs.ibm.com
type=HADRHA
```

6.2.3 Creating sites

Create sites that map all the HMCs, hosts, and storage devices. Create an active site where the workloads are running and a backup site that acts as a backup for the workloads during a disaster or a potential disaster situation.

Sites are logical names that represent your sites. A site name can be any American Standard Code for Information Interchange (ASCII) string that is limited to 64 characters. A site name cannot contain any special characters or spaces.

By default, the active site is the home site. You can configure only two sites. When you create sites, the replication type of the site is asynchronous by default. After you create sites, you can change the type of storage replication to synchronous.

To create sites for the HADRHA type of deployment of the VMRM solution, complete the following steps in the KSYS LPAR:

1. Add the home site (Site1) by running the following command:

   ```
   ksysmgr add site <Site1> sitetype=home
   ```

2. Add the backup site (Site2) by running the following command:

   ```
   ksysmgr add site <Site2> sitetype=backup
   ```

6.2.4 Adding HMCs to the KSYS subsystem

The KSYS interacts with the HMC for discovery, verification, monitoring, recovery, and cleanup operations. HMCs that are configured at both the active and backup sites provide details about the hosts and VIOS partitions that are managed by the HMCs at each site. The HADRHA type of deployment of the VMRM solution cannot be implemented without configuring the HMCs. Therefore, you must provide the HMC details to the KSYS.

> **Note:** The HMC user, whose username and password details are provided to the KSYS, must have `hmcsuperadmin` privileges with remote access enabled.

To add the HMCs to a specific site, complete the following steps in the KSYS LPAR:

1. To add the HMC (for example, HMC name: HMC1_name, IP address of the HMC: HMC IP1, login: `hscroot`, password: `abc123`) that manages the host or hosts in the active site (Site1), run the following command:

   ```
   ksysmgr add hmc <HMC1_name> ip=<HMC IP1> login=hscroot password=<abc123>
   site=<Site1>
   ```

2. Add the HMC (for example, HMC name: HMC2_name, IP address of the HMC: HMC IP2, login: `hscroot`, password: `abc123`) that manages the host or hosts in the backup site (Site2), run the following command:

   ```
   ksysmgr add hmc <HMC2_name> ip=<HMC IP2> login=hscroot password=<abc123>
   site=<Site2>
   ```

6.2.5 Adding hosts to the KSYS subsystem

The KSYS monitors and manages the DR operations across sites. The KSYS requires that each host must be paired to another host across sites. This type of pairing enables the VMs to move from one host to another host across sites. Plan the host pairing across sites in advance, and then implement the pairing.

After the HMCs are added to the KSYS, you can review the list of hosts that are managed by each HMC, and then identify the hosts that you want to add to the KSYS for DR. Connect the source hosts and target hosts to different HMCs across sites. If you connect the source hosts and target hosts to the same HMC, it leads to an invalid configuration in the KSYS subsystem and can cause failures in DR operations.

When a host is added to a host group, all the VMs on the host are included by default in the DR management scope. However, DR management starts only after you configure the subsystems and run the discovery and verification operations. Therefore, if you plan to exclude a set of VMs after adding the hosts, you can unmanage those VMs, and then run the discovery and verification operations.

To add the hosts to the KSYS configuration, complete the following steps in the KSYS LPAR:

1. Add the managed host (for example, hostname `Host1, Host2`), which is running the workload, to the KSYS subsystem by running the following commands:

   ```
   ksysmgr add host <Host1> site=<Site1>
   ksysmgr add host <Host2> site=<Site1>
   ```

2. Add the backup host (for example, hostname `Host3`), which acts as a backup host, to the KSYS subsystem by running the following command:

   ```
   ksysmgr add host <Host3> site=<Site2>
   ```

6.2.6 Adding a storage agent

After adding hosts to the KSYS subsystem, you must add storage agents to the KSYS subsystem. For different types of storage systems, the parameters for adding a storage agent might be different. For more information about the different storage types, see 9.4, “Configuring VMRM HA by using the GUI” on page 245.

To add a storage agent, run the following command:

```
ksysmgr add storage_agent <name> hostname|ip=<storage> login=<username>
password=<password> type=<type of storage> serialnumber=<storage_serialnumber>
site=<site_name>
```

6.2.7 Creating a host group

You can group a set of hosts based on your business requirements. For example, you can group the hosts that run similar types of workloads. You also can group important hosts so that the monitoring and recovery operations can be performed for a set of hosts together and quickly. In disaster situations, you can move a host group separately to the backup site.

Here are the guidelines to manage host groups*:*

- A host already must be added to the KSYS configuration settings and the host must be paired with a backup host at the backup site.
- Each host in a site must be a part of a host group. If a host is not added to any host groups, the host is automatically added to the Default_HG host group during the discovery operation.
- If you add or remove hosts from a host group, you must run a discovery operation to manage or unmanage all the VMs from the recovery management. The modified host group displays the correct list of managed VMs only after a discovery operation.
- If we remove all hosts from Default_HG, the disk group corresponding to Default_HG is not removed. The disk groups are retained with the removed hosts.
- The corresponding hosts in the backup site that are paired with the active site hosts are grouped logically within the same host group. For example, if host1 at the active site is paired with host2 at the backup site and you create a host group hg1 with host1, then host2 automatically is added to the host group hg1.
- Each host group must be associated with a separate disk group. The disks in the disk group must not be shared among different host groups. The disk groups are named by using the following format:

  ```
  VMRDG_{peer_domain_name}_{site_name}_{host_group_ID}
  ```

  However, the disk group name must not exceed the maximum number of characters that is supported for a consistency group (CG) at the storage level.
- For IBM SAN Volume Controller and IBM DS8000 Storage Systems, host groups can span across a single type of storage. Multiple host groups can use same type of storage disks, but the disks must not be shared among different host groups.

To create a host group, complete the following steps:

1. Identify the available disks that you can designate as the repository disk and the high availability (HA) disk for the SSP cluster on the home site in the same way as for VMRM HADR by running the following command for the VIOSs, which are part of the host group on the home site:

   ```
   ksysmgr query viodisk vios=VIOS1,VIOS2,VIOS3,VIOS4
   ```

2. Identify the available `ha_disk` and `repo_disk` by using the **`ksysmgr query vios`** command at the backup site. You can use the **`modify host_group option`** after creating the host group to add the backup site's SSP disks.

   ```
   ksysmgr query viodisk vios=VIOS5,VIOS6,VIOS7,VIOS8 site=sitename
   ```

3. You can create symmetric or asymmetric host group and add the existing hosts to it:

   – Symmetric host group

     Before creating a symmetric host group, you must create host pairs. After the hosts are added to the KSYS subsystem, identify the hosts that must be paired across the active site and the backup site. Each backup host in the host pair must meet all the resource requirements so that the backup host can run the same workload in a disaster or a potential disaster situation. Pair the identified host (for example, hostname: `Host1, Host3`) in the active site to the identified host (for example, hostname: `Host2, Host4`) in the backup site by running the following commands:

     ```
     ksysmgr pair host Host1 pair=Host2
     ksysmgr pair host Host3 pair=Host4
     ```

     Now, to create a symmetric host group (for example, host group name: `Host_group1`, ha_disk: `SSP_disk1`, repo_disk: `SSP_disk2`), run the following command:

     ```
     ksysmgr add host_group Host_group1 hosts=Host1,Host3 ha_disk=SSP_disk1
     repo_disk=SSP_disk2
     ```

     Note: After you add one host from the host-pair to a host group, the other host of the host-pair automatically is added to the respective host group in the other site. These hosts form a symmetric host group, which contains one-to-one paired hosts.

   – Asymmetric host group

     To create an asymmetric host group (for example, host group name: `Host_group1`, HA disk: `SSP_disk1`, repo_disk: `SSP_disk2`) and add the existing hosts (for example, hosts: `Host1`, `Host2`, `Host3`, `Host4`, `Host5`) to the asymmetric host group, run the following command:

     ```
     ksysmgr add host_group Host_group1 hosts=Host1,Host2,Host3,Host4,Host5
     mxn_pairing=yes ha_disk=SSP_disk1 repo_disk=SSP_disk2
     ```

     Note: By default, the **`mxn_pairing`** attribute is set to `no`. To create an asymmetric host group, which contains one-to-many paired hosts, set the **`mxn_pairing`** attribute to `yes`. Do not pair the hosts before adding the hosts to the host group. Specify the host and host-group pair of all hosts manually.

6.2.8 Adding ha_disk and repo_disk at the backup site to the host group

You can use the **`modify host_group option`** after creating the host group to add the backup site's SSP disks:

```
ksysmgr modify host_group Host_group1 options ha_disk=Backup_site_SSP_disk1
repo_disk=Backup_site_SSP_disk2 site=Backup_sitename
```

6.2.9 Unmanaging VMs

You might not want VMRM to manage all the VMs or VIOSs in your environment. You can unmanage VMs or VIOSs by running the appropriate command:

- To unmanage VIOSs, run the following command:

```
ksysmgr unmanage vios <viosname[,...]>
```

- To unmanage VMs, run the following command:

```
ksysmgr unmanage vm
   name=<vmname> host=<hostname> | uuid=<lparuuid> | ALL host=<hostname> | ALL
   host_group=<host_group_name>
```

Note: If you are planning to manage only a few of the VMs in the managed hosts, you can use the **ALL** option of the unmanage command. Then, after all the VMs are unmanaged, you can add the VMs that you want to be managed by using the **ksysmgr manage vm** command. The command syntax is as follows:

```
ksysmgr manage vm
   name=<vmname> host=<hostname> | uuid=<lparuuid> | ALL host=<hostname> | ALL
   host_group=<host_group_name>
```

6.2.10 Modifying any attributes

For VMRM HA or VMRM DR, some attributes or parameters might need to be changed for your environment. These changes can be made now or later. If you choose to change these attributes later, run the KSYS discovery and verify operations after you make any changes. The attributes that can be changed are described in 3.5, “Setting up HA policies” on page 78 and 4.7, “Managing and administering VMRM DR” on page 144.

6.2.11 Discovering and verifying

Now, you put everything together and activate the functions by running the discovery and verification functions. Run these operations after any changes are made to the VMRM environment. You can run the KSYS discovery and verify operations at the site level or host group level.

Complete the following steps:

1. To perform the discovery and verify operations at the site level, run the following command:

   ```
   ksysmgr discover site Austin verify=yes
   ```

2. To perform the discovery and verify operations for a specific host group, run the following command:

   ```
   ksysmgr discover host_group hg_name verify=true
   ```

3. To perform the discovery and the DR-only verify operations for a specific host group, run the following command:

   ```
   ksysmgr discover host_group hg_name verify=true option=DRonly
   ```

After the discovery and verify operations complete, you have completed configuring the VMRM HADRHA environment.

6.2.12 Installing virtual machine agents

To help manage AIX and Linux VMs, you might want to install the agents in those VMs, as described in 7.1, “Installing VM Agents” on page 200.

6.2.13 Example configuration

Example 6-1 displays the commands that are used to create a VMRM HADRHA environment in our lab. This environment has the following components:

- Two KSYS LPARs
- Two HMCs at the home site
- One HMC at the backup site
- Four hosts at the home site
- Two hosts at the backup site
- Two IBM XIV Storage Systems, one at each site
- Four managed VMs

Example 6-1 Command sequence for deploying a VMRM HADRHA environment

```
ksysmgr add ksyscluster HADRHA_TEST\
   ksysnodes=ksys913.ausprv.stglabs.ibm.com,ksys907.aus.stglabs.ibm.com\
   type=HADRHA

ksysmgr add site India sitetype=home
ksysmgr add site Austin sitetype=backup

ksysmgr add hmc gdrhmc8 site=India login=hscroot\
   hostname=gdrhmc8.aus.stglabs.ibm.com

ksysmgr add hmc e17vhmc2 site=India login=hscroot\
   hostname=e17vhmc2.aus.stglabs.ibm.com

ksysmgr add hmc gdrhmc3 site=Austin login=hscroot\
   hostname=gdrhmc3.aus.stglabs.ibm.com

ksysmgr add host Yin-8247-42L-211E9DA site=India
ksysmgr add host Yang-8286-42A-101417V site=India
ksysmgr add host p9zzrt site=India
ksysmgr add host jrainier1-9105-42A_783C431 site=India
ksysmgr add host e17bass-8247-22L-2133A6A site=Austin
ksysmgr add host coat_8286-42A-SN21009DW site=Austin

ksysmgr add storage_agent XIV106 login=admin site=India serialnumber=1310106\
   storagetype=XIV hostname=9.xxx.xxx.xxx

ksysmgr add storage_agent XIV141 login=admin site=Austin serialnumber=1310141\
   storagetype=XIV hostname=9.xxx.xxx.xxx

ksysmgr q viodisk\
   vios=yangv2,yinv2,yinv1,yangv1,zzrtv1,zzrtv2,jrainier1v1,jrainier1v2

ksysmgr add hg HG1\
hosts=Yang-8286-42A-101417V,Yin-8247-42L-211E9DA,p9zzrt,jrainier1-9105-42A_783C431
,e17bass-8247-22L-2133A6A,coat_8286-42A-SN21009DW
ha_disk=01MOlCTTIxNDU2MDA1MDc2ODAyODIxMjQ1MzAwMDAwMDAwMDAwMENCRA==
repo_disk=01M0lCTTIxNDU2MDA1MDc2ODAyODIxMjQ1MzAwMDAwMDAwMDAwMENERg==
mxn_pairing=yes

ksysmgr q viodisk vios=coatv1,coatv2,e17bassv1,e17bassv2 site=Austin

ksysmgr modify hg HG1 options
ha_disk=01M0lCTTIxNDUxMjQ2MDA1MDc2ODAyOTYwQ0QwMzgwMDAwMDAwMDAwMDkwMQ==
repo_disk=01M0lCTTIxNDUxMjQ2MDA1MDc2ODAyOTYwQ0QwMzgwMDAwMDAwMDAwMDkwMg==
site=Austin

ksysmgr unmanage vm ALL host_group=HG1
ksysmgr manage vm yin001
ksysmgr manage vm yin002
ksysmgr manage vm yin008
ksysmgr manage vm yin009
ksysmgr modify system ha_monitor=enable
ksysmgr  discover site India verify=yes
```

Example 6-2 shows that the KSYS cluster type is HADRHA. It shows that there are two KSYS nodes in this environment.

Example 6-2 HADRHA VMRM environment

```
# ksysmgr q cluster
Name:                HADRHA_TEST
State:               Online
Type:                HADRHA
Ksysnodes:           ksys907.aus.stglabs.ibm.com:2:Online
                     ksys913.ausprv.stglabs.ibm.com:1:Online    (Managing node)
```

Example 6-3 displays the host group information. You can see the two SSP names and the `repo_disks` and `ha_disks` on each site.

Example 6-3 The host group information

```
# ksysmgr q hg
Name:                HG1
Home Site Hosts:     jrainier1-9105-42A_783C431
                     Yin-8247-42L-211E9DA
                     p9zzrt
                     Yang-8286-42A-101417V
Backup Site Hosts:   coat_8286-42A-SN21009DW
                     e17bass-8247-22L-2133A6A
Memory_capacity:     Priority-Based Settings
                     low:100
                     medium:100
                     high:100
CPU_capacity:        Priority-Based Settings
                     low:100
                     medium:100
                     high:100
Skip_power_on:       None
Sriov_override:      No
Site:                India
Vswitchmap:          Not currently set
Vlanmap:             Not currently set
```

```
DrVswitchmap:        Not currently set
DrVlanmap:           Not currently set
HA_monitor:          enable
Lpm_support:         None
Proactiveha:         disable
Restart_policy:      auto
VM_failure_detection_speed:    normal
Host_failure_detection_time:   90
Type:                asymmetric
Custom CG Name:
Backup Site CG Name:

SSP Clusters Attributes
Sspname:             KSYS_HADRHA_TEST_1_1
Sspstate:            UP
Ssp_version:         VIOS 3.1.4.10
VIOS:                jrainier1v2
                     jrainier1v1
                     yinv2
                     yinv1
                     zzrtv2
                     zzrtv1
                     yangv2
                     yangv1
Repo_disk:           01M0lCTTIxNDU2MDA1MDc2ODAyODIxMjQ1MzAwMDAwMDAwMDAwMENERg==
HA_disk:             01M0lCTTIxNDU2MDA1MDc2ODAyODIxMjQ1MzAwMDAwMDAwMDAwMENCRA==
Ssp_site:            India

Sspname:             KSYS_HADRHA_TEST_1_2
Sspstate:            UP
Ssp_version:         VIOS 3.1.4.10
VIOS:                coatv1
                     coatv2
                     e17bassv1
                     e17bassv2
Repo_disk:
01M0lCTTIxNDUxMjQ2MDA1MDc2ODAyOTYwQ0QwMzgwMDAwMDAwMDAwMDkwMg==
HA_disk:
01M0lCTTIxNDUxMjQ2MDA1MDc2ODAyOTYwQ0QwMzgwMDAwMDAwMDAwMDkwMQ==
Ssp_site:            Austin
```

Example 6-4 displays the information of the VMs that are managed in the VMRM HADRHA environment.

Example 6-4 Managed VMs in the VMRM HADRHA environment

```
# ksysmgr q vm state=manage
Managed VMs:HADRHA
        yin001
        yin009
        yin002
        yin008

All Managed VMs:
Name:                yin001
UUID:                285AF45C-224B-4A76-A126-CD48FD86C76D
```

```
DRState:             READY
HAState: READY_TO_MOVE
Dr Test State:       INIT
Host:                jrainier1-9105-42A_783C431
Priority:            Medium
Skip_power_on:       None
VM_failure_detection_speed:    normal
HA_monitor:          disable
Proactiveha:         disable
Homehost:            jrainier1-9105-42A_783C431
BackupSiteHomehost:  none
VM_status:           NO_OPERATION_IN_PROGRESS
Version_conflict:    No
DrTargetHost:        coat_8286-42A-SN21009DW
AppMessaging:        enable
Active Pool:         DefaultPool
PoolMap:             None

LPM Validation Status
LPM validation was successful for Hosts:
        Yin-8247-42L-211E9DA
        Yang-8286-42A-101417V
LPM validation failed for Hosts:
        p9zzrt

Name:                yin002
UUID:                3DF30F3A-26EC-44E4-B2DE-7881C5CE72B6
DRState:             READY
HAState:             READY
Dr Test State:       INIT
Host:                jrainier1-9105-42A_783C431
Priority:            Medium
Skip_power_on:       None
VM_failure_detection_speed:    normal
HA_monitor:          disable
Proactiveha:         disable
Homehost:            jrainier1-9105-42A_783C431
BackupSiteHomehost:  none
VM_status:           NO_OPERATION_IN_PROGRESS
Version_conflict:    No
DrTargetHost:        e17bass-8247-22L-2133A6A
AppMessaging:        enable
Active Pool:         DefaultPool
PoolMap:             None

LPM Validation Status
LPM validation was successful for Hosts:
        Yin-8247-42L-211E9DA
        Yang-8286-42A-101417V
LPM validation failed for Hosts:
        p9zzrt

Name:                yin008
UUID:                3FD7CBF8-8FF3-44C6-8ECC-BB5C9A1E0A99
DRState:             READY
```

```
HAState:             READY
Dr Test State:       INIT
Host:                Yin-8247-42L-211E9DA
Priority:            Medium
Skip_power_on:       None
VM_failure_detection_speed:    normal
HA_monitor:          disable
Proactiveha:         disable
Homehost:            Yin-8247-42L-211E9DA
BackupSiteHomehost:  none
VM_status:           NO_OPERATION_IN_PROGRESS
Version_conflict:    No
DrTargetHost:        e17bass-8247-22L-2133A6A
AppMessaging:        enable
Active Pool:         DefaultPool
PoolMap:             None

LPM Validation Status
LPM validation was successful for Hosts:
        p9zzrt
        Yang-8286-42A-101417V
LPM validation failed for Hosts:
        jrainier1-9105-42A_783C431

Name:                yin009
UUID:                3D78FF61-91B7-4D92-8048-C5ECCB26AC1B
DRState:             READY
HAState:             READY
Dr Test State:       INIT
Host:                Yin-8247-42L-211E9DA
Priority:            Medium
Skip_power_on:       None
VM_failure_detection_speed:    normal
HA_monitor:          disable
Proactiveha:         disable
Homehost:            Yin-8247-42L-211E9DA
BackupSiteHomehost:  none
VM_status:           NO_OPERATION_IN_PROGRESS
Version_conflict:    No
DrTargetHost:        coat_8286-42A-SN21009DW
AppMessaging:        enable
Active Pool:         DefaultPool
PoolMap:             None

LPM Validation Status
LPM validation was successful for Hosts:
        jrainier1-9105-42A_783C431
        p9zzrt
        Yang-8286-42A-101417V
```

6.3 Limitations

The following limitations apply when working with high availability and disaster recovery (HADR) and HADRHA deployment types of VMRM:

- VMRM DR has a workgroup option. However, it is not supported in the VMRM HADR or HADRHA environments.
- When you manually shut down or restart a VM, the dependent applications are not affected. The recovery of dependent applications is considered only when failure occurred with the parent application, the VM, or the host.
- Remove the default host group (Default_HG) before configuring the HADR and HADRHA types of deployment with PowerHA SystemMirror. To remove the default host group from the KSYS subsystem, run the following command:

  ```
  rmrsrc -s "Name='Default_HG'" IBM.VMR_HG
  ```

- Disable the quick discovery feature before running the Live Partition Mobility (LPM) and restart operations on VMs.

6.4 Managing the VMRM HADRHA environment

The management of the VMRM HADR environment is the same as what is documented in Chapter 3, “Planning and deploying IBM VMRM HA” on page 43 and Chapter 4, “Planning and deploying IBM VMRM DR” on page 93.

6.4.1 Installing GUI file sets

To use VMRM DR and manage KSYS nodes by using the GUI, you must install the GUI server and GUI agent file sets on a system. The LPAR in which you want to install the GUI file set must be running IBM AIX 7.2 with Technology Level 2 Service Pack 1 (7200-02-01) or later. You can choose to install the GUI server and GUI agent file sets on one of the KSYS nodes. For more information about installing the GUI, see Chapter 9, “IBM VMRM GUI deployment” on page 237.

7

Common tasks across the IBM VMRM family

IBM Virtual Machine Recovery Manager (VMRM) is a group of solutions based on a common management infrastructure. There are many tasks that are common across each of the VMRM solutions:

- VMRM High Availability (HA) (VMRM HA)
- VMRM Disaster Recovery (DR) (VMRM DR)
- VMRM HADR
- VMRM HADRHA

The following topics are described in this chapter:

- Installing VM Agents
- Setting up the VM Agent
- Uninstalling VM Agents
- Setting contacts for event notification
- Backing up and restoring the configuration data

7.1 Installing VM Agents

VM Agents are components that are installed in virtual machines (VMs) or logical partitions (LPARs). These optional agents offer robust monitoring of the VMs and applications that are running in VMs. You can manage HA applications in VMs by using a lightweight application monitoring framework (AppMon).

7.1.1 Installing a VM Agent in an AIX VM

To install a VM Agent in an AIX VM, complete the following steps:

1. Run the following command in the AIX VM, as shown in Example 7-1.

Example 7-1 Installing a VM Agent in an AIX VM

```
# installp -acFXYd . -V2 ksys.vmmon.rte
```

2. To verify whether the installation of VM Agent is successful, run the **lslpp** command, as shown in Example 7-2.

Example 7-2 Checking the VM Agent installation

```
# lslpp -l ksys.vmmon.rte
  File set                      Level  State      Description
  ----------------------------------------------------------------------------
Path: /usr/lib/objrepos
  ksys.vmmon.rte             1.7.0.0  COMMITTED  Base Server Runtime

Path: /etc/objrepos
  ksys.vmmon.rte             1.7.0.0  COMMITTED  Base Server Runtime
```

3. Ensure that the **ksysvmmgr** command installed correctly by using the command that is shown in Example 7-3.

Example 7-3 Checking ksysvmmgr

```
# /usr/sbin/ksysvmmgr
Usage: ksysvmmgr [<FLAGS>] <ACTION> [<CLASS>] [<NAME>] [<ATTRIBUTES>]
KSYSVMMGR-002(ERROR): <ACTION> parameter is mandatory.
 For <ACTION> parameter, possible actions are:
"add,query,modify,delete,status,resume,suspend,start,stop,help,refresh,backup,rest
ore,snap,sync".
 Retry by using one of the possible actions.
Or refer to complete output of "ksysvmmgr -h"

#ksysvmmgr query vmm
VmMonitor
 log=2
 period=1
 version=1.7.0.0
 comment=2023-01-03 09:55:28
```

4. Ensure that the binary file for the VM Agent daemon is installed correctly by using the command that is shown in Example 7-4.

Example 7-4 Checking the binary file of the VM Agent daemon

```
# /usr/sbin/ksys_vmmd
0513-095 The request for subsystem refresh was completed successfully.
```

5. To verify whether the VM Agent daemon is enabled, run the **`lssrc -s ksys_vmm`** command. The status of the `ksys_vmm` subsystem must be `Active` in the output of this command, as shown in Example 7-5.

Example 7-5 Checking the agent daemon

```
# lssrc -s ksys_vmm
Subsystem         Group            PID          Status
 ksys_vmm                          9699654      active
```

7.1.2 Installing a VM Agent in a Linux VM

To install the VM Agent Red Hat Package Manager (RPM) packages in a Linux VM, complete the following steps:

1. Ensure that the following Reliable Scalable Cluster Technology (RSCT) packages are installed in the Linux VM:

   - `rsct.core`
   - `rsct.opt.storagerm`
   - `rsct.core.utils`
   - `rsct.basic`
   - `DynamicRM`

   Example 7-6 shows the command and expected output.

Example 7-6 Listing the RSCT packages

```
# rpm -qa | egrep "rsct|Dynamic"
rsct.basic-3.3.0.3-22237.ppc64le
rsct.core-3.3.0.3-22237.ppc64le
DynamicRM-2.0.7-7.ppc64le
rsct.opt.storagerm-3.3.0.3-22237.ppc64le
rsct.core.utils-3.3.0.3-22237.ppc64le
```

Note: You can download the packages from Service and productivity tools.

For more information about configuring the repository to easily install those packages, see IBM Documentation.

2. Install the VM Agent RPM packages based on the following Linux distributions in the VM:
   - In Red Hat Enterprise Linux (RHEL) (Little Endian) VMs, run the command that is shown in Example 7-7.

Example 7-7 Installing a VM Agent in a Red Hat Enterprise Linux VM

```
# rpm -ivh vmagent-1.7.0-1.0.el7.ppc64le.rpm
Preparing...                          ################################# [100%]
Updating / installing...
   1:vmagent-1.7.0-1.0.el7            ################################# [100%]
Starting ksys_vmm daemon.
```

Ensure that the Resource Monitoring and Control (RMC) connection between the VMs and HMC exists. If the firewall is enabled on the RHEL VM, the RMC connection might be broken. Modify the firewall on the VMs to enable the RMC connection with the HMC by using the commands that are shown in Example 7-8.

Example 7-8 Modifying a firewall in Red Hat Enterprise Linux

```
# firewall-cmd --zone=public --permanent --add-port=657/tcp
# firewall-cmd --zone=public --permanent --add-port=657/udp
# firewall-cmd --reload
# systemctl <start|stop|status> firewalld
```

   - In SUSE Linux Enterprise Server (Little Endian) VMs, run the command that is shown in Example 7-9.

Example 7-9 Installing a VM Agent in SUSE Linux Enterprise Server

```
# rpm -ivh vmagent-1.7.0-1.0.suse123.ppc64le.rpm
Preparing...                          ################################# [100%]
Updating / installing...
   1:vmagent-1.7.0-1.0.suse123        ################################# [100%]
Starting ksys_vmm daemon.
ksys_vmm has been started.
```

7.2 Setting up the VM Agent

If you configure the HA function at the VM level or application level, you must set up the VMM and the AppMon in each VM for which VM failure detection is required.

You can install the VM Agent to monitor the VM and applications on the VMs only on the following operating systems:

- AIX 6.1 or later
- IBM PowerLinux:
   - RHEL (Little Endian) Version 7.4 or later
   - SUSE Linux Enterprise Server (Little Endian) Version 12.3 or later

Currently, the VM Agent that provides VM-level or application-level monitoring is not supported for the IBM i operating system or other Linux distributions. However, you can enable these VMs for host-level health management. In addition, you can perform manual restart and Live Partition Mobility (LPM) operations on these VMs.

Note: You can configure the VM Agent only by using the **ksysvmmgr** command. You *cannot* configure the VM Agent by using the VMRM HA GUI.

7.2.1 The ksysvmmgr command and utility

The **ksysvmmgr** command (Figure 7-1) provides a consistent interface to manage the VM monitor (VMM) and applications. The **ksysvmmgr** command interacts with the VMM daemon over a UNIX socket.

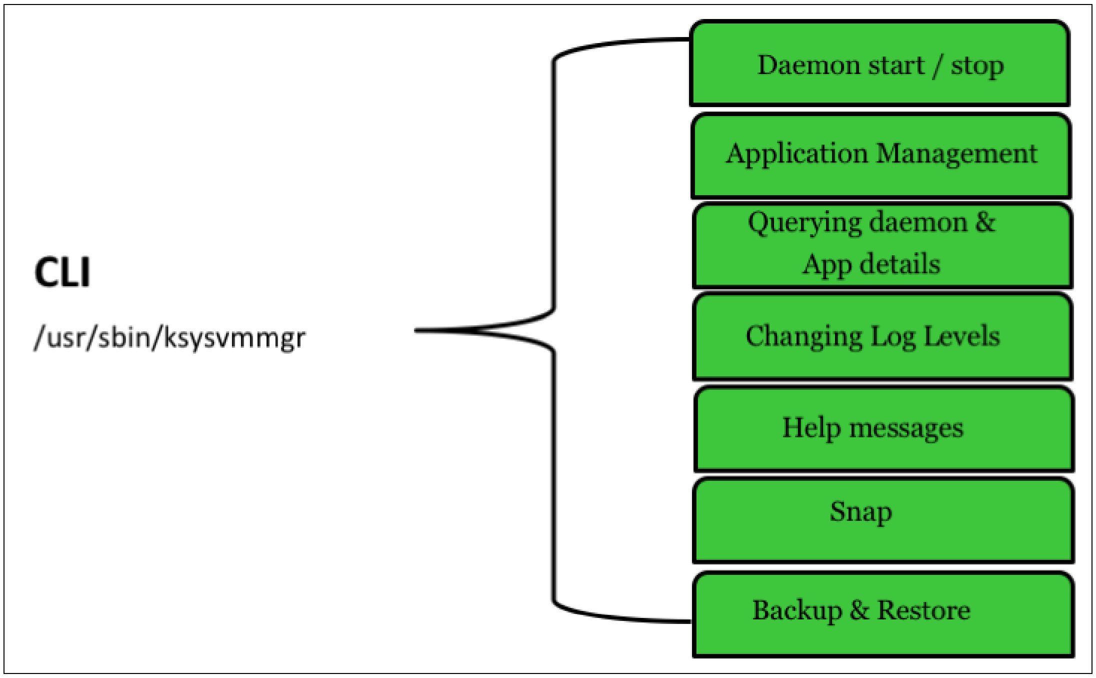


Figure 7-1 The ksysvmmgr command

Example 7-10 shows the **ksysvmmgr** command syntax.

Example 7-10 The ksysvmmgr command syntax

```
# ksysvmmgr
Usage: ksysvmmgr [<FLAGS>] <ACTION> [<CLASS>] [<NAME>] [<ATTRIBUTES>]
KSYSVMMGR-002(ERROR): <ACTION> parameter is mandatory.
 For <ACTION> parameter, possible actions are:
"add,query,modify,delete,status,resume,suspend,start,stop,help,start,stop,status,s
ync".
 Retry by using one of the possible actions.
Or refer to complete output of "ksysvmmgr -h"
```

After you install the VM Agent file sets successfully, complete the procedures in the following sections to set up the VMM in each guest VM.

VMM daemon

The VMM daemon must be started in each VM in which that agent is installed. To start monitoring the VMs and applications, run the command that is shown in Example 7-11.

Example 7-11 Starting the VMM daemon

```
# ksysvmmgr start
0513-059 The ksys_vmm Subsystem has been started. Subsystem PID is 6488526.

# ksysvmmgr status
Subsystem         Group            PID          Status
 ksys_vmm                          6488526      active
```

VM monitor

The **ksysvmmgr** command configures the classes and attributes, as shown in Example 7-12.

Example 7-12 Listing the VMM details

```
# ksysvmmgr query vmm
VmMonitor
 log=2
 period=1
 version=1.0
 comment=2018-10-26 16:02:11
 rebootappstarttype=VMM
 VmUUID=3bf44186-0679-4032-bf4c-95b24901822
```

When you start the VMM, the VMM daemon sends heartbeats to the host monitor (HM) when they are requested by the HM so that the KSYS subsystem can monitor the VMs.

The VMM can have the following attributes:

version Specifies the version of XML. This mandatory attribute is set to `1.0` for the current version of VMM and cannot be modified.

log Specifies the log level of the VMM daemon. This attribute can have the following values:

- `0` Only errors are logged. It is the default value.
- `1` Warnings also are logged.
- `2` Informational messages also are logged.
- `3` Details of the operation are logged. This information is used for debugging.

period Specifies the time duration in seconds between two consecutive occurrences of checks that are performed by the Application Management Engine (AME). By default, the value of this attribute is 1 second. The value of this attribute must be in the range 0 - 6. For best monitoring performance, do not modify the default value.

rebootappstarttype Specifies the method in which the applications must be started when the VM is restarted on a new host. This attribute can have the following values:

- `VMM` Directs the VM Agent to start the applications immediately after the VM is restarted on the new host.

OS Specifies that the applications must be started by the operating system or by a user after the VM restarts on a new host. If the application is not started by the operation system or a user, the VM Agent starts the applications.

To modify the VMM parameters, run the following commands:

- **# ksysvmmgr modify log=3**
- **# ksysvmmgr modify period=2**
- **# ksysvmmgr modify rebootappstarttype=OS**

7.2.2 Application Management Engine

The AME validates the application monitoring configuration, starts and stops applications, monitors application health, restarts applications in there is a failure, and informs the Application Reporting (AR) thread about the application configuration and status.

To register applications in the VMM daemon so that they are monitored for HA, run the command that is shown in Example 7-13.

Example 7-13 Adding an application to be monitored by AME

```
# ksysvmmgr -s add app app1 monitor_script=/applic/mon1.sh
start_script=/applic/start_app1.sh stop_script=/applic/stop_app1.sh
Adding application "app1" into configuration successfully performed.
```

To check the attributes of all applications, run the command **ksysvmmgr query app**, as shown in Example 7-14.

Example 7-14 Checking the attributes of all applications

```
# ksysvmmgr query app
Application name=app1
 version=
 uuid=1542231184972777000
 desc=
 monitored=1
 monitor_script=/applic/mon1.sh
 monitor_period=30
 monitor_timeout=15
 monitor_failure_threshold=5
 stop_script=/applic/stop_app1.sh
 stop_stabilization_time=25
 stop_max_failures=3
 start_script=/applic/start_app1.sh
 start_stabilization_time=25
 start_max_failures=3
 max_restart=3
 nooftimes_restarted=0
 critical=no
 type=
 instancename=
 database=
 vendor_id=
 status=NORMAL (GREEN)
```

After you add an application, if the application fails or stops working correctly, the VM Agent attempts to restart the application in the same VM for the number of times that is specified in the **max_restart** attribute for the VM, which is set to 3 by default. If the application is still not working correctly, the KSYS subsystem notifies you about the issue. You can manually review the problem and restart the application.

Mark important applications as critical by running the command that is shown in Example 7-15.

Example 7-15 Marking important applications as critical

```
# ksysvmmgr -s modify app app1 critical=yes
Modifying application "app1" into configuration successfully performed.
```

When you mark an application as critical and the application fails or stops working correctly, the VM Agent attempts to restart the application for the number of times that is specified in the **max_restart** attribute for the VM. If the application is still not working correctly, the KSYS subsystem notifies you about the issue and attempts to restart the VM on the same host. If the application is still not working correctly, that is, if the application status is displayed as RED when you run the **ksysmgr query app** command, the KSYS restarts the VM on another host within the host group based on the specified policies.

Application class

The application class contains the following mandatory attributes:

- **monitor_script**: A mandatory script that is used by the VM Agent to verify application health. This script is run regularly (based on the **monitor_period** attribute value) and the result is checked for the following values:
  - 0: Application is working correctly.
  - Any value other than 0: Application is not working correctly or failed.

  After several successive failures (based on the **monitor_failure_threshold** attribute value), the application is declared as failed. Based on the specified policies, the KSYS subsystem determines whether to restart the VM.
- **stop_script**: A mandatory script that is used by the VM Agent to stop the application if the application must be restarted.
- **start_script**: A mandatory script that is used by the VM Agent to start the application if the application must be restarted.

The application class contains the following optional attributes:

- **monitored**: Specifies whether the application is monitored by the KSYS subsystem. This attribute can have the following values:
  - 1 (default): The application monitoring is active.
  - 0: The application monitoring is suspended.
- **monitor_period**: Specifies the time in seconds after which the application monitoring must occur. The default value of 30 seconds specifies that the **monitor_script** script is run by the VM Agent every 30 seconds.
- **monitor_timeout**: Specifies the waiting time in seconds to receive a response from the **monitor_script** script. The default value is 10 seconds, which means that the VMM waits for 10 seconds to receive a response from the **monitor_script** script, after which the script is considered as failed.

- **monitor_failure_threshold**: Specifies the number of successive failures of the **monitor_script** script that is necessary before the VMM restarts the application. A restart operation is performed by successively calling the **stop_script** and **start_script** scripts.
- **stop_stabilization_time**: Specifies the waiting time in seconds to receive a response from the **stop_script** script. The default value is 25 seconds, which means that the VMM waits for 25 seconds to receive a response from the **stop_script** script, after which the script is considered as failed.
- **stop_max_failures**: Specifies the number of successive failures of the **stop_script** script that is necessary before the VMM considers that it cannot stop the application. The default value is set to 3.
- **start_stabilization_time**: Specifies the waiting time in seconds to receive a response from the **start_script** script. The default value is 25 seconds, which means the VMM waits for 25 seconds to receive a response from the **start_script** script, after which the script is considered as failed.
- **start_max_failures**: Specifies the number of successive failures of the **start_script** script that is necessary before the VMM considers that it cannot start the application. The default value is set to 3.
- **max_restart**: Specifies the number of cycles of successive VM restart operations that result in a monitoring failure before the daemon pronounces that restarting at VM level is insufficient. By default, this attribute is set to 3.
- **status**: Specifies the dynamic status of application that is returned by AME. This attribute cannot be modified.
- **version**: Specifies the application version. This attribute does not have a default value.
- **critical**: Marks the application as critical. The valid values are Yes and No (default). If you mark an application as critical, the failure of the application is sent to the KSYS subsystem for further action.
- **type**: Specifies the type of application. By default, the **type** attribute does not have any value that indicates general applications. Other supported values are ORACLE, IBM DB2, and SAPHANA. This attribute is case-sensitive and you must use uppercase characters. For these types of applications, if you do not specify start, stop, and monitor scripts, internal scripts of the VMM are used.
- **instancename**: Specifies the instance name for applications. This attribute is applicable only for applications whose scripts need an instance name as an argument. For example:
  - If the application type is ORACLE, the **instancename** attribute must be specified with the Oracle instance name.
  - If the application type is DB2, the **instancename** attribute must be specified with the IBM Db2 instance owner.
  - If the application type is SAPHANA, the **instancename** attribute must be specified with the SAP HANA instance name.
- **database**: Specifies the database that the applications must use. This attribute is applicable only for applications whose scripts require **database** as an argument.
  For example:
  - If the application type is ORACLE, the **database** attribute must be specified with the Oracle system identifier (SID).
  - If the application type is DB2, the **database** attribute is not required.
  - If the application type is SAPHANA, the **database** attribute must be specified with the SAP HANA database.

VMRM HA built-in scripts

Apart from any general application that you want the VM Agent to monitor, the VMRM HA solution supports applications that can be monitored by using the built-in scripts in the corresponding versions of operating systems, as shown in the Table 7-1.

Table 7-1 Version support matrix for application types and operating systems

Application type	AIX operating system	Linux operating system (RHEL and SUSE Linux Enterprise Server)
Oracle	Oracle Database 12.1 or later	Not supported
Db2	IBM Db2 11.3 or later	IBM Db2 10.5 or later
SAPHANA	Not supported	SAP HANA 2.0 or later

Specific parameters for built-in supported application agents are shown in Table 7-2.

Table 7-2 Application agent-specific parameters

Attribute	Oracle	IBM Db2	SAP HANA
`type`	Oracle	Db2	SAPHANA
`version`	Taken from application	Taken from application	Taken from application
`database`	Oracle SID	Db2 database	SAP HANA database
`start_script`	`/usr/sbin/agents/oracle/startoracle`	`/usr/sbin/agents/db2/stopdb2`	`/usr/sbin/agents/sap/startsaphana`
`stop_script`	`/usr/sbin/agents/oraclestartoracle`	`/usr/sbin/agents/db2/stoporacle`	`/usr/sbin/agents/sap/stopsaphan`

Application dependencies

If some applications have dependencies, for example, if you must specify a sequence of applications to start or stop, specify the dependencies, as shown in Figure 7-2.

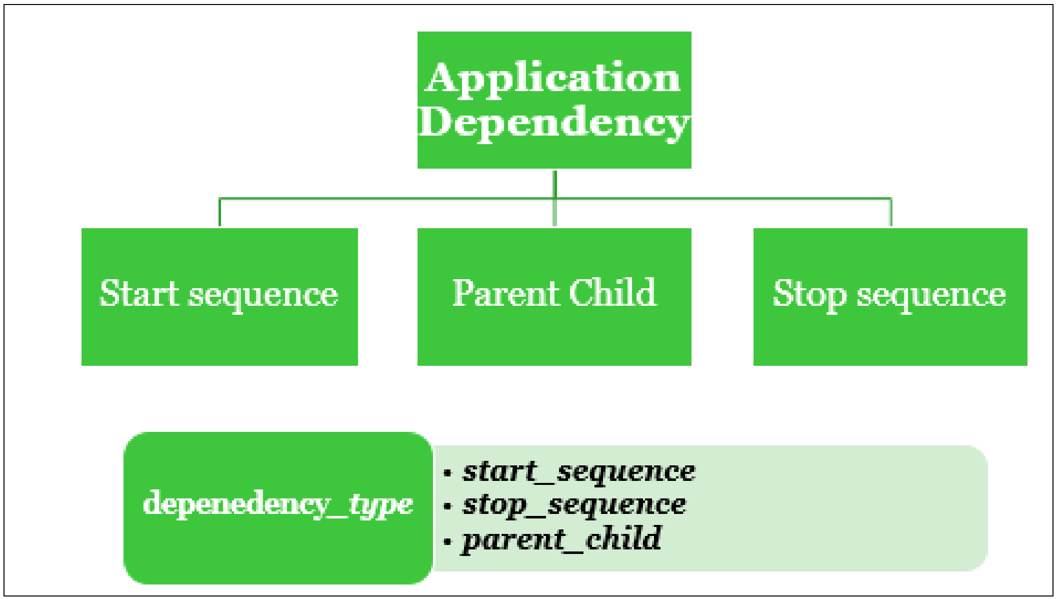


Figure 7-2 Application dependencies

The start_sequence application dependency

This policy defines the order in which the applications start.

The stop_sequence application dependency

This policy defines the order in which the applications must be stopped.

In Example 7-16, the dependencies type **start_sequence** and **stop_sequence** were added to applications app1, app2, and app3.

Example 7-16 Adding start_sequence dependencies

```
# ksysvmmgr -s add dependency dependency_list=app1,app2,app3
dependency_type=start_sequence
Adding dependency "dependency_list=app1,app2,app3" into configuration successfully
performed.

