

IBM i
7.4

Availability
Implementing high availability



Note

Before using this information and the product it supports, read the information in [“Notices” on page 195.](#)

This edition applies to IBM i 7.3 (product number 5770-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

This document may contain references to Licensed Internal Code. Licensed Internal Code is Machine Code and is licensed to you under the terms of the IBM License Agreement for Machine Code.

© **Copyright International Business Machines Corporation 1998, 2019.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Implementing high availability.....	1
What's new for IBM i 7.4.....	1
PDF file for Implementing high availability.....	3
Installing IBM PowerHA SystemMirror for i licensed program.....	4
Uninstalling IBM PowerHA SystemMirror for i licensed program.....	5
Planning your high availability solution.....	5
Cluster applications.....	5
Identifying resilient applications.....	6
IBM i architecture for cluster-enabled applications.....	6
Writing a highly available cluster application.....	6
Making application programs resilient.....	7
Restarting highly available cluster applications.....	8
Calling a cluster resource group exit program.....	8
Application CRG considerations.....	9
Managing application CRG takeover of IP addresses.....	9
Example: Application cluster resource group failover actions.....	13
Example: Application exit program.....	13
Planning clusters.....	13
Hardware requirements for clusters.....	13
Software requirements for clusters.....	14
Communications requirements for clusters.....	14
Dedicate a network for clusters.....	15
Tips: Cluster communications.....	15
Performance planning for clusters.....	16
Planning multiple-release clusters.....	18
Performance planning for clusters.....	18
Planning advanced node failure detection.....	19
Hardware requirements for the advanced node failure detection.....	19
Software requirements for the advanced node failure detection.....	19
Planning checklist for clusters	20
Planning environment resiliency.....	22
Planning for a cluster administrative domain.....	23
Planning monitored resources entries (MRE).....	23
Planning data resiliency.....	23
Determine which data should be made resilient.....	24
Determine site configuration.....	24
PowerHA supported storage servers.....	25
Supported external storage communication methods.....	26
Data Storage command-line interface (DSCLI)	26
Storage Area Network (SAN) volume controller (SVC) usage.....	27
Copy Services Management (CSM) Storage Controller.....	27
Planning geographic mirroring.....	28
Hardware requirements for geographic mirroring.....	28
Software requirements for geographic mirroring.....	28
Communications requirements for geographic mirroring.....	28
Journal planning for geographic mirroring.....	29
Backup planning for geographic mirroring.....	29
Performance planning for geographic mirroring.....	30
Planning switched logical units (LUNs).....	31
Hardware requirements for switched logical units.....	32
Software requirements for switched logical units.....	32

Communications requirement for Switched logical units.....	33
Planning the FlashCopy feature.....	33
Hardware requirements for the FlashCopy feature.....	33
Software requirements for the FlashCopy feature.....	34
Communications requirements for the FlashCopy feature.....	34
Planning Metro Mirror.....	34
Hardware requirements for Metro Mirror.....	34
Software requirements for Metro Mirror.....	35
Communications requirement for Metro Mirror.....	35
Journal planning for Metro Mirror.....	36
Backup planning for Metro Mirror.....	36
Performance planning for Metro Mirror.....	36
Planning Global Mirror.....	37
Hardware requirements for Global Mirror.....	37
Software requirements for Global Mirror.....	37
Communications requirement for Global Mirror.....	38
Journal planning for Global Mirror.....	39
Backup planning for Global Mirror.....	39
Performance planning for Global Mirror.....	39
Planning for DS8000 Full System HyperSwap.....	40
Hardware requirements for DS8000 Full System HyperSwap.....	40
Software requirements for DS8000 Full System HyperSwap.....	40
Communications requirements for DS8000 Full System HyperSwap.....	40
Performance requirements for DS8000 Full System HyperSwap.....	40
Planning DS8000 HyperSwap with independent auxiliary storage pools (IASPs).....	41
Hardware requirements for DS8000 HyperSwap with independent auxiliary storage pools (IASPs).....	41
Software requirements for DS8000 HyperSwap with independent auxiliary storage pools (IASPs).....	41
Communications requirements for DS8000 HyperSwap with independent auxiliary storage pools (IASPs).....	42
Journal planning for DS8000 HyperSwap with independent auxiliary storage pools (IASPs).....	42
Backup planning for DS8000 HyperSwap with independent auxiliary storage pools (IASPs).....	42
Performance requirements for DS8000 HyperSwap with independent auxiliary storage pools (IASPs).....	43
Security planning for high availability.....	43
Distributing cluster-wide information.....	43
Considerations for using clusters with firewalls.....	43
Maintaining user profiles on all nodes.....	44
Planning for PowerHA policies.....	44
PowerHA policies for cluster administrative domain resources.....	45
The PowerHA administrative domain resource policies qualifiers and values.....	46
QCST_CRG_CANCEL_FAILOVER PowerHA policy.....	47
The PowerHA QHA_COMM_STRICT_CERT_CHECK high availability policy.....	48
Implementing PowerHA.....	48
Configuring high availability infrastructure.....	49
Setting up TCP/IP for high availability.....	50
Setting TCP/IP configuration attributes.....	50
Starting the INETD server.....	50
Configuring clusters.....	51
Creating a cluster.....	51
Specifying message queues.....	55
Performing switchovers.....	55
Configuring nodes.....	56
Starting nodes.....	57
Enabling nodes to be added to a cluster.....	57

Adding nodes	57
Adding a node to a device domain.....	58
Configuring advanced node failure detection.....	59
Configuring advanced node failure detection on hardware management console (HMC) with CIM server.....	59
Configuring advanced node failure detection on hardware management console (HMC) with REST server.....	61
Configuring advanced node failure detection in a Virtual I/O Server (VIOS) on an Integrated Virtualization Manager (IVM) managed server.....	62
Configuring Cluster Resource Groups.....	63
Starting a CRG.....	64
Creating cluster resource groups (CRGs).....	64
Configuring a Cluster Resource Group container.....	66
Create a cluster resource group (CRG) container.....	67
Scenarios: Configuring high availability.....	70
Scenario: Geographic mirroring.....	70
Scenario: Metro Mirror.....	72
Scenario: Global Mirror.....	73
Configuring cluster administrative domains.....	75
Creating a cluster administrative domain	75
Adding a node to the cluster administrative domain.....	76
Starting a cluster administrative domain.....	76
Synchronization of monitored resource.....	77
Adding monitored resource entries.....	78
Configuring independent disk pools.....	78
Creating an independent disk pool.....	78
Making an independent disk pool highly available.....	79
Configuring copy descriptions.....	79
Adding an ASP copy description.....	80
Adding a SVC copy description.....	82
Starting copy sessions.....	83
Starting an ASP session.....	84
Starting a CSM session.....	85
Starting a SVC session.....	86
Adding an high availability policy.....	87
Configuring geographic mirroring.....	88
Configuring Metro Mirror.....	89
Configuring Global Mirror.....	89
Configuring switched logical units (LUNs).....	90
Configuring a FlashCopy session.....	91
Configuring DS8000 Full System HyperSwap.....	91
Defining HyperSwap Affinity.....	92
Configuring DS8000 HyperSwap with independent auxiliary storage pools (IASPs).....	92
Configuring LUN level switching in the HyperSwap enviroment on IBM i	93
Managing PowerHA.....	94
Scenarios: Managing high availability solutions.....	94
Scenarios: Performing backups in a high-availability environment.....	94
Scenario: Performing backups in geographic mirroring environment.....	94
Scenario: Performing a FlashCopy function.....	95
Scenario: Upgrading operating system in a high-availability environment.....	96
Example: Upgrading operating system.....	97
Managing clusters.....	98
Adjusting the PowerHA version.....	99
Adjusting the cluster version of a cluster.....	100
Deleting a cluster.....	101
Displaying cluster configuration.....	101
Saving and restoring cluster configuration.....	102
Monitoring cluster status.....	102

Specifying message queues.....	103
Cluster deconfiguration checklist.....	104
Managing nodes.....	104
Displaying node properties.....	104
Stopping nodes.....	105
Removing nodes	105
Removing a node from a device domain.....	106
Add a cluster monitor to a node.....	106
Removing a cluster monitor	107
Managing cluster resource groups (CRGs).....	107
Displaying CRG status.....	107
Stopping a CRG.....	109
Deleting a CRG.....	109
Changing the recovery domain for a CRG.....	109
Managing a cluster resource group (CRG) container.....	110
Starting a cluster resource group (CRG) container.....	111
Ending a cluster resource group (CRG) container.....	111
Deleting a cluster resource group (CRG) container.....	112
Displaying a cluster resource group (CRG) container.....	113
Adding nodes and configuration objects using the Configure CRG Container command.....	114
Adding a cluster node to the recovery domain of a CRG container.....	114
Adding a CRG to a CRG container.....	115
Removing nodes and configuration objects using the Configure CRG Container command.....	115
Removing a CGR from a CRG container.....	116
Removing a cluster node from the recovery domain of a CRG container.....	116
Changing the primary node of a cluster resource group (CRG) container using the Change CRG Container (CHGCRGCNR) command.....	117
Changing the current recovery domain of a cluster resource group (CRG) container.....	117
Managing failover outage events.....	119
Managing cluster administrative domains.....	122
Displaying cluster administrative domains.....	122
Stopping a cluster administrative domain.....	123
Deleting a cluster administrative domain.....	124
Changing the properties of a cluster administrative domain.....	124
Managing monitored resource entries.....	125
Managing independent disk pools.....	146
Quiescing an independent disk pool.....	146
Resuming an independent disk pool.....	146
Managing copy descriptions.....	146
Displaying an ASP copy description.....	147
Displaying a SVC copy description.....	147
Changing an ASP copy description.....	148
Changing a SVC copy description.....	149
Removing an ASP copy description.....	149
Removing a SVC copy description.....	150
PowerHA configuration description types.....	150
Adding an HA configuration description.....	151
Displaying an HA configuration description.....	152
Changing an HA configuration description.....	153
Removing an HA configuration description.....	153
Managing PowerHA policies.....	154
Work with PowerHA policies.....	154
Displaying a PowerHA policy.....	155
Changing a PowerHA policy.....	155
Saving PowerHA policies.....	156
Restoring PowerHA policies.....	157
Removing PowerHA policies.....	158
Managing geographic mirroring.....	159

Suspending geographic mirroring.....	159
Resuming geographic mirroring.....	160
Detaching mirror copy.....	161
Reattaching mirror copy.....	162
Deconfiguring geographic mirroring	163
Changing geographic mirroring properties.....	164
Managing Metro Mirror.....	164
Suspending Metro Mirror.....	164
Resuming Metro Mirror sessions.....	165
Detaching Metro Mirror copy.....	165
Reattaching Metro Mirror.....	166
Ending Metro Mirror.....	166
Displaying or changing Metro Mirror properties.....	167
Managing Global Mirror.....	168
Suspending Global Mirror.....	168
Resuming Global Mirror.....	168
Detaching Global Mirror copy.....	169
Reattaching Global Mirror.....	169
Ending Global Mirror.....	170
Changing Global Mirror session properties.....	170
Managing switched logical units (LUNs).....	171
Making switched logical units (LUNs) available and unavailable.....	171
Managing the FlashCopy technology.....	171
Updating a FlashCopy session.....	171
Reattaching a FlashCopy session.....	172
Detaching a FlashCopy session.....	172
Deleting a FlashCopy session.....	172
Restoring data from a FlashCopy session.....	173
Changing FlashCopy properties.....	173
Managing DS8000 Full System HyperSwap.....	174
Displaying HyperSwap Status.....	174
Perform a Planned HyperSwap.....	174
Suspend HyperSwap Replication.....	174
Resume HyperSwap Replication.....	174
Recovering from an unplanned HyperSwap Failover.....	174
Managing DS8000 HyperSwap with independent auxiliary storage pools (IASPs).....	175
Displaying HyperSwap Status.....	175
HyperSwap planned switchover of SYSBAS.....	176
HyperSwap planned switchover of independent auxiliary storage pool (IASP).....	176
HyperSwap planned switchover with HyperSwap and LUN switching.....	176
CRG Planned switchover with HyperSwap and LUN switching.....	176
HyperSwap failover with HyperSwap and LUN switching.....	177
Two primary case.....	177
CRG Failover HyperSwap and LUN switching.....	177
Live partition mobility switch with HyperSwap and affinity.....	178
DS8000 HyperSwap IASP with FlashCopy.....	178
Troubleshooting your high availability solution.....	178
Troubleshooting clusters.....	178
Determine if a cluster problem exists.....	179
Gathering recovery information for a cluster.....	180
Common cluster problems.....	181
Partition errors.....	183
Determining primary and secondary cluster partitions.....	184
Changing partitioned nodes to failed.....	185
Partitioned cluster administrative domains.....	185
Tips: Cluster partitions.....	186
Cluster recovery.....	187
Recovering from cluster job failures.....	187

Recovering a damaged cluster object.....	187
Recovering a cluster after a complete system loss.....	188
Recovering a cluster after a disaster.....	188
Restoring a cluster from backup tapes.....	189
Troubleshooting geographic mirroring.....	189
Geographic mirroring messages.....	189
Troubleshooting Metro Mirror, Global Mirror, and FlashCopy.....	190
Troubleshooting HyperSwap.....	190
Related information for Implementing high availability.....	191
Notices.....	195
Programming interface information.....	196
Trademarks.....	196
Terms and conditions.....	197

Implementing high availability

For IBM® i environments, a task-based approach is used to implement high availability. The *task-based approach* allows you to design and build a customized high-availability solution for your business, using different interfaces for technologies that are related to high availability.

You are required to install the IBM PowerHA® SystemMirror® for i licensed program number (5770-HAS) on each system that is participating in high availability. The task-based approach uses the PowerHA graphical interface from which you can create and manage the cluster, cluster resource groups, cluster administrative domains, and independent ASPs. With the task-based approach, other interfaces, such as the CL commands, can also be used to manage the technologies within your solution.

Note: By using the code examples, you agree to the terms of the [Code license and disclaimer information](#).

What's new for IBM i 7.4

Read about new or changed information for the High Availability (HA) technologies topic collection.

What's New as of December 2019

PowerHA SystemMirror for i 7.4 added improvements to the administrative domain that simplify the deployment and management of high-availability environments. These are:

- Increased the cluster administrative domain monitored resource entry limit to support up to 200,000 resources entries - an increase of over 340% to support the largest environments.
- New parameters for the Work with Cluster Administrative Domain Monitored Resource Entries (**WRKCADMRE**) command enable filtering based on criteria like monitored resource, library, resource type, and global status. Filters can be combined and support generic wild cards.
- The Add Cluster Administrative Domain Monitored Resource Entry (**ADDCADMRE**) command now supports ***ALL** and wild cards on the monitored resource and library parameters. In addition, the omit parameter has been added. The new options are supported for user profiles, authorization lists, classes, job descriptions and subsystem descriptions. These simplify administrative domain setups; a single command can be used to add multiple resources at one time.

Additional enhancements to the PowerHA administrative domain include:

- PowerHA enhanced support for replication of encrypted passwords set using the QSYSUPWD API. Previously, the QSYSUPWD API caused the user-affected profile to be marked as inconsistent within the administrative domain.
- Improved control over changing the synchronization option for an administrative domain using the Change Cluster Administrative Domain (**CHGCAD**) command even when some nodes in the administrative domain are inactive.
- The Work with Cluster Administrative Domain Monitored Resource Entries (**WRKCADMRE**) command has been enhanced to work even while clustering is inactive. With this functionality, users can view monitored resources within an administrative domain on a local node even during maintenance windows.

HyperSwap in LUN-level switching environments improvements:

- Enhanced integrated recovery from a data-center outage in a HyperSwap with a LUN-level switching environment that enables HyperSwap protection to be restored using a single command.

CRG container switching improvements:

- PowerHA improved the behavior of the Change CRG Container (**CHGCRGCNR**) command ***SAMESITE** functions. It is now more consistent in handling the ordering of a recovery domain.

Copy Services Manager (CSM) functionality enhancements

Support for CSM for DS8000 Metro Mirror and Global Mirror and HyperSwap with Global Mirror sessions.

- The following commands are new for the IBM PowerHA for i Licensed Program:
 - Start Copy Services Manager (CSM) Session ([STRCSMSSN](#)) command
 - Change Copy Services Manager (CSM) Session ([CHGCSMSSN](#)) command
 - Display Copy Services Manager (CSM) Session ([DSPCSMSSN](#)) command
 - Retrieve Copy Services Manager (CSM) Session ([RTVCSMSSN](#)) command
 - End Copy Services Manager (CSM) Session ([ENDCSMSSN](#)) command
- The following commands are enhanced for the IBM PowerHA for i Licensed program:
 - Add HA Configuration Description ([ADDHACFGD](#)) command
 - Change HA Configuration Description ([CHGHACFGD](#)) command
 - Display HA Configuration Description ([DSPHACFGD](#)) command
 - Work with HA Configuration Description ([WRKHACFGD](#)) command
 - Remove HA Configuration Description ([RMVHACFGD](#)) command
- The following APIs are enhanced for the IBM PowerHA for i Licensed Program:
 - Retrieve HA Configuration Description ([QhaRetrieveConfigurationDesc](#)) API

Currently, there is no support for CSM from within the PowerHA GUI.

HyperSwap functionality enhancements

Improvements and expansion of HyperSwap functionality in PowerHA

- Integrated recovery improvements made to HyperSwap with LUN level switching components.
- HyperSwap functionality with Global Mirror for site resiliency now available via the CSM storage controller support.
- The following APIs are enhanced for the IBM PowerHA for i Licensed Program:
 - Retrieve HA Status ([QhaRetrieveStatus](#)) API

Currently, there is no support for HyperSwap with Global Mirror from within the PowerHA GUI.

High Availability (HA) cluster policies

Introducing HA policies to help PowerHA users modify the cluster behavior in their high availability environment. Policies can be classified by the section of the cluster environment they manage, for example, the Cluster Resource Group (CRG), or communications.

- The following policy commands are new for the IBM PowerHA for i Licensed Program:
 - Add High Availability (HA) Policy ([ADDHAPCY](#)) command
 - Display High Availability (HA) Policy ([DSPHAPCY](#)) command
 - Save High Availability (HA) Policy ([SAVHAPCY](#)) command
 - Change High Availability (HA) Policy ([CHGHAPCY](#)) command
 - Removing High Availability (HA) Policy ([RMVHAPCY](#)) command
 - Restore High Availability (HA) Policy ([RSTHAPCY](#)) command
- The following commands have been enhanced for the IBM PowerHA for i Licensed Program:
 - Start Cluster Administrative Domain ([STRCAD](#)) command
- The following APIs are new for the IBM PowerHA for i Licensed Program:
 - Retrieve Policy ([QhaRetrievePolicy](#)) API

- The following policies are new for the IBM PowerHA for i Licensed Program:
 - QHA_COMM_STRICT_CERT_CHECK
 - QCST_AD_CREATE
 - QCST_AD_DELETE
 - QCST_AD_RESTORE
 - QCST_CRG_CANCEL_FAILOVER

Currently, there is no support for HA policies from within the PowerHA GUI.

Automated management of the Cluster Administrative Domain (CAD)

The administrative domain HA policies, QCST_AD_CREATE, QCST_AD_DELETE, and QCST_AD_RESTORE enable users to:

- automate the addition of Modified Resource Entries (MREs) across nodes in the administrative domain.
- automate deletion of MRE entries across the nodes in the administrative domain.
- restore MREs in the administrative domain, if required.

Additional cluster management features

Two additional HA policies assist users with cluster management:



- The CRG HA policy, QCST_CRG_CANCEL_FAILOVER integrates control over the ability to cancel automatic CRG failovers.
- The communication policy, QHA_COMM_STRICT_CERT_CHECK allows users to change the default security settings between the cluster nodes and storage devices.

Additional HA enhancements

- The following APIs are new for the IBM PowerHA for i Licensed Program:
 - [Cluster Policy APIs](#)
- The following APIs are enhanced for the IBM PowerHA for i Licensed Program:
 - [Cluster Resource Group APIs](#)

How to see what's new or changed

To help you see where technical changes have been made, this information uses:


- The  image to mark where new or changed information begins.
- The  image to mark where new or changed information ends.

In PDF files, you might see revision bars (|) in the left margin of new and changed information.



To find other information about what's new or changed in this release, see the [Memo to users](#).

PDF file for Implementing high availability

You can view and print a PDF file of this information about implementing high availability.

To view or download the PDF version of this document, select [Implementing high availability](#) .

You can view or download these related topic collection PDFs:


- [High availability overview](#)  contains the following topics:
 - Benefits of high availability
 - High availability criteria
 - Components of high availability
 - IBM PowerHA SystemMirror for i overview
- [High availability technologies](#)  contains the following topics:
 - IBM i Cluster technology
 - Advanced node failure detection
 - Cluster administrative domain
 - PowerHA data replication technologies
 - High availability management
 - Resource Monitoring and Control (RMC)

Saving PDF files

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF link in your browser.
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

You need Adobe Reader installed on your system to view or print these PDFs. You can download a free copy from the [Adobe Web site](http://www.adobe.com/products/acrobat/readstep.html) (www.adobe.com/products/acrobat/readstep.html) .

Related reference

[Related information for Implementing high availability](#)

Installing IBM PowerHA SystemMirror for i licensed program

Before you can implement an IBM i high-availability solution, you must install the IBM PowerHA SystemMirror for i licensed program (5770-HAS) on each system that participates in high availability.

Before installing the IBM PowerHA SystemMirror for i licensed program, you should have completed the following installation requirements:

1. Install or upgrade to i 7.2 or i 7.3 operating system.
2. Install IBM i operating system Option 41 (HA Switchable Resources).

To install the IBM PowerHA for i licensed program, complete the following steps:

1. Enter GO LICPGM from a command line.
2. At the Work with Licensed Programs display, select option 11 (Install licensed programs).
3. Select Product 5770-HAS, option *BASE to install IBM PowerHA SystemMirror for i. Press enter.
4. At the Install Options display, type in the name of your installation device as requested. Press enter to start the installation.

5. Using asynchronous geographic mirroring, metro mirroring, global mirroring or DS8000® HyperSwap® with IASPs requires IBM PowerHA for i Enterprise Edition (option 1) be installed. Select Product 5770-HAS, option 1 to install IBM PowerHA for i Enterprise Edition. Press enter.
6. Using PowerHA graphical interface, commands, synchronous geographic mirroring, switched logical units, or FlashCopy® requires IBM PowerHA for i Standard Edition (option 2) be installed. Select Product 5770-HAS, option 2 to install IBM PowerHA for i Standard Edition. Press enter.
7. Using DS8000 Full System HyperSwap requires IBM PowerHA for i Express® Edition (option 3) be installed. Select Product 5770-HAS, option 3 to install IBM PowerHA for i Express Edition. Press enter.

After successfully installing the IBM PowerHA SystemMirror for i licensed program, you need to restart the INETD server. For information about how to start INETD, see [“Starting the INETD server” on page 50](#).

Uninstalling IBM PowerHA SystemMirror for i licensed program

If you no longer want to use interfaces or functions associated with IBM PowerHA SystemMirror for i licensed program, you need to uninstall the product.

To uninstall the IBM PowerHA SystemMirror for i licensed program, complete these steps:

1. Type `G0 LICPGM` and press enter. The Work with licensed programs menu appears.
2. Select option 12 (Delete licensed programs). The Delete licensed programs display appears.
3. Type 4 (Delete) in the Option column in front of 5770-HAS.
4. Press enter. You are shown the **Confirm Delete of Licensed Programs** display.
5. Press enter if your selections are correct. Press F12 to make corrections.
6. You receive confirmation messages from the system when the licensed programs are deleted.
7. Press F12 to return to the Work with licensed programs menu.

If you have difficulty deleting a licensed program following these steps, type **ENDSBS *ALL *IMMED** and press enter. Then proceed with step 1 again.

Planning your high availability solution

Before configuring an IBM i high-availability solution, proper planning is necessary to ensure all the requirements for the solution have been met.

Each high availability technology has minimum requirements that should be met before configuring a specific solution. In addition to these requirements, it is important to also determine which resources should be made resilient. These resources, such as applications, data, and devices, should be evaluated to determine whether they should be highly available. If they require high availability, it is important to make any necessary changes to the environment prior to configuring a solution for high availability. For example, you might have data that resides in SYSBAS, which should be highly available. Before configuring a solution, you should move that data to an independent disk pool. Applications might also require changes to enable high availability.

Cluster applications

Application resilience is one of the key elements in a clustered environment. If you are planning to write and use highly available applications in your cluster you should be aware that these applications have specific availability specifications.

By taking advantage of resilient applications in your cluster, an application can be restarted on a different cluster node without requiring you to reconfigure the clients. In addition, the data that is associated with the application will be available after switchover or failover. This means that the application user can experience minimal, or even seamless, interruption while the application and its data switch from the primary node to the backup node. The user does not need to know that the application and data have moved on the back end.

In order to achieve application resiliency in your cluster, applications that meet certain availability specifications must be used. Certain characteristics must be present in the application in order for it to be switchable, and therefore always available to the users of the application in the cluster. See [High Availability and Clusters](#) for details on these application traits. Because these requirements exist, you have the following options for using a switchable application in your cluster:

- 1. Purchase a cluster-enabled software application**

Software products that are cluster-enabled meet certain high-availability requirements.

- 2. Write or change your own application to make it highly available**

Independent software vendors and application programmers can customize applications to allow them to be switchable in a IBM i clustered environment.

Once you have a resilient application, it must be managed within your cluster.

Identifying resilient applications

Not every application will give you the availability benefits of clustering.

An application must be resilient in order to take advantage of the switchover and failover capabilities provided by clustering. Application resilience allows the application to be restarted on the backup node without having to reconfigure the clients using the application. Therefore your application must meet certain requirements to take full advantage of the capabilities offered by clustering.

IBM i architecture for cluster-enabled applications

Additional end-user value is provided by any application that is highly available, recognizing applications that continue to be available in the event of an outage, planned or unplanned.

IBM i has provided an application resilience architecture that supports various degrees of highly available application. Applications on the high end of this spectrum demonstrate highly available characteristics, provide automation of the highly available environment, and are managed through high availability management interfaces.

These applications have the following characteristics:

- The application can switch over to a backup cluster node when the primary node becomes unavailable.
- The application defines the resilient environment in the Resilient Definition and Status Data Area to enable automatic configuration and activation of the application by a cluster management application.
- The application provides application resilience by means of an application CRG exit program to handle cluster related events, taking advantage of the capabilities of the IBM i cluster resource services.
- The application provides an application restart function that repositions the user to an application menu screen or beyond.

Applications that demonstrate more stringent availability and restart characteristics have the following characteristics:

- The application provides enhanced application resilience through more robust handling of cluster events (action codes) by the application CRG exit program.
- The application provides a greater level of application restart support. For host-centric applications, the user will be repositioned to a transaction boundary by commitment control or checkpoint functions. For client-centric applications, the user will experience a seamless failover with minimal service interruption.

Writing a highly available cluster application

A highly available application is one that can be resilient to a system outage in a clustered environment.

Several levels of application availability are possible:

1. If an application error occurs, the application restarts itself on the same node and corrects any potential cause for error (such as corrupt control data). You can view the application as though it had started for the first time.
2. The application performs some amount of checkpoint-restart processing. You can view the application as if it were close to the point of failure.
3. If a system outage occurs, the application is restarted on a backup server. You can view the application as though it had started for the first time.
4. If a system outage occurs, the application is restarted on a backup server and performs some amount of checkpoint-restart processing across the servers. You can view the application as if it were close to the point of failure.
5. If a system outage occurs, a coordinated failover of both the application and its associated data to another node or nodes in the cluster occurs. You can view the application as though it had started for the first time.
6. If a system outage occurs, a coordinated failover of both the application and its associated data to another node or nodes in the cluster occurs. The application performs some amount of checkpoint-restart processing across the servers. You can view the application as if it were close to the point of failure.

Note: In cases 1 through 4 above, you are responsible for recovering the data.

Making application programs resilient

Learn how to make application programs resilient.

A resilient application is expected to have the following characteristics:

- The application can be restarted on this node or another node
- The application is accessible to the client through the IP address
- The application is stateless or state information is known
- Data that is associated with the application is available after switchover

The three essential elements that make an application resilient to system outages in a clustered environment are:

The application itself

How tolerant is the application to errors or to system outages, and how transparently can the application restart itself?

The application can handle this through the use of clustering capabilities.

Associated data

When an outage occurs, does it affect the availability of any associated data?

You can store critical data in switched disks which allow data to remain available during an outage. Alternatively, a cluster middleware IBM Business Partner replication product that takes advantage of the clustering capabilities can handle this.

Control capabilities and administration

How easy is it to define the environment that supports the availability of the data and the application?

IBM PowerHA SystemMirror for i licensed program provides several interfaces to configure and manage high-availability solutions and technology. The IBM PowerHA SystemMirror for i licensed program provides the following interfaces:

PowerHA graphical interface

Use the graphical interface to easily configure, monitor, and manage your High Availability solution. For customers that are upgrading from a release before 7.2, it combines the simplicity of the High Availability Solutions Manager graphical interface with the flexibility of the Cluster Resource Services graphical interface in a single graphical interface.

PowerHA commands

These commands provide similar functions but are available through a command-line interface.

PowerHA APIs

These PowerHA APIs allow you to work with new function for independent disk pools.

In addition, you can also use a third-party cluster management interface that uses the clustering APIs and also combines resilient applications with resilient data can handle this.

Related information

[High availability management](#)

Restarting highly available cluster applications

To restart an application, the application needs to know its state at the time of the failover or switchover.

State information is application specific; therefore, the application must determine what information is needed. Without any state information, the application can be restarted on your PC. However, you must reestablish your position within the application.

Several methods are available to save application state information for the backup system. Each application needs to determine which method works best for it.

- The application can transfer all state information to the requesting client system. When a switchover or failover occurs, the application uses the stored state on the client to reestablish the state in the new server. This can be accomplished by using the `Distribute Information API` or `Clustered Hash Table APIs`.
- The application can replicate state information (such as job information and other control structures that are associated with the application) on a real-time basis. For every change in the structures, the application sends the change over to the backup system.
- The application can store pertinent state information that is associated with it in the exit program data portion of the cluster resource group for that application. This method assumes that a small amount of state information is required. You can use the `Change Cluster Resource Group (QcstChangeClusterResourceGroup)` API to do this.
- The application can store state information in a data object that is being replicated to the backup systems along with the application's data.
- The application can store state information in a data object contained in the IASP that also contains the application's data.
- The application can store the state information about the client.
- No state information is saved, and you need to perform the recovery.

Note: The amount of information that is required to be saved is lessened if the application uses some form of checkpoint-restart processing. State information is only saved at predetermined application checkpoints. A restart takes you back to the last known checkpoint which is similar to how database's commitment control processing works.

Calling a cluster resource group exit program

The cluster resource group exit program is called during different phases of a cluster environment.

This program establishes the environment necessary resiliency for resources within a cluster. The exit program is optional for a resilient device CRG but is required for the other CRG types. When a cluster resource group exit program is used, it is called on the occurrence of cluster-wide events, including the following:

- A node leaves the cluster unexpectedly
- A node leaves the cluster as a result of calling the `End Cluster Node (QcstEndClusterNode)` API or `Remove Cluster Node Entry (QcstRemoveClusterNodeEntry)` API
- The cluster is deleted as a result of calling the `Delete Cluster (QcstDeleteCluster)` API
- A node is activated by calling the `Start Cluster Node (QcstStartClusterNode)` API
- Communication with a partitioned node is re-established

The exit program completes the following processes:

- Runs in a named activation group or the caller's activation group (*CALLER).

- Ignores the restart parameter if the exit program has an unhandled exception or is canceled.
- Provides a cancel handler.

When a cluster resource group API is run, the exit program is called from a separate job with the user profile specified on the `Create Cluster Resource Group` (`QcstCreateClusterResourceGroup`) API. The separate job is automatically created by the API when the exit program is called. If the exit program for a data CRG is unsuccessful or ends abnormally, the cluster resource group exit program is called on all active nodes in the recovery domain by using an action code of `Undo`. This action code allows any unfinished activity to be backed out and the original state of the cluster resource group to be recovered.

Suppose an unsuccessful switchover occurs for a device CRG. After switching back all the devices, if all of the devices were varied-on successfully on the original primary node, clustering calls the exit program on the original primary node by using an action code of `Start`.

If the exit program for an application CRG is unsuccessful or ends abnormally, cluster resource services attempt to restart the application if the status of the CRG is active. The cluster resource group exit program is called by using an action code of `Restart`. If the application cannot be restarted in the specified maximum number of attempts, the cluster resource group exit program is called by using an action code of `Failover`. The restart count is reset only when the exit program is called by using an action code of `start`, which can be the result of a start CRG, a failover, or a switchover.

When the cluster resource group is started, the application CRG exit program called on the primary node is not to return control to cluster resource services until the application itself ends or an error occurs. After an application CRG is active, if cluster resource services must notify the application CRG exit program of some event, another instance of the exit program is started in a different job. Any action code other than `Start` or `Restart` is expected to be returned.

When a cluster resource group exit program is called, it is passed a set of parameters that identify the cluster event being processed, the current state of the cluster resources, and the expected state of the cluster resources.

For complete information about cluster resource group exit programs, including what information is passed to the exit program for each action code, see `Cluster Resource Group Exit Program` in the Cluster API documentation. Sample source code has been provided in the `QUSRTOOL` library which can be used as a basis for writing an exit program. See the `TCSTAPPEXT` member in the `QATTSYSC` file.

Application CRG considerations

An application cluster resource group manages application resiliency.

Managing application CRG takeover of IP addresses

You can manage application CRG takeover of IP addresses by using cluster resource services. You can also manage them manually.

You can manage the application takeover IP address that is associated with an application CRG in two ways. The easiest way, which is the default, is to let cluster resource services manage the takeover IP address. This method directs cluster resource services to create the takeover IP address on all nodes in the recovery domain, including nodes subsequently added to the recovery domain. When this method is selected, the takeover IP address cannot currently be defined on any node in the recovery domain.

The alternative way is to manage the takeover IP addresses yourself. This method directs cluster resource services to not take any steps to configure the takeover IP address; the user is responsible for configuration. You must add the takeover IP address on all nodes in the recovery domain (except on replicate nodes) before starting the cluster resource group. Any node to be added to the recovery domain of an active CRG must have the takeover IP address configured before being added.

Related concepts

[Example: Application cluster resource group failover actions](#)

This example shows how one failover scenario works. Other failover scenarios can work differently.

Multiple subnets

It is possible to have the application takeover IP address work across multiple subnets, although the default is to have all recovery domain nodes on the same subnet. To configure the application takeover IP address when the nodes in the recovery domain span multiple subnets, you need to enable the switchover environment.

Enabling application switchover across subnets with IPv4

Clustering, in general, requires that all cluster nodes in the recovery domain of an application cluster resource group reside on the same LAN (use the same subnet addressing). Cluster resource services supports a user configured takeover IP address when configuring application CRGs.

Address Resolution Protocol (ARP) is the network protocol that is used to switch the configured application takeover IP address from one node to another node in the recovery domain. To enable the application switchover across subnets, you need to use the virtual IP address support and the Routing Information Protocol (RIP) for IPv4.

The following manual configuration steps are required to enable the switchover environment. **This set of instructions must be done on all the nodes in the recovery domain, and repeated for the other nodes in the cluster that will become nodes in the recovery domain for the given application CRG.**

1. Select an IPv4 takeover IP address to be used by the application CRG.
 - To avoid confusion, this address should not overlap with any other existing addresses used by the cluster nodes or routers. For example, if choosing 19.19.19.19, ensure that 19.0.0.0 (19.19.0.0) are not routes known by the system routing tables.
 - Add the takeover interface (for example, 19.19.19.19). Create it with a line description of *VIRTUALIP, subnet mask of 255.255.255.255 (host route), maximum transmission unit of 1500 (any number in the range 576-16388), and autostart of *NO. This takeover address (for example, 19.19.19.19) must exist as a *VIRTUALIP address before identifying it as an associated local interface in next step. It does not, however, have to be active.
2. Associate the intended takeover IP address with one or both of the IP addresses that you specify to be used by cluster communications when you create the cluster or add a node to the cluster.
 - For example, this means that you make the 19.19.19.19 takeover address an associated local interface on the IP address for the cluster node. This must be done for each cluster address on each cluster node.
Note: The cluster addresses must be ended to accomplish this change under the Configure TCP/IP (CFGTCP) command.
3. Create the cluster and create any CRGs. For the application CRG, specify `QcstUserCfgrTakeoverIpAddr` for the **Configure takeover IP address** field. Do not start any application CRGs.
4. Using Configure TCP/IP applications (option 20) from the Configure TCP/IP menu, then Configure Routed (option 2), then Change Routed attributes (option 1), ensure that the Supply field is set to *YES. If not, set it to *YES. Then start or restart Routed (RIP or RIP-2) on each cluster node.
 - NETSTAT option 3 shows the Routed using a local port if currently running. Routed must be running and advertising routes (ensure that the Supply field is set to *YES) on every cluster node in the CRG recovery domain.
5. Ensure that all the commercial routers in the network that interconnect the recovery domain LANs are accepting and advertising host routes for RIP.
 - This is not necessarily the default setting for routers. The language varies with router manufacturer, but the RIP interfaces settings should be set to send host routes and receive dynamic hosts.
 - This also applies to both the router interfaces that point to the systems as well as the router-to-router interfaces.

Note: Do not use an IBM i machine as the router in this configuration. Use a commercial router (IBM or otherwise) that is designed for routing purposes. IBM i routing cannot be configured to handle this function.

6. Manually activate the takeover address on one of the cluster nodes:

- a) Wait up to 5 minutes for RIP to propagate the routes.
- b) Ping the takeover address from all nodes in the CRG recovery domain and from selected clients on the LANs who will be using this address.
- c) Ensure the takeover address is ended again.

(Clustering will start the address on the specified primary node when the CRGs are started.)

7. Start the application CRGs.

- The takeover address is started by clustering on the specified, preferred node, and RIP advertises the routes throughout the recovery domain. RIP might take up to 5 minutes to update routes across the domain. The RIP function is independent from the start CRG function.