# ksysvmmgr -s add dependency dependency_list=app1,app2,app3
dependency_type=stop_sequence
Adding dependency "dependency_list=app1,app2,app3" into configuration successfully
performed.
```

Example 7-17 uses the command **ksysvmmgr q dependency** to list the dependencies.

Example 7-17 Listing dependencies after the start_sequence and stop_sequence dependencies

```
# ksysvmmgr q dependency
Dependency depuuid=1542239347575681000
 dependency_type=start_sequence
 dependency_list=app1,app2,app3
 strict=YES
Dependency depuuid=1542239435934976000
 dependency_type=stop_sequence
 dependency_list=app1,app2,app3
 strict=YES
```

The parent_child application dependency

This policy defines the **parent_child** dependency between the applications.

Only one level of **parent_child** dependency is allowed:

- In this policy, if App1 is the parent and App2 is the child, App1 starts first.
- If App1 cannot start, App2 does not start.
- If App1 and App2 start in order and App1 stops because of any reason, App2 stops. App1 must be restarted, and then App2 is restarted.

In Example 7-18, the dependency **parent_child** was added between the applications app4 and app5.

Example 7-18 Adding parent_child dependence

```
# ksysvmmgr -s add dependency dependency_list=app4,app5
dependency_type=parent_child
Adding dependency "dependency_list=app4,app5" into configuration successfully
performed.
```

To list the dependencies after adding the **parent_child** dependency, run the command **ksysvmmgr q dependency**, as shown in Example 7-19.

Example 7-19 Listing dependencies after adding the parent_child dependency

```
# ksysvmmgr q dependency
Dependency depuuid=1542239347575681000
 dependency_type=start_sequence
 dependency_list=app1,app2,app3
 strict=YES
Dependency depuuid=1542239435934976000
 dependency_type=stop_sequence
 dependency_list=app1,app2,app3
 strict=YES
Dependency depuuid=1542239846084192000
 dependency_type=parent_child
 dependency_list=app4,app5
 strict=YES

# ksysvmmgr q dependency 1542239846084192000
Dependency depuuid=1542239846084192000
 dependency_type=parent_child
 dependency_list=app4,app5
 strict=YES
```

Application dependency class

The application dependency class contains the following mandatory attributes:

- **dependency_type**: Specifies the type of dependency between applications. This attribute can have the following values:
  - **start_sequence**: Specifies the order in which the applications must be started as mentioned in the **dependency_list** attribute. The **dependency_list** attribute must have more than one application for this dependency type.
  - **stop_sequence**: Specifies the order in which the applications must be stopped as mentioned in the **dependency_list** attribute. The **dependency_list** attribute must have more than one application for this dependency type.
  - **parent_child**: Specifies the parent-child relationship of the two specified applications in which one application is the parent and the other is the child. The parent application must start first and then the child application must start. Stop the child application first and then stop the parent application. If the parent application fails, the child application stops automatically.
- **dependency_list**: Specifies the list of applications that have a dependency among them. The dependency class also contains the following optional attributes:

  strict: Specifies whether to continue the script or command if the dependency policy cannot be followed. If the strict attribute is set to `Yes`, the next application is not started until the previous application starts and is in the normal state. If the strict attribute is set to `No`, the next application is started immediately after the first application is started regardless of the state of the first application. This attribute is applicable only for the **start_sequence** dependency.

7.3 Uninstalling VM Agents

This section shows how to uninstall the VM Agents.

7.3.1 Uninstalling a VM Agent in an AIX VM

To uninstall a VM Agent in AIX, complete the following steps:

1. Stop the VM Agent module in the AIX VM, as shown in Example 7-20.

Example 7-20 Stopping the AIX VM Agent

```
# ksysvmmgr status
Subsystem         Group            PID          Status
 ksys_vmm                          9568676      active

(0) root @ rt11001: /
# ksysvmmgr stop
0513-044 The ksys_vmm Subsystem was requested to stop.

(0) root @ rt11001: /
# ksysvmmgr status
Subsystem         Group            PID          Status
 ksys_vmm                                       inoperative
```

2. Uninstall the VM Agent file sets from the AIX VM by running the command that is shown in Example 7-21.

Example 7-21 Uninstalling the VM Agent file sets from AIX

```
# installp -u ksys*
.
.
.
Installation Summary
--------------------
Name                        Level           Part        Event       Result
-------------------------------------------------------------------------------
ksys.vmmon.rte              1.3.0.0         ROOT        DEINSTALL   SUCCESS
ksys.vmmon.rte              1.3.0.0         USR         DEINSTALL   SUCCESS
```

7.3.2 Uninstalling a VM Agent in a Linux VM

To uninstall a VM Agent in a Linux VM, complete the following steps:

1. Stop the VM Agent module in the Linux VM, as shown in Example 7-22.

Example 7-22 Stopping the VM Agent module in the Linux VM

```
# ksysvmmgr status
ksys_vmm daemon is active.

# ksysvmmgr stop
ksys_vmm has been requested to stop.

# ksysvmmgr status
ksys_vmm daemon is currently inoperative.
```

2. Uninstall the VM Agent package from the Linux VM, as shown in Example 7-23.

Example 7-23 Uninstalling the VM Agent package from the Linux VM

```
# rpm -e vmagent
Stopping ksys_vmm daemon.
ksys_vmm daemon is currently inoperative.
```

7.4 Setting contacts for event notification

The KSYS subsystem tracks various events that occur in the environment, analyzes the situation, and notifies the registered contacts about any issues. Add the contact information to the KSYS subsystem so that you can receive notifications about any situation that might need your action.

You can add the following contact information for a specific user:

- Email address
- Phone number with the phone carrier’s email address
- Pager email address

> **Note:** The KSYS node must have a public IP address to send the event notifications successfully.

To register contact details so that you can receive notification from KSYS, run the following commands in the KSYS LPAR:

- To add the email address of a specific user to receive notifications, run the following command:

  ```
  ksysmgr add notify user=username contact=email_address
  ```

  Example 7-24 shows how to add and list an email address for a specific user.

Example 7-24 Adding and listing an email address for a specific user

```
# ksysmgr add notify user=Francisco contact=francisco.almeida@testamail.com
successfully added user information

# ksysmgr query notify contact
User:            Francisco
Contact:         francisco.almeida@testamail.com
```

You can add multiple email addresses for a specific user. However, you cannot add multiple email addresses simultaneously. Run the command multiple times to add multiple email addresses, as shown in Example 7-25.

Example 7-25 Adding multiple email addresses

```
# ksysmgr add notify user=Francisco contact=francisco.almeida@mailtes.com
successfully added user information

# ksysmgr query notify contact
User:            Francisco
Contact:         francisco.almeida@testamail.com

User:            Francisco
Contact:         francisco.almeida@mailtes.com
```

- To add a specific user to receive a System Management Services (SMS) notification, run the following command:

  ```
  ksysmgr add notify user=username
  contact=10_digit_phone_number@phone_carrier_email_address
  ```

  Example 7-26 shows how to add a specific user to receive an SMS notification.

Example 7-26 Adding a specific user to receive an SMS notification

```

# ksysmgr add notify user=Beatriz contact=1234567890@tomymail.com
successfully added user information

# ksysmgr query notify contact
User:            Beatriz
Contact:         1234567890@tomymail.com
```

  Specify the phone number along with the email address of the phone carrier to receive an SMS notification. To determine the email address of your phone carrier, contact the phone service provider.

- To add a specific user to receive a pager notification, run the following command:

  ```
  ksysmgr add notify user=username contact=pager_email_address
  ```

  Example 7-27 shows how to add a specific user to receive a pager notification.

Example 7-27 Adding a specific user to receive a pager notification

```
# ksysmgr add notify user=Dayana contact=1234567890@skytel.com
successfully added user information
# ksysmgr query notify contact
User:            Beatriz
Contact:         1234567890@tomymail.com

User:            Dayana
Contact:         1234567890@skytel.com
```

- To remove a specific user, run the following command:

  ```
  ksysmgr delete notify user=username
  ```

  Example 7-28 shows how to remove a specific user notification.

Example 7-28 Removing a user notification

```
#ksysmgr query notify contact
User:            Beatriz
Contact:         1234567890@tomymail.com

# ksysmgr delete notify user=Beatriz
successfully deleted user information

#ksysmgr query notify contact
```

7.5 Backing up and restoring the configuration data

A backup of all the current configuration settings of the KSYS environment can be saved as a snapshot. A snapshot preserves the configuration details of the KSYS environment at a specific point in time. For example, a snapshot file contains information about the existing sites, details about the managing HMCs and the managed hosts in a specific site, and the storage device details in the site. Back up your current configuration settings after you configure the sites, hosts, HMCs, and storage devices initially. If a snapshot of the current KSYS configuration settings is saved, you can restore the configuration settings later by applying the snapshot on the KSYS configuration. The snapshots are useful during node upgrades or environment malfunctions because snapshots eliminate the need to reconfigure the sites, hosts, HMCs, and storage devices. For example, if the KSYS node must be reinstalled, a snapshot can be restored so that you do not need to re-create sites, hosts, and other resources.

To restore the `DETAILED` type of snapshot, the version of VMRM DR must be the same as the version when the snapshot was captured. The snapshot must be captured on the home site only, and must be restored *only* on the home site. When the snapshot is restored, ensure that all VMs are on the home site.

Saving and restoring snapshots

Use the **ksysmgr** command to save the configuration snapshots. The snapshots are saved in an XML format. When you create a snapshot, the **ksysmgr** command appends the date and time to the specified file name to follow the `filename.DateTime` name convention. By default, the snapshot files are saved in the `/var/ksys/snapshots` directory. However, you can specify the path where the snapshot files must be saved.

Important guidelines for saving and restoring snapshots

- Ensure that the `/var` file system has enough space for the snapshot files before you back up the configuration data.
- If the KSYS node must be reinstalled, the snapshot files must be saved in a different location so that the snapshot files can be used later for restoring the configuration settings by using the **ksysmgr** command. Remote copy the snapshot files to another system to copy the snapshot files from another system to the KSYS node after the installation is complete.
- A snapshot file that is captured at a different site *cannot* be restored. To restore a snapshot file, the snapshot file must be captured on the same site.
- To obtain the tertiary disk information after restoring a detailed snapshot, the discovery operation must be run with the **dr_test** flag.
- If the source hosts and target hosts are configured to the same HMC, it leads to an invalid configuration in the KSYS subsystem. If a snapshot of such an invalid configuration is saved, the restore operation fails.

You can perform the following snapshot operations:

- Saving a snapshot

  To save a snapshot, use the following command syntax:

  ```
  ksysmgr add snapshot filepath=full_file_prefix_path|file_prefix
  ```

  For example, to back up the configuration data of your KSYS environment once a week with no more than *five* backup files concurrently, run the following command:

  ```
  ksysmgr add snapshot filepath=/home/ksysdir/myksysbackup
  ```

  The **ksysmgr** command saves the snapshot after archiving and compressing the file.

- Viewing or querying the existing snapshot file

  The command syntax to view or query the existing snapshot file is as follows:

  ```
  ksysmgr query snapshot filepath=full_file_prefix_path
  ```

  For example:

  ```
  ksysmgr query snapshot filepath=/var/ksys/snapshots/myksysbackup
  _DETAILED_2022-10-12_04:07:52.xml.tar.gz
  ```

  An example view of the results of the query is shown in Example 7-29.

Example 7-29 The ksysmgr query snapshot output

```
File:          /var/ksys/snapshots/myksysbackup _DETAILED_2019-12-12_04:07:52.xml
Type:          DETAILED
VMRM Version:  1.7.0.0
Date:          2022-10-12
Time:          04:07:52
---------------------------
Cluster:
--------
Name:          DR_TEST
Node:          <hostname>
Type:          DR
```

- Restoring a snapshot file to the KSYS node

  To restore a saved snapshot on a KSYS node where the operating system was reinstalled, or on another LPAR that must be used as the KSYS LPAR, ensure that the `HOST` variable is set. You can set the `HOST` variable as shown by running the following command:

  ```
  #  export HOST=host_name
  ```

  To restore the configuration data on a KSYS node, run the following command:

  ```
  ksysmgr restore snapshot filepath=full_file_prefix_path
  ```

  For example:

  ```
  ksysmgr restore snapshot filepath=/home/ksysdir/myksysbackup
  _DETAILED_2022-10-12_04:07:52.xml.tar.gz
  ```

  This command decompresses and unarchives the snapshot file, and then applies the configuration settings to the KSYS node.

- Restoring a KSYS snapshot in PowerHA SystemMirror that is configured with a multiple KSYS node configuration

  To restore the KSYS snapshot in PowerHA SystemMirror that is configured with a multiple KSYS node configuration, run the following command in the PowerHA SystemMirror cluster node:

  ```
  /opt/IBM/ksys/samples/pha/ksyscluster -restore <filepath or filename>
  ```

  For *filepath,* include the file name along with the file path. For *filename*, the system checks the `/var/ksys/snapshots/` directory and the current directory from where you are running the **`restore`** command. You can run the **`snapshot restore`** command in any PowerHA SystemMirror cluster node that is configured with a multiple KSYS node configuration.

8

KSYS high availability

This chapter provides information about how to achieve high availability (HA) for the KSYS orchestrator node in IBM Virtual Machine Recovery Manager (VMRM). It also shows how to configure a 2-node or multinode cluster, and explains failover scenarios with examples.

KSYS HA is common feature for all supported cluster configurations, that is, disaster recovery (DR), HA, high availability and disaster recovery (HADR), and HADRHA.

The following topics are described in this chapter:

- Overview and capabilities
- Creating a 2-node or multi-node KSYS cluster
- Collecting and restoring the snapshot for a KSYS cluster
- Log analysis and troubleshooting
- Migration considerations with PowerHA

8.1 Overview and capabilities

This section provides an overview of the KSYS HA solution. KSYS HA brings clustering technology to the KSYS node to enable your environment to continue to run if there is a failure in the KSYS node.

8.1.1 Overview

KSYS HA is a new feature that was introduced with VMRM 1.7. Before Version 1.7, HA for KSYS was achieved by using PowerHA SystemMirror.

With this new KSYS HA feature, two or more nodes can be configured in a KSYS cluster so that if a KSYS node goes down, the others can take over and continue the orchestration.

VMRM KSYS internally uses Reliable Scalable Cluster Technology (RSCT) components such as Topology services and Group services to achieve HA. Both of these distributed subsystems operate within a peer domain. A *peer domain* is a set of nodes that know about each other and share resources. On these nodes, the RSCT components run various operations that are necessary to achieve HA.

When the KSYS multinode is created, the first KSYS node that was specified during the configuration becomes a group leader (GL) and the subsequent KSYS nodes are considered as non-GL nodes. The GL is the node that controls all the resources, handles all KSYS operations, and makes sure that the updated resource configuration details are synced to the non-GL nodes.

KSYS HA feature implementation is common for all the cluster configuration types: HA, DR, HADR, and HADRHA.

KSYS internal threads like daily scheduler, discovery and verification threads, policy manager threads, and FDE threads are active only in GL nodes and disabled in non-GL nodes. When a non-GL KSYS node becomes the active GL node, these threads become active and continue the operations by referring to the registry details. The registry resource details always are in sync with all the online KSYS nodes in the KSYS cluster.

As a best practice, keep the time synchronized across all KSYS nodes in the KSYS cluster, which can help in analyzing the logs during the GL transition. As part of event notification configuration to receive email notifications, make sure that the emails can be sent from all the KSYS nodes in the KSYS cluster,

Figure 8-1 on page 219 shows a multinode KSYS cluster managing a typical VMRM DR configuration.

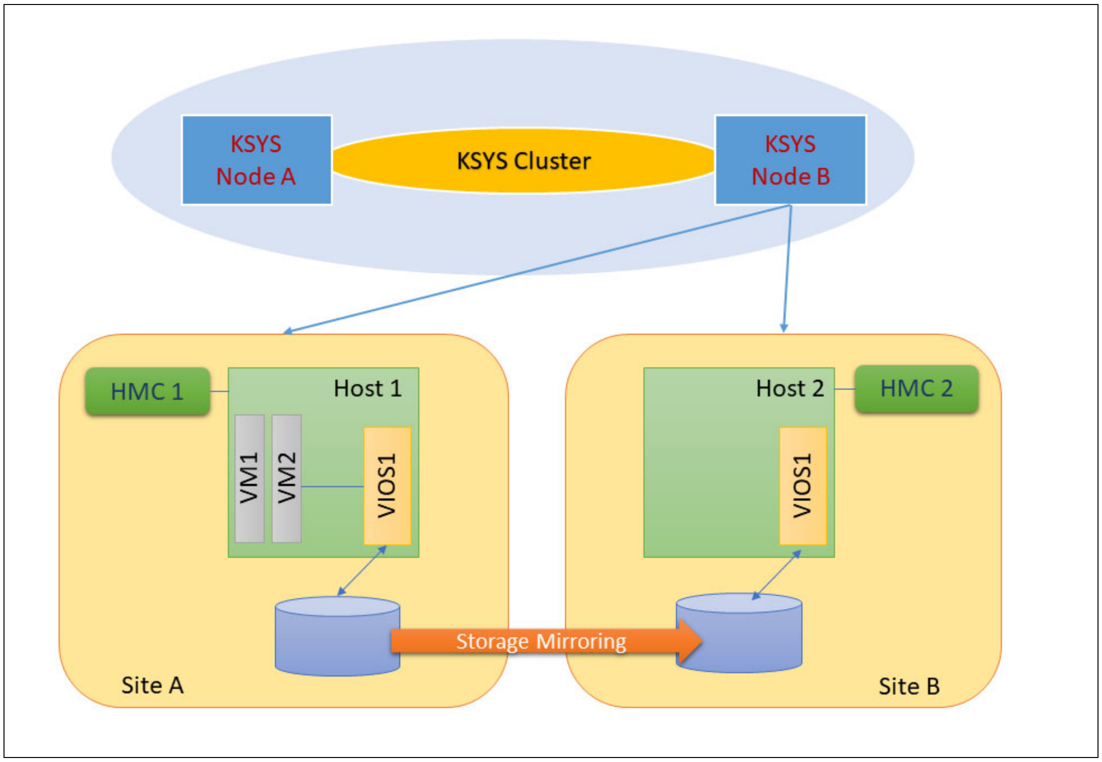


Figure 8-1 Multi KSYS node cluster managing a DR configuration

8.1.2 Capabilities

This section describes the following capabilities:

- KSYS high availability
- State change notifications
- KSYS cluster modification
- Snapshot enhancement

KSYS high availability

A GL KSYS can become inoperative due to many reasons, such as the following items:

- CEC failure
- VM failure or restart
- KSYS daemon restart
- Network connectivity issues
- Network or adapter issues
- Cable pull
- Planned or unplanned site outages

In this case, a non-GL KSYS node becomes the GL node and controls the orchestration. When the previously affected KSYS comes back online, it automatically is included in the KSYS cluster as a non-GL node.

A new class that is called IBM.VMR_SITE_CLD is implemented in the KSYS to store all KSYS node details and the status. Example 8-1 shows the two-node cluster configuration with details like node name, identifier, and the state.

Example 8-1 KSYS cluster nodes

```
# lsrsrc IBM.VMR_SITE_CLD Name KsysNode KsysState
Resource Persistent Attributes for IBM.VMR_SITE_CLD
resource 1:
        Name      = "Node_2"
        KsysNode  = "2"
        KsysState = "Up"
resource 2:
        Name      = "Node_1"
        KsysNode  = "1"
        KsysState = "Up"
```

The GL node is maintained at the RSCT level of IBM.VMR_SITE_CLD, as shown in Example 8-2. It can be checked by running the **lssrc** command.

Example 8-2 Group leader node details in KSYS

```
# lsrsrc -c IBM.VMR_SITE_CLD ManagingNode
Resource Class Persistent Attributes for IBM.VMR_SITE_CLD
resource 1:
        ManagingNode = "1"

#  lssrc -ls IBM.VMR | grep Group
Group IBM.VMR:
   Group Leader: ksys110.aus.stglabs.ibm.com, 0x10d5984bcf580bec, 1
```

The KSYS cluster, the node IDs, and details about participant nodes in the cluster can be queried by running the **lsrpdomain** and **lsrpnode** commands, as shown in Example 8-3.

Example 8-3 The lsrpdomain and lsrpnode query output

```
# lsrpdomain
Name OpState RSCTActiveVersion MixedVersions TSPort GSPort
K_HA Online  3.2.6.4           No            12347  12348
(0) root @ ksys110: /
# lsrpnode -i
Name                        OpState RSCTVersion NodeNum NodeID
ksys105.aus.stglabs.ibm.com Online  3.2.6.4     2       fdcacd23181e25e8
ksys110.aus.stglabs.ibm.com Online  3.2.6.4     1       10d5984bcf580bec
```

These details also can be queried by running **ksysmgr**, as shown in Example 8-4.

Example 8-4 Running ksysmgr to display nodes in ksyscluster including state and type

```
Managing node.
# ksysmgr q ksyscluster
Name:               K_HA
State:              Online
Type:               DR
Ksysnodes:          ksys105.aus.stglabs.ibm.com:2:Online
                    ksys110.aus.stglabs.ibm.com:1:Online    (Managing node)
```

State change notifications

With this support, new events are introduced to indicate GroupLeader changes and the KSYS status.

When a non-GL node becomes a GL, the KSYS_MANAGING_NODE_CHANGED event is generated from the new GL node. When a KSYS node goes down and leaves the KSYS cluster or comes up and rejoins the KSYS cluster, KSYS_NODE_STATUS_CHANGED events are generated.

Example 8-5 shows the notification formats.

Example 8-5 New events that are related to KSYS high availability

```
---------EVENT START--------
KSYS_MANAGING_NODE_CHANGED event has occurred. Details are as follows:
Event:              KSYS_MANAGING_NODE_CHANGED
Type:               Warning Event
Time:               Tue Jul 12 03:04:36 CDT 2022
Entity Affected:    KSYS
Resource Affected:  ksys105.aus.stglabs.ibm.com
Description:        0000-532 Managing KSYS node changed. New Managing KSYS node:
ksys105.aus.stglabs.ibm.com
---------EVENT END----------

---------EVENT START--------
KSYS_NODE_STATUS_CHANGED event has occurred. Details are as follows:
Event:              KSYS_NODE_STATUS_CHANGED
Type:               Warning Event
Time:               Sun Jul 10 05:12:36 CDT 2022
Entity Affected:    KSYS
Resource Affected:  ksys105.aus.stglabs.ibm.com
Description:        0000-531 KSYS ksys105.aus.stglabs.ibm.com Status changed.
State: Down
---------EVENT END----------
```

KSYS cluster modification

With this new KSYS HA feature, an existing single node KSYS environment can have a new KSYS node as a backup non-GL node. The **ksysmgr** command is enhanced to add or remove a node from a KSYS cluster.

Any resource addition, modification, or deletion in the KSYS configuration is populated to the other nodes in the KSYS cluster too so that when the KSYS node becomes the GL, it has the latest configuration information, as demonstrated in Example 8-6. In this example, an attribute in an RCCP class is updated on the GL node only. When the attribute is queried on the non-GL node, the attribute is now changed to the same value as the GL node.

Example 8-6 KSYS GL node attribute changes also are changed in non-GL nodes

```
ksys202gui (GL) and ksys822p (non-GL) are part of a KSYS Cluster.

Initial display of RCCP attribute on both nodes:
from root @ ksys202gui (GL)
   # lsrsrc -c IBM.VMR_SITE NotificationLevel
   Resource Class Persistent Attributes for IBM.VMR_SITE
   resource 1:
           NotificationLevel = "low"
from root @ ksys822p (GL)
```

```
   # lsrsrc -c IBM.VMR_SITE NotificationLevel
   Resource Class Persistent Attributes for IBM.VMR_SITE
   resource 1:
           NotificationLevel = "low"

Modify RCCP attribute on GL node only:
from root @ ksys202gui (GL)
   # ksysmgr modify system notification_level=high
   KSYS notification_level has been updated

   # lsrsrc -c IBM.VMR_SITE NotificationLevel
   Resource Class Persistent Attributes for IBM.VMR_SITE
   resource 1:
           NotificationLevel = "high"

Now, display the attribute on the non-GL node to show that it is updated
to match the GL node:

from root @ ksys822p (GL)
   #  lsrsrc -c IBM.VMR_SITE NotificationLevel
   Resource Class Persistent Attributes for IBM.VMR_SITE
   resource 1:
           NotificationLevel = "high"

   (0) root @ ksys822p: /
   #
```

Snapshot enhancement

The snapshot feature is enhanced so it can now be taken for a single or multinode KSYS from the GL KSYS node. If the collected snapshot was taken from a cluster with two KSYS nodes, the snapshot can be restored to create the 2-node KSYS cluster.

The snapshot can be restored on a new set of KSYS nodes. Snapshots are documented in 8.3, “Collecting and restoring the snapshot for a KSYS cluster” on page 225.

8.1.3 Cluster behavior in error scenarios

This section explains how the KSYS cluster behaves in different scenarios like a KSYS node going down when an operation is in progress, a failure is detected, or a split-brain scenario occurs.

These scenarios are explained by using two KSYS node clusters: KSYS A and KSYS B. KSYS A is the GL or managing node and KSYS B is a non-GL node.

Discovery and verify operations

If the discovery or verify operations start from **ksysmgr** and the operation is in progress, if KSYS A goes down during that time, KSYS B becomes the GL node. Rerun the discovery and verify operations on the new GL node (KSYS B).

Move and DR rehearsal operation between sites for DR, HADR, HADRHA cluster types

If a user triggers the move operation, the KSYS can go down in two possible scenarios:

- The GL node KSYS A goes down before ActiveSiteID of HG/WG changes. In this case, the user can trigger the move operation from the new GL node KSYS B.
- The GL node KSYS A goes down after ActiveSiteID of the HG/WG changes. In this case, run the recovery operation from the new GL node KSYS B.

The move LPM operation and automatic VM or CPC failure handling for HA, HADR, and HADRHA cluster types

If the GL node KSYS A goes down during these operations or there is a VM or CPC failure, the new GL node KSYS B identifies these scenarios and continues these operations.

Connectivity lost between two KSYS nodes (split-brain scenario)

In such scenarios, both KSYS A and KSYS B might think that the other node went down, so they both become GL nodes. In such cases, **ksysmgr** commands can be run on both KSYS nodes. This scenario should not cause any functional behavior changes. For example, in a VM or CPC failure, both KSYS nodes might identify and attempt to handle the failure, but either one can succeed in doing so. The other KSYS node might report failure for that operation. This scenario should not affect any resource configuration changes.

Such scenarios can be identified by monitoring the notifications and getting a KSYS_MANAGING_NODE_CHANGED event from both nodes, with each reporting the other node as down by sending KSYS_NODE_STATUS_CHANGED. In such scenarios, take corrective measures.

8.1.4 Site considerations for KSYS

For a single-node KSYS implementation, the KSYS logical partition (LPAR) is preferably at the backup site. With this new feature of KSYS HA implementation, there is no such site-specific restriction for the second KSYS node. The second node that is added to the existing single-node KSYS cluster can be in either the backup or home site. The nodes running KSYS should not be managed by the KSYS subsystem. The KSYS cluster nodes must be able to communicate freely without any network-related hindrances.

8.2 Creating a 2-node or multi-node KSYS cluster

Before attempting to create a 2-node or multi-node KSYS cluster, be aware of the following points:

- The KSYS nodes that are added to KSYS cluster should have similar resources (CPU, memory, and storage). All the KSYS nodes should have connectivity to all communication components like HMC, Storage, GUI, and sendmail.
- As a best practice, use the same RSCT version on all the KSYS nodes of the KSYS cluster. However, if the RSCT already is installed and you do not want to update it, you can create the cluster in mixed mode.

  In a mixed-mode cluster, the KSYS node with the latest RSCT version should be added first. Then, add more KSYS nodes.

Example 8-7 shows a KSYS cluster with mixed RSCT versions. This cluster is different than the cluster that is shown in Example 8-4 on page 220.

Example 8-7 Mixed version KSYS cluster

```
# lsrpdomain
Name   OpState RSCTActiveVersion MixedVersions TSPort GSPort
SMR_DR Online  3.2.5.4           Yes           12347  12348

(0) root @ ksys202gui: /
# lsrpnode -i
Name                           OpState RSCTVersion NodeNum NodeID
ksys822p.aus.stglabs.ibm.com   Online  3.2.6.4     2       880de792138beee6
ksys202gui.aus.stglabs.ibm.com Online  3.2.5.4     1       7d091aa6c346cbe6
```

To prepare a KSYS node to add to a KSYS cluster, run the **preprpnode** command on the KSYS node that is going to be added to the KSYS cluster, as shown in Example 8-8.

Example 8-8 Preparing to add a KSYS node to a KSYS cluster

```
# preprpnode ksys105.aus.stglabs.ibm.com

(0) root @ ksys105:
```

Note: For more information about **preprpnode**, see preprpnode Command.

Here is the syntax to create and add the KSYS node to the KSYS cluster:

```
# ksysmgr add ksyscluster -h
ksysmgr add ksyscluster
      [<ksysclustername>]
      [type=<HA|DR|HADR|HADRHA|CLOUDDR|HYBRID>]
      ksysnodes=<ksysnode1[,ksysnode2,...]>
      [sync=<yes|no>]
    add => ad*, cr*, make, mk
    ksyscluster => ksysclu*, clu*
    Note: type=DR is the default
```

Note: **CLOUDDR** and **HYBRID** are not enabled for the type parameter. They are for future reference.

```
# ksysmgr add ksyscluster <name> ksysnodes=node1,node2
# ksysmgr add ksyscluster <name> ksysnodes=node3
```

An example of adding KSYS nodes to a KSYS cluster is shown in Example 8-9.

Example 8-9 Adding KSYS nodes to a KSYS cluster

```
# date;ksysmgr add ksyscluster SMR_DR
ksysnodes=ksys202gui.aus.stglabs.ibm.com,ksys822p.aus.stglabs.ibm.com type=DR
sync=yes
Wed Nov 16 07:46:19 CST 2022
Adding node to current cluster configuration
Ksyscluster has been created, running verify now
Ksyscluster has been verified, running sync now
Stopping KSYS subsystem ...
   Waiting for KSYS subsystem to stop ...
```

```
Starting KSYS subsystem ...
Ksyscluster SMR_DR created on ksys202gui.aus.stglabs.ibm.com. Modifying the
cluster to add remaining nodes.
Adding node to current cluster configuration
Starting ksysnodes
Ksysnodes started successfully
Ksyscluster SMR_DR successfully modified.
KSYS subsystem has started. You can begin adding site definitions, HMCs, storage
agents, etc
```

To remove KSYS nodes from the existing KSYS cluster, run the following command on the GL node:

```
ksysmgr modify ksyscluster cluster_name remove ksysnodes=ksys_node
```

8.3 Collecting and restoring the snapshot for a KSYS cluster

Here is the **ksysmgr** command syntax to collect a snapshot for the KSYS cluster. In a multinode KSYS cluster, the snapshot includes the details of all the KSYS nodes.

```
# ksysmgr add snapshot -h

ksysmgr add snapshot
      [filepath=<full file prefix path | file prefix>]
    add => ad*, cr*, make, mk
    snapshot => snap*
```

Example 8-10 shows an example of creating a snapshot.

Example 8-10 Using ksysmgr to create a snapshot

```
(0) root @ ksys110: /
# ksysmgr add snapshot
Taking snapshot...
Created: /var/ksys/snapshots/snap.xml_DETAILED_2022-11-12_17:06:40.xml.tar.gz
Successfully created a configuration snapshot:
/var/ksys/snapshots/snap.xml_DETAILED_2022-11-12_17:06:40.xml.tar.gz

(0) root @ ksys110: /
#  ksysmgr add snapshot filepath=/tmp/test
Taking snapshot...
Created: /tmp/test_DETAILED_2022-11-12_17:06:55.xml.tar.gz
Successfully created a configuration snapshot:
/tmp/test_DETAILED_2022-11-12_17:06:55.xml.tar.gz

(0) root @ ksys110: /
```

The **ksysmgr query** command is enhanced to query the KSYS details within the collected snapshot. Example 8-11 shows the command syntax to query and restore the KSYS cluster configuration.

Example 8-11 ksysmgr syntax to query the content of the collected snaps

```
# ksysmgr query snapshot -h

ksysmgr query snapshot
    [filepath=<full file prefix path>]
    query => q*, ls, get, sh*
    snapshot => snap*
```

Example 8-12 shows the summary output of a snapshot query.

Example 8-12 The ksysmgr query snapshot details

```
(0) root @ ksys110: /
#  ksysmgr query snapshot
filepath=/tmp/test_DETAILED_2022-11-12_17:06:55.xml.tar.gz
---- Snapshot Contents ----
File:         /tmp/test_DETAILED_2022-11-12_17:06:55.xml
VMRM Version: 1.4.0.0
Date:         2022-11-12
Time:         17:06:55
---------------------------

Cluster:
--------
Name:        K_HA
Node:        ksys110.aus.stglabs.ibm.com,ksys105.aus.stglabs.ibm.com
Type:        HYBRID
---------------------------
```

The syntax to restore a snapshot follows. Make sure that **preprpnode** runs before you perform the restoration, as shown in Example 8-13.

Example 8-13 The restore snapshot command

```
# ksysmgr restore snapshot -h

ksysmgr restore snapshot
    filepath=<full file prefix path>
    restore => resto*
    snapshot => snap*
```

An example of restoring a snapshot is shown in Example 8-14.

Example 8-14 A ksysmgr restore snapshot

```
(0) root @ ksys110: /
#./ksysmgr restore snapshot
filepath=/tmp/test_DETAILED_2022-11-12_17:06:55.xml.tar.gz
WARNING: This action would remove the existing VMRM configuration
Do you want to proceed? [y|n]
y
```

```
INFO: Restoring snapshot on these nodes ksys110.aus.stglabs.ibm.com
ksys105.aus.stglabs.ibm.com
Restoring configuration...
Creating cluster...
Updating registry...
Successfully restored registry files!
Starting VMR daemon...
Successfully restored snapshot:/tmp/test_DETAILED_2022-11-12_17:06:55.xml!
Run discovery to apply changes.
INFO: Restore completed successfully

(0) root @ ksys110: /
# ksysmgr q ksyscluster
Name:                K_HA
State:               Online
Type:                DR
Ksysnodes:           ksys105.aus.stglabs.ibm.com:2:Online
                     ksys110.aus.stglabs.ibm.com:1:Online    (Managing node)
(0) root @ ksys110: /
```

A KSYS cluster configuration can be restored to a different set of nodes, as shown in Example 8-15. Make sure to run the **preprpnode** command on all the KSYS nodes, as shown in Example 8-8 on page 224.

Example 8-15 Restoring a snapshot to different KSYS nodes

```
(0) root @ ksys810: /
# preprpnode ksys810.aus.stglabs.ibm.com
(0) root @ ksys810: /

# Note: This preprpnode command should be run on other KSYS node
ksys811.ausprv.stglabs.ibm.com also.

(0) root @ ksys810: /
# ksysmgr restore snapshot
filepath=/tmp/test_DETAILED_2022-11-12_17:06:55.xml.tar.gz
WARNING: This action would remove the existing VMRM configuration
Do you want to proceed? [y|n]
y
INFO: Existing nodes in multinode configuration are ksys110.aus.stglabs.ibm.com
ksys105.aus.stglabs.ibm.com
Do you want to continue with same ksysnodes? [y|n]
n
Do you want to change it into single node configuration, enter yes or no
no
Enter the new nodes separated by space.
ksys810.ausprv.stglabs.ibm.com ksys811.ausprv.stglabs.ibm.com
INFO: Restoring snapshot on these nodes ksys811.ausprv.stglabs.ibm.com
ksys810.ausprv.stglabs.ibm.com
This may take a few minutes to safely remove the ksysclsuter
Removed tmp files successfully
Restoring configuration...
Creating cluster...
Updating registry...
Successfully restored registry files!
Starting VMR daemon...
```

```
Successfully restored snapshot:/tmp/test_DETAILED_2022-11-12_17:06:55.xml!
Run discovery to apply changes.
INFO: Restore completed successfully

(0) root @ ksys810: /
```

8.4 Log analysis and troubleshooting

The following information is useful to isolate and resolve issues and for analyzing the log files in a KSYS cluster.

8.4.1 Analyzing the log files

The logs for **ksysmgr**, KSYS, and storage agents should be looked at only on the GL KSYS node. There are not any active logs or useful information in the logs of a non-GL KSYS node. The troubleshooting details for DR, HA, HADR, and HADRHA are applicable for this feature. Any **ksysmgr** error messages can be found in `/var/ksys/log/ksysmgr.log`.

KSYS logs are in the `/var/ct/cluster_name/log/mc/IBM.VMR/` directory on the GL. Example 8-16 shows when the GL transition happens between nodes in the KSYS cluster. In this 2-node KSYS cluster example, ksys822 is the managing node (GL Node) and ksys202gui is the GL node.

Example 8-16 KSYS logs

```
# rpttr -odict /var/ct/cluster_name/log/mc/IBM.VMR/trace.ksys.* > ksys.log
# vi ksys.log
...
..
[62] 11/19/22 T(2057) _VMR 01:40:04.869913 DEBUG VMRDaemon.C[628]: Domain
MemberShipChanged!!! NodeID: 1. <<<<<<<<<<<<<<<<<<
[62] 11/19/22 T(2057) _VMR 01:40:04.869929 DEBUG VMRDaemon.C[630]: pMembersAdded=
0, numMembersAdded=0
[62] 11/19/22 T(2057) _VMR 01:40:04.869930 DEBUG VMRDaemon.C[631]:
pMembersRemoved=2, numMembersRemoved=1
[62] 11/19/22 T(2057) _VMR 01:40:04.869931 DEBUG VMRDaemon.C[646]: Node
[ksys822p.aus.stglabs.ibm.com] KSYS is OFFLINE!

[62] 11/19/22 T(2057) _VMR 01:40:04.869947 DEBUG VMR_SITE_CLD.C[2765]:  nodeid:2,
Local_State:Down, glNode:1
...
[62] 11/19/22 T(2057) _VMR 01:40:07.985716 DEBUG VMR_SITE_CLD.C[1879]: Node:2
KsysState: Down
[62] 11/19/22 T(515) _VMR 01:40:07.986588 DEBUG VMR_SITE.C[8000]: INFO:
eventNotify entering. event:KSYS_NODE_STATUS_CHANGED, event type:2, comp:KSYS,
notificationLevel:low, dupEventProcess:
yes
...
[62] 11/19/22 T(515) _VMR 01:40:07.986827 DEBUG VMR_SITE_CLD.C[2976]:
updateManagingNode called. node_id:1

[62] 11/19/22 T(2057) _VMR 01:40:07.987568 DEBUG VMR_SITE_CLD.C[1328]:
ManagingNode Change Applied!
```

```
[62] 11/19/22 T(937) _VMR 01:40:07.987910 DEBUG VMR_SITE.C[12051]: INFO:
sendNotification entering. event:KSYS_NODE_STATUS_CHANGED, event type:2,
comp:KSYS, notificationLevel:low, dupEventProcess:yes
...
[62] 11/19/22 T(2057) _VMR 01:40:08.087473 VMR_HMCRccp::chgClassCommitted Entered.
[62] 11/19/22 T(2057) _VMR 01:40:08.087483   DEBUG VMR_SITE_CLD.C[1365]: Managing
node updated :1
[62] 11/19/22 T(2057) _VMR 01:40:08.087486 VMR_HMCRccp::chgClassCommitted Leaving.
```

When the node ksys822p restarts, it joins the KSYS cluster as non-GL node. The logs that are shown in Example 8-17 indicate that the KSYS node started as a non-GL node.

Example 8-17 KSYS log node started on a non-group leader node

```
# rpttr -odict /var/ct/cluster_name/log/mc/IBM.VMR/trace.ksys.* > ksys.log
# vi ksys.log

[77] 11/19/22 T(772) _VMR 02:33:08.143561656DEBUG VMRRmcp.C[285]: VMRRmcp Init,
START
[77] 11/19/22 T(1029) _VMR 02:33:08.195047062 DEBUG VMR_SITE_CLD.C[1879]: Node:2
KsysState: Up
....

[77] 11/19/22 T(772) _VMR 02:33:08.369378156DEBUG VMR_SITE.C[6638]: Not a
GroupLeader node!. skipping initializing Quick discovery!
[77] 11/19/22 T(772) _VMR 02:33:08.369379812DEBUG VMR_SITE.C[6480]: Not a
GroupLeader node!. skipping initializing Detailed discovery!
[77] 11/19/22 T(772) _VMR 02:33:08.369384285DEBUG VMR_SITE.C[14347]: Not a
GroupLeader node!. skipping startupAutoIntiatedProgressCheck!
[77] 11/19/22 T(772) _VMR 02:33:08.369386880DEBUG VMRRmcp.C[290]: VMRRmcp Init,
FINISH
```

For the new GL KSYS node, ksys202gui, the logs are shown in Example 8-18.

Example 8-18 KSYS logs new group leader

```
[62] 11/19/22 T(2057) _VMR 02:33:15.673821 DEBUG VMRDaemon.C[628]: Domain
MemberShipChanged!!! NodeID: 1. <<<<<<<<<<<<<<<<<<
[62] 11/19/22 T(2057) _VMR 02:33:15.673836 DEBUG VMRDaemon.C[630]: pMembersAdded=
2, numMembersAdded=1
[62] 11/19/22 T(2057) _VMR 02:33:15.673837 DEBUG VMRDaemon.C[631]:
pMembersRemoved=0, numMembersRemoved=0
[62] 11/19/22 T(2057) _VMR 02:33:15.673839 DEBUG VMRDaemon.C[633]: Node
[ksys822p.aus.stglabs.ibm.com] KSYS is ONLINE!