Important:

- If the above procedure is not followed for all cluster nodes in the application CRG recovery domain, the cluster hangs during the switchover process.
- Even though you do not perform a failover to replica nodes, it is a good idea to perform the procedure on the replica nodes in the event that they might be changed at a later date in time to become a backup.
- If you want to use multiple virtual IP addresses, then each one will require a separate application CRG and a separate IP address with which to be associated. This address may be another logical IP address on the same physical adapter or it may be another physical adapter altogether. Also, care must be taken to prevent ambiguities in the routing tables. This is best achieved by doing the following:
 - Add a *DFTRROUTE to the routing table for each virtual IP address.
 - To use multiple IP address use CFGTCP (option 2).
 - Set all parameters, including the next hop, the same to reach the router of choice; however, the Preferred binding interface should be set to the local system IP address that is associated with the virtual IP address that is represented by this route.

Enabling application switchover across subnets with IPv6

Clustering, in general, requires that all cluster nodes in the recovery domain of an application cluster resource group reside on the same LAN (use the same subnet addressing). Cluster resource services supports a user configured takeover IP address when configuring application CRGs.

Address Resolution Protocol (ARP) is the network protocol that is used to switch the configured application takeover IP address from one node to another node in the recovery domain. To enable the application switchover across subnets, you need to use the virtual IP address support and the Routing Information Protocol Next Generation (RIPng) for IPv6.

The following manual configuration steps are required to enable the switchover environment. **This set of instructions must be done on all the nodes in the recovery domain, and repeated for the other nodes in the cluster that will become nodes in the recovery domain for the given application CRG.**

1. Select an IPv6 takeover IP address to be used by the application CRG.

- To avoid confusion, this address should not overlap with any other existing addresses used by the cluster nodes or routers.
- It is recommended that this address is defined with a shorter IPv6 address prefix than any other IPv6 address that shares the same IPv6 prefix to ensure that the correct address is chosen for the source address in outbound packets.
- Add the takeover interface (for example, 2001:0DB8:1234::1. Create it with a line description of *VIRTUALIP, maximum transmission unit of 1500 (any number in the range 576-16388), and autostart of *NO.

2. Create the cluster and create any CRGs. For the application CRG, specify `QcstUserCfgrTakeoverIpAddr` for the **Configure takeover IP address** field. Do not start any application CRGs.
3. Use the Change RIP Attributes (CHGRIPA) command to set the RIPng attributes. Run the command: `CHGRIPA AUTOSTART(*YES) IP6COND(*NEVER) IP6ACPDFT(*NO) IP6SNDONLY(*VIRTUAL)`.
4. Ensure there is an IPv6 link-local address active on the system. An IPv6 link-local address starts with 'fe80:'.
5. Use the Add RIP Interface (ADDRIPIFC) command add a RIP interface used by the OMPROUTED server to advertise the virtual address used for the takeover IP address. For example, if fe80::1 is the active IPv6 link-local address, run the command: `ADDRIPIFC IFC('fe80::1') RCVDYNNET(*YES) SNDSTTRTE(*YES) SNDHOSTRTE(*YES) SNDONLY(*VIRTUAL)`.
6. Restart the OMPROUTED server using the following commands:
 - a) `ENDTCPSVR SERVER(*OMPROUTED) INSTANCE(*RIP)`
 - b) `STRTCPSVR SERVER(*OMPROUTED) INSTANCE(*RIP)`
7. Ensure that all the commercial routers in the network that interconnect the recovery domain LANs are accepting and advertising host routes for RIPng.
 - This is not necessarily the default setting for routers. The language varies with router manufacturer, but the RIPng interfaces settings should be set to send host routes and receive dynamic hosts.
 - This also applies to both the router interfaces that point to the systems as well as the router-to-router interfaces.

Note: Do not use an IBM i machine as the router in this configuration. Use a commercial router (IBM or otherwise) that is designed for routing purposes. IBM i routing cannot be configured to handle this function.
8. Manually activate the takeover address on one of the cluster nodes:
 - a) Wait up to 5 minutes for RIP to propagate the routes.
 - b) Ping the takeover address from all nodes in the CRG recovery domain and from selected clients on the LANs who will be using this address.
 - c) Ensure that the takeover address is ended again.
(Clustering will start the address on the specified primary node when the CRGs are started.)
9. Start the application CRGs.
 - The takeover address is started by clustering on the specified, preferred node, and RIPng advertises the routes throughout the recovery domain. RIPng might take up to 5 minutes to update routes across the domain. The RIPng function is independent from the start CRG function.

Important:

- If the above procedure is not followed for all cluster nodes in the application CRG recovery domain, the cluster hangs during the switchover process.
- Even though you do not perform a failover to replica nodes, it is a good idea to perform the procedure on the replica nodes in the event that they might be changed at a later date in time to become a backup.
- If you want to use multiple virtual IP addresses, then each one will require a separate application CRG and a separate IP address with which to be associated. This address may be another logical IP address on the same physical adapter or it may be another physical adapter altogether. Also, care must be taken to prevent ambiguities in the routing tables. This is best achieved by doing the following:
 - Add a *DFTRROUTE to the routing table for each virtual IP address.
 - To use multiple IP address use CFGTCP (option 2).
 - Set all parameters, including the next hop, the same to reach the router of choice; however, the Preferred binding interface should be set to the local system IP address that is associated with the virtual IP address that is represented by this route.

Example: Application cluster resource group failover actions

This example shows how one failover scenario works. Other failover scenarios can work differently.

The following happens when a cluster resource group for a resilient application fails over due to exceeding the retry limit or if the job is canceled:

- The cluster resource group exit program is called on all active nodes in the recovery domain for the CRG with an action code of failover. This indicates that cluster resource services is preparing to failover the application's point of access to the first backup.
- Cluster resource services ends the takeover Internet Protocol (IP) connection on the primary node.
- Cluster resource services starts the takeover IP address on the first backup (new primary) node.
- Cluster resource services submits a job that calls the cluster resource group exit program only on the new primary node with an action code of Start. This action restarts the application.

Related concepts

Managing application CRG takeover of IP addresses

You can manage application CRG takeover of IP addresses by using cluster resource services. You can also manage them manually.

Example: Application exit program

This code example contains an application cluster resource group exit program.

You can find this code example in the QUSRTOOL library.

Sample source code is provided in the QUSRTOOL library, which can be used as a basis for writing an exit program. See the TCSTAPPEXT member in the QATTSYSC file. To view the sample source code, issue one of the following commands:

- DSPPFM QUSRTOOL/QATTSYSC TCSTAPPEXT
- STRSEU SRCFILE(QUSRTOOL/QATTSYSC) SRCMBR(TCSTAPPEXT)
- WRKMBRPDM FILE(QUSRTOOL/QATTSYSC) MBR(TCSTAPPEXT), then place a 5 in front of the member name

If you receive CPF8056, EDT0213, or PDM0308 messages when running the commands, QUSRTOOL files need to be converted from save files to source physical files. Issue this command, CALL PGM(QUSRTOOL/UNPACKAGE) PARM('*ALL ' 1).

Note: By using the code examples, you agree to the terms of the [Code license and disclaimer information](#).

Planning clusters

Before implementing a high-availability solution, you must ensure that you met all prerequisites for clusters.

Hardware requirements for clusters

To implement a high-availability solution, you need to plan and configure a cluster. A cluster groups systems and resources in a high availability environment.

The following are the minimum hardware requirements for clusters:

- You will need at least two systems or partitions running IBM i. Cluster supports up to 128 systems within a cluster. Any System i[®] model that is capable of running IBM i V4R4M0, or later, is compatible for using clustering.
- External uninterruptible power supply or equivalent is recommended to protect from a sudden power loss which could result in a cluster partition.
- If you plan to use data resiliency technologies that require independent disk pools, you will also need to plan for hardware specific to your chosen data resiliency technology. You can also use different methods of disk protection to prevent failover from occurring should a protected disk fail.

Related concepts

[Planning data resiliency](#)

Data resilience is the ability for data to be available to users or applications. You can achieve data resiliency by using IBM i cluster technology with PowerHA technologies or logical replication technologies.

Related reference

[Planning checklist for clusters](#)

Complete the cluster configuration checklist to ensure that your environment is prepared properly before you begin to configure your cluster.

Related information

[Uninterruptible power supply](#)

[IP multicasting](#)

[Disk protection](#)

Software requirements for clusters

In order to use clustering, you must have the correct software and licenses.

1. Latest supported release of IBM i operating system installed.
2. TCP/IP Connectivity Utilities feature installed.
3. If you plan to use data resiliency technologies, there are additional requirements.
4. Option 41 (High Availability Switchable Resources) is required if you plan to use the following interfaces:
 - IBM PowerHA SystemMirror for i licensed program. This licensed program provides the following interfaces which require Option 41:
 - PowerHA graphical interface
 - PowerHA commands
 - PowerHA APIs
5. You can also use IBM Business Partner product or write your own high availability management application by using Cluster APIs.

Related concepts

[Determine site configuration](#)

PowerHA technologies provide several IBM i disaster recovery and high availability technologies.

[Planning data resiliency](#)

Data resilience is the ability for data to be available to users or applications. You can achieve data resiliency by using IBM i cluster technology with PowerHA technologies or logical replication technologies.

Related reference

[Planning checklist for clusters](#)

Complete the cluster configuration checklist to ensure that your environment is prepared properly before you begin to configure your cluster.

Related information

[Cluster APIs](#)

Communications requirements for clusters

Use any type of communications media in your clustering environment as long as it supports Internet Protocol (IP).

Cluster resource services uses TCP/IP and UDP/IP protocols to communicate between nodes. Local area networks (LANs), wide area networks (WANs), OptiConnect system area networks (SANs), or any

combination of these connectivity devices are supported. Your choice should be based on the following factors:

- Volume of transactions
- Response time requirements
- Distance between the nodes
- Cost considerations

You can use these same considerations when determining the connection media to be used to connect primary and backup locations of resources. When planning your cluster, it is recommended that you designate one or more of your backup nodes in remote locations in order to survive a site loss disaster.

To avoid performance problems that might be caused by inadequate capacity, you need to evaluate the communication media that is used to handle the volumes of information that are sent from node to node. You can choose which physical media you prefer to use such as token ring, Ethernet, asynchronous transfer mode (ATM), SPD OptiConnect, or Virtual OptiConnect (a high-speed internal connection between logical partitions).

Related reference

[Planning checklist for clusters](#)

Complete the cluster configuration checklist to ensure that your environment is prepared properly before you begin to configure your cluster.

Dedicate a network for clusters

During normal operations, base clustering communication traffic is minimal. It is, however, highly recommended that you have redundant communication paths configured for each node in a cluster.

A redundant communications path means that you have two lines configured between two nodes in a cluster. If a failure on the first communication path occurs, the second communication path can take over to keep communications running between the nodes, thereby minimizing conditions that can put one or more nodes of the cluster into a cluster partition. One thing to consider when configuring these paths is that if both of your communications lines go into the same adapter on the system, these lines are still at risk if this single adapter fails. However, it should be noted that a cluster partition is not always avoidable. If your system experiences a power loss or if a hardware failure occurs, the cluster can become partitioned. By configuring two lines, you can dedicate one line for clustering traffic and the other line for the normal traffic and also for the backup line if the dedicated line for clustering goes down. The typical network-related cluster partition can best be avoided by configuring redundant communications paths between all nodes in the cluster.

Tips: Cluster communications

Consider these tips when you set up your communications paths.

- Be sure you have adequate bandwidth on your communication lines to handle the non cluster activity along with the clustering heartbeat function and continue to monitor for increased activity.
- For best reliability, do not configure a single communication path linking one or more nodes.
- Do not overburden the line that is responsible for ensuring that you are still communicating with a node.
- Eliminate as many single points of failure as possible, such as having two communication lines coming into a single adapter, same input-output processor (IOP), or same expansion unit.
- If you have an extremely high volume of data being passed over your communication lines, you may want to consider putting data replication and heartbeat monitoring on separate networks.
- User Datagram Protocol (UDP) multicast is the preferred protocol that the cluster communications infrastructure uses to send cluster management information between nodes in a cluster. When the physical media supports multicast capabilities, cluster communications uses the UDP multicast to send management messaging from a given node to all local cluster nodes that support the same subnet address. Messages that are sent to nodes on remote networks are always sent by using UDP point-to-point capabilities. Cluster communications does not rely on routing capability for multicast messages.

- The multicast traffic that supports cluster management messaging tends to fluctuate by nature. Depending on the number of nodes on a given LAN (that supports a common subnet address) and the complexity of the cluster management structure that is chosen by the cluster administrator, cluster-related multicast packets can easily exceed 40 packets per second. Fluctuations of this nature can have a negative effect on older networking equipment. One example is congestion problems on devices on the LAN that serve as Simple Network Management Protocol (SNMP) agents that need to evaluate every UDP multicast packet. Some of the earlier networking equipment does not have adequate bandwidth to keep up with this type of traffic. You need to ensure that you or the network administrator has reviewed the capacity of the networks to handle UDP multicast traffic to make certain that clustering does not have a negative effect on the performance of the networks.

Performance planning for clusters

Since potentially significant differences exist in your communications environment, you have the capability to adjust variables that affect cluster communications to best match your environment.

The default values should normally be acceptable to most common environments. If your particular environment is not well suited for these defaults, you can tune cluster communications to better match your environment. Base-level tuning and advanced level tuning are available.

Base-level tuning

Base-level tuning allows you to set the tuning parameters to a predefined set of values identified for high, low, and normal timeout and messaging interval values. When the normal level is selected, the default values are used for cluster communications performance and configuration parameters. Selecting the low level causes clustering to increase the heartbeating interval and the various message timeout values. With fewer heartbeats and longer timeout values, the cluster is less sensitive to communications failures. Selecting the high level causes clustering to decrease the heartbeating interval and the various message timeout values. With more frequent heartbeats and shorter timeout values, the cluster is more sensitive to communications failures.

Advanced-level tuning

With advanced-level tuning, individual parameters can be tuned by using a predefined ranges of values. This allows more granular tuning to meet any special circumstances in your communications environment. If an advanced level of tuning is desired, it is recommended that you obtain help from IBM support personnel or equivalent. Setting the individual parameters incorrectly can easily result in decreased performance.

Tunable cluster communications parameters

The Change Cluster Resource Services (QcstChgClusterResourceServices) API enables some of the cluster topology services and cluster communications performance and configuration parameters to be tuned to better suit the many unique application and networking environments in which clustering occurs.

The **Change Cluster (CHGCLU)** command provides a base level of tuning, while the QcstChgClusterResourceServices API provides both base and advanced levels of tuning.

The QcstChgClusterResourceServices API and **Change Cluster Configuration (CHGCLUCFG)** command can be used to tune cluster performance and configuration. The API and command provide a base level of tuning support where the cluster will adjust to a predefined set of values identified for high, low, and normal timeout and messaging interval values. If an advanced level of tuning is desired, usually anticipated with the help of IBM support personnel, then individual parameters can be tuned through the use of the API over a predefined value range. Inappropriate changes to the individual parameters can easily lead to degraded cluster performance.

When and how to tune cluster parameters

The **CHGCLU** command and the QcstChgClusterResourceServices API provide for a fast path to setting cluster performance and configuration parameters without your needing to understand the details.

This base level of tuning primarily affects the heartbeating sensitivity and the cluster message timeout values. The valid values for the base level of tuning support are:

1 (High Timeout Values/Less Frequent Heartbeats)

Adjustments are made to cluster communications to decrease the heartbeating frequency and increase the various message timeout values. With fewer heartbeats and longer timeout values, the cluster will be slower to respond (less sensitive) to communications failures.

2 (Default Values)

Normal default values are used for cluster communications performance and configuration parameters. This setting can be used to return all parameters to the original default values.

3 (Low Timeout Values/More Frequent Heartbeats)

Adjustments are made to cluster communications to decrease the heartbeating interval and decrease the various message timeout values. With more frequent heartbeats and shorter timeout values, the cluster is quicker to respond (more sensitive) to communications failures.

Example response times are shown in the following table for a heartbeat failure leading to a node partition:

Note: Times are specified in minutes:seconds format.

	1 (Less sensitive)			2 (Default)			3 (More sensitive)		
	Detectio n of Heartbe at Problem	Analysis	Total	Detectio n of Heartbe at Problem	Analysis	Total	Detectio n of Heartbe at Problem	Analysis	Total
Single subnet	00:24	01:02	01:26	00:12	00:30	00:42	00:04	00:14	00:18
Multiple subnets	00:24	08:30	08:54	00:12	04:14	04:26	00:04	02:02	02:06

Depending on typical network loads and specific physical media being used, a cluster administrator might choose to adjust the heartbeating sensitivity and message timeout levels. For example, with a high speed high-reliability transport, such as OptiConnect with all systems in the cluster on a common OptiConnect bus, one might desire to establish a more sensitive environment to ensure quick detection leading to faster failover. Option 3 is chosen. If one were running on a heavily loaded 10 Mbs Ethernet bus and the default settings were leading to occasional partitions just due to network peak loads, option 1 could be chosen to reduce clustering sensitivity to the peak loads.

The Change Cluster Resource Services API also allows for tuning of specific individual parameters where the network environmental requirements present unique situations. For example, consider again a cluster with all nodes common on an OptiConnect bus. Performance of cluster messages can be greatly enhanced by setting the message fragment size parameter to the maximum 32,500 bytes to better match the OptiConnect maximum transmission unit (MTU) size than does the default 1,464 bytes. This reduces the overhead of fragmentation and reassembly of large messages. The benefit, of course, depends on the cluster applications and usage of cluster messaging resulting from those applications. Other parameters are defined in the API documentation and can be used to tune either the performance of cluster messaging or change the sensitivity of the cluster to partitioning.

Related reference

[QcstChgClusterResourceServices API](#)

Related information

[Change Cluster \(CHGCLU\) command](#)

Changing cluster resource services settings

The default values affecting message timeout and retry are set to account for most typical installations. However, it is possible to change these values to more closely match your communications environment.

The values can be adjusted in one of these ways:

- Set a general performance level that matches your environment.
- Set values for specific message tuning parameters for more specific adjustment

In the first method, the message traffic is adjusted to one of three communications levels. The normal level is the default and is described in detail in Heartbeat monitoring.

The second method should normally be done only under the advisement of an expert.

The Change Cluster Resource Services (QcstChgClusterResourceServices) API describes details on both methods.

Related reference

[QcstChgClusterResourceServices API](#)

Related information

[Heartbeat monitoring](#)

Planning multiple-release clusters

If you are creating a cluster that includes nodes at multiple cluster versions, then certain steps are required when you create the cluster.

By default, the current cluster version is set to the potential cluster version of the first node added to the cluster. This approach is appropriate if this node is at the lowest version level to be in the cluster.

However, if this node is at a later version level, then you cannot add nodes with a lower version level. The alternative is to use the target cluster version value when you create a cluster to set the current cluster version to one less than the potential cluster version of the first node added to the cluster.

Note: If you are using the IBM PowerHA SystemMirror for i licensed program, it is required on all systems within the cluster.

For example, consider the case where a two-node cluster is to be created. The nodes for this cluster follow:

Node identifier	Release	Potential cluster version
Node A	V7R1	7
Node B	V7R2	8

If the cluster is to be created from Node B, care must be taken to indicate that this will be a mixed-release cluster. The target cluster version must be set to indicate that the nodes of the cluster will communicate at one less than the requesting node's potential node version.

Performance planning for clusters

When changes are made to a cluster, the overhead necessary to manage the cluster can be affected.

The only resources that clustering requires are those necessary to perform heartbeat monitoring, to manage the cluster resource groups and the cluster nodes, and to handle any messaging taking place between cluster resource groups and cluster nodes. After your clustering environment is operational, the only increase in overhead is if you make changes to the cluster.

During a normal operating environment, clustering activity should have minimal effect on your clustered systems.

Planning advanced node failure detection

Advanced node failure detection function can be used to reduce the number of failure scenarios which result in cluster partitions.

Before implementing advanced node failure detection, you must ensure that you have met all the prerequisites.

- To prevent cluster partitions when a cluster node has actually failed, a Hardware Management Console (HMC) v7 or Virtual I/O Server (VIOS) partition on an Integrated Virtualization Manager (IVM) managed server can be used.
- For each cluster node, determine the type of server that the cluster monitor will be using to monitor that node. If the node is managed either by an IVM or by an HMC at version V8R8.5.0 or earlier, then a common information model (CIM) server can be used. If the node is managed by an HMC at version V8R8.5.0, then a representational state transfer (REST) server can be used.

Note: For cluster nodes managed by HMCs at version V8R8.5.0, you may choose to use either a CIM server or a REST server. The REST server is recommended because CIM servers are not supported for later versions of HMC.

- Each node that is to have failures reported to it, will need to have a cluster monitor configured.

Hardware requirements for the advanced node failure detection

Advanced node failure detection feature can be used provided all the hardware requirements are met.

The following minimum hardware requirements are needed for the advanced node failure detection feature:

- At least two IBM i models or logical partitions.
- Either Hardware Management Console (HMC) or a Virtual I/O Server (VIOS) on an Integrated Virtualization Manager (IVM) managed server.

Software requirements for the advanced node failure detection

To use the advanced node failure detection function in an IBM i high-availability solution, the minimum software requirements should be met.

Each node planning to use the advanced node failure detection feature with common information model (CIM) servers has the following software requirements:

- 5770-SS1 Base operating system option 33 - Portable Application Solutions Environment
- 5770-SS1 Base operating system option 30 - Qshell
- 5733-SC1 - IBM Portable Utilities for IBM i
- 5733-SC1 option 1 - OpenSSH, OpenSSL, zlib
- 5770-UME IBM Universal Manageability Enablement
- 5770-HAS IBM PowerHA for i LP
- HMC version V8R8.5.0 or earlier. This is the last version of HMC to support the CIM server.

Note: IVM uses the CIM server.

Each node planning to use the advanced node failure detection feature with representational state transfer (REST) servers has the following software requirements:

- 5770-SS1 Base operating system option 3 - Extended Base Directory Support
- 5770-SS1 Base operating system option 33 - Portable Application Solutions Environment
- 5733-SC1 - IBM Portable Utilities for IBM i (Only required for initial configuration of a cluster monitor.)
- 5733-SC1 option 1 - OpenSSH, OpenSSL, zlib (Only required for initial configuration of a cluster monitor.)
- 5770-HAS IBM PowerHA for i LP
- HMC version V8R8.5.0 or later. This is the first version of HMC to support the REST server.

- PowerHA for i new function cluster monitor HMC REST support PTF

Planning checklist for clusters

Complete the cluster configuration checklist to ensure that your environment is prepared properly before you begin to configure your cluster.

<i>Table 1. TCP/IP configuration checklist for clusters</i>	
TCP/IP requirements	
---	Start TCP/IP on every node you plan to include in the cluster using the Start TCP/IP (STRTCP) Command .
---	Configure the TCP loopback address (127.0.0.1) and verify that it shows a status of Active. Verify the TCP/IP loopback address by using the Work with TCP/IP Network Status (WRKTCPSTS) Command on every node in the cluster.
---	Verify that the IP addresses used for clustering on a node have a status of Active. Use the Work with TCP/IP Network Status (WRKTCPSTS) Command to check the status of the IP addresses.
---	Verify that the Internet Daemon (INETD) server is active on all nodes in the cluster. If INETD server is not active, you need to start the INETD server. For information about how to start INETD server, see “Starting the INETD server” on page 50.
---	Verify that user profile for INETD, which is specified in /QIBM/ProdData/OS400/INETD/inetd.conf, does not have more than minimal authority. If this user profile has more than minimal authority, starting cluster node will fail. By default, QUSER is specified as the user profile for INETD.
---	Verify every cluster IP address on every node in the cluster can route to and send UDP datagrams to every other IP address in the cluster. If any cluster node uses an IPv4 address, then every node in the cluster needs to have an active IPv4 address (not necessarily configured as a Cluster IP address) that can route to and send TCP packets to that address. Also, if any cluster node uses an IPv6 address, then every node in the cluster needs to have an active IPv6 address (not necessarily configured as a Cluster IP address) that can route to and send TCP packets to that address. Use the PING command, specifying a local IP address, and the TRACEROUTE command, specifying UDP messages can be useful in determining if two IP addresses can communicate. PING and TRACEROUTE do not work between IPv4 and IPv6 addresses, or if a firewall is blocking PING and TRACEROUTE .
---	Verify that ports 5550 and 5551 are not being used by other applications. These ports are reserved for IBM clustering. Port usage can be viewed by using the Work with TCP/IP Network Status (WRKTCPSTS) command . Port 5550 is opened and is in a Listen state by clustering after INETD is started.

<i>Table 2. Administrative domain checklist for clusters</i>	
Cluster resource services cluster interface considerations	
	Install IBM PowerHA SystemMirror for i (iHASM licensed program (5770-HAS). A valid license key must exist on all cluster nodes that will be in the high-availability solution.
---	Install Option 41 (IBM i - HA Switchable Resources) . A valid license key must exist on all cluster nodes that will be in the device domain.
---	Verify that all host servers are started by using the Start Host Server (STRHOSTSVR) Command: STRHOSTSVR SERVER(*ALL)

<i>Table 3. Security configuration checklist for clusters</i>	
Security requirements	
---	Set the Allow Add to Cluster (ALWADDCLU) network attribute appropriately on the target node if you are trying to start a remote node. This should be set to *ANY or *RQSAUT depending on your environment. If this attribute is set to *RQSAUT, then IBM i option 34 (Digital Certificate Manager) and the CCA Cryptographic Service Provider (Option 35) must be installed. See Enable a node to be added to a cluster for details on setting the ALWADDCLU network attribute.
---	Enable the status of the user profile for INETD specified in /QIBM/ProdData/OS400/INETD/inetd.conf. It must not have *SECADM or *ALLOBJ special authorities. By default, QUSER is specified as the user profile for INETD.
---	Verify that the user profile that calls the cluster resource services APIs exists on all cluster nodes and has *IOSYSCFG authority.
---	Verify that the user profile to run the exit program for a cluster resource group (CRG) exists on all recovery domain nodes.

<i>Table 4. Job configuration checklist for clusters</i>	
Job considerations	
---	Jobs can be submitted by the cluster resource services APIs to process requests. The jobs either run under the user profile to run the exit program specified when creating a cluster resource group, or under the user profile that requested the API (for varying on devices in resilient device CRGs only). Ensure that the subsystem that services the job queue associated with the user profile is configured as: *NOMAX for the number of jobs it can run from that job queue.
---	Jobs are submitted to the job queue specified by the job description that is obtained from the user profile defined for a CRG. The default job description causes the jobs to be sent to the QBATCH job queue. Because this job queue is used for many user jobs, the exit program job might not run in a timely fashion. Consider a unique job description with a unique user queue.
---	When exit program jobs are run, they use routing data from the job description to choose which main storage pool and run time attributes to use. The default values result in jobs that are run in a pool with other batch jobs that have a run priority of 50. Neither of these may produce the desired performance for exit program jobs. The subsystem initiating the exit program jobs (the same subsystem that is using the unique job queue) should assign the exit program jobs to a pool that is not used by other jobs initiated by the same subsystem or other subsystems. In addition, the exit program jobs should be assigned a run priority of 15 so that they run before almost all other user jobs.
---	Set the <u>QMLTTHDACN</u> system value to 1 or 2.

There are several software interfaces available for configuring and managing your cluster. One of these interfaces is PowerHA graphical interface. If you choose to use PowerHA, the following requirements must be satisfied.

<i>Table 5. PowerHA configuration checklist for clusters</i>	
PowerHA graphical interface considerations	
---	Install IBM PowerHA SystemMirror for i licensed program. A valid license key must exist on all cluster nodes that will be in the high-availability solution.
---	Install Option 41 (HA Switchable Resources). A valid license key must exist on all cluster nodes that will be in the device domain.
---	Verify that all host servers are started by using the Start Host Server (STRHOSTSVR) command: STRHOSTSVR SERVER(*ALL)

Table 5. PowerHA configuration checklist for clusters (continued)

PowerHA graphical interface considerations	
---	Verify that the Administration Server is started by using the Start TCP/IP Server (STRTCPSVR) command: STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)

Table 6. Advanced node failure detection checklist for clusters

Advanced node failure detection considerations when using a CIM server or IVM	
---	Determine which cluster nodes are or can be managed with a Hardware Management Console (HMC) or a Virtual I/O Server (VIOS) partition on an Integrated Virtualization Manager (IVM) managed server
---	Determine which cluster node(s) are to receive messages when some other cluster node fails
---	On each cluster node that is to receive a message from an HMC or IVM, the following things must be done.
	Install base operating system option 33 - IBM Portable Application Solutions Environment for i
	Install 5733-SC1 - IBM Portable Utilities for i
	Install 5733-SC1 option 1 - OpenSSH, OpenSSL, zlib
	Install 5770-UME - IBM Universal Manageability Enablement for i.
	Configure the enableAuthentication and sslClientVerificationMode properties for the 5770-UME product.
	Copy a digital certificate file from the HMC or VIOS and add it to an IBM i truststore.
	Start the *CIMOM server with STRTCPSVR *CIMOM CL command
	Configure the cluster monitor(s) with the ADDCLUMON CL command
Advanced node failure detection considerations when using a REST server	
---	Determine which cluster nodes are or can be managed with a Hardware Management Console (HMC) REST server
---	Determine which cluster node(s) are to receive messages when some other cluster node fails
---	On each cluster node that is to receive a message from an HMC, the following things must be done.
	Install base operating system option 3 - Extended Base Directory Support.
	Install base operating system option 33 - IBM Portable Application Solutions Environment for i
	Install 5733-SC1 - IBM Portable Utilities for i (Only required for initial configuration of a cluster monitor.)
	Install 5733-SC1 option 1 - OpenSSH, OpenSSL, zlib (Only required for initial configuration of a cluster monitor.)
	Copy a digital certificate file from the HMC and add it to an IBM i truststore.
	Configure the cluster monitor(s) with the ADDCLUMON CL command

Planning environment resiliency

Environment resiliency ensures that your objects and attributes remain consistent among resources defined in the high-availability environment. You need to identify which resources require a consistent environment to function properly and create a cluster administrative domain that will ensure that these resource attributes remain consistent in your high availability solution.

Planning for a cluster administrative domain

The cluster administrative domain requires planning to manage resources that are synchronized among nodes within a cluster administrative domain. In order to ensure that an application will run consistently on any system in a high-availability environment, all resources that affect the behavior of the application need to be identified, as well as the cluster nodes where the application will run, or where application data might reside.

A cluster administrator can create a cluster administrative domain and add monitored resources that are synchronized among nodes. The IBM i cluster provides a list of system resources that can be synchronized by a cluster administrative domain, represented by monitored resource entries (MREs).

When designing a cluster administrative domain, you should answer the following questions:

What nodes will be included in the cluster administrative domain?

You should determine what nodes in a cluster are to be managed by the cluster administrative domain. These are the cluster nodes representing the systems where an application can run or where the application data is stored, and that require a consistent operational environment. Nodes cannot be in multiple cluster administrative domains. For example, if you have four nodes in a cluster (Node A, Node B, Node C and Node D), Nodes A and B can be in one cluster administrative domain and Nodes C and D can be in another. However you cannot have Nodes B and C in a third cluster administrative domain and still have them in their original cluster administrative domain.

What will be the naming convention for cluster administrative domains?

Depending on the complexity and size of your clustered environment, you might want to establish a standard naming convention for peer CRGs and cluster administrative domains. Since a peer CRG is created when you create a cluster administrative domain, you will want to differentiate other peer CRGs from those that represent cluster administrative domains. For example, peer CRGs that represent cluster administrative domains can be named *ADMDMN1*, *ADMDMN2*, and so forth, while other peer CRGs can be named *PEER1*. You can also use the [List Cluster Resource Group Information \(QcstListClusterResourceGroupIn\)](#) API to determine whether the peer CRG is used as a cluster administrative domain. A peer CRG which represents a cluster administrative domain can be identified by its application identifier, which is `QIBM.AdminDomain`.

Planning monitored resources entries (MRE)

Monitored resources are IBM i objects that can be defined within a cluster administrative domain. These resources need to remain consistent across the systems in a high-availability environment otherwise during an outage applications might not perform as expected. You should plan which supported resources within your environment should be monitored.

You need to determine which system resources need to be synchronized. You can select attributes for each of these resources to customize what is synchronized. Applications that run on multiple nodes might need specific environment variables to run properly. In addition data that spans several nodes might also require certain user profiles to be accessed. Be aware of the operational requirements for your applications and data before you determine what resources need to be managed by a cluster administrative domain.

Planning data resiliency

Data resilience is the ability for data to be available to users or applications. You can achieve data resiliency by using IBM i cluster technology with PowerHA technologies or logical replication technologies.

For IBM i supported implementations of data resilience, you have several choices of technologies. When these technologies are combined with IBM i cluster resource services, you can build a complete high-availability solution. These technologies can be categorized this way:

IBM i Independent disk pool technologies

These technologies are all based on IBM i implementation of independent disk pools. For high availability that uses independent disk pool technologies, it is required that all data that needs to be resilient be

stored in an independent disk pool. In many cases, this requires migrating data to independent disk pools. This information assumes that migration of data has been completed.

The following IBM i supported technologies are based on independent disk pools:

- Switched logical units (LUNs)
- Geographic mirroring
- Metro Mirror
- Global Mirror
- HyperSwap with independent auxiliary storage pools (IASPs)

DS8000 Full System HyperSwap technology

DS8000 Full System HyperSwap is an IBM System Storage® technology, which has been integrated into PowerHA to provide a minimal downtime high availability solution for storage outages (seconds to minutes). Full System HyperSwap can also be combined with live partition mobility to define and implement affinity between the POWER® server hosting the IBM i logical partition and the storage server hosting the data.

Logical replication technologies

Logical replication is a journal-based technology, where data is replicated to another system in real time. Logical replication technologies use IBM i cluster resource services and journaling with IBM Business Partner applications. These solutions require a high availability business partner application to configure and manage the environment. This information does not provide specific requirements for these IBM Business Partner solutions. If you are implementing a logical replication solution for high availability, consult information related to application or contact a service representative.

Determine which data should be made resilient

Understand what types of data you should consider making resilient.

Determining which data you need to make resilient is similar to determining which kind of data you need to back up and save when you prepare a back up and recovery strategy for your systems. You need to determine which data in your environment is critical to keeping your business up and running.

For example, if you are running a business on the Web, your critical data can be:

- Today's orders
- Inventory
- Customer records

In general, information that does not change often or that you do not need to use on a daily basis probably does not need to be made resilient.

Determine site configuration

PowerHA technologies provide several IBM i disaster recovery and high availability technologies.

For PowerHA technologies, which involve two copies of the data, such as Geographic mirroring, Metro Mirror, Global Mirror and HyperSwap, there are considerations for planning the sites where the data will reside. One site is typically considered the production or source site. This site contains your production data, which is mirrored or copied to the remote site. The remote site, sometime referred to as a backup or target site, contains the mirrored copy of the production data. When a site-wide disaster occurs at the production site, the backup site resumes your business with the mirrored data. Before you configure one of these technologies, consider the following regarding your site plans.

Determine which sites will be production and backup sites

Assess the current hardware and software resources that are in place at each site to determine if there are any missing components that will be necessary for a cross-site mirroring solution.

Determine the distance between production and backup sites

Depending on your communication bandwidth and other factors, distance between sites can affect performance and latency in the mirroring technology you choose. Some cross-site mirroring technologies are better suited for sites that are at great distances, while others may have performance degradation.

For more information about disk pools, see [Planning your disk pools](#).

Related tasks


[Enabling and accessing disk units](#)

PowerHA supported storage servers

IBM System Storage provides enhanced storage capabilities.

PowerHA supports the Metro Mirror, Global Mirror, LUN switching, and FlashCopy technologies with the following storage servers: DS8000 storage family, SAN Volume Controller (SVC), and the IBM Storwize® models. For more information on specific implementations, see the following guides.

- [IBM i and IBM Storwize Family: A Practical Guide to Usage Scenarios](#) 

- [IBM i and IBM System Storage: A Guide to Implementing External Disks on IBM i](#) 

Depending on the IBM System Storage Device, the IBM PowerHA SystemMirror for i licensed program also requires:

- For DS8000 System Storage Devices, the IBM PowerHA for i licensed program also requires storage command-line interface (DSCLI). DSCLI is required for all of the IBM DS8000 Series System Storage solutions, such as FlashCopy, Metro Mirror, and Global Mirror.
- There is a requirement to have DSCLI installed on each of the systems or partitions participating in the high availability solution, which uses these storage solutions.
- DSCLI has these additional software requirements:
 - Java™ Version 1.4
 - Option 35 (CCA Cryptographic Service Provider) installed on each system or partition
- For SAN Volume Controller (SVC), or Storwize System Storage Devices, the IBM PowerHA for i licensed program also requires:
 - Portable Utilities for IBM i (5733-SC1)

Related concepts

[Communications requirement for Metro Mirror](#)

Before configuring PowerHA solution that uses Metro Mirror, ensure that the minimum communication requirements have been met.

[Communications requirement for Global Mirror](#)

Before configuring a PowerHA solution that uses Global Mirror, you should ensure that the minimum communication requirements have been met.

[Managing switched logical units \(LUNs\)](#)

Switched logical units are independent disk pools created from logical units created in an IBM System Storage that have been configured as part of a device cluster resource group (CRG).

[Hardware requirements for the FlashCopy feature](#)

To use the FlashCopy technology in an PowerHA solution, ensure that the minimum hardware requirements are met.

[Communications requirements for the FlashCopy feature](#)

To use the FlashCopy technology in a PowerHA solution, ensure that the minimum communications requirements are met.

[Scenario: Global Mirror](#)

This scenario describes an PowerHA solution that is based on external storage and provides disaster recovery and high availability for storage systems that are separated by great distances. Global Mirror is an IBM Systems Storage solution that copies data asynchronously from the storage unit at the production site to the storage unit at the backup site. In this way, data remains consistent at the backup site.

Scenario: Metro Mirror

This scenario describes a PowerHA solution, which is based on external storage and provides disaster recovery and high availability for storage systems, which are separated by short distances. Metro Mirror is an IBM System Storage solution that copies data synchronously from the storage unit at the production site to the storage unit at the backup site. In this way data remains consistent at the backup site.

Scenario: Performing a FlashCopy function

In this example, an administrator wants to perform a backup from the remote copy of data that is stored in an external storage unit at the backup site. Using the FlashCopy function available with IBM Storage Solutions, the administrator reduces his backup time considerably.

Related tasks

Configuring a FlashCopy session

For IBM i high-availability environments that use IBM System Storage technology, you can configure a FlashCopy session to create a point-in-time copy of data.