[62] 11/19/22 T(2057) _VMR 02:33:15.673851 DEBUG VMR_SITE_CLD.C[2765]:  nodeid:2,
Local_State:Up, glNode:1
....
[62] 11/19/22 T(2057) _VMR 02:33:15.673877 DEBUG VMRDaemon.C[639]: UPDATE UP!
[62] 11/19/22 T(515) _VMR 02:33:18.680280 DEBUG VMR_SITE_CLD.C[2779]: Callback
called to update node
[62] 11/19/22 T(515) _VMR 02:33:18.680295 DEBUG VMR_SITE_CLD.C[2875]: Entered
VMR_SITE_CLDRccp::add_ksysSiteCld NodeID: 2
[62] 11/19/22 T(515) _VMR 02:33:18.680301 DEBUG VMR_SITE_CLD.C[2881]: NodeID
Str:Node_2
```

```
[62] 11/19/22 T(515) _VMR 02:33:18.680305 DEBUG VMR_SITE_CLD.C[2885]: RCP Already
present. no need to create.
[62] 11/19/22 T(515) _VMR 02:33:18.680309 DEBUG VMR_SITE_CLD.C[1484]: nodeID(i):2,
(s):2
[62] 11/19/22 T(515) _VMR 02:33:18.680313 DEBUG VMR_SITE_CLD.C[2838]:
SITE:Node_2(0) KSYS State is being changed from: Down to: Up
[62] 11/19/22 T(2057) _VMR 02:33:18.806663 DEBUG VMR_SITE_CLD.C[1879]: Node:2
KsysState: Up
[62] 11/19/22 T(515) _VMR 02:33:18.807879 DEBUG VMR_SITE.C[8000]: INFO:
eventNotify entering. event:KSYS_NODE_STATUS_CHANGED, event type:2, comp:KSYS,
notificationLevel:low, dupEventProcess:
yes
[62] 11/19/22 T(515) _VMR 02:33:18.807954 DEBUG VMR_SITE_CLD.C[2976]:
updateManagingNode called. node_id:1
[62] 11/19/22 T(515) _VMR 02:33:18.807956 DEBUG VMR_SITE_CLD.C[2979]: No update
needed. ManagingNodeID:1
[62] 11/19/22 T(515) _VMR 02:33:18.807957 DEBUG VMR_SITE_CLD.C[2820]: No need to
update the threads as Managing node not changed!
...
[62] 11/19/22 T(937) _VMR 02:33:19.150712 DEBUG VMR_SITE.C[12051]: INFO:
sendNotification entering. event:KSYS_NODE_STATUS_CHANGED, event type:2,
comp:KSYS, notificationLevel:low, dupEventProcess:yes
```

Note: The logs can be collected from both the GL and non-GL nodes, unlike the **ksysmgr** commands, which run only on the GL KSYS node.

Group leader node and node status check

KSYS maintains all the KSYS node information in the new RCCP that is called IBM.VMR_SITE_CLD. If there are two KSYS nodes in the KSYS cluster, there will be two IBM.VMR_SITE_CLD RCCP resource configurations. The GL node information can be found in the IBM.VMR_SITE_CLD RCCP class, as shown in Example 8-19.

Example 8-19 Managing KSYS node check

```
(0) root @ ksys202gui: /
# lsrsrc IBM.VMR_SITE_CLD Name KsysNode KsysState
Resource Persistent Attributes for IBM.VMR_SITE_CLD
resource 1:
        Name      = "Node_2"
        KsysNode  = "2"
        KsysState = "Up"
resource 2:
        Name      = "Node_1"
        KsysNode  = "1"
        KsysState = "Up"

(0) root @ ksys202gui: /
#  lsrsrc -c IBM.VMR_SITE_CLD ManagingNode
Resource Class Persistent Attributes for IBM.VMR_SITE_CLD
resource 1:
        ManagingNode = "1"

(0) root @ ksys202gui: /
```

8.4.2 Error notifications and events

The KSYS subsystem tracks various events that occur in the environment and saves the information in the `/var/ksys/events.log` file on the GL KSYS node. The KSYS subsystem also sends emails and text notifications to the administrator if the contact information is registered while configuring the KSYS subsystem. The notifications are sent only from the GL KSYS node.

The **`ksysmgr`** commands can be run only from the GL KSYS node. If you attempt to run the commands on the non-GL node, an error message appears, as shown in Example 8-20. This feature will be enhanced to query and run operations from non-GL KSYS node in future releases.

Example 8-20 The ksysmgr output of both non-GL and GL KSYS nodes

```
(0) root @ ksys822p: /
# hostname
ksys822p.aus.stglabs.ibm.com

(0) root @ ksys822p: /
# ksysmgr q ksyscluster
ERROR: ksysmgr operations are not allowed from non-GL Node. Run commands from GL
Node:ksys202gui.aus.stglabs.ibm.com

(1) root @ ksys822p: /
#

# hostname
ksys202gui.aus.stglabs.ibm.com

(0) root @ ksys202gui: /
# ksysmgr query ksyscluster
Name:               SMR_DR
State:              Online
Type:               DR
Ksysnodes:          ksys202gui.aus.stglabs.ibm.com:1:Online    (Managing node)
                    ksys822p.aus.stglabs.ibm.com:2:Online

(0) root @ ksys202gui: /
```

When a non-GL KSYS node goes down, the `KSYS_NODE_STATUS_CHANGED` event is sent from the GL KSYS node. The event contains the node name and its status as `Down`. When this node rejoins the KSYS cluster, the same event is sent with the status as `Up`.

When a GL KSYS node goes down, the non-GL KSYS node takes over and sends the `KSYS_NODE_STATUS_CHANGED` event with the status as `Down` for the previous GL node. This node also sends the `KSYS_MANAGING_NODE_CHANGED` event notification that the node now is the GL node.

8.5 Migration considerations with PowerHA

This section describes the migration considerations from VMRM 1.6 (or an earlier version) when it is configured with PowerHA.

Before VMRM 1.7, KSYS HA could be achieved only by using PowerHA SystemMirror software where PowerHA SystemMirror was configured to monitor and manage the KSYS daemon by using custom scripts. If this usage was the only usage of PowerHA SystemMirror, most of the features of PowerHA SystemMirror were not used because it was used only to monitor the software or watch for network failures in the KSYS node. With this new feature in VMRM V1.7, PowerHA SystemMirror is no longer required to achieve KSYS HA.

If PowerHA is installed, you can perform the steps that are described in this section to migrate the KSYS nodes to VMRM 1.7 as an offline migration.

8.5.1 Migration overview

In this sample scenario, the KSYS cluster is created with PowerHA SystemMirror on node KSYS_A (GL node) and node KSYS_B. Complete the following steps:

1. Stop PowerHA service on both nodes.
2. Upgrade the node KSYS_A and verify that it has the latest version.
3. Upgrade the node KSYS_B and verify that it has latest version.
4. PowerHA can be uninstalled. From now on, the KSYS HA is handled by the KSYS node itself.
5. Check for the KSYS cluster, and run discovery and verify operations.

8.5.2 Detailed migration steps

Here are the detailed steps with an example showing how to migrate the existing VMRM 1.6 that is configured with PowerHA to VMRM 1.7.

Example 8-21 shows the starting configuration.

Example 8-21 Upgrade scenario test cluster details

```
(0) root @ ksys915: /usr/es/sbin/cluster/utilities
# date; clcmd /opt/IBM/ksys/ksysmgr query version
Fri Nov 18 07:06:24 CST 2022

-------------------------------
NODE ksys916.ausprv.stglabs.ibm.com
-------------------------------
Ksysmgr version: 1.6.0.0
Ksys version:    1.6.0.0

-------------------------------
NODE ksys915.ausprv.stglabs.ibm.com
-------------------------------
Ksysmgr version: 1.6.0.0
Ksys version:    1.6.0.0

(0) root @ ksys915: /usr/es/sbin/cluster/utilities
```

```
# cltopinfo
Cluster Name:    dd_test
Cluster Type:    Linked
Heartbeat Type:  Unicast
Repository Disks:
        Site 1 (site1@ksys915): hdisk1
        Site 2 (site2@ksys916): hdisk2
Cluster Nodes:
        Site 1 (site1):
                ksys915
        Site 2 (site2):
                ksys916

There are 2 nodes and 1 networks defined

NODE ksys915:
        Network net_ether_01
                ksys915 10.xxx.xxx.xxx

NODE ksys916:
        Network net_ether_01
                ksys916 10.xxx.xxx.xxx

Resource Group ksysRG
        Startup Policy   Online On First Available Node
        Fallover Policy  Fallover To Next Priority Node In The List
        Fallback Policy  Never Fallback
        Participating Nodes      ksys915 ksys916

(0) root @ ksys915: /usr/es/sbin/cluster/utilities
#

(0) root @ ksys915: /usr/es/sbin/cluster/utilities
# clRGinfo
-----------------------------------------------------------------------------
Group Name                   State            Node
-----------------------------------------------------------------------------
ksysRG                       ONLINE           ksys915
                             OFFLINE          ksys916


(0) root @ ksys915: /usr/es/sbin/cluster/utilities
# clcmd lssrc -ls clstrmgrES| grep state
Current state: ST_STABLE
Current state: ST_STABLE
```

1. Run discovery and verification operations on the GL node, which in this case it is *ksys915*. as shown in Example 8-22.

Example 8-22 The ksysmgr verify command on the GL node

```
(0) root @ ksys915: /usr/es/sbin/cluster/utilities
# ksysmgr -t verify site INDIA
06:26:35 Site verification started for INDIA
        06:26:54 Default_HG verification has started
        06:26:54 HG verification has started
        06:26:54 gdrnova1-8286-42A-107C5DT verification has started
        06:26:54 gdrnova1-8286-42A-107C5DT verification has completed
        06:26:54 gdrnova110 DR verification has started
        06:26:54 gdrnova110 DR verification has completed
        06:26:54 gdrnova106 DR verification has started
        06:26:54 gdrnova106 DR verification has completed
        06:26:54 gdrnova107 DR verification has started
        06:26:54 gdrnova107 DR verification has completed
        06:26:54 Default_HG verification has completed
        06:26:54 Disk Group verification on storage subsystem started for
Workgroup wg_gdrnova1
        06:29:35 Disk Group verification on storage subsystem completed for
Workgroup wg_gdrnova1
        06:29:50 gdrnova208 DR verification has started
        06:29:50 gdrnova210 DR verification has started
        06:29:50 gdrnova209 DR verification has started
        06:29:50 gdrnova207 DR verification has started
        06:30:01 gdrnova208 DR verification has completed
        06:30:01 gdrnova210 DR verification has completed
        06:30:01 gdrnova209 DR verification has completed
        06:30:01 gdrnova207 DR verification has completed
        06:30:01 Disk Group verification on storage subsystem started for
Workgroup wg_gdrnova2
        06:32:44 Disk Group verification on storage subsystem completed for
Workgroup wg_gdrnova2
        06:32:49 HG verification has completed
06:33:13 Verification has finished for INDIA
7 out of 7 VMs have been successfully verified
```

2. Stop the PowerHA service on both nodes by running **`smit clstop`**.

Example 8-23 Stopping the PowerHA cluster

```
Command: OK            stdout: yes           stderr: no

Before command completion, additional instructions may appear below.

ksys915: 0513-004 The Subsystem or Group, clinfoES, is currently inoperative.
ksys915: 0513-044 The clevmgrdES Subsystem was requested to stop.
ksys915: Nov 18 2022 07:07:21/usr/es/sbin/cluster/utilities/clstop: called with
flags -N -g
ksys916: 0513-004 The Subsystem or Group, clinfoES, is currently inoperative.
ksys916: Nov 18 2022 07:11:07/usr/es/sbin/cluster/utilities/clstop: called with
flags -N -g
ksys916: 0513-044 The clevmgrdES Subsystem was requested to stop.
```

```
(0) root @ ksys915: /usr/es/sbin/cluster/utilities
# date; clcmd lssrc -ls clstrmgrES| grep state
Fri Nov 18 07:12:18 CST 2022
Current state: ST_INIT
Current state: ST_INIT

(127) root @ ksys915: /usr/es/sbin/cluster/utilities
# date; clRGinfo
Fri Nov 18 07:12:36 CST 2022
Cluster IPC error: The cluster manager on node ksys915.ausprv.stglabs.ibm.com is
in ST_INIT or NOT_CONFIGURED state and cannot process the IPC request.

(0) root @ ksys916: /usr/es/sbin/cluster/utilities
# lssrc -ls clstrmgrES| grep state
Current state: ST_INIT
```

3. Migrate the KSYS nodes from Version 1.6 to Version 1.7.

   As part of the migration, the KSYS daemon is restarted, and you might see the transition of GL between the nodes. as shown in Example 8-24.

Example 8-24 Upgrading the KSYS code

```
(0) root @ ksys915: /# date; ksysmgr query version
Fri Nov 18 07:27:29 CST 2022
ERROR: ksysmgr operations are not allowed from non-GL Node. Run commands from GL
Node:
# lslpp -l | grep ksys
  ksys.ha.license            1.7.0.0  COMMITTED  Base Server Runtime
  ksys.hautils.rte           1.7.0.0  COMMITTED  Base Server Runtime
  ksys.license               1.7.0.0  COMMITTED  Base Server Runtime
  ksys.main.cmds             1.7.0.0  COMMITTED  Base Server Runtime
  ksys.main.msg.en_US.cmds   1.7.0.0  COMMITTED  Base Server Runtime - US
  ksys.main.rte              1.7.0.0  COMMITTED  Base Server Runtime
```

4. Verify that the RSCS cluster is built correctly on both the nodes by running **`lsrsrc`** on the cluster nodes (in our case, `IBM.VMR_SITE_CLD`), as shown in Example 8-25.

Example 8-25 RSCS query

```
(0) root @ ksys915: /
# lsrsrc IBM.VMR_SITE_CLD
Resource Persistent Attributes for IBM.VMR_SITE_CLD
resource 1:
        Name             = "Node_1"
        SiteID           = 0
...
        KsysNode         = "1"
        KsysState        = "Up"
        KsysNodeList     = {}
        ActivePeerDomain = "dd_test"
resource 2:
        Name             = "Node_2"
        SiteID           = 0
 ...
        KsysNode         = "2"
        KsysState        = "Up"
        KsysNodeList     = {}
        ActivePeerDomain = "dd_test"
```

Note: After migrating to Version 1.7, if the output to the **lsrsrc** command that is shown in Example 8-25 shows only one node entry, restart the KSYS daemon on both nodes by using **stopsrc -s IBM.VMR -c;startsrc -s IBM.VMR**. The scenario with only one IBM.VMR_SITE_CLD RCP can happen when both nodes start concurrently, which never happens when the KSYS cluster is created by running the **ksysmgr create ksyscluster** command.

5. If you are not using PowerHA SystemMirror for any other nodes, you can uninstall it. If you continue to use PowerHA SystemMirror, then stop monitoring the KSYS nodes in PowerHA SystemMirror, and you can continue to use PowerHA SystemMirror for any other activities. From now on, the KSYS HA is handled by the KSYS nodes.

9

IBM VMRM GUI deployment

This chapter introduces the IBM Virtual Machine Recovery Manager High Availability (VMRM HA) GUI for Power deployment.

The following topics are described in this chapter:

- Overview
- GUI requirements
- Configuring VMRM HA by using the GUI
- VMRM dashboard
- GUI limitations

9.1 Overview

The GUI supports administrative functions and displays the topology of the high availability (HA), disaster recovery (DR), high availability and disaster recovery (HADR), and HADRHA KSYS configurations. The deployment wizard provides an easy way to deploy the VMRM solutions for all cluster types.

With the VRRM GUI, you can create and manage your VMRM environment by monitoring the status of the VMRM components and restart virtual machines (VMs), migrate VMs, and clean up VMs. The GUI supports enhanced security capabilities for managing your VMRM environment, such as user-role definition and two-factor authentication.

9.2 GUI requirements

To use the VMRM DR and manage KSYS nodes by using the GUI, install the GUI server and GUI agent file sets on a system. The logical partition (LPAR) in which you want to install the GUI file sets, must be running IBM AIX 7.2 with Technology Level 2 Service Pack 1 (7200-02-01) or later. You can choose to install the GUI server and GUI agent file sets on one of the KSYS nodes.

Install the GUI server and GUI agent file sets before you start using the VMRM DR GUI. Depending on your system environment and your requirements, choose the appropriate procedure to install the GUI server and GUI agent file sets.

Before installing the GUI on your KSYS host, verify the file sets that are needed by running the **lslpp** command, as shown in Example 9-1.

Example 9-1 The lslpp command output to check GUI requirements

```
(0) root @ capzp1p10: /
# lslpp -l |grep ksys.*
  ksys.drutils.rte          1.7.0.0  COMMITTED  Base Server Runtime
  ksys.ha.license           1.7.0.0  COMMITTED  Base Server Runtime
  ksys.hautils.rte          1.7.0.0  COMMITTED  Base Server Runtime
  ksys.hsmon.rte            1.7.0.0  COMMITTED  Base Server Runtime
  ksys.license              1.7.0.0  COMMITTED  Base Server Runtime
  ksys.main.cmds            1.7.0.0  COMMITTED  Base Server Runtime
  ksys.main.msg.DE_DE.cmds  1.7.0.0  COMMITTED  Base Server Runtime - German
  ksys.main.msg.ES_ES.cmds  1.7.0.0  COMMITTED  Base Server Runtime - Spanish
  ksys.main.msg.FR_FR.cmds  1.7.0.0  COMMITTED  Base Server Runtime - French
  ksys.main.msg.IT_IT.cmds  1.7.0.0  COMMITTED  Base Server Runtime - Italian
  ksys.main.msg.JA_JP.cmds  1.7.0.0  COMMITTED  Base Server Runtime - Japanese
  ksys.main.msg.PT_BR.cmds  1.7.0.0  COMMITTED  Base Server Runtime -
  ksys.main.msg.ZH_CN.cmds  1.7.0.0  COMMITTED  Base Server Runtime -
  ksys.main.msg.ZH_TW.cmds  1.7.0.0  COMMITTED  Base Server Runtime -
  ksys.main.msg.en_US.cmds  1.7.0.0  COMMITTED  Base Server Runtime - US
  ksys.main.rte             1.7.0.0  COMMITTED  Base Server Runtime
  ksys.mirror.ds8k.rte      1.7.0.0  COMMITTED  Base Server Runtime
  ksys.mirror.emc.rte       1.7.0.0  COMMITTED  Base Server Runtime
  ksys.mirror.hitachi.rte   1.7.0.0  COMMITTED  Base Server Runtime
  ksys.mirror.svc.rte       1.7.0.0  COMMITTED  Base Server Runtime
  ksys.mirror.unity.rte     1.7.0.0  COMMITTED  Base Server Runtime
  ksys.mirror.xiv.rte       1.7.0.0  COMMITTED  Base Server Runtime
  ksys.ui.agent             1.7.0.0  COMMITTED  VMRestart User Interface -
  ksys.ui.common            1.7.0.0  COMMITTED  VMRestart User Interface -
  ksys.ui.server            1.7.0.0  COMMITTED  VMRestart User Interface -
  ksys.vmmon.rte            1.7.0.0  COMMITTED  Base Server Runtime
  ksys.drutils.rte          1.7.0.0  COMMITTED  Base Server Runtime
  ksys.hautils.rte          1.7.0.0  COMMITTED  Base Server Runtime
  ksys.hsmon.rte            1.7.0.0  COMMITTED  Base Server Runtime
  ksys.main.cmds            1.7.0.0  COMMITTED  Base Server Runtime
  ksys.main.rte             1.7.0.0  COMMITTED  Base Server Runtime
  ksys.mirror.ds8k.rte      1.7.0.0  COMMITTED  Base Server Runtime
  ksys.mirror.emc.rte       1.7.0.0  COMMITTED  Base Server Runtime
  ksys.mirror.hitachi.rte   1.7.0.0  COMMITTED  Base Server Runtime
  ksys.mirror.svc.rte       1.7.0.0  COMMITTED  Base Server Runtime
  ksys.mirror.unity.rte     1.7.0.0  COMMITTED  Base Server Runtime
  ksys.mirror.xiv.rte       1.7.0.0  COMMITTED  Base Server Runtime
  ksys.ui.agent             1.7.0.0  COMMITTED  VMRestart User Interface -
  ksys.ui.server            1.7.0.0  COMMITTED  VMRestart User Interface -
  ksys.vmmon.rte            1.7.0.0  COMMITTED  Base Server Runtime
(0) root @ capzp1p10: /
```

Note: You can install the VMRM GUI on servers other than KSYS host by installing both the GUI server file sets, as described in 9.3.2, "Installing GUI server file sets" on page 243.

9.3 Installing the GUI

Install the following GUI server and GUI agent file sets before you start using the VMRM DR GUI. If you are installing the GUI on a system that is running the KSYS, install the GUI server and GUI agents. For a KSYS system where you will not be running the GUI server, install the GUI agent. For a system that is not running a KSYS but is managing one or more KSYS systems, install the GUI server file sets.

Depending on your system environment and your requirements, choose a procedure to install the GUI server and GUI agent file sets:

- 9.3.1, "Installing the GUI server file sets and GUI agent file sets" on page 239
- 9.3.2, "Installing GUI server file sets" on page 243
- 9.3.3, "Installing GUI agent file sets" on page 243

9.3.1 Installing the GUI server file sets and GUI agent file sets

To install the GUI server and GUI agent file sets on a machine where the KSYS file sets already are installed, complete the following steps:

1. Ensure that all the prerequisites that are specified in "GUI requirements" on page 238 are met.
2. To install both the GUI server and the GUI agent file sets on one of the KSYS nodes, run the following command:

   ```
   installp -acFXYd fileset_location -V2 [-e filename.log] ksys.ui.server
   ksys.ui.agent ksys.ui.common
   ```

Example 9-2 shows the output.

Example 9-2 Installing GUI file sets on KSYS hosts (server and client)

```
# installp -acFXYd . -V2 /tmp/uilog.txt ksys.ui.server ksys.ui.agent
ksys.ui.common
+-----------------------------------------------------------------------------+
                    Pre-installation Verification...
+-----------------------------------------------------------------------------+
Verifying selections...done
Verifying requisites...done
Results...
... output omitted...

Installation Summary
--------------------
Name                        Level           Part        Event       Result
-------------------------------------------------------------------------------
ksys.ui.server              1.7.0.0         USR         APPLY       SUCCESS
ksys.ui.server              1.7.0.0         ROOT        APPLY       SUCCESS
ksys.ui.common              1.7.0.0         USR         APPLY       SUCCESS
ksys.ui.agent               1.7.0.0         USR         APPLY       SUCCESS
ksys.ui.agent               1.7.0.0         ROOT        APPLY       SUCCESS
```

3. To install the open source software packages, which are not included in the installed file sets, go to one of the following procedures, depending on your system environment:
   – “If your system is connected to the internet” on page 240
   – “If your system is configured to use an HTTP proxy to access the internet” on page 242
   – “If your system is not connected to the internet” on page 242

If your system is connected to the internet

If your system is connected to the internet, run the following command in your system:

```
/opt/IBM/ksys/ui/server/dist/server/bin/vmruiinst.ksh
```

This command downloads and installs the open source software packages that are not included in the file sets because these files are licensed under the GNU General Public License (GPL). The output is shown in Example 9-3.

Example 9-3 Running /opt/IBM/ksys/ui/server/dist/server/bin/vmruiinst.ksh

```
# /opt/IBM/ksys/ui/server/dist/server/bin/vmruiinst.ksh
Warning: "/tmp/vmruiinst.downloads" does not exist. Creating...
"/tmp/vmruiinst.downloads" has been created.

Checking if the requisites have already been downloaded...
        ** "info-6.6-2.aix6.1.ppc.rpm" needs to be retrieved.
        ** "cpio-2.13-1.aix6.1.ppc.rpm" needs to be retrieved.
        ** "readline-8.0-2.aix6.1.ppc.rpm" needs to be retrieved.
        ** "libiconv-1.16-1.aix6.1.ppc.rpm" needs to be retrieved.
        ** "bash-5.0.18-1.aix6.1.ppc.rpm" needs to be retrieved.
        ** "gettext-0.20.2-1.aix6.1.ppc.rpm" needs to be retrieved.
        ** "libgcc-8.3.0-2.aix7.2.ppc.rpm" needs to be retrieved.
        ** "libstdcplusplus-8.3.0-2.aix7.2.ppc.rpm" needs to be retrieved.
        Total number of requisite downloads needed: 8
```

```
This will download and install the packages that are needed by VMRM UI installation:
To use the Virtual Machine Recovery Manager HADR for AIX GUI, you must install third-party
files. These third-party files were not included in the server file sets because they are
licensed under the General Public License (GPL). This script downloads and installs the files
that are required by SQLite and Node.js.
    SQLite dependencies:                   | Node.js dependencies:
    ====================================== | =======================
        bash                info           | libgcc
        libiconv            readline       | libstdc++
        gettext             cpio           |
The files that are required for Node.js are used on the server, and are also
installed on each cluster node automatically during the cluster discovery
operation.
IBM does not offer support for these files if the files are used outside the
context of the Virtual Machine Recovery Manager HADR GUI.

Do you want to download and install these files? (y/n)  y
***
***
    The downloads have started and can take several minutes.
    Wait for the downloads to complete.
***
(NOTE: The progress bar is a best-guess approximation, and may not be perfectly accurate)

Downloading "/tmp/vmruiinst.downloads/info-6.6-2.aix6.1.ppc.rpm"...
Downloading "/tmp/vmruiinst.downloads/cpio-2.13-1.aix6.1.ppc.rpm"...
Downloading "/tmp/vmruiinst.downloads/readline-8.0-2.aix6.1.ppc.rpm"...
Downloading "/tmp/vmruiinst.downloads/libiconv-1.16-1.aix6.1.ppc.rpm"...
Downloading "/tmp/vmruiinst.downloads/bash-5.0.18-1.aix6.1.ppc.rpm"...
Downloading "/tmp/vmruiinst.downloads/gettext-0.20.2-1.aix6.1.ppc.rpm"...
Downloading "/tmp/vmruiinst.downloads/libgcc-8.3.0-2.aix7.2.ppc.rpm"...
Downloading "/tmp/vmruiinst.downloads/libstdcplusplus-8.3.0-2.aix7.2.ppc.rpm"...
[======================================>]  12734559 @ 12734559 (100.00%)

"info-6.6-2.aix6.1.ppc.rpm" has been successfully downloaded.
"cpio-2.13-1.aix6.1.ppc.rpm" has been successfully downloaded.
"readline-8.0-2.aix6.1.ppc.rpm" has been successfully downloaded.
"libiconv-1.16-1.aix6.1.ppc.rpm" has been successfully downloaded.
"bash-5.0.18-1.aix6.1.ppc.rpm" has been successfully downloaded.
"gettext-0.20.2-1.aix6.1.ppc.rpm" has been successfully downloaded.
"libgcc-8.3.0-2.aix7.2.ppc.rpm" has been successfully downloaded.
"libstdcplusplus-8.3.0-2.aix7.2.ppc.rpm" has been successfully downloaded.

Attempting to install any needed requisites.
Warning: "/opt/IBM/ksys/ui/lib" does not exist. Creating...
"/opt/IBM/ksys/ui/lib" has been created.

-- output omitted ...

Adding execution permission to the PAM module (/opt/IBM/ksys/ui/server/lib/auth/smuiauth)
Configuring the PAM system for authentication support for our module.

Attempting to start the server...
The server was successfully started.
The installation completed successfully. To use the Virtual Machine Recovery Manager HADR GUI,
open a web browser and enter the following URL:

 https://9.x.x.x:3000/login
```

Important: Answer “y” to the process for it to download and install the software.

After the **vmruiinst.ksh** command completes, a message displays a URL for the VMRM HA GUI server. This URL is used to connect a web browser to the GUI server LPAR. Go to 9.4, “Configuring VMRM HA by using the GUI” on page 245 to continue configuring your VMRM system.

If your system is configured to use an HTTP proxy to access the internet

If your system is configured to use an HTTP proxy to access the internet, run the following command in your system to specify the proxy information:

```
/opt/IBM/ksys/ui/server/dist/server/bin/vmruiinst.ksh -p
```

You also can specify the proxy information by using the **http_proxy** environment variable:

```
/opt/IBM/ksys/ui/server/dist/server/bin/vmruiinst.ksh [-p <HTTP_PROXY>] [-P
<HTTPS_PROXY>]
```

The results are the same, as shown in Example 9-3 on page 240.

After the **vmruiinst.ksh** command completes, a message displays a URL for the VMRM HA GUI server. This URL is used to connect a web browser to the GUI server LPAR. Go to 9.4, “Configuring VMRM HA by using the GUI” on page 245 to continue configuring your VMRM system.

If your system is not connected to the internet

If your system is not connected to the internet, complete the following steps:

1. Copy the `vmruiinst.ksh` file from your system to a system that is running the AIX operating system and that has internet access.
2. Run the **vmruiinst.ksh -d /directory** command. **/directory** is the location where you want to download the open source software packages, for example, **/vmruiinst.ksh -d /tmp/vmrui_rpms**. The following package managers are downloaded into the specified directory:
   - info-6.6-2.aix6.1.ppc.rpm
   - cpio-2.13-1.aix6.1.ppc.rpm
   - readline-8.0-2.aix6.1.ppc.rpm
   - libiconv-1.16-1.aix6.1.ppc.rpm
   - bash-5.0.18-1.aix6.1.ppc.rpm
   - gettext-0.20.2-1.aix6.1.ppc.rpm
   - libgcc-8.3.0-2.aix7.1.ppc.rpm
   - libstdcplusplus-8.3.0-2.aix7.1.ppc.rpm
3. Copy the downloaded software packages to a local system directory.
4. In your system, run the **vmruiinst.ksh -i /directory** command. **/directory** is the location where you copied the downloaded software packages.

The output is similar to Example 9-3 on page 240.

After the **vmruiinst.ksh** command completes, a message displays a URL for the VMRM HA GUI server. This URL is used to connect a web browser to the GUI server LPAR. Go to 9.4, “Configuring VMRM HA by using the GUI” on page 245 to continue configuring your VMRM system.

9.3.2 Installing GUI server file sets

If you want to install the GUI on a system that is not running a KSYS, install the GUI server file sets. The GUI agent file sets must be installed on each of your KSYS systems that will be managed by the GUI. To install only the GUI server file sets on a machine where GUI agent file sets and KSYS file sets are not installed, complete the following steps:

1. Ensure that all the prerequisites that are specified in 9.2, “GUI requirements” on page 238 are met.
2. To install only the GUI server file sets on a separate system that manages all the KSYS nodes, run the following command:

   ```
   installp -acFXYd fileset_location -V2 [-e filename.log] ksys.ha.license
   ksys.ui.server ksys.ui.common
   ```

3. To install the open source software packages, which are not included in the installed file sets, choose one of the following procedures depending on your system environment:
   - “If your system is connected to the internet” on page 240
   - “If your system is configured to use an HTTP proxy to access the internet” on page 242
   - “If your system is not connected to the internet” on page 242

9.3.3 Installing GUI agent file sets

To communicate with the GUI, the KSYS needs the GUI agent installed. If you are not running the GUI server on your KSYS system, then you install only the agent file sets. This section describes the steps that are required to install only GUI agents on a machine where the KSYS file sets are installed and the GUI server file sets will not be installed. Install the KSYS file sets on the machine before installing the GUI agent file sets.

1. Ensure that all the prerequisites that are specified in “GUI requirements” on page 238 are met.
2. To install only GUI agent file sets on a separate system that manages all the KSYS nodes, run the following command:

   ```
   installp -acFXYd fileset_location -V2 [-e filename.log] ksys.ui.agent
   ksys.ui.common
   ```

3. To install the open source software packages, which are not included in the installed file sets, choose one of the following procedures, depending on your system environment:
   - “Installing the agent file sets when your machine is connected to the internet” on page 244
   - “Installing the agent file sets when you are using an HTTP proxy” on page 244
   - “If your system is not connected to the internet” on page 242

Installing the agent file sets when your machine is connected to the internet

If your system is connected to the internet, run the following command in the GUI agent LPAR:

```
/opt/IBM/ksys/ui/agent/lib/vmragentinst.ksh
```

This command downloads and installs the open source software packages that are not included in the file sets because these files are licensed under the GPL.

Installing the agent file sets when you are using an HTTP proxy

If your system is configured to use an HTTP proxy to access the internet, run the following command in your system to specify the proxy information:

```
/opt/IBM/ksys/ui/agent/lib/vmragentinst.ksh -p
```

You also can specify the proxy information by using the **`http_proxy`** environment variable.

Installing the agent file set when your machine is not connected to the internet

If your system is not connected to the internet, complete the following steps:

1. Copy the `vmragentinst.ksh` file from your system to a system that is running the AIX operating system and has internet access.
2. Run the **`vmragentinst.ksh -d /directory`** command. **`/directory`** is the location where you want to download the open source software packages, for example, `/vmragentinst.ksh -d /tmp/vmrui_rpms`. The following package managers are downloaded into the specified directory:

   ```
   libgcc-8.3.0-2.aix7.1.ppc.rpm
   libstdcplusplus-8.3.0-2.aix7.1.ppc.rpm
   ```

3. Copy the downloaded software packages to a directory in your system.
4. In your system, run the **`vmragentinst.ksh -i /directory`** command. **`/directory`** is the location where you copied the downloaded software packages.

9.3.4 Installing the VMRM DR GUI on AIX 7.3

Starting with VMRM DR 1.6, the VMRM DR GUI supports AIX 7.3.

To install the GUI file sets on the AIX 7.3 operating system, complete the following steps:

1. Follow the procedure that is described in 9.3.1, “Installing the GUI server file sets and GUI agent file sets” on page 239, and then run the **`vmruiinst.sh`** script.
2. Manually download and install the `libgcc` and `libstdc++` libraries that are compatible with the AIX 7.3 operating system. You can download these packages from the following links:
   - gcc10 rpms
   - meta rpms
3. To start the GUI server, run the following command:

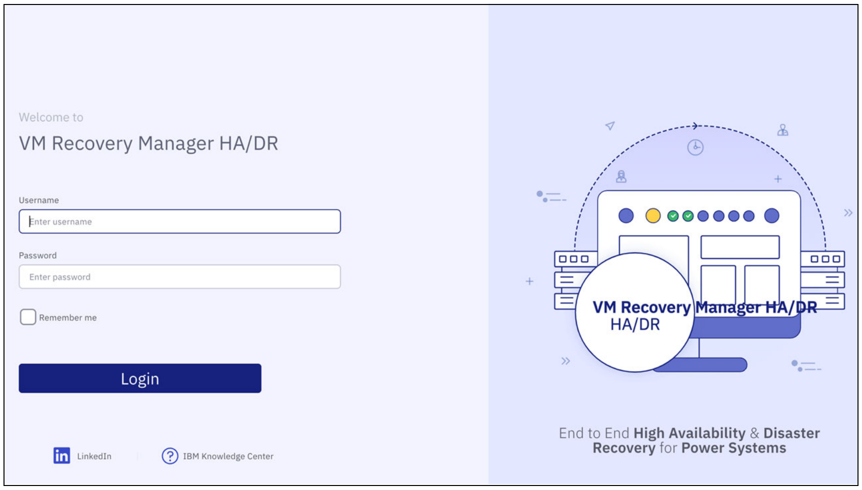
   ```
   startsrc -s vmruiserver
   ```

9.4 Configuring VMRM HA by using the GUI

This section demonstrates how to do the initial configuration and discovery of the infrastructure for a VMRM HA cluster that uses the GUI.

Complete the following steps:

1. After installing the VMRM GUI, use the URL that was presented at the end of the installation to log in to the GUI (see Figure 9-3 on page 246). The login window is shown in Figure 9-1.



Welcome to

VM Recovery Manager HA/DR

Username

Enter username

Password

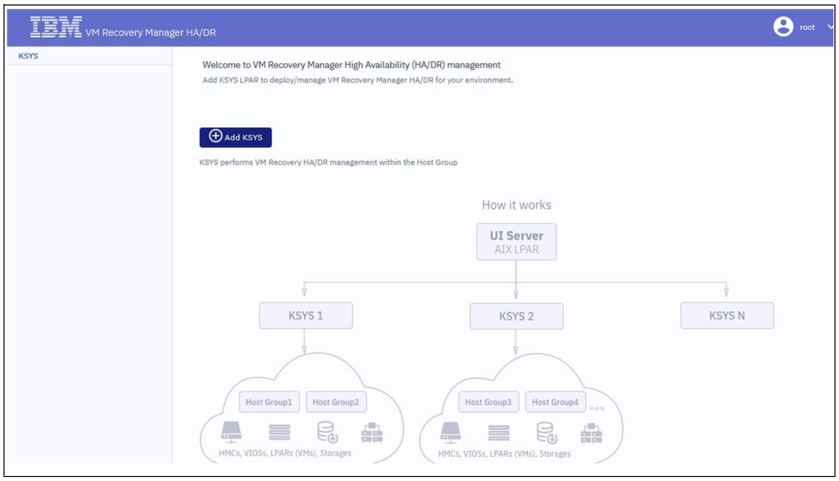
Enter password

□ Remember me

Login
LinkedIn
IBM Knowledge Center
VM Recovery Manager HA/DR
End to End High Availability & Disaster Recovery for Power Systems

Figure 9-1 VMRM GUI login window

After logging in to the VMRM HA GUI, the window that is shown in Figure 9-2 opens.



Welcome to VM Recovery Manager High Availability (HA/DR) management

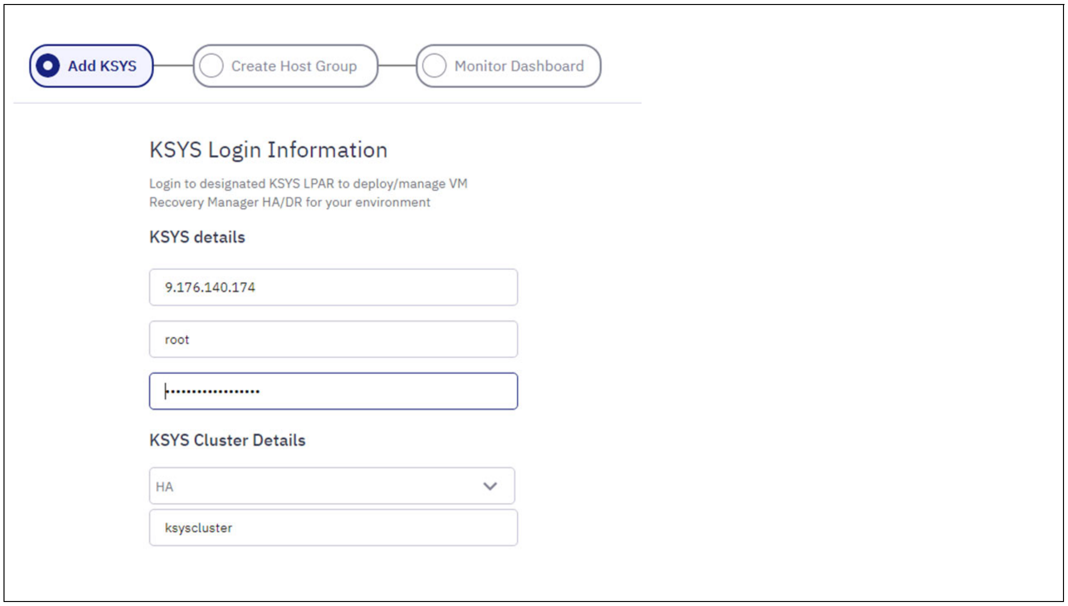
Add KSYS LPAR to deploy/manage VM Recovery Manager HA/DR for your environment.

KSYS performs VM Recovery HA/DR management within the Host Group

Figure 9-2 First login window

2. Add a KSYS by clicking **Add KSYS**. The VMRM GUI can manage one or more KSYS systems.

3. After clicking **Add KSYS**, as shown in Figure 9-3, input the following KSYS login information:
   - KSYS IP address
   - Root user
   - Password
   - Cluster Type
4. In this case, we chose **HA** as the cluster type. Here is where you define what type of cluster that you are defining: HA, DR, HADR, or HADRHA. After you input the KSYS login information, add the host group, and then select **Create Host Group**.



KSYS Login Information

Login to designated KSYS LPAR to deploy/manage VM Recovery Manager HA/DR for your environment

KSYS details

9.176.140.174

root

••••••••••••••••

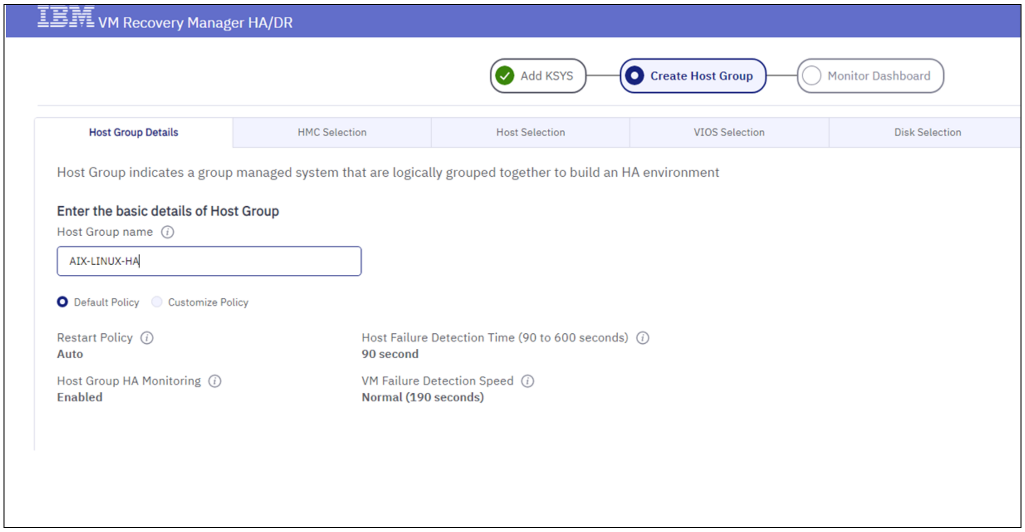
KSYS Cluster Details

HA

ksyscluster

Figure 9-3 Login information that is needed to add a KSYS

5. In the Create Host Group window, add the host group name, as shown in Figure 9-4. You can choose to take the default policies for the host group or you can customize them here.



Host Group indicates a group managed system that are logically grouped together to build an HA environment

Enter the basic details of Host Group

Host Group name ⓘ

AIX-LINUX-HA

● Default Policy ○ Customize Policy

Restart Policy ⓘ
Auto

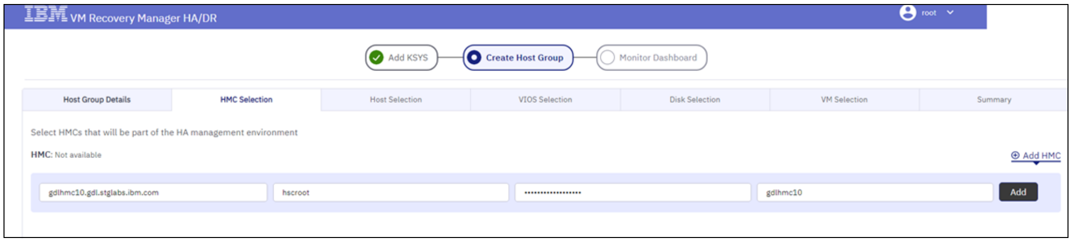
Host Failure Detection Time (90 to 600 seconds) ⓘ
90 second

Host Group HA Monitoring ⓘ
Enabled

VM Failure Detection Speed ⓘ
Normal (190 seconds)

Figure 9-4 Creating a host group

6. Go to the **HMC** tab. In the HMC Selection window, enter the Hardware Management Console (HMC) information, as shown in Figure 9-5.



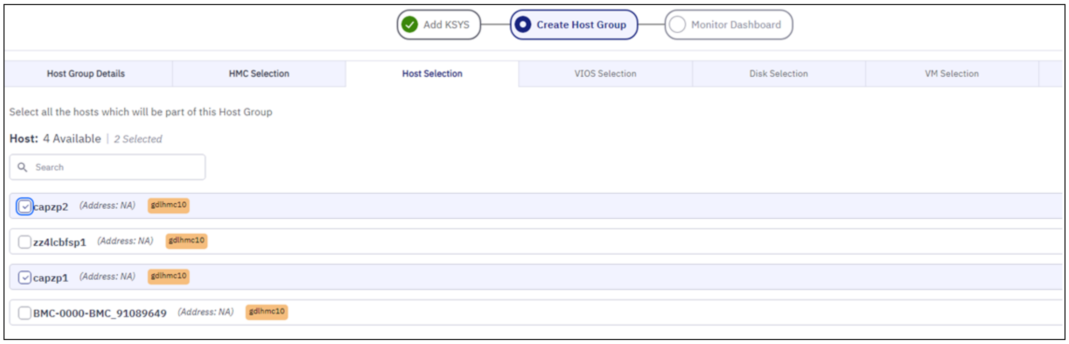
Select HMCs that will be part of the HA management environment

HMC: Not available

gdlhmc10.gdl.stglabs.ibm.com | hscroot | •••••••••••••••••• | gdlhmc10

Figure 9-5 HMC selection window

7. Select the **Host Selection** tab. In the Host Selection window, select the hosts that will be part of this host group. The hosts that are listed are the hosts that the HMC is managing. In this case, select hosts `capzp1` and `capzp2`, as shown in Figure 9-6.



Select all the hosts which will be part of this Host Group

Host: 4 Available | *2 Selected*

☑ capzp2 *(Address: NA)* gdlhmc10

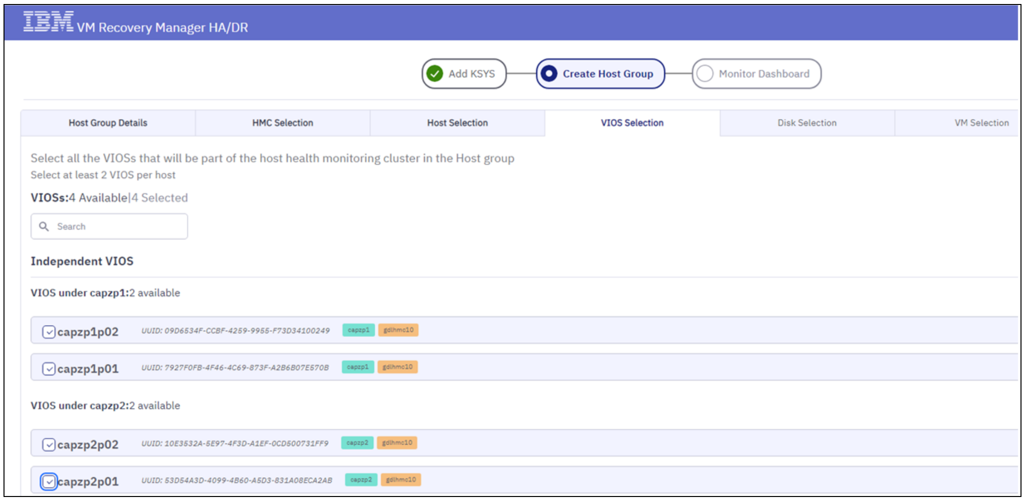
☐ zz4lcbfsp1 *(Address: NA)* gdlhmc10

☑ capzp1 *(Address: NA)* gdlhmc10

☐ BMC-0000-BMC_91089649 *(Address: NA)* gdlhmc10

Figure 9-6 Selecting hosts to add

8. In the Virtual I/O Server (VIOS) Selection window, select the VIOSs from the hosts, as shown in Figure 9-7. The VIOSs are discovered from the hosts in the host group. You should have at least two VIOS per host with a maximum of 12 hosts and 24 VIOS in a single host group.



Select all the VIOSs that will be part of the host health monitoring cluster in the Host group
Select at least 2 VIOS per host

VIOSs:4 Available|4 Selected

Independent VIOS

VIOS under capzp1:2 available

☑ capzp1p02 *UUID: 09D6534F-CCBF-4259-9955-F73D34100249* capzp1 gdlhmc10

☑ capzp1p01 *UUID: 7927F0FB-4F46-4C69-873F-A2B6B07E570B* capzp1 gdlhmc10

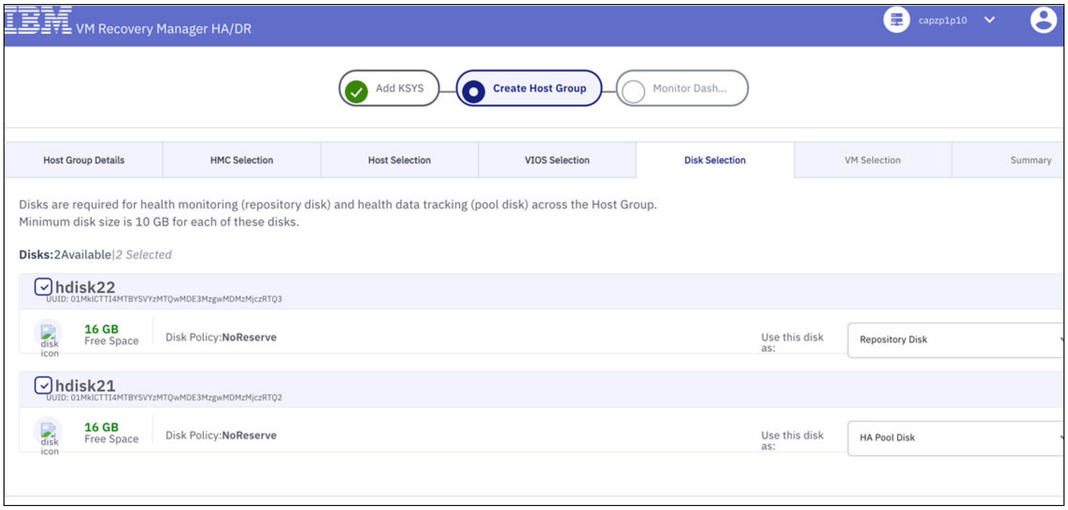
VIOS under capzp2:2 available

☑ capzp2p02 *UUID: 10E3532A-5E97-4F3D-A1EF-0CD500731FF9* capzp2 gdlhmc10

☑ capzp2p01 *UUID: 53D54A3D-4099-4B60-A5D3-831A08ECA2AB* capzp2 gdlhmc10

Figure 9-7 VIOS Selection window

9. Select the **Disk Selection** tab. The GUI looks for unused disks that are connected to all the VIOSs and meet the requirements for the Shared Storage Pool (SSP) disks. You must have two disks, each with at least 10 GB each, which are shared between all VIOSs. Choose the disks to use as the Repository Disk and HA Pool Disk, as shown in Figure 9-8.



Disks are required for health monitoring (repository disk) and health data tracking (pool disk) across the Host Group.
Minimum disk size is 10 GB for each of these disks.

Disks:2Available|*2 Selected*

☑ **hdisk22**
UUID: 01MkICTTI4MTBYSVYzMTQwMDE3MzgwMDMzMjczRTQ3

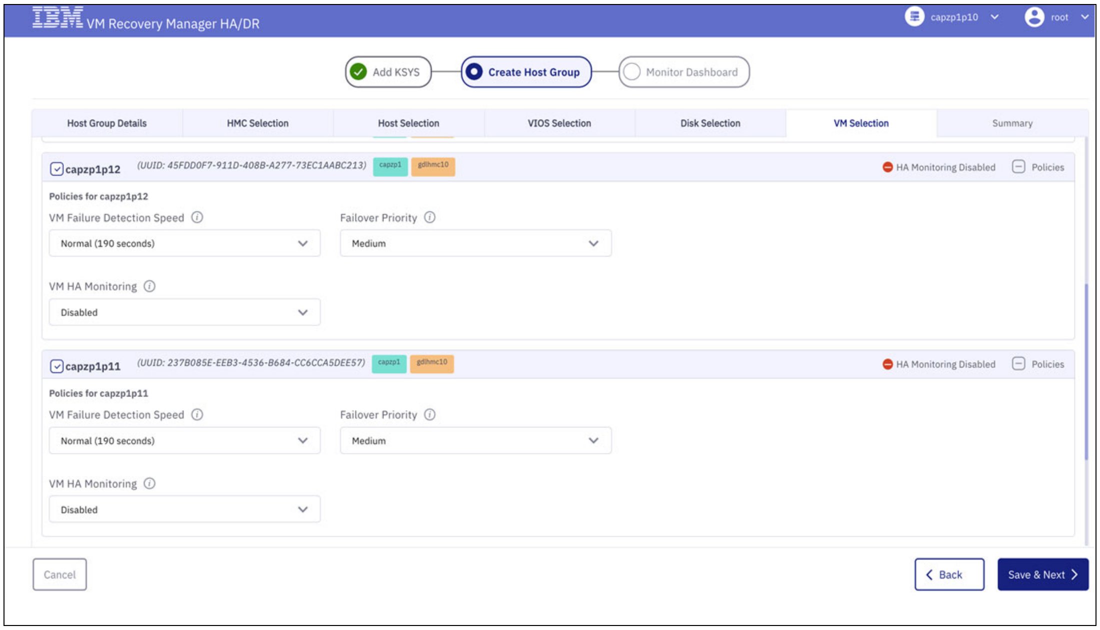
16 GB Free Space | Disk Policy:**NoReserve** | Use this disk as: Repository Disk

☑ **hdisk21**
UUID: 01MkICTTI4MTBYSVYzMTQwMDE3MzgwMDMzMjczRTQ2

16 GB Free Space | Disk Policy:**NoReserve** | Use this disk as: HA Pool Disk

Figure 9-8 VIOS disks selection

10. Select the **VM Selection** tab. In the VM Selection window, you are prompted to select the VMs that will be managed on this host group. The VMs that are listed are the ones running on the hosts that you selected earlier for the host group. Select the VMs and click **Policies** to change any VM-specific policies that must be modified as shown in Figure 9-9.



☑ **capzp1p12** *(UUID: 45FDD0F7-911D-408B-A277-73EC1AABC213)* capzp1 gdlhmc10 — HA Monitoring Disabled — Policies

Policies for capzp1p12

VM Failure Detection Speed: Normal (190 seconds)

Failover Priority: Medium

VM HA Monitoring: Disabled

☑ **capzp1p11** *(UUID: 237B085E-EEB3-4536-B684-CC6CCA5DEE57)* capzp1 gdlhmc10 — HA Monitoring Disabled — Policies

Policies for capzp1p11

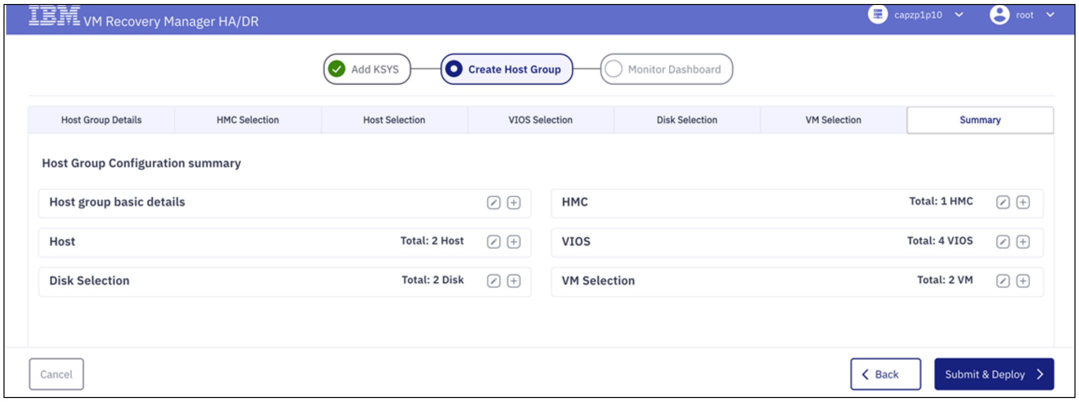
VM Failure Detection Speed: Normal (190 seconds)

Failover Priority: Medium

VM HA Monitoring: Disabled

Figure 9-9 VM selection and policy setup

11. Click the **Summary** tab. The summary shows the details of the host group that you configured, as shown in Figure 9-10 on page 249.

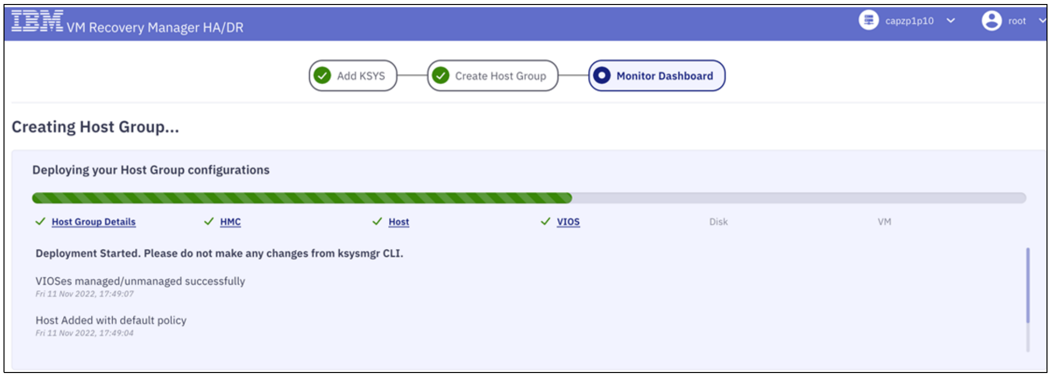


Host Group Configuration summary

Host group basic details		HMC	Total: 1 HMC
Host	Total: 2 Host	VIOS	Total: 4 VIOS
Disk Selection	Total: 2 Disk	VM Selection	Total: 2 VM

Figure 9-10 Summary configuration

When you click **Submit & Deploy**, the deployment of the host group configuration starts, as shown in Figure 9-11. This task might take some time as the KSYS cluster is built. Status messages and a status bar provide updates on the progress of the deployment.



Creating Host Group...

Deploying your Host Group configurations

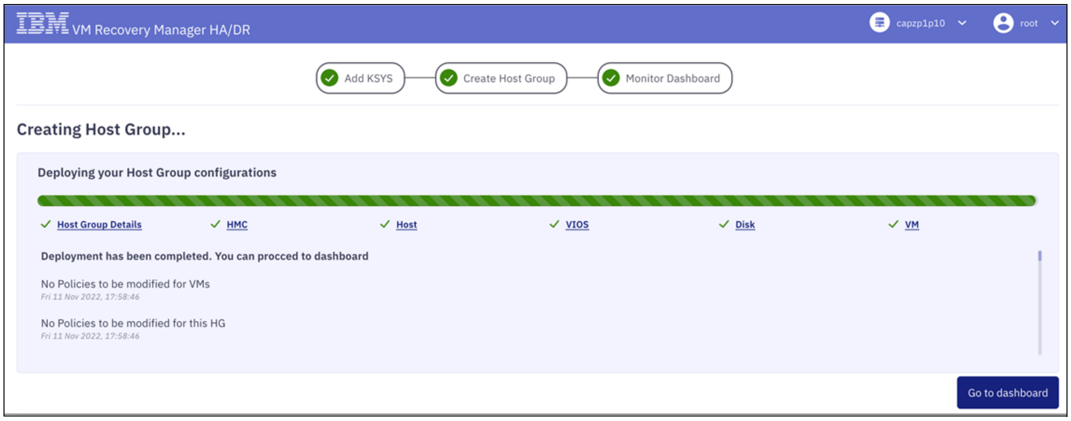
Deployment Started. Please do not make any changes from ksysmgr CLI.

VIOSes managed/unmanaged successfully
Fri 11 Nov 2022, 17:49:07

Host Added with default policy
Fri 11 Nov 2022, 17:49:04

Figure 9-11 Deployment of host group

When the deployment is finished, the final window looks like Figure 9-12, which shows that the host group was built.



Creating Host Group...

Deploying your Host Group configurations

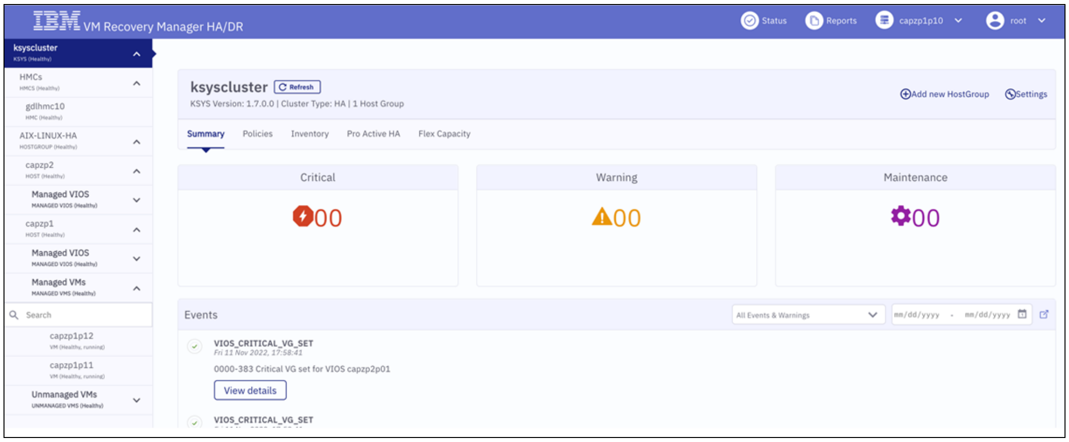
Deployment has been completed. You can procced to dashboard

No Policies to be modified for VMs
Fri 11 Nov 2022, 17:58:46

No Policies to be modified for this HG
Fri 11 Nov 2022, 17:58:46

Figure 9-12 Deployment finished

12. When the deployment finishes, click **Go to dashboard** to access the management options. The screen looks like Figure 9-13.



ksyscluster

KSYS Version: 1.7.0.0 | Cluster Type: HA | 1 Host Group

VIOS_CRITICAL_VG_SET
Fri 11 Nov 2022, 17:58:41
0000-383 Critical VG set for VIOS capzp2p01

VIOS_CRITICAL_VG_SET

Figure 9-13 VMRM GUI Dashboard

9.5 VMRM dashboard

When you register a KSYS and build a host group, the dashboard is available for use in further configuration activities and to show you the status of your environment. This section shows the different features in the dashboard and operations that can be done with the GUI.

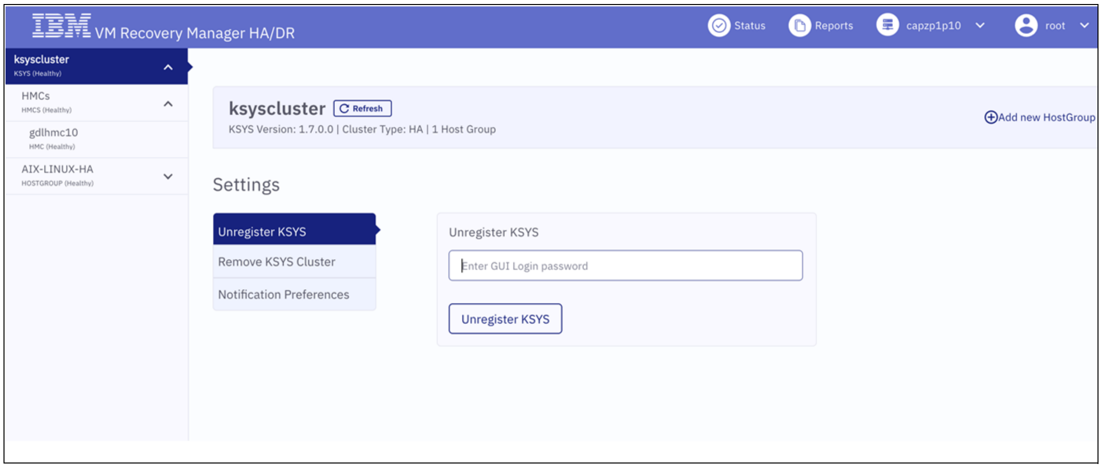
Even though this section focuses on VMRM HA configuration, the concepts are the same for the other KSYS types, and the GUI can manage the other configurations too.

9.5.1 Cluster management with VMRM GUI

The VMRM GUI can manage KSYS systems in many ways:

- Register or unregister a KSYS.
- Remove a KSYS cluster.
- Add a host group.
- Modify notification preferences.

Select the `ksyscluster`, as shown in Figure 9-14 on page 251.



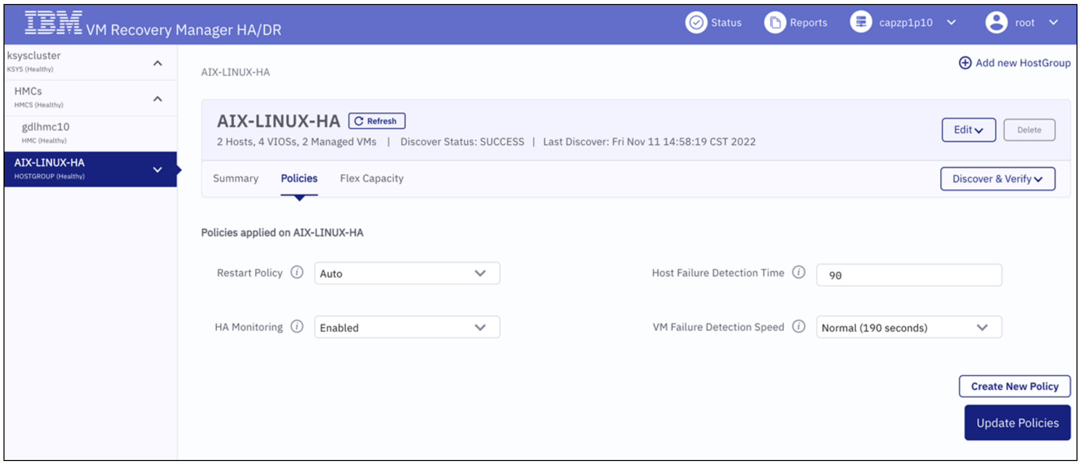
ksyscluster

KSYS Version: 1.7.0.0 | Cluster Type: HA | 1 Host Group

Unregister KSYS

Figure 9-14 Ksysculster register, unregister, and notifications

To set and update specific cluster policies, click the host group name, as shown in Figure 9-15. You can set policies and the flex capacity for the cluster.



AIX-LINUX-HA

2 Hosts, 4 VIOSs, 2 Managed VMs | Discover Status: SUCCESS | Last Discover: Fri Nov 11 14:58:19 CST 2022

Policies applied on AIX-LINUX-HA

Restart Policy: Auto

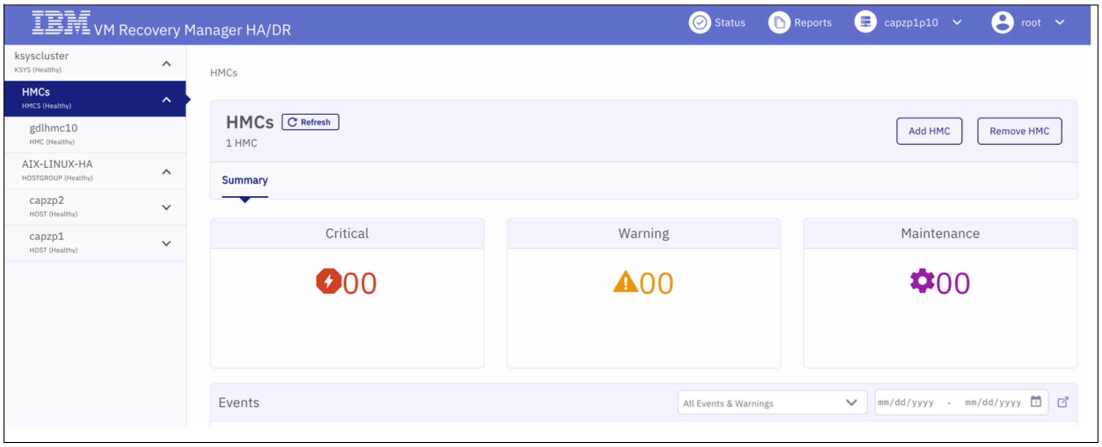
Host Failure Detection Time: 90

HA Monitoring: Enabled

VM Failure Detection Speed: Normal (190 seconds)

Figure 9-15 Host group policies management

To manage HMCs, select the **HCM** tab. You can add or remove an HMC by clicking **Add HCM** or **Remove HMC**, as shown in Figure 9-16.



HMCs

1 HMC

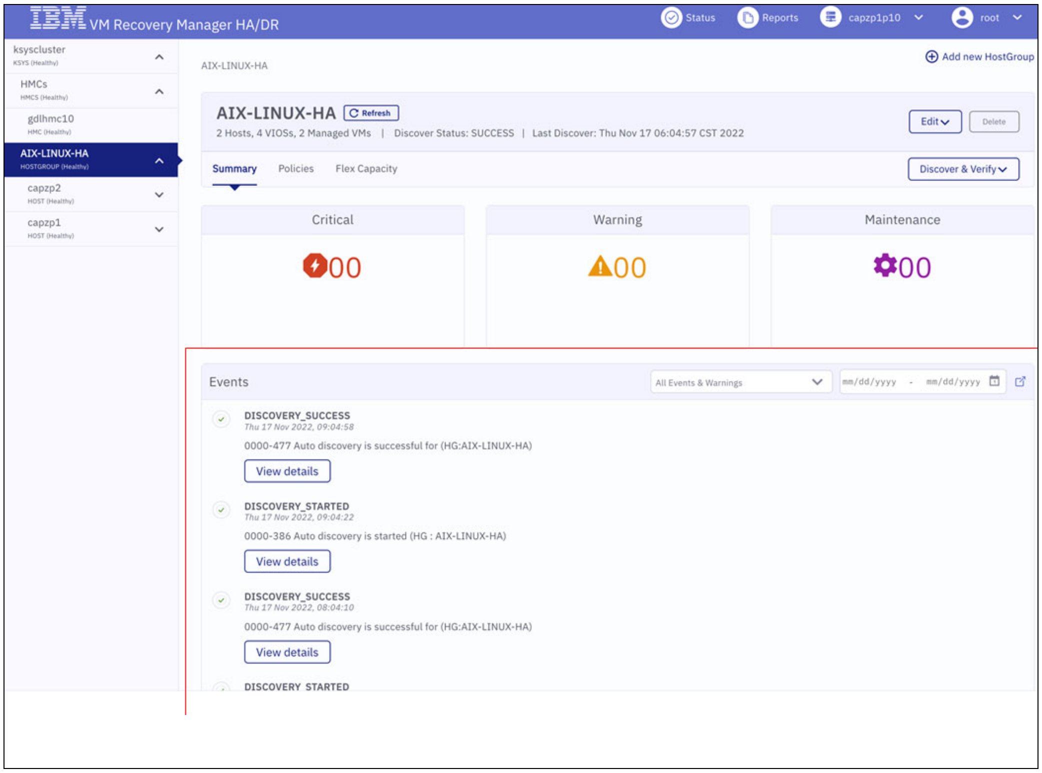
Critical	Warning	Maintenance
00	00	00

Figure 9-16 Adding or removing an HMC to KSYS

By selecting the host group, you can manage the host group in the following ways:

- View summary.
- View last events that occurred in the KSYS cluster.
- Change or add policies to the host group.
- Manage capacity resources.
- Add or remove host groups.

Figure 9-17 shows these options.



2 Hosts, 4 VIOSs, 2 Managed VMs | Discover Status: SUCCESS | Last Discover: Thu Nov 17 06:04:57 CST 2022

DISCOVERY_SUCCESS
Thu 17 Nov 2022, 09:04:58
0000-477 Auto discovery is successful for (HG:AIX-LINUX-HA)

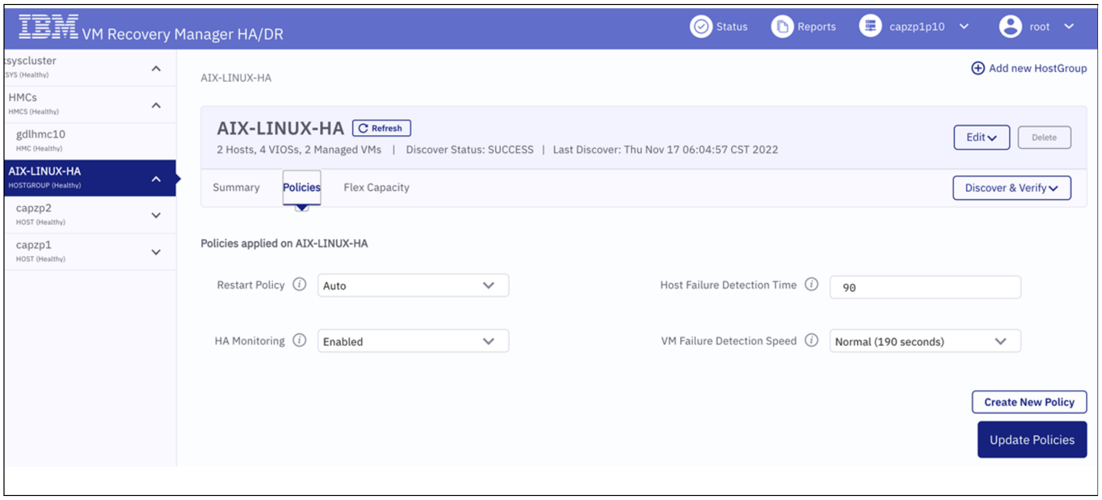
DISCOVERY_STARTED
Thu 17 Nov 2022, 09:04:22
0000-386 Auto discovery is started (HG : AIX-LINUX-HA)

DISCOVERY_SUCCESS
Thu 17 Nov 2022, 08:04:10
0000-477 Auto discovery is successful for (HG:AIX-LINUX-HA)

DISCOVERY_STARTED

Figure 9-17 Summary host group events

To check, edit, or add the host group policies, click the name of host group, as shown in Figure 9-18 on page 253.



AIX-LINUX-HA

2 Hosts, 4 VIOSs, 2 Managed VMs | Discover Status: SUCCESS | Last Discover: Thu Nov 17 06:04:57 CST 2022

Policies applied on AIX-LINUX-HA

Restart Policy: Auto

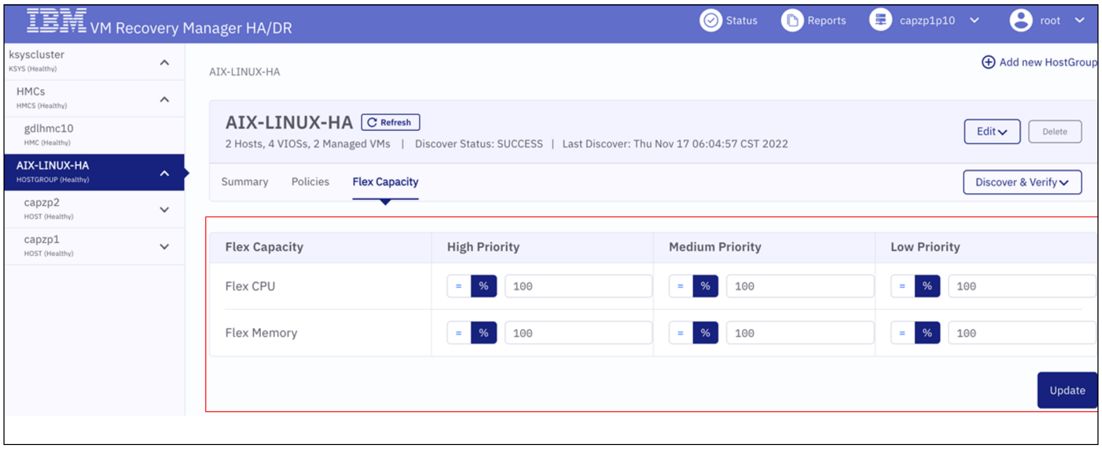
Host Failure Detection Time: 90

HA Monitoring: Enabled

VM Failure Detection Speed: Normal (190 seconds)

Figure 9-18 Host groups policy management

To check and manage flex capacity for CPU and memory for the different VM priorities, see Figure 9-19.



AIX-LINUX-HA

2 Hosts, 4 VIOSs, 2 Managed VMs | Discover Status: SUCCESS | Last Discover: Thu Nov 17 06:04:57 CST 2022

Flex Capacity	High Priority	Medium Priority	Low Priority
Flex CPU	= % 100	= % 100	= % 100
Flex Memory	= % 100	= % 100	= % 100

Figure 9-19 Host group capacity

To add or remove a host from the host group, click **Edit**, as shown in Figure 9-20.

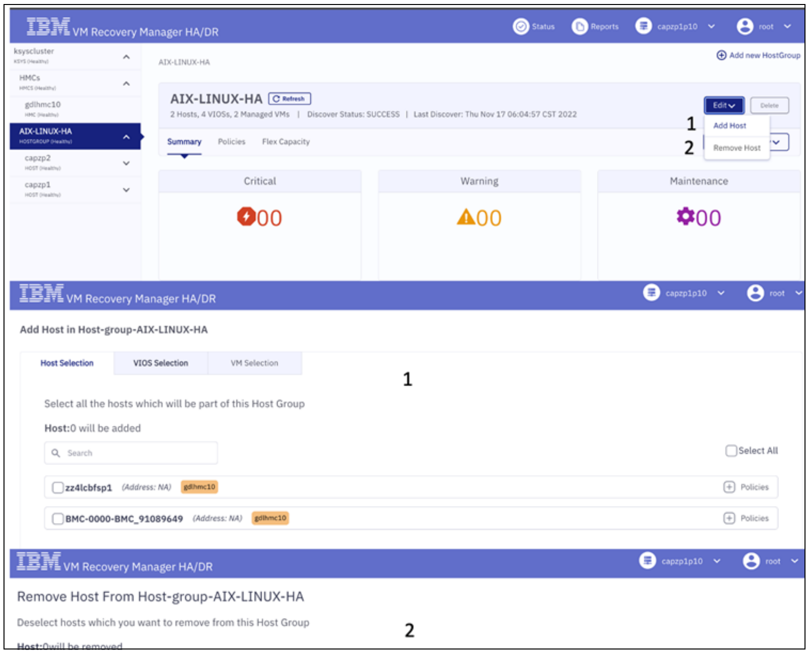

IBM VM Recovery Manager HA/DR
Status
Reports
capzp1p10
root
ksyscluster
HMCs
gdlhmc10
AIX-LINUX-HA
capzp2
capzp1
AIX-LINUX-HA
Add new HostGroup
AIX-LINUX-HA
Refresh
2 Hosts, 4 VIOSs, 2 Managed VMs | Discover Status: SUCCESS | Last Discover: Thu Nov 17 06:04:57 CST 2022
Edit
Delete
1
Add Host
2
Remove Host
Summary
Policies
Flex Capacity
Critical
00
Warning
00
Maintenance
00
IBM VM Recovery Manager HA/DR
capzp1p10
root
Add Host in Host-group-AIX-LINUX-HA
Host Selection
VIOS Selection
VM Selection
1
Select all the hosts which will be part of this Host Group
Host:0 will be added
Search
Select All
zz4lcbfsp1 (Address: NA) gdlhmc10
Policies
BMC-0000-BMC_91089649 (Address: NA) gdlhmc10
Policies
IBM VM Recovery Manager HA/DR
capzp1p10
root
Remove Host From Host-group-AIX-LINUX-HA
Deselect hosts which you want to remove from this Host Group
2
Host:0will be removed

Figure 9-20 Adding or removing a host from host groups

9.5.2 Performing cluster operations by using the VMRM GUI

The section describes the following cluster options that you can do by using the VMRM GUI:

- Discovery and verify
- Hosts and VIOSs within hosts groups

Discovery and verify

Clicking **Discovery & Verify** shows three options:

- Discover Host Group
- Verify Host Group
- Discover and Verify Host Group

These options are shown in Figure 9-21.

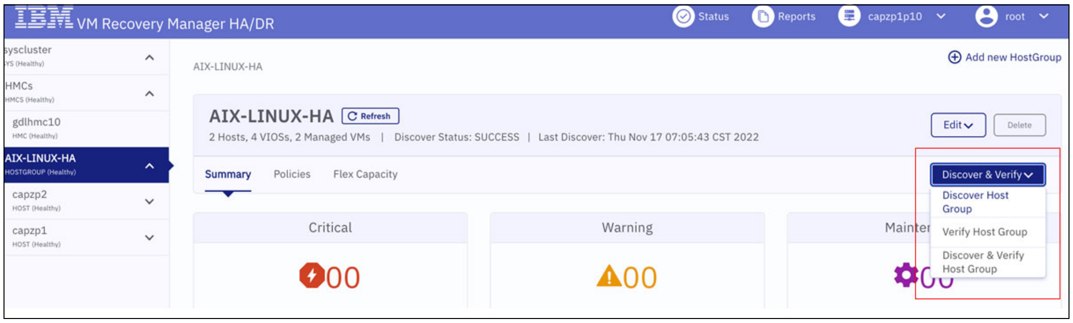
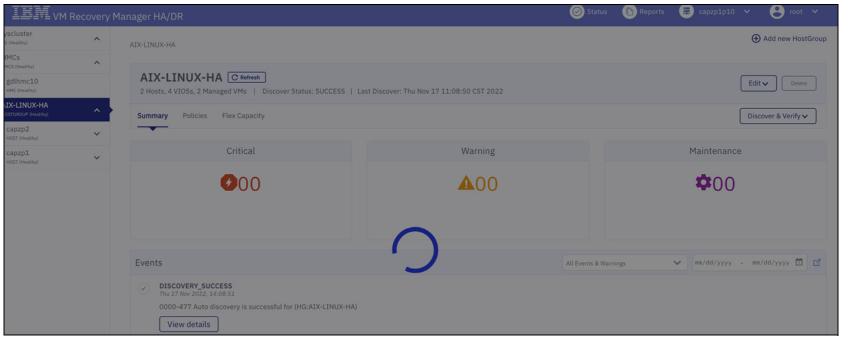


Figure 9-21 Discovery & Verify window

When you click **Discovery and Verify Host Group**, the window shows a spinning circle while the action is launched, as shown in Figure 9-22 on page 255.



AIX-LINUX-HA

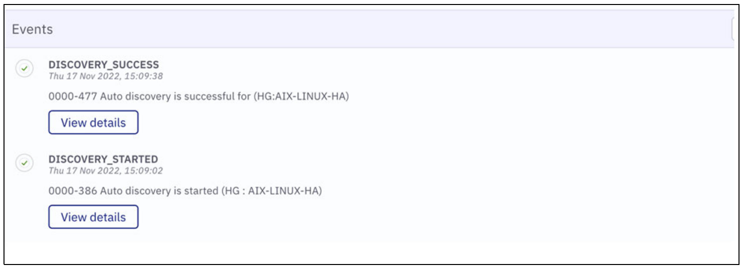
2 Hosts, 4 VIOSs, 2 Managed VMs | Discover Status: SUCCESS | Last Discover: Thu Nov 17 11:08:50 CST 2022

DISCOVERY_SUCCESS
Thu 17 Nov 2022, 14:08:51

0000-477 Auto discovery is successful for (HG:AIX-LINUX-HA)

Figure 9-22 Discovery and Verify running

Wait for the task to finish. During this process, you cannot do anything else on the GUI. When it finishes, VMRM GUI returns the control of the GUI, and the output that is related to the operation is displayed, as shown in Figure 9-23.



Events

DISCOVERY_SUCCESS
Thu 17 Nov 2022, 15:09:38

0000-477 Auto discovery is successful for (HG:AIX-LINUX-HA)

DISCOVERY_STARTED
Thu 17 Nov 2022, 15:09:02

0000-386 Auto discovery is started (HG : AIX-LINUX-HA)

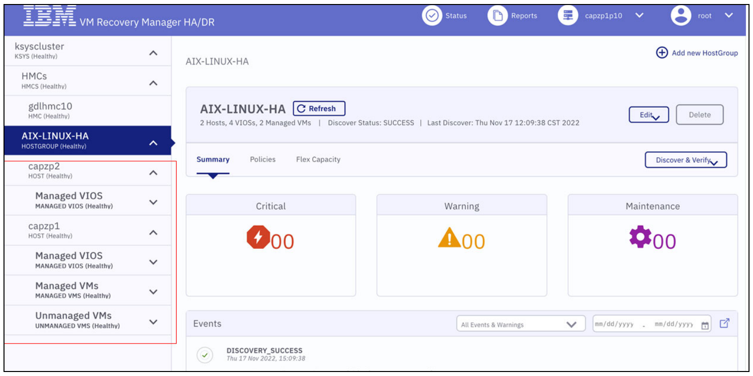
Figure 9-23 Details of the discovery operation

Hosts and VIOSs within hosts groups

Through the VMRM GUI, you can manage operations on hosts and VIOSs that are associated with host groups:

- Host group components and policies:
  - Add or remove a host from the host group.
  - Work with all VMs that are related to a host within the host group.
  - Manage and unmanaged all VIOSs that are related to a host within the host group.
- On VIOSs:
  - Check the SSP cluster.
  - Work with policies.

In the following windows, you can display all the operations, as shown in Figure 9-24.



AIX-LINUX-HA

2 Hosts, 4 VIOSs, 2 Managed VMs | Discover Status: SUCCESS | Last Discover: Thu Nov 17 12:09:38 CST 2022

DISCOVERY_SUCCESS
Thu 17 Nov 2022, 15:09:38

Figure 9-24 Host, VIOSs, and VMs options

The add or remove host option is shown in Figure 9-25.

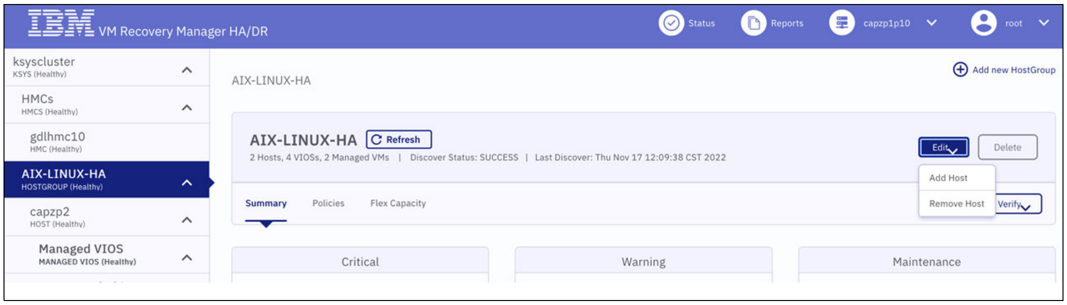


Figure 9-25 Add or remove host

Working with VMs, you can view the status; migrate; restart; and clean up the VM from the host group window that is shown in Figure 9-26.

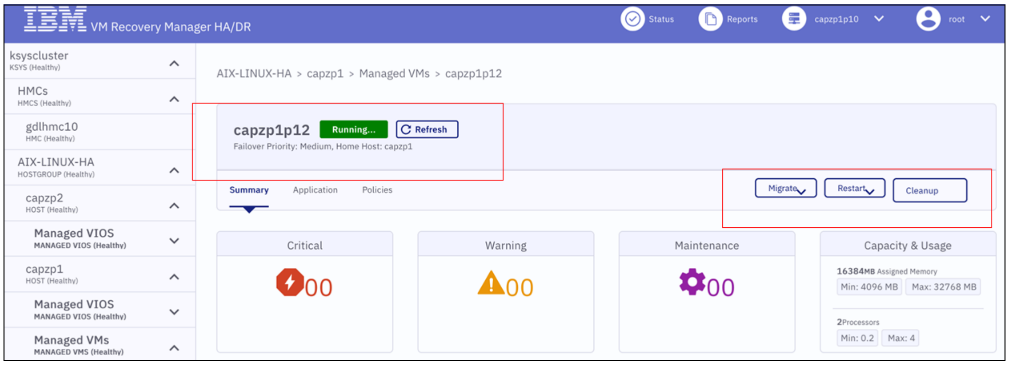
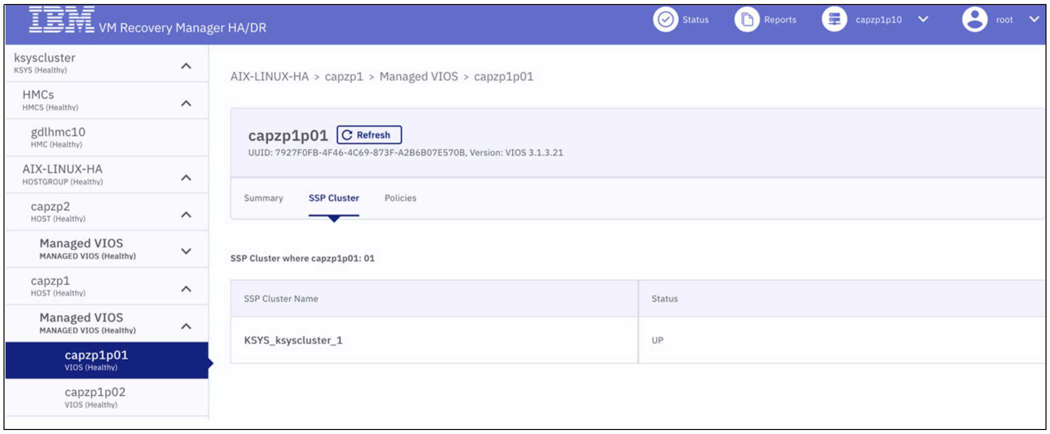


Figure 9-26 VM-related tasks

You can perform VIOS management tasks within the VMRM GUI, such as managing an SSP's cluster status or unmanaging a VIOS, as shown in Figure 9-27.



SSP Cluster Name	Status
KSYS_ksyscluster_1	UP

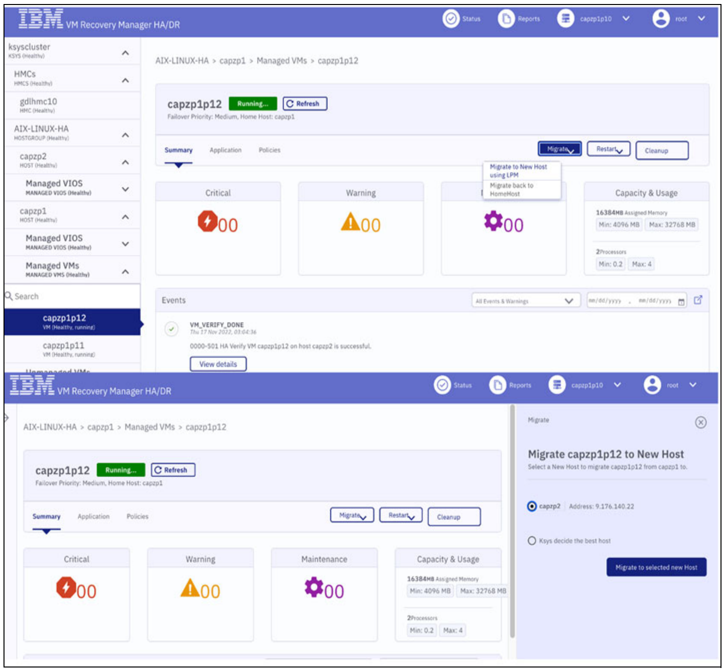
Figure 9-27 VIOS-related tasks

9.5.3 Migration tests

This section shows the VMRM HA migration tests that we ran.

VM Live Partition Mobility migration test

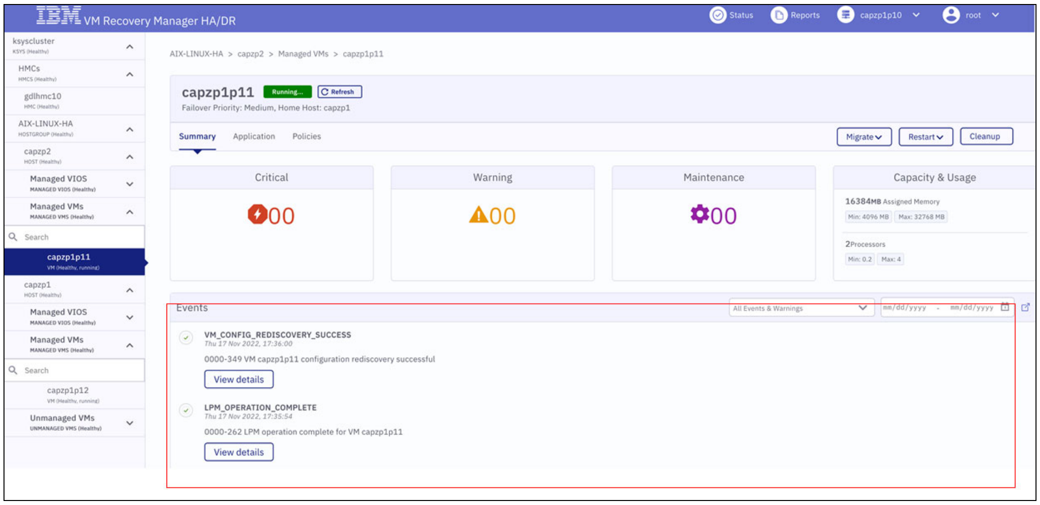
This test performs a Live Partition Mobility (LPM) move of VM capzp1p12. You can let KSYS decide which hosts within the host group migrate, or you can pick an available host from the list, as shown in Figure 9-29.



VM_VERIFY_DONE
Thu 17 Nov 2022, 03:04:36
0000-501 HA Verify VM capzp1p12 on host capzp2 is successful.

Figure 9-28 Migrating VM with Live Partition Mobility

When the LPM operation finishes, the VMRM GUI sends a notification to you about the result of the operation (success or failure) in the event window. as shown in Figure 9-29.



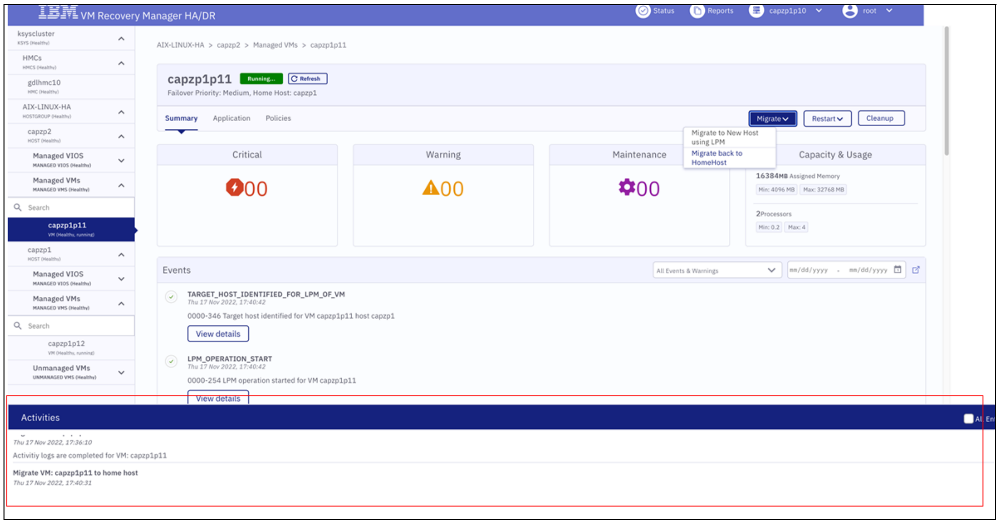
VM_CONFIG_REDISCOVERY_SUCCESS
Thu 17 Nov 2022, 17:36:00
0000-349 VM capzp1p11 configuration rediscovery successful

LPM_OPERATION_COMPLETE
Thu 17 Nov 2022, 17:35:54
0000-262 LPM operation complete for VM capzp1p11

Figure 9-29 LPM result window

Recover test

You can move the VM to the home host by clicking **Migrate back to home**, as shown in Figure 9-30.



TARGET_HOST_IDENTIFIED_FOR_LPM_OF_VM
Thu 17 Nov 2022, 17:40:42
0000-346 Target host identified for VM capzp1p11 host capzp1

LPM_OPERATION_START
Thu 17 Nov 2022, 17:40:42
0000-254 LPM operation started for VM capzp1p11

Thu 17 Nov 2022, 17:36:10
Activitiy logs are completed for VM: capzp1p11

Migrate VM: capzp1p11 to home host
Thu 17 Nov 2022, 17:40:31

Figure 9-30 Migrate back to home window

VM restart move test

This test performs a VM restart to move VM capzp1p11. This test also can restart the home host or recover a VM. In this example, we run **Restart** → **Restart & Bring to New Host**.

Select VM capzp1p11, and then select **Restart** → **Restart & Bring to New Host**, as shown in Figure 9-31.

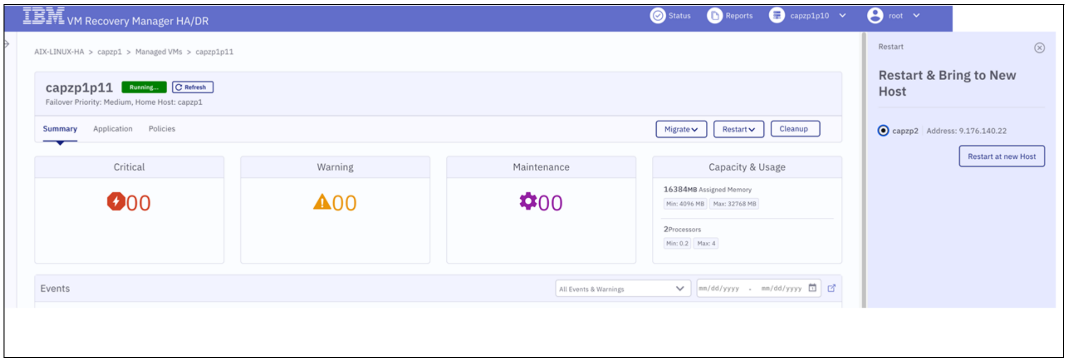
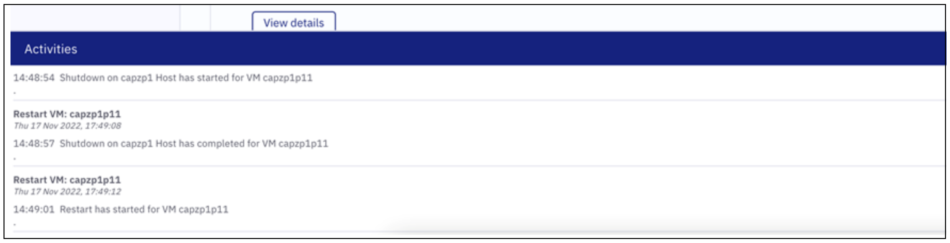


Figure 9-31 Restart move operation window

You can check the progress of the restart operation in the activities window, as shown in Figure 9-32.



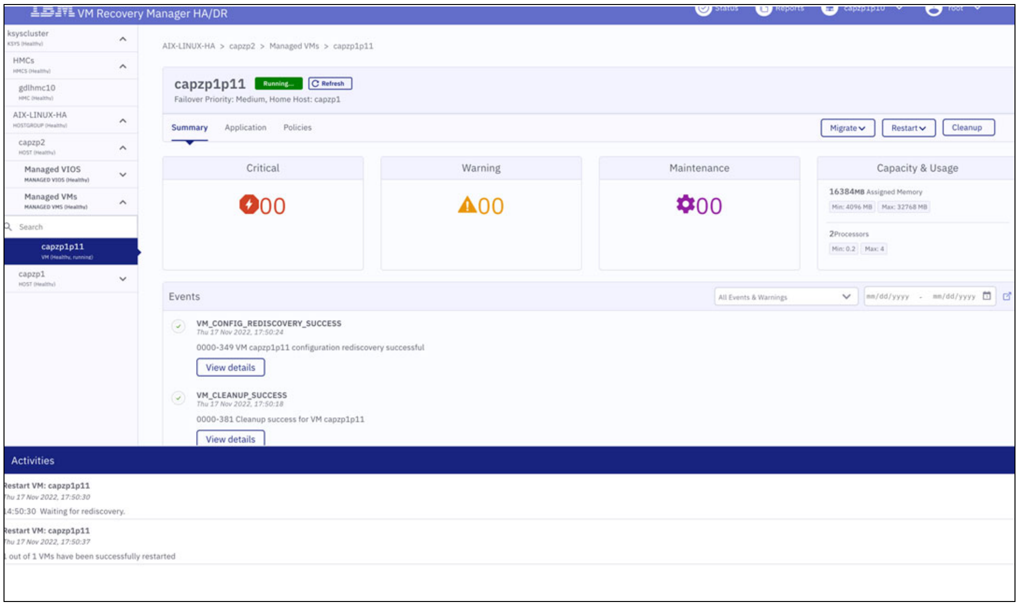
```
14:48:54 Shutdown on capzp1 Host has started for VM capzp1p11
.