Configuring switched logical units (LUNs)

Switched logical units is an independent disk pool that is controlled by a device cluster resource group and can be switched between nodes within a cluster. For IBM i high availability solutions that use switchable logical units with IBM® System Storage™, you need to configure an ASP Copy Description that defines the host identifiers and volume groups for each cluster node in which the ASP device can be switched.

Configuring Metro Mirror

For IBM i high availability solutions that use IBM System Storage Metro Mirror technology, you need to configure a session between the IBM i machine and IBM System Storage external storage units that have Metro Mirror configured. In IBM i, Metro Mirror sessions do not set up the mirroring on the external storage units, but rather sets up a relationship between the IBM i systems and the existing Metro Mirror configuration on external storage units.

Configuring Global Mirror

For IBM i high availability solutions that use IBM System Storage Global Mirror technology, you need to configure a session between the IBM i machine and IBM System Storage external storage units that have Global Mirror configured. In IBM i, Global Mirror sessions do not set up the mirroring on the external storage units, but rather sets up a relationship between the IBM i systems and the existing Global Mirror configuration on external storage units.

Supported external storage communication methods

Determine which interface to your storage system works best in your network

Selection of a communication method depends on which storage area network (SAN) you are planning to use, supporting hardware and software, and network size/topology.

There are several ways that PowerHA can work with the storage devices. These include:

- Data Storage command-line interface (DSCLI)
- Storage Area Network (SAN) volume controller
- Copy Services Management (CSM)

Data Storage command-line interface (DSCLI)

DSCLI management is one type of optional configuration of PowerHA enterprise storage servers.

The Data storage command-line interface is a tool that communicates with DS8000 series storage units. It is designed to provide simplified management control of Peer-to-peer remote copy sessions. With this tool, you can manage or monitor the status of copy sessions, create logical storage volumes, create and manage resource groups or change and delete copy sessions.

Using the DS8000 series requires that cluster nodes maintain communication in order to monitor replication status, failover messages, and switching actions. Communication is through the data storage command-line interface (DSCLI)

Some notes and prerequisites for DSCLI usage include:

- For DS8000 System Storage Devices, the IBM PowerHA for i licensed program also requires storage command-line interface (DSCLI). DSCLI can be used for all IBM DS8000 Series System Storage solutions, such as FlashCopy, Metro Mirror, Global Mirror, and use with LUN level switching.
- There is a requirement to have DSCLI installed on each of the systems or partitions participating in the high availability solution.
- DSCLI has additional software requirements:
 - A supported Java version.
 - That Option 35 (CCA Cryptographic Service Provider) is installed on each system or partition.

For further information about DSCLI, visit the [Command-line interface](#) section of the DS8870 Knowledge Center.

Storage Area Network (SAN) volume controller (SVC) usage

SVC is a hardware and software storage solution implementing IBM Spectrum virtualization technologies

SAN Volume Controller (SVC) appliances map physical volumes in the storage device to virtualized volumes, making them visible to host systems and other applications. SVC provides Copy Services functions that can be used to improve availability and support disaster recovery. These include Metro Mirror, Global Mirror, and Flash Copy.

PowerHA interfaces are compatible with SVC. After the basic SVC environment is configured, PowerHA can create copy sessions with the volumes. Using PowerHA with SVC management creates an automated highly available disaster recovery solution with minimal additional configuration. The PowerHA SVC interfaces are compatible with:

- the IBM Storwize V3700, V5000, V7000, V9000 series
- IBM SAN Volume Controller
- hardware running IBM Spectrum Virtualize

For information about setting up and configuring the SVC to run with PowerHA for i, consult: [SAN Volume Controller Knowledge Center](#).

Copy Services Management (CSM) Storage Controller

The Copy Services Management (CSM) storage controller

Copy Services Manager (CSM) controls copy services in storage environments. Copy services are features used by storage systems such as IBM® DS8000® to configure, manage, and monitor data-copy functions. Copy services include Metro Mirror, Global Mirror, and HyperSwap with Global Mirror.

PowerHA uses configuration descriptions to connect to CSM servers to access and manage copy service functions of key external storage components by providing connection and authentication information.

Prerequisites for using CSM on an IBM i for communications with the storage units include:

- Copy Services Manager (CSM) server
- 5770-SS1 Base operating system option 3 - Extended Base Directory Support
- 5770-SS1 Base operating system option 33 - Portable Application Solutions Environment

Note: In some instances both DSCLI and CSM are used in combination where DSCLI is used for Flash Copy and LUN Level Switching, and Copy Services manager is used for managing the replication of Metro Mirror or Global Mirror.

For additional information, see the [IBM Copy Services Manager](#) section of the DS8870 Knowledge Center.

Planning geographic mirroring

Geographic mirroring is a sub-function of cross-site mirroring. This technology provides disaster recovery and high availability in IBM i environments.

Hardware requirements for geographic mirroring

If you plan to use geographic mirroring for IBM i high availability, ensure that the minimum hardware requirements are met.

- All independent disk pool hardware requirements must be met.
- At least two IBM i models, which can be separated geographically, are required.
- At least two sets of disks at each site that are roughly of similar capacity are required.
- A separate storage pool for jobs using geographic mirrored independent disk pools should be configured. Performing geographic mirroring from the main storage pool can cause the system to hang under extreme load conditions.
- Geographic mirroring is performed when the disk pool is available. When geographic mirroring is being performed, the system value for the time of day (QTIME) should not be changed.
- Communications requirements for independent disk pools are critical because they affect throughput.
- Geographic mirroring traffic is dispersed round robin across the potentially multiple communication lines available to it. It is recommended that if multiple lines are provided for geographic mirroring, that those lines be of similar speed and capacity.
- It is recommended that a separate communication line be used for the clustering heartbeat to prevent contention with the geographic mirroring traffic.

Software requirements for geographic mirroring

If you plan to use geographic mirroring as part of an IBM i high availability solution, the following software is required.

- To use advanced features of geographic mirroring, IBM PowerHA SystemMirror for i license program must be installed.
- To use new and enhanced functions and features of this technology, it is recommended that you install the most current release and version of the operating system on each system or logical partition that is participating in a high-availability solution that is based on this technology. If the production system and backup system are at different operating system releases, it is required that the backup system be at the more current release. This scenario can be used to upgrade a production environment to the next release.

Note: Once the IASP has been switched and varied on to the newer release system, it cannot be switched back until the new target system has also been upgraded.

- To perform some of the disk management tasks necessary to implement independent disk pools, use the Configure Device ASP (CFGDEVASP) command, or IBM Navigator for i.
- You need to install IBM i Option 41 HA Switchable Resources. Option 41 gives you the capability to switch independent disk pools between systems. To switch an independent disk pool between systems, the systems must be members of a cluster and the independent switched disk must be associated with a device cluster resource group in that cluster. Option 41 is also required for working with high availability management interfaces, which are provided as part of the IBM PowerHA SystemMirror for i licensed program.

Communications requirements for geographic mirroring

When you are implementing an IBM i high-availability solution that uses geographic mirroring, you should plan communication lines so that geographic mirroring traffic does not adversely affect system performance.

The following is recommended:

- Geographic mirroring can generate heavy communications traffic. If geographic mirroring shares the same IP connection with another application, for example clustering, then geographic mirroring might

be suspended, which results in synchronization. Likewise, clustering response might be unacceptable, which results in partitioned nodes. Geographic mirroring should have its own dedicated communication lines. Without its own communication line, geographic mirroring can contend with other applications that use the same communication line and affect user network performance and throughput. This also includes the ability to negatively affect cluster heartbeat monitoring, resulting in a cluster partition state. Therefore, it is recommended that you have dedicated communication lines for both geographic mirroring and clusters. Geographic mirroring supports up to four communications lines.

Geographic mirroring distributes changes over multiple lines for optimal performance. The data is sent on each of the configured communication lines in turn, from 1 to 4, over and over again. Four communication lines allow for the highest performance, but you can obtain relatively good performance with two lines.

If you use more than one communication line between the nodes for geographic mirroring, it is best to separate those lines into different subnets, so that the usage of those lines is balanced on both systems.

- If your configuration is such that multiple applications or services require the use of the same communication line, some of these problems can be alleviated by implementing Quality of Service (QoS) through the TCP/IP functions of IBM i. The IBM i quality of service (QoS) solution enables the policies to request network priority and bandwidth for TCP/IP applications throughout the network.
- Ensure that throughput for each data port connection matches. This means that the speed and connection type should be the same for all connections between system pairs. If throughput is different, performance will be gated by the slowest connection.
- Consider the delivery method for a geographic mirroring ASP session. Before 7.1, the mirroring uses synchronous communication between the production and mirror copy systems. This delivery method is best for low latency environments. In 7.1, asynchronous support was added, which means asynchronous communications is used between the production and mirror copy systems. This delivery method is best for high latency environments. This delivery method will consume more system resources on the production copy node than synchronous delivery.
- Consider configuring a virtual private network for TCP/IP connections for the following advantages:
 - Security of data transmission by encrypting the data
 - Increased reliability of data transmission by sending greater redundancy

Related reference

[Quality of Service \(QoS\)](#)

Journal planning for geographic mirroring

When implementing high availability based on IBM i geographic mirroring, you should plan for journal management.

Journal management prevents transactions from being lost if your system ends abnormally. When you journal an object, the system keeps a record of the changes you make to that object. Regardless of the high availability solution that you implement, journaling is considered a best practice to prevent data loss during abnormal system outages.

Related information

[Journal management](#)

Backup planning for geographic mirroring

Before implementing high availability based on geographic mirroring, you should understand and plan a backup strategy within this environment.

Before configuring any high-availability solution, assess your current backup strategy and make appropriate changes if necessary. Geographic mirroring does not allow concurrent access to the mirror copy of the independent disk pool, which has implications to performing remote backups. If you want to back up from the geographically mirrored copy, you must quiesce mirroring on the production system and suspend the mirrored copy with tracking enabled. Tracking allows for changes on the production to be tracked so that they can be synchronized when the mirrored copy comes back online. Then you must vary on the suspended "mirror" copy of the independent disk pool, perform the backup procedure, vary off

"the suspended mirror copy" and then resume the independent disk pool to the original production host. This process only requires "partial data resynchronization" between the production and mirrored copies.

Your system is running exposed while doing the backups and when synchronization is occurring. It is also recommended that you suspend mirroring with tracking enabled, which speeds up the synchronization process. Synchronization is also required for any persistent transmission interruption, such as the loss of all communication paths between the source and target systems for an extended period of time. You can also use redundant communication paths to help eliminate some of those risks associated with a communication failure.

It is recommended that you should also use geographic mirroring in at least a three system, or logical partitions, where the production copy of the independent disk pool can be switched to another system at the same site that can maintain geographic mirroring.

Related concepts

Scenario: [Performing backups in geographic mirroring environment](#)

This scenario provides an overview of tasks that are necessary when performing a remote backup in a PowerHA solution that uses geographic mirroring.

Performance planning for geographic mirroring

When implementing a geographic mirroring solution, you need to understand and plan your environment to minimize potential effects on performance.

A variety of factors can influence the performance of geographic mirroring. The following factors provide general planning considerations for maximizing performance in a geographic mirroring environment:

CPU considerations

Geographic mirroring increases the CPU load, so there must be sufficient excess CPU capacity. You might require additional processors to increase CPU capacity. As a general rule, the partitions you are using to run geographic mirroring need more than a partial processor. In a minimal CPU configuration, you can potentially see 5 - 20% CPU overhead while running geographic mirroring. If your backup system has fewer processors in comparison to your production system and there are many write operations, CPU overhead might be noticeable and affect performance.

Base pool size considerations

If asynchronous delivery transmission is used for geographic mirroring, it may be necessary to also increase the amount of storage in the base pool of the system. The amount to increase the base pool by depends primarily on the amount of latency which occurs due to the distance between the two systems. Larger amounts of latency will require larger amounts of the base pool.

Machine pool size considerations

For optimal performance of geographic mirroring, particularly during synchronization, increase your machine pool size by at least the amount given by the following formula:

- The amount of extra machine pool storage is: $300 \text{ MB} + .3\text{MB} \times \text{the number of disk ARMs in the independent disk pool}$. The following examples show the additional machine pool storage needed for independent disk pools with 90 disk ARMs and a 180 disk ARMs, respectively:
 - $300 + (.3 \times 90 \text{ ARMs}) = 327 \text{ MB}$ of additional machine pool storage
 - $300 + (.3 \times 180 \text{ ARMs}) = 354 \text{ MB}$ of additional machine pool storage

The extra machine pool storage is required on all nodes in the cluster resource group (CRG) so that the target nodes have sufficient storage in case of switchover or failover. As always, the more disk units in the independent disk pool, the better the performance should be, as more things can be done in parallel.

To prevent the performance adjuster function from reducing the machine pool size, you should do one of the following:

1. Set the machine pool minimum size to the calculated amount (the current size plus the extra size for geographic mirroring from the formula) by using Work with Shared Storage Pools (WRKSHRPOOL) command or Change Shared Storage Pool (CHGSHRPOOL) command.

Note: It is recommended to use this option with the Work with Shared Storage Pools (WRKSHRPOOL) option.

2. Set the Automatically adjust memory pools and activity levels (QPFRADJ) system value to zero, which prohibits the performance adjuster from changing the size of the machine pool.

Disk unit considerations

Disk unit and IOA performance can affect overall geographic mirroring performance. This is especially true when the disk subsystem is slower on the mirrored system. When geographic mirroring is in a synchronous mirroring mode, all write operations on the production copy are gated by the mirrored copy writes to disk. Therefore, a slow target disk subsystem can affect the source-side performance. You can minimize this effect on performance by running geographic mirroring in asynchronous mirroring mode. Running in asynchronous mirroring mode alleviates the wait for the disk subsystem on the target side, and sends confirmation back to the source side when the changed memory page is in memory on the target side.

System disk pool considerations

Similar to any system disk configuration, the number of disk units available to the application can have a significant affect on its performance. Putting additional workload on a limited number of disk units might result in longer disk waits and ultimately longer response times to the application. This is particularly important when it comes to temporary storage in a system configured with independent disk pools. All temporary storage is written to the SYSBAS disk pool. If your application does not use a lot of temporary storage, then you can get by with fewer disk arms in the SYSBAS disk pool. You must also remember that the operating system and basic functions occur in the SYSBAS disk pool. This is also true for the mirror copy system since, in particular, the TCP messages that are sent to the mirror copy can potentially page in the system asp.

Network configuration considerations

Network cabling and configuration can potentially impact geographic mirroring performance. In addition to ensuring that network addressing is set up in different subnets for each set of data port IP addresses, network cabling and configuration should also be set up in the same manner.

Planning switched logical units (LUNs)

A single copy of the data is maintained on the logical units within the IBM® System Storage™ storage unit.

When an outage occurs on the primary node, access to the data on the switchable logical units switches to a designated backup node. Additionally, independent disk pools can be used in a cross-site mirroring (XSM) environment. This allows a mirror copy of the independent disk pool to be maintained on a system that is (optionally) geographically distant from the originating site for availability or protection purposes.

Careful planning is required if you plan to take advantage of switchable logical units residing on independent disk pools or cross-site mirroring (XSM).

You should also evaluate your current system disk configuration to determine if additional disk units may be necessary. Similar to any system disk configuration, the number of disk units available to the application can have a significant affect on its performance. Putting additional workload on a limited number of disk units might result in longer disk waits and ultimately longer response times to the application. This is particularly important when it comes to temporary storage in a system configured with independent disk pools. All temporary storage is written to the SYSBAS disk pool. If your application does not use much temporary storage, then you can get by with fewer disk arms in the SYSBAS disk pool. You must also remember that the operating system and basic functions occur in the SYSBAS disk pool.

Before you can use IBM Navigator for i to perform any disk management tasks, such as creating an independent disk pool, you need to set up the proper authorizations for dedicated service tools (DST).

Hardware requirements for switched logical units

To configure and manage an PowerHA solution that uses switched logical units technology, you should ensure that the minimum hardware requirements are met.

The following minimum hardware requirements are recommended:

- At least two IBM i partitions or systems that are separated geographically with at least one IBM System Storage external storage unit that is attached to each system. The IBM System Storage external storage units are supported on all System i models that support Fibre Channel attachment for external storage.
- PowerHA supports switched logical units (LUNs) on DS8000, SAN Volume Controller, and Storwize. For specific Fibre Channel adapters supported, see [IBM System Storage Interoperation Center \(SSIC\)](#).
- Appropriate disk sizing for the system storage should be completed before any configuration. With switched logical units you have one set of disks.

For more information on the storage technologies that are provided by IBM i, see [PowerHA supported storage servers](#).

Related information

[PowerHA SystemMirror for IBM i Cookbook](#)

[IBM System Storage DS8000 Information Center-> Copy Services](#)

[IBM i and IBM Storwize Family: A Practical Guide to Usage Scenarios](#)

[IBM SAN Volume Controller Information Center](#)

Software requirements for switched logical units

Before configuring an IBM i high-availability solution that uses switched logical units (LUNs), ensure that the minimum software requirements have been met.

Switched logical units have the following minimum software requirements:

- Each IBM i model within the high-availability solution must be running at least IBM i 7.1 for use with the IBM PowerHA SystemMirror for i licensed program.
- IBM PowerHA SystemMirror for i licensed program installed on each system participating in the high-availability solution that uses switched logical units.
- You need to install IBM i Option 41 HA Switchable Resources. Option 41 gives you the capability to switch independent disk pools between systems. To switch an independent disk pool between systems, the systems must be members of a cluster and the independent switched disk must be associated with a device cluster resource group in that cluster. Option 41 is also required for working with high availability management interfaces, which are provided as part of the IBM PowerHA SystemMirror for i licensed program.
- For DS8000 System Storage Devices, the IBM PowerHA for i licensed program also requires storage command-line interface (DSCLI). DSCLI is required software for all the IBM System Storage solutions, such as FlashCopy technology, Metro Mirror, Global Mirror, there is a requirement to have DSCLI installed each of the systems or partitions participating in the high availability solution, which uses these storage solutions. DSCLI has these additional software requirements:
 - Java Version 1.4
 - Option 35 (CCA Cryptographic Service Provider) installed on each system or partition
- For SAN Volume Controller (SVC), or Storwize System Storage Devices, the IBM PowerHA SystemMirror for i licensed program also requires the following:
 - Portable Utilities for IBM i (5733-SC1)
- Ensure that the latest PTF are installed.

For more information on the storage technologies that are provided by IBM i, see [PowerHA supported storage servers](#).

Communications requirement for Switched logical units

Before configuring a PowerHA solution that uses switched logical units, ensure that the minimum communication requirements have been met.

To use the Switched logical unit technology, you must be using or planning to use a storage area network (SAN).

A SAN is a dedicated, centrally managed, secure information infrastructure that enables any-to-any interconnection between systems and storage systems. SAN connectivity is required for using IBM System Storage.

The following are the minimum communication requirements for a PowerHA solution that uses switched logical units:

- The System i product supports various SAN switches and directors. Refer to the IBM System Storage Interoperation Center (SSIC) website, for a complete list of supported switches and directors.
- In addition, taking advantage of multipath I/O is highly recommended in order to improve overall resiliency and performance. Multipath I/O provides the ability to have multiple Fibre Channel devices that are configured to the same logical disk units within the storage. When correctly configured this allows single devices, or I/O enclosures to fail without losing connections to the disk units. Multipath also provides performance benefits by spreading workloads across all available connections (paths). Each connection for a multipath disk unit function independently. Several connections provide improved resiliency by allowing disk storage to be used even if a single path fails.
- Switched logical units require at least one TCP/IP communications interface between the systems in the cluster.

Planning the FlashCopy feature

You can use the FlashCopy feature as a means to reduce your backup window in PowerHA environments that use the external storage units of the IBM System Storage. Before using the FlashCopy feature, ensure that the minimum requirements have been met.

Hardware requirements for the FlashCopy feature

To use the FlashCopy technology in an PowerHA solution, ensure that the minimum hardware requirements are met.

The following minimum hardware requirements are needed for the FlashCopy feature:

- At least one IBM i attached to an IBM System Storage device. For a FlashCopy to a IBM i target system or partition (Where the FlashCopy target is not *NONE), both the FlashCopy source and FlashCopy target systems or partitions must be attached to the same external storage device.
- PowerHA supports FlashCopy on DS8000, SAN Volume Controller, and Storwize. For specific Fibre Channel adapters supported, see [IBM System Storage Interoperation Center \(SSIC\)](#).
- Appropriate disk sizing for the system storage should be completed before any configuration.
 - For FlashCopy with DS8000 System Storage Devices, you need one set of disks for the source, an equal set of disk units for the target, and another set for each consistency group. Space efficient FlashCopy (FlashCopy SE) can be used to reduce this disk requirement.
 - For FlashCopy with SAN Volume Controller (SVC), or Storwize System Storage Devices, you need one set of disks for the source, and an equal set of disk units for the target.

For more information about the storage technologies that are provided by IBM, see [“PowerHA supported storage servers”](#) on page 25.

Related concepts

[PowerHA supported storage servers](#)

IBM System Storage provides enhanced storage capabilities.

Related information

[PowerHA SystemMirror for IBM i Cookbook](#)

Software requirements for the FlashCopy feature

To use the FlashCopy technology in an PowerHA solution, the minimum software requirements should be met.

The FlashCopy feature has the following minimum software requirements:

- Each IBM i model within the PowerHA solution must be running at least IBM(r) iV6R1 for use with the IBM PowerHA SystemMirror for i licensed program.
Note: For prior releases, you can still use the IBM Advanced Copy Services for PowerHA on i, which is an offering from Lab Services, to work with IBM System Storage solutions.
- IBM PowerHA SystemMirror for i installed on each system.
- Ensure that the latest PTF have been installed.

Communications requirements for the FlashCopy feature

To use the FlashCopy technology in a PowerHA solution, ensure that the minimum communications requirements are met.

The following minimum communication requirements should be met for the FlashCopy feature:

- At least two IBM i partitions or systems that have at least one IBM(r) System Storage(r) external storage unit that is attached to each system. The IBM(r) System Storage(r) external storage units are supported on all System i(r) models that support Fibre Channel attachment for external storage.
- PowerHA supports Metro Mirror on DS8000, SAN Volume Controller, and Storwize. For specific Fibre Channel adapters supported, see [IBM System Storage Interoperation Center \(SSIC\)](#).

For more information on the storage technologies that are provided by IBM i, see [“PowerHA supported storage servers”](#) on page 25.

Related concepts

[PowerHA supported storage servers](#)
IBM System Storage provides enhanced storage capabilities.

Planning Metro Mirror

IBM PowerHA SystemMirror for i supports Metro Mirror, which provides high availability and disaster recovery. To effectively configure and manage a high availability solution that uses this technology, proper planning is required.

Related information

[Guidelines and recommendations for using Copy Services functions with DS8000](#)

Hardware requirements for Metro Mirror

To configure and manage an PowerHA solution that uses Metro Mirror technology, you should ensure that the minimum hardware requirements are met.

The following minimum hardware requirements are recommended:

- At least two IBM i partitions or systems that are separated geographically with at least one IBM System Storage external storage unit that is attached to each system. The IBM System Storage external storage units are supported on all System i models that support Fibre Channel attachment for external storage.
- PowerHA supports Metro Mirror on DS8000, SAN Volume Controller, and Storwize. For specific Fibre Channel adapters supported, see [IBM System Storage Interoperation Center \(SSIC\)](#).
- Appropriate disk sizing for the system storage should be completed before any configuration. You need one set of disk for the source, and an equal set of disk units for the target.

For more information on the storage technologies that are provided by IBM i, see [PowerHA supported storage servers](#).

Related information

[PowerHA SystemMirror for IBM i Cookbook](#)

[IBM System Storage DS8000 Information Center-> Copy Services](#)

[IBM i and IBM Storwize Family: A Practical Guide to Usage Scenarios](#)

[IBM SAN Volume Controller Information Center](#)

Software requirements for Metro Mirror

Before configuring an IBM i high-availability solution that uses Metro Mirror, ensure that the minimum software requirements have been met.

Metro Mirror has the following minimum software requirements:

- Each IBM i model within the high-availability solution must be running at least IBM i V6R1 for use with the IBM PowerHA SystemMirror for i licensed program.

Note: For prior releases, you can still use the IBM Advanced Copy Services for PowerHA on i, which is an offering from Lab Services, to work with IBM System Storage solutions.

- IBM PowerHA SystemMirror for i licensed program installed on each system participating in the high-availability solution that will use the mirror.
- You need to install IBM i Option 41 HA Switchable Resources. Option 41 gives you the capability to switch independent disk pools between systems. To switch an independent disk pool between systems, the systems must be members of a cluster and the independent switched disk must be associated with a device cluster resource group in that cluster. Option 41 is also required for working with high availability management interfaces, which are provided as part of the IBM PowerHA SystemMirror for i licensed program.
- For DS8000 System Storage Devices, the IBM PowerHA for i licensed program also requires storage command-line interface (DSCLI). DSCLI is required software for all the IBM System Storage solutions, such as FlashCopy technology, Metro Mirror, Global Mirror, there is a requirement to have DSCLI installed each of the systems or partitions participating in the high availability solution, which uses these storage solutions. DSCLI has these additional software requirements:
 - Java Version 1.4
 - Option 35 (CCA Cryptographic Service Provider) installed on each system or partition
- For SAN Volume Controller (SVC), or Storwize System Storage Devices, the IBM PowerHA SystemMirror for i licensed program also requires the following:
 - Portable Utilities for IBM i (5733-SC1)
- Ensure that the latest PTF have been installed.

Related information

[PowerHA SystemMirror for IBM i Cookbook](#)

[IBM System Storage DS8000 Information Center-> Copy Services](#)

[IBM i and IBM Storwize Family: A Practical Guide to Usage Scenarios](#)

Communications requirement for Metro Mirror

Before configuring PowerHA solution that uses Metro Mirror, ensure that the minimum communication requirements have been met.

To use the Metro Mirror technology, you must be using or planning to use a storage area network (SAN).

A SAN is a dedicated, centrally managed, secure information infrastructure that enables any-to-any interconnection between systems and storage systems. SAN connectivity is required for using IBM System Storage.

The following are the minimum communication requirements for a PowerHA solution that uses Metro Mirror:

- The System i product supports a variety of SAN switches and directors. Refer to the IBM System Storage Interoperation Center (SSIC) website, for a complete list of supported switches and directors.
- In addition, taking advantage of multipath I/O is highly recommended in order to improve overall resiliency and performance. Multipath I/O provides the ability to have multiple Fibre Channel devices that are configured to the same logical disk units within the storage. When correctly configured this allows single devices, or I/O enclosures to fail without losing connections to the disk units. Multipath also provides performance benefits by spreading workloads across all available connections (paths). Each connection for a multipath disk unit functions independently. Several connections provide improved resiliency by allowing disk storage to be used even if a single path fails.

Related concepts

[PowerHA supported storage servers](#)

IBM System Storage provides enhanced storage capabilities.

Related reference

[Storage area network \(SAN\) Web site](#)

Related information

[IBM SAN Volume Controller Information Center](#)

Journal planning for Metro Mirror

Journaling is important for increasing recovery time for all high availability solutions. In the case of IBM System Storage based technologies, such as Metro Mirror, it is vital that journaling be used to force write operations to external storage units, since mirroring of data occurs outside of IBM i storage.

Journal management prevents transactions from being lost if your system ends abnormally. When you journal an object, the system keeps a record of the changes you make to that object. Regardless of the high availability solution that you implement, journaling is considered a best practice to prevent data loss during abnormal system outages.

Related information

[Journal management](#)

Backup planning for Metro Mirror

With Metro Mirror, you can use the FlashCopy feature to create a copy of data stored in IBM System Storage external storage units.

FlashCopy operations provide the ability to create point-in-time copies. As soon as the FlashCopy operation is processed, both the source and target volumes are available for application use. The FlashCopy feature can be used with other IBM System Storage technologies, such as Metro Mirror and Global Mirror, to create consistent, point-in-time copy of data at a remote site, which then can be backed up with your standard backup procedures. You should complete the following before implementing the FlashCopy technology:

- Identify the source volumes and target volumes for FlashCopy relationships. You should select FlashCopy target volumes in different ranks for better performance.
- Understand FlashCopy data consistency considerations. There are environments where data is stored in system memory cache and written to disk at some later time. To avoid these types of restart actions, ensure that all data that is related to the FlashCopy source volume has been written to disk before you perform the FlashCopy operation.
- You can use an existing Metro Mirror source volume as a FlashCopy target volume. This allows you to create a point-in-time copy using a target volume of a FlashCopy pair and then mirror that data to a source Metro Mirror volume at a remote location.

Performance planning for Metro Mirror

You should understand these performance considerations prior to configuring Metro Mirror.

Before you use Metro Mirror, consider the following requirements and guidelines:

- The source and target volumes in a Metro Mirror relationship must be the same storage type.

- The source and target logical volumes must be the same size or the target must be larger in size.
- For Metro Mirror environments, distribute the work loads by not directing all updates to a small set of common volumes on a single target storage unit. The performance impact at the target site storage unit adversely affects the performance at the source site.
- Similar to any system disk configuration, the number of disk units available to the application can have a significant affect on its performance. Putting additional workload on a limited number of disk units might result in longer disk waits and ultimately longer response times to the application. This is particularly important when it comes to temporary storage in a system configured with independent disk pools. All temporary storage is written to the SYSBAS disk pool. If your application does not use a lot of temporary storage, then you can get by with fewer disk arms in the SYSBAS disk pool. You must also remember that the operating system and basic functions occur in the SYSBAS disk pool.

Related information

[Guidelines and recommendations for using Copy Services functions with DS8000](#)

Planning Global Mirror

IBM PowerHA SystemMirror for i supports Global Mirror, which provides high availability and disaster recovery in environments that use external storage solutions. To effectively configure and manage high availability that uses this technology, proper planning is required.

Related information

[Guidelines and recommendations for using Copy Services functions with DS8000](#)

Hardware requirements for Global Mirror

To configure and manage an PowerHA solution that uses Global Mirror technology, you should ensure that the minimum hardware requirements are met.

The following minimum hardware requirements should be met for Global Mirror:

- At least two IBM i partitions or systems that are separated geographically with at least one IBM System Storage external storage unit that is attached to each system. The IBM System Storage external storage units are supported on all System i models that support Fibre Channel attachment for external storage.
- PowerHA supports Global Mirror on DS8000, SAN Volume Controller, and Storwize. For specific Fibre Channel adapters supported, see [IBM System Storage Interoperation Center \(SSIC\)](#).
- Appropriate disk sizing for the system storage should be completed before any configuration. You need one set of disk for the source, and an equal set of disk units for the target and another set for each consistency copy.

For more information on the storage technologies that are provided by IBM i, see [PowerHA supported storage servers](#).

Related information

[PowerHA SystemMirror for IBM i Cookbook](#)

[IBM System Storage DS8000 Information Center-> Copy Services](#)

[IBM i and IBM Storwize Family: A Practical Guide to Usage Scenarios](#)

[IBM SAN Volume Controller Information Center](#)

Software requirements for Global Mirror

Before configuring a PowerHA solution that uses Global Mirror, ensure that the minimum software requirements have been met.

Global Mirror has the following minimum software requirements:

- Each IBM i model with in the high-availability solution must be running at least IBM i V6R1 for use with the IBM PowerHA SystemMirror for i licensed program.

Note: For prior releases, you can still use the IBM Advanced Copy Services for PowerHA on i, which is an offering from Lab Services, to work with IBM System Storage solutions. If you are using Global Mirror on

multiple platforms, or if you want to implement Global Mirror on multiple IBM i partitions, you can also use the IBM Advanced Copy Services for PowerHA on i.

- IBM PowerHA SystemMirror for i licensed program must be installed on each system participating in the high-availability solution that use Global Mirror.
- For DS8000 System Storage Devices, the IBM PowerHA for i licensed program also requires storage command-line interface (DSCLI). DSCLI is required software for all the IBM System Storage solutions, such as FlashCopy technology, Metro Mirror, Global Mirror, there is a requirement to have DSCLI installed each of the systems or partitions participating in the high availability solution, which uses these storage solutions. DSCLI has these additional software requirements:
 - Java Version 1.4
 - Option 35 (CCA Cryptographic Service Provider) installed on each system or partition
- For SAN Volume Controller (SVC), or Storwize System Storage Devices, the IBM PowerHA SystemMirror for i licensed program also requires the following:
 - Portable Utilities for IBM i (5733-SC1)
- Ensure that the latest PTF have been installed.

Related information

[PowerHA SystemMirror for IBM i Cookbook](#)

[IBM System Storage DS8000 Information Center-> Copy Services](#)

[IBM i and IBM Storwize Family: A Practical Guide to Usage Scenarios](#)

Communications requirement for Global Mirror

Before configuring a PowerHA solution that uses Global Mirror, you should ensure that the minimum communication requirements have been met.

To use the Global Mirror technology you must be using or planning to use a storage area network (SAN).

A SAN is a dedicated, centrally managed, secure information infrastructure that enables any-to-any interconnection between systems and storage systems. SAN connectivity is required for using IBM System Storage.

The following are the minimum communication requirements for a PowerHA solution that use Global Mirror:

- The System i product supports a variety of SAN switches and directors. Refer to the IBM System Storage Interoperation Center (SSIC) website, for a complete list of supported switches and directors.
- In addition, taking advantage of multipath I/O is highly recommended in order to improve overall resiliency and performance. Multipath I/O provides the ability to have multiple Fibre Channel devices that are configured to the same logical disk units within the storage. When correctly configured this allows single devices, or I/O enclosures to fail without losing connections to the disk units. Multipath also provides performance benefits by spreading workloads across all available connections (paths). Each connection for a multipath disk unit functions independently. Several connections provide improved resiliency by allowing disk storage to be used even if a single path fails.

Related concepts

[PowerHA supported storage servers](#)

IBM System Storage provides enhanced storage capabilities.

Related reference

[Storage area network \(SAN\) Web site](#)

Related information

[IBM SAN Volume Controller Information Center](#)

Journal planning for Global Mirror

Journaling is important for decreasing recovery time for all high availability solutions. In the case of IBM System Storage based technologies, such as Global Mirror, journaling forces write operations to external storage units, which is necessary because data mirroring occurs outside of IBM i storage.

Journal management prevents transactions from being lost if your system ends abnormally. When you journal an object, the system keeps a record of the changes you make to that object. Regardless of the high availability solution that you implement, journaling is considered a best practice to prevent data loss during abnormal system outages.

Related information

[Journal management](#)

Backup planning for Global Mirror

When using Global Mirror technology within your high-availability solution, you can use the FlashCopy feature to create point-in-time copy of your data.

FlashCopy operations provide the ability to create point-in-time copies. As soon as the FlashCopy operation is processed, both the source and target volumes are available for application use. The FlashCopy feature can be used with other IBM System Storage technologies, such as Metro Mirror and Global Mirror, to create consistent, point-in-time copy of data at a remote site, which then can be backed up with your standard backup procedures. You should complete the following before implementing the FlashCopy technology:

- Identify the source volumes and target volumes for FlashCopy relationships. You should select FlashCopy target volumes in different ranks for better performance.
- Understand FlashCopy data consistency considerations. There are environments where data is stored in system memory cache and written to disk at some later time. To avoid these types of restart actions, ensure that all data that is related to the FlashCopy source volume has been written to disk before you perform the FlashCopy operation.

Performance planning for Global Mirror

You should understand these performance considerations before configuring Global Mirror.

Before you use Global Mirror, consider these performance guidelines:

- The source and target volumes in a Global Mirror relationship must be the same storage type.
- The source and target logical volumes must be the same size or the target must be the same size or the target must be larger in size.
- Similar to any system disk configuration, the number of disk units available to the application can have a significant affect on its performance. Putting additional workload on a limited number of disk units might result in longer disk waits and ultimately longer response times to the application. This is particularly important when it comes to temporary storage in a system configured with independent disk pools. All temporary storage is written to the SYSBAS disk pool. If your application does not use a lot of temporary storage, then you can get by with fewer disk arms in the SYSBAS disk pool. You must also remember that the operating system and basic functions occur in the SYSBAS disk pool.

Related information

[Guidelines and recommendations for using Copy Services functions with DS8000](#)

Planning for DS8000 Full System HyperSwap

You can use HyperSwap as a means to help reduce or eliminate outages due to storage and SAN-related outages in high availability environments that use the external storage units of the IBM Systems Storage DS8000 devices.

Hardware requirements for DS8000 Full System HyperSwap

To use the DS8000 Full System HyperSwap technology in an PowerHA solution, ensure that the minimum hardware requirements are met.

The following minimum hardware requirements are needed for DS8000 Full System HyperSwap:

- One System i model/logical partition with all storage provided by two IBM System Storage DS8000 external storage units that are attached to the system.
- Two supported IBM Systems Storage DS8000. Supported IBM System Storage units:
 - DS8700 or DS8800 (with release 6.3 SP7)
 - DS8870 with release 7.2
- Appropriate disk sizing for the system storage should be completed before any configuration. You need one set of disks on the source DS8000 unit, and an equivalent sized set of disks on the target DS8000 unit.

For information on storage technologies that are provided by IBM, see [“PowerHA supported storage servers”](#) on page 25.

Software requirements for DS8000 Full System HyperSwap

To use the DS8000 Full System HyperSwap technology in an IBM i high-availability solution, the minimum software requirements must be met.

The DS8000 Full System HyperSwap feature has the following minimum software requirements:


- IBM i model must be at IBM i 7.2.
- IBM PowerHA for i Express Edition licensed program must be installed.

Communications requirements for DS8000 Full System HyperSwap

To use the DS8000 HyperSwap technology, you must be using or planning to use a storage area network (SAN).

A SAN is a dedicated, centrally managed, secure information infrastructure that enables any-to-any interconnection between systems and storage systems. SAN connectivity is required for using IBM System Storage DS8000 external storage units.

IBM i product supports various SAN switches and directors. Refer to the IBM System Storage Interoperation Center (SSIC) website, for a complete list of supported adapters, switches and directors.

See the [IBM PowerHA SystemMirror for i wiki](#)  for the specific storage version numbers needed to work on IBM i.

At least one POWER model running IBM i attached to an IBM System Storage device. For a FlashCopy to a IBM i target system or partition and the FlashCopy target is not *NONE), both the FlashCopy source and FlashCopy target systems or partitions must be attached to the same external storage device.

Related information

[IBM System Storage Interoperation Center \(SSIC\)](#)

Performance requirements for DS8000 Full System HyperSwap

You should understand these performance considerations before configuring HyperSwap.

Before you use DS8000 HyperSwap, consider the following requirements and guidelines:

- The source and target volumes in a HyperSwap relationship must be the same storage type.