Restart VM: capzp1p11
Thu 17 Nov 2022, 17:49:08
14:48:57 Shutdown on capzp1 Host has completed for VM capzp1p11
.

Restart VM: capzp1p11
Thu 17 Nov 2022, 17:49:12
14:49:01 Restart has started for VM capzp1p11
.
```

Figure 9-32 Activities window

When the operation finishes, the VM is on the other host, as shown in Figure 9-33.



Failover Priority: Medium, Home Host: capzp1

16384MB Assigned Memory
Min: 4096 MB Max: 32768 MB

2Processors
Min: 0.2 Max: 4

VM_CONFIG_REDISCOVERY_SUCCESS
Thu 17 Nov 2022, 17:50:24
0000-349 VM capzp1p11 configuration rediscovery successful

VM_CLEANUP_SUCCESS
Thu 17 Nov 2022, 17:50:18
0000-381 Cleanup success for VM capzp1p11

Restart VM: capzp1p11
Thu 17 Nov 2022, 17:50:30
14:50:30 Waiting for rediscovery.

Restart VM: capzp1p11
Thu 17 Nov 2022, 17:50:37
1 out of 1 VMs have been successfully restarted

Figure 9-33 VM restart operation finish window

9.6 GUI limitations

The VMRM GUI has the following limitations:

- The VMRM GUI does not support multiple sessions that originate from the same computer.
- The VMRM GUI does not support duplicate names for the host group, HMC, host, VIOS, VMs, site, workgroup, and storage agent. If a duplicate name exists in the KSYS configuration, the GUI might encounter an error during the host group creation or while displaying the dashboard data.
- The VMRM GUI refreshes automatically after each topology change (for example, VM migration operation and host migration operation). After the refresh operation of VMRM GUI completes, the default KSYS dashboard opens. Expand the topology view in the Activity window to view the log information for a specific entity.
- Any operation that is performed by a user from the command-line interface (CLI) of VMRM DR is not displayed in the activity window of the VMRM GUI.
- GUI reports show details only about operations that are triggered from the GUI. The operations that are triggered from the CLI are not displayed in the GUI reports.

10

Advanced topics

The following topics are described in this chapter:

- IBM Virtual Machine Recovery Manager DR coexistence with other products
- SAN storage general considerations for the VMRM DR environment
- SAN fabric setup for the IBM VMRM DR environment
- Storage components in the IBM VMRM DR solution

10.1 IBM Virtual Machine Recovery Manager DR coexistence with other products

This section describes how the following three IBM software products work together with IBM Virtual Machine Recovery Manager (VMRM) DR:

- IBM Power Virtualization Center (PowerVC)
- IBM PowerHA SystemMirror
- IBM PowerVM NovaLink

10.1.1 IBM PowerVC

IBM PowerVC is a virtualization management offering that is used to create and manage virtual machines (VMs) on IBM Power servers by using a PowerVM or PowerKVM hypervisor. The PowerVC offering can coexist with the VMRM DR solution. The PowerVC functions can be divided into logical partition (LPAR) movement and provisioning and storage area network (SAN) changes.

Moving an LPAR (VM) from one host to another host

The functions help move LPARs (VMs):

- Live Partition Mobility (LPM)
- Remote restart
- Capacity management

If a VM is moved to another host that is in the same host group as before the move, run a **`ksys discovery`** operation after the move. If you do not run a **`ksys discovery`** operation, the daily discovery operation picks up the changes.

If a VM is moved to a host that is not in the same host group, more attention might be needed:

- If the VM is in workgroup, then after the move it cannot be in that workgroup anymore.
- For some storage systems, the disk replication might need to be redefined, for example, the Hitachi storage systems. For more information, see “Limitations for Hitachi disks” on page 289.

Therefore, avoid moving a VM to a host that is not in the host group.

Storage area network changes

The storage management functions, which include storage area network functions, can be divided into the following tasks:

- New VM provisioning
- Adding storage resources to existing VMs
- Reducing or removing storage resources from existing VMs
- AIX Live Kernel Updates

For these activities, new SAN zoning and logical unit number (LUN) masking might be needed on both the production and disaster recovery (DR) sites and LUN replication might need to be changed. During an AIX Live Update process, temporary storage is added to the LPAR, and later the temporary storage is removed from this LPAR. Do not perform a Live Update operation when you are running a DR operation that uses VMRM DR.

10.1.2 PowerHA SystemMirror software

The PowerHA SystemMirror software provides cluster-based high availability (Standard Edition) and DR (Enterprise Edition) (HADR) solutions. The VMRM DR solution can operate with PowerHA SystemMirror 7.1 or later when you follow the guidelines that are required to deploy both solutions together.

Disaster recovery by using PowerHA SystemMirror Enterprise Edition

When using PowerHA SystemMirror Enterprise Edition to perform DR for some of the VMs in your environment, do not deploy the VMRM DR solution for those VMs. In this case, exclude those VMs from VMRM DR management. To exclude the PowerHA VMs from the VMRM DR configuration before you discover resources in the VMRM DR solution, run the **ksysmgr unmanage** command.

High availability by using PowerHA SystemMirror Standard Edition

PowerHA SystemMirror Standard Edition is deployed within a site. PowerHA creates a cluster of a set of VMs within the active site for high availability (HA) management. If you are configuring such a cluster within the active site of the VMRM DR environment and want to move the whole cluster to the DR site during a DR event, consider the following guidelines:

- Include all the VMs in the cluster to the VMRM DR management.
- Perform a test failover of the cluster to the backup site to validate whether that cluster starts correctly on the backup site.

To use VMRM DR with PowerHA SystemMirror, PowerHA SystemMirror and Cluster Aware AIX (CAA) must support the **CAA_AUTO_START_DR** tunable parameter. This tunable parameter has been supported since PowerHA 7.2.4. If this tunable parameter is enabled, CAA identifies repository disks based on PVID instead of UDID or Universally Unique Identifier (UUID). Therefore, the CAA cluster starts with a replicated repository disk on the DR site.

To check whether your installed `bos.cluster.rte` file set in your AIX level supports the **CAA_AUTO_START_DR** tunable parameter, run the following command:

```
# clctrl -tune -a |grep dr_enabled
mytestcluster(2a1010f2-e6b6-11ec-8005-4237c7f48e02).dr_enabled = 1
```

Important: Do *not* change this parameter with the **clctrl** command manually. PowerHA SystemMirror makes the changes for you.

To check whether your installed PowerHA SystemMirror supports the **CAA_AUTO_START_DR** tunable parameter, run the following command:

```
# clmgr q cluster |grep DR
CAA_AUTO_START_DR="Enabled"
```

The default value of this tunable parameter is “Enabled”, which is the recommended setting. If the value is “Disabled”, you can enable it by running the following commands:

```
# clmgr modify cluster CAA_AUTO_START_DR=enable
# clmgr sync cluster
```

After synchronizing the cluster, this tunable parameter is enabled in both PowerHA and CAA. You can check the settings in both PowerHA and CAA by running the following command:

```
# clmgr q cluster |grep DR
CAA_AUTO_START_DR="Enabled"
# clctrl -tune -a |grep dr_enabled
mytestcluster(2a1010f2-e6b6-11ec-8005-4237c7f48e02).dr_enabled = 1
```

When deployed with PowerHA SystemMirror 7.1.0 (or later), the cluster may be started directly in the DR site after a DR or DR rehearsal move if **CAA_AUTO_START_DR** is enabled in both the PowerHA SystemMirror and CAA clusters.

Some extra steps might be required to start the cluster on the DR site after a DR or DR rehearsal move that uses the VMRM DR solution, for example, if **CAA_AUTO_START_DR** is disabled or **CAA_AUTO_START_DR** is not supported.

Here are the steps to recover a PowerHA SystemMirror cluster in this case. Assume that the OSs of all the cluster nodes are started and running on the DR site. The following steps are needed only on one of the PowerHA SystemMirror cluster nodes on the DR site.

1. Find the primary repository disk on the DR site by running the following command:

   ```
   # clmgr q repos
   hdisk4 (00f9079b44840599)
   hdisk5 (00f9079b4432e097)
   ```

   The first disk in the list (hdisk4 in the example output) is the primary repository disk, and the other (hdisk5 in the example output) disks are backup repository disks for the cluster. hdisk4 is a replica of the primary repository disk (in a DR move) or a clone of the replica of the primary repository disk (in a DR rehearsal move), and hdisk5 is a replica of the backup repository disk (in a DR move) or a clone of the replica of the backup repository disk (in a DR rehearsal move). Backup repository disks are empty except for their PVID.

2. Remove any CAA information from the DR site primary repository disk by running the following command:

   ```
   # CAA_FORCE_ENABLED=true rmcluster -fr hdisk4
   WARNING: Force continue.
   rmcluster: Successfully removed hdisk4.
   ```

3. To write the repository disk information by using the information, run the following command:

   ```
   CAA_FORCE_ENABLED=true chrepos -fc hdisk4
   ```

4. To start the cluster in the backup site, run the following command:

   ```
   clusterconf
   ```

5. Start the PowerHA SystemMirror cluster by running the following command:

   ```
   clmgr on cluster
   ```

Note: PowerHA SystemMirror depends on hostname, network, and IP addresses. Therefore, if the IP addresses are changed during DR or DR rehearsal moves, the procedure might not work. The `ghostdev` setting is important too. The default value of it is `ghostdev=0`. It is the setting that is required for this procedure.

10.1.3 PowerVM NovaLink

At the time of writing, the VMRM solution works with PowerVM servers that are managed by an HMC. You can use NovaLink with VMRM if there are HMCs deployed. In this configuration, VMRM requires that the HMCs are set to be in the master mode. For initial discovery, the customer must ensure that this setup is the case, but for day-to-day operation, VMRM includes some sample scripts that can be registered as pre- and post-scripts, which change the HMC to master mode before a VMRM operation occurs and back to non-master mode after the operation.

These scripts are in `/opt/IBM/ksys/samples/hmc_novalink`. For more information, see Enabling HA/DR for VM in an IBM PowerVM HMC and NovaLink coexistence environment: Using IBM VM Recovery Manager HA/DR Custom_validation and hmc-novalinke scripts.

10.2 SAN storage general considerations for the VMRM DR environment

DR involves setting up a methodology and enabling procedures to follow in a disaster so that you can recover your entire environment (or at least the most critical parts of your environment) so that your company can continue operating with minimal or no impact to the business.

To be effective, a DR solution must automate many of these procedures. which speeds the recovery of your servers and applications and minimizes the chance of mistakes through human error. VMRM DR can automate the recovery of your Power server in a failure.

To achieve this objective, the data that is used by your LPARs or VMs must be replicated to storage that is available in the backup site. The SAN connectivity, SAN zoning, and LUN masking must be prepared in the backup site, where the applications continue to run in a failure at the primary site.

The VMRM DR solution relies on the storage subsystem to replicate the data from the active site to the backup site.

During the KSYS discovery phase, the storage subsystem follows this process:

1. The KSYS interacts with the HMC to get the list of VMs and the corresponding Virtual I/O Server (VIOS) information. Then, the KSYS interacts with the VIOS to fetch the storage disk information that is used by these VMs.
2. The KSYS verifies the disk pair to check whether the disk is set up for replication. The replication must be defined and data replication must be in place for all the related data disks.

> **Note:** For the Dell EMC Unity storage system, the replication relationships are created during the KSYS discovery process.

3. The KSYS checks whether the disks on the storage subsystem are part of any existing composite or consistency groups (CGs). If the disk is part of any existing composite group, the discovery operation fails.
4. The KSYS creates a composite group for each site that contains the corresponding disks and enables data consistency. The KSYS uses this composite group to change the replication direction of the corresponding disks during a planned recovery operation.

The verify process validates the SAN connectivity, SAN zoning, and LUN masking to make sure that the VMs can be recovered in the backup site.

During a disaster or planned move process, the following process occurs:

1. The KSYS shuts down any VMs on the production site that are not down.
2. The KSYS fails over the storage replication to the DR site, making the DR disks writable and reversing the storage replication direction if possible, for example, in a planned failover.
3. The KSYS creates the LPARs on the DR site and stars them with the replicated storage.

These processes require that the SAN connectivity, SAN zoning, LUN masking, and storage systems are set up properly to enable the VMs to access the replicated disks.

At the time of writing, the following storage systems are supported:

- IBM SAN Volume Controller, IBM FlashSystem, and IBM Storwize Storage System

  Metro Mirror (synchronous), Global Mirror (asynchronous), and Global Mirror with Change Volumes (asynchronous) are supported. HyperSwap is supported for a shared storage environment.

- Dell EMC – Symmetrix Remote Data Facility (SRDF)

  Synchronous (SRDF/S) and Asynchronous (SRDF/A) replication are supported.

- IBM DS8000 series

  Global Mirror (asynchronous) is supported.

- IBM XIV and IBM FlashSystem A9000 Storage Systems

  Both synchronous and asynchronous mirroring are supported.

- Hitachi Virtual Storage Platform (VSP) G200, G400, G600, G800, and G1000 storage systems

  Both synchronous and asynchronous data replication are supported by using Hitachi TrueCopy remote replication and Hitachi Universal Replicator (HUR) technologies.

- Dell EMC Unity Storage System

  Both asynchronous and synchronous replication are supported.

10.3 SAN fabric setup for the IBM VMRM DR environment

The VMs on the home site (active site) must be fully virtualized. Figure 10-1 on page 267 shows the VMRM SAN connectivity and zoning requirements.

SAN connectivity and zoning must be configured so that VIOSs can access the disks that are relevant to the hosts across the host pairs. For example, a disk D1 that is connected to the VIOS of a host must have a mirror disk D1_M that is connected to the VIOS of the paired host in the backup site. Any connectivity issues can cause the VMRM DR verification to fail.

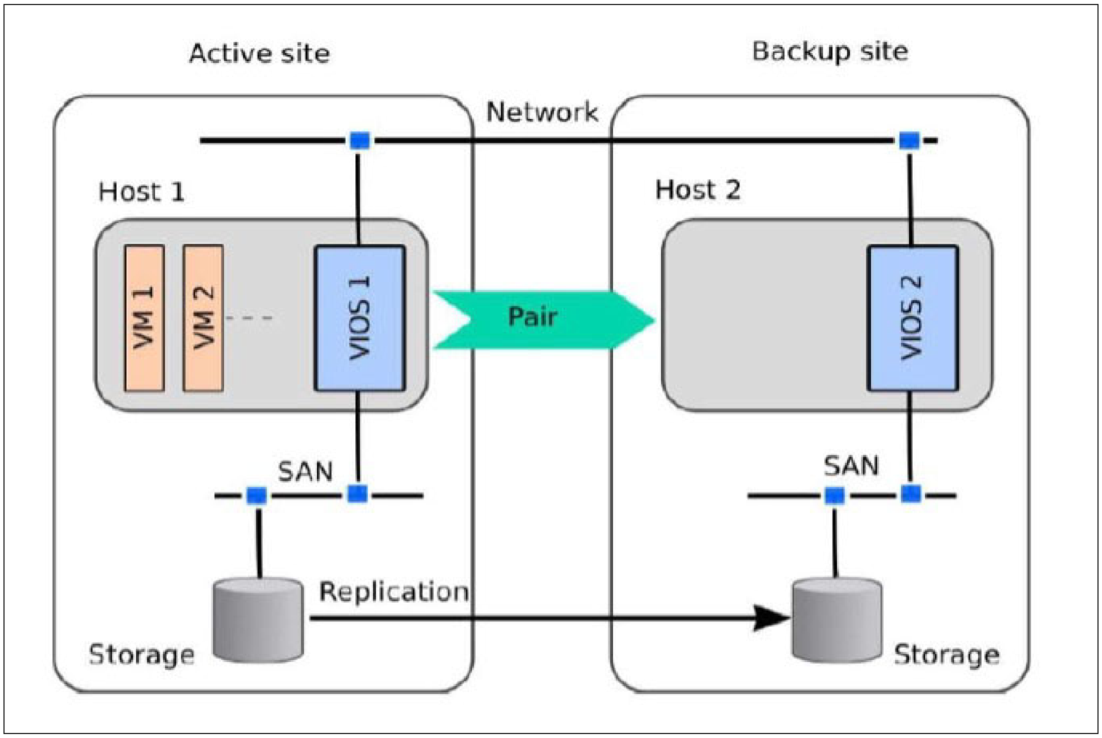


Figure 10-1 VMRM SAN connectivity and zoning requirements

Mapping NPIV for VMRM DR

To support N_Port ID Virtualization (NPIV) for VMRM DR, SAN connectivity must be performed do that the SAN fabrics of the VIOSs on the paired hosts do not connect to each other, as shown in Figure 10-2.

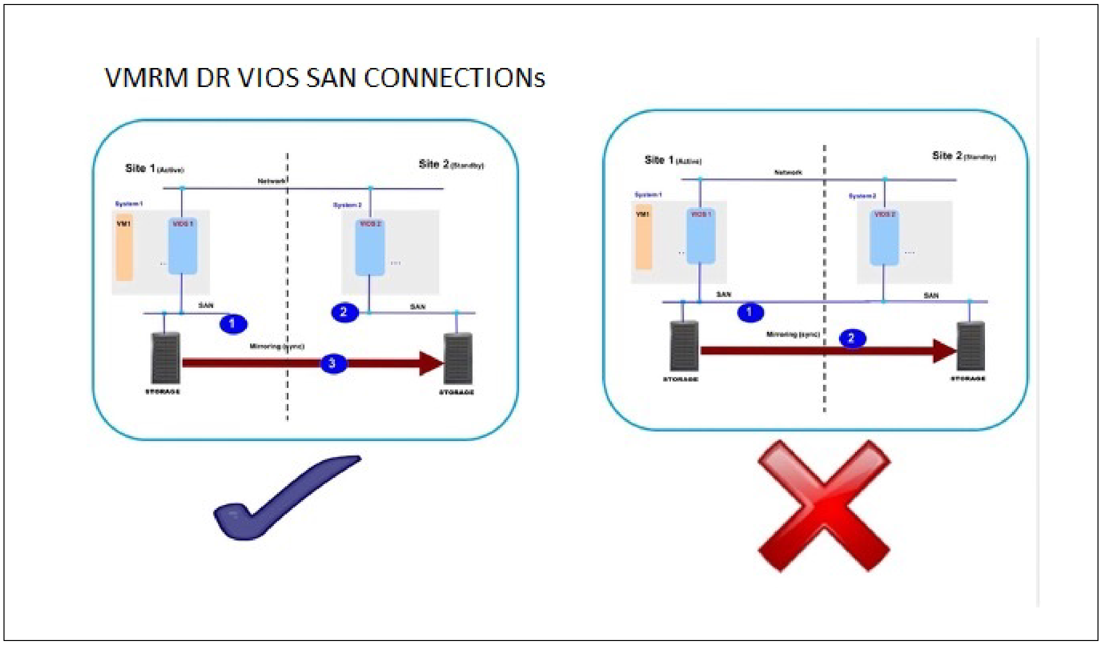


Figure 10-2 SAN fabric isolation requirement

To map the NPIV for VMRM DR, complete the following steps:

1. Create a SAN zone in a switch that consists of the NPIV worldwide port number (WWPN) of the VM and the WWPN of the source SAN subsystem.
2. In the source SAN subsystem, mask both the LUNs and the WWPN of the NPIV client.
3. Create a SAN zone in a switch that consists of both the NPIV WWPN and the WWPN of the target SAN.
4. In the target SAN subsystem, mask both the mirrored LUNs and the WWPN of the NPIV client.
5. The SAN connectivity and SAN zoning on the target site must be set so that each disk in a VM that is moved to the target (DR) site can access the replicated disks on the DR site with the same number of paths and through the same number of SAN fabrics as in the source site.

Note: This requirement is relaxed in VM Recovery Manager DR 1.6 and later when using VIOS 3.1.3 and later.

Mapping virtual Small Computer System Interface for VMRM DR

To map the virtual Small Computer System Interface (vSCSI) for VMRM DR, complete the following steps:

1. Create a SAN zone in a switch that consists of both the source VIOS WWPN and the WWPN of the storage subsystem.
2. In the source storage subsystem, ensure that the LUN is masked with the WWPN of the source VIOS.
3. Create a SAN zone in a switch that consists of both the target VIOS WWPN and the WWPN of the target storage subsystem.
4. In the target storage subsystem, ensure that the mirrored LUN is masked with the WWPN of the target VIOS.

10.4 Storage components in the IBM VMRM DR solution

The following sections describe how to configure the various support storage subsystems that are supported by VMRM DR.

10.4.1 Setting up the Dell EMC Symmetrix / VMAX storage

This section describes the following topics:

- Concept
- Installing and configuring the SYMAPI client on the KSYS node
- Adding the storage systems to VMRM
- Configuration for DR rehearsal
- Adding and removing disks from VMs

Concept

The VMRM DR solution implements DR with SRDF storage systems by using the Dell EMC supplied Symmetrix Command-Line Interface (SYMCLI). The VMRM DR solution uses the Symmetrix Application Program Interface (SYMAPI) server that runs on the Dell EMC Solution Enabler server node for the SYMCLI operations. The Solution Enabler software from Dell EMC must be installed and configured on the KSYS server to access the Dell EMC storage systems.

Solution Enabler has two ways to access and manage the Dell EMC Symmetrix and VMAX storage systems:

- In-band, through Small Computer System Interface (SCSI) commands, usually over Fibre Channel (FC) connections on storage devices (LUNs) that are called *gatekeepers*. This Solution Enabler environment is called a Solution Enabler server or SYMAPI server.
- The second option is out-band through Internet Protocol network connections to a SYMAPI server that is used to access and manage the Dell EMC Symmetrix and VMAX storage systems. Because the KSYS server might not be on the same site as the storage systems it manages, it might not be able to access gatekeepers from the storage systems to the KSYS server. Therefore, it is common that the out-band configuration is used in the VM Recovery Manager DR environment. The out-band configuration is also called a Solution Enable client, and it is shown in Figure 10-3.

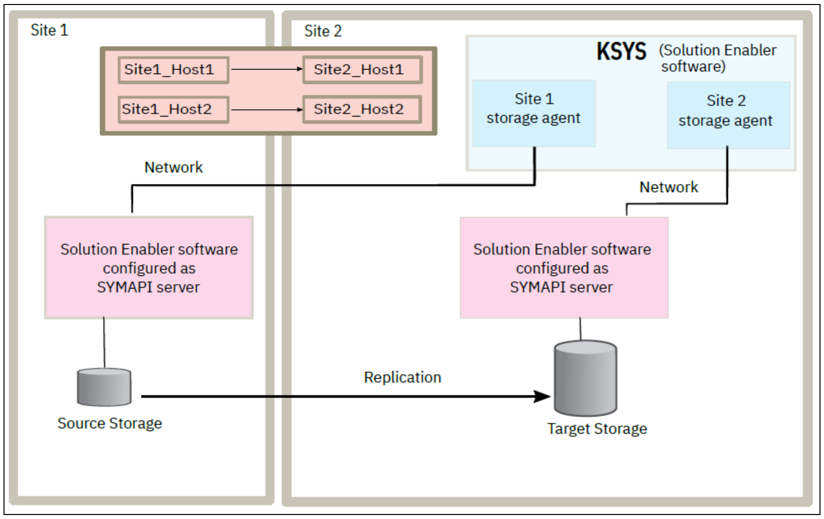


Figure 10-3 Relationship between KSYS and Dell EMC Symmetrix and VMAX storage systems

To enable DR of Dell EMC storage systems, complete the following steps before you implement the VMRM DR solution:

1. Plan the storage deployment and mirroring functions that are necessary for your environment. This step is related to the applications and middleware that are deployed in the environment.
2. Use the Dell EMC tools to configure and deploy the storage systems.
3. Use the SYMCLI interface to discover the storage devices that are deployed.

All Dell EMC SRDF operations in the VMRM DR solution are performed on a *composite group*, which is a group of disks that belong to multiple storage arrays. The CG that is enabled in the Dell EMC storage devices for consistency is known as the composite group. The composite groups operate simultaneously to preserve the integrity and consistency of the dependent write operation of data that is distributed across multiple arrays. Consistency for an SRDF replicated resource is maintained at the composite group level on the Dell EMC storage device.

The VMRM DR solution supports SRDF replicated resources in the following modes:

- SRDF/S (synchronous) replication

  In the synchronous mode, when the host issues a write operation to the source of the composite group, the Dell EMC storage device responds to the host after the target Dell EMC storage device acknowledges that it received and checked the data.

- SRDF/A (asynchronous) replication

  In the asynchronous mode, the Dell EMC storage device provides dependent, write-consistent, and point-in-time data to the auxiliary storage devices that slightly lags in time from the primary storage devices. Asynchronous mode is managed in sessions. In the asynchronous mode, the data is transferred in predefined cycles (delta sets). You can change this default cycle time to change the time difference of dependent write operations on the auxiliary storage devices that suit your business requirement.

We do not describe the details of configuring SYMAPI servers in this book. However, confirm with your storage administrator that the entries `SYMAPI_ALLOW_RDF_SYMFORCE = TRUE` and `SYMAPI_USE_RDFD = ENABLE` are set in the `/var/symapi/config/options` file on the SYMAPI servers on the home and backup (DR) sites.

Dell EMC SRDF storage agent configuration for IBM VMRM describes how to configure both SYMAPI servers and clients.

The next section describes how to configure Solution Enabler on the KSYS server as a Solution Enabler client.

Installing and configuring the SYMAPI client on the KSYS node

Your storage administrator should have the Solution Enabler software installation media, and they can assist you with the installation. For more information about software download and installation instructions, see Dell EMC Solutions Enabler Installation and Configuration Guide.

> **Note:** It is important to enter yes (Y), which is the default answer for the following question during the Solutions Enabler installation on the KSYS node:
>
> ```
> Install Dell EMC Solutions Enabler Certificates for secure client/server
> operation? [Y]:
> ```
>
> If the Dell EMC Solutions Enabler Certificates for secure client and server operation are not installed on the KSYS node, the communication between the KSYS node and the Dell EMC Storage through the SYMAPI server fails, unless a `NONSECURE` configuration is performed, which is not recommended.

After the Dell EMC Solutions Enabler is installed on the KSYS node, the configuration file `/var/symapi/config/netcnfg` must be modified to include the SYMAPI servers IP addresses (and other pertinent configuration details) that the SYMCLI uses to communicate with the Dell EMC storage systems.

The netcnfg file creates the definition of a service name, which is basically a mapping to the IP address, hostname, and port number of the SYMAPI servers that are listening to the SYMAPI functions that are performed through the SYMCLI commands. You can create one service name per storage device. This service name is used to tell the SYMCLI which SYMAPI server is used to perform a command, which determines which storage device receives the commands from which site.

Table 10-1 shows the parameters that must be used in the /var/symapi/config/netcnfg file to create the service names.

Table 10-1 Parameters in /var/symapi/config/netcnfg for the service name definition

Parameter	Explanation
Service name	The user can choose the value that is used as the service name. This value determines which storage that you want to run commands against. You can use a maximum of 31 characters.
Paring method	A “-” should be used to indicate that there is no pairing.
Protocol	The TCP/IP protocol must be used. This protocol is used for communication with the SYMAPI server.
SYMAPI server hostname	The hostname of the SYMAPI server (maximum of 511 characters).
SYMAPI server IP address	The IP address of the SYMAPI server.
SYMAPI server port	The port that is used for communication with the SYMAPI server. The default port is 2707, but this port can be modified by the user. Confirm with the Dell EMC Storage admin which port is being used in the SYMAPI server.
Security level	You can choose between SECURE, NONSECURE, or ANY (which tries SECURE first and then NONSECURE, if it is available).

One service name per line must be defined in the /var/symapi/config/netcnfg file. The syntax that must be used is shown in Example 10-1.

Example 10-1 Syntax of the /var/symapi/config/netcnfg file

```
+-( Service Name )
|              +-( Pairing Method )
|              |  +-( Protocol )
|              |  |      +-( Server's Nodname )
|              |  |      |        +-( Server's Address )
|              |  |      |        |                +-(Listening Port )
|              |  |      |        |                |     +-( Security Level)
|              |  |      |        |                |     |
EMC_STOR_SITE1 -  TCPIP  node001  111.222.333.444  2707  ANY
EMC_STOR_SITE2 -  TCPIP  node002  111.222.333.555  2707  ANY
```

In this scenario, the /var/symapi/config/netcnfg file contains two service names. One points to the Dell EMC VMAX Storage with storage security identifier (SID) 000196800508, and the other points to the Dell EMC VMAX Storage with SID 000196800573. The IP address that is used in this file points to the SYMAPI servers, which have gatekeeper disks from the storage systems.

Example 10-2 shows the contents of the /var/symapi/config/netcnfg file from another example.

Example 10-2 Contents of the /var/symapi/config/netcnfg file from an example environment

```
# grep -v "\#" /var/symapi/config/netcnfg

SYMAPI_SITE_508 - TCPIP r7r3m106 10.xxx.xxx.xxx 2707 ANY
SYMAPI_SITE_573 - TCPIP r7r3m107 10.xxx.xxx.xxx 2707 ANY
```

Now that the installation and configuration of the Dell EMC Solutions Enabler on the KSYS node are complete, use the SYMCLI commands to test whether the communication between the KSYS node and both Dell EMC VMAX Storage devices is working properly through the SYMAPI servers. To complete this task, export the variable **SYMCLI_CONNECT**, which contains the service name of the SYMAPI server that you plan to use (one of the names that is created in the /var/symapi/config/netcnfg file), and the variable **SYMCLI_CONNECT_TYPE**, which has the value of REMOTE, to specify that this operation is a remote operation that uses TCP/IP.

Example 10-3 shows the communication with storage 000196800508 (using the SYMAPI server SYMAPI_SITE_508). Both storages are displayed because the SRDF replication is configured, but you can see that storage 000196800508 is Local, and storage 000196800573 is Remote.

Example 10-3 Testing communication through SYMAPI_SITE_508

```
# export SYMCLI_CONNECT_TYPE=REMOTE
# export SYMCLI_CONNECT=SYMAPI_SITE_508
# symcfg list

                                S Y M M E T R I X

                                       Mcode    Cache      Num Phys  Num Symm
    SymmID       Attachment  Model     Version  Size (MB)  Devices   Devices

    000196800508 Local       VMAX100K  5977      216064        18     13001
    000196800573 Remote      VMAX100K  5977      217088         0      9387
```

Example 10-4 shows the communication with storage 000196800573 by using SYMAPI server SYMAPI_SITE_573. Both storages are displayed because the SRDF replication is configured, but you can see that storage 000196800573 is Local, while 000196800508 storage is Remote.

Example 10-4 Testing communication through SYMAPI_SITE_573

```
# export SYMCLI_CONNECT_TYPE=REMOTE
# export SYMCLI_CONNECT=SYMAPI_SITE_573
# symcfg list

                                S Y M M E T R I X

                                       Mcode    Cache      Num Phys  Num Symm
    SymmID       Attachment  Model     Version  Size (MB)  Devices   Devices

    000196800573 Local       VMAX100K  5977      217088        15      9387
    000196800508 Remote      VMAX100K  5977      216064         0     13001
```

Tip: To see which variables were exported, run **symcli -def** to see the exported environment variables that are relevant to the Dell EMC Solutions Enabler:

```
# symcli -def
Symmetrix Command-Line Interface (SYMCLI) Version V8.1.0.0 (Edit Level: 2054)
built with SYMAPI Version V8.1.0.0 (Edit Level: 2054)
Current settings of the SYMCLI environmental variables:
SYMCLI_CONNECT                : SYMAPI_SITE_508
SYMCLI_CONNECT_TYPE           : REMOTE
```

This concludes the installation and configuration of the Dell EMC Solutions Enabler on the KSYS node. The KSYS node works as a SYMAPI client, communicating with the Dell EMC Storage devices through the SYMAPI servers.

Adding the storage systems to VMRM

Use the **ksysmgr** command to add the storage systems to the VMRM DR environment. Repeat this command for each storage subsystem that is involved in your VMRM DR environment. The syntax is as follows:

```
# ksysmgr add storage_agent -h

ksysmgr add storage_agent <storage_agent_name>
      hostname | ip =<hostname | ip>
      site=<sitename>
      storagetype=<type>
      serialnumber=<number>
    add => create, make
    storage_agent => storage*, sta
```

`ip` is the IP address of the storage controller (or SYMAPI server) that is obtained from the `/var/symapi/config/netcnfg` file. The `serialnumber` is the SID of the Dell EMC Storage system, and the `storagetype` is `emc` in this case.

Example 10-5 shows the storage agents that are added in our test environment.

Example 10-5 Adding storage agents in an example environment

```
(0) root @ pbrazos001: /
# ksysmgr add storage_agent sa_Poughkeepsie_508 site=Poughkeepsie
serialnumber=000196800508 storagetype=emc ip=10.xxx.xxx.xxx
Adding storage agent this may take a few minutes...
Storage_agent sa_Poughkeepsie_508 was added

(0) root @ pbrazos001: /
# ksysmgr add storage_agent sa_Austin_573 site=Austin serialnumber=000196800573
storagetype=emc ip=10.xxx.xxx.xxx
Adding storage agent this may take a few minutes...
Storage_agent sa_Austin_573 was added
```

Tip: During this step, the KSYS node uses the script `/opt/IBM/ksys/storages/EMC/get_emc_stg_info` to contact the storage controller and obtain information about the storage that you are adding. For more information about this operation, see the `/var/ksys/log/ksys_srdf.log` log file.

Use the **ksysmgr query storage_agent** command to determine whether the storage agents were added properly, as shown in Example 10-6.

Example 10-6 Checking whether the storage agents were added

```
(0) root @ pbrazos001: /
# ksysmgr query storage_agent
Name:            sa_Poughkeepsie_508
Serial:          196800508
Storagetype:     SRDF
Site:            Poughkeepsie
Ip:              10.xxx.xxx.xxx
Login:           default

Name:            sa_Austin_573
Serial:          196800573
Storagetype:     SRDF
Site:            Austin
Ip:              10.xxx.xxx.xxx
Login:           default
```

During this action, the resource class IBM.VMR_SA is populated with the storage agent information, as shown in Example 10-7.

Example 10-7 Resource class IBM.VMR_SA populated with storage agent information

```
(0) root @ pbrazos001: /
# lsrsrc IBM.VMR_SA
Resource Persistent Attributes for IBM.VMR_SA
resource 1:
        SAname           = "sa_Poughkeepsie_508"
        SA_serial        = "196800508"
        storageType      = 227
        siteID           = 1
        ipAddr           = "10.xxx.xxx.xxx"
        userID           = "default"
        password         = "default"
        StgInfVendor     = "EMC"
        StgInfProductID  = "SYMMETRIX"
        StgInfRevision   = "5977"
        Phase            = "READY"
        PhaseDetail      = 0
        ActivePeerDomain = "itsocluster"
resource 2:
        SAname           = "sa_Austin_573"
        SA_serial        = "196800573"
        storageType      = 227
        siteID           = 2
        ipAddr           = "10.xxx.xxx.xxx"
        userID           = "default"
        password         = "default"
        StgInfVendor     = "EMC"
        StgInfProductID  = "SYMMETRIX"
        StgInfRevision   = "5977"
        Phase            = "READY"
        PhaseDetail      = 0
        ActivePeerDomain = "itsocluster"
```

Configuration for DR rehearsal

Dell EMC SRDF has a **symclone** feature that creates the mirror copy of an existing target disk on the target storage. This extra copy is used by VMRM to activate the VM on the target site. Dell EMC Symmetrix **symclone** supports three operations:

Create The create operations create a clone of the target disk by using the **symclone create** command.

Activate The activate operation activates the clone by using the **symclone activate** command.

Terminate The terminate operation deletes the pairing information from the storage subsystem and removes any hold on the target device. You must “terminate” while the pair is in the Copied state to get a fully valid data copy.

The size of the target disk and the extra disk that is used for cloning should be the same as the source. The configuration of a clone copy is required only on the target storage for DR rehearsal.

Create a text file with the disk IDs of the target disks and the clone disks for creating and activating the clones. The file name can be any user-defined name. In this example, `clone_disk_id` is the file name that is used for reference. The command syntax for the **symclone create** operation is as follows:

```
/usr/symcli/bin/symclone -sid <target_storage_id> -f <clone_disk_id> create -diff
-nop -force
```

To check the mirror status between target disk and extra clone disk, run the following command:

```
symclone -sid 573 list | grep -E “disk_ids”
```

Example 10-8 shows the status of mirroring between the target disk and the clone disk.

Example 10-8 symclone mirroring status

```
# symclone -sid 573 list | grep -E "0307E|02F8D|03075|03078|0307C|0307D"
02EC8 409605 02F8D   X.X. Created
02EC9 409605 03075   X.X. Created
02ECB 409605 03078   X.X. Created
02ECF 409605 0307C   X.X. Created
02EC0 409605 0307D   X.X. Created
02F6C 409605 0307E   X.X. Created
```

After the clone is created, the status of mirroring is shown in the **symclone list** output. Activate mirroring between the clone and the target disk by using the **symclone activate** command and wait until the status shows “Copied”. If the mirroring state is not “Copied”, then the verify operation for DR test in VMRM fails.

The command syntax for **symclone activate** is as follows:

```
/usr/symcli/bin/symclone -sid <target_storage_id> -f <clone_disk_id> activate -nop
-force
```

Adding and removing disks from VMs

During KSYS discovery operations, a composite group is created in Dell EMC storage agents. The composite group often goes into an error state while removing or adding disks in VMs. If you want to remove or add a disk to the VMs that are managed by VMRM, perform specific steps in the storage agents to ensure that the composite group is in an error-free state in the subsequent KSYS operations.

To add a disk to a VM, complete the following steps:

1. Map the disk to the VM.
2. Add the disk to the SRDF group in the storage agent.
3. Run the discovery operation at the KSYS node.

To remove a disk from a VM, complete the following steps:

1. Unmap the disk from the VM.
2. Remove the LUN or disk from the composite group.
3. Remove the LUN or disk from the SRDF group.
4. Run the discovery operation at the KSYS node.

10.4.2 Setting up SAN Volume Controller and Storwize systems

The way the KSYS node communicates with the SAN Volume Controller is through **ssh**. It issues storage command-line interface (CLI) commands through **ssh** to the SAN Volume Controller. The SAN Volume Controller username that is used on each SAN Volume Controller storage system must have an Administrator role to manage all functions of the storage system. KSYS must be able to **ssh** to the storage system as this user without supplying a password. To do this task, create an ssh private and public key pair (by running the command **ssh-keygen -t rsa**) and share the public key (`/.ssh/id_rsa.pub`) to your storage administrator. Your storage administrator uses the public key to enable the SAN Volume Controller user to **ssh** to the SAN Volume Controller storage systems without a password.

The command to register a SAN Volume Controller storage system to VMRM DR is as follows:

```
ksysmgr add storage_agent <storage_agent_name>
   hostname | ip =<hostname | ip>
   site=<sitename>
   storagetype=svc
   clusterid=<number> | serialnumber=<number>
   login=<username>
```

`storage_agent_name` is a user-supplied name. You can find the cluster ID of the SAN Volume Controller storage system by running the **svcinfo lscluster** command as follows:

```
ssh usrid@ipaddr svcinfo lscluster
```

For our test environment, the command and subsequent output are shown in Example 10-9 on page 277.

Example 10-9 Getting the SAN Volume Controller cluster information and ID

```
# ssh admin@itsosvcindia svcinfo lscluster
id               name      location partnership      bandwidth id_alias
00000200A08109B2 storwize3 local                               00000200A08109B2
00000200A583340E Storwize6 remote   fully_configured 62        00000200A583340E
0000010020A06150 Storwize4 remote   fully_configured 62        0000010020406150
00000200A0A4914C Storwize7 remote   fully_configured 102      00000200A084914C
```

The cluster ID for this SAN Volume Controller storage system should be `00000200A08109B2` for the subsystem in India. We have another one in the US with cluster ID `0000010020A06150.` The storage systems in both the home and backup sites must be registered to the KSYS node. The commands to register them both into the VMRM DR environment are shown in Example 10-10.

Example 10-10 Adding SAN Volume Controller storage agents to the VMRM DR configuration

```
#ksysmgr add storage_agent sw31_home hostname=itsosvcindia login=admin
serialnumber=200A08109B2 site=INDIA storagetype=svc

#ksysmgr add storage_agent sw41_backup hostname=itsosvcusa login=admin
serialnumber=10020A06150 site=USA storagetype=svc
```

The output from the command in Example 10-10 is shown in Example 10-11.

Example 10-11 Query storage_agent results for SAN Volume Controller

```
# ksysmgr query storage_agent
Name:                sw41_backup
Serial:              10020A06150
Storagetype:         SVC
Site:                USA
Ip:                  119.xxx.xxx.xxx
Login:               admin

Name:                sw31_home
Serial:              200A08109B2
Storagetype:         SVC
Site:                INDIA
Ip:                  119.yyy.yyy.yyy
Login:               admin
```

Before running **`ksys discovery`** on your cluster, your storage administrator must start the replication of all the disks that are managed by VMRM DR. The replication pairs are defined and replicate. If DR rehearsal is configured, the IBM FlashCopy® relationships must be defined. The SAN zoning and LUN masking must be configured too.

Here are some sample commands that can be used to prepare the storage systems. These commands are run by your storage administrators.

1. Create a relationship between a source disk andan auxiliary disk:

   – For async (Global Mirror):

   ```
   svctask mkrcrelationship -master <source_disk> - aux <remote_disk> -name
   <relationship_name> -cluster <remote_clusterid/cluster_name> -global
   ```

   – For sync (Metro Mirror):

   ```
   svctask mkrcrelationship -master <source_disk> - aux <remote_disk> -name
   <relationship_name> -cluster <remote_clusterid/cluster_name>
   ```

> **Note:** **mkrcrelationship** creates disk replications only between a source disk and a target storage disk. The relationships must be started. The command requires the `clusterid` of the target storage, which can be obtained by using the **svcinfo lscluster** command, as shown in Example 10-9 on page 277.

2. List the relationship that is created by using either of the following two methods:

   – **svcinfo lsrcrelationship**

   – **svcinfo lsrcrelationship <relationship_name>/<id>**

3. Start the replication by starting a relationship at the storage level. To start replication copying from a source vDisk to a target vDisk, run the following command:

   ```
   svctask startrcrelationship <relationship_name>/<id>
   ```

4. Create the relationship for the DR rehearsal at the target site storage by using either of the following two methods:

   – For a snapshot copy, run this command:

   ```
   svctask mkfcmap -cleanrate 0 -copyrate 0 -source <source_disk_name> - target
   <target_disk_name>
   ```

   – For a clone, run this command:

   ```
   svctask mkfcmap -source <source_disk_name> -target <target_disk_name>
   -copyrate 100
   ```

10.4.3 Setting up the IBM DS8000 Storage Systems

DS8000 Storage Systems use a concept that is called a *session* to manage consistent groups. A session is a logical collection of disk volumes across multiple storage systems that are managed together to create consistent copies of data. All storage operations in the VMRM DR solution are performed on a session ID.

During the discovery phase, the KSYS interacts with the HMC and the VIOS to retrieve the storage disk information that is used by the VMs. Then, the KSYS creates a session in each site and adds all the disks to this session. The KSYS uses sessions to change the replication direction during a planned or unplanned recovery operation.

Example 10-12 on page 279 show the output from a **ksysmgr query disk_group** command.

Example 10-12 ksysmgr query disk_group command

```
#  ksysmgr query disk_group
Name:                VMRDG_AB_HADRHA_BackupSite_1
Site:                BackupSite
Hosts:               e50cat-8247-22L-2133A5A
                     e10kacha-8284-22A-1073C6T
CG:                  2

Name:                VMRDG_AB_HADRHA_HomeSite_1
Site:                HomeSite
Hosts:               e52den-8247-22L-21339EA
                     e52pen-8247-22L-2133AAA
CG:                  1
```

Notice that the CG is a session number and not a name.

> **Note:**
>
> - The VMRM DR solution supports only the Global Mirror (asynchronous) mode of data replication across sites.
> - The VMRM DR solution supports only a single DS8000 storage system per site, which means that all storage devices must be configured as a single DS8000 cluster per site.

The VMRM DR solution uses the DS8000 Series Command-Line Interface (DSCLI) client to interact with the DS8000 Storage Systems. The **dscli** command is installed in /opt/ibm/dscli/dscli. The installation media can be downloaded from IBM Fix Central.

Your storage administrator must create a user on each DS8000 Storage System who has the “Administrator” role to manage all functions of the storage system. The verification of connectivity and access to the storage system can be achieved as shown in Example 10-13.

Example 10-13 Verifying DS8000 connectivity and access

```
# /opt/ibm/dscli/dscli -user fvtadmin -passwd passw0rd -hmc1 9.xxx.xxx.xxx lssi
Date/Time: November 11, 2022 10:37:04 AM CST IBM DSCLI Version: 7.9.10.275 DS: -
Name  ID               Storage Unit     Model WWNN             State  ESSNet
============================================================================
ds8k5 IBM.2107-75NR571 IBM.2107-75NR570 951   5005076309FFC5D5 Online Enabled
```

As shown in Example 10-13, fvadmin is the username; passw0rd is the password; and 9.xxx.xxx.xxx is the IP address of the HMC within the DS8000 Storage System.

The command to add a DS8000 storage system to VMRM DR is as follows:

```
ksysmgr add storage_agent <storage_agent_name>
      hostname | ip =<hostname | ip>
      site=<sitename>
      storagetype=ds8k
      login=<username>
      password=<password>
```

storage_agent name is user-supplied name. Example 10-14 shows the command to add a DS8000 storage agent to VMRM DR.

Example 10-14 Adding a DS8000 storage agent to the VMRM DR configuration

```
# ksysmgr add storage_agent ds8k5 hostname=9.xxx.xxx.xxx site=HomeSite
storagetype=ds8k login=fvtadmin password=passwd0rd

   # ksysmgr add storage_agent ds8k8 hostname=9.yyy.yyy.yyy site=BackupSite
   storagetype=ds8k login=fvtadmin password=passwd0rd
```

The storage systems in both the production and DR sites must be registered to the VMRM DR environment. The following output is from our test environment and the result of our previous example:

```
# ksysmgr query storage_agent
Name:                   ds8k8
Serial:                 75Y4151
Storagetype:            DS8K
Site:                   BackupSite
Ip:                     9.xxx.xxx.xxx
Login:                  fvtadmin

Name:                   ds8k5
Serial:                 75NR571
Storagetype:            DS8K
Site:                   HomeSite
Ip:                     9.yyy.yyy.yyy
Login:                  fvtadmin
```

Before running **ksys discovery**, your storage administrator must have prepared the LUN replications for all the disks of the VMs that are managed by VMRM DR, which means that the replication pairs are defined and replicating. If DR rehearsal is configured, the FlashCopy relationships must be defined.

The FlashCopy for DR rehearsal might be different than the FlashCopy for an asynchronous configuration. Here is an example command to create a FlashCopy of a LUN for rehearsal on the DS8000 Storage System on the DR site:

```
mkflash -persist -dev IBM.2107-75BLD21 07ac:07ae
```

Here are some sample commands to prepare the storage systems. These commands are run by your storage administrators. If the commands are issued from the KSYS server, add /opt/ibm/dscli/dscli -user fvtadmin -passwd password_of_fvtadmiin -hmc1 IP_of_hmc1_of_DS8K in front of the commands, where fvtadmiin is the user to access the DS8000 storage system.

1. Check the PPRC paths, where 75NR571 is the serial number of the DS8000 Storage System on which the command is issued. You can find the serial number by running the **lssi** command:

   ```
   lspprcpath -dev IBM.2107-75NR571 00
   ```

2. Obtain the LUN details to create pprcpath by running the following command:

   ```
   lsavailpprcport -dev IBM.2107-75LY981 -remotedev IBM.2107-75BLD21 -remotewwnn
   5005076304FFD5A0 00:07
   ```

3. Create pprcpath between the two LUNs by running the following command. This task *must* be performed from both directions.

```
mkpprcpath -dev IBM.2107- 75NR571 -remotedev IBM.2107-75LY981 -remotewwnn
5005076308FFC6D4 -srclss 00 -tgtlss 01 I0130:I0002
```

4. Create PPRC pairs between disks by running the following command:

```
mkpprc -dev IBM.2107-75LY981 -remotedev IBM.2107-75NR571 -type gcp 00DB:0302
```

5. List the PPRC by running the following command:

```
lspprc -dev IBM.2107-75LY981 - remotedev IBM.2107-75NR571 00DB
```

6. List the FlashCopy copies by running the following command:

```
lsflash -dev IBM.2107-75LY981 00DB
```

7. Create FlashCopy copies by running the following command:

```
mkflash -tgtinhibit -nocp - record -dev IBM.2107-75NR571 0508:0509
```

8. Create FlashCopy copies for DR rehearsal by running the following command:

```
mkflash -persist -dev IBM.2107-75BLD21 07ac:07ae
```

9. Remove a FlashCopy by running the following command:

```
rmflash -dev IBM.2107- 75NR571 0508:0509
```

10. Check the sessions by running the following commands:

```
lssession -dev IBM.2107- 75LY981 02
lssession -dev IBM.2107- 75NR571 00-ff
```

11. Create a session by running the following command:

```
mksession -dev IBM.2107- 75NR571 -lss IBM.2107-75NR571/05 09
```

12. Add disk to a session by running the following command:

```
chsession -dev IBM.2107- 75NR571 -lss IBM.2107-75NR571/05 -action add -volume
0508 09
```

13. Remove a disk from a session by running the following command:

```
chsession -dev IBM.2107- 75NR571 -lss A0 -action remove -volume A002 03
```

14. Remove a session by running the following command:

```
rmsession -dev IBM.2107- 75NR571 -lss 03 01
```

15. Display the Global Mirror session (session 01, LSS 04) by running the following command:

```
showgmir -dev IBM.2107- 75LY981 -session 01 IBM.2107-75LY981/04
```

16. To view the CG, run **lssession**, which shows disks and the session ID:

```
lssession -dev IBM.2107- 75LY981 <lss>
```

10.4.4 Setting up VMRM DR on Hitachi storage systems

This section describes the following items about setting up VMRM DR on Hitachi storage systems:

- Concept
- Requirements
- Command Control Interface
- Hitachi Open Remote Copy Manager
- Installing the CCI software
- Configuring the KSYS server as a CCI client

- Adding the storage systems to VMRM DR
- Limitations for Hitachi disks

Concept

The VMRM DR solution supports DR for third-party vendor storage from Hitachi. The VMRM DR solution supports both synchronous and asynchronous data replications by using Hitachi TrueCopy remote replication and HUR technologies.

> **Note:** VMRM DR supports the following models of the Hitachi storage system:
>
> - Hitachi VSP G200
> - Hitachi VSP G400
> - Hitachi VSP G600
> - Hitachi VSP G800
> - Hitachi VSP G1000
>
> VMRM DR supports both synchronous and asynchronous modes of storage replication.

The setup of VMRM DR for Hitachi mirrored storage system involves the following steps:

1. Plan the storage deployment and replication that are necessary for your environment. This process is related to the applications and middleware that must be deployed in the environment that you want to include in the recovery management by using the VMRM DR solution.
2. Use the storage configuration tools that are provided by Hitachi to configure the storage devices that you define in step 1, and deploy the devices. These devices should be prepared by your storage administrators.
3. Use the `ksysmgr` interface to discover the deployed storage devices and define the DR policies for the applications or VMs that are using the mirrored storage.

Requirements

The VMRM DR solution requires the following components for Hitachi storage configuration:

- Command Control Interface (CCI) software for AIX. For more information about CCI, see the Hitachi CCI documentation that is maintained by Hitachi. The CCI software must be installed on the KSYS LPAR to communicate with the CCI server.
- The VMRM DR solution requires CCI Version 01-39-03/04 with model RAID-Manager/AIX.
- All ports of the Hitachi storage system must be accessible to the KSYS node.

Command Control Interface

Storage replication on the Hitachi storage systems is managed by a CCI agent. CCI is similar to the Solution Enabler system from Dell EMC. There are two types of installations of CCI: One is in-band and one is out-of-band.

An-in band installation needs a physical connection (FC usually) to manage directly a storage LUN from the Hitachi storage system that is managed. This storage device is called the *command device*. An in-band installation is also called a *CCI server*.

An out-of-band installation is used to communicate with the Hitachi storage systems through an in-band CCI installation. An out-of-band installation is also called a *CCI client*. Configure the KSYS LPAR to be an out-of-band CCI installation for all the Hitachi storage systems that are registered in the VMRM DR environment.

Figure 10-4 shows the relationship between the KSYS server, CCI client, CCI server, and the Hitachi storage systems.

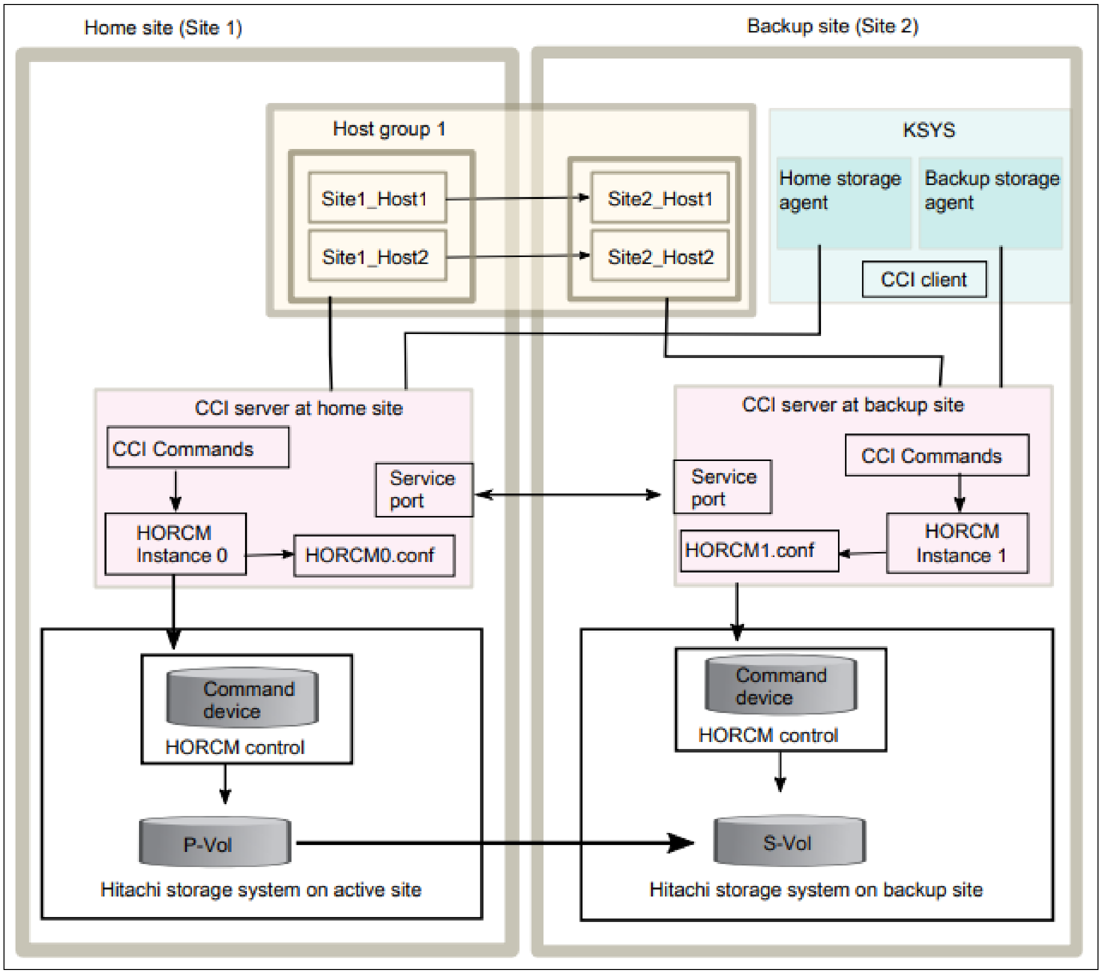


Figure 10-4 Relationship between the KSYS and Hitachi storage systems

Most likely, the CCI servers are installed and configured for the Hitachi storage systems that are related to your VMRM DR configuration. If not, ask your storage administrator to install and configure the necessary CCI servers. The steps to configure a CCI server is beyond the scope of this book.

Hitachi Open Remote Copy Manager

The Hitachi Open Remote Copy Manager (HORCM) is in the CCI server or client. The HORCM operates as a daemon process. When activated, the HORCM refers to CCI configuration definition files that also are on the CCI server or client. The HORCM instance communicates with the storage system and remote CCI servers.

The following sections describe the steps to configure the KSYS server as a CCI client for the Hitachi storage systems that will be registered to the VMRM DR environment.

Installing the CCI software

Ask your storage administrator to get the software or ask your storage administrator to install the CCI software on to the KSYS server.

Configuring the KSYS server as a CCI client

The storage administrator must provide the IP addresses of the CCI servers and the port numbers of the HORCM instances for each Hitachi storage system. The following steps are based on an example: two Hitachi storage systems, one on the production site and one on the DR site. The storage administrator has provided the following information:

- On the Hitachi storage system on the production (source) site, the CCI server IP address is 10.xxx.xxx.xxx (UDP), and the port number is 52323.
- On the Hitachi storage system on the DR (target) site, the CCI server IP address is 10.yyy.yyy.yyy (UDP), and the port number is 52323.

Complete the following steps:

1. On the KSYS server, define a HORCM instance for each Hitachi storage system. If DR rehearsal is needed, another HORCM instance is needed for each Hitachi storage system on the DR site. For each instance, select an instance number, a UDP port number, and a service name. As an example, we select the following values:

Source Hitachi	11	52327	hamon1
Target Hitachi	12	52326	hamon2
DR Rehearsal	13	52325	hamon3

   Assume that the IP address of the KSYS server is `10.xxx.xxx.xxx`. Here are the three configuration files that you need to create on the KSYS server and the contents of each file:

   – For the source instance 11:

   ```
   # cat  horcm11.conf
   HORCM_CMD
   \\.\IPCMD-10.xxx.xxx.xxx-52323

   HORCM_MON
   10.xxx.xxx.xxx hamon1              1000            3000
   ```

   – For the target instance 12:

   ```
   # cat  horcm12.conf
   HORCM_CMD
   \\.\IPCMD-10.xxx.xxx.xxx-52323

   HORCM_MON
   10.xxx.xxx.xxx hamon2              1000            3000
   ```

   – For the DR rehearsal instance 13:

   ```
   # cat  horcm13.conf
   HORCM_CMD
   \\.\IPCMD-10.xxx.xxx.xxx-52323

   HORCM_MON
   10.xxx.xxx.xxx hamon3              1000            3000
   ```

2. Add the service names and the port numbers to the `/etc/services` file:

   ```
   # grep hamon /etc/services
   hamon1      52327/udp
   hamon2      52326/udp
   hamon3      52325/udp
   ```

3. After adding those three entries, refresh the `InetD` daemon by running the following command:

   ```
   # refresh -s InetD
   ```

4. Start the services for each instance as shown here:

   ```
   #  /HORCM/usr/bin/horcmstart.sh 11
   #  /HORCM/usr/bin/horcmstart.sh 12
   #  /HORCM/usr/bin/horcmstart.sh 13
   ```

5. Verify whether the instances are running as follows:

   ```
   # ps -ef |grep horcm
       root  9961818       1   0   Nov 05      -  0:02 horcmd_013
       root 14156230       1   0 00:02:16      -  0:00 horcmd_012
       root 14221638       1   0 00:02:15      -  0:00 horcmd_011
   ```

Here is the command to stop an instance:

```
# /HORCM/usr/bin/horcmshutdown.sh  XX
```

“XX” is the instance number. The Hitachi log file on the KSYS server is at `/var/ksys/log/ksys_cci.log`.

Adding the storage systems to VMRM DR

After the HORCM instances are configured and started, register them in the VMRM DR environment by running the command that is shown in Example 10-15.

Example 10-15   Adding a Hitachi storage agent to a VMRM DR configuration

```
# ksysmgr add storage_agent G1000 serialnumber=57558 hostname=10.xxx.xxx.xxx
login=fvtadmin site=INDIA storagetype=hitachi instance=11

#ksysmgr add storage_agent G350 serialnumber=460724 hostname=10.xxx.xxx.xxx
login=fvtadmin site=USA storagetype=hitachi instance=12 drinstance=13
```

The login ID, password, and storage serial numbers are provided by your storage administrator. Notice how the HORCM instance for DR rehearsal was added to the environment by verifying the storage agent definitions, as shown in Example 10-16.

Example 10-16   Querying a storage agent for Hitachi storage

```
# ksysmgr q storage_agent
Name:                   G350
Serial:                 60724
Storagetype:            Hitachi
Site:                   USA
Ip:                     10.xxx.xxx.xxx
Login:                  fvtadmin
Instance:               12
DrInstance:             13

Name:                   G1000
Serial:                 57558
Storagetype:            Hitachi
Site:                   INDIA
Ip:                     10.xxx.xxx.xxx
Login:                  fvtadmin
Instance:               11
DrInstance:             default
```

After the storage administrator prepares the storage replication (defines volume groups and replication pairs and starts the replications), you can run **`ksys discovery`**. The KSYS discovery process adds entries that are related to the consistent groups of the host groups and workgroups to the instance configuration files. For example, after discovery, the configuration file for the source Hitachi storage systems is shown in Example 10-17.

Example 10-17 Hitachi configuration file after discovery

```
# cat  horcm11.conf
HORCM_CMD
\\.\IPCMD-10.xxx.xxx.xxx-52323

HORCM_MON
10.xxx.xxx.xxx hamon1               1000            3000

HORCM_LDEV
cg_doit3001_005 cg_doit3001_005_1 357558 650 0
cg_doit3001_005 cg_doit3001_005_2 357558 647 0
cg_doit3001_005 cg_doit3001_005_3 357558 646 0
cg_doit3001_005 cg_doit3001_005_4 357558 649 0
cg_doit3001_005 cg_doit3001_005_5 357558 648 0

HORCM_INST
cg_doit3001_005 10.xxx.xxx.xxx hamon2

HORCM_LDEV
cg_doit3006_010 cg_doit3006_010_1 357558 653 0
cg_doit3006_010 cg_doit3006_010_2 357558 655 0
cg_doit3006_010 cg_doit3006_010_3 357558 652 0
cg_doit3006_010 cg_doit3006_010_4 357558 651 0
cg_doit3006_010 cg_doit3006_010_5 357558 654 0

HORCM_INST
cg_doit3006_010 10.xxx.xxx.xxx hamon2
```

The configuration file for the target Hitachi storage systems is shown in Example 10-18.

Example 10-18 Configuration file for Hitachi target storage

```
# cat  horcm12.conf
HORCM_CMD
\\.\IPCMD-10.xxx.xxx.xxx-52323

HORCM_MON
10.xxx.xxx.xxx hamon2               1000            3000

HORCM_LDEV
cg_doit3001_005 cg_doit3001_005_1 460724 59 0
cg_doit3001_005 cg_doit3001_005_2 460724 56 0
cg_doit3001_005 cg_doit3001_005_3 460724 55 0
cg_doit3001_005 cg_doit3001_005_4 460724 58 0
cg_doit3001_005 cg_doit3001_005_5 460724 57 0

HORCM_INST
cg_doit3001_005 10.xxx.xxx.xxx hamon1
```

```
HORCM_LDEV
cg_doit3006_010 cg_doit3006_010_1 460724 62 0
cg_doit3006_010 cg_doit3006_010_2 460724 64 0
cg_doit3006_010 cg_doit3006_010_3 460724 61 0
cg_doit3006_010 cg_doit3006_010_4 460724 60 0
cg_doit3006_010 cg_doit3006_010_5 460724 63 0

HORCM_INST
cg_doit3006_010 10.xxx.xxx.xxx hamon1
```

During KSYS discovery for DR rehearsal (`dr_test=yes`), entries of the LUNs that are related to the DR rehearsal copies are added to the instance configuration files. For example, after KSYS discovery for DR rehearsal, the configuration file for DR rehearsal is shown in Example 10-19.

Example 10-19 DR rehearsal configuration file

```
# cat  horcm13.conf
HORCM_CMD
\\.\IPCMD-10.xxx.xxx.xxx-52323

HORCM_MON
10.xxx.xxx.xxx hamon3               1000            3000

HORCM_LDEV
cg_doit3006_010 cg_doit3006_010_1 460724 72 0
cg_doit3006_010 cg_doit3006_010_2 460724 74 0
cg_doit3006_010 cg_doit3006_010_3 460724 71 0
cg_doit3006_010 cg_doit3006_010_4 460724 70 0
cg_doit3006_010 cg_doit3006_010_5 460724 73 0

HORCM_INST
cg_doit3006_010 10.xxx.xxx.xxx hamon2

HORCM_LDEV
cg_doit3001_005 cg_doit3001_005_1 460724 69 0
cg_doit3001_005 cg_doit3001_005_2 460724 66 0
cg_doit3001_005 cg_doit3001_005_3 460724 65 0
cg_doit3001_005 cg_doit3001_005_4 460724 68 0
cg_doit3001_005 cg_doit3001_005_5 460724 67 0

HORCM_INST
cg_doit3001_005 10.xxx.xxx.xxx hamon2
```

In these example outputs, note the following items:

- There are two workgroups that are configured in this example VMR DR environment, which result in two consistent (volume) groups in the storage systems. Each workgroup corresponds to a pair of blocks in each of the output files (the `HORCM_LDEV` and `HORCM_INST` blocks).
- cg_doit3001_005 and cg_doit3006_010 are consistent groups in the storage systems for the two workgroups. The consistent group name for each workgroup is the same on both the target site and the source site. In this example, the consistent group name is cg_doit3001_005 for one workgroup and cg_doit3006_010 for the other workgroup.
- Logical devices (LDEVs) are specific to the SID, which is either `357558` or `460724` in the example output.

For DR rehearsal, in addition to the HORCM instance, the following steps must be done on the target Hitachi storage systems to create the third copy (the mirror copy of the target disks) before the DR rehearsal discovery:

1. In the GUI of the target storage, create a dummy host on the port that has the target host.

   Note: Do not assign a worldwide port name (WWPN) in this stage.

2. Create an LDEV with the size equal to the size of the target logical disk. The LDEV is used as the shadow image of the target LDEV.
3. Map the path of the LUN to the dummy host that you created in the earlier steps.
4. To create a clone, select **Replication** → **Local replication** → **Create SI**.
5. When the shadow image is created, resync the shadow image. To resync the pair, select **Replication** → **Local replication** → **Select the replication** → **Resync Pair**.

Example 10-20 shows the results of **`query disk_group`**.

Example 10-20 ksysmgr query disk_group

```
# ksysmgr query disk_grpup
Name:                VMRDG_hitachi_USA_5
Site:                USA
Hosts:               doit3-8233-E8B-06DA59R
CG:                  cg_doit3006_010

Name:                VMRDG_hitachi_INDIA_5
Site:                INDIA
Hosts:               doit4-8233-E8B-06DA5AR
CG:                  cg_doit3006_010

Name:                VMRDG_hitachi_INDIA_4
Site:                INDIA
Hosts:               doit4-8233-E8B-06DA5AR
CG:                  cg_doit3001_005

Name:                VMRDG_hitachi_USA_4
Site:                USA
Hosts:               doit3-8233-E8B-06DA59R
CG:                  cg_doit3001_005
```

Limitations for Hitachi disks

Be aware of the following limitations when using Hitachi storage systems in the VMRM DR solution:

- The device names (**`dev_name`** attributes) must map to LDEVs and the device groups (**`dev_group`** attributes) must be defined under the `HORCM_LDEV` section in the `horcm.conf` file.
- The VMRM DR solution uses the `dev_group` attribute for any basic operation that is related to the Hitachi storage systems. Some examples of basic operations are **`pairresync`**, **`pairevtwait`**, and **`horctakeover`**. If several device names are in a device group, the device group must be consistency enabled.
- For command devices, the "Security" option in the Command Device Attributes panel must be *disabled* and the "User Authentication" option must be *enabled*. Otherwise, the required information, such as the LDEV ID, journal volume ID, CG ID, and volume type, is not displayed in any command output. The KSYS subsystem requires this information to monitor the state of storage subsystem disks.
- The HUR technology requires journal groups. Each pair relationship in a journal group is called a *mirror*. A mirror ID is required for the 3-data-center (3DC) configuration. In a 3DC configuration, two or more restore journal groups can be set for one master journal group. At the time of writing, VMRM DR supports a 2-data-center (2DC) configuration, which does not require a mirror ID. The VMRM DR configuration uses 0 mirror ID for synchronous (TrueCopy) and asynchronous (Universal Copy) configuration.
- The VMRM DR solution does not trap Simple Network Management Protocol (SNMP) notification events for HUR storage. If an HUR link goes down when the hosts are functional and later the HUR link is repaired, you must manually resynchronize the disk pairs.
- The KSYS subsystem does not control the creation of disk pairs. Create the disk pairs before you start the KSYS partition.
- Dynamic manipulation of disk groups is not supported for Hitachi storage systems. The KSYS subsystem might break the grouping of the disks in a disk group during the group manipulation operation. When a disk is removed from a disk group, the disk moves into a simplex state.

  The following cases result in disk removal from a disk group. In these cases, the Hitachi storage subsystem removes the pair relationship.

  – Removing disks from a VM
  – Performing an LPM operation or Remote Restart operation across host groups
  – Restoring a snapshot
  – Unmanaging a VM from the KSYS subsystem
  – Removing a host from host group and adding the host to another host group
  – Removing a VM from workgroup
  – Removing a cluster

  The disk pair must be explicitly re-created before adding the same disk or VM to the VMRM DR management.
- Hosts that are managed by the VMRM DR solution cannot contain volume groups with both HUR-protected and non-HUR-protected disks. A host must contain a HUR-protected disk.
- All hosts within a site that are managed by the VMRM DR solution must use the same HORCM instance.

- All disks within a site must belong to the same journal volume.
- Do *not* add any special characters to the HORCM configuration file. Use only spaces to separate all the fields in the HORCM file.

10.4.5 Setting up IBM XIV Storage Systems

The XIV Storage System provides a grid architecture and includes copy functions that can be used for various data protection scenarios, such as DR, data migration, and online backup. These functions provide point-in-time copies, which are known as snapshots or full volume copies. The XIV Storage System also includes remote copy capabilities in either synchronous or asynchronous mode. In the VMRM DR solution, you can configure both synchronous and asynchronous mirroring for the XIV Storage System.

The VMRM DR solution creates a mirror snapshot group on the source site. The mirror copy of the snapshot group has the same name as the CG. With each discovery operation, the VMRM DR solution deletes older snapshot groups and creates another set of snapshot groups.

The VMRM DR solution uses the XIV Storage System Command-Line Interface (XCLI) client to interact with the XIV Storage Systems. You can download the installation media from this site.

A user with the storage administrator role and password is needed to register an XIV Storage System to the VMRM DR environment. The following commands can be used to check the connectivity between the KSYS server and an XIV Storage System:

```
xcli -u admin -p adminadmin -m 9.xxx.xxx.xxx time_list
xcli -u admin -p adminadmin -m 9.yyy.yyy.yyy vol_list
```

In this case, `admin` is the user on the XIV Storage System and `adminadmin` is the password of this user. The command to add an XIV Storage System to a VMRM DR environment is as follows:

```
ksysmgr add storage_agent <storage_agent_name>
      hostname | ip =<hostname[,hostname2,hostname3] | ip[,ip2,ip3]>
      site=<sitename>
      storagetype=xiv
      serialnumber=<number>
      login=<username>
      [password=<password>]
```

Multiple IP addresses can be specified so that communication is established on a different port and IP address if one of the ports or the network fails. When running a command, the IBM XIV Storage System Command-Line Interface (XCLI) receives these multiple IP addresses and tries to connect to each of the IP addresses until communication with one of the IP addresses is successful. Example 10-21 shows adding an XIV storage system.

Example 10-21 Adding an XIV Storage System storage agent

```
ksysmgr add storage_agent Site1_Storage1 site=Site1
  storagetype=XIV
  ip=10.xx.yy.zz
  serialnumber=441108
  login=fvtadmin
  password=XXXX
```

Example 10-22 show the output from **ksysmgr query storage_agent**.

Example 10-22 Querying XIV storage agent

```
# ksysmgr query storage_agent
Name:    Site1_storage1
Serial:  441108
Storagetype:    XIV
Site:    Site1
Ip:      10.xx.yy.zz
Login:   fvtadmin