- The source and target logical volumes must be the same size.
- As with any synchronous replication technology, there are distance and bandwidth limitations that can affect performance.
- Similar to any system disk configuration, the number of disk units available to the application can have a significant effect on its performance.
- Putting more workload on a limited number of disk units may result in longer disk waits and ultimately longer response times to the application.

Planning DS8000 HyperSwap with independent auxiliary storage pools (IASPs)

When planning a HyperSwap configuration with a PowerHA logical unit (LUN) switching environment and or a live partition mobility environment, the following requirements must be met.

Hardware requirements for DS8000 HyperSwap with independent auxiliary storage pools (IASPs)

To use the DS8000 HyperSwap with IASPs technology in a PowerHA solution, ensure that the following minimum hardware requirements are met.

- Two IBM i logical partitions (on the same or separate POWER servers) with all storage provided by two IBM System Storage DS8000 external storage units that are attached to the systems.
- Two supported IBM Systems Storage DS8000. Supported IBM System Storage units:
 - DS8700 or DS8800 (with release 6.3 SP7)
 - DS8870 with release 7.2
- Appropriate disk sizing for the system storage should be completed before any configuration. You need one set of disks on the source DS8870 unit, and an equivalent sized set of disks on the target DS8870 unit. To protect both partitions from storage outages, you also need extra disk to replicate SYSBAS from each system to the other. For example, if you have partitions A and B, the storage for partition A should be enough to store SYSBAS A, IASP A, and SYSBAS B (copy). The storage for partition B should be enough to store SYSBAS B, IASP B (copy), and SYSBAS A (copy).

For information on storage technologies that are provided by IBM, see [“PowerHA supported storage servers” on page 25](#).

Software requirements for DS8000 HyperSwap with independent auxiliary storage pools (IASPs)

To use the DS8000 HyperSwap technology with IASPs in an IBM i high-availability solution, the minimum software requirements must be met.

The IASP-based HyperSwap has the following minimum software requirements:


- Both IBM i partitions must be at IBM i 7.2 at Technology Refresh (TR) 4 or at IBM i 7.3.
- IBM PowerHA for i Enterprise Edition licensed program must be installed on both partitions, with the latest HA Group PTF installed.
- The PowerHA product requires IBM i Option 41 HA Switchable Resources as a prerequisite.
- For PowerHA to interact with the DS8870 System Storage device, the storage command-line interface (DSCLI) is required. DSCLI has these additional software requirements:
 - Java Version 1.4 (or higher)
 - Option 35 (CCA Cryptographic Service Provider) installed on each system or partition
- Before you can use IBM Navigator for i to perform any disk management tasks you need to set up the proper authorizations for dedicated service tools (DST).

Communications requirements for DS8000 HyperSwap with independent auxiliary storage pools (IASPs)

To use the DS8000 HyperSwap technology, you must be using or planning to use a storage area network (SAN).

A SAN is a dedicated, centrally managed, secure information infrastructure that enables any-to-any interconnection between systems and storage systems. SAN connectivity is required for using IBM System Storage DS8000 external storage units.

IBM i product supports various SAN switches and directors. Refer to the [IBM System Storage](#)

[Interoperation Center \(SSIC\)](#)  website for a complete list of supported adapters, switches, and directors.

Taking advantage of multipath I/O is highly recommended in order to improve overall resiliency and performance. Multipath I/O provides the ability to have multiple Fibre Channel devices that are configured to the same logical disk units within the storage. When correctly configured, this allows single devices, or I/O enclosures to fail without losing connections to the disk units. Multipath I/O also provides performance benefits by spreading workloads across all available connections (paths). Each connection for a multipath disk unit functions independently. Several connections provide improved resiliency by allowing disk storage to be used even if a single path fails.

Journal planning for DS8000 HyperSwap with independent auxiliary storage pools (IASPs)

Journaling is important for improved recovery time for all high availability solutions, and is highly recommended. In the case of IBM System Storage based technologies, such as HyperSwap, it is vital that journaling be used to force write operations to external storage units, since mirroring of data occurs outside of IBM i storage.

Journal management prevents transactions from being lost if your system ends abnormally. When you journal an object, the system keeps a record of the changes you make to that object. Regardless of the high availability solution that you implement, journaling is considered a best practice to prevent data loss during abnormal system outages.

Backup planning for DS8000 HyperSwap with independent auxiliary storage pools (IASPs)

With HyperSwap, you can use the FlashCopy feature to create a copy of data that is stored in IBM System Storage external storage units.

FlashCopy operations provide the ability to create point-in-time copies. As soon as the FlashCopy operation is processed, both the source and target volumes are available for application use. The FlashCopy feature can be used with other IBM System Storage technologies, such as Metro Mirror and Global Mirror, to create consistent, point-in-time copy of data at a remote site, which then can be backed up with your standard backup procedures. You should complete the following before implementing the FlashCopy technology:

- Identify the source volumes and target volumes for FlashCopy relationships. You should select FlashCopy target volumes in different ranks for better performance.
- Understand FlashCopy data consistency considerations. There are environments where data is stored in system memory cache and written to disk at some later time. To avoid these types of restart actions, ensure that all data that is related to the FlashCopy source volume has been written to disk before you perform the FlashCopy operation.
- You can use an existing HyperSwap source volume as a FlashCopy target volume. Select this option to create a point-in-time copy that uses a target volume of a FlashCopy pair and then mirror that data to a source HyperSwap volume at a remote location.

Performance requirements for DS8000 HyperSwap with independent auxiliary storage pools (IASPs)

You should understand these performance considerations before configuring HyperSwap.

Before you use HyperSwap, consider the following requirements and guidelines:

- The source and target volumes in a HyperSwap Metro Mirror relationship must be the same storage type.
- The source and target logical volumes must be the same size.
- As with any synchronous replication technology, there are distance and bandwidth limitations that can affect performance.
- Similar to any system disk configuration, the number of disk units available to the application can have a significant affect on its performance. Putting more workload on a limited number of disk units may result in longer disk waits and ultimately longer response times to the application. This is important when it comes to temporary storage in a system configured with IASPs. All temporary storage is written to the SYSBAS disk pool. If your application does not use a lot of temporary storage, then you can get by with fewer disk arms in the SYSBAS disk pool. Remember, the operating system and basic functions occur in the SYSBAS disk pool.

Planning HyperSwap with Global Mirror

For LUN level switching, MetroMirror, GlobalMirror, DS8000 with IASPs you may use Copy Services Manager (CSM) to control your storage devices. CSM requires a CSM server For more information about CSM visit the Knowledge Center for Copy Services Manager.

Security planning for high availability

Prior to configuring your high-availability solution, you should reassess the current security strategies in your environment and make any appropriate changes to facilitate high availability.

Distributing cluster-wide information

Learn about the security implications of using and managing cluster-wide information.

The `Distribute Information (QcstDistributeInformation)` API can be used to send messages from one node in a cluster resource group recovery domain to other nodes in that recovery domain. This can be useful in exit program processing. However, it should be noted that there is no encryption of that information. Secure information should not be sent with this mechanism unless you are using a secure network.

Non persistent data can be shared and replicated between cluster nodes by using the Clustered Hash Table APIs. The data is stored in non persistent storage. This means the data is retained only until the cluster node is no longer part of the clustered hash table. These APIs can only be used from a cluster node that is defined in the clustered hash table domain. The cluster node must be active in the cluster.

Other information distributed by using cluster messaging is similarly not secured. This includes the low level cluster messaging. When changes are made to the exit program data, there is no encryption of the message containing that data.

Considerations for using clusters with firewalls

If you are using clustering in a network that uses firewalls, you should be aware of some limitations and requirements.

If you are using clustering with a firewall, you need to give each node the ability to send outbound messages to and receive inbound messages from other cluster nodes. An opening in the firewall must exist for each cluster address on each node to communicate with every cluster address on every other node. IP packets traveling across a network can be of various types of traffic. Clustering uses ping, which is type ICMP, and also uses UDP and TCP. When you configure a firewall, you can filter traffic based on the type. For clustering to work the firewall needs to allow traffic of ICMP, UDP and TCP. Outbound traffic can be sent on any port and inbound traffic is received on ports 5550 and 5551.

In addition, if you are making use of advanced node failure detection, any cluster node that is to receive failure messages from a Hardware Management Console (HMC) or a Virtual I/O Server (VIOS) on an Integrated Virtualization Manager (IVM) managed server must be able to communicate with that HMC or VIOS partition. The cluster node will send to the HMC or VIOS on the IP address that is associated with the HMC's or VIOS domain name and to port 5989. The cluster node will receive from the HMC or VIOS on the IP address that is associated with the cluster node's system name and on port 5989.

Maintaining user profiles on all nodes

You can use two mechanisms for maintaining user profiles on all nodes within a cluster.

In a high-availability environment, a user profile is considered to be the same across systems if the profile names are the same. The name is the unique identifier in the cluster. However, a user profile also contains a user identification number (UID) and group identification number (GID). To reduce the amount of internal processing that occurs during a switchover, where the independent disk pool is made unavailable on one system and then made available on a different system, the UID and GID values should be synchronized across the recovery domain for the device CRG. Administrative Domain can be used to synchronize user profiles, including the UID and GID values, across the cluster.

One mechanism is to create a cluster administrative domain to monitor shared resources across nodes in a cluster. A cluster administrative domain can monitor several types of resources in addition to user profiles, providing easy management of resources that are shared across nodes. When user profiles are updated, changes are propagated automatically to other nodes if the cluster administrative domain is active. If the cluster administrative domain is not active, the changes are propagated after the cluster administrative domain is activated. This method is recommended because it automatically maintains user profiles with a high-availability environment.

With the second mechanism, administrators can also use Management Central in IBM Navigator for i to perform functions across multiple systems and groups of systems. This support includes some common user-administration tasks that operators need to perform across the multiple systems in their cluster. With Management Central, you can perform user profile functions against groups of systems. The administrator can specify a post-propagation command to be run on the target systems when creating a user profile.

Important:

- If you plan to share user profiles that use password synchronization within a cluster, you must set the Retain Server Security (QRETSVRSEC) system value to 1.
- If you change QRETSVRSEC to 0 after you add a monitored resource entry (MRE) for a user profile, and then change a password (if password is being monitored), the global status for the MRE is set to Inconsistent. The MRE is marked as unusable. Any changes made to the user profile after this change are not synchronized. To recover from this problem, change QRETSVRSEC to 1, remove the MRE, and add the MRE again.

Related tasks

Creating a cluster administrative domain

In a high-availability solution, the cluster administrative domain provides the mechanism that keeps resources synchronized across systems and partitions within a cluster.

Planning for PowerHA policies

PowerHA policies are designed to modify the behavior of the High Availability (HA) environment

In an environment running IBM PowerHA SystemMirror for i, PowerHA policies establish actions and capabilities that PowerHA uses when processing instructions. These policies provide a single point of control for the administration of changes to operations. Each policy has a name with additional information that identifies the individual policy, including the domain, such as the name of an administrative domain, or a cluster resource group (CRG) that the policy controls. Policies contain qualifiers that identify the individual instance of that policy and extend or limit the scope of the policy's management functions.

There are different types of PowerHA policies based on the behaviors modified. These are:

- administrative domain policies control and modify the configuration parameters associated with the operating environment.
- CRG policies configure the resources used to manage the high availability environment.
- communication policies control the parameters that configure the communication connections between the systems in the cluster environment.

Regardless of the policy type, all PowerHA policies require some common information, including:

- the name of the policy.
- a domain name, specifying the domain to which the policy applies. For example, for an administrative domain policy, the policy domain is the name of the administrative domain; for a CRG policy, the policy domain is the name of the CRG.

Policies can require additional values to differentiate it from other policies in the domain or to supply information unique to the individual policy. For more information about setting up or using HA policies visit the [Adding HA policies](#) and [Managing HA policies](#) pages of the Knowledge Center.

PowerHA policies for cluster administrative domain resources

Easily manage adding, deleting, and restoring resources to nodes in the cluster administrative domain using PowerHA policies

In an environment running IBM PowerHA SystemMirror for i, PowerHA policies for cluster administrative domain resources provide users with a single point of control for management of resources in the administrative domain. Resources that were added manually or using scripts calling the **ADDCADMRE** command now can be created and managed automatically with the PowerHA policies for the cluster administrative domain resources.

The PowerHA policies for administrative domain resources are:

QCST_AD_CREATE

The QCST_AD_CREATE policy specifies which resources will be automatically added to the specified cluster administrative domain when the resource is created. Normally, resources must be manually added to the cluster administrative domain after they are created. If a QCST_AD_CREATE policy is specified for a resource type and a resource of that type is created, a monitored resource entry (MRE) will be automatically created for the resource. This MRE will monitor all of the attributes for the resource.

QCST_AD_DELETE

The QCST_AD_DELETE policy automates and simplifies management of the removal of monitored resources and their respective MREs from a cluster. If an administrative domain uses the QCST_AD_DELETE policy with its monitored resources, then a resource deleted on one node of the cluster administrative domain can be deleted on all other active cluster nodes. Once the resource has been deleted on all cluster nodes, the MRE for the resource is also removed from the cluster administrative domain.

QCST_AD_RESTORE

The QCST_AD_RESTORE high availability policy streamlines resource attribute updates when restoring monitored resources. Normally, resources with a MRE in the cluster administrative domain which are restored are immediately updated to match the attribute values in the cluster administrative domain, essentially ignoring the restore operation. The QCST_AD_RESTORE policy specifies which resources, or resource types will honor restore operations in the specified cluster administrative domain. When the QCST_AD_RESTORE policy is specified the restored version of the attribute values will be propagated to other nodes in the cluster administrative domain.

The QCST_AS_RESTORE PowerHA policy only applies to MREs that exist in the administrative domain at the time of the restore. MREs are not added to the administrative domain as a result of this policy.

Configuring a PowerHA policy for administrative domain resources

Each PowerHA administrative domain resource policy is defined by the cluster administrative domain name specified in the domain name field and the resource type specified in the **RSCTYPE** keyword in the policy qualifier field. The name of any defined cluster administrative domain resource type may be specified. In addition the special value *ALL can be specified for the resource type, indicating all resource types supported by that policy.

When configuring a PowerHA policy for the cluster administrative domain you need:

- a specific PowerHA policy name, for example, QCST_AD_CREATE.
- the name of the administrative domain the policy will apply to.
- the names of the resource type or types that the policy will create resource entries for.
- **Note:** depending on the type, you may require a list of libraries.

With this information available, you can create or configure an PowerHA policy in your admin domain.

The PowerHA administrative domain resource policies qualifiers and values

PowerHA policies for administrative domain resources contain policy qualifiers designated as resource types (RSCTYPE). Supported resource types and the associated policy values are listed in Table 1 below:

Table 7. Table of qualifier resource types and their possible policy values

Policy qualifier	Policy value	Notes
RSCTYPE(*ALL)	<ul style="list-style-type: none"> • LIB(*ALL) • LIB(NAME1 NAME2...) 	
RSCTYPE(*ASPDEV)	*BLANK	
RSCTYPE(*AUTL)	*BLANK	
RSCTYPE(*CLS)	<ul style="list-style-type: none"> • LIB(*ALL) • LIB(NAME1 NAME2...) 	
RSCTYPE(*ENVVAR)	*BLANK	This resource type is supported by QCST_AD_DELETE only
RSCTYPE(*ETHLIN)	*BLANK	
RSCTYPE(*JOB)	<ul style="list-style-type: none"> • LIB(*ALL) • LIB(NAME1 NAME2...) 	
RSCTYPE(*OPTDEV)	*BLANK	
RSCTYPE(*PRTDEV)	*BLANK	
RSCTYPE(*SBSD)	<ul style="list-style-type: none"> • LIB(*ALL) • LIB(NAME1 NAME2...) 	
RSCTYPE(*TAPDEV)	*BLANK	
RSCTYPE(*USTPRF)	*BLANK	

Policy value definitions.

LIB(*ALL)

indicating that the resource type can be created in any library.

***BLANK**

indicating that the resource type does not require any library.

LIB(NAME1 NAME2...)

using only resources contained in the specified libraries.

Important:

1. If LIB(*ALL) is specified with the RSCTYPE(*ALL) policy qualifier the policy will cover all resource types, whether or not the resource type requires a library.
2. Objects restored to the system are not covered under the QCST_AD_CREATE PowerHA policy.
3. The QCST_AD_CREATE policy only affects resources created on active cluster nodes in a cluster that is not partitioned.

Examples

This example defines an instance of the QCST_AD_CREATE PowerHA policy used in the policy domain, ADMINDMN:

```
ADDHAPCY PCY(QCST_AD_CREATE) PCYDMN(ADMINDMN) QUAL('RSCTYPE(*ASPDEV)') VALUE(*BLANK)
```

This policy ensures that when a resource type (RSCTYPE) of ASP device description is created in policy domain, a MRE assigned to it is created in the administrative domain ADMINDMN.

QCST_CRG_CANCEL_FAILOVER PowerHA policy

Automatically prevent a failover operation in a CRG

The QCST_CRG_CANCEL_FAILOVER policy can prevent some failovers from taking place.

Each QCST_CRG_CANCEL_FAILOVER policy is uniquely defined by the cluster resource group name specified in the domain name field, the failover scope specified in the **SCOPE** keyword in the policy qualifier field, and an EVENT value for the policy value field.

To add a QCST_CRG_CANCEL_FAILOVER policy to a cluster resource group (CRG) supply:

- the name of the CRG.
- The policy qualifier value for the **SCOPE** policy qualifier. These values are:
 - *SITE**
indicating that the policy will apply only to failovers where the new primary node is in the same site as the original primary node.
 - *CRSSITE**
indicating that the policy will apply only to failovers where the new primary node is in a different site than the current primary node.
 - *BOTH**
indicating that the policy applies to all failovers regardless of where the current and new primary nodes are located.
- The policy value field requires a value for the Event. The Event contains a list of event types the QCST_CRG_CANCEL_FAILOVER should cancel. At least one value needs to be specified. Values for EVENT are:
 - *CLUFAIL**
The failover was caused by one of the following cluster events:
 - a **CHGCLURCY(*END)** ending the RGM or CCTL jobs.
 - a critical job end
 - a node in the cluster crashed.
 - *CRGFAIL**
The failover was caused by one of the following cluster events:
 - a **CHGCLURCY(*END)** ending jobs other than the RGM or CCTL jobs.
 - a CRG job end

- a node in the cluster crashed.

***ENDCLUNOD**

The failover was caused by the **ENDCLUNOD** command.

***ENDSYS**

The failover was caused by an **ENDSYS** or an **ENDSBS (*ALL)** action on the primary cluster node.

***ENDTCP**

The failover was caused by invoking the **ENDTCP** command on the primary cluster node.

***PWRDWSYS**

The failover was caused by the **PWRDWSYS** command.

***ALL**

All actions listed in the above values that cause failovers.

For example, a QCST_CRG_CANCEL_FAILOVER policy set for a CRG named CRG1 created:

```
CRG1: SCOPE(*SITE) EVENT(ENDTCP)
```

Indicates that if a failover is being attempted due to an ENDTCP on the primary node, and the first backup node is in the same site that the failover occurs in, that failover should be canceled.

The PowerHA QHA_COMM_STRICT_CERT_CHECK high availability policy

Control security behavior in your high availability network

The PowerHA policy, QHA_COMM_STRICT_CERT_CHECK controls the configuration of security settings governing communication between PowerHA and a storage device using IBM Copy Services Manager (CSM). If enabled, PowerHA uses the information contained in the CSM high availability configuration description to establish a secure connection.

To add the QHA_COMM_STRICT_CERT_CHECK policy to a PowerHA environment you will need to have:

- a CSM communication environment with the storage device.
- the names of the HA configuration description or descriptions for the Policy Qualifier field.
- a policy value to indicate if communication with storage devices requires strict certificate validation or if this security is not to be used.
 - *YES specifies that strict certification validation is enforced. This is the default value if the policy is not specified.
 - *NO specifies that strict certification is not used in the policy. PowerHA will ignore untrusted certificates, such as self-signed certificates, or expired certificate errors when communicating with CSM.

For example, to add a policy to the PowerHA environment to not require strict certification validation in communications with the CSM storage device on the network, enter:

```
ADDHAPCY PCY(QHA_COMM_STRICT_CERT_CHECK) PCYDMN(*NONE) QUAL('c:fgd(test)') VALUE(*NO)
```

this creates a policy using your HA configuration description that turns off the strict certification validation requirements.

Implementing PowerHA

The task-based approach to configuring and managing IBM i high availability allows you to configure and manage a customized high-availability solution that is based on your business needs. Graphical and command-line interfaces are used for configuring and managing your high-availability solution.

The task-based approach gives the knowledgeable user the means to customize and implement a personalized solution.

PowerHA graphical interface

The PowerHA graphical interface allows you to configure and manage cluster technologies, which are integral to a high-availability solution. To use this interface, the PowerHA licensed program must be installed. With this interface you can perform the following functions from any node in the cluster:

- Create and manage a cluster
- Create and manage nodes
- Create and manage cluster resource groups
- Create and manage cluster administrative domains
- Create and manage monitored resources
- Create and manage independent ASPs
- Configure and manage geographic mirroring
- Configure and manage Metro Mirror
- Configure and manage Global Mirror
- Configure and manage FlashCopy
- Monitor the status of your high availability solution
- Perform cluster related operations, such as switchovers for planned outages

Disk Management interface

The Disk Management interface allows you to configure and manage independent disk pools which are necessary when implementing several data resiliency technologies. Depending on the type of data resiliency technology that is implemented, installation requirements might be necessary to use some of these functions:

- Create a disk pool
- Make a disk pool available
- Make a disk pool unavailable
- Configure geographic mirroring

PowerHA command-line interface

The command-line interface allows you to perform many different high availability tasks with CL commands. For each cluster-related task, the corresponding CL command has been identified.

PowerHA application programming interface

These application programming interfaces (APIs) allow you to work with PowerHA version, and retrieve PowerHA related information.

Related information

[PowerHA commands](#)

[PowerHA APIs](#)

Configuring high availability infrastructure

Before you can configure a high-availability solution in your IBM i environment, ensure that you have completed the appropriate planning and understand your resources and goals for high availability and disaster recovery. Use configuration scenarios for high availability and tasks that are associated with high availability technologies to create your own high-availability solution.

Setting up TCP/IP for high availability

Because cluster resource services uses only IP to communicate with other cluster nodes, which are systems or logical partitions within a high availability environment, all cluster nodes must be IP-reachable, which means that you must have IP interfaces configured to connect the nodes in your cluster.

IP addresses must be set up either manually by the network administrator in the TCP/IP routing tables on each cluster node or they might be generated by routing protocols running on the routers in the network. This TCP/IP routing table is the map that clustering uses to find each node; therefore, each node must have its own unique IP address.

Each node can have up to two IP addresses assigned to it. These addresses must not be changed in any way by other network communications applications. Be sure when you assign each address that you take into account which address uses which kind of communication line. If you have a preference for using a specific type of communication media, make sure that you configure the first IP address by using your preferred media. The first IP address is treated preferentially by the reliable message function and heartbeat monitoring. Every cluster IP address on every node must be able to reach every other IP address in the cluster. If any cluster node uses an IPv4 address, then every node in the cluster needs to have an active IPv4 address (not necessarily configured as a cluster IP address) that can route to and send TCP packets to that address. Also, if any cluster node uses an IPv6 address, then every node in the cluster needs to have an active IPv6 address (not necessarily configured as a cluster IP address) that can route to and send TCP packets to that address. One way to verify that one address can reach another address is if you can ping and use a UDP message trace route in both directions; however, PING and TRACEROUTE do not work between IPv4 and IPv6 addresses, or if a firewall is blocking them.

Note: You need to be sure that the loopback address (127.0.0.1) is active for clustering. This address, which is used to send any messages back to the local node, is normally active by default. However, if it has been ended by mistake, cluster messaging cannot function until this address has been restarted.

Setting TCP/IP configuration attributes

To enable cluster resource services, certain attribute settings are required in the TCP/IP configuration of your network.

You must set these attributes before you can add any node to a cluster:

- Set IP datagram forwarding to *YES by using the **CHGTCPA (Change TCP/IP Attributes)** command if you plan to use a System i product as the router to communicate with other networks and you have no other routing protocols running on that server.
- Set the INETD server to START. See “Starting the INETD server” on page 50 for information about starting the INETD server.
- Set User Datagram Protocol (UDP) CHECKSUM to *YES using the **CHGTCPA (Change TCP/IP Attributes)** command.
- Set MCAST forwarding to *YES if you are using bridges to connect your token ring networks.
- If you are using OptiConnect for IBM i to communicate between cluster nodes, start the QSOC subsystem by specifying STRSBS(QSOC/QSOC).

Starting the INETD server

The Internet Daemon (INETD) server must be started in order for a node to be added or started, as well as for merge partition processing.

It is recommended that the INETD server always be running in your cluster.

You can start the INETD server through IBM Navigator for i by completing the following steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. In the navigation tree, expand **i5/OS Management** and select **Network**.
4. On the Network page, select **TCP/IP Servers**. A list of available TCP/IP servers is displayed.
5. From the list, select **INETD**.

6. From the **Select Action** menu, select **Start**. The status of the server changes to **Started**.

Alternatively, you can start the INETD server by using the Start TCP/IP Server (STRTCPSVR) command and specifying the SERVER(*INETD) parameter. When the INETD server is started, a User QTCP (QTOGINTD) job is present in the Active Jobs list on the node.

Related reference

[STRTCPSVR \(Start TCP/IP Server\) command](#)

Configuring clusters

Any IBM i implementation of high availability requires a configured cluster to control and manage resilient resources. When used with other data resiliency technologies, such as switched disk, cross-site mirroring, or logical replication, cluster technology provides the key infrastructure that is necessary for high-availability solutions.

Cluster resource services provides a set of integrated services that maintain cluster topology, perform heartbeat monitoring, and allow creation and administration of cluster configuration and cluster resource groups. Cluster resource services also provides reliable messaging functions that keep track of each node in the cluster and ensures that all nodes have consistent information about the state of cluster resources. The Cluster Resource Service graphical user interface, which is part of the IBM PowerHA SystemMirror for i (IHASM) licensed program number (5770-HAS), allows you to configure and manage clusters within your high-availability solution. In addition, the licensed program also provides a set of control language (CL) commands that will allow you to work with cluster configurations.

There is also application program interfaces (APIs) and facilities that can be used by application providers or customers to enhance their application availability.

In addition to these IBM technologies, high availability business partners provide applications that use clusters with logical replication technology.

Creating a cluster

To create a cluster, you need to include at least one node in the cluster and you must have access to at least one of the nodes that will be in the cluster.

If only one node is specified, it must be the system that you are currently accessing. For a complete list of requirements for creating clusters, see the [“Planning checklist for clusters ”](#) on page 20.

If you will be using switchable devices in your cluster or by using cross-site mirroring technologies to configure a high-availability solution, there are additional requirements. See [Scenarios: Configuring high availability solutions](#) for several configuration examples of high-availability solutions which use these technologies. Each scenario provides step-by-step configuration tasks and an overview of outage coverage this solution provides. You can use these examples to configure your high-availability solution or customize them to suit your needs.

Use the following steps to create a cluster using the PowerHA graphical interface:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, select **Create a new cluster**.
5. Follow the instructions in the Create Cluster wizard to create the cluster.

After you create the new cluster, the Welcome page changes to display the name of the cluster at the top of the page. The Welcome page lists several tasks for working with clusters.

After you have created a cluster you need to add any additional nodes and create CRGs.

Related information

[Create Cluster \(CRTCLU\) command](#)

[Create Cluster \(QcstCreateCluster\) API](#)

Enabling nodes to be added to a cluster

Before you can add a node to a cluster, you need to set a value for the Allow add to cluster (ALWADDCLU) network attribute.

Use the **Change Network Attributes (CHGNETA)** command on any server that you want to set up as a cluster node. The **CHGNETA** command changes the network attributes of a system. The ALWADDCLU network attribute specifies whether a node allows another system to add it as a node in a cluster.

Note: You must have *IOSYSCFG authority to change the network attribute ALWADDCLU.

Possible values follow:

***SAME**

The value does not change. The system is shipped with a value of *NONE.

***NONE**

No other system can add this system as a node in a cluster.

***ANY**

Any other system can add this system as a node in a cluster.

***RQSAUT**

Any other system can add this system as a node in a cluster only after the cluster add request has been authenticated.

The ALWADDCLU network attribute is checked to see if the node that is being added is allowed to be part of the cluster and whether to validate the cluster request through the use of X.509 digital certificates. A *digital certificate* is a form of personal identification that can be verified electronically. If validation is required, the requesting node and the node that is being added must have the following installed on the systems:

- IBM i Option 34 (Digital Certificate Manager)
- IBM i Option 35 (CCA Cryptographic Service Provider)

When *RQSAUT is selected for the ALWADDCLU, the certificate authority trust list for the IBM i cluster security server application must be correctly set up. The server application identifier is QIBM_QCST_CLUSTER_SECURITY. At a minimum, add certificate authorities for those nodes that you allow to join the cluster.

Adding nodes

The IBM i PowerHA graphical interface allows you to create a cluster with multiple nodes. After the cluster has been created you may add additional nodes through an active node in the cluster. A cluster can contain up to 128 nodes.

Use the following steps to add a node to an existing cluster using the PowerHA graphical interface:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Nodes**.
5. On the **Cluster Nodes** tab, select **Add Cluster node ...** from the **Select Action** menu.
6. Specify the required information and click **OK**.

Starting nodes

Starting a cluster node activates clustering and cluster resource services on a node in an IBM i high availability environment.

A node can start itself and is able to rejoin the current active cluster, provided it can find an active node in the cluster.

To start clustering on a node using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.

3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Nodes**.
5. On the **Cluster Nodes** page, select **Start** from the context menu of the node you want to start.

Adding a node to a device domain

A device domain is a subset of nodes in a cluster that shares device resources.

If you are implementing a high-availability solution that contains independent disk pools-based technologies, such as switched disk or cross-site mirroring, you must define the node as a member of a device domain. After you add the node to a device domain, you can create a device cluster resource group (CRG) that defines the recovery domain for the cluster. All nodes that will be in the recovery domain for a device CRG must be in the same device domain. A cluster node can belong to only one device domain.

To create and manage device domains, you must have PowerHA Option 41 (HA Switchable Resources) installed. A valid license key must exist on all cluster nodes in the device domain.

The PowerHA graphical interface simplifies device domain management by ensuring that the required nodes are in a device domain when a device CRG is created or when a node is added to a device CRG.

To add a node to a device domain using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click **Cluster Nodes**.
5. On the **Cluster Nodes** page, select **Properties ...** from the context menu of the node you want to add to a device domain.
6. Click **Edit** in the General section of the **Properties** page.
7. Specify the name of the device domain to which you want to add the node in the **Device Domain** field and click **Save**.

Creating cluster resource groups (CRGs)

Cluster resource groups (CRGs) manage high availability resources, such as applications, data, and devices. Each CRG type manages the particular type of resource in a high-availability environment.

The PowerHA graphical interface allows you to create different CRGs for management of your high availability resources. Each CRG type can be used separately or in conjunction with other CRGs. For example, you may have a stand-alone business application that requires high availability. After you have enabled the application for high availability, you can create CRGs to help manage availability for that application.

If you want only an application, not its data to be available in the event of an outage, you can create an application CRG. However, if you want to have both the data and application available, you can store both within an independent disk pool, which you can define in a device CRG. If an outage occurs, the entire independent disk pool is switched to a backup node, making both the application and its data available.

Creating application CRGs

If you have applications in your high-availability solution that you want to be highly available, you can create an application cluster resource group (CRG) to manage failovers for that application.

You can specify to allow an active takeover IP address when you create the application CRG. When you start an application CRG that allows for an active takeover IP address, the CRG is allowed to start.

To create an application CRG using the PowerHA graphical interface, complete the following steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Resource Groups**.

5. On the **Cluster Resource Group** page, select **Create Cluster Resource Group ...** from the **Select Action** menu.
6. Follow the instructions in the **Create Cluster Resource Group** wizard to create an application CRG.

Creating data CRGs

Data cluster resource groups (CRGs) are primarily used with logical replication applications, which are provided by several high availability Business Partners. If you are implementing a high-availability solution based on logical replication you can create a data CRG to assist the replication of data between primary and backup nodes.

To create a data CRG PowerHA graphical interface, complete the following steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Resource Groups**.
5. On the **Cluster Resource Group** page, select **Create Cluster Resource Group ...** from the **Select Action** menu.
6. Follow the instructions in the Create Cluster Resource Group wizard to create a data CRG.

Creating device CRGs

A device cluster resource group (CRG) is made up of a pool of hardware resources that can be switched as an entity. To create switchable devices within a high-availability solution, the nodes that use these devices need to be a part of a device CRG.

Prior to creating a device CRG, add all nodes that will share a switchable resource to a device domain. The PowerHA graphical interface simplifies this by ensuring that the required nodes are in a device domain when creating a device CRG.

To create a device CRG using the PowerHA graphical interface, complete the following steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Resource Groups**.
5. On the **Cluster Resource Group** page, select **Create Cluster Resource Group ...** from the **Select Action** menu.
6. Follow the instructions in the **Create Cluster Resource Group** wizard to create a device CRG.

Creating peer CRGs

You can create a peer CRG to define node roles in load-balancing environments.

To create a peer CRG in a cluster using the PowerHA graphical interface, complete the following steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Resource Groups**.
5. On the **Cluster Resource Group** page, select **Create Cluster Resource Group ...** from the **Select Action** menu.
6. Follow the instructions in the Create Cluster Resource Group wizard to create a peer CRG.

Starting a CRG

Starting a cluster resource group (CRG) enables resilience for the CRG.

To start a CRG using the PowerHA graphical interface, complete the following steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.

2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Resource Groups**.
5. On the **Cluster Resource Group** page, select **Start** from the context menu of the CRG you want to start.

Related information

[Start Cluster Resource Group \(STRCRG\) command](#)

[Create Cluster Resource Group \(QcstCreateClusterResourceGroup\) API](#)

Specifying message queues

You can either specify a cluster message queue or a failover message queue. These message queues help you determine causes of failures in your PowerHA environment.

A cluster message queue is used for cluster-level messages and provides one message, which controls all cluster resource groups (CRGs) failing over to a specific node. A failover message queue is used for CRG-level messages and provides one message for each CRG that is failing over.

Specifying a cluster message queue

Note: You can also configure a cluster to use a cluster message queue by specifying the message queue while running the Create Cluster wizard.

To specify a cluster message queue using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, select **Properties ...** from the **Select Action** menu.
5. Click **Edit** in the Advanced section of the **Properties** page.
6. Specify the cluster message queue information in the **Cluster Message Queue** field and click **Save**.

Specifying a failover message queue

To specify a failover message queue using the PowerHA graphical interface, complete these steps:

1. In a web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the IBM Navigator for i window.
4. On the **PowerHA** page, click **Cluster Resource Groups**.
5. On the **Cluster Resource Group** page, select **Properties ...** from the context menu of the CRG for which you want a failover message queue.
6. Click **Edit** in the Advanced section of the **Properties** page.
7. Specify the failover message queue information in the **Failover Message Queue** field and click **Save**.

Related information

[Create cluster](#)

[Create cluster resource group](#)

[Change cluster resource group](#)

Performing switchovers

Switchovers can be performed to test the high availability solution or to handle a planned outage for the primary node, such as a backup operation or scheduled system maintenance.

Performing a manual switchover causes the current primary node to switch over to the first backup node. The recovery domain of the cluster resource group defines these roles. When a switchover occurs, the roles of the nodes that are currently defined in the recovery domain change such that:

- The current primary node is assigned the role of last active backup.
- The current first backup is assigned the role of primary node.
- Subsequent backups are moved up one in the order of backups.

A switchover is only allowed on application, data, and device CRGs that have a status of Active.

Note: If you are performing a switchover on a device CRG, you should synchronize the user profile name, UID, and GID for performance reasons. Cluster administrative domain simplifies synchronization of user profiles.

To perform a switchover using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Click **PowerHA** from the IBM Navigator for i window.
3. On the **PowerHA** page, click on **Cluster Resource Groups**.
4. On the **Cluster Resource Groups** page, select **Switchover ...** from the context menu of the CRG that you want to switchover.
5. Click **OK** on the confirmation panel.

The selected cluster resource group is now switched to the backup node. The Status column is updated with the new node name.

There is another way to perform a switchover of a CRG that is managing an Independent ASP using the PowerHA graphical interface:

To perform a switchover using the PowerHA[®] graphical interface, follow these steps:

1. In a web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details ...** from the context menu of the Independent ASP managed by the device CRG that you want to switchover.
6. On the **Independent ASPs Details** page, select **Switch within Site...** or **Make Production Copy...** from the context menu of the Independent ASP, depending upon which kind of switchover you want to perform.
7. Click **OK** on the confirmation panel.

Related concepts

[Cluster administrative domain](#)

Related tasks

[Configuring cluster administrative domains](#)

In a high-availability environment, it is necessary that the application and operational environment remain consistent among the nodes that participate in high availability. Cluster administrative domain is the PowerHA implementation of environment resiliency and ensures that the operational environment remains the consistent across nodes.

Related information

[Change Cluster Resource Group Primary \(CHGCRGPRI\) command](#)

[Initiate Switchover \(QcstInitiateSwitchOver\) API](#)

Configuring nodes

Nodes are systems or logical partitions that are participating in an IBM i high availability solution.

There are several tasks related to node configuration. When you use the Create Cluster wizard, you can configure a simple two-node cluster. You can add additional nodes up to a total of 128.

Depending on the technologies that comprise your high-availability solution, additional node configuration tasks might be required.

Starting nodes

Starting a cluster node activates clustering and cluster resource services on a node in an IBM i high availability environment.

A node can start itself and is able to rejoin the current active cluster, provided it can find an active node in the cluster.

To start clustering on a node using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Nodes**.
5. On the **Cluster Nodes** page, select **Start** from the context menu of the node you want to start.

Related information

[Start Cluster Node \(STRCLUNOD\) command](#)

[Start Cluster Node \(QcstStartClusterNode\) API](#)

Enabling nodes to be added to a cluster

Before you can add a node to a cluster, you need to set a value for the Allow add to cluster (ALWADDCLU) network attribute.

Use the **Change Network Attributes (CHGNETA)** command on any server that you want to set up as a cluster node. The **CHGNETA** command changes the network attributes of a system. The ALWADDCLU network attribute specifies whether a node allows another system to add it as a node in a cluster.

Note: You must have *IOSYSCFG authority to change the network attribute ALWADDCLU.

Possible values follow:

***SAME**

The value does not change. The system is shipped with a value of *NONE.

***NONE**

No other system can add this system as a node in a cluster.

***ANY**

Any other system can add this system as a node in a cluster.

***RQSAUT**

Any other system can add this system as a node in a cluster only after the cluster add request has been authenticated.

The ALWADDCLU network attribute is checked to see if the node that is being added is allowed to be part of the cluster and whether to validate the cluster request through the use of X.509 digital certificates. A *digital certificate* is a form of personal identification that can be verified electronically. If validation is required, the requesting node and the node that is being added must have the following installed on the systems:

- IBM i Option 34 (Digital Certificate Manager)
- IBM i Option 35 (CCA Cryptographic Service Provider)

When *RQSAUT is selected for the ALWADDCLU, the certificate authority trust list for the IBM i cluster security server application must be correctly set up. The server application identifier is QIBM_QCST_CLUSTER_SECURITY. At a minimum, add certificate authorities for those nodes that you allow to join the cluster.

Adding nodes

The IBM i PowerHA graphical interface allows you to create a cluster with multiple nodes. After the cluster has been created you may add additional nodes through an active node in the cluster. A cluster can contain up to 128 nodes.

Use the following steps to add a node to an existing cluster using the PowerHA graphical interface:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Nodes**.
5. On the **Cluster Nodes** tab, select **Add Cluster node ...** from the **Select Action** menu.
6. Specify the required information and click **OK**.

Related information

[Add Cluster Node Entry \(ADDCLUNODE\) command](#)

[Add Cluster Node Entry \(QcstAddClusterNodeEntry\) API](#)

Adding a node to a device domain

A device domain is a subset of nodes in a cluster that shares device resources.

If you are implementing a high-availability solution that contains independent disk pools-based technologies, such as switched disk or cross-site mirroring, you must define the node as a member of a device domain. After you add the node to a device domain, you can create a device cluster resource group (CRG) that defines the recovery domain for the cluster. All nodes that will be in the recovery domain for a device CRG must be in the same device domain. A cluster node can belong to only one device domain.

To create and manage device domains, you must have PowerHA Option 41 (HA Switchable Resources) installed. A valid license key must exist on all cluster nodes in the device domain.

The PowerHA graphical interface simplifies device domain management by ensuring that the required nodes are in a device domain when a device CRG is created or when a node is added to a device CRG.

To add a node to a device domain using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click **Cluster Nodes**.
5. On the **Cluster Nodes** page, select **Properties ...** from the context menu of the node you want to add to a device domain.
6. Click **Edit** in the General section of the **Properties** page.
7. Specify the name of the device domain to which you want to add the node in the **Device Domain** field and click **Save**.

Related information

[Add Device Domain Entry \(ADDDEVDMNE\) command](#)

[Add Device Domain Entry \(QcstAddDeviceDomainEntry\) API](#)

Configuring advanced node failure detection

Advanced node failure detection can be used to prevent cluster partitions when a cluster node has actually failed. A Hardware Management Console (HMC) or a Virtual I/O Server (VIOS) partition on an Integrated Virtualization Manager (IVM) managed server can be used.



In this example, a HMC is being used to manage two different IBM systems. For example, the HMC can power up each system or configure logical partitions on each system. In addition, the HMC is monitoring the state of each system and logical partitions on each system. Assume that each system is a cluster node and cluster resource services is monitoring a heartbeat between the two cluster nodes.

With the advanced node failure detection function, cluster resource services can be configured to make use of the HMC. For example, Node A can be configured to have a cluster monitor that uses the HMC. Whenever HMC detects that Node B fails (either the system or the logical partition for Node B), it notifies cluster resource services on Node A of the failure. Cluster resource services on Node A then marks Node B as failed and perform failover processing rather than partitioning the cluster.

Likewise, Node B can also be configured to have a cluster monitor. In this example, then, a failure of either Node A or Node B would result in a notification from the HMC to the other node.

Advanced node failure detection implementation differs depending on the method of connection to the HMC server. Select your method of connection from the list:

- [Configuring advanced node failure detection on hardware management console \(HMC\) with REST server](#)
- [Configuring advanced node failure detection in a Virtual I/O Server \(VIOS\) on an Integrated Virtualization Manager \(IVM\) managed server](#)
- [Configuring advanced node failure detection on hardware management console \(HMC\) with CIM server.](#)

Follow the instructions in the links to configure advanced node failure detection in your network.

Configuring advanced node failure detection on hardware management console (HMC) with CIM server

A Hardware Management Console (HMC) can be used with advance node failure detection to prevent cluster partitions when a cluster node has actually failed.

Prior to configuration, verify the *CIMOM TCP and the *SSHD TCP servers are running.

1. To ensure the *CIMOM TCP server is running on your IBM i. Look for the QUMECIMOM job within the QSYSWRK subsystem to determine if it is running. If the server is not running, start it using the command **STRTCPSVR *CIMOM**.
2. Ensure the *SSHD TCP server is running on your IBM i. At the command line display, enter **STRTCPSVR *SSHD**. To start the *SSHD server, set the QSHRMEMCTL system value is set to 1.

Note: You must have access to the HMC either through the physical monitor and keyboard or remotely through a configured SSH client. You cannot access the HMC with telnet or web interface. Detailed

information about connections to the HMC are found in the section, [Setting up secure script execution between SSH clients and the HMC](#).

The *CIMOM TCP server must be configured and started on each cluster node that has a cluster monitor configured on it. The default configuration of the *CIMOM server that is provided by the installation of the 5770-UME LP must be changed so that the IBM i system can communicate with the CIM server.

Use these steps to assist you in setting up the HMC to monitor for node failures. The cluster nodes to be monitored must register with the HMC through a CIM server on one of the nodes. To register the CIM and cluster require digital certification. The HMC must be used to copy this file to the cluster node with the following steps:

1. Access the HMC or connect to it with a Secure Shell (SSH) session.
2. At the HMC or in the SSH, locate the security certification file to share with your IBM i cluster node. The file is similar to, `/etc/Pegasus/server.pem QSECOFR@LP0236A:/server_name.pem`. Prepare to copy the file to your server with the **SCP** command. Before initiating this secure copy, change the location name from LP0236A to the name of your IBM i system. Change the file `server_name.pem` to the name of your HMC, for example, `yourHMC.pem`.
3. At the HMC or in the SSH, copy to your IBM i cluster node your modified file using the secure copy **SCP** command: `scp /etc/Pegasus/server.pem QSECOFR@YOUR_IBM_i_system:/yourHMC.pem`.
You must have a home directory associated with your profile on the IBM i. For example: if using the QSECOFR profile as the profile running the **SCP** command, you need a `/home/QSECOFR` directory in the integrated file system on the IBM i. Verify that you have the directory created in the correct profile.
4. Sign off the HMC or close your SSH session.

With the digital certificate on your IBM i cluster node, follow this procedure to enter the file into the truststore:

5. Sign on your IBM i system and open the command line display.
6. In the command line display, enter **call qp2term** to enter the PASE shell environment.
7. Locate the HMC digital certificate: `yourHMC.pem/QOpenSys/QIBM/UserData/UME/Pegasus/ssl/truststore/yourHMC.pem`.
8. Add this digital certificate to your IBM i system truststore with the **MOVE** command: `mv/QOpenSys/QIBM/ProdData/UME/Pegasus/bin/cimtrust -a -U QSECOFR -f /QOpenSys/QIBM/UserData/UME/Pegasus/ssl/truststore/yourHMC.pem -T s`.
9. Press F3 to exit the PASE environment.
10. On the command line display enter **ENDTCPSVR *CIMOM** to end the CIM server.

To configure the *CIMOM server to communicate with the IBM i, change the `enableAuthentication` and `sslClientVerificationMode` security settings following these steps:

11. Restart the CIM server and pick up the new certificate, enter **STRTCPSVR *CIMOM** in the command line.
12. In the command line display, enter **call qp2term** to start PASE shell and run the **CIMCONFIG** command.
13. Enter `/QOpenSys/QIBM/ProdData/UME/Pegasus/bin/cimconfig -s enableAuthentication=false -p`.
14. Enter `/QOpenSys/QIBM/ProdData/UME/Pegasus/bin/cimconfig -s sslClientVerificationMode=optional -p`.

These two alterations change the security configuration attributes, permitting the IBM I to communicate with the CIM server. See [Authentication on CIMOM](#) for more information about `sslClientVerificationMode` attribute.

15. Exit the PASE shell with F3 and end the *CIMOM server using **ENDTCPSVR *CIMOM**.
16. Restart the *CIMOM server again from the command line with the **STRTCPSVR *CIMOM**.

Installing a new version of software on the HMC partition may generate a new certificate which will then cause communication between the HMC partition and the cluster node to fail producing error CPFBB CB

with error code 4. If this occurs, add the new digital certificate to the truststore on the nodes which have that HMC or VIOS partition configured in a cluster monitor.

You are ready to perform the cluster configuration sequence using either the **ADDCLUMON** command or with the IBM Navigator for i. Follow the instructions in the topic, [Add a cluster monitor to a node](#). For additional information about the **ADDCLUMON**, see the [Add Cluster Monitor \(ADDCLUMON\)](#) command in the Knowledge Center.

Configuring advanced node failure detection on hardware management console (HMC) with REST server

A Hardware Management Console (HMC) can be used with advanced node failure detection to prevent cluster partitions when a cluster node has actually failed.

1. Using HMC with a Representational state transfer (REST) server requires HMC version V8R8.5.0 or greater.
2. The Add cluster monitor (**ADDCLUMON**) command must be used with the representational state transfer (REST) server. The PowerHA® graphical interface only supports the Common Informational Model (CIM) server for the cluster monitor.
3. Check the QSSLPCL system value. Verify that it is set correctly for the release currently running.

Note: An incorrect value in QSSLPCL may result in a CPFBBBCB diagnostic message with reason code 4.

These steps guide you through obtaining the digital certificate of your HMC, storing it and referencing it to allow advanced node failure detection for the cluster node.

Important: This guide describes steps making use of features of both HMC and of the Digital Certificate Manager. Changes to either of these products may cause portions of this guide to become invalid. If you suspect such changes are preventing you from following the steps outlined in this guide successfully, contact your technical support provider.

Begin by extracting the digital certificates for the HMC and copying them to the IBM i system in the cluster node with these steps:

1. Sign on your IBM i system and open the command line display.
2. In the command line display, enter **CALL QP2TERM** to enter the PASE shell environment.
3. Retrieve the digital certificates from the HMC with this command:

```
openssl s_client -connect HMC_name:443 < /dev/null | awk '/BEGIN/,/END/{ if(/BEGIN/){a++;}  
out="HMC_name"a".pem"; print > out}'
```

Replace *HMC_name* with the name of your system's HMC. This copies the certificates into files named *HMC_name1.pem* ... *HMC_nameN.pem*, where *N* is the number of certificates copied from your system's HMC.

4. Press F3 to exit the **QP2TERM** environment.
5. Run the following command for each of certificate file to convert the CCSID to 819 (ASCII)

```
CHGATR OBJ('HMC_nameX.pem') ATR(*CCSID) VALUE(819).
```

Create a certificate store to hold the digital certificates by following these steps:

6. Open the IBM Navigator for i and click **Internet Configurations**.
7. On the **Internet Configurations** page, click **Digital Certificate Manager**.
You need to enter your user profile and password.
8. In the **Digital Certificate Manager** page, click **Create New Certificate Store**.
9. In the page that appears, you should have an option for ***SYSTEM**. Make sure that the button is selected and click **Continue**.

If the ***SYSTEM** option is not there, you already have a ***SYSTEM** store created. Skip forward to step 12.

10. Select **No - Do not create a certificate in the certificate store**.
11. Create a password for the ***SYSTEM** store and click **Continue**.

The password is case-sensitive. It is recommended not to use special characters. This password is not attached to a user profile and it will not lock you out of the system after too many retries.

You have successfully created the *SYSTEM store.

Select the *SYSTEM certificate store by following these steps:

12. Click **Select a Certificate Store** and select the *SYSTEM option, click **continue**.
13. Sign in with the password for the certificate store and click **Continue**, then **Manage Certificates**.

Import the HMC certificates into the security store.

14. Select **Import certificate** and click **Continue**.

If your HMC has only one certificate, perform these steps for that certificate. If your HMC has multiple certificates, perform these steps for each certificate except the first certificate (*HMC_name1.pem*), starting with the last certificate and moving backwards through the list of certificates. For example, if there are three certificates: *HMC_name1.pem*, *HMC_name2.pem*, and *HMC_name3.pem*, perform these steps for *HMC_name3.pem* first, then for *HMC_name2.pem*.

15. Select **Certificate Authority (CA)** and click **Continue**.
16. Enter the path name of the certificate you want to import. For example, the path and file name may be */HMC_name1.pem*. Click **Continue**.

The selected security certificate is imported into the security store.

After importing the certificates, sign on to your IBM i and use the command line to run the Add cluster monitor (**ADDCLUMON**) command to run the cluster configuration steps. For additional information about **ADDCLUMON**, see the [Add Cluster Monitor \(ADDCLUMON\)](#) command in the Knowledge Center.

As an alternative option to importing digital certificates, consider setting a PowerHA policy to manage communications throughout the cluster. To learn about PowerHA policies read [“Planning for PowerHA policies”](#) on page 44, and for information on implementing and managing PowerHA policies consult the [“Managing PowerHA policies”](#) on page 154 section.

Configuring advanced node failure detection in a Virtual I/O Server (VIOS) on an Integrated Virtualization Manager (IVM) managed server

A Virtual I/O Server (VIOS) partition on an Integrated Virtualization Manager (IVM) managed server can be used with advance node failure detection to prevent cluster partitions when a cluster node has actually failed.

Prior to configuration, verify the *CIMOM TCP and the *SSHD TCP servers are running.

1. To ensure the *CIMOM TCP server is running on your IBM i. Look for the QUMECIMOM job within the QSYSWRK subsystem to determine if it is running. If the server is not running, start it using the command **STRTCPSVR *CIMOM**.
2. Ensure the *SSHD TCP server is running on your IBM i. At the command line display enter: **STRTCPSVR *SSHD** to start the *SSHD server. Verify the **QSHRMEMCTL** system value is set to 1.

The representational state transfer (REST) server is not supported by IVM.

To implement advanced node failure detection in a VIOS partition on an IVM managed server begin by obtaining and copying the digital certificate to your IBM i system. The certificate requires further configuration before adding detection monitors.

Use these steps to help assist you in setting up the VIOS partition to monitor for node failures. To register the cluster node you need to obtain the digital certificate and have the VIOS copy the file to the IBM i:

1. Open a telnet session and sign on to the VIOS partition.
2. Switch to a non-restricted shell by entering `oem_setup_env`.
3. Locate the security certification file to share with your IBM i cluster node. The file is similar to, `/usr/bin/scp /opt/freeware/cimom/pegasus/etc/cert.pem QSECOFR@system-name:/server.pem`. Prepare to copy the file to your server by changing `system-name` to the name of your IBM i system. Change the file `server.pem` to the name of your VIOS partition, for example, `yourVIOS.pem`.

Your file will resemble: `/usr/bin/scp /opt/freeware/cimom/pegasus/etc/cert.pem`
`QSECOFR@YOUR_IBM_i_system:/yourVIOS.pem`.

4. Copy to your IBM i cluster node your modified file using the secure copy **SCP** command: `/usr/bin/scp /opt/freeware/cimom/pegasus/etc/cert.pem`
`QSECOFR@YOUR_IBM_i_system:/yourVIOS.pem`.
5. Start the CIMOM server running in the VIOS partition by entering **startnetsvc cimserver**.
6. Sign off of the VIOS partition.

With the digital certificate on your IBM i cluster node, follow this procedure to enter the file into the truststore:

7. Sign on your IBM i system and open the command line display.
8. In the command line display, enter **call qp2term** to enter the PASE shell environment.
9. Locate the VIOS digital certificate: `yourVIOS.pem` and add this digital certificate to your IBM i system trusts with the **MOVE** command: `mv yourVIOS.pem/QOpenSys/QIBM/ProdData/UME/Pegasus/bin/cimtrust -a -U QSECOFR -fyourVIOS.pem -T s`.
10. Press F3 to exit the PASE environment.
11. On the command line display enter **ENDTCPSVR *CIMOM** to end the CIM server.

To configure the *CIMOM server to communicate with the IBM I, change the `enableAuthentication` and `sslClientVerificationMode` security settings following these steps:

12. Restart the CIM server and pick up the new certificate with **STRTCPSVR *CIMOM** in the command line.
13. At the command line display, enter **call qp2term** to start PASE shell and run the **CIMCONFIG** command.
14. Enter `/QOpenSys/QIBM/ProdData/UME/Pegasus/bin/cimconfig -s enableAuthentication=false -p`.
15. Enter `/QOpenSys/QIBM/ProdData/UME/Pegasus/bin/cimconfig -s sslClientVerificationMode=optional -p`.

These two alterations change the security configuration attributes, permitting the IBM I to communicate with the CIM server. See [Authentication on CIMOM](#) for more information about `sslClientVerificationMode` attribute.

16. Exit the PASE shell with F3 and end the *CIMOM server using **ENDTCPSVR *CIMOM**.
17. Restart the *CIMOM server again from the command line with the **STRTCPSVR *CIMOM**.

Installing a new version of software on the HMC partition may generate a new certificate which will then cause communication between the HMC partition and the cluster node to fail producing error CPFBBBCB with error code 4. If this occurs, add the new digital certificate to the truststore on the nodes which have that HMC or VIOS partition configured in a cluster monitor.

You are ready to perform the cluster configuration sequence using either the **ADDCLUMON** command or with the IBM Navigator for i. Follow the instructions in the topic, [Add a cluster monitor to a node](#). For additional information about the **ADDCLUMON**, see the [Add Cluster Monitor \(ADDCLUMON\)](#) command in the Knowledge Center.

Configuring Cluster Resource Groups

Manage cluster-wide resources using Cluster Resource Groups (CRGs).

A CRG manages resources within an IBM i high availability environment. Users can perform many cluster management functions through tasks that access CRGs. Each CRG has a recovery domain that defines which cluster nodes a cluster resource represented by the CRG can be accessed.

There are 3 CRG types commonly used in high availability environments: device (used mostly for external storage), data (for logical replication), and application (often used with logical replication to start applications). For additional information about CRG types and usage, consult the [Cluster resource group \(CRG\)](#) topic in [High availability technologies](#).

Starting a CRG

Starting a cluster resource group (CRG) enables resilience for the CRG.

To start a CRG using the PowerHA graphical interface, complete the following steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Resource Groups**.
5. On the **Cluster Resource Group** page, select **Start** from the context menu of the CRG you want to start.

Related information

[Start Cluster Resource Group \(STRCRG\) command](#)

[Create Cluster Resource Group \(QcstCreateClusterResourceGroup\) API](#)

Creating cluster resource groups (CRGs)

Cluster resource groups (CRGs) manage high availability resources, such as applications, data, and devices. Each CRG type manages the particular type of resource in a high-availability environment.

The PowerHA graphical interface allows you to create different CRGs for management of your high availability resources. Each CRG type can be used separately or in conjunction with other CRGs. For example, you may have a stand-alone business application that requires high availability. After you have enabled the application for high availability, you can create CRGs to help manage availability for that application.

If you want only an application, not its data to be available in the event of an outage, you can create an application CRG. However, if you want to have both the data and application available, you can store both within an independent disk pool, which you can define in a device CRG. If an outage occurs, the entire independent disk pool is switched to a backup node, making both the application and its data available.

Creating application CRGs

If you have applications in your high-availability solution that you want to be highly available, you can create an application cluster resource group (CRG) to manage failovers for that application.

You can specify to allow an active takeover IP address when you create the application CRG. When you start an application CRG that allows for an active takeover IP address, the CRG is allowed to start.

To create an application CRG using the PowerHA graphical interface, complete the following steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Resource Groups**.
5. On the **Cluster Resource Group** page, select **Create Cluster Resource Group ...** from the **Select Action** menu.
6. Follow the instructions in the **Create Cluster Resource Group** wizard to create an application CRG.

Related information

[Create Cluster Resource Group \(CRTCRG\) command](#)

[Create Cluster Resource Group \(QcstCreateClusterResourceGroup\) API](#)

Creating data CRGs

Data cluster resource groups (CRGs) are primarily used with logical replication applications, which are provided by several high availability Business Partners. If you are implementing a high-availability solution based on logical replication you can create a data CRG to assist the replication of data between primary and backup nodes.

To create a data CRG PowerHA graphical interface, complete the following steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Resource Groups**.
5. On the **Cluster Resource Group** page, select **Create Cluster Resource Group ...** from the **Select Action** menu.
6. Follow the instructions in the Create Cluster Resource Group wizard to create a data CRG.

Related information

[Create Cluster Resource Group \(CRTCRG\) command](#)

[Create Cluster Resource Group \(QcstCreateClusterResourceGroup\) API](#)

Creating device CRGs

A device cluster resource group (CRG) is made up of a pool of hardware resources that can be switched as an entity. To create switchable devices within a high-availability solution, the nodes that use these devices need to be a part of a device CRG.

Prior to creating a device CRG, add all nodes that will share a switchable resource to a device domain. The PowerHA graphical interface simplifies this by ensuring that the required nodes are in a device domain when creating a device CRG.

To create a device CRG using the PowerHA graphical interface, complete the following steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Resource Groups**.
5. On the **Cluster Resource Group** page, select **Create Cluster Resource Group ...** from the **Select Action** menu.
6. Follow the instructions in the **Create Cluster Resource Group** wizard to create a device CRG.

Related information

[Create Cluster Resource Group \(CRTCRG\) command](#)

[Create Cluster Resource Group \(QcstCreateClusterResourceGroup\) API](#)

Creating peer CRGs

You can create a peer CRG to define node roles in load-balancing environments.

To create a peer CRG in a cluster using the PowerHA graphical interface, complete the following steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Resource Groups**.
5. On the **Cluster Resource Group** page, select **Create Cluster Resource Group ...** from the **Select Action** menu.
6. Follow the instructions in the Create Cluster Resource Group wizard to create a peer CRG.

Related information

[Create Cluster Resource Group \(CRTCRG\) command](#)

[Create Cluster Resource Group \(QcstCreateClusterResourceGroup\) API](#)

Configuring a Cluster Resource Group container

Learn how to manage multiple Cluster Resource Groups (CRGs) with the CRG container

About CRG containers

CRG containers serve as the control object for a collection of CRGs managed as a single entity for HA operations.

CRG containers can manage device, data, and application CRGs. Similar to the CRGs it manages, the CRG container provides the ability to perform a switchover or failover locally or across sites. A CRG managed by a CRG container is considered a managed CRG. Managed CRGs must maintain consistency with the managing CRG container.

Configuration requirements

For a CRG container to manage CRGs, and for CRGs to remain consistent with the CRG container, these requirements must be in place:

Container recovery domain

Within the CRG container, all managed CRG recovery domains must be a subset of the CRG container recovery domain. A CRG container's recovery domain must have all the nodes located in every managed CRGs' recovery domain.

Cluster nodes

The recovery domain of a CRG managed by a container must have all of its nodes located in the CRG container recovery domain.

CRG

Only device, data, and application CRGs can be managed by a CRG container. A managed CRG can be in only one container.

Site

In the HA environment, a site contains a subset of recovery domain nodes in the same physical location. The CRG parameter SITE is required when creating a CRG container. The CRG container is designed to perform its functions at a site level and require nodes to be associated with named sites in their recovery domains, representing the nodes in the same physical location. Managed CRGs using sites in their recovery domains must match the site names that the container CRG uses.

For CRG types Data and Application that do not contain sites, the CRG container logically divides these into sites. For example, a container Site1 has nodes A and B, and Site2 has nodes C and D. A data CRG has nodes A and C, which the container would manage as though the data CRG had a Site1 of node A and a Site2 of node C.

Consistency

A managed CRG is considered consistent with its container CRG only if the managed CRG has the same source site as the container.

These rules ensure that the CRG container maintains the management functions for the CRGs within it.

CRG container status

A CRG container can have the status of Active, Inactive, or Indoubt depending on the statuses of the CRGs that it manages. The status is dependent on the behavior of the managed CRGs:

Active

A CRG container has the status of Active if all managed CRGs are Active and if all the managed CRGs are consistent with the CRG container.

Inactive

A CRG container is Inactive if all the managed CRGs are consistent with the container but at least one CRG is inactive.

Indoubt

The container is Indoubt status if at least one managed CRG has an inconsistent recovery domain or if at least one managed CRG has a status of Indoubt.

Like CRGs, a CRG container must be Active to provide protection and switching capabilities.

CRG container failover events

Similar to CRG control of switching resources in the event of a failover, the CRG containers controls failovers for managed CRGs. A CRG container:

- Can perform a failover only if it has a status of Active.
- Allows managed CRGs to failover if the managed primary CRG has failed.
- Can change its source site. As a result of a failover, if the CRG container new primary is in the target site, all managed CRGs are switched to the other site to maintain consistency with the CRG container.

Managed CRGs

If a CRG is a managed CRG inside a container some of its management capabilities are limited.

Cluster configuration operations remain unchanged. Users can add and remove nodes in the recovery domain or assign configuration objects. Cluster management operations for a managed CRG are handled by the CRG container primarily. In some circumstances managed CRGs can perform some management operations:

- If the CRG container has a status of Inactive, management operations are allowed on a managed CRG if the result of the operation keeps the managed CRG consistent with the CRG container.
- If the CRG container has a status of Indoubt, all CRG management operations are allowed for the managed CRG.
- When the status of the container is Active, all management operations on the managed CRG are not allowed.

If a managed CRG requires management operations to be performed on it, then the CRG container must be made Inactive and the CRG removed from the container and reconfigured.

For information about implementing CRG containers in a high availability environment see:

- [“Create a cluster resource group \(CRG\) container” on page 67](#) to view an example of setting up a CRG container.
- [“Managing a cluster resource group \(CRG\) container” on page 110](#) for information and examples of CRG container usage.

Create a cluster resource group (CRG) container

Learn how to create and configure a CRG container to manage a group of CRGs

Cluster resource group (CRG) containers manage some or all of a cluster's CRGs as a single entity. While a CRG container can be created by itself with no CRGs and any CRGs added to it at a later time with the Configure CRG Container (**CFGCRGCNR**) command, this example assumes that users already have created the cluster resource groups that they want managed by a CRG container.

In this example, a cluster named **HA_CLSTR** consists of three IBM System i nodes spread across two sites. They are configured as such:

- **NODE01**, serves as the primary node and is located at **SITE01**.
- **NODE02** also is located at **SITE01** and serves as a backup node.
- **NODE03** is a backup node situated at **SITE02**.

This cluster contains three CRGs

- a device CRG, **DEVCRG**.
- a data CRG, **DATACRG01**.

- another data CRG, **DATA CRG02**.

Each CRG has a recovery domain:

CRG	SITE01		SITE02
	NODE01	NODE02	NODE03
DEVCRG	Primary	Backup 1	Backup 2
DATA CRG01	Primary	Backup 2	Backup 1
DATA CRG02	Primary	Backup 2	Backup1

With this information in hand, a CRG container named HACNR can be created and configured to manage all three CRGs as a single unit.

Open the Create CRG Container (**CRTCRG CNR**) command screen.

1. On the command line type **CRTCRG CNR** and press F4.
The Create CRG Container (**CRTCRG CNR**) command screen displays.
2. Type in a name for the container, HACNR in the first field.

Supply the information for the recovery domain of the CRG container. Remember that the recovery domain used by the CRG container must contain all the nodes listed in all the recovery domains of the CRGs managed by the container. The CRG container requires two sites in its recovery domain even if some managed CRGs do not.

3. At the Recovery domain node list enter the name of the first node for the recovery domain.
4. Select either ***PRIMARY** or ***BACKUP** for the Node role field.
5. Optional: Depending on the size of the cluster and the number of nodes, users can assign a specific numbered order in the Backup sequence number field to designate the order of the node in the recovery domain.
***LAST** can be used to designate that the CRG node will assume the last place in the recovery domain after a switchover or failover operation. If, however, ***LAST** is specified for more than one node, then the first node specified with ***LAST** will become the last backup node, the second node specified with ***LAST** will have the next to last backup node role.
6. Type in the name of the site that the node is a member of.
This is a requirement for a CRG container.
7. Repeat steps 3 through 6 to enter the information for the second node in the CRG container recovery domain.
To enter additional nodes of the recovery domain into the list, type a + in the for more values field and press enter to expand the Recovery domain node list section. After all recovery domain nodes have been entered, press Enter to return to the main screen of the Create CRG Container (**CRGCRG CNR**) command.

```

Specify More Values for Parameter RCYDMN

Type choices, press Enter.

Node identifier . . . . . NODE01          Name
Node role . . . . . *PRIMARY             *PRIMARY, *BACKUP
Backup sequence number . . . . *LAST      1-127, *LAST
Site name . . . . . SITE01              Name

Node identifier . . . . . NODE02          Name
Node role . . . . . *BACKUP              *PRIMARY, *BACKUP
Backup sequence number . . . . *LAST      1-127, *LAST
Site name . . . . . SITE01              Name

Node identifier . . . . . NODE03          Name
Node role . . . . . *BACKUP              *PRIMARY, *BACKUP
Backup sequence number . . . . *LAST      1-127, *LAST
Site name . . . . . SITE03              Name

F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys

Create CRG Container
(CRTRCGCNR)

Type choices, press Enter.

Configuration object list . . . > DEVCRG          Name, *NONE
+ for more values
Text description . . . . . > 'Device CRG for cluster HACLSTR'

Specify More Values for Parameter CFGOBJ

Type choices, press Enter.

Configuration object list . . . > DEVCRG          Name, *NONE
DTACRG01

```

Once the recovery domain for the CRG container has been entered, the Configuration object list can be created. Configuration objects used by a CRG container are application, data, and device CRGs.

8. Specify the name of the configuration object (CRG) for the CRG container to manage.

To enter additional CRGs into the Configuration object list, type a + in the for more values field and press enter to open the Specify More Values for Parameter **CFGOBJ** display. After all configuration objects have been entered, press Enter to return to the main screen of the Create CRG Container (**CRTRCGCNR**) command.

Note: Alternatively, the value of ***NONE** can be left for the Configuration object list. If ***NONE** is entered in this command, users need to add the names of the CRGs for the container to manage using the Configure CRG container (**CFGCRGCNR**) command.

9. Optional: Type in a description of the CRG container in the Text description field.

10. Press Enter to create the CRG container.

The CRG container **HACNR** is created with the specified recovery domain and the CRGs supplied in the Configuration objects list for the container become the managed CRGs of the new CRG container.

An example of creating a CRG container from the command line using the configuration described at the beginning of this page looks like:

```

CRTRCGCNR CNR(HACNR) RCYDMN((NODE01 *PRIMARY *LAST SITE01) (NODE03 *BACKUP *LAST SITE02))
TEXT('Resiliency Container')

```

A CRG container, **HACNR** is created with **NODE01** and **NODE02**, and **NODE03** with their respective roles and site locations.

If any required nodes or CRGs were not entered in the lists when running the Create CRG container (**CRTCRCGNR**) command, the CRG container can be updated to include additional nodes or CRGs with the Configure CRG container (**CFGCRGCNR**) command.

Consult these topics for instructions and examples:

- [“Starting a cluster resource group \(CRG\) container” on page 111](#)
- [“Ending a cluster resource group \(CRG\) container” on page 111](#)
- [“Displaying a cluster resource group \(CRG\) container” on page 113](#)
- [“Adding nodes and configuration objects using the Configure CRG Container command” on page 114](#)
- [“Removing nodes and configuration objects using the Configure CRG Container command” on page 115](#)
- [“Changing the primary node of a cluster resource group \(CRG\) container using the Change CRG Container \(CHGCRGCNR\) command” on page 117](#)
- [Changing the recovery domain of a cluster resource group \(CRG\) container](#)

Refer to the information above when following the examples presented in the links.

Scenarios: Configuring high availability

Configuration scenarios provide examples of different PowerHA environments and step-by-step configuration tasks to help you implement a high-availability solution that is based on your needs and resiliency requirements.

These scenarios contain descriptions of the business objectives for high availability and provide a graphic that illustrates the resources within the high-availability solution. Each solution example contains step-by-step instructions to set up and test high availability. However, this information does not cover all configuration cases and additional testing may be required to verify high availability.

For additional details on specific environments, see the following Redbooks®:

- PowerHA SystemMirror for IBM i Cookbook
- IBM i and IBM Storwize Family: A Practical Guide to Usage Scenarios
- Simple Configuration Example for Storwize V7000 FlashCopy and PowerHA SystemMirror for i

Related information

[PowerHA SystemMirror for IBM i Cookbook](#)

[IBM System Storage DS8000 Information Center-> Copy Services](#)

[IBM i and IBM Storwize Family: A Practical Guide to Usage Scenarios](#)

[Simple Configuration Example for Storwize V7000 FlashCopy and PowerHA SystemMirror for i](#)

Scenario: Geographic mirroring

This scenario describes an IBM i high-availability solution that uses geographic mirroring in a two node cluster. This solution provides both disaster recovery and high availability.

Overview

Geographic mirroring is a PowerHA technology where data is mirrored to a copy of the independent disk pool at the remote location. This solution provides disaster recovery in the event of a site-wide outage on the production system (System 1). In that situation, failover to the backup site (System 2) occurs, where operations can continue on the mirrored copy of the data. This solution provides a simple and less expensive alternative to external storage-based solutions, such as IBM System Storage Global Mirror and Metro Mirror. However, geographic mirroring does not offer all the performance options that the external storage solutions provide.

Objectives

This solution has the following advantages:

- Provides availability for your business resources during planned outages

- Provides availability for business resources during unplanned outages
- Provides availability for business resources during a disaster
- Enables data to remain current and may not need to be synchronized

This solution has the following restrictions:

- There is no concurrent access to the disk pool. Only the production copy is normally accessed. However, you can detach the mirror copy for offline processing of a second copy of the data.
- Potentially affects performance because increased central processing unit (CPU) is required to support geographic mirroring
- Consider using redundant communication paths and adequate bandwidth

Details

The following graphic illustrates this solution:



Configuration steps

Complete the following steps to configure the high availability technologies that are associated with this scenario using the PowerHA graphical interface:

1. [Complete planning checklist for cluster](#)
2. [Create a cluster](#)
3. [Create a cluster administrative domain](#)
4. [Start a cluster administrative domain](#)
5. [Create an independent disk pool](#)
6. [Add monitored resource entries](#)
7. [Make the independent ASP highly available](#)
8. [Configure geographic mirroring](#)
9. [Vary on the independent ASP](#)
10. [Perform a switchover to test your high-availability solution](#)

Complete the following steps to configure the high availability technologies that are associated with this scenario using commands:

1. [Complete planning checklist for clusters](#)
2. [Create a cluster](#)
3. [Add nodes](#)
4. [Start nodes](#)
5. [Add nodes to device domain](#)
6. [Create a cluster administrative domain](#)
7. [Start cluster administrative domain](#)
8. Create an independent disk pool using [Configure Device ASP](#).
9. [Add monitor resource entries](#)
10. [Create device CRG](#)
11. [Start a device CRG](#)
12. Use [Vary Configuration](#) to make the disk pool available.
13. Perform a [switchover](#) to test the configuration.

Scenario: Metro Mirror

This scenario describes a PowerHA solution, which is based on external storage and provides disaster recovery and high availability for storage systems, which are separated by short distances. Metro Mirror is an IBM System Storage solution that copies data synchronously from the storage unit at the production site to the storage unit at the backup site. In this way data remains consistent at the backup site.

Overview

The Metro Mirror solution provides a high availability and disaster recovery by using external storage units within a metropolitan area. The independent disk pool is replicated between the external storage devices to provide availability for both planned and unplanned outages. When Metro Mirror receives a host update to the production volume, it completes the corresponding update to the backup volume. Metro Mirror supports a maximum distance of 300 km (186 mi). Delays in response times for Metro Mirror are proportional to the distance between the volumes.

This scenario covers the configuration of IBM-supplied IBM i high availability technology and does not provide installation or configuration instructions regarding IBM System Storage DS8000 series. This information assumes that an IBM System Storage solution is already in place before the IBM i high availability configuration. For installation and configuration information about DS8000, see [Copy Services](#)

in the IBM System Storage DS8000 Information Center .

A similar scenario can also be accomplished with other system storage technologies. For more information on storage technologies that support Metro Mirror, see [“PowerHA supported storage servers” on page 25](#).

Objectives

This solution has the following advantages:

- Replication is entirely managed by the external storage unit, thus no IBM i CPU is used. Replication continues in the storage unit even when the system experiences a system-level failure.
- Availability for business resources during planned or unplanned outages, which include maintenance outages or software/PTF related outages as well as disaster recovery.
- I/O remains consistent and does not need to be synchronized
- Fast recovery times when used with journaling. Journaling recovers data more quickly in the event of an unplanned outage or failover. Journaling forces data changes to disk where the mirroring is occurring. If you do not use journaling, you might lose data that is in memory. Journaling provides recovery of these data-level transactions and helps with the recovery times.
- The ability to use the FlashCopy function on the source or target side of Metro Mirror.

This solution has the following restrictions:

- Requires external storage hardware
- Consider using redundant communication paths and adequate bandwidth
- There is no concurrent access to the disk pool

Details

The following graphic illustrates this solution:



Configuration steps

Complete the following steps to configure the high availability technologies that are associated with this scenario using the PowerHA graphical interface:

1. [Complete planning checklist for clusters](#)
2. [Create a cluster of two active nodes](#)
3. [Create a cluster administrative domain](#)
4. [Start a cluster administrative domain](#)
5. [Create an independent disk pool](#)
6. [Add monitored resource entries](#)
7. [Make the independent ASP highly available](#)
8. [Configure Metro Mirror](#)
9. [Make disk pool available](#)
10. [Perform a switchover to test your high-availability solution](#)

Complete the following steps to configure the high availability technologies that are associated with this scenario using other interfaces:

1. [Complete planning checklist for clusters](#)
2. [Create a cluster](#)
3. [Add nodes](#)
4. [Start nodes](#)
5. [Add nodes to device domain](#)
6. [Create a cluster administrative domain](#)
7. [Start a cluster administrative domain](#)
8. [Create an independent disk pool using \[Configure Device ASP\]\(#\)](#).
9. [Add monitored resource entries](#)
10. [Create a device CRG](#)
11. [Start a device CRG](#)
12. [Configure Metro Mirror session](#)
13. [Make disk pool available](#)
14. [Perform a switchover to test your high-availability solution.](#)

Related concepts

[PowerHA supported storage servers](#)

IBM System Storage provides enhanced storage capabilities.