Name:    Site2_storage2
Serial:  57558
Storagetype:    XIV
Site:    Site2
Ip:      10.x1.yy.zz
Login:   fvtadmin
```

Note:

- The XIV Storage System and IBM FlashSystem A9000 are supported only with VIOS 3.1.0.20 or later.
- The XIV Storage System and IBM FlashSystem A9000 require HMC 9.9.1.0 or later.
- The XIV Storage System is supported only with XCLI 4.8.0.6 or later.

Limitations for XIV

Be aware of the following limitations when using XIV replication with VMRM DR:

- The snapshot disk on the target storage system *cannot* be modified.
- After any configuration settings change for asynchronous mirroring, you must run the DR discovery operation, and then run the DR test-discovery operation. The configuration changes do not take effect if you do not run a DR discovery operation before the DR test discovery.
- XIV Storage System supports up to 128 VMs per host group.
- Based on the version of XIV Storage System firmware (FW), a 128 - 512 of the disks can be added to a CG.
- For a VM that is configured with vSCSI disks, before performing asynchronous failover rehearsal, run the **cfgmgr** command.
- For asynchronous mirroring in a VM that is configured with vSCSI disk after the first DR-test (DR rehearsal), you must manually map snapshot LUNs from the target SAN to the target VIOS.

10.4.6 Setting up the Dell EMC Unity storage systems

The KSYS subsystem communicates with the Dell EMC Unity storage systems by using REST APIs that are provided by the storage vendor. For more information about any specific security requirements for these APIs, see the storage vendor documentation. The VMRM DR solution supports Dell EMC Unity storage system 5.0.6.0.6.252 or later and supports both asynchronous and synchronous replication.

The KSYS subsystem creates a CG at the home site and at the backup site for a Dell EMC Unity storage system. Unlike other storage systems, you do not need to create a disk-pair because the KSYS subsystem automatically creates the disk-pair. If a disk with the same name is not found in the target storage, the KSYS subsystem creates a LUN with the same name and with the same size as the target storage and uses the LUN as a disk-pair. The Dell EMC Unity storage system does not allow you to add or remove disks from the CG or perform any other disk management operations. Any update in the disk configuration during the replication session breaks the existing replication session, and a new replication session starts with the updated disk configurations.

For more information about adding a Dell EMC Unity storage system to the VMRM DR environment, see the IBM Virtual Machine Recovery Manager DR Deployment Guide.

11

Scenarios and examples

This chapter provides scenarios for IBM Virtual Machine Recovery Manager (VMRM) HADR. It describes the recovery procedure of each scenario.

To test different failure scenarios, simulate or create failures that might happen in your real production environment. The VMRM development team wrote *“How to inject failure: IBM Virtual Machine Recovery Manager HADR”* to provide some guidance in how to do simulate or create failures.

The following topics are described in this chapter:

- High availability scenarios
- Disaster recovery scenarios

11.1 High availability scenarios

The following section describes how KSYS handles virtual machine (VM) and CEC failures.

11.1.1 Environment details

Figure 11-1 shows the environment that is used for the test scenarios for VMRM HA in this section.

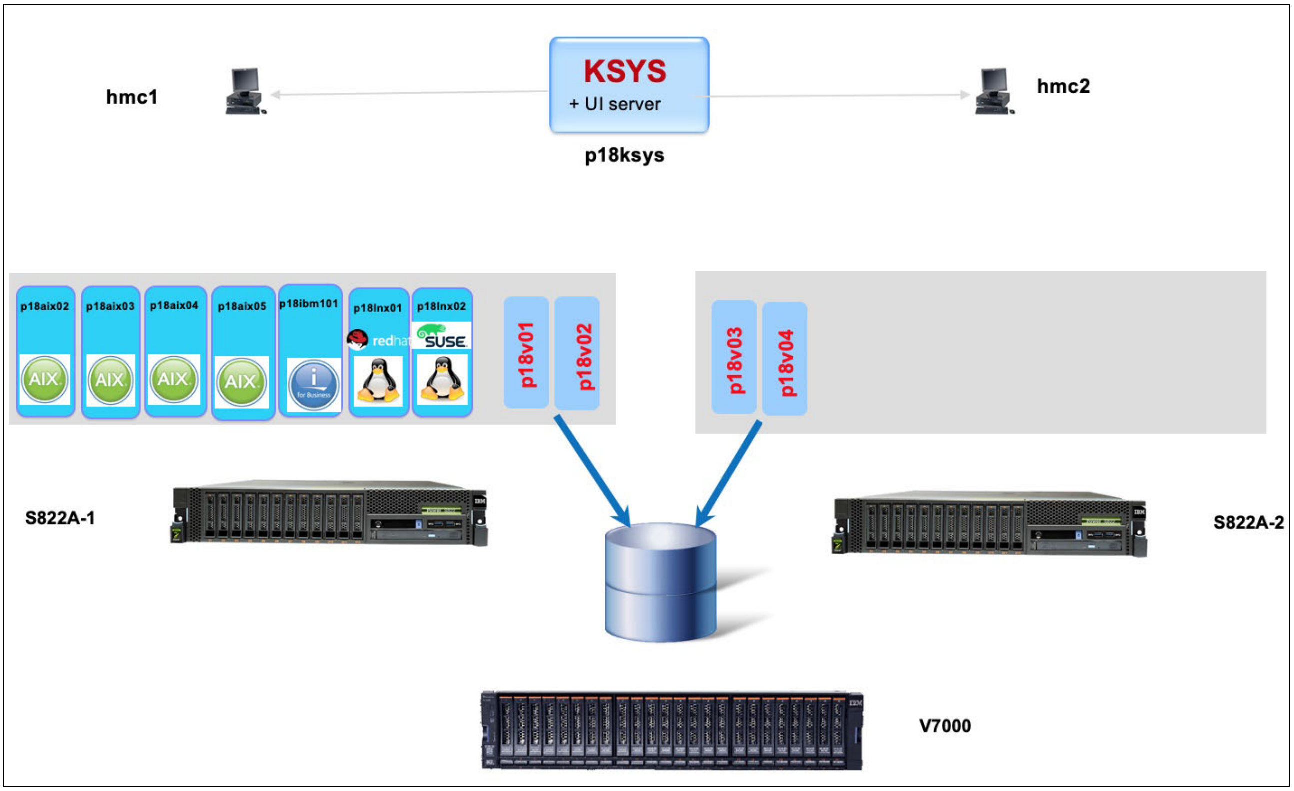


Figure 11-1 Environment that is used for the VMRM HA test scenarios

The environment consists of the following items:

- One KSYS
- Two IBM Power S822 servers (S822A-1 and S822A-2)
- Two Hardware Management Consoles (HMCs) (HMC1 and HMC2)
- One IBM Storwize V7000 that is used for shared storage

Example 11-1 shows the KSYS cluster that is being used.

Example 11-1 Listing the KSYS cluster

```
p18ksys:/ # ksysmgr query cluster
Name:            ksyscluster
State:           Online
Type:            HA
```

The HMCs that are used in this environment are shown in Example 11-2.

Example 11-2 Listing the HMCs

```
p18ksys:/ # ksysmgr query hmc
Name:                hmc2
Ip:                  129.xxx.xxx.xxx
Login:               hscroot

                        Managed Host List:

Hostname                               UUID
=========                               ====
Server-8284-22A-SN10EE85P               fc68b423-a590-3db7-86e9-a7b7d26a07f0
============================================================================


Name:                hmc1
Ip:                  129.xxx.xxx.xxx
Login:               hscroot

                        Managed Host List:

Hostname                               UUID
=========                               ====
Server-8284-22A-SN101AFDR               07e502a4-5051-3867-bd64-11adc2fe8e68
============================================================================
```

The host group that is used in this scenario is shown in Example 11-3.

Example 11-3 Listing the host group

```
p18ksys:/ # ksysmgr query host_group
Name:                HG_TCHU
Hosts:               Server-8284-22A-SN101AFDR
                     Server-8284-22A-SN10EE85P
Memory_capacity:     Priority-Based Settings
                     low:100
                     medium:100
                     high:100
CPU_capacity:        Priority-Based Settings
                     low:100
                     medium:100
                     high:100
Skip_power_on:       No
HA_monitor:          enable
Restart_policy:      auto
VM_failure_detection_speed:    normal
Host_failure_detection_time:   90

SSP Cluster Attributes
Sspname:             KSYS_ksyscluster_1
Sspstate:            UP
Ssp_version:         VIOS 3.1.0.11
VIOS:                p18v02
                     p18v01
                     p18v04
                     p18v03
```

11.1.2 Linux VM failures

This scenario simulates a Linux VM failure that is being managed by IBM Virtual Machine Recovery Manager High Availability (VMRM HA).

Complete the following steps:

1. Find where the test VM is allocated before initiating the Linux VM failure. Example 11-4 shows VM p18lnx02 is on host Server-8284-22A-SN101AFDR.

Example 11-4 Listing the location of VM p18lnx02

```
p18ksys:/ # ksysmgr query vm p18lnx02
Name:                p18lnx02
UUID:                495778C3-80DB-4FE3-989D-E38C905450E8
State:               VERIFY
Host:                Server-8284-22A-SN101AFDR
Priority:            High
VM_failure_detection_speed:    fast
HA_monitor:          enable
Homehost:            Server-8284-22A-SN10EE85P
VM_status:           NO_OPERATION_IN_PROGRESS
Version_conflict:    No
```

2. Verify the test VM by listing all VMs that are allocated to source host Server-8284-22A-SN101AFDR, as shown in Example 11-5.

Example 11-5 Listing VMs on Server-8284-22A-SN101AFDR

```
hscroot@p18vhmc1:~> lsrefcode -m  Server-8284-22A-SN101AFDR -r lpar -F lpar_name
p18v03
p18ibmi01
p18v04
p18aix02
p18aix03
p18aix04
p18aix05
p18lnx02
```

3. List all VMs that are allocated to the target host, in this case the original home host, Server-8284-22A-SN10EE85P, as shown in Example 11-6.

Example 11-6 Listing VMs on target Server-8284-22A-SN10EE85P

```
hscroot@p18vhmc2:~> lsrefcode -m Server-8284-22A-SN10EE85P -r lpar -F lpar_name
p18v01
p18v02
p18lnx01
```

4. Check the version of Linux in VM p18lnx02, as shown in Example 11-7. Verify that the version is supported, as shown in Table 3-1 on page 44.

Example 11-7 Checking the Linux version on VM p18lnx02

```
p18lnx02:/etc # cd ..
p18lnx02:/ # cat /etc/os-release
NAME="SLES"
VERSION="15"
VERSION_ID="15"
```

```
PRETTY_NAME="SUSE Linux Enterprise Server 15"
ID="sles"
ID_LIKE="suse"
ANSI_COLOR="0;32"
CPE_NAME="cpe:/o:suse:sles:15"
```

5. Simulate a Linux kernel crash, as shown in Example 11-8.

Example 11-8 Simulating a Linux crash

```
p18lnx02:/ # sh -x system_crash.sh
kernel.panic=0
+ echo c
sysrq: SysRq : Trigger a crash
Oops: Kernel access of bad area, sig: 11 [#1]
SMP NR_CPUS=2048
NUMA
pSeries
.
.
.
Kernel panic - not syncing: Fatal exception
---[ end Kernel panic - not syncing: Fatal exception
```

On HMC1, p18vhmc1, p18lnx02 changed the reference code, as shown in Example 11-9.

Example 11-9 VM p18lnx02 reference code after a Linux kernel crash

```
p18lnx02:B200A101 LP=00009
```

Example 11-10 shows that in HMC 2, p18vhmc2, VM p18lnx02 restarted.

Example 11-10 VM p18lnx02 initializing on Server-8284-22A-SN10EE85P

```
p18lnx02:CA00E140
```

6. Monitor the KSYS to see the VM restart of p18lnx02, as shown in Example 11-11.

Example 11-11 Monitoring the VM restart

```
p18ksys:/ # ksysmgr query system status monitor=yes
Host_group HG_TCHU is in Ready state
Press Q to quit monitoring for activity
Restart in progress for Host_group HG_TCHU
        Stopping HA monitoring for VM p18lnx02
        HA monitoring for VM p18lnx02 stopped
        Shutdown has started for VM p18lnx02
        Shutdown has completed for VM p18lnx02
        Restart has started for VM p18lnx02
        Starting HA monitoring for VM p18lnx02
        HA monitoring for VM p18lnx02 started
Restart on Target host Server-8284-22A-SN10EE85P has completed for VM p18lnx02
```

7. Check the status of VM p18lnx02 on host Server-8284-22A-SN10EE85P, as shown in Example 11-12.

Example 11-12 Listing VMs on host Server-8284-22A-SN10EE85P

```
hscroot@p18vhmc2:~> lsrefcode -m Server-8284-22A-SN10EE85P -r lpar -F lpar_name
p18v01
p18v02
p18lnx01
p18lnx02
```

After the final restart of VM p18lnx02, the reference on host Server-8284-22A-SN101ADFDR is cleared, as shown in Example 11-13.

Example 11-13 Listing VMs on host Server-8284-22A-SN101AFDR

```
scroot@p18vhmc1:~> lsrefcode -m  Server-8284-22A-SN101AFDR -r lpar -F lpar_name
p18v03
p18ibmi01
p18v04
p18aix02
p18aix03
p18aix04
p18aix05
```

8. Check the status of VM p18lnx02 by running the **ksysmgr** command, as shown in Example 11-14.

Example 11-14 Listing VM p18lnx02

```
p18ksys:/ # ksysmgr query vm p18lnx02
Name:                p18lnx02
UUID:                495778C3-80DB-4FE3-989D-E38C905450E8
State:               READY
Host:                Server-8284-22A-SN10EE85P
Priority:            High
VM_failure_detection_speed:    fast
HA_monitor:          enable
Homehost:            Server-8284-22A-SN10EE85P
VM_status:           NO_OPERATION_IN_PROGRESS
Version_conflict:    No

LPM Validation Status
LPM validation was successful for Hosts:
        Server-8284-22A-SN10EE85P
```

11.1.3 AIX VM failures

This scenario simulates an AIX VM failure when managed by VMRM HA.

Complete the following steps:

1. Find where the test VM is allocated before initiating the AIX VM failure. Example 11-15 shows that VM p18aix02 is on source host Server-8284-22A-SN101AFDR.

Example 11-15 Listing VM p18aix02

```
p18ksys:/ # ksysmgr query vm  p18aix02
Name:                p18aix02
UUID:                52138D9D-034C-4114-AA45-4E2DA66D8761
State:               VERIFY
Host:                Server-8284-22A-SN101AFDR
Priority:            Medium
VM_failure_detection_speed:    normal
HA_monitor:          enable
Homehost:            Server-8284-22A-SN10EE85P
VM_status:           NO_OPERATION_IN_PROGRESS
Version_conflict:
```

2. List all VMs that are allocated on source host Server-8284-22A-SN101AFDR, as shown in Example 11-16.

Example 11-16 Listing VMs that are allocated on host Server-8284-22A-SN101AFDR

```
hscroot@p18vhmc1:~> lsrefcode -m  Server-8284-22A-SN101AFDR -r lpar -F lpar_name
p18v03
p18ibmi01
p18v04
p18aix02
p18aix03
p18aix04
p18aix05
```

3. List all VMs that are allocated on target host Server-8284-22A-SN10EE85P, as shown in Example 11-17.

Example 11-17 Listing VMs that are allocated on host Server-8284-22A-SN10EE85P

```
hscroot@p18vhmc2:~> lsrefcode -m Server-8284-22A-SN10EE85P -r lpar -F lpar_name
p18v01:
p18v02:
p18lnx01:Linux ppc64le
p18lnx02:Linux ppc64le
```

4. Check the version of AIX in VM p18aix02, as shown in Example 11-18. Verify that the version is supported, as shown in Table 3-1 on page 44.

Example 11-18 Checking the AIX version on VM p18aix02

```
p18aix02:/ # oslevel -s
7200-03-02-1846
```

5. Simulate the AIX kernel crash, as shown in Example 11-19.

Example 11-19 Simulating an AIX kernel crash

```
p18aix02:/vm_crash # sh -x aix_crash.sh
+ + hostname -s
shost=p18aix02
+ PS1=p18aix02:$PWD #
+ alias __A=
+ alias __B=
+ alias __C=
+ alias __D=
+ alias __H=
.
.
.
+ ./crash_vm -c
Crash ..
Uhh.. I am crashing
crash
Illegal Trap Instruction Interrupt in Kernel
.panic_trap+000000             tweq    r14,r14             r14=0000000000000002
KDB(0)> PuTTY
```

On HMC1, p18vhmc1, VM p18aix02 changed the reference code, as shown in Example 11-20.

Example 11-20 VM p18aix02 reference code after a kernel crash

```
p18aix02:0c20
```

On HMC 2, p18vhmc2, VM p18aix02 restarted, as shown in Example 11-21.

Example 11-21 VM p18aix02 initializing on Server-8284-22A-SN10EE85P

```
p18aix02:CA00E140
```

6. Monitor the KSYS to see the restart of VM p18aix02, as shown in Example 11-22.

Example 11-22 Monitoring the VM restart

```
p18ksys:/ # ksysmgr query system status monitor=yes
Host_group HG_TCHU is in Ready state
Press Q to quit monitoring for activity
Restart in progress for Host_group HG_TCHU
        Stopping HA monitoring for VM p18aix02
        HA monitoring for VM p18aix02 stopped
        Shutdown has started for VM p18aix02
        Shutdown has completed for VM p18aix02
        Restart has started for VM p18aix02
        Starting HA monitoring for VM p18aix02
        HA monitoring for VM p18aix02 started
        Restart on Target host Server-8284-22A-SN10EE85P has completed for VM p18aix02
        Configuration cleanup started for VM p18aix02
        VM monitoring for VM p18aix02 started
        Configuration cleanup completed for VM p18aix02
1 out of 1 VM have been successfully restarted
```

After the final restart of VM p18aix02, the reference code on host Server-8284-22A-SN101ADFDR is cleared, as shown in Example 11-23.

Example 11-23 Listing the VMs on host Server-8284-22A-SN101AFDR

```
scroot@p18vhmc1:~> lsrefcode -m  Server-8284-22A-SN101AFDR -r lpar -F lpar_name
p18v03
p18ibmi01
p18v04
p18aix03
p18aix04
p18aix05
```

7. Check the target, and in this case also the home host, of VM p18aix02, as shown in Example 11-24.

Example 11-24 Listing VMs on host Server-8284-22A-SN10EE85P

```
scroot@p18vhmc2:~> lsrefcode -m Server-8284-22A-SN10EE85P -r lpar -F lpar_name
p18v01:
p18v02:
p18aix02:
p18lnx01:Linux ppc64le
p18lnx02:Linux ppc64le
```

8. Check the host of VM p18aix02 by running the **ksysmgr** command, as shown in Example 11-25.

Example 11-25 Listing VM p18aix02

```
p18ksys:/ #  ksysmgr query vm  p18aix02
Name:                    p18aix02
UUID:                    52138D9D-034C-4114-AA45-4E2DA66D8761
State:                   READY_TO_MOVE
Host:                    Server-8284-22A-SN10EE85P
Priority:                Medium
VM_failure_detection_speed:    normal
HA_monitor:              enable
Homehost:                Server-8284-22A-SN10EE85P
VM_status:               NO_OPERATION_IN_PROGRESS
Version_conflict:        No

LPM Validation Status
LPM validation was successful for Hosts:
        Server-8284-22A-SN10EE85P
```

11.1.4 Host or CPC failure

This scenario simulates a host crash of host Server-8284-22A-SN101AFDR.

Complete the following steps:

1. List the VMs that are available on host Server-8284-22A-SN101AFDR, as shown in Example 11-26.

Example 11-26 Listing VMs that are available on host Server-8284-22A-SN101AFDR

```
hscroot@p18vhmc1:~> lsrefcode -m  Server-8284-22A-SN101AFDR -r lpar -F
lpar_name:refcode
p18v03:
p18ibmi01:00000000
p18v04:
p18aix02:
p18aix03:
p18aix04:
p18aix05:
p18lnx02:Linux ppc64le
```

2. List the VMs that are available on target host Server-8284-22A-SN10EE85P, as shown in Example 11-27.

Example 11-27 Listing VMs that are available on host Server-8284-22A-SN10EE85P

```
hscroot@p18vhmc2:~> lsrefcode -m Server-8284-22A-SN10EE85P -r lpar -F
lpar_name:refcode
p18v01:
p18v02:
p18lnx01:Linux ppc64le
```

3. Simulate a host crash by immediately shutting down both Virtual I/O Servers (VIOSs) from source host Server-8284-22A-SN10EE85P, as shown in Example 11-28.

Example 11-28 Shutting down both VIOSs on host Server-8284-22A-SN10EE85P

```
chsyscfg    chsyspwd    chsysstate
hscroot@p18vhmc1:~> chsysstate -m Server-8284-22A-SN101AFDR -r lpar -n p18v03 -o
shutdown --immed
hscroot@p18vhmc1:~> chsysstate -m Server-8284-22A-SN101AFDR -r lpar -n p18v04 -o
shutdown --immed
```

All VMs from host Server-8284-22A-SN10EE85P have failed, as shown in Example 11-29.

Example 11-29 VMs that failed on host Server-8284-22A-SN10EE85P

```
p18ibmi01:A6040266
p18v04:00000000
p18aix02:0c20
p18aix03:CA00E175
p18aix04:CA00E175
p18aix05:CA00E175
p18lnx02:00000000
```

4. Check that all monitored VMs restarted in host Server-8284-22A-SN10EE85P by running the **ksysmgr** command, as shown in Example 11-30.

Example 11-30 VM restarting on host Server-8284-22A-SN10EE85P

```
p18ksys:/ # ksysmgr query system status monitor=yes
Host_group HG_TCHU is in Ready state
Press Q to quit monitoring for activity
Restart in progress for Host_group HG_TCHU
        Stopping HA monitoring for VM p18lnx02
        HA monitoring for VM p18lnx02 stopped
        Shutdown has started for VM p18lnx02
        Shutdown has completed for VM p18lnx02
        Restart has started for VM p18lnx02
        Starting HA monitoring for VM p18lnx02
        HA monitoring for VM p18lnx02 started
        Restart on Target host Server-8284-22A-SN10EE85P has completed for VM
p18lnx02
        Stopping HA monitoring for VM p18aix03
        Stopping HA monitoring for VM p18aix04
        HA monitoring for VM p18aix04 stopped
        Stopping HA monitoring for VM p18aix02
        HA monitoring for VM p18aix02 stopped
        Stopping HA monitoring for VM p18aix05
        Shutdown has started for VM p18ibmi01
        Starting VM monitoring for VM p18lnx02
        HA monitoring for VM p18aix03 stopped
        HA monitoring for VM p18aix05 stopped
        Shutdown has completed for VM p18ibmi01
        Restart has started for VM p18ibmi01
        Shutdown has started for VM p18aix04
        Shutdown has started for VM p18aix02
        Shutdown has started for VM p18aix05
        Shutdown has started for VM p18aix03
        Shutdown has completed for VM p18aix04
        Shutdown has completed for VM p18aix02
        Restart has started for VM p18aix04
        Restart has started for VM p18aix02
        Shutdown has completed for VM p18aix05
        Restart has started for VM p18aix05
        Starting HA monitoring for VM p18aix04
        HA monitoring for VM p18aix04 started
        Starting HA monitoring for VM p18aix02
        HA monitoring for VM p18aix02 started
        Starting HA monitoring for VM p18aix05
        HA monitoring for VM p18aix05 started
        Shutdown has completed for VM p18aix03
        Restart has started for VM p18aix03
        Starting HA monitoring for VM p18aix03
        HA monitoring for VM p18aix03 started
        Restart on Target host Server-8284-22A-SN10EE85P has completed for VM
p18ibmi01
        Configuration cleanup started for VM p18ibmi01
        ERROR: Restart has encountered an error for VM p18ibmi01 during
Configuration Cleanup
```

```
        Restart on Target host Server-8284-22A-SN10EE85P has completed for VM
p18aix02
        Restart on Target host Server-8284-22A-SN10EE85P has completed for VM
p18aix04
        Restart on Target host Server-8284-22A-SN10EE85P has completed for VM
p18aix05
        Restart on Target host Server-8284-22A-SN10EE85P has completed for VM
p18aix03
        Configuration cleanup started for VM p18aix02
        VM monitoring for VM p18aix02 started
        Configuration cleanup started for VM p18lnx02
        ERROR: Restart has encountered an error for VM p18lnx02 during
Configuration Cleanup
        ERROR: Restart has encountered an error for VM p18aix02 during
Configuration Cleanup
        Configuration cleanup started for VM p18aix04
        VM monitoring for VM p18aix04 started
        ERROR: Restart has encountered an error for VM p18aix04 during
Configuration Cleanup
        Configuration cleanup started for VM p18aix03
        Configuration cleanup started for VM p18aix05
        VM monitoring for VM p18aix03 started
        VM monitoring for VM p18aix05 started
        ERROR: Restart has encountered an error for VM p18aix03 during
Configuration Cleanup
        ERROR: Restart has encountered an error for VM p18aix05 during
Configuration Cleanup
6 out of 6 VMs have been successfully restarted
```

5. List the VMs on host Server-8284-22A-SN10EE85P. All partitions that are monitored by KSYS from the failed host Server-8284-22A-SN101AFDR restarted on host Server-8284-22A-SN10EE85P, as shown in Example 11-31.

Example 11-31 Listing VMs on host Server-8284-22A-SN10EE85P

```
hscroot@p18vhmc2:~> lsrefcode -m Server-8284-22A-SN10EE85P -r lpar -F
lpar_name:refcode
p18v01:
p18ibmi01:00000000
p18v02:
p18aix02:
p18aix03:
p18aix04:
p18aix05:
p18lnx01:Linux ppc64le
p18lnx02:Linux ppc64le
```

6. List the VMs on source host Server-8284-22A-SN101AFDR. You see that the referenced VMs are all down, as shown in Example 11-32.

Example 11-32 Listing the remaining referenced VMs

```
hscroot@p18vhmc1:~> lsrefcode -m  Server-8284-22A-SN101AFDR -r lpar -F
lpar_name:refcode
p18v03:00000000
p18ibmi01:00000000
p18v04:00000000
```

```
p18aix02:00000000
p18aix03:00000000
p18aix04:00000000
p18aix05:00000000
p18lnx02:00000000
```

7. Start the VIOS from host Server-8284-22A-SN101AFDR, as shown in Example 11-33.

Example 11-33 Starting the VIOS from host Server-8284-22A-SN101AFDR

```
hscroot@p18vhmc1:~> chsysstate -m Server-8284-22A-SN101AFDR -r lpar -n p18v03 -o
on -f default_profile
hscroot@p18vhmc1:~> chsysstate -m Server-8284-22A-SN101AFDR -r lpar -n p18v04 -o
on -f default_profile
```

8. Perform discovery and verification operations on host group `HG_TCHU`, as shown in Example 11-34.

Example 11-34 Performing discovery and verification operations on host group HG_TCHU

```
p18ksys:/ # ksysmgr discovery host_group HG_TCHU verify=yes
Running discovery on Host_group HG_TCHU, this may take few minutes...
        Existing HA trunk adapter found for VIOS p18v01
        Existing HA trunk adapter found for VIOS p18v02
        Existing HA trunk adapter found for VIOS p18v04
        Existing HA trunk adapter found for VIOS p18v03
        Preparing VIOS in Server-8284-22A-SN101AFDR for HA management
        VIOS in Server-8284-22A-SN101AFDR prepared for HA management
        Preparing VIOS in Server-8284-22A-SN10EE85P for HA management
        VIOS in Server-8284-22A-SN10EE85P prepared for HA management
        Preparing VM p18aix03 in Host Server-8284-22A-SN10EE85P for HA management
        VM p18aix03 in Host Server-8284-22A-SN10EE85P Prepared for HA management
        Preparing VM p18aix04 in Host Server-8284-22A-SN10EE85P for HA management
        VM p18aix04 in Host Server-8284-22A-SN10EE85P Prepared for HA management
        Preparing VM p18lnx02 in Host Server-8284-22A-SN10EE85P for HA management
        VM p18lnx02 in Host Server-8284-22A-SN10EE85P Prepared for HA management
        Preparing VM p18aix02 in Host Server-8284-22A-SN10EE85P for HA management
        VM p18aix02 in Host Server-8284-22A-SN10EE85P Prepared for HA management
        Preparing VM p18aix05 in Host Server-8284-22A-SN10EE85P for HA management
        VM p18aix05 in Host Server-8284-22A-SN10EE85P Prepared for HA management
        Existing first HA client adapter found for VM p18lnx02
        Existing first HA client adapter found for VM p18aix03
        Existing second HA client adapter found for VM p18aix03
        Existing first HA client adapter found for VM p18aix04
        Existing second HA client adapter found for VM p18aix04
        Existing second HA client adapter found for VM p18lnx02
        Existing first HA client adapter found for VM p18aix02
        Existing second HA client adapter found for VM p18aix02
        Existing first HA client adapter found for VM p18aix05
        Existing second HA client adapter found for VM p18aix05
        Skipping VM p18lnx02 on Host Server-8284-22A-SN10EE85P due to some other
process in progress
        Discovery has started for VM p18aix03
        Configuration information retrieval started for VM p18aix03
        Discovery has started for VM p18ibmi01
        Configuration information retrieval started for VM p18ibmi01
        Discovery has started for VM p18aix04
        Configuration information retrieval started for VM p18aix04
        Discovery has started for VM p18aix02
        Configuration information retrieval started for VM p18aix02
        Discovery has started for VM p18aix05
        Configuration information retrieval started for VM p18aix05
        Configuration information retrieval completed for VM p18aix03
        Discovery for VM p18aix03 is complete
        Configuration information retrieval completed for VM p18ibmi01
        Discovery for VM p18ibmi01 is complete
        Configuration information retrieval completed for VM p18aix04
        Discovery for VM p18aix04 is complete
        Configuration information retrieval completed for VM p18aix02
        Discovery for VM p18aix02 is complete
        Configuration information retrieval completed for VM p18aix05
        Discovery for VM p18aix05 is complete
        VM monitor state has moved to 'STARTED' for VM p18aix03
        VM monitor state has moved to 'STARTED' for VM p18aix04
        VM monitor state has moved to 'STARTED' for VM p18aix02
        VM monitor state has moved to 'STARTED' for VM p18aix05
Discovery has finished for HG_TCHU
1 managed VM has been skipped for discovery
5 out of 6 managed VMs have been successfully discovered

Host_group verification started for HG_TCHU
        p18aix03 verification has started
        p18ibmi01 verification has started
        p18aix04 verification has started
        p18lnx02 verification has started
        p18aix02 verification has started
        p18aix05 verification has started
        p18ibmi01 verification has completed
        p18lnx02 verification has completed
        p18aix05 verification has completed
        p18aix04 verification has completed
        p18aix02 verification has completed
        p18aix03 verification has completed
Verification has finished for HG_TCHU
6 out of 6 VMs have been successfully verified
```

After the discovery and verification of host group HG_TCHU, the VMs that are referenced on host Server-8284-22A-SN101AFDR are cleared, as shown in Example 11-35.

Example 11-35 Listing VMs on host Server-8284-22A-SN101AFDR post-discovery

```
hscroot@p18vhmc1:~> lsrefcode -m  Server-8284-22A-SN101AFDR -r lpar -F
lpar_name:refcode
p18v03:
p18v04:
```

11.2 Disaster recovery scenarios

This section describes the following topics:

- Environment details
- DR rehearsal
- Unplanned move and cleanup on the source system
- Moving back to the original site after it is recovered

11.2.1 Environment details

Figure 11-2 shows the environment that is used for the test scenarios for VMRM DR in this section.

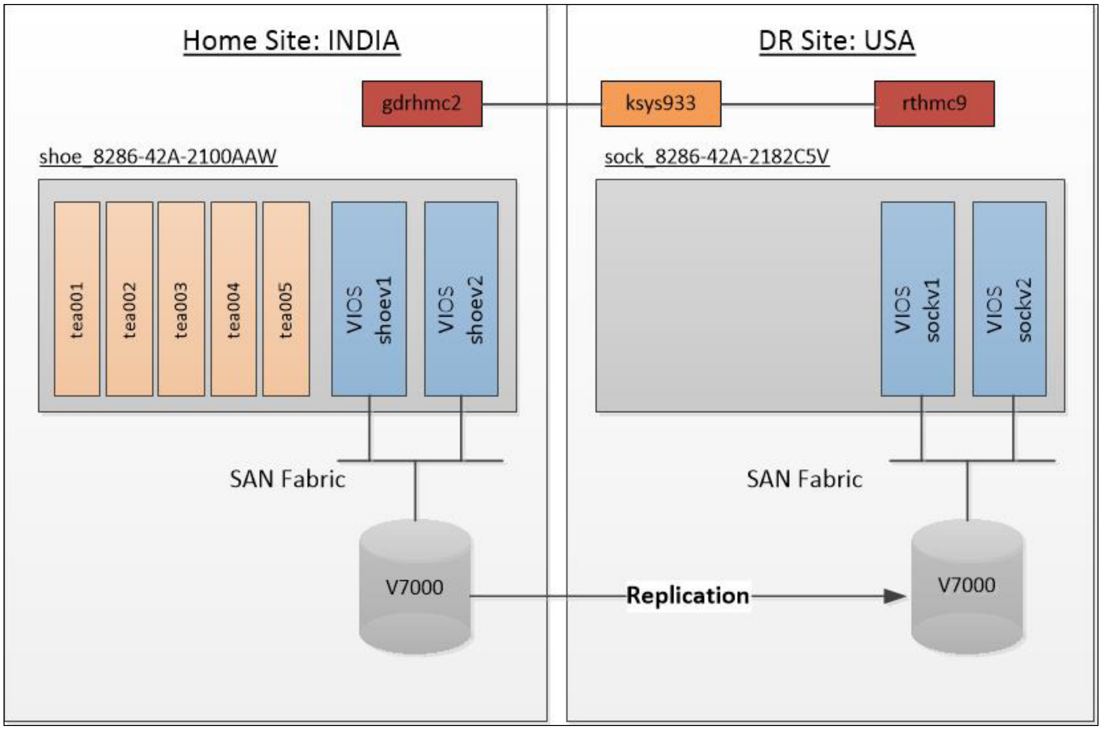


Figure 11-2 Environment that is used for the VMRM DR test scenarios

The test environment is composed of the following items:

- Two sites: USA and INDIA.
- One KSYS: ksys933, which is on the disaster recovery (DR) site.
- Two IBM Storwize V7000 Storage Systems with one on each site.
- Two HMCs: `gdrhmc2` on the home site and `rthmc9` on the DR site.
- Two IBM Power S824 servers: shoe_8286-42A-2100AAW on the home site and sock_8286-42A-2182C5V on the DR site. Each host has two VIOSs. Five VMs on the home host are managed by VMRM DR.

Here are outputs about the VMRM DR configuration for the test environment:

- Example 11-36 shows the KSYS cluster definition.

Example 11-36 query cluster

```
# ksysmgr query cluster
Name:                Redbooks
State:               Online
Type:                DR
Ksysnodes:           ksys933.ausprv.stglabs.ibm.com:1:Online
```

- Example 11-37 shows the sites that are defined in the environment.

Example 11-37 query site

```
# ksysmgr query site
Name:                USA
Sitetype:            BACKUP
Active Host_groups:  None
Active Workgroups:   None

Name:                INDIA
Sitetype:            HOME
Active Host_groups:  Default_HG, HG
Active Workgroups:   Default_WG_2, wg_tea
```

- Example 11-38 shows the HMCs.

Example 11-38 query HMC

```
# ksysmgr query hmc
Name:                rthmc9_backup
Site:                USA
Ip:                  9.xxx.xxx.xxx
Login:               hscroot

                        Managed Host List:

Hostname                               UUID
=========                               ====
sock_8286-42A-2182C5V                   9e44f545-5924-357e-adc2-5e38ea05edde
============================================================================


Name:                gdrhmc2_home
Site:                INDIA
Ip:                  9.xxx.xxx.xxx
Login:               hscroot

                        Managed Host List:

Hostname                               UUID
=========                               ====
shoe_8286-42A-2100AAW                   226c726d-ac81-343e-8d0e-fa9c59b2799b
============================================================================
```

- Example 11-39 shows the two hosts in the environment.

Example 11-39 query hosts

```
# ksysmgr query host
Name:                sock_8286-42A-2182C5V
UUID:                9e44f545-5924-357e-adc2-5e38ea05edde
FspIp:               10.xxx.xxx.xxx
Host_group:          HG
Pair:                shoe_8286-42A-2100AAW
Vswitchmap:          Not currently set
Vlanmap:             Not currently set
DrVswitchmap:        Not currently set
DrVlanmap:           Not currently set
Skip_power_on:       None
Site:                USA
VIOS:                sockv2
                     sockv1
HMCs:                rthmc9_backup
MachineSerial:       2182C5V
ProcPools:           DefaultPool

Name:                shoe_8286-42A-2100AAW
UUID:                226c726d-ac81-343e-8d0e-fa9c59b2799b
FspIp:               10.xxx.xxx.xxx
Host_group:          HG
Pair:                sock_8286-42A-2182C5V
Vswitchmap:          Not currently set
Vlanmap:             Not currently set
DrVswitchmap:        Not currently set
DrVlanmap:           Not currently set
Skip_power_on:       None
Site:                INDIA
VIOS:                shoev1
                     shoev2
HMCs:                gdrhmc2_home
MachineSerial:       2100AAW
ProcPools:           DefaultPool
```

The output that is shown in Example 11-39 tells us that these two hosts are paired and in a host group HG.

- Example 11-40 shows the host group.

Example 11-40 Host group information

```
# ksysmgr query host_group
Name:                HG
Home Site Hosts:     shoe_8286-42A-2100AAW
Backup Site Hosts:   sock_8286-42A-2182C5V
Workgroups:          Default_WG_2
                     wg_tea
Memory_capacity:     Priority-Based Settings
                     low:100
                     medium:100
                     high:100
CPU_capacity:        Priority-Based Settings
```

```
                     low:100
                     medium:100
                     high:100
Skip_power_on:       None
Sriov_override:      No
Site:                INDIA ==> Default_WG_2, wg_tea
Vswitchmap:          Not currently set
Vlanmap:             Not currently set
DrVswitchmap:        Not currently set
DrVlanmap:           Not currently set
Type:                symmetric
Custom CG Name:
Backup Site CG Name:

Name:                Default_HG
Home Site Hosts:     none
Backup Site Hosts:   none
Workgroups:          none
Memory_capacity:     Priority-Based Settings
                     low:100
                     medium:100
                     high:100
CPU_capacity:        Priority-Based Settings
                     low:100
                     medium:100
                     high:100
Skip_power_on:       None
Sriov_override:      No
Site:                INDIA
Vswitchmap:          Not currently set
Vlanmap:             Not currently set
DrVswitchmap:        Not currently set
DrVlanmap:           Not currently set
Type:                symmetric
Custom CG Name:
Backup Site CG Name:
```

There are two host groups: Default_HG and HG are defined in the environment. The host group Default_HG is the default host group and host group HG is a user-defined host group. There are no hosts in the default host group. Both hosts shoe_8286-42A-2100AAW and sock_8286-42A-2182C5V are in host group HG.

- Example 11-41 shows the workgroups that are defined in the environment.

Example 11-41 Workgroup information

```
# ksysmgr query workgroup
Name:                wg_tea
VMs:                 tea001
                     tea005
                     tea004
                     tea003
                     tea002
Host_group:          HG
Site:                INDIA
Custom CG Name:      cg_tea
Backup Site CG Name: cg_tea
```

```
Vswitchmap:         Not currently set
Vlanmap:            Not currently set
DrVswitchmap:       Not currently set
DrVlanmap:          Not currently set

Name:               Default_WG_2
Host_group:         HG
Site:               INDIA
Custom CG Name:
Backup Site CG Name:
Vswitchmap:         Not currently set
Vlanmap:            Not currently set
DrVswitchmap:       Not currently set
DrVlanmap:          Not currently set
```

There are two workgroups in the environment, and both of them are in host group HG. Workgroup Default_WG_2 is the default workgroup of this host group. There are no VMs in the default workgroup. The other workgroup that is called wg_tea is the only workgroup that contains any VMs.

- Example 11-42 shows the storage agent information.

Example 11-42 Storage agent information

```
# ksysmgr query storage_agent
Name:               sw41_backup
Serial:             10020A06150
Storagetype:        SVC
Site:               USA
Ip:                 9.xxx.xxx.xxx
Login:              admin

Name:               sw31_home
Serial:             200A08109B2
Storagetype:        SVC
Site:               INDIA
Ip:                 9.xxx.xxx.xxx
Login:              admin
```

- Example 11-43 shows the information of the managed VIOSs.

Example 11-43 Managed VIOSs

```
# ksysmgr query vios
Name:               sockv1
Site:               USA
UUID:               573BFB34-0D3B-474A-BE2B-6B310AA06970
Host:               sock_8286-42A-2182C5V
Version:            VIOS 3.1.4.00
State:              MANAGED

Name:               sockv2
Site:               USA
UUID:               79C8C918-50D8-4054-B4D4-DCCA395B699B
Host:               sock_8286-42A-2182C5V
Version:            VIOS 3.1.4.00
State:              MANAGED
```

```
Name:                shoev2
Site:                INDIA
UUID:                2F2F2012-7FFF-41CB-AC34-B5C4F7E270D6
Host:                shoe_8286-42A-2100AAW
Version:             VIOS 3.1.4.00
State:               MANAGED

Name:                shoev1
Site:                INDIA
UUID:                61D81B55-70B6-4786-A9DB-00B86F369763
Host:                shoe_8286-42A-2100AAW
Version:             VIOS 3.1.4.00
State:               MANAGED
```

- Example 11-44 shows the information about all the managed VMs.

Example 11-44 Querying managed VMs

```
# ksysmgr q vm state=manage
Managed VMs:
        tea001
        tea005
        tea004
        tea003
        tea002

All Managed VMs:
Name:                tea002
UUID:                6D76218A-3AA1-4096-A12B-542770EC00F9
State:               READY_TO_MOVE
Dr Test State:       READY_TO_DRTEST
Host:                shoe_8286-42A-2100AAW
Priority:            Medium
Skip_power_on:       None
Homehost:            shoe_8286-42A-2100AAW
DrTargetHost:        sock_8286-42A-2182C5V
Active Pool:         DefaultPool
PoolMap:             None

Name:                tea004
UUID:                68251FEB-C3F5-409A-B1A5-5BE079D88C31
State:               READY_TO_MOVE
Dr Test State:       READY_TO_DRTEST
Host:                shoe_8286-42A-2100AAW
Priority:            Medium
Skip_power_on:       None
Homehost:            shoe_8286-42A-2100AAW
DrTargetHost:        sock_8286-42A-2182C5V
Active Pool:         DefaultPool
PoolMap:             None

Name:                tea003
UUID:                6D33DC93-AB24-4573-BF41-CFB1F644D233
State:               READY_TO_MOVE
Dr Test State:       READY_TO_DRTEST
```

```
Host:                shoe_8286-42A-2100AAW
Priority:            Medium
Skip_power_on:       None
Homehost:            shoe_8286-42A-2100AAW
DrTargetHost:        sock_8286-42A-2182C5V
Active Pool:         DefaultPool
PoolMap:             None

Name:                tea001
UUID:                13FBF3CE-A560-4279-A161-0F92E13AFD76
State:               READY_TO_MOVE
Dr Test State:       READY_TO_DRTEST
Host:                shoe_8286-42A-2100AAW
Priority:            Medium
Skip_power_on:       None
Homehost:            shoe_8286-42A-2100AAW
DrTargetHost:        sock_8286-42A-2182C5V
Active Pool:         DefaultPool
PoolMap:             None

Name:                tea005
UUID:                58FB1DAC-F64A-4722-A140-68AD9B6CE5F5
State:               READY_TO_MOVE
Dr Test State:       READY_TO_DRTEST
Host:                shoe_8286-42A-2100AAW
Priority:            Medium
Skip_power_on:       None
Homehost:            shoe_8286-42A-2100AAW
DrTargetHost:        sock_8286-42A-2182C5V
Active Pool:         DefaultPool
PoolMap:             None
```

In Example 11-44 on page 312, there are five VMs that are managed by the VMRM DR environment and all of them are in the “READY_TO_MOVE” state and “READY_TO_DRTEST” DR Test state. These VMs are prepared and ready for a DR rehearsal test and to be recovered in the DR site if the production site is destroyed.

11.2.2 DR rehearsal

Every business environment has different DR test requirements. For example, some companies do a DR test yearly. One of the most usable and practical use cases of VMRM DR is that you can perform a DR test without affecting your production environment. This function of VMRM DR is called a DR rehearsal.

Before you run a DR rehearsal, run DR rehearsal discovery and verify operations. The DR rehearsal discovery operation starts a clone copy of the replicated storage and the DR rehearsal verify operation checks whether the clone copy for DR rehearsal move is ready. If not, the DR rehearsal verify operation fails. If the verify operation fails, the usual cause is that you wait for the storage clone copy to complete before performing the DR rehearsal verify operation again until the verify operation is successful.

The DR rehearsal operation can be performed on one of three levels: *site*, *host group*, and *workgroup*. Because there is only one workgroup in our environment, which contains all the managed VMs, running the DR rehearsal operations at any of the three levels yields the same result. We perform the operations on the workgroup level, which is the most common scenario.

Before performing DR rehearsal operations, configure the VMRM DR environment, which means that the KSYS discovery and verify operations successfully run; the VMs are in the “READY_TO_MOVE” state; and the clone copy of the replicated storage is created.

To perform a DR rehearsal, complete the following steps:

1. Run KSYS discovery with `dr_test=yes`, as shown in Example 11-45.

Example 11-45 Discovery operation for DR test