Scenario: Global Mirror

This scenario describes an PowerHA solution that is based on external storage and provides disaster recovery and high availability for storage systems that are separated by great distances. Global Mirror is an IBM Systems Storage solution that copies data asynchronously from the storage unit at the production site to the storage unit at the backup site. In this way, data remains consistent at the backup site.

Overview

The Global Mirror solution provides a disaster recovery solution by using external storage units across long distances. The independent disk pool is replicated between the external storage devices to provide availability for both planned and unplanned outages.

This scenario covers the configuration of IBM-supplied IBM i high availability technology and does not provide installation or configuration instructions regarding IBM System Storage DS8000 series. This information assumes that an IBM System Storage solution is already in place before the IBM i high availability configuration. For installation and configuration information about DS8000, see [Copy Services](#)

in the [IBM System Storage DS8000 Information Center](#) .

A similar scenario can also be accomplished with other system storage technologies. For more information on storage technologies that support Global Mirror, see [“PowerHA supported storage servers” on page 25](#).

Objectives

Cross-site mirroring with Global Mirror provides the following advantages:

- Replication is entirely managed by the external storage unit, thus no IBM i CPU is used. Replication continues in the storage unit even when the system experiences a system-level failure.
- Availability for business resources during planned or unplanned outages, which include maintenance outages or software/PTF related outages as well as disaster recovery.
- Fast recovery times when used with journaling. Journaling recovers data more quickly in the event of an unplanned outage or failover. Journaling forces data changes to disk where the mirroring is occurring. If you do not use journaling, you might lose data that is in memory. Journaling provides recovery of these data-level transactions and helps with the recovery times.
- The ability to use the FlashCopy function on the source or target side of Global Mirror.

This solution has the following restrictions:

- The solution requires IBM System Storage DS8000 server hardware.
- To achieve acceptable performance, consider using redundant communication paths and adequate bandwidth.
- There is no concurrent access to the disk pool.
- A consistency group is required for the Global Mirror target copy. A consistency group is not required for the Global Mirror source copy, but it is highly recommended.
- Reverse replication occurs automatically on a switchover only if the new target has a consistency group. Reverse replication never occurs automatically on a failover.
- When reverse replication does not occur on a switchover or failover, the configuration will consist of two source copies.
 - If the desired target copy node has a consistency group, then a reattach operation will convert it to a target copy and automatically initiate replication.
 - If the desired target copy node does not have a consistency group, then recovery requires manual intervention with the System Storage DS8000 Storage Manager interface to initiate replication and synchronize the current source and target.

Details

The following graphic illustrates this solution:



Configuration steps

Complete the following steps to configure the high availability technologies that are associated with this scenario using the PowerHA graphical interface:

1. [Complete planning checklist for cluster](#)
2. [Create a cluster](#)
3. [Create a cluster administrative domain](#)
4. [Start a cluster administrative domain](#)
5. [Create an independent disk pool](#)
6. [Add monitored resource entries](#)

7. [Make the independent ASP highly available](#)
8. [Configure Global Mirror](#)
9. [Vary on the independent ASP](#)
10. [Perform a switchover to test your high-availability solution](#)

Complete the following steps to configure the high availability technologies associated with this scenario using other interfaces:

1. [Complete planning checklist for cluster](#)
2. [Create a cluster](#)
3. [Add a nodes](#)
4. [Start a node](#)
5. [Add nodes to a device domain](#)
6. [Create cluster administrative domain](#)
7. [Start a cluster administrative domain](#)
8. Create an independent disk pool using [Configure Device ASP](#).
9. [Add ASP copy description](#)
10. [Add monitored resource entries](#)
11. [Create a device CRG](#)
12. [Start a device CRG](#)
13. [Start ASP session](#)
14. [Configure global mirror session](#)
15. [Make disk pool available](#)
16. Perform a [switchover](#) to test your high-availability solution

Related concepts

[PowerHA supported storage servers](#)

IBM System Storage provides enhanced storage capabilities.

Configuring cluster administrative domains

In a high-availability environment, it is necessary that the application and operational environment remain consistent among the nodes that participate in high availability. Cluster administrative domain is the PowerHA implementation of environment resiliency and ensures that the operational environment remains the consistent across nodes.

Creating a cluster administrative domain

In a high-availability solution, the cluster administrative domain provides the mechanism that keeps resources synchronized across systems and partitions within a cluster.

To create the cluster administrative domain, a user must have *IOSYSCFG authority and authority to the QCLUSTER user profile. To manage a cluster administrative domain, a user must be authorized to the CRG that represents the cluster administrative domain, the QCLUSTER user profile, and cluster resource group commands.

To create a cluster administrative domain using the PowerHA graphical interface, complete the following steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Administrative Domains**.

5. On the **Cluster Administrative Domain** page, select **Create Administrative Domain ...** from the Select Action menu.
6. Specify the cluster administrative domain and click **OK**.

Related concepts

[Maintaining user profiles on all nodes](#)

You can use two mechanisms for maintaining user profiles on all nodes within a cluster.

Related information

[Create Cluster Administrative Domain \(CRTCAD\) command](#)

[Create Cluster Administrative Domain \(QcstCrtClusterAdminDomain\) API](#)

Adding a node to the cluster administrative domain

You can add additional nodes to a cluster administrative domain within a high-availability solution.

Before adding a node to a cluster administrative domain, ensure that node is also part of the cluster in which the cluster administrative domain resides. If it is not, you cannot add the node to the cluster administrative domain. The cluster administrative domain does not have to be active, but the resources will just not be made consistent until it is active.

When you add a node to the administrative domain, the MREs from the domain are copied to the node being added. If the monitored resource does not exist on the new node, it is created by the cluster administrative domain. If the monitored resource already exists on the node being added, it is synchronized with the rest of the cluster administrative domain if the domain is active. That is, the values of the attributes for each monitored resource on the node that is joining are changed to match the global values for the monitored resources in the active domain.

To add a node to a cluster administrative domain using the PowerHA graphical interface, follow these steps:

1. Log on to the system with your user profile and password.
2. Click **PowerHA** from the IBM Navigator for i window.
3. On the **PowerHA** page, click on **Cluster Administrative Domains**.
4. On the **Administrative Domains** page, select **Domain Nodes ...** from the context menu of the cluster administrative domain to which you want to add a node.
5. On the **Domain Nodes** page, select **Add Domain Node ...** from the Select Action menu.
6. Select the node you want to add and click **OK**.

Related information

[Add Cluster Administrative Domain Node Entry \(ADDCADNODE\) command](#)

[Add Node To Recovery Domain \(QcstAddNodeToRcvyDomain\) API](#)

Starting a cluster administrative domain

Cluster administrative domains provide environment resiliency for resources within an IBM i high-availability solution.

When the cluster administrative domain is started, any change made to any monitored resource while the cluster administrative domain was ending is propagated to all active nodes in the cluster administrative domain.

To start a cluster administrative domain using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Administrative Domains**.
5. On the **Cluster Administrative Domains** page, select **Start** from the context menu of the cluster administrative domain you want to start.

The Status column shows that the cluster administrative domain is started.

Related concepts

[Synchronization of monitored resource](#)

Synchronization of monitored resources occurs when monitored resources are changed on nodes which have been defined in the cluster administrative domain.

Related information

[Start Cluster Administrative Domain \(STRCAD\) command](#)

Synchronization of monitored resource

Synchronization of monitored resources occurs when monitored resources are changed on nodes which have been defined in the cluster administrative domain.

During this synchronization process, the cluster administrative domain attempts to change each resource with attributes whose values do not match its global values, unless there is a pending change for that resource. Any pending change is distributed to all active nodes in the domain and applied to each affected resource on each node. When the pending changes are distributed, the global value is changed and the global status of each affected resource is changed to *consistent* or *inconsistent*, depending on the outcome of the change operation for the resource on each node. If the affected resource is changed successfully on every active node in the domain, the global status for that resource is *consistent*. If the change operation failed on any node, the global status is set to *inconsistent*.

If changes are made to the same resource from multiple nodes while the cluster administrative domain is inactive, all of the changes are propagated to all of the active nodes as part of the synchronization process when the domain is started. Although all pending changes are processed during the activation of the cluster administrative domain, there is no guaranteed order in which the changes are processed. If you make changes to a single resource from multiple cluster nodes while the cluster administrative domains inactive, there is no guaranteed order to the processing of the changes during activation.

If a node joins an inactive cluster administrative domain (that is, the node is started while the cluster administrative domain is ended), the monitored resources are not resynchronized until the cluster administrative domain is started.

Note: The cluster administrative domain and its associated exit program are IBM-supplied objects. They should not be changed with the QcstChangeClusterResourceGroup API or the Change Cluster Resource Group (CHGCRG) command, or unpredictable results will occur.

After a cluster node that is part of a cluster administrative domain is ended, monitored resources can still be changed on the inactive node. When the node is started again, the changes will be resynchronized with the rest of the cluster administrative domain. During the resynchronization process, the cluster administrative domain applies any changes from the node that was inactive to the rest of the active nodes in the domain, unless changes had also been made in the active domain while the node was inactive. If changes were made to a monitored resource both in the active domain and on the inactive node, the changes made in the active domain are applied to the joining node. In other words, no changes made to any monitored resource are lost, regardless of the status of the node. You can specify the synchronization option to control synchronization behavior.

If you want to end a cluster node that is part of a cluster administrative domain, and not allow changes made on the inactive node to be propagated back to the active domain when the node is started (for example, when ending the cluster node to do testing on it), you must remove the node from the administrative domain peer CRG before you end the cluster node.

Related concepts

[Remove Admin Domain Node Entry \(RMVCADNODE\) command](#)

Related tasks

[Starting a cluster administrative domain](#)

Cluster administrative domains provide environment resiliency for resources within an IBM i high-availability solution.

Related information

[Remove CRG Node Entry \(RMVCRGNODE\) command](#)

Adding monitored resource entries

You can add a monitored resource entry (MRE) to a cluster administrative domain. Monitored resource entries define critical resources so that changes made to these resources are kept consistent across a high-availability environment.

To add a monitored resource entry using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click on **PowerHA** in the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Administrative Domains**.
5. On the **Cluster Administrative Domains** page, select **Monitored Resource ...** from the context menu of the cluster administrative domain to which you want to add the monitored resource.
6. On the **Monitored Resource** page, select **Add Monitored Resource(s) ...** from the **Select Action** menu.
7. Specify the monitored resource information and click **OK**.

Related tasks

[Selecting attributes to monitor](#)

After you have added monitored resource entries, you can select attributes associated with that resource to be monitored by the cluster administrative domain.

Related information

[Add Admin Domain MRE \(ADDCADMRE\) command](#)

[Add Monitored Resource Entry \(QfpadAddMonitoredResourceEntry\) API](#)

Configuring independent disk pools

In a high-availability environment, it is necessary that the application and its data remain consistent among the nodes that participate in high availability. An independent disk pool is a disk pool that contains objects, the directories, or libraries that contain the objects, and other object attributes such as authorization and ownership attributes. An independent disk pool can be used to help in this situation.

Related information

[Disk pools](#)

[IBM eServer iSeries Independent ASPs: A Guide to Moving Applications to IASPs](#)

Creating an independent disk pool

To create an independent disk pool, you can use the PowerHA graphical interface, the Configuration and Service graphical interface, or the Configure Device ASP (CFGDEVASP) command.

To use the PowerHA graphical interface to create a new independent disk pool, follow these steps:

1. In a web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click on **PowerHA** in the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Independent ASPs**.
5. On the **Independent ASPs** page, click on **Show All Others ...** to show any independent disk pools that are not currently highly available.
6. Select **Create Independent ASP ...** from the **Select Action** menu in the All Other table.
7. Follow the instructions in the **Create Independent ASP** wizard to create an independent disk pool.

To use the Configuration and Service graphical interface to create a new independent disk pool, follow these steps:

Note: To work with disk within the IBM Navigator for i, you must have the appropriate password configuration for Dedicated Service Tools. With the New Disk Pool wizard you can include unconfigured disk units in a parity set, and you can start device parity protection and disk compression. As you add disk units, do not spread disk units that are in same parity set across multiple disk pools, because failure to one parity set would affect multiple disk pools.

Configuration and Service graphical interface (IBM Navigator for i)

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Select **Configuration and Service** from your IBM Navigator for i window.
4. Select **Disk Units**.
5. From the **Select Actions** menu, select **New Disk Pool**.
6. Follow the wizard's instructions to add disk units to a new disk pool.
7. Print your disk configuration to have it available in a recovery situation.
8. Record the relationship between the independent disk pool name and number.

The Configure Device ASP (CFGDEVASP) command can be used to create a new independent disk pool. For more information on the command, see [CFGDEVASP \(Configure Device ASP\) command](#).

Note: Add independent disk pools when your system is fully restarted. If you must use the New Disk Pool wizard in the dedicated service tools (DST) mode, you need to create an associated device description for the independent disk pool when the system is fully restarted. Use the Create Device Description (ASP) (CRTDEVASP) command to create the device description. Name the device description and resource name the same as you name the independent disk pool. You can use the Work with Device Descriptions (WRKDEV D) command to verify that the device description and independent disk pool name match.

Making an independent disk pool highly available

To make an independent disk pool highly available, it becomes managed by clustering using a device cluster resource group.

To use the PowerHA graphical interface to make an independent disk pool highly available, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs Details** page, click **Make Highly Available...** from the context menu of the Independent ASP that you want to make highly available.
6. Follow the instructions in the **Make Highly Available** wizard to make the independent disk pool highly available.

Configuring copy descriptions

Copy descriptions provide the information used in specific ASP sessions

Copy descriptions contain information required by IBM PowerHA SystemMirror for i to manage and control a specific copy of an independent auxiliary storage pool (IASP) in a high availability solution. The two types of copy descriptions used by PowerHA are:

- [ASP copy descriptions](#).
- [SVC copy descriptions](#).

Adding an ASP copy description

Establish the connectivity between the systems with the ASP copy description

To add an auxiliary storage pool (ASP) copy description to your IBM PowerHA environment you need to supply some or all of the following information depending on the type of copy relationship between the systems.

For all copy descriptions, have the following:

- an ASP device description name.
- the name of the device domain.

Copy descriptions for Metro Mirror, Global Mirror, or LUN Level Switching, require additional information about the storage host, including:

- the name of the cluster resource group (CRG).
- the cluster node name for the target copy location.

Note: This target location field is only needed if the copy description is for a FlashCopy session.

- a user name for IBM PowerHA to provide the storage host when creating the connection.
- the password for user account and any security credentials.
- IP addresses to the storage host.
- the name of the storage unit containing the partition or the LUNs.
- logical unit numbers of the disks in the ASP.
- consistency group information.

Note: For Global Mirror copy descriptions consistency group information is required.

When using LUN level switching:

- host identifier numbers for the nodes in the CRG recovery domain.
- volume groups associated with the host identifiers.

The Add Auxiliary Storage Pool Copy Description (**ADDASPCPYD**) command creates an ASP copy description. This procedure demonstrates how to create an ASP copy description for use in geographic mirroring, a Metro Mirror, a Global Mirror, a FlashCopy, or LUN level switch relationship.

The Add ASP Copy description screen can be accessed by using:

- the Work with Cluster (**WRKCLU**) command menu. Select option 10, Work with ASP copy descriptions and use option 1, Add copy to create a copy description.
- entering the **WRKASPCPYD** command that opens the Work with ASP Copy Descriptions screen. Use option 1, Add copy.
- typing the **ADDASPCPYD** command and pressing F4.

To Add an ASP copy description using the **WRKCLU** command menu, follow these steps:

Begin by selecting a name of the copy description, the storage connection type, and the associated ASP device description.

1. At the Work with Cluster (**WRKCLU**) command menu select option 10 Work with ASP copy descriptions to go to the Work with ASP copy descriptions screen.
2. On the Work with ASP copy descriptions screen, select 1 Add copy. Press Enter.
3. The Select Storage Connection screen appears. Depending on your storage controller and copy types, select:
 - 1, **Base** for geographic mirroring.
 - 2, **DSCLI** for DS8000 Metro Mirror, Global Mirror, FlashCopy, and LUN level switches.

Press Enter. The Add ASP Copy Description (**ADDASPCPYD**) command screen opens.

Next, provide the basic information all copy descriptions require:

4. On the top section of the Add ASP Copy Description (**ADDASPCPYD**) command screen, supply the following information to create the copy description:
 - a) the name of the ASP copy description to be created
 - b) the name of the ASP device description to be associated with the copy description.
 - c) the domain the host is a member of in the Device domain field, or type* to indicate the current domain of the node.
 - d) a cluster resource group name in the Cluster resource group field.
*NONE may be used with FlashCopy copy descriptions.
 - e) the cluster resource group site name in the Cluster resource group site field.
*NONE may be used if no cluster resource group is specified.

Provide information for the Storage host section. Storage host information is required for ASP copy descriptions using Metro Mirror, Global Mirror, and FlashCopy copy sessions.

5. Under the Storage Host section, provide the information necessary for PowerHA to create a connection:
 - a) type in the user name that PowerHA will supply to the storage host to create a connection.
 - b) enter the password associated with the user account.
 - c) provide the IP address of the storage host.

All copy descriptions require an entry in the Location field

6. In the Location field enter the cluster node that will control the IASP. Depending on the type of copy this description is for enter:
 - *DEFAULT for LUN level switching, Metro Mirror, and Global Mirror copies.
 - node - name if the copy description will be used for a FlashCopy target.
 - *NONE for a copy description that is for a no target FlashCopy which is not assigned to a specific system. This is a, no target FlashCopy.

Provide the Logical unit name (LUN) information if a copy description will use Logical unit name (LUN) switching. LUN information is required for ASP copy descriptions using Metro Mirror, Global Mirror, LUN level switching, and FlashCopy copy sessions.

7. Specify the LUN or LUNs associated with the copy description:
 - a) type in the name of the IBM System Storage device that contains the LUNs.
 - b) provide the logical unit numbers in the Logical unit range fields.
 - c) when using a Global Mirror copy description, provide the logical unit numbers for the consistency group in the Consistency group range fields.

Provide the recovery domain information if a copy description will use Logical unit name (LUN) switching.

8. Supply the connection information for each node in the CRG site recovery domain:
 - a) type in the name of the participating cluster node or nodes in the recovery domain.
 - b) specify the name of the IBM System Storage host identifiers that represents each cluster node on the storage device.
 - c) supply the name of the volume group or groups associated with the host identifier in the Volume group field.

If the copy description uses HyperSwap, you need to provide information for a second storage host, LUN and recovery domain configurations. Repeat steps 5, 7, and 8 for the secondary host.

9. When all information has been entered, press Enter to create the ASP copy description.

To verify that the entries in the copy description correct, use the **DSPASPCPYD** command or select option 5 on the Work with ASP copy descriptions menu page.

For details about the **ADDASPCPYD** command and specific fields, consult the F1 Help or visit the **ADDASPCPYD**, page.

Adding a SVC copy description

Establish the connectivity between the systems with the SVC copy description

To add a Storage Area Network (SAN) Volume Controller (SVC) copy description to your IBM PowerHA environment you need to supply some or all of the following information depending on the type of copy relationship between the systems.

For all copy descriptions, have the following:

- an auxiliary storage pool (ASP) device description name.
- the name of the device domain.
- the name of the cluster resource group (CRG).
- the cluster node name for the target copy location.

Note: This target location field is only needed if the copy description is for a FlashCopy session.

- a user name for IBM PowerHA to provide the storage host when creating the connection.
- the key file for user account.
- IP addresses to the storage host.
- the name of the storage unit containing the partition or the virtual disks.
- the virtual disk numbers of the disks in the ASP.

When using LUN level switching:

- host identifier numbers for the nodes in the CRG recovery domain.
- volume groups associated with the host identifiers.

The Add SAN Volume Controller Copy Description (**ADDSVCCPYD**) command creates a SVC copy description. This procedure demonstrates how to create an SVC copy description for use in geographic mirroring, a Metro Mirror, a Global Mirror, a FlashCopy, or LUN level switch relationship.

The Add SVC ASP Copy description screen can be accessed by using:

- the Work with Cluster (**WRKCLU**) command menu. Select option 10, Work with ASP copy descriptions and use option 1, Add copy to create a copy description.
- entering the **WRKASPCPYD** command that opens the Work with ASP Copy Descriptions screen. Use option 1, Add copy.
- typing the **ADDSVCCPYD** command and pressing F4.

To Add an SVC copy description using the **WRKCLU** command menu, follow these steps:

Begin by selecting a name of the copy description, the storage connection type, and the associated ASP device description.

1. At the Work with Cluster (**WRKCLU**) command menu select option 10 Work with ASP copy descriptions to go to the Work with ASP copy descriptions screen.
2. On the Work with SVC copy descriptions screen, select 1 Add copy and specify the ASP device description in the ASP Device field and type a name for the copy description in the ASP Copy field. Press Enter.
3. The Select Storage Connection screen appears. Using a SVC storage controller, select:
 - 3, **SVC** for SAN Volume Controller and Storewize System Storage Devices.

Press Enter. The Add SVC ASP Copy Description (**ADDSVCCPYD**) command screen opens.

Next, provide the basic information all copy descriptions require:

4. On the top section of the Add SVC ASP Copy Description (**ADDSVCCPYD**) command screen, supply the following information to create the copy description:
 - a) type in the name of the SVC copy description to be created.
 - b) enter the name of the SVC device description to be associated with the copy description.

- c) type the CRG name in the Cluster resource group field.
 - *NONE may be used for CRG name for FlashCopy copy descriptions.
 - d) type the cluster resource group site name in the Cluster resource group site field.
 - The option, *NONE may be used with FlashCopy copy descriptions.
 - e) enter the name of the cluster node associated with the copy description in the Node identifier field.
 - If *CRG was entered in the Cluster resource group field in **d.** above, then the Node identifier field here is *CRG.
 - If using FlashCopy, the node entry can be a specific node name or *NONE if using a no target FlashCopy.
5. Under the Storage Host section, provide the information necessary for PowerHA to create a connection:
- a) supply the user name of the SSH account used to connect to the SVC in the User name field.
 - b) in the Secure shell key file field, enter the local path to the SSH key pair used to authenticate the user with the SVC.
 - c) type in the IP address to connect to the SVC.

SVC copy descriptions require the logical references to the storage the SVC ASP uses.

6. In the Virtual disk range fields specify the virtual disks associated with the copy description:
- a) enter the beginning of the range in the Range start field.
 - b) enter the end of the range in the End range field.
 - c) determine which host identifiers to assign the virtual disk range to in the event the cluster node becomes the primary host for the CRG.
 - Use host identifiers for LUN level switching environments. Add the numeric identifiers of the host or the hosts from the recovery domain.
 - Configurations not using LUN switching can enter *ALL.

All SVC copy descriptions need a domain name.

7. In the Device domain field, enter the domain the host is a member of, or * to indicate the current domain of the node.

Provide the recovery domain information if a copy description will use Logical unit name (LUN) switching.

8. Supply the connection information for each node in the CRG site recovery domain:
- a) type in the name of the participating cluster node or nodes in the recovery domain.
 - b) specify the name of the SVC host identifiers that represents each cluster node on the storage device.
9. Once all information has been entered, press Enter to create the SVC ASP copy description.

To verify that the entries in the copy description correct, use the **DSPSVCCPYD** command or select option 5 on the Work with ASP copy descriptions menu page.

For details about the **ADDSVCCPYD** command and specific fields, consult the F1 Help or visit the **ADDSVCCPYD**, page.

Starting copy sessions

Learn about how to start ASP copy sessions for your high availability environment

A session is required to link two independent auxiliary storage pools (IASP) copy descriptions together and to indicate the type of copy relationship between the two. PowerHA creates a session for each storage communication method differently. Depending on your storage hardware and configuration select:

- ASP session for DS8000 System Storage devices using DSCLI or systems using a geographic mirror.
- CSM session for DS8000 System Storage devices using CSM.
- SVC session for IBM Storwize V3700, V5000, V7000, V9000, hardware running Spectrum Virtualize, and SAN Volume Controller (SVC) devices.

Most sessions use System Storage and Copy Services technologies to establish connections between the IASP copies. Metro Mirror, Global Mirror, FlashCopy, HyperSwap, and LUN level switch connections require one of these hardware-specific communication methods.

A geographic mirroring copy does not use System Storage and Copy Services technologies. A geographic mirror is created internally on the system and can be created using any type of storage compatible with that system.

Starting an ASP session

Start an ASP session between two systems using the Start ASP Session (STRASPSSN) command

Before starting a session, an auxiliary storage pool (ASP) device description, an ASP copy description for the source and an ASP copy description for the target systems are required. For information and instructions about device descriptions and ASP copy descriptions see the links to [Configuring copy descriptions](#) and [Configuring an ASP device](#).

The Start ASP Session (**STRASPSSN**) command creates a copy session between two systems. This procedure demonstrates how to create an ASP session for use in a DS8000 Metro Mirror, Global Mirror, or FlashCopy relationship.

The Start ASP Session screen can be accessed by:

- using the Work with Cluster (**WRKCLU**) command menu. Select option 10, Work with ASP copy descriptions and use option 21, Start session. Press Enter to open the Select Storage Connection panel.
- entering the **WRKASPCPYD** command that opens the Work with ASP Copy Descriptions screen. Use option 21, Start session. Press Enter to open the Select Storage Connection panel.
- typing the **STRASPSSN** command and pressing F4.

To create an ASP session with PowerHA and a storage unit using the **WRKCLU**, follow these steps:

1. At the Work with Cluster (**WRKCLU**) command menu select option 10 Work with ASP copy descriptions to go to the Work with ASP copy descriptions screen.
2. On the Work with ASP Copy Descriptions page, enter option 21, Start session in front of the copy description to be used in the session. Press Enter.
3. The Select Storage Connection screen appears. Depending on the session type, select:
 - option 1, BASE for a geographic mirroring session.
 - option 2, DSCLI for DS8000 Metro Mirror, Global Mirror, or FlashCopy sessions.Press Enter. The Start ASP Session (STRASPSSN) command screen appears.
4. On Start ASP Session (STRASPSSN) command screen. Enter the name for the new session in the Session field.
5. In the Session type field, enter session type.
6. In the ASP copy fields enter the preferred source and preferred target copy descriptions.
7. Type in the name of the device domain, or * to indicate the device domain for the current node. Then press Enter.
8. Depending on the session type entered, additional, different fields will be required.
 - For Metro Mirror and Global Mirror copy sessions. No other fields are needed.
 - For a FlashCopy session, specify the FlashCopy type and connection relationship.
 - a. Specify the type of FlashCopy in the type field:

***NOCOPY**

Data is copied only as it changes on the source copy. Useful for reducing space usage needed for FlashCopy.

***COPY**

Data is copied in the background. Useful for FlashCopy images that will exist for some time, or for reducing the performance impact that the target copy has on the source copy after the copy has completed.

b. Indicate if the connection relationship is to be maintained after the FlashCopy completes.

- For Geographic mirroring, indicate if the connection will be synchronous or asynchronous.

9. After providing the appropriate information needed for the session type, press Enter to start the copy session.

To create a session from the command line, you could enter:

```
STRASPSSN SSN(session-name) TYPE(*GEOMIR | *METROMIR | *GLOBALMIR | *FLASHCOPY)
ASPCPY(ASP copy description-name) SSPTIMO(*CFG | number of seconds)
PRIORITY(*CFG | *LOW | *MEDIUM | *HIGH) TRACKSPACE(*CFG | %) DEVDMN(* | device domain-name)
```

to start a session in the current device domain.

On the Work with ASP Copy Descriptions page, the ASP session is shown under the ASP Session and Session Type columns.

For additional information about the session, select option 25 on the Work with ASP Copy Descriptions page or use the **DSPASPSSN** command to display the session.

For details about the **STRASPSSN** or **DSPASPSSN** command and specific fields, consult the F1 Help or visit the **STRASPSSN** and **DSPASPSSN** pages.

Starting a CSM session

Start a CSM ASP session between two systems using the Start CSM Session (STRCSMSSN) command

Before starting a session, an ASP device description, an ASP copy description for the source and an ASP copy description for the target systems are required. In addition to the device and copy descriptions, a CSM session requires an High Availability (HA) configuration description to communicate with the CSM storage manager. For information and instructions about device descriptions, ASP copy descriptions, and HA configuration descriptions see the links to Configuring copy descriptions and Configuring an ASP device below.

The Start Copy Services Manager (CSM) Auxiliary Storage Pool (ASP) Session (**STRCSMSSN**) command creates a copy session between two systems. This procedure demonstrates how to create an CSM session for use in a Metro Mirror or Global Mirror relationship.

The Start CSM Session screen can be accessed by:

- using the Work with Cluster (**WRKCLU**) command menu. Select option 10, Work with ASP copy descriptions and use option 21, Start session. Press Enter to open the Select Storage Connection panel.
- entering the **WRKASPCPYD** command that opens the Work with ASP Copy Descriptions screen. Use option 21, Start session. Press Enter to open the Select Storage Connection panel.
- typing the **STRCSMSSN** command and pressing F4.

To create an CSM session with PowerHA and a storage unit using the **WRKCLU**, follow these steps:

1. At the Work with Cluster (**WRKCLU**) command menu select option 10 Work with ASP copy descriptions to go to the Work with ASP copy descriptions screen.
2. On the Work with ASP Copy Descriptions page, enter option 21, Start session. Press Enter to open the Select Storage Connection panel.
3. The Select Storage Connection screen appears. Select option 4, CSM from the Select the storage connection interface menu. Press Enter.
4. The Start CSM Session (STRCSMSSN) command screen appears. Enter the name for the new session in the Session field.
5. In the Session type field, enter session type.
6. Enter the CRG name.

7. After providing the appropriate information needed for the session type, press Enter to start the copy session.

To create a session from the command line, you could enter:

```
STRCSMSSN SSN(session-name) TYPE(*METROMIR | *GLOBALMIR) ASPCPY(ASP copy description-name)
DEVDMN(* | device domain-name)
```

to start a session in the current device domain.

On the Work with ASP Copy Descriptions page, the CSM session is shown under the ASP Session and Session Type columns.

For additional information about the session, select option 25 on the Work with ASP Copy Descriptions page or use the **DSPCSMSSN** command to display the session.

For details about the **STRCSMSSN** or **DSPCSMSSN** command and specific fields, consult the F1 Help or visit the [STRCSMSSN](#) and [DSPCSMSSN](#) page.

Starting a SVC session

Start a SVC ASP copy session between two systems using the Start SVC Session (STRSVCSSN) command

Before starting a session, an ASP device description, an SVC copy description for the source and an SVC copy description for the target systems are required. For information and instructions about device descriptions and ASP copy descriptions see the links to Configuring copy descriptions and Configuring an ASP device below.

The Start SVC Session (**STRSVCSSN**) command creates a copy session between two systems. This procedure demonstrates how to create an ASP session for use in a Metro Mirror, Global Mirror, or FlashCopy relationship.

The Start SVC Session screen can be accessed by:

- using the Work with Cluster (**WRKCLU**) command menu. Select option 10, Work with ASP copy descriptions and use option 21, Start session. Press Enter to open the Select Storage Connection panel.
- entering the **WRKASPCPYD** command that opens the Work with ASP Copy Descriptions screen. Use option 21, Start session. Press Enter to open the Select Storage Connection panel.
- typing the **STRSVCSSN** command and pressing F4.

To create an SVC session with PowerHA and a storage unit using the **WRKCLU**, follow these steps:

1. At the Work with Cluster (**WRKCLU**) command menu select option 10 Work with ASP copy descriptions to go to the Work with ASP copy descriptions screen.
2. On the Work with ASP Copy Descriptions page, enter option 21, Start session. Press Enter to open the Select Storage Connection panel.
3. The Select Storage Connection screen appears. Select option 3, SVC from the Select the storage connection interface menu. Press Enter.
4. On the Start SVC Session (**STRSVCSSN**) command page, type a name for your session in the Session field.
5. In the Session type field enter the type of session to create.
6. Type in the name of the device domain, or * to indicate the device domain for the current node. Then press Enter.
7. Depending on the session type entered, different fields will be required
 - For a Metro Mirror or Global Mirror session, provide the name of your cluster resource group (CRG).
 - For a FlashCopy session you enter:
 - a. The preferred source and target ASP copy descriptions.
 - b. If this session is an incremental flash copy.

- c. The rate (from 0-100) at which the data is copied from the virtual source disks to the target virtual disks.
- d. The rate (from 0-100) at which the cleaning process is done on the FlashCopy mapping.
- e. The grain size in kilobytes.
- f. A consistency group and a reverse consistency group.

Note: Using the default *GEN allows the system to generate the consistency group names for you on the storage device.

- 8. After providing the appropriate information needed for the session type, press Enter to start the copy session.

To create a session from the command line, you could enter:

```
STRSVCSSN SSN(session-name) TYPE(*GEOMIR | *METROMIR | *GLOBALMIR | *FLASHCOPY) ASPCPY(ASP copy
description-name)
SSPTIMO(*CFG | number of seconds) PRIORITY(*CFG | *LOW | *MEDIUM | *HIGH)
TRACKSPACE(*CFG | %) DEVDMN(* | device domain-name)
```

to start a session in the current device domain.

On the Work with ASP Copy Descriptions page, the SVC session is shown under the ASP Session and Session Type columns.

For additional information about the session, select option 25 on the Work with ASP Copy Descriptions page or use the **DSPSVCSN** command to display the session.

For details about the **STRSVCSN** or **DSPSVCSN** command and specific fields, consult the F1 Help or visit the [STRSVCSN](#) and [DSPSVCSN](#) page.

Adding an high availability policy

Adding an HA policy can simplify management of PowerHA tasks

The Add High Availability (HA) Policy (**ADDHAPCY**) command creates a policy to control specific behavior related to your cluster and IBM PowerHA SystemMirror for i high availability environment. This procedure demonstrates how to create an HA policy for your cluster.

The Add HA Policy screen can be accessed by:

- using the Work with Cluster (**WRKCLU**) command menu. Select option 12, Work with HA policies and use option 1, Add policy. Press F4 to open the **ADDHAPCY** panel.
- running the **WRKCLU** with the ***HAPCY** option: **WRKCLU OPTION(*HAPCY)** on the command line.
- entering the **WRKHAPCY** command that opens the Work with HA policies screen. Use option 1, Add policy and press F4 to open the **ADDHAPCY** panel.
- typing the **ADDHAPCY** command and pressing F4.

To add an HA policy using the **ADDHAPCY** command, follow these steps:

1. Type the **ADDHAPCY** command into the command line and press F4.
This opens the Add HA Policy (**ADDHAPCY**) command screen.
2. Enter the name of the HA policy to add.
QHA_COMM_STRICT_CERT_CHECK for example.
3. Specify the name of the domain to which the policy applies. Enter:

- the name of the domain the HA policy applies to.
- *NONE if the HA policy applies to no specific domain.

4. Add any HA policy-specific information in the Policy Qualifier field.

The possible values depend on the specific HA policy you are adding to the cluster domain. Check the definition for that policy for additional information.

5. Type any HA policy-specific values in the Policy value field, or enter *BLANK.

The possible values of this field depend on the specific HA policy you are adding. Check the definition for that policy for additional information.

6. Press Enter to add the policy to your cluster domain.

To add an instance of the **QCST_CRG_CANCEL_FAILOVER** PowerHA policy using a sequence from the command line, enter:

```
ADDHAPCY PCY(QCST_CRG_CANCEL_FAILOVER) PCYDMN(CRG) QUAL('SCOPE(*SITE)') VALUE('EVENT(*CLUFAIL *ENDTCP *PWRDWN SYS)')
```

to create an instance of the policy for the policy domain CRG and qualifier **SCOPE** of ***SITE** to prevent failovers of **EVENT** types ***CLUFAIL**, **ENDTCP**, and ***PWRDWN SYS**.

Verify that the entries in the HA policy are correct with the Display HA Policy (**DSPHAPCY**) command. If changes are required, they are made with the Change HA Policy (**CHGHAPCY**) command.

For details about the **ADDHAPCY** command and specific fields, consult the F1 Help or visit the [ADDHAPCY](#) page.

Configuring geographic mirroring

Geographic mirroring is a subfunction of cross-site mirroring. To configure a high-availability solution by using geographic mirroring, you need to configure a mirroring session between the production system and the backup system.

Before configuring geographic mirroring, you must have an active cluster, nodes, and CRG. The independent disk pools which you plan to use for geographic mirroring must also be varied off (unavailable) to complete configuration. The topic, [Scenario: Geographic mirroring](#), provides step-by-step instructions for setting up a high-availability solution that is based on geographic mirroring.

To use the PowerHA graphical interface to configure geographic mirroring follow these steps:

1. In a web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details ...** from the context menu of the independent disk pool for which you want to configure geographic mirroring.
6. On the **Independent ASP Details** page, select **Configuring Mirroring ...** from the context menu of the production copy of the independent disk pool.
7. Follow the instructions in the **Create Independent ASP** wizard to create an independent disk pool.

To use the Configuration and Service graphical interface to configure geographic mirroring, follow the steps below. The Configuration and Service graphical interface does not show up if IBM PowerHA SystemMirror for i licensed program is installed.

Configuration and Service graphical interface (IBM Navigator for i)

1. Log on to the system with your user profile and password.
2. Log on to the system with your user profile and password.
3. Select **Configuration and Service** from your IBM Systems Director Navigator for i window.
4. Select **Disk Pools**.
5. Select the disk pool that you want to use as the production (source) copy.
6. On the **Independent ASP Details** page, select **Configure Mirroring...** from the context menu of the production copy of the independent disk pool.
7. Follow the instructions in the **Configure Mirroring** wizard to configure geographic mirroring.

Related information


[Configure Geographic Mirror \(CFGGEOMIR\) command](#)

Configuring Metro Mirror

For IBM i high availability solutions that use IBM System Storage Metro Mirror technology, you need to configure a session between the IBM i machine and IBM System Storage external storage units that have Metro Mirror configured. In IBM i, Metro Mirror sessions do not set up the mirroring on the external storage units, but rather sets up a relationship between the IBM i systems and the existing Metro Mirror configuration on external storage units.

Before creating a Metro Mirror session on IBM i, you should have configured Metro Mirror on the IBM System Storage external storage units.

- For information about using Metro Mirror on IBM System Storage DS8000, see [Copy Services in the IBM](#)

[System Storage DS8000 Information Center](#) 

- For information about using Metro Mirror with SAN Volume Controller (SVC) or Storwize storage devices, see [IBM SAN Volume Controller Information Center](#).

To use the PowerHA graphical interface to configure Metro Mirror, follow these steps:

1. In a web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details ...** from the context menu of the independent disk pool for which you want to configure Metro Mirror.
6. On the **Independent ASP Details** page, select **Configure Mirroring ...** from the context menu of the production copy of the independent disk pool.
7. Follow the instructions in the **Configure Mirroring** wizard to configure Metro Mirror.

To use the Configuration and Service graphical interface to configure Metro Mirror session, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Select **Configuration and Service** from your IBM Navigator for i window.
4. Select **Disk Pools**.
5. Select the disk pool that you want to use as the production (source) copy.
6. From the **Select Actions** menu, select **New Session**.
7. Follow the wizard's instructions to complete the task.

Related concepts

[PowerHA supported storage servers](#)

IBM System Storage provides enhanced storage capabilities.

Related information

[Add ASP Copy Description \(ADDASPCPYD\) command](#)


[Start ASP Session \(STRASPSSN\) command](#)

Configuring Global Mirror

For IBM i high availability solutions that use IBM System Storage Global Mirror technology, you need to configure a session between the IBM i machine and IBM System Storage external storage units that have Global Mirror configured. In IBM i, Global Mirror sessions do not set up the mirroring on the external storage units, but rather sets up a relationship between the IBM i systems and the existing Global Mirror configuration on external storage units.

Before creating a Global Mirror session on IBM i, you should have configured Global Mirror on the IBM System Storage external storage units.

- For information about using Global Mirror on IBM System Storage DS8000, see [Copy Services in the IBM](#)

[System Storage DS8000 Information Center](#) 

- For information about using Global Mirror with SAN Volume Controller (SVC) or Storwize storage devices, see [IBM SAN Volume Controller Information Center](#).

To use the PowerHA graphical interface to create a new independent disk pool, follow these steps:

1. In a web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details ...** from the context menu of the independent disk pool for which you want to configure Global Mirror.
6. On the **Independent ASPs Details** page, select **Configure Mirroring ...** from the context menu of the production copy of the independent disk pool.
7. Follow the instructions in the **Create Independent ASP** wizard to create an independent disk pool.

To configure global mirroring, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Select **Configuration and Service** from your IBM Navigator for i window.
4. Select **Disk Pools**.
5. Select the disk pool that you want to use as the production (source) copy.
6. From the **Select Actions** menu, select **New Session**.
7. Follow the wizard's instructions to complete the task.

Related concepts

[PowerHA supported storage servers](#)

IBM System Storage provides enhanced storage capabilities.

Related information

[Add ASP Copy Description \(ADDASPCPYD\) command](#)

[Start ASP Session \(STRASPSSN\) command](#)

Configuring switched logical units (LUNs)

Switched logical units is an independent disk pool that is controlled by a device cluster resource group and can be switched between nodes within a cluster. For IBM i high availability solutions that use switchable logical units with IBM® System Storage™, you need to configure an ASP Copy Description that defines the host identifiers and volume groups for each cluster node in which the ASP device can be switched.

In IBM i, the creation of an ASP Copy Description for switchable logical units does not set up the host identifiers and volume groups on the external storage units, but rather sets up a relationship between the IBM i systems and existing host identifiers and volume groups on the external storage units.

Before creating a copy description for switchable logical units on IBM i, you should have configured the logical units on the IBM System Storage external storage unit as well as created the independent auxiliary storage pool and device cluster resource group that will control the switching. For information about using the IBM System Storage DS8000®, see IBM System Storage DS8000 Information Center.

For details on using other storage technologies, see [“PowerHA supported storage servers” on page 25](#).

To configure switchable logical units, follow these steps:

1. Enter the Add ASP Copy Description (**ADDASPCPYD**) command at an IBM i command prompt.

2. Enter the appropriate names for ASP device, cluster resource group, cluster resource group site, IBM System Storage host, location, and logical unit name.
3. Enter the appropriate cluster node names, host identifiers, and volume groups in the recovery domain field.
4. Create an ASP Copy Description for every ASP device that is to use switchable logical units. All ASP devices in the cluster resource group must be defined by a separate ASP copy description.

Related concepts

[PowerHA supported storage servers](#)

IBM System Storage provides enhanced storage capabilities.

Configuring a FlashCopy session

For IBM i high-availability environments that use IBM System Storage technology, you can configure a FlashCopy session to create a point-in-time copy of data.

For information on using the FlashCopy feature on IBM System Storage, see [“PowerHA supported storage servers”](#) on page 25.

Configuring a FlashCopy when IBM PowerHA SystemMirror for i licensed program is installed

To configure FlashCopy by using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the PowerHA window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to create a FlashCopy.
6. On the **Independent ASP Details** page, select **Create FlashCopy...** from the context menu of which you want to create the FlashCopy.
7. Follow the instructions in the Create FlashCopy wizard to create a FlashCopy.

Related concepts

[PowerHA supported storage servers](#)

IBM System Storage provides enhanced storage capabilities.

Configuring DS8000 Full System HyperSwap

For System i high availability solutions using HyperSwap, detection of the HyperSwap configuration is automatic on the System i machine after appropriate configuration has been performed on the IBM System Storage external storage units.

The steps assume knowledge of configuring and managing an IBM System Storage DS8000. For information about using an IBM System Storage DS8000 unit, see [Copy Services in the IBM System Storage DS8000 Information Center](#).

To configure HyperSwap, follow these steps:

1. Create LUNs on the source DS8000.
2. Assign LUNs on source DS8000 to the System i machine.
3. Create LUNs on the target DS8000. Do not assign them to the System i until after Metro Mirror is configured.
4. Configure Metro Mirror between the source and target DS8000.
5. Assign the LUNs on the target DS8000 to the same System i machine.
6. Verify the HyperSwap configuration with the Display HyperSwap Status (DSPHYSSTS) command.

To understand how HyperSwap interfaces with affinity, see [“Defining HyperSwap Affinity”](#) on page 92

If your established HyperSwap environment requires additional disk units for more capacity, read [Adding disk units to a HyperSwap configuration](#).

Related tasks

[Defining HyperSwap Affinity](#)

By using DS8000 HyperSwap combined with logical unit (LUN) level switching and or PowerVM Live Partition Mobility, it is possible to define which IBM i systems should use which IBM System Storage DS8000 as their primary. Upon accomplishing a live partition mobility switch or a LUN switching CRG switch, if the partition is no longer running on the preferred IBM System Storage unit, a HyperSwap switchover to the secondary IBM System Storage unit is done as part of the switching process.

Related information

[Change HyperSwap Status \(CHGHYSSTS\) command](#)

[Display HyperSwap Status \(DSPHYSSTS\) command](#)

[Live Partition Mobility](#)

Defining HyperSwap Affinity

By using DS8000 HyperSwap combined with logical unit (LUN) level switching and or PowerVM Live Partition Mobility, it is possible to define which IBM i systems should use which IBM System Storage DS8000 as their primary. Upon accomplishing a live partition mobility switch or a LUN switching CRG switch, if the partition is no longer running on the preferred IBM System Storage unit, a HyperSwap switchover to the secondary IBM System Storage unit is done as part of the switching process.

To define which DS8000 unit can be used with which IBM i systems, HA configuration descriptions are used. The Add HA Configuration Description (ADDHACFGD) command can be used to define an affinity relationship between the serial number of the server that is hosting the IBM i partition and the IBM System Storage unit identifier of the DS8000 storage server.

Related tasks

[Configuring DS8000 Full System HyperSwap](#)

For System i high availability solutions using HyperSwap, detection of the HyperSwap configuration is automatic on the System i machine after appropriate configuration has been performed on the IBM System Storage external storage units.

Related information

[Add HyperSwap Storage Description \(ADDHYSSTGD\) command](#)

[Change HyperSwap Storage Description \(CHGHYSSTGD\) command](#)

[Remove HyperSwap Storage Description \(RMVHYSSTGD\) command](#)

[Live Partition Mobility](#)

Configuring DS8000 HyperSwap with independent auxiliary storage pools (IASPs)

IASP-based HyperSwap environments require both HyperSwap and logical unit number (LUN) switching configuration.

These steps assume the user has experience configuring and managing an IBM System Storage DS8000. For information about using an IBM System Storage DS8000 unit, see [Copy Services in the IBM System Storage DS8000 Information Center](#).

If necessary, use HyperSwap independently as a disk protection solution in a single-system environment without any LUN configuration. This has limited uses.

Inside a high availability environment with IASPs, both HyperSwap and LUN switching must be configured. The IASPs in the HyperSwap configuration require LUN volume groups separate from any of the SYSBAS LUNs. Any secondary IASPs in the same HyperSwap relationship associate with the primary IASP only. Primary and secondary IASPs cannot split into separate relationships. Other primary IASPs or user defined file system (UDFS IASP) outside of the HyperSwap environment have separate defined relationships.

IBM i high availability solutions using DS8000 HyperSwap automatically detect the HyperSwap IASPs after the DS8000 is configured appropriately.

To configure HyperSwap for use with IASPs, follow these steps:

1. Create LUNs on the source DS8000 system.
2. Assign those LUNs on the source DS8000 to the System i partition.
Note: The IASP LUNs must be in separate volume groups from any SYSBAS LUNs, on both the source and target DS8000.
3. Create LUNs on the target DS8000 but do not assign them to the IBM i until after the Metro Mirror has been configured.
Note: The IBM i device driver ensures data consistency for HyperSwap switchover and failover operations. Do not use Metro Mirror consistency groups here.
4. Configure Metro Mirror between the source and target DS8000 with the **mkpprcpath** command on the DS8000 from the DSCLI.
5. Start Peer-to-Peer Remote Copy (PPRC) with the **mkpprc** command on the DS8000 from the DSCLI.
6. Assign the LUNs on the target DS8000 to the same IBM i partition.
7. Verify the HyperSwap configuration with the Display HyperSwap Status (**DSPHYSSTS**) command.
The status of the HyperSwap drive pairs configured should display in the DSCLI

If your established HyperSwap environment requires additional disk units for more capacity, read [Adding disk units to a HyperSwap configuration](#).

Configuring LUN level switching in the HyperSwap environment on IBM i

Perform the following steps to set up the LUN level switching in an IASP-based HyperSwap environment on the IBM i partition:

1. Pause PPRC with the **pausepprc** command on the DS8000 from the DSCLI.
2. Create the IASP with the Configure Device ASP (**CFGDEVASP**) command.
To see the units for the IASP, use the Display HyperSwap Status (DSPHYSSTS) command.
3. Resume replication with the Change HyperSwap Status command, **CHGHYSSTS OPTION(*START) ASPDEV(iasp-name)**.
4. Create the cluster, the device domain, and device CRG to control the switching.
All nodes in the recovery domain of the device CRG must be in the same device domain.
5. Create the ASP device description on the backup node.
6. Use the Add ASP Copy Description (**ADDASPCPYD**) command to configure both LUN level switching and HyperSwap.
The nodes, host connections, and volume groups, which can access the IASP are entered in the recovery domain parameter. The storage host information, LUN ranges, and recovery domain information for the second DS8000 in the HyperSwap relationship are entered by using the **STGHOST2**, **LUN2**, and **RCYDMN2** parameters.
7. Create an ASP copy description for every ASP device that is to use LUN level switching with HyperSwap.
All ASP devices in the cluster resource group must be defined by a separate ASP copy description.
8. Verify the HyperSwap configuration using the Display HyperSwap Status (DSPHYSSTS) command and the correct ASP copy description configuration using the Display ASP Copy Description (DSPASPCPYD) command.
To see the new units for the IASP, use the Display HyperSwap Status (**DSPHYSSTS**) command.

Managing PowerHA

After you have configured a PowerHA solution, you can manage that solution by using several interfaces that are related to high availability.

Scenarios: Managing high availability solutions

As a system operator or administrator of your high-availability solution, you need to perform common tasks like backup and system maintenance in your high-availability environment.

The following scenarios provide instructions on performing common system tasks, such as backups and upgrades, as well as examples of managing high-availability events, such as cluster partitions and failover. For each scenario, a model environment has been chosen. The instructions for each scenario correspond to that particular high-availability solution and are meant for example purposes only.

Scenarios: Performing backups in a high-availability environment

Depending on your high availability-solution and your backup strategy, the method for backing up data can be different. However, there is a common set of tasks when you perform backup operations for systems in a high availability environment.

In several high availability-solutions, you have the capability of performing remote backups from the second copy of data that is stored on the backup system. Remote backups allow you to keep your production system operational, while the second system is backed up. Each of these scenarios provides examples of two high-availability solutions where backups are performed remotely on the backup system.

In the first scenario, remote backups are performed in a high availability solution that uses geographic mirroring technology. The second scenario shows how the FlashCopy feature can be used in a high-availability environment that use IBM System Storage solutions, such as metro or global mirror.

Scenario: Performing backups in geographic mirroring environment

This scenario provides an overview of tasks that are necessary when performing a remote backup in a PowerHA solution that uses geographic mirroring.

Overview

In this example, a system administrator needs to perform a backup of data stored on independent disk pools that are used in a high-availability solution based on geographic mirroring technology. The administrator does not want to affect the production system by taking it offline to perform the backup. Instead the administrator plans to temporarily detach the mirrored copy, and then perform a backup from the second copy of data located on independent disk pools at a remote location.

Note: Detaching the mirrored copy essentially ends geographic mirroring until the copy is reattached to the production. During the time it is detached, high availability and disaster recovery are not operational. If an outage to the production system occurs during this process, some data will be lost.

Details

The following graphic illustrates this environment:



Configuration steps

Complete the following steps when performing a backup of a mirror copy using the PowerHA graphical interface:

1. [“Detaching mirror copy” on page 161](#)
2. [Making disk pool available](#)

3. [Backing up independent disk pool](#)
4. [Make disk pool unavailable](#)
5. [“Reattaching mirror copy” on page 162](#)

Complete the following steps when performing a backup of a mirror copy using other interfaces:

1. [“Quiescing an independent disk pool” on page 146](#)
2. [“Detaching mirror copy” on page 161](#)
3. [“Resuming an independent disk pool” on page 146](#)
4. [Making disk pool available](#)
5. [Backing up independent disk pool](#)
6. [Make disk pool unavailable](#)
7. [“Reattaching mirror copy” on page 162](#)

Scenario: Performing a FlashCopy function

In this example, an administrator wants to perform a backup from the remote copy of data that is stored in an external storage unit at the backup site. Using the FlashCopy function available with IBM Storage Solutions, the administrator reduces his backup time considerably.

Overview

In this example, a system administrator needs to perform a backup of data that is stored on IBM System Storage external storage units. The administrator does not want to affect the production system by taking it offline to perform the backup. Instead, the administrator plans to perform a FlashCopy operation, which takes a point-in-time capture of the data. From this data, the administrator backs up the data to external media. The FlashCopy operation only takes a few seconds to complete, thus reducing the time for the entire backup process.


Although in this example the FlashCopy feature is being used to for backup operations, it should be noted that the FlashCopy feature has multiple uses. For example, FlashCopy can be used for data warehousing to reduce query workload on production systems, or for duplicating production data to create a test environment.

A similar scenario can also be accomplished with other system storage technologies. For more information on storage technologies that support FlashCopy, see [“PowerHA supported storage servers” on page 25](#).

Configuration steps

Complete the following steps when performing a FlashCopy using the PowerHA graphical interface:

1. Configure the IBMSystem Storage external storage units forFlashCopy. For information about using the FlashCopy function on IBM System StorageDS8000, see [Copy Services in the IBM System Storage](#)

[DS8000 Information Center](#) 

2. [“Configuring a FlashCopy session” on page 91](#)
3. [Make disk pool available](#)
4. [Backing up independent disk pool](#)

Complete the following steps when performing a FlashCopy using other interfaces:

1. Configure the IBMSystem Storage external storage units forFlashCopy. For information about using the FlashCopy function on IBMSystem StorageDS8000, see [Copy Services in the IBM System Storage](#)

[DS8000 Information Center](#) 

2. [“Quiescing an independent disk pool” on page 146](#)

3. [“Configuring a FlashCopy session” on page 91](#)
4. [“Resuming an independent disk pool” on page 146](#)
5. [Make disk pool available](#)
6. [Backing up independent disk pool](#)

Related concepts

[PowerHA supported storage servers](#)

IBM System Storage provides enhanced storage capabilities.

Scenario: Upgrading operating system in a high-availability environment

In this example, a system administrator is upgrading the operating system for two IBM i systems in a PowerHA solution that is based on geographic mirroring.

Overview

The system administrator needs to upgrade the operating system for two systems in the high-availability environment. In this example, there are two nodes: System 1 and System 2. System 1 is the production copy and System 2 is the mirror copy. Both systems are at IBM i V7R1. The independent disk pool is online, geographic mirroring is active, and the systems are synchronized. The system administrator wants to upgrade both of these systems to IBM i 7.2.

Details

The following graphic illustrates the environment:



Configuration steps

1. [Detach the mirror copy \(System 2\)](#).
2. [End the CRG \(System 2\)](#).
3. [Stop the node \(System 2\)](#).
4. [Upgrading System 2 to the new release. See Upgrading or replacing IBM i and related software for details.](#)
5. [Install IBM PowerHA SystemMirror for i licensed program.](#)
6. [Make disk pool available](#) and test applications on System 2. Testing the applications ensures that they operate as expected within the new release. After application tests are completed, you can finish the upgrade by completing the rest of these steps.
7. [Make disk pool unavailable](#) on the detached mirrored copy (System 2).
8. [Reattach mirrored copy](#). This initiates a resynchronization of the mirrored data. After the resynchronization is completed, you can continue the upgrade process.
9. [Performing switchovers](#). This makes the mirrored copy (System 2) the new production copy and the production copy (System 1) becomes the new mirrored copy.
Note: Geographic mirroring is suspended because you cannot perform geographic mirroring from n-1 to n. You can perform geographic mirroring from n to n-1 without problems. In this scenario, geographic mirroring is suspended after a switchover is completed. Data is now no longer mirrored during the remainder of the upgrade process because there is no longer a valid backup system.
10. [End the CRG \(System 1\)](#).
11. [Stop the node \(System 1\)](#).
12. [Upgrade System 1 to the new release. See Upgrading or replacing IBM i and related software for details.](#)

13. [Install IBM PowerHA SystemMirror for i licensed program.](#)
14. [Start nodes \(System 1\).](#)
15. [Start CRGs \(System 1\).](#)
16. [Resume mirroring](#)
17. [Perform switchover.](#) This switches the current mirrored copy (System 1) back to the production copy and the production copy (System 2) to become the mirrored copy. This is the original configuration before the upgrade.
18. [Adjusting the cluster version of a cluster](#)
19. [Adjusting the high availability version of PowerHA LP](#)

Example: Upgrading operating system

In a high-availability environments, you must perform specific actions prior to performing operating system upgrades.

The following examples can help you determine what you need to do to perform an upgrade in your cluster environment. Before performing the upgrade or any actions you should first determine the current cluster version for your cluster.

Notes:

1. 7.1 represents the current release of the operating system.
2. 7.2 represents the new release of the operating system.
3. V6R1 represents the prior release of the operating system.

Example 1: The node to be upgraded is at IBM i 7.1. All other nodes in the cluster are at IBM i 7.1 or higher. The current cluster version is 7.

Action:

1. [Upgrade](#) node to IBM i 7.2.
2. [Start](#) the upgraded node.

Example 2: The node to be upgraded is at IBM i 7.1. All other nodes in the cluster are at IBM i 7.1 or higher. The current cluster version is 6.

Action:

1. [Upgrade](#) the node to IBM i 7.2.
2. [Start](#) the upgraded node.

Example 3: The node to be upgraded is IBM i V5R4. All other nodes in the cluster are at IBM i V5R4 or higher. The current cluster version is 5.

Action:

1. [Upgrade](#) the node to IBM i 7.1.
2. [Start](#) the upgraded node.

Example 4: The node to be upgraded is at IBM i V6R1. All other nodes in the cluster are at IBM i V5R4 or higher. The current cluster version is 5.

Actions:

1. [Upgrade](#) all nodes to V6R1.
2. [Start](#) all of the upgraded nodes.
3. [Change](#) the cluster version to 6.
4. [Upgrade](#) the node to 7.2.
5. [Start](#) the upgraded node.

Example 5: The node to be upgraded is at IBM i V5R4 or lower. All other nodes in the cluster are at IBM i V5R4 or lower. The current cluster version is less than or equal to 5.

Actions:

1. Upgrade all nodes to V6R1.
2. Start all of the upgraded nodes.
3. Change the cluster version to 6.
4. Upgrade the node to 7.2.
5. Start the upgraded node.

The following table provides actions you need to take when performing an upgrade in a cluster environment.

Table 8. Upgrading nodes to IBM i 7.2

Current[®] release of node you are upgrading	Current cluster version	Actions
V7R1	6 or 7	<ol style="list-style-type: none"> 1. <u>Upgrade</u> the node to IBM i 7.2. 2. <u>Start</u> the upgraded node.
V6R1	5 or 6	<ol style="list-style-type: none"> 1. <u>Upgrade</u> the node to IBM i 7.2. 2. <u>Start</u> the upgraded node.
V5R4 or lower	less than or equal to 5	<ol style="list-style-type: none"> 1. <u>Upgrade</u> all nodes to V6R1. 2. <u>Start</u> all of the upgraded node. 3. <u>Change</u> the cluster version to 6. 4. <u>Upgrade</u> the node to IBM i 7.2. 5. <u>Start</u> the upgraded node.

Managing clusters

Using the PowerHA graphical interface, you can perform many tasks that are associated with the cluster technology that is the basis of your IBM i high availability solution. These tasks help you manage and maintain your cluster.

Note: The PowerHA graphical interface allows you to perform these tasks from any node in the cluster.

Some of the changes that you can make to the cluster after you configure it include the following:

Cluster tasks

- [“Creating a cluster” on page 51](#)
- [“Deleting a cluster” on page 101](#)
- [“Specifying message queues” on page 55](#)
- [Add a node to a cluster](#)
- [Remove nodes from a cluster](#)
- [Start a cluster node](#)
- [End a cluster node](#)
- [“Displaying node properties” on page 104](#)
- [“Adding a node to a device domain” on page 58](#)
- [“Removing a node from a device domain” on page 106](#)
- [“Add a cluster monitor to a node” on page 106](#)

- [“Removing a cluster monitor ” on page 107](#)
- [“Monitoring cluster status” on page 102](#)
- [Adjust the cluster version of a cluster to the latest level](#)
- [“Adjusting the PowerHA version” on page 99](#)

Cluster resource group tasks

- [“Creating cluster resource groups \(CRGs\)” on page 64](#)
- [“Deleting a CRG” on page 109](#)
- [“Starting a CRG” on page 54](#)
- [“Stopping a CRG” on page 109](#)
- Add a node to a cluster resource group
- Remove a node from a cluster resource group
- [“Changing the recovery domain for a CRG” on page 109](#)
- [“Performing switchovers” on page 55](#)
- [“Displaying CRG status” on page 107](#)
- Add a node to a device domain
- Remove a node from a device domain

Cluster administrative domain tasks

- [“Creating a cluster administrative domain ” on page 75](#)
- [“Deleting a cluster administrative domain” on page 124](#)
- [“Changing the properties of a cluster administrative domain” on page 124](#)
- [“Starting a cluster administrative domain” on page 76](#)
- [“Stopping a cluster administrative domain” on page 123](#)
- [“Adding a node to the cluster administrative domain” on page 76](#)
- [“Adding monitored resource entries” on page 78](#)
- [“Removing monitored resource entries” on page 126](#)
- [“Listing monitored resource entries” on page 126](#)
- [“Displaying monitored resource entry messages” on page 145](#)

Miscellaneous tasks

- [“Displaying cluster configuration” on page 101](#)
- [“Saving and restoring cluster configuration” on page 102](#)
- [“Cluster deconfiguration checklist” on page 104](#)
- [“Managing failover outage events” on page 119](#)

Adjusting the PowerHA version

The PowerHA version is the version at which the nodes in the cluster that is managed by the PowerHA product are actively communicating with each other.

The PowerHA version values determine which functions can be used by the PowerHA product. The PowerHA version may require a certain cluster version in order to operate. For example, PowerHA version 2.0 requires a current cluster version of 7.

The current PowerHA version is set when a cluster is created. If a cluster exists, the current PowerHA version is set to the lowest supported version.

Like cluster version, PowerHA has a current and potential version level. The current PowerHA version is the version at which the nodes in the cluster, which are known by the PowerHA product are actively communicating with each other. The potential PowerHA version is the highest PowerHA version the node can support. The PowerHA version cannot be changed until all PowerHA nodes are installed with a common potential PowerHA version. The potential PowerHA version can be between n and $n+3$. For example, the current PowerHA version is 2.0, NODE1 has a potential PowerHA version of 3.0, NODE2 has a potential PowerHA version of 4.0, and NODE3 has a potential PowerHA version of 5.0. All three nodes can support version 3.0, so the current PowerHA version can be adjusted to 3.0.

Beginning with PowerHA version 2.0, if a node with an incompatible potential PowerHA version is added to the cluster, the node will successfully be added, but the node will be considered "unknown" to PowerHA. If a node is unknown to PowerHA, certain product functions cannot be performed on the node. A node is known to PowerHA if the node has the PowerHA product installed, and the potential PowerHA version is compatible with the current PowerHA version.

For users of Cluster Administrative Domain, when the current PowerHA version is adjusted to 3.0 or higher, monitored resource entries in the cluster administrative domain may be affected. If all attributes supported at the previous cluster and PowerHA versions are being monitored for a monitored resource entry, then PowerHA will automatically update that monitored resource entry to also monitor any new attributes supported at the current cluster version and current PowerHA version.

The current PowerHA version can be changed with the **Change Cluster Version (CHGCLUVER)** command.

The **Change Cluster Version (CHGCLUVER)** command can only be used to adjust to a higher cluster or PowerHA version. If you want to adjust the PowerHA version by two, the **CHGCLUVER** command must be run twice.

The current cluster version cannot be set higher than the lowest potential node version in the cluster. Likewise, the current PowerHA version cannot be set higher than the lowest potential PowerHA version of any node in the cluster. PowerHA potential version of any node in the cluster. To view the potential node and PowerHA versions, use the **Display Cluster Information (DSPCLUINF)** command.

To adjust the PowerHA version using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Select **PowerHA** from the IBM Navigator for i window.
4. On the PowerHA page, select **Properties ...** from the Select Action menu next to the cluster name.
5. Click **Edit** in the General section.
6. Select a new PowerHA version and click **Save**.

Related concepts

[Cluster version](#)

Related information

[Change Cluster Version \(CHGCLUVER\) command](#)

Adjusting the cluster version of a cluster

The cluster version defines the level at which all the nodes in the cluster are actively communicating with each other.

Cluster versioning is a technique that allows the cluster to contain systems at multiple release levels and fully interoperate by determining the communications protocol level to be used.

To change the cluster version, all nodes in the cluster must be at the same potential version. The cluster version can then be changed to match the potential version. This allows the new function to be used. The version can only be increased by one. It cannot be decremented without deleting the cluster and re-creating it at a lower version. The current cluster version is initially set by the first node that is defined in the cluster. Subsequent nodes added to the cluster must be equal to the current cluster version or the next level version; otherwise, they cannot be added to the cluster.

If you are upgrading a node to a new release, you must ensure that the node has the appropriate cluster version. Cluster only supports a one version difference. If all the nodes in the cluster are at the same release, you should upgrade to the new release, before changing the cluster version. This ensures that all functions associated with the new release are available. See the topic, [“Scenario: Upgrading operating system in a high-availability environment”](#) on page 96 for detailed actions for upgrading to a new release.

To adjust the cluster version using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, select **Properties ...** from the **Select Action** menu next to the cluster name.
5. Click **Edit** in the General section.
6. Select a new cluster version and click **Save**.

Related concepts

[Cluster version](#)

Related information

[Change Cluster Version \(CHGCLUVER\) command](#)

[Adjust Cluster Version \(QcstAdjustClusterVersion\) API](#)

Deleting a cluster

When you delete a cluster, cluster resource services ends on all active cluster nodes and they are removed from the cluster.

You must have at least one active node before you can delete a cluster. If you have switched disks or other switchable devices in your cluster, you must first remove each node from the device domain before you delete your cluster. Otherwise, you might not be able to add the disks back into another cluster.

To delete a cluster using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, select **Delete Cluster** from the Select Action menu next to the cluster name.
5. Click **Yes** on the confirmation panel.

Related tasks

[Removing a node from a device domain](#)

A *device domain* is a subset of nodes in a cluster that share device resources.

Related information

[Delete Cluster \(DLTCLU\) command](#)

[Delete Cluster \(QcstDeleteCluster\) API](#)

Displaying cluster configuration

You can display a detailed report that provides information on the cluster configuration. The cluster configuration report provides detailed information about the cluster, node membership list, configuration and tuning parameters, and each cluster resource group in the cluster.

To display cluster configuration, complete the following steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **Cluster Resource Services** page, select the **Display Configuration Information** task. This displays the Cluster Configuration and Properties page. You can save this page as a file or print it.

To display cluster configuration from the command-line, use either of these commands:

- [Display Cluster Information \(DSPCLUINF\) command](#)
- [Work with Cluster \(WRKCLU\) command](#)

Saving and restoring cluster configuration

If you use clustering on your systems, it is still important that you create a backup and recovery strategy to protect your data.

If you are planning on using clustering as your backup strategy so that you have one system up and running while the other system is down when its being backed up, it is recommended that you have a minimum of three systems in the cluster. By having three systems in the cluster, you will always have one system to switch over to should a failure occur.

Saving and restoring cluster resource groups

You can save a cluster resource group whether the cluster is active or inactive. The following restrictions apply for restoring a cluster resource group:

- If the cluster is up and the cluster resource group is not known to that cluster, you cannot restore the cluster resource group.
- If the node is not configured for a cluster, you cannot restore a cluster resource group.

You can restore a cluster resource group if the cluster is active, the cluster resource group is not known to that cluster, the node is in the recovery domain of that cluster resource group, and the cluster name matches that in the cluster resource group. You can restore a cluster resource group if the cluster is configured but is not active on that node and if that node is in the recovery domain of that cluster resource group.

Preparing for a disaster

In the event of a disaster, you might need to reconfigure your cluster. In order to prepare for such a scenario, it is recommended that you save your cluster configuration information and keep a hardcopy printout of that information.

1. Use the **Save Configuration (SAVCFG)** command or the **Save System (SAVSYS)** command after making cluster configuration changes so that the restored internal cluster information is current and consistent with other nodes in the cluster. See Saving configuration information for details on performing a SAVCFG or SAVSYS operation.
2. Print a copy of the cluster configuration information every time you change it. You can use the **Display Cluster Information (DSPCLUINF)** command to print the cluster configuration. Keep a copy with your backup tapes. In the event of a disaster, you might need to reconfigure your entire cluster.

Related information

[Saving configuration information](#)

[Save Configuration \(SAVCFG\) command](#)

[Save System \(SAVSYS\) command](#)

[Display Cluster Information \(DSPCLUINF\) command](#)

Monitoring cluster status

The PowerHA graphical interface presents the overall status of the cluster via status icons.

To obtain consistent information, you can either access the cluster information from an active node in the cluster, or start this node and retry the request.

To monitor cluster status using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.

3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, status icons show the overall status of the cluster.

To see the overall status of the cluster from the command-line, use either of these commands:

- [Display Cluster Information \(DSPCLUINF\) command](#)
- [Display Cluster Resource Group Information \(DSPCRGINF\) command](#)
- [Work with Cluster \(WRKCLU\) command](#)

Related tasks

Starting nodes

Starting a cluster node activates clustering and cluster resource services on a node in an IBM i high availability environment.

Related information

[List Cluster Information \(QcstListClusterInfo\) API](#)

[List Device Domain Info \(QcstListDeviceDomainInfo\) API](#)

[Retrieve Cluster Resource Services Information \(QcstRetrieveCRSInfo\) API](#)

[Retrieve Cluster Information \(QcstRetrieveClusterInfo\) API](#)

[List Cluster Resource Groups \(QcstListClusterResourceGroups\) API](#)

[List Cluster Resource Group Information \(QcstListClusterResourceGroupInf\) API](#)

Specifying message queues

You can either specify a cluster message queue or a failover message queue. These message queues help you determine causes of failures in your PowerHA environment.

A cluster message queue is used for cluster-level messages and provides one message, which controls all cluster resource groups (CRGs) failing over to a specific node. A failover message queue is used for CRG-level messages and provides one message for each CRG that is failing over.

Specifying a cluster message queue

Note: You can also configure a cluster to use a cluster message queue by specifying the message queue while running the Create Cluster wizard.

To specify a cluster message queue using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, select **Properties ...** from the **Select Action** menu.
5. Click **Edit** in the Advanced section of the **Properties** page.
6. Specify the cluster message queue information in the **Cluster Message Queue** field and click **Save**.

Specifying a failover message queue

To specify a failover message queue using the PowerHA graphical interface, complete these steps:

1. In a web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the IBM Navigator for i window.
4. On the **PowerHA** page, click **Cluster Resource Groups**.
5. On the **Cluster Resource Group** page, select **Properties ...** from the context menu of the CRG for which you want a failover message queue.
6. Click **Edit** in the Advanced section of the **Properties** page.
7. Specify the failover message queue information in the **Failover Message Queue** field and click **Save**.

Cluster deconfiguration checklist

To ensure complete deconfiguration of a cluster, you must systematically remove different cluster components.

<i>Table 9. Independent disk pool deconfiguration checklist for clusters</i>	
Independent disk pool requirements	
---	If you are using switched disk pools, the tower should be switched to the node which is the SPCN owner before deconfiguring the cluster resource group. You can use Initiate Switchover (QcstInitiateSwitchOver) API or the Change Cluster Resource Group Primary (CHGCRGPRI) command to move the CRG back to the SPCN owner. If this step is not performed, you will not be able to mark the tower private for that system.
---	If you plan to remove a subset of an independent disk pool group or remove the last independent disk pool in the switchable devices, you must end the CRG first. Use the End Cluster Resource Group (ENDCRG) command.
---	If you want delete an independent disk pool that is participating in a cluster, it is strongly recommended that you first delete the device cluster resource group (CRG). See “Deleting a CRG” on page 109 for details. You can also use the Remove CRG Device Entry (RMVCRGDEVE) command to remove the configuration object of the independent disk pool from the CRG.
---	After you have removed the configuration object of the independent disk pool from the cluster switchable device, you can delete an independent disk pool .
---	Delete the device description for an independent disk pool by completing these tasks: 1. On a command-line interface, type WRKDEVD DEVD(*ASP) and press Enter. 2. Page down until you see the device description for the independent disk pool that you want to delete. 3. Select Option 4 (Delete) by the name of the device description and press Enter.

<i>Table 10. Cluster resource group deconfiguration checklist for clusters</i>	
Cluster resource group requirement	
---	Delete cluster resource group by completing the either of the following steps: 1. If clustering is not active on the node, then type DLTCRG CRG(CRGNAME) on a command-line interface. CRGNAME is the name of the CRG that you want to delete. Press Enter. 2. If clustering is active on the node, then type DLTCRGCLU CLUSTER(CLUSTERNAME) CRG(CRGNAME) on a command-line interface. CLUSTERNAME is the name of the cluster. CRGNAME is the name of the CRG that you want to delete. Press Enter.

Managing nodes

System and logical partitions that are a part of an IBM i high availability environment are called nodes. You can perform several managing tasks that pertain to nodes.

Displaying node properties

You can display and manage properties that are associated with nodes that are configured as part of your high-availability environment by using the PowerHA graphical interface.

To display node properties using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Nodes**.

5. On the **Cluster Nodes** page, select **Properties ...** from the context menu of a node view with its properties.
 - The General page displays the name of the node and the system IP address for that node.
 - The Clustering page displays the following information:
 - The cluster interface IP addresses that are used by clustering to communicate with other nodes in the cluster.
 - The potential version of the node specifies the version and modification level at which the nodes in the cluster are actively communicating with each other.
 - The device domains that are configured in the selected cluster. If you select a device domain in the list, the nodes that belong to the selected device domain are also displayed.

Related information

[Work with cluster \(WRKCLU\) comand](#)

Stopping nodes

Stopping or ending a node ends clustering and cluster resource services on that node.

To stop clustering on a node using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click **Cluster Nodes**.
5. On the **Cluster Nodes** page, select **Stop** from the context menu of the nodes you want to stop.
6. Click **Yes** on the confirmation panel.

Related information

[End Cluster Node \(ENDCLUNOD\) command](#)

[End Cluster Node \(QcstEndClusterNode\) API](#)

Removing nodes

You might need to remove a node from a cluster if you are performing an upgrade of that node or if the node no longer needs to participate in the IBM i high-availability environment.

To remove a node from an existing cluster using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Nodes**.
5. On the **Cluster Nodes** page, select **Remove** from the context menu of the node you want to remove.
6. Click **Yes** on the confirmation window.

Related tasks

[Deconfiguring geographic mirroring](#)

If you no longer want the capability to use geographic mirroring for a specific disk pool or disk pool group, you can select to **Deconfigure Geographic Mirroring**. If you deconfigure geographic mirroring, the system stops geographic mirroring and deletes the mirror copy of the disk pools on the nodes in the mirror copy site.

Related information

[Remove Cluster Node Entry \(RMVCLUNODE\) command](#)

[Remove Cluster Node Entry \(QcstRemoveClusterNodeEntry\) API](#)

Removing a node from a device domain

A *device domain* is a subset of nodes in a cluster that share device resources.

Important:

Be cautious when removing a node from a device domain. If you remove a node from a device domain, and that node is the current primary point of access for any independent disk pools, those independent disk pools remain with the node being removed. This means that those independent disk pools are no longer accessible from the remaining nodes in the device domain.

After a node is removed from a device domain, it cannot be added back to the same device domain if one or more of the existing cluster nodes still belong to that same device domain. To add the node back to the device domain, you must:

1. Delete the independent disk pools currently owned by the node being added to the device domain.
2. Restart the system by performing an IPL on the node.
3. Add the node to the device domain.
4. Re-create the independent disk pools that were deleted in step 1.