```
# ksysmgr discovery workgroup wg_tea dr_test=yes
15:21:54  Running dr_test discovery on Workgroup wg_tea, this may take a few
minutes...
15:22:11  Storage state synchronization has started for Workgroup wg_tea
15:22:11  Storage state synchronization has completed for Workgroup wg_tea
15:22:26  Discovery has started for VM tea001
15:22:26  Configuration information retrieval started for VM tea001
15:22:26  Discovery has started for VM tea005
15:22:26  Configuration information retrieval started for VM tea005
15:22:26  Discovery has started for VM tea004
15:22:26  Configuration information retrieval started for VM tea004
15:22:26  Discovery has started for VM tea003
15:22:26  Configuration information retrieval started for VM tea003
15:22:26  Discovery has started for VM tea002
15:22:26  Configuration information retrieval started for VM tea002
15:22:32  Configuration information retrieval completed for VM tea001
15:22:32  Configuration information retrieval completed for VM tea005
15:22:32  Configuration information retrieval completed for VM tea004
15:22:32  Configuration information retrieval completed for VM tea003
15:22:32  Configuration information retrieval completed for VM tea002
15:22:32  Storage information retrieval from VIOS started for VM tea001
15:22:32  Storage information retrieval from VIOS started for VM tea005
15:22:32  Storage information retrieval from VIOS started for VM tea004
15:22:32  Storage information retrieval from VIOS started for VM tea003
15:22:32  Storage information retrieval from VIOS started for VM tea002
15:22:32  Storage information retrieval from VIOS completed for VM tea001
15:22:32  Discovery for VM tea001 is complete
15:22:32  Storage information retrieval from VIOS completed for VM tea005
15:22:32  Discovery for VM tea005 is complete
15:22:32  Storage information retrieval from VIOS completed for VM tea003
15:22:32  Discovery for VM tea003 is complete
15:22:32  Storage information retrieval from VIOS completed for VM tea002
15:22:32  Discovery for VM tea002 is complete
15:22:37  Storage information retrieval from VIOS completed for VM tea004
15:22:37  Discovery for VM tea004 is complete
15:22:48  Disk Group creation on storage subsystem started for Workgroup wg_tea
15:23:08  Disk Group creation on storage subsystem completed for Workgroup wg_tea
15:23:17  Dr_test Discovery has finished for wg_tea
5 out of 5 managed VMs have been successfully discovered
Dr_test setup for Workgroup wg_tea is successful
```

2. Run KSYS verify with `dr_test=yes`, as shown in Example 11-46.

Example 11-46 Verifying workgroups for DR test

```
# ksysmgr verify workgroup wg_tea dr_test=yes
15:53:01 Workgroup dr_test verification started for wg_tea
15:53:10  Disk Group verification on storage subsystem started for Workgroup
wg_tea
15:53:10  Disk Group verification on storage subsystem completed for Workgroup
wg_tea
15:53:10  dr_test Verification has finished for wg_tea
5 out of 5 VMs have been successfully verified.
```

3. Both KSYS discovery and verify operations for DR rehearsal are successful. Start the DR rehearsal move by running the command that is shown in Example 11-47. The site name for the DR site is USA (home site is INDIA).

Example 11-47 DR rehearsal move

```
# ksysmgr move wg wg_tea to=USA dr_test=yes
You have not setup DR test related VLANs/vSwitches to isolate network.
Have you isolated network in a different way and want to bring up DR test VMs
[y|n]
```

The warning is important. It reminds us to check whether we defined virtual LAN (VLAN) or vSwitch mapping to isolate the network. There might be network address conflict between the VMs that are created on the DR site for DR testing and the production VMs on the production site. If the network is stretched between the production and DR site, this conflict might impact the applications on the production site.

4. In our testing environment, the network is stretched. Therefore, we define VLAN, vSwitch, or both mappings, as shown in Example 11-48.

Example 11-48 Modifying the network connectivity

```
# ksysmgr modify wg wg_tea network=vswitchmap sites=INDIA,USA INDIA=ETHERNET0
USA=SWDRTEST dr_test=yes

For Workgroup wg_tea attributes 'network' was successfully modified.
DR test vSwitch table has been successfully modified. Consider running the
discovery and verify operations

# ksysmgr modify wg wg_tea network=vlanmap sites=INDIA,USA INDIA=1 USA=101
dr_test=yes
For Workgroup wg_tea attributes 'network' was successfully modified.
DR test VLAN table has been successfully modified. Consider running the discovery
and verify operations

# ksysmgr q wg wg_tea
Name:                wg_tea
VMs:                 tea001
                     tea005
                     tea004
                     tea003
                     tea002
Host_group:          HG
Site:                INDIA
Custom CG Name:      cg_tea
```

```
Backup Site CG Name: cg_tea
Vswitchmap:          Not currently set
Vlanmap:             Not currently set
DrVswitchmap:        [home/backup] ETHERNET0/SWDRTEST
DrVlanmap:           [home/backup] 1/101
```

Note: To remove a VLAN or vSwitch mapping, use the `policy=delete` option:

```
ksysmgr modify wg wg_tea network=vswitchmap sites=INDIA,USA INDIA=ETHERNET0
USA=SWDRTEST policy=delete dr_test=yes
```

5. Run the KSYS discovery and verify operations after the VLAN and vSwitch mapping changes are done, as shown in Example 11-49.

Example 11-49 Discovery command on a workgroup after the changes

```
#  ksysmgr discovery workgroup wg_tea dr_test=yes
18:27:58  Running dr_test discovery on Workgroup wg_tea, this may take a few
minutes...
18:28:15  Storage state synchronization has started for Workgroup wg_tea
18:28:15  Storage state synchronization has completed for Workgroup wg_tea
18:28:25  Discovery has started for VM tea001
18:28:25  Configuration information retrieval started for VM tea001
18:28:25  Discovery has started for VM tea005
18:28:25  Configuration information retrieval started for VM tea005
18:28:25  Discovery has started for VM tea004
18:28:25  Configuration information retrieval started for VM tea004
18:28:25  Discovery has started for VM tea003
18:28:25  Configuration information retrieval started for VM tea003
18:28:25  Discovery has started for VM tea002
18:28:25  Configuration information retrieval started for VM tea002
18:28:36  Configuration information retrieval completed for VM tea001
18:28:36  Configuration information retrieval completed for VM tea005
18:28:36  Configuration information retrieval completed for VM tea004
18:28:36  Configuration information retrieval completed for VM tea003
18:28:36  Configuration information retrieval completed for VM tea002
18:28:36  Storage information retrieval from VIOS started for VM tea001
18:28:36  Storage information retrieval from VIOS started for VM tea005
18:28:36  Storage information retrieval from VIOS started for VM tea004
18:28:36  Storage information retrieval from VIOS started for VM tea003
18:28:36  Storage information retrieval from VIOS started for VM tea002
18:28:36  Storage information retrieval from VIOS completed for VM tea001
18:28:36  Discovery for VM tea001 is complete
18:28:36  Storage information retrieval from VIOS completed for VM tea005
18:28:36  Discovery for VM tea005 is complete
18:28:36  Storage information retrieval from VIOS completed for VM tea004
18:28:36  Discovery for VM tea004 is complete
18:28:36  Storage information retrieval from VIOS completed for VM tea003
18:28:36  Discovery for VM tea003 is complete
18:28:36  Storage information retrieval from VIOS completed for VM tea002
18:28:36  Discovery for VM tea002 is complete
18:28:51  Disk Group creation on storage subsystem started for Workgroup wg_tea
18:29:11  Disk Group creation on storage subsystem completed for Workgroup wg_tea
18:29:21  Dr_test Discovery has finished for wg_tea
5 out of 5 managed VMs have been successfully discovered
Dr_test setup for Workgroup wg_tea is successful
```

```
#  ksysmgr verify workgroup wg_tea dr_test=yes
18:30:16 Workgroup dr_test verification started for wg_tea
18:30:25  Disk Group verification on storage subsystem started for Workgroup
wg_tea
18:30:25  Disk Group verification on storage subsystem completed for Workgroup
wg_tea
18:30:25  dr_test Verification has finished for wg_tea
5 out of 5 VMs have been successfully verified
```

6. Run the DR rehearsal move command. During the DR rehearsal move, as shown in Example 11-50, you can use the HMC GUI on the DR site to verify that the DR test VMs are being created.

Example 11-50   DR rehearsal move command after the changes

```
# ksysmgr move wg wg_tea to=USA dr_test=yes
You have not setup DR test related VLANs/vSwitches to isolate network.
Have you isolated network in a different way and want to bring up DR test VMs
[y|n]
y
19:39:19 Workgroup dr_test verification started for wg_tea
19:39:33 Workgroup dr_test verification finished for wg_tea
19:39:37 Workgroup dr_test move started for wg_tea to USA, this may take a few
minutes...
19:40:55  Restart on USA Site has started for VM tea001
19:40:55  Restart on USA Site has started for VM tea005
19:40:55  Restart on USA Site has started for VM tea004
19:40:55  Restart on USA Site has started for VM tea003
19:40:55  Restart on USA Site has started for VM tea002
19:41:33  Restart on USA Site has completed for VM tea003
19:41:33  Move has completed for VM tea003
19:41:57  Restart on USA Site has completed for VM tea005
19:41:57  Move has completed for VM tea005
19:42:07  Restart on USA Site has completed for VM tea004
19:42:07  Move has completed for VM tea004
19:42:26  Restart on USA Site has completed for VM tea002
19:42:26  Move has completed for VM tea002
19:43:24  Restart on USA Site has completed for VM tea001
19:43:24  Move has completed for VM tea001
Workgroup dr_test move completed for Workgroup wg_tea to USA
5 out of 5 VMs have been successfully moved for wg_tea to USA
```

The VMs for the DR test are on the DR site with the cloned disks. Figure 11-3 shows the GUI display from the HMC on the DR site before the DR rehearsal move was issued. It has only one logical partition (LPAR), which is called `dummy_test`. The LPAR already was there.

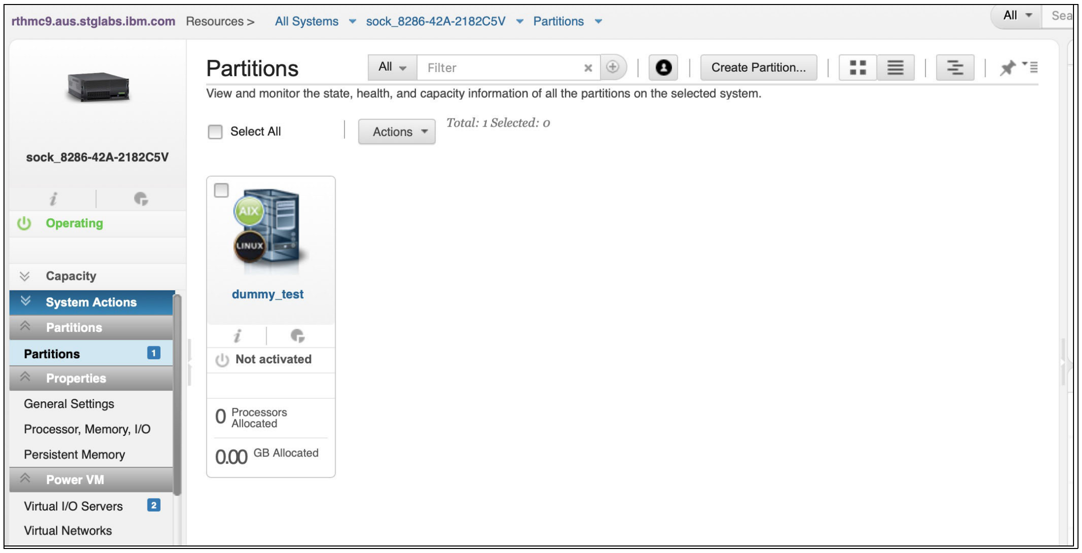


Figure 11-3 HMC on the DR site before the DR rehearsal move

Figure 11-4 shows the GUI display from the HMC on the DR site after the DR rehearsal move was issued. The five LPARs (VMs) for DR test are there. They are using the clone copy of the replicated storage on the DR site. The OS is running on these LPARs. The DR test operations can be started.

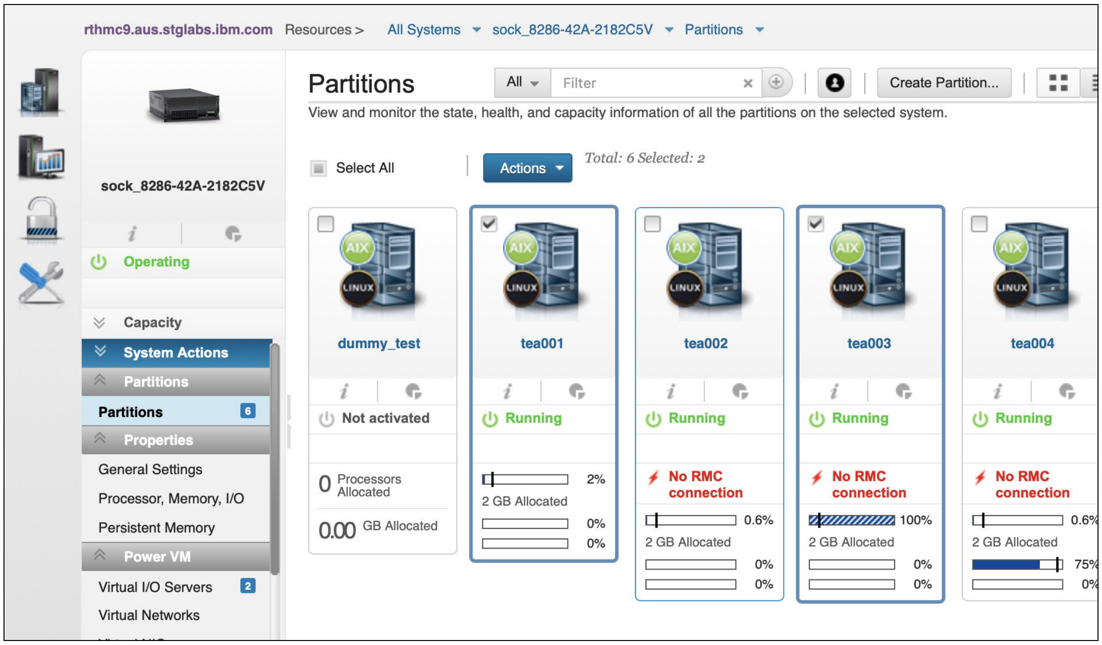


Figure 11-4 HMC on the DR site after the DR rehearsal move

After the DR test tasks complete, run a cleanup to remove the VMs on the DR site that were created by the DR rehearsal process. The cleanup also resets the logical unit number (LUN) masking so that the replicated storage (not the clone copy of the replicated storage) is mapped to the worldwide port numbers (WWPNs) of the VMs.

To do a cleanup, complete the following steps:

1. Perform a cleanup as shown in Example 11-51.

Example 11-51 Cleanup after a DR test

```
# ksysmgr cleanup wg wg_tea dr_test=yes
20:10:45  Cleanup started for wg_tea
20:10:45  Shutdown on sock_8286-42A-2182C5V Host has started for VM tea001
20:10:45  Shutdown on sock_8286-42A-2182C5V Host has completed for VM tea001
20:10:45  Configuration cleanup started for VM tea001
20:10:46  Shutdown on sock_8286-42A-2182C5V Host has started for VM tea005
20:10:46  Shutdown on sock_8286-42A-2182C5V Host has started for VM tea004
20:10:46  Shutdown on sock_8286-42A-2182C5V Host has started for VM tea003
20:10:46  Shutdown on sock_8286-42A-2182C5V Host has started for VM tea002
20:10:51  Shutdown on sock_8286-42A-2182C5V Host has completed for VM tea005
20:10:51  Configuration cleanup started for VM tea005
20:10:51  Shutdown on sock_8286-42A-2182C5V Host has completed for VM tea004
20:10:51  Configuration cleanup started for VM tea004
20:10:51  Shutdown on sock_8286-42A-2182C5V Host has completed for VM tea003
20:10:51  Configuration cleanup started for VM tea003
20:10:51  Shutdown on sock_8286-42A-2182C5V Host has completed for VM tea002
20:10:51  Configuration cleanup started for VM tea002
20:11:10  Configuration cleanup completed for VM tea001
20:11:15  Configuration cleanup completed for VM tea004
20:11:24  Configuration cleanup completed for VM tea005
20:11:25  Configuration cleanup completed for VM tea002
20:11:39  Storage level configuration cleanup started for wg_tea
20:11:39  Configuration cleanup completed for VM tea003
20:12:07  Storage level configuration cleanup completed for wg_tea
20:12:07  Cleanup completed for wg_tea
```

   All the VMs for DR test are removed, and the storage mappings are reset back as before the DR rehearsal discovery. The DR Test State of the VMs is `RECOVERY_DRTEST_CLEANVM`. The HMC GUI on the DR site returns back with only the one LPAR, as shown in Figure 11-3 on page 318.

2. Check the state of the managed VMs, as shown in Example 11-52.

Example 11-52 Querying the VMs after DR cleanup

```
# ksysmgr q vm state=manage
Managed VMs:
        tea001
        tea005
        tea004
        tea003
        tea002

All Managed VMs:
Name:                 tea002
UUID:                 6D76218A-3AA1-4096-A12B-542770EC00F9
State:                READY_TO_MOVE
Dr Test State:        RECOVERY_DRTEST_CLEANVM
Host:                 shoe_8286-42A-2100AAW
Priority:             Medium
Skip_power_on:        None
Homehost:             shoe_8286-42A-2100AAW
```

```
DrTargetHost:        sock_8286-42A-2182C5V
Active Pool:         DefaultPool
PoolMap:             None

Name:                tea004
UUID:                68251FEB-C3F5-409A-B1A5-5BE079D88C31
State:               READY_TO_MOVE
Dr Test State:       RECOVERY_DRTEST_CLEANVM
Host:                shoe_8286-42A-2100AAW
Priority:            Medium
Skip_power_on:       None
Homehost:            shoe_8286-42A-2100AAW
DrTargetHost:        sock_8286-42A-2182C5V
Active Pool:         DefaultPool
PoolMap:             None

Name:                tea003
UUID:                6D33DC93-AB24-4573-BF41-CFB1F644D233
State:               READY_TO_MOVE
Dr Test State:       RECOVERY_DRTEST_CLEANVM
Host:                shoe_8286-42A-2100AAW
Priority:            Medium
Skip_power_on:       None
Homehost:            shoe_8286-42A-2100AAW
DrTargetHost:        sock_8286-42A-2182C5V
Active Pool:         DefaultPool
PoolMap:             None

Name:                tea001
UUID:                13FBF3CE-A560-4279-A161-0F92E13AFD76
State:               READY_TO_MOVE
Dr Test State:       RECOVERY_DRTEST_CLEANVM
Host:                shoe_8286-42A-2100AAW
Priority:            Medium
Skip_power_on:       None
Homehost:            shoe_8286-42A-2100AAW
DrTargetHost:        sock_8286-42A-2182C5V
Active Pool:         DefaultPool
PoolMap:             None

Name:                tea005
UUID:                58FB1DAC-F64A-4722-A140-68AD9B6CE5F5
State:               READY_TO_MOVE
Dr Test State:       RECOVERY_DRTEST_CLEANVM
Host:                shoe_8286-42A-2100AAW
Priority:            Medium
Skip_power_on:       None
Homehost:            shoe_8286-42A-2100AAW
DrTargetHost:        sock_8286-42A-2182C5V
Active Pool:         DefaultPool
PoolMap:             None
```

11.2.3 Unplanned move and cleanup on the source system

To simulate a disaster situation, turn off the host (managed system) on the production site without first gracefully shutting down the VMs.

To recover the VMRM DR-managed VMs, complete the following steps:

1. Verify the disk replication pairs, as shown in Example 11-53.

Example 11-53 Verifying the disk replication pairs

```
# ksysmgr query disk_pair
Storage: sw31_home (INDIA)       <->     Storage: sw41_backup (USA)
=====================================================================
6005076802820426C80000000000019D <-> 600507640081018540000000000017CD
6005076802820426C80000000000019E <-> 600507640081018540000000000017CE
6005076802820426C80000000000019F <-> 600507640081018540000000000017CF
6005076802820426C8000000000001A0 <-> 600507640081018540000000000017D0
6005076802820426C8000000000001A1 <-> 600507640081018540000000000017D1
6005076802820426C8000000000001A4 <-> 600507640081018540000000000017E7
6005076802820426C8000000000001DE <-> 600507640081018540000000000017D5
6005076802820426C8000000000001DF <-> 600507640081018540000000000017D6
6005076802820426C8000000000001E0 <-> 600507640081018540000000000017D7
6005076802820426C8000000000001E1 <-> 600507640081018540000000000017D8
6005076802820426C8000000000001E2 <-> 600507640081018540000000000017D9
6005076802820426C8000000000001F3 <-> 600507640081018540000000000017E5

Tertiary Disks:
Source disk                      ->                   Tertiary disk
====================================================================
600507640081018540000000000017CD ->600507640081018540000000000017DF
600507640081018540000000000017CE ->600507640081018540000000000017E0
600507640081018540000000000017CF ->600507640081018540000000000017E1
600507640081018540000000000017D0 ->600507640081018540000000000017E2
600507640081018540000000000017D1 ->600507640081018540000000000017E3
600507640081018540000000000017D5 ->600507640081018540000000000017DA
600507640081018540000000000017D6 ->600507640081018540000000000017DB
600507640081018540000000000017D7 ->600507640081018540000000000017DC
600507640081018540000000000017D8 ->600507640081018540000000000017DD
600507640081018540000000000017D9 ->600507640081018540000000000017DE
600507640081018540000000000017E5 ->600507640081018540000000000017E6
600507640081018540000000000017E7 ->600507640081018540000000000017E8
```

   The Tertiary copy is the clone copy, which is for DR rehearsal. For real DR situations, the Tertiary copy is not used.

2. Verify the consistent groups, as shown in Example 11-54.

Example 11-54 Querying disk groups

```
# ksysmgr query disk_group
Name:                VMRDG_redbooks_USA_4
Site:                USA
Hosts:               sock_8286-42A-2182C5V
CG:                  cg_tea
FG:                   cg_tea

Name:                VMRDG_redbooks_INDIA_4
```

```
Site:                   INDIA
Hosts:                  shoe_8286-42A-2100AAW
CG:                     cg_tea
FG:                     None
```

3. Start the VMs on the DR site.

   The command to start the LPARs on the DR site can be run at multiple levels, that is, site, host group, or workgroup (not supported in high availability and disaster recovery (HADR) and HADRHA). Examples are shown for each option in Example 11-55.

Example 11-55 Commands to move VMs to the DR site

```
ksysmgr [-f] move site
      from=<sitename>
      to=<sitename>
      [force=<true|false>]
      [dr_type=<planned|unplanned>]
      [cleanup=<yes|no>]
      [skip_shutdown=<yes|no>]

or

ksysmgr [-f] move host_group <name>
      to=<sitename>
      [force=<true|false>]
      [dr_type=<planned|unplanned>]
      [cleanup=<yes|no>]
      [skip_shutdown=<yes|no>]

or

ksysmgr [-f] move workgroup <name>
      to=<site_name>
      [force=<true|false>]
      [dr_type=<planned|unplanned>]
      [cleanup=<yes|no>]
      [skip_shutdown=<yes|no>]
```

If you do not specify the **`dr_type`** attribute, the **`ksysmgr`** command starts a planned recovery by default. The LPARs automatically restart in the backup site.

In a planned recovery, the KSYS automatically cleans up the source site from where the move was initiated. In an unplanned recovery, you must manually clean up the source site after the local site HMCs and hosts become operational again.

Note: If you specify the `cleanup=no` attribute during a planned recovery, the VMs are not cleaned up from the source site.

For unplanned move operations, you can set the **`skip_shutdown`** attribute to `yes` to indicate that the source site is not operational, so the KSYS subsystem does not attempt operations such as shutting down the VMs on the source site. Ensure that the source site is not operational before you use this attribute.

Note: If a move operation for a specific host group or workgroup fails, the state of the host group or workgroup becomes `RECOVERY_VM_ONLINE`.

In this case, you cannot start the move operation for the entire site unless the failed host group or workgroup recovered. Recover the failed host groups and workgroups in a host group before you attempt a move operation for the entire site.

You can continue to move individually the other host groups and workgroups to the backup site.

For our example, we run the command that is shown in Example 11-56.

Example 11-56 Unplanned move command at the workgroup level

```
# ksysmgr move wg wg_tea to=USA dr_type=unplanned skip_shutdown=yes
You are initiating a failover across sites
Do you want to proceed? [y|n]
y
20:47:59 Workgroup move started for wg_tea to USA, this may take a few minutes...
20:48:13  Storage mirror reversal has started
20:48:14  Mirroring will be setup for Workgroup wg_tea from USA to INDIA
20:48:14  Storage mirror reversal has completed
20:48:45  Restart on USA Site has started for VM tea001
20:48:45  Restart on USA Site has started for VM tea005
20:48:45  Restart on USA Site has started for VM tea004
20:48:45  Restart on USA Site has started for VM tea003
20:48:45  Restart on USA Site has started for VM tea002
20:49:25  Restart on USA Site has completed for VM tea001
20:49:25  Move has completed for VM tea001
20:49:25  Rediscovering configuration for VM tea001 started on USA
20:49:25  Restart on USA Site has completed for VM tea005
20:49:25  Move has completed for VM tea005
20:49:25  Rediscovering configuration for VM tea005 started on USA
20:50:06  Restart on USA Site has completed for VM tea003
20:50:06  Move has completed for VM tea003
20:50:06  Rediscovering configuration for VM tea003 started on USA
20:50:56  Restart on USA Site has completed for VM tea004
20:50:56  Move has completed for VM tea004
20:50:56  Rediscovering configuration for VM tea004 started on USA
20:51:11  Rediscovering configuration for VM tea005 has completed on USA
20:51:21  Restart on USA Site has completed for VM tea002
20:51:21  Move has completed for VM tea002
20:51:21  Rediscovering configuration for VM tea002 started on USA
20:51:52  Rediscovering configuration for VM tea001 has completed on USA
20:51:57  Rediscovering configuration for VM tea004 has completed on USA
20:51:57  Rediscovering configuration for VM tea003 has completed on USA
20:52:12  Rediscovering configuration for VM tea002 has completed on USA
Workgroup move completed for Workgroup wg_tea to USA
5 out of 5 VMs have been successfully moved for wg_tea to USA
```

The VMs are now started on the DR site and the applications can be started.

11.2.4 Moving back to the original site after it is recovered

After the original site recovers and you are preparing to move the VMs back, complete the following steps:

1. Resynchronize storage.

   For an unplanned recovery, resynchronize the storage data from the active site to the backup site. The relevant command depends on what level that the move was performed, that is, site, host group or work group. Choose the relevant command from the following commands:

   ```
   ksysmgr resync site active_site_name
   ksysmgr resync host_group active_hg_name
   ksysmgr resync workgroup active_workgroup_name
   ```

   In our example, we run the command at the workgroup level:

   ```
   # ksysmgr resync workgroup wg_tea
   Workgroup wg_tea resync has started
   Check the results on the individual storage systems
   ```

   Now, ask your storage administrator to check the storage replication status. Before moving the VMs back, make sure that the replication is in the correct state.

2. Run cleanup.

   After the IBM Power server is turned on, first start the VIOSs, and then run cleanup to remove the LPARs on the hosts. The cleanup can be on the site, host group, or workgroup level. In our example, we run the cleanup on the workgroup level, as shown in Example 11-57.

Example 11-57 Cleanup on workgroup wg_tea

```
# ksysmgr cleanup wg wg_tea
21:36:11  Configuration cleanup started for VM tea001
21:36:11  Configuration cleanup started for VM tea005
21:36:11  Configuration cleanup started for VM tea004
21:36:11  Configuration cleanup started for VM tea003
21:36:11  Configuration cleanup started for VM tea002
21:36:11  Configuration cleanup completed for VM tea002
21:36:14  Configuration cleanup completed for VM tea001
21:36:14  Configuration cleanup completed for VM tea005
21:36:24  Configuration cleanup completed for VM tea003
21:36:30  Configuration cleanup completed for VM tea004
```

3. Now that the VMs on the original production site are cleaned up, prepare the VMRM DR environment so that if a disaster occurred on the current site, we can restart the VMs on the other site or even move the VMs back to where they were before the disaster. Run another discovery and verify operation, as shown in Example 11-58.

Example 11-58 Discovery action preparing to move

```
#  ksysmgr discovery workgroup wg_tea
21:48:51  Running discovery on Workgroup wg_tea, this may take a few minutes...
21:49:09  Storage state synchronization has started for Workgroup wg_tea
21:49:09  Storage state synchronization has completed for Workgroup wg_tea
21:49:26  Discovery has started for VM tea001
21:49:26  Configuration information retrieval started for VM tea001
21:49:26  Discovery has started for VM tea005
21:49:26  Configuration information retrieval started for VM tea005
```

```
21:49:26  Discovery has started for VM tea004
21:49:26  Configuration information retrieval started for VM tea004
21:49:26  Discovery has started for VM tea003
21:49:26  Configuration information retrieval started for VM tea003
21:49:26  Discovery has started for VM tea002
21:49:26  Configuration information retrieval started for VM tea002
21:49:32  Configuration information retrieval completed for VM tea001
21:49:32  Configuration information retrieval completed for VM tea005
21:49:32  Configuration information retrieval completed for VM tea004
21:49:32  Configuration information retrieval completed for VM tea003
21:49:32  Configuration information retrieval completed for VM tea002
21:49:32  Storage information retrieval from VIOS started for VM tea001
21:49:32  Storage information retrieval from VIOS started for VM tea005
21:49:32  Storage information retrieval from VIOS started for VM tea004
21:49:32  Storage information retrieval from VIOS started for VM tea003
21:49:32  Storage information retrieval from VIOS started for VM tea002
21:49:32  Storage information retrieval from VIOS completed for VM tea001
21:49:32  Discovery for VM tea001 is complete
21:49:32  Storage information retrieval from VIOS completed for VM tea005
21:49:32  Discovery for VM tea005 is complete
21:49:32  Storage information retrieval from VIOS completed for VM tea004
21:49:32  Discovery for VM tea004 is complete
21:49:32  Storage information retrieval from VIOS completed for VM tea003
21:49:32  Discovery for VM tea003 is complete
21:49:32  Storage information retrieval from VIOS completed for VM tea002
21:49:32  Discovery for VM tea002 is complete
21:52:47  Disk Group creation on storage subsystem started for Workgroup wg_tea
21:53:03  Disk Group creation on storage subsystem completed for Workgroup wg_tea
21:53:19  Discovery has finished for wg_tea
5 out of 5 managed VMs have been successfully discovered

#  ksysmgr verify workgroup wg_tea
21:53:56 Workgroup verification started for wg_tea
21:54:33 tea001 DR verification has started
21:54:33 tea005 DR verification has started
21:54:33 tea004 DR verification has started
21:54:33 tea003 DR verification has started
21:54:33 tea002 DR verification has started
21:54:43 tea004 DR verification has completed
21:54:43 tea003 DR verification has completed
21:54:43 tea002 DR verification has completed
21:54:53 tea001 DR verification has completed
21:54:53 tea005 DR verification has completed
21:54:53  Disk Group verification on storage subsystem started for Workgroup
wg_tea
21:54:58  Disk Group verification on storage subsystem completed for Workgroup
wg_tea
21:55:09  Verification has finished for wg_tea
5 out of 5 VMs have been successfully verified
```

4. Do a final status check on the VMs, as shown in Example 11-59.

Example 11-59 Final status check on the VMs

```
# ksysmgr q vm state=manage
Managed VMs:
        tea001
        tea005
        tea004
        tea003
        tea002

All Managed VMs:
Name:                tea002
UUID:                6D76218A-3AA1-4096-A12B-542770EC00F9
State:               READY_TO_MOVE
Dr Test State:       READY
Host:                sock_8286-42A-2182C5V
Priority:            Medium
Skip_power_on:       None
Homehost:            shoe_8286-42A-2100AAW
DrTargetHost:        shoe_8286-42A-2100AAW
Active Pool:         DefaultPool
PoolMap:             None

Name:                tea004
UUID:                68251FEB-C3F5-409A-B1A5-5BE079D88C31
State:               READY_TO_MOVE
Dr Test State:       READY
Host:                sock_8286-42A-2182C5V
Priority:            Medium
Skip_power_on:       None
Homehost:            shoe_8286-42A-2100AAW
DrTargetHost:        shoe_8286-42A-2100AAW
Active Pool:         DefaultPool
PoolMap:             None

Name:                tea003
UUID:                6D33DC93-AB24-4573-BF41-CFB1F644D233
State:               READY_TO_MOVE
Dr Test State:       READY
Host:                sock_8286-42A-2182C5V
Priority:            Medium
Skip_power_on:       None
Homehost:            shoe_8286-42A-2100AAW
DrTargetHost:        shoe_8286-42A-2100AAW
Active Pool:         DefaultPool
PoolMap:             None

Name:                tea001
UUID:                13FBF3CE-A560-4279-A161-0F92E13AFD76
State:               READY_TO_MOVE
Dr Test State:       READY
Host:                sock_8286-42A-2182C5V
Priority:            Medium
Skip_power_on:       None
```

```
Homehost:           shoe_8286-42A-2100AAW
DrTargetHost:       shoe_8286-42A-2100AAW
Active Pool:        DefaultPool
PoolMap:            None

Name:               tea005
UUID:               58FB1DAC-F64A-4722-A140-68AD9B6CE5F5
State:              READY_TO_MOVE
Dr Test State:      READY
Host:               sock_8286-42A-2182C5V
Priority:           Medium
Skip_power_on:      None
Homehost:           shoe_8286-42A-2100AAW
DrTargetHost:       shoe_8286-42A-2100AAW
Active Pool:        DefaultPool
PoolMap:            None

After both discovery and verify run successfully, the other site is ready to
recover the managed VMs.
```

The VMs are in a "READY_TO_MOVE" state, which means that the other site is ready to recover the managed VMs. It also is ready if we want to move the VMs back to their original site.

5. Move the VMs back to the original site.

   To move the VMs back, perform a planned move. This move is the default move, and it is shown in Example 11-60.

Example 11-60 Moving production back to the production site

```
# ksysmgr move wg wg_tea to=INDIA
You are initiating a failover across sites
Do you want to proceed? [y|n]
y
22:00:10 Workgroup move started for wg_tea to INDIA, this may take a few
minutes...
22:00:24  Shutdown on wg_tea Workgroup has started for VM tea001
22:00:24  Shutdown on wg_tea Workgroup has started for VM tea005
22:00:24  Shutdown on wg_tea Workgroup has started for VM tea004
22:00:24  Shutdown on wg_tea Workgroup has started for VM tea003
22:00:24  Shutdown on wg_tea Workgroup has started for VM tea002
22:01:23  Shutdown on wg_tea Workgroup has completed for VM tea002
22:01:34  Shutdown on wg_tea Workgroup has completed for VM tea001
22:01:34  Shutdown on wg_tea Workgroup has completed for VM tea005
22:01:34  Shutdown on wg_tea Workgroup has completed for VM tea004
22:01:34  Shutdown on wg_tea Workgroup has completed for VM tea003
22:01:34  Storage mirror reversal has started
22:01:35  Mirroring will be setup for Workgroup wg_tea from INDIA to USA
22:01:40  Storage mirror reversal has completed
22:02:14  Restart on INDIA Site has started for VM tea001
22:02:14  Restart on INDIA Site has started for VM tea005
22:02:14  Restart on INDIA Site has started for VM tea004
22:02:14  Restart on INDIA Site has started for VM tea003
22:02:14  Restart on INDIA Site has started for VM tea002
22:03:08  Restart on INDIA Site has completed for VM tea003
22:03:08  Move has completed for VM tea003
```

```
22:03:08  Configuration cleanup started on wg_tea Workgroup for VM tea003
22:03:18  Restart on INDIA Site has completed for VM tea004
22:03:18  Move has completed for VM tea004
22:03:18  Configuration cleanup started on wg_tea Workgroup for VM tea004
22:03:28  Configuration cleanup successful on wg_tea Workgroup for VM tea003
22:03:28  Rediscovering configuration for VM tea003 started on INDIA
22:03:38  Configuration cleanup successful on wg_tea Workgroup for VM tea004
22:03:38  Rediscovering configuration for VM tea004 started on INDIA
22:03:53  Restart on INDIA Site has completed for VM tea001
22:03:53  Move has completed for VM tea001
22:03:53  Configuration cleanup started on wg_tea Workgroup for VM tea001
22:03:53  Restart on INDIA Site has completed for VM tea005
22:03:53  Move has completed for VM tea005
22:03:53  Configuration cleanup started on wg_tea Workgroup for VM tea005
22:03:53  Rediscovering configuration for VM tea004 has completed on INDIA
22:03:53  Rediscovering configuration for VM tea003 has completed on INDIA
22:04:03  Configuration cleanup successful on wg_tea Workgroup for VM tea001
22:04:03  Rediscovering configuration for VM tea001 started on INDIA
22:04:08  Configuration cleanup successful on wg_tea Workgroup for VM tea005
22:04:08  Rediscovering configuration for VM tea005 started on INDIA
22:04:33  Rediscovering configuration for VM tea001 has completed on INDIA
22:04:33  Rediscovering configuration for VM tea005 has completed on INDIA
22:04:33  Restart on INDIA Site has completed for VM tea002
22:04:33  Move has completed for VM tea002
22:04:33  Configuration cleanup started on wg_tea Workgroup for VM tea002
22:04:43  Configuration cleanup successful on wg_tea Workgroup for VM tea002
22:04:43  Rediscovering configuration for VM tea002 started on INDIA
22:04:48  Rediscovering configuration for VM tea002 has completed on INDIA
Workgroup move completed for Workgroup wg_tea to INDIA
5 out of 5 VMs have been successfully moved for wg_tea to INDIA
```

During a planned move, KSYS performs the following actions:

1. Shut down gracefully the VMs,
2. Reverse the storage replication.
3. Restart the VMs on the other site.
4. Clean up the VMs on the original site.

Another use case for a planned move is to use data center migration. If you want to migrate LPARs from one data center to another data center, put them under VMRM DR, and a planned move migrates them to the other data center. Then, remove the LPARs from the VMRM DR environment.

Note: The procedure in this section works with most VMs. However, you might encounter a situation where not all the VMs are recovered successfully. If that happens, see the following sections in IBM Virtual Machine Recovery Manager DR for Power Systems Deployment Guide:

- Recovering the failed VMs
- Moving the VMs by using the `force` option
- Moving the VMs by using other options

Abbreviations and acronyms

2DC	2-data-center
3DC	3-data-center
ACLX	Access Control Logix
AME	Application Management Engine
API	application programming interface
AppMon	application monitoring framework
AR	Application Reporting
ASCII	American Standard Code for Information Interchange
AWS	Amazon Web Services
BRO	Business Recovery Objective
CA	continuous availability
CAA	Cluster Aware AIX
CCI	Command Control Interface
CG	consistency group
CLI	command-line interface
CoD	Capacity on Demand
DR	disaster recovery
DSCLI	DS8000 Series Command-Line Interface
ESB	Enterprise Service Bus
ESS	Entitled Systems Support
FC	Fibre Channel
FFDC	first failure data capture
FW	firmware
GDPS	Geographically Dispersed Parallel Sysplex
GL	group leader
GLVM	Geographic Logical Volume Manager
GPL	GNU General Public License
HA	high availability
HADR	high availability and disaster recovery
HM	host monitor
HMC	Hardware Management Console
HORCM	Hitachi Open Remote Copy Manager
HPC	high-performance computing
HTTPS	HTTP Secure
HUR	Hitachi Universal Replicator
IBM	International Business Machines Corporation
iSCSI	internet Small Computer Systems Interface
ISDL	IBM Systems Development Labs
LCB	LPAR control blob
LDEV	logical device
LMB	logical memory block
LPAR	logical partition
LPM	Live Partition Mobility
LUN	logical unit number
LVM	Logical Volume Manager
MSP	mover service partition
MxN	M host-to-N host
NPIV	N_Port ID Virtualization
NRO	Network Recovery Objective
PLM	Partition Load Manager
REST	Representational State Transfer
RHCSA	Red Hat Certified System Administrator
RHEL	Red Hat Enterprise Linux
RMC	Resource Monitoring and Control
RPM	Red Hat Package Manager
RPO	Recovery Point Objective
RPP	resource pool provisioning
RSCT	Reliable Scalable Cluster Technology
RTO	Recovery Time Objective
SAN	storage area network
SCSI	Small Computer System Interface
SEA	Shared Ethernet Adapter
SID	storage security identifier or system identifier
SMIT	System Management Interface Tool
SMS	System Management Services
SNMP	Simple Network Management Protocol
SR-IOV	Single-Root I/O Virtualization
SRDF	Symmetrix Remote Data Facility
SRR	Simplified Remote Restart
SSP	Shared Storage Pool

SYMAPI	Symmetrix Application Program Interface
SYMCLI	Symmetrix Command-Line Interface
UUID	Universally Unique Identifier
vFC	virtual Fibre Channel
VIOS	Virtual I/O Server
VLAN	virtual LAN
VM	virtual machine
VMM	VM monitor
VMRM	Virtual Machine Recovery Manager
vNIC	Virtual Network Interface Controller
vSCSI	virtual Small Computer System Interface
VSP	Virtual Storage Platform
WWN	worldwide name
WWPN	worldwide port number
XCLI	XIV Storage System Command-Line Interface

Related publications

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

IBM Redbooks

The following IBM Redbooks publications provide additional information about the topics in this document. Some publications that are referenced in this list might be available in softcopy only.

- *High Availability and Disaster Recovery Options for IBM Power Cloud and On-Premises*, REDP-5656
- *IBM Power Systems High Availability and Disaster Recovery Updates: Planning for a Multicloud Environment*, REDP-5663
- *Implementing IBM VM Recovery Manager for IBM Power Systems*, SG24-8426

You can search for, view, download, or order these documents and other Redbooks, Redpapers, web docs, drafts, and additional materials, at the following website:

ibm.com/redbooks

Online resources

These websites are also relevant as further information sources:

- IBM Virtual Machine Recovery Manager for HA - Part 1 Concepts & Deployment (YouTube video)

  https://www.youtube.com/watch?v=a6Z4smbmo0U
- IBM Virtual Machine Recovery Manager HA for Power

  https://www.ibm.com/docs/en/vmrmha/1.7
- IBM Virtual Machine Recovery Manager HA for Power Deployment Guide

  https://www.ibm.com/docs/en/SSHQN6_1.7/pdf/ha_pdf.pdf
- IBM Virtual Machine Recovery Manager for DR (GDR) - Part 3 Advanced Features (YouTube video)

  https://www.youtube.com/watch?v=EnitHiMHdKo
- IBM Virtual Machine Recovery Manager DR for Power

  https://www.ibm.com/docs/en/vmrmdr/1.7
- IBM Virtual Machine Recovery Manager DR for Power Deployment Guide

  https://www.ibm.com/docs/en/SSHQV4_1.7/pdf/dr_pdf.pdf

- IBM Virtual Machine Recovery Manager V1.4 - Deploying a “HADR” type KSYS (YouTube video)

  https://www.youtube.com/watch?v=wAwDE915bwo
- Site-specific IP configurations in IBM Recovery Manager DR

  https://www.ibm.com/downloads/cas/LP4BPAV3

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Redbooks

IBM Virtual Machine Recovery Manager for IBM Power Cookbook

SG24-8539-00

ISBN 0738461261

(0.5” spine)
0.475”<->0.873”
250 <-> 459 pages

SG24-8539-00

ISBN 0738461261

Printed in U.S.A.