To remove a node from a device domain using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Nodes**.
5. On the **Cluster Nodes** page, select **Properties ...** from the context menu of the node you want to add to a device domain.
6. Click **Edit** in the General section of the **Properties** page.
7. Clear the **Device Domain** field and click **Save**.

Related tasks

Deleting a cluster

When you delete a cluster, cluster resource services ends on all active cluster nodes and they are removed from the cluster.

Related information

Remove Device Domain Entry (RMVDEVDMNE) command

Remove Device Domain Entry (QcstRemoveDeviceDomainEntry) API

Add a cluster monitor to a node

The PowerHA graphical interface can now use Hardware Management Console (HMC) or a Virtual I/O Server (VIOS) partition on an Integrated Virtualization Manager (IVM) managed server to detect when a cluster node fails. This new capability allows more failure scenarios to be positively identified and avoids cluster partition situations.

The PowerHA graphical interface allows you to use the HMC or VIOS on an IVM managed server to monitor and manage the state of each system. Once a monitor is set up, HMC or IVM provide notification of node failures. A cluster monitor can be used to reduce the number of failure scenarios which result in cluster partitions.

PowerHA GUI only supports the Common Informational Model (CIM) server for the cluster monitor. The Add Cluster Monitor command must be used if you want to use the representational state transfer (REST) server.

To add a cluster monitor to an existing cluster using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.

4. On the **PowerHA** page, click on **Cluster Nodes** .
5. On the **Cluster Nodes** page, select **Properties ...** from the context menu of the node to which you want to add a cluster monitor.
6. In the Cluster Monitors section of the **Properties** page, select **Add Cluster Monitor ...** from the **Select Action** menu.
7. Specify the cluster monitor information and click **OK**.

Related information

[Add Cluster Monitor \(ADDCLUMON\) command](#)

Removing a cluster monitor

A *cluster monitor* provides another source of information to allow cluster resource services to determine when a cluster node has failed.

Important:

Be cautious when removing a cluster monitor. If you remove a node from a cluster monitor, and that node is the current primary point of access for any CRG, that node could partition when in fact, the node really failed. This means the user must now do manual steps to become highly available again.

PowerHA GUI only supports the Common Informational Model (CIM) server for the cluster monitor. The Remove Cluster Monitor command must be used if you want to use the representational state transfer (REST) server.

To remove a cluster monitor using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Nodes** .
5. On the **Cluster Nodes** page, select **Properties ...** from the context menu of the node to which you want to remove a cluster monitor.
6. In the **Cluster Monitors** section of the **Properties** page, select **Remove ...** from the context menu of the cluster monitors you want to remove.
7. Click **Yes** on the confirmation panel.

Related information

[Remove Cluster Monitor \(RMVCLUMON\) command](#)

Managing cluster resource groups (CRGs)

Cluster resource groups (CRGs) manage resilient resources within an IBM i high availability environment. They are a cluster technology that defines and controls switching resources to backup systems in the event of an outage.

Displaying CRG status

You can monitor the status of cluster resource groups (CRG) in your high-availability environment. You can use these status messages to validate changes in the CRG or to determine problems with the CRG.

To display the CRG status using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Resource Groups**.

The following are possible status values for a CRG:

Table 11. Status values for CRGs

Possible values	Description
Started	The CRG is currently started.
Stopped	The CRG is currently stopped.
Indoubt	The information about this CRG within the high availability solution might not be accurate. This status occurs when the CRG exit program is called with an action of undo and fails to complete successfully.
Restored	The CRG was restored on its node and has not been copied to other nodes in the cluster. When clustering is started on the node, the CRG will be synchronized with the other nodes and its status is set to inactive.
Inactive	Cluster resource services for the CRG is not active on the node. The node might have failed, the node might have been ended, or the CRG job on that node might not be running.
Deleting	The CRG is in the process of being deleted from the cluster.
Changing	The CRG is in the process of being changed. The CRG is reset to its previous status when the change has been successfully completed.
Stopping	The CRG is in the process of being stopped.
Adding	The CRG is in the process of being added to the cluster.
Starting	The CRG is in the process of being started.
Switching	The CRG is in the process of switching over to another node.
Adding node	A new node is in the process of being added to the cluster. The CRG is reset to its previous status when the node has been successfully added.
Removing node	A node is in the process of being removed from the CRG. The CRG is reset to its previous status when the node has been successfully removed.
Changing node status	The status of a node in the recovery domain for a CRG is currently being changed.

Related information

[Display CRG Information \(DSPCRGINF\) command](#)

[Work with Cluster \(WRKCLU\) command, option 9 \(Work with cluster resource groups\)](#)

Stopping a CRG

Cluster resource groups (CRGs) manage resilient resources within an IBM i high availability environment. They are a cluster technology that defines and controls switching resilient resources to backup systems in the event of an outage.

You might want to stop the CRG to end automatic failover capability in your high-availability environment. For example, you might be performing an IPL on one of the systems that is defined in the CRG.

To stop a CRG using PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Resource Groups**.
5. On the **Cluster Resource Group** page, select **Stop** from the context menu of the CRG that you want to stop.
6. Click **Yes** on the confirmation panel.

Related information

[End Cluster Resource Group \(ENDCRG\) command](#)

[End Cluster Resource Group \(QcstEndClusterResourceGroup\) API](#)

Deleting a CRG

You can delete a cluster resource group by using the PowerHA graphical interface or PowerHA commands.

You can delete a cluster resource group by using the PowerHA graphical interface. In order to delete a CRG, it must be inactive.

To delete a CRG using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Resource Groups**.
5. On the **Cluster Resource Group** page, select **Delete** from the context menu of the CRG that you want to delete.
6. Click **Yes** on the confirmation panel.

Related information

[Delete CRG Cluster \(DLTCRGCLU\) command](#)

[Delete Cluster Resource Group \(DLTCRG\) command](#)

[Delete Cluster Resource Group \(QcstDeleteClusterResourceGroup\) API](#)

Changing the recovery domain for a CRG

The recovery domain controls recovery actions for a subset of nodes that are defined in a cluster resource group (CRG).

To use the PowerHA graphical interface to make an independent disk pool available, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Resource Groups**.
5. On the **Cluster Resource Group** page, select **Recovery Domain ...** from the context menu of the CRG of which you want to change the recovery domain.
6. Once on the **Recovery Domain** page, you can add and remove nodes, change node roles, change site names, and change data port IP addresses.

Related information

[Add Cluster Resource Group Node Entry \(ADDCRGNODE\) command](#)

[Change Cluster Resource Group \(CHGCRG\) command](#)

[Remove Cluster Resource Group Node Entry \(RMVCRGNODE\) command](#)

[Add a Node to Recovery Domain \(QcstAddNodeToRcvyDomain\) API](#)

[Change Cluster Resource Group \(QcstChangeClusterResourceGroup\) API](#)

[Remove Node from Recovery Domain \(QcstRemoveNodeFromRcvyDomain\) API](#)

Creating site names and data port IP addresses

If you are using geographic mirroring, the nodes defined in the recovery domain node of the device cluster resource group must have a data port IP address and site name.

The site name is associated with a node in the recovery domain for a device cluster resource group, applicable only to geographic mirroring. When you are configuring a geographic mirroring environment for high availability, each node at different sites must be assigned to a different site name.

To create the data port IP address and site names for nodes in the recovery domain, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the Cluster Resource Services page, click the **Work with Cluster Resource Groups** task to show a list of cluster resource groups in the cluster.
5. On the Cluster Resource Group tab, click the context icon next to the device cluster resource group, and then select **Properties**.
6. On the Recovery Domain page, select **Edit**.
7. To use an existing data port IP address, select it from the list and click **OK**. To add a new data port IP address, click **Add**. In the Add Data Port IP Address window, enter the IP address.
8. In the Edit window, you can specify the Site name.

Managing a cluster resource group (CRG) container

The cluster resource group (CRG) container manages multiple CRGs within an IBM i High Availability (HA) environment

CRG containers manage CRGs that control resilient resources. They are a cluster technology that defines and controls switching groups of resources to backup sites and systems in the event of a planned or unplanned outage.

CRG containers rely on much of the underlying technology that CRGs use and thus utilize many of the same commands that the CRGs use. Many functions of the CRG container can be managed from the Work with Cluster Resource Groups screen used to create and manage CRGs. Some commands, however, are different for containers even though they may perform a task like a CRG command. CRG containers use a CNR suffix to distinguish the command is used on a CRG container. For example, the Start CRG (**STRCRG**) command for a CRG container is **STRCRGCNR**, Start CRG container. Table below lists related commands between CRGs and CRG containers.

CRG command	CRG container command
Create CRG (CRTCRG)	Create CRG container (CRTCRGCNR)
Delete CRG (DLTCRG)	Delete CRG container (DLTCRGCNR)
Start CRG (STRCRG)	Start CRG container (STRCRGCNR)
End CRG (ENDCRG)	End CRG container (ENDCRGCNR)
Display CRG information (DSPCRGINF)	Display CRG container (DSPCRGCNR)

CRG command	CRG container command
Change CRG primary (CHGCRGPRI)	Configure CRG container (CFGCRGCNR)
	Change CRG Container (CHGCRGCNR)

With the CRG container commands and CRG commands, users can change, start, end, and display a containers properties and perform switches overs to backup systems.

Starting a cluster resource group (CRG) container

Steps and considerations for starting a cluster resource group container

Refer to the topics “Configuring a Cluster Resource Group container” on page 66 and “Create a cluster resource group (CRG) container” on page 67 for the information about the setup of the cluster,CRGs and CRG container used in the example steps. Here, across two sites, the cluster has a CRG container, **HACNR**, that contains the device and data CRGs.

Like cluster resource groups (CRGs), CRG containers begin in the Inactive status. For a CRG container to perform its management tasks, the Start CRG container (**STRCRGCNR**) command must be issued. Running this command changes the container status from Inactive or Indoubt to Active.

To run the Start CRG container (**STRCRGCNR**) command and start a CRG container successfully, the cluster and container must meet these requirements:

- The cluster node must have a status of Active within the cluster.
- The CRG container must have at least one managed CRG in it.
- The CRG container status cannot be Active.

For example, the CRG container **HACNR** currently has the Inactive status, ready to start and make Active.

To start the CRG container **HACNR** do the following:

1. At the command line type in **STRCRGCNR** and press F4.
2. On the Start CRG Container (**STRCRGCNR**) command screen, type in the name of the CRG container to start in the Container field.
Here, HACNR is typed into the field.
3. Press Enter to start the CRG container.

The CRG container starts and the system displays the message: The **STRCRGCNR** command completed successfully.

The resources in the managed CRGs are now resilient.

An example of starting a CRG container from the command line using the configuration described at the beginning of this page looks like:

```
STRCRGCNR CNR(HACNR)
```

The command starts the CRG container **HACNR** and its managed CRGs.

Another method of starting the CRG container is through the **Work with Cluster (WRKCLU) command screen > 9. Work with Cluster Resource Groups > option 8 = Start**, to open the Start CRG Container screen. Follow the steps above from this point to start the CRG container.

To verify that the CRG container has started and has a status of Active, run the Display CRG Information (**DSPCRGINF**) command to display a list of all CRGs and CRG containers in the cluster, including the current status.

Ending a cluster resource group (CRG) container

Steps and considerations for stopping a cluster resource group container

Refer tp the topics “Configuring a Cluster Resource Group container” on page 66 and “Create a cluster resource group (CRG) container” on page 67 for the information about the setup of the cluster,CRGs and

CRG container used in the example steps. Here, across two sites, the cluster has a CRG container, **HACNR**, that contains the device and data CRGs.

Like cluster resource groups (CRGs), CRG containers with Active status can be ended. Running the End CRG Container (**ENDCRGCNR**) command sets the CRG container status to Inactive. In this state, the CRG container cannot provide any switchover or failover security. In addition, the **ENDCRGCNR** command disables resiliency for all managed CRGs in the container.

To run the End CRG container (**ENDCRGCNR**) command and end a CRG container successfully, the cluster and container must meet these requirements:

- the cluster node must have a status of Active within the cluster.
- the **ENDCRGCNR** command cannot be called from an exit program..
- the CRG container status cannot be Inactive.

For example, the CRG container **HACNR** is currently has the Active and managing the CRGs it contains. It is ready to end, if required.

To end the CRG container do the following:

1. At the command line type in **ENDCRGCNR** and press Enter.
2. On the End CRG Container (**ENDCRGCNR**) command screen, type in the name of the CRG container to end in the Container field.

Here, HACNR is typed into the field.

3. Press Enter to end the CRG container.

The CRG container ends and the message, The **ENDCRGCNR** command completed successfully. The status of the CRG container and its managed CRGs is Inactive. Resources in the managed CRGs are no longer resilient.

An example of ending a CRG container from the command line using the configuration described at the beginning of this page looks like:

```
ENDCRGCNR CNR(HACNR)
```

The command ends the CRG container HACNR and its managed CRGs.

Another method of ending the CRG container is through the **Work with Cluster (WRKCLU) command screen > 9. Work with Cluster Resource Groups > option 9 = End**, to open the End CRG Container screen. Follow the steps above from this point to end the CRG container.

To verify that the CRG container has been changed to Inactive status, use the Display CRG Information (**DSPCRGINF**) command to view the status.

Deleting a cluster resource group (CRG) container

Using the Delete Cluster Resource Group Container (**DLTCRGCNR**) command

Refer to the topics “[Configuring a Cluster Resource Group container](#)” on page 66 and “[Create a cluster resource group \(CRG\) container](#)” on page 67 for the information about the setup of the cluster, CRGs and CRG container used in the example steps. Here, across two sites, the cluster has a CRG container, **HACNR**, that contains the device and data CRGs.

CRG containers can be deleted from all active cluster nodes in its recovery domain with the Delete Cluster Resource Group Container (**DLTCRGCNR**) command. Running the Delete Cluster Resource Group Container (**DLTCRGCNR**) command deletes the CRG container object from each active cluster node. If there are inactive cluster nodes, the CRG container object will be deleted when the node or nodes become active again.

To run the Delete Cluster Resource Group Container (**DLTCRGCNR**) command and delete a CRG container successfully, the cluster and container must meet these requirements:

- the cluster node running the command must have a status of Active within the cluster.
- the CRG container status cannot be Active.

- managed CRGs must be removed from the container before running **DLTCRGCNR**. This can be done using the Configure CRG Container (**CFGCRGCNR**) command.

The CRG container **HACNR** is currently has the status of Active and is managing the CRGs it contains. In this example, the user wants to make changes to the HA environment and will delete the container.

Before deleting the CRG container the status must be changed to Inactive and the managed CRGs removed.

1. End the CRG container with the End CRG Container (**ENDCRGCNR**) command or use option 9 on the Work with Cluster Resource Groups screen.

See [Ending a cluster resource group container](#) for instructions and considerations.

2. Using the ***RMVCRG** action in the Configure CRG Container (**CFGCRGCNR**) command to remove the managed CRGs from the CRG container.

This task can be done by removing the CRG from the CRG container with option 4, Remove on the Work with Configuration Objects screen too. For more information about removing CRGs from a CRG container, see the topic, [“Removing nodes and configuration objects using the Configure CRG Container command”](#) on page 115.

After removing all the managed CRGs from the Inactive CRG container, the CRG container is ready to be deleted.

3. On the Delete CRG Container (**DLTCRGCNR**) command screen, type in the name of the CRG container to delete in the Container field.

Here, HACNR is typed into the field.

4. Press Enter to delete the CRG container.

The CRG container is deleted from all active cluster nodes and the system displays the message, Command **DLTCRGCNR** completed successfully.

An example of deleting a CRG container from the command line using the example configuration described looks like:

```
DLTCRGCNR CNR(HACNR)
```

This will delete the CRG container **HACNR** from the cluster **HA_CLSTR**.

Another method of deleting the CRG container is through the **Work with Cluster (WRKCLU) command screen > 9. Work with Cluster Resource Groups > option 4 = Delete**, to open the Delete CRG Container screen.

To verify that the CRG container has been deleted, use the Display CRG Information (**DSPCRGINF**) command to view the status.

Displaying a cluster resource group (CRG) container

Display or print information about CRG containers

To check or verify the information about a CRG container, users can run the Display CRG Container (**DSPCRGCNR**) command.

To run the Display Cluster Resource Group Container (**DSPCRGCNR**) command successfully, it must be invoked from a node in the cluster.

To display the CRG container information do the following:

1. At the command line type in **DSPCRGCNR** and press F4.
2. On the Display CRG Container (**DSPCRGCNR**) command screen, type in the name of the CRG container in the Container field.

Here, HACNR is typed into the field.

3. Press Enter to display the CRG container information.

Pressing Enter again displays the Configuration Object Information section. Here, information about the managed CRGs is displayed. Pressing Enter a third time, the Recovery Domain Information including nodes, node status and current role can be found.

An example of ending a CRG container from the command line using the configuration described at the beginning of this page looks like this:

```
DSPCRGCNR CNR (HACNR)
```

Another method of finding the CRG container information is through the **Work with Cluster (WRKCLU) command screen > 9. Work with Cluster Resource Groups** and using the various options to view the information about the recovery domain, option 6, configuration option information, option 7, and status, option 5.

Adding nodes and configuration objects using the Configure CRG Container command

Adding objects and cluster nodes with the Configure CRG Container (**CFGCRGCNR**) command

Refer to the topics “Configuring a Cluster Resource Group container” on page 66 and “Create a cluster resource group (CRG) container” on page 67 for the information about the setup of the cluster, CRGs and CRG container used in the example steps. Here, across two sites, the cluster has a CRG container, **HACNR**, that contains the device and data CRGs.

Configure CRG Container (**CFGCRGCNR**) command allows users to make changes to the cluster resource group (CRG) container by either adding or removing cluster nodes or by adding or removing CRGs to the CRG container.

To run the Configure CRG Container (**CFGCRGCNR**) command and make changes to the nodes or CRGs of the container, the cluster and container must meet these requirements:

- the cluster node running the command must have a status of Active within the cluster.
- At least one node in the current recovery domain for the CRG container must have the status of Active.

Depending on the specific action, additional requirements or conditions will apply.

These examples demonstrate the addition functions of the Configure CRG Container (**CFGCRGCNR**) command. The cluster **HA_CLSTR** is operating with one node on each of the two sites **NODE01** at **SITE01** and **NODE03** at **SITE02**. The CRG container, **HACNR** currently is operating with one device CRG and one data CRG. The configuration must be changed to include a second data CRG named **DATA CRG02**, and another node, **NODE02** will be added to **SITE01**.

Adding a cluster node to the recovery domain of a CRG container

Before adding **DATA CRG02** to **HACNR**, another node, **NODE02** must be added to recovery domain of the CRG container because it is part of the recovery domain of **DATA CRG02**. To add a node to the recovery domain of the CRG container make sure in addition to other restrictions that:

- A member of the cluster containing the other nodes, CRG, and CRG container.
- The node is not already a member of the recovery domain of the CRG Container.
- If the node being added is a primary node, then the CRG container status must be changed to Inactive.

Add the new node, **NODE02** to **HACNR**.

1. At the command line type in **CFGCRGCNR** and press enter.
2. On the Configure CRG Container (**CFGCRGCNR**) command screen, type in the name of the CRG container to start in the Container field.
Here, **HACNR** is typed into the field.
3. Type the specific action in the Action field and press Enter.
In this case, the action is ***ADDNOD**.
If necessary, press **F4** to view all the parameter options.
4. The Configuration object list field appears. Enter the name of the node, **NODE02** to add to the CRG container. Press Enter.

NODE02 is added to the CRG container **HACNR**.

An example of adding a node to a CRG container from the command line using the configuration described:

```
CFGCRGCNR CNR(HACNR) ACTION(*ADDNOD) CFGOBJ(NODE02)
```

The command adds the node, **NODE02** to CRG container **HACNR**.

Another method of adding a cluster node to the CRG container is through the **Work with Cluster (WRKCLU) command screen > 9. Work with Cluster Resource Groups > option 6 = Recovery domain** for the CRG container, to open the Work with Recovery Domain screen, select **option 1 = Add node**.

Adding a CRG to a CRG container

To add **DATACRG02** to the CRG container **HACNR**, the CRG must be:

- Configured for use in the cluster.
- Must not be a managed CRG inside another CRG container.
- All cluster nodes assigned to the CRG recovery domain must be included in the recovery domain of the CRG container.

When ready, add **DATACRG02** to **HACNR**.

1. At the command line type in **CFGCRGCNR** and press enter.
2. On the Configure CRG Container (**CFGCRGCNR**) command screen, type in the name of the CRG container to start in the Container field.
Here, **HACNR** is typed into the field.
3. Type the specific action in the Action field and press Enter.
In this case, the action is ***ADDCRG**.
If necessary, press F4 to view all the parameter options.
4. The Configuration object list field appears. Enter the name of the CRG, **DATACRG02** to add to the CRG container. Press Enter.

DATACRG02 is added to the CRG container **HACNR**.

An example of adding a CRG to a CRG container from the command line using the configuration described:

```
CFGCRGCNR CNR(HACNR) ACTION(*ADDCRG) CFGOBJ(DATACRG02)
```

The command adds the CRG **DATACRG02** to CRG container **HACNR**.

Another method of adding a CRG to the CRG container is through the **Work with Cluster (WRKCLU) command screen > 9. Work with Cluster Resource Groups > option 7 = Configuration objects** for the CRG container, to open the Work with Configured objects screen, here, select option **1 = Add**.

Removing nodes and configuration objects using the Configure CRG Container command

Remove objects and cluster nodes with the Configure CRG Container (**CFGCRGCNR**) command

Refer to the topics [“Configuring a Cluster Resource Group container” on page 66](#) and [“Create a cluster resource group \(CRG\) container” on page 67](#) for the information about the setup of the cluster, CRGs and CRG container used in the example steps. Here, across two sites, the cluster has a CRG container, **HACNR**, that contains the device and data CRGs.

To run the Configure CRG Container (**CFGCRGCNR**) command and make changes to the nodes or CRGs of the cluster resource group (CRG) container, the cluster and container must meet these requirements:

- The cluster node running the command must have a status of Active within the cluster.
- At least one node in the current recovery domain for the CRG container must have the status of Active.

Depending on the specific action, additional requirements of conditions will apply.

These examples demonstrate the removal functions of the Configure CRG Container (**CFGCRGCNR**) command. The cluster **HA_CLSTR** is operating with two nodes at **SITE01, NODE01** and **NODE02**. **SITE02** has a single node, **NODE03**, The CRG container, **HACNR** is currently operating with one device CRG and

two data CRGs. The configuration must be changed and **DATA CRG02** must be removed and **NODE02** removed from the recovery domain of **HACNR**.

Removing a CRG from a CRG container

Before removing **DATA CRG02** from **HACNR**, make sure in addition to other restrictions that:

- the CRG container must be ended first to a status of Inactive if removing the last CRG.
- the CRG itself cannot have the status of Active.

To remove **DATA CRG02** from **HACNR**.

1. At the command line type in **CFGCRG CNR** and press enter.
2. On the Configure CRG Container (**CFGCRG CNR**) command screen, type in the name of the CRG container to start in the Container field.
Here, **HACNR** is typed into the field.
3. Type the specific action in the Action field and press Enter.
In this case, the action is ***RMVCRG**.
If necessary, press F4 to view all the parameter options.
4. The Configuration object list field appears. Enter the name of the CRG, **DATA CRG02** to remove from the container. Press Enter.

DATA CRG02 is removed from the CRG container **HACNR**.

An example of removing a node to a CRG container from the command line using the configuration described:

```
CFGCRG CNR (HACNR) ACTION(*RMVCRG) CFGOBJ (DATA CRG02)
```

The command removes the CRG, **DATA CRG02** from CRG container **HACNR**.

Another method of removing a CRG from the CRG container is through the **Work with Cluster (WRKCLU) command screen > 9. Work with Cluster Resource Groups > option 7 = Configuration objects** for the CRG container, to open the Work with Configured objects screen, here, select option **4 = Remove**.

Removing a cluster node from the recovery domain of a CRG container

Before removing **NODE02** from **HACNR**, the CRG **DATA CRG02** was removed. Now **NODE02** can be removed from the recovery domain of the CRG container because no longer required. To remove a node from the recovery domain of the CRG container make sure in addition to other restrictions that:

- If a CRG container has no backup nodes, the primary node cannot be removed.
- The status of the CRG container cannot be Active.

Remove **NODE02** from **HACNR**.

1. At the command line type in **CFGCRG CNR** and press enter.
2. On the Configure CRG Container (**CFGCRG CNR**) command screen, type in the name of the CRG container to start in the Container field.
Here, **HACNR** is typed into the field.
3. Type the specific action in the Action field and press Enter.
In this case, the action is ***RMVNOD**.
If necessary, press F4 to view all the parameter options.
4. The Configuration object list field appears. Enter the name of the node, **NODE02** to remove from the CRG container. Press Enter.

NODE02 is removed from the CRG container **HACNR**.

An example of removing a node from a CRG container from the command line using the configuration described:

The command removes the node, **NODE02** from CRG container **HACNR**.

Another method of removing a cluster node from the CRG container is through the **Work with Cluster (WRKCLU) command screen > 9. Work with Cluster Resource Groups > option 6 = Recovery domain** for the CRG container, to open the Work with Recovery Domain screen, select option **4 = Remove node**.

Changing the primary node of a cluster resource group (CRG) container using the Change CRG Container (CHGCRGCNR) command

Using the Change CRG Container (**CHGCRGCNR**) command to adjust the recovery domain of a CRG container

By running the Change Cluster Resource Group (CRG) Container (**CHGCRGCNR**) command, a user can manage the recovery domain of a CRG. How this is done depends on the status of the CRG container: The node running the Change CRG Container (**CHGCRGCNR**) command must be an active node in the cluster.

When running the Change CRG Container (**CHGCRGCNR**) command, it is the Recovery domain action parameter field that determines how the container will change the recovery domain. There are three recovery domain action parameters. Each modifies the recovery domain node list of the **RCYDMN** parameter. The three change actions are:

***CHGPRI**

When the CRG container is in Active status, the Recovery domain action (**RCYDMNACN**) ***CHGPRI** initiates an administrative switchover of all the CRGs managed by the CRG container to a new primary node.

***CHGCUR**

If a container has the status of Inactive or Indoubt, the Recovery domain action (**RCYDMNACN**) ***CHGCUR** to change the current primary node to the next specified node in the Recovery domain. The Recovery domain node list (**RCYDMN**) contains the changes to the node roles and will initiate the changes when the container becomes Active.

***CHGPREFER**

This parameter changes the preferred roles of the nodes of the recovery domain. The Recovery domain node list (**RCYDMN**) contains the changes to the node roles and will initiate the changes when the container becomes Active.

While the Recover domain action parameter instructs the CRG container to reorder the recovery domain, the parameter Switch type (**SWTTYP**) determines how the new primary node is selected. Used in sequence with the Recovery domain action parameter ***CHGPRI**, the two switch types indicate whether the CRG container moves the primary to a node on the same site or across to the mirror site.

***SAMESITE**

The ***SAMESITE** parameter specifies that the new primary node for the CRG container remains within the same site.

***CRSSITE**

The ***CRSSITE** switch type indicates that the new primary node for the CRG container moves to other site of the recovery domain.

This parameter can be used only with the Recovery domain action (**RCYDMNACN**) of ***CHGPRI**.

Changing the current recovery domain of a cluster resource group (CRG) container

See how to change the current recovery domain node roles with the Change CRG Container (**CHGCRGCNR**) command

The the topics “Configuring a Cluster Resource Group container” on page 66 and “Create a cluster resource group (CRG) container” on page 67 contains the basic information about the setup of the cluster, CRGs and CRG container used in the example steps. Here, using the Change CRG container (**CHGCRGCNR**) command the cluster is modified to contain four cluster nodes across two sites. The device and the two data CRGs are active in the cluster.

This table displays the relevant information about the current recovery domain for CRG container HACNR:

Node name	Current node role
NODE01	Primary node
NODE02	Backup 1
NODE03	Backup 2
NODE04	Backup 3 (*LAST)

The steps in the example begin with the CRG container HACNR in this configuration.

Users can change the current recovery domain of the CRG container with the Change Cluster Resource Group (CRG) Container (**CHGCRGCNR**) command.

When using the command to change the order in the recovery domain of a CRG container, the CRG container must not be in the Active state. The options of Recovery domain action (**RCYDMNACN**) parameters, therefore are ***CHGCUR** or ***CHGPREFER**. Both actions require the CRG container to be stopped before the changes are made to the Recovery domain node list (**RCYDMN**). Refer to the [“Changing the primary node of a cluster resource group \(CRG\) container using the Change CRG Container \(CHGCRGCNR\) command” on page 117](#) for information about the types of actions.

This set of example steps begins after the CRG container has been stopped with either the End CRG Container (**ENDCRGCNR**) command or option 9, End on the Work with Cluster Resource Groups menu display. In these steps, the recovery domain for CRG container **HACNR** must be changed to reflect that the primary node will be changed to **NODE02**.

After the CRG container is Inactive, use the Change Cluster Resource Group (CRG) Container (**CHGCRGCNR**) command to begin the Recovery domain action (**RCYDMNACN**). changes to the recovery domain node list can be made

1. At the command line type in **CHGCRGCNR** and press F4.

The Change CRG Container (**CHGCRGCNR**) command display opens.

2. Type in the name of the container. In this case, **HACNR**.

3. In the Recovery domain action field, select either ***CHGCUR** or ***CHGPREFER** and press Enter.

The recovery domain node list displays the current recovery domain of the container for a recovery domain action of ***CHGCUR**, or the preferred recovery domain for a recovery domain action of ***CHGPREFER**.

4. With the Recovery domain node list displayed, change the Node role field for the **NODE01** entry, replace ***PRIMARY** with ***BACKUP**.

5. In the **NODE02** entry, change ***BACKUP** to ***PRIMARY**. Change **1** in the Backup sequence number to ***LAST**.

6. Press Enter to make the changes.

The system displays the screen with the command and message, **COMMAND CHGCRGCNR completed successfully**.

After successful completion of the command, the recovery domain for the container will be:

Node name	New current node role
NODE02	Primary node
NODE03	Backup 1
NODE04	Backup 2
NODE01	Backup 3 (*LAST)

NODE02 is now the primary node while **NODE01** has moved to the ***LAST** backup position.

An example of running this ***CHGCUR** or ***CHGPREFER** Recovery domain action from the command line looks like:

```
CHGCRGCNR CNR(HADOCCNR01) RCYDMNACN(*CHGCUR) RCYDMN((NODE01 *BACKUP *LAST) (NODE02 *PRIMARY *LAST) (NODE03 *BACKUP 1) (NODE04 *BACKUP 2))
```

These results are the same as the table above.

Review the changes to the recovery domain using the Display CRG Container (**DSPCRGCNR**) command or with option 6, Recovery domain on the Work with Cluster Resource Groups screen.

Managing failover outage events

Typically, a failover results from a node outage, but there are other reasons that can also generate a failover. Different system or user actions can potentially cause failover situations.

It is possible for a problem to affect only a single cluster resource group (CRG) that can cause a failover for that CRG but not for any other CRG.

Four categories of outages can occur within a cluster. Some of these events are true failover situations where the node is experiencing an outage, while others require investigation to determine the cause and the appropriate response. The following tables describe each of these categories of outages, the types of outage events that fall into that category and the appropriate recovery action you should take to recover.

Category 1 outages: Node outage causing failover

Node-level failover occurs, causing the following to happen:

- For each CRG, the primary node is marked *inactive* and made the last backup node.
- The node that was the first backup becomes the new primary node.

Failovers happen in this order:

1. All device CRGs
2. All data CRGs
3. All application CRGs

Notes:

1. If a failover for any CRG detects that none of the backup nodes are active, the status of the CRG is set to *indoubt* and the CRG recovery domain does not change.
2. If all of cluster resource services fails, then the resources (CRGs) that are managed by cluster resource services go through the failover process.

Failover outage event
ENDTCP(*IMMED or *CNTRLD with a time limit) is issued.
ENDSYS (*IMMED or *CNTRLD) is issued.
PWRDWNSYS(*IMMED or *CNTRLD) is issued.
Initial program load (IPL) button is pressed while cluster resource services is active on the system.
End Cluster Node (API or command) is called on the primary node in the CRG recovery domain.
Remove Cluster Node (API or command) is called on the primary node in the CRG recovery domain.
HMC delayed power down of the partition or panel option 7 is issued.
ENDSBS QSYSWRK(*IMMED or *CNTRLD) is issued.

Category 2 outages: Node outage causing partition or failover

These outages will cause either a partition or a failover depending on whether advanced node failure detection is configured. Refer to the columns in the table. If advanced node failure detection is configured, failover occurs in most cases and Category 1 outage information applies. If advanced node failure detection is not configured, partition occurs and the following applies:

- The status of the nodes not communicating by cluster messaging is set to a Partition status. See [Cluster partition](#) for information about partitions.
- All nodes in the cluster partition that do not have the primary node as a member of the partition will end the active cluster resource group.

Notes:

1. If a node really failed but is detected only as a partition problem and the failed node was the primary node, you lose all the data and application services on that node and no automatic failover is started.
2. You must either declare the node as failed or bring the node back up and start clustering on that node again. See [Change partitioned nodes to failed](#) for more information.

Failover outage event	No advanced node failure detection	HMC	VIOS on IVM
CEC hardware outage (CPU, for example) occurs.	partition	failover	partition or failover
Operating system software machine check occurs.	partition	failover	failover
HMC immediate power off or panel option 8 is issued.	partition	failover	failover
HMC partition restart or panel option 3 is issued.	partition	failover	failover
Power loss to the CEC occurs.	partition	partition	partition

Category 3 outages: CRG fault causing failover

For a system using a Virtual I/O Server (VIOS) partition on an Integrated Virtualization Manager (IVM) managed server, a CEC hardware failure could result in either failover or partition. Which occurs depends upon the type of system and the hardware failure. For example, in a blade system, a CEC failure that prevents VIOS on an IVM managed server from running results in a partition since VIOS is unable to report any failure. In the same system in which a single blade fails but VIOS on an IVM managed server continues to run, failover results since VIOS is able to report the failure.

When a CRG fault causes a failover, the following happens:

- If only a single CRG is affected, failover occurs on an individual CRG basis. This is because CRGs are independent of each other.
- If someone cancels several cluster resource jobs, so that several CRGs are affected at the same time, no coordinated failover between CRGs is performed.
- The primary node is marked as Inactive in each CRG and made the last backup node.
- The node that was the first backup node becomes the new primary node.
- If there is no active backup node, the status of the CRG is set to Indoubt and the recovery domain remains unchanged.

Table 14. Category 3 outages: CRG fault causing failover

Failover outage event
The CRG job has a software error that causes it to end abnormally.
Application exit program failure for an application CRG.

Category 4 outages: Communication outage causing partition

This category is similar to category 2. These events occur:

- The status of the nodes not communicating by cluster messaging are set to Partition status. See [Cluster partition](#) for information about partitions.
- All nodes and cluster resource services on the nodes are still operational, but not all nodes can communicate with each other.
- The cluster is partitioned, but each CRG's primary node is still providing services.

The normal recovery for this partition state should be to repair the communication problem that caused the cluster partition. The cluster will resolve the partition state without any additional intervention.

Note: If you want the CRGs to fail over to a new primary node, ensure that the old primary node is not using the resources before the node is marked as failed. See [Change partitioned nodes to failed](#) for more information.

Table 15. Category 4 outages: Communication outage causing partition

Failover outage event
Communications adapter, line, or router failure on cluster heartbeat IP address lines occurs.
ENDTCPIFC is affecting all cluster heartbeat IP addresses on a cluster node.

Outages with active CRGs

- If the CRG is Active and the failing node is *not* the primary node, the following results:
 - The failover updates the status of the failed recovery domain member in the CRG's recovery domain.
 - If the failing node is a backup node, the list of backup nodes is reordered so that active nodes are at the beginning of the list.
- If the CRG is Active and the recovery domain member is the primary node, the actions the system performs depend on which type of outage has occurred.
 - Category 1 outages: Node outage causing failover
 - Category 2 outages: Node outage causing partition
 - Category 3 outages: CRG fault causing failover
 - Category 4 outages: Communication outage causing partition

Outages with inactive CRGs

When there is an outage with CRGs, the following occur:

- The membership status of the failed node in the cluster resource group's recovery domain is changed to either Inactive or Partition status.
- The node roles are not changed, and the backup nodes are not reordered automatically.
- The backup nodes are reordered in an Inactive CRG when the **Start Cluster Resource Group (STRCRG)** command or the `Start Cluster Resource Group (QcstStartClusterResourceGroup)` API is called.

Note: The Start Cluster Resource Group API will fail if the primary node is not active. You must issue the **Change Cluster Resource Group (CHGCRG)** command or the `Change Cluster Resource Group (QcstChangeClusterResourceGroup)` API to designate an active node as the primary node, and then call the Start Cluster Resource Group API again.

Managing cluster administrative domains

After a cluster administrative domain is created and the appropriate monitored resource entries (MREs) are added, the cluster administrator should monitor the activity within the administrative domain to ensure that the monitored resources remain consistent. Using PowerHA graphical interface or the PowerHA command-line interfaces, you can manage and monitor a cluster administrative domain.

Related tasks

Displaying cluster administrative domains

You can manage and monitor the status of cluster administrative domains in your high-availability environment.

Stopping a cluster administrative domain

Cluster administrative domains provide environment resiliency for resources within an IBM i high-availability solution. You might need to stop a cluster administrative domain to temporarily end synchronization of monitored resources.

Deleting a cluster administrative domain

Using the PowerHA graphical interface, you can delete a cluster administrative domain. Deleting a cluster administrative domain ends synchronization of monitored resources that are defined in the cluster administrative domain. In order to delete a cluster administrative domain, it must be inactive.

Changing the properties of a cluster administrative domain

Using the PowerHA graphical interface, you can change properties to an existing cluster administrative domain. These properties control synchronizations of monitored resource entries that are defined in the cluster administrative domain.

Managing monitored resource entries

The PowerHA graphical interface allows you to manage monitored resource entries in your cluster administrative domain. A cluster administrative domain ensures that changes made to these monitored resources remain consistent on each node within the high-availability environment.

Displaying cluster administrative domains

You can manage and monitor the status of cluster administrative domains in your high-availability environment.

This graphical interface provides the ability to list the MREs along with the global status for each resource. Detailed information can be displayed by selecting an MRE. This information includes the global value for each attribute that is associated with the MRE, along with an indication whether the attribute is consistent or inconsistent with the domain. If the global status of a monitored resource is inconsistent, the administrator should take the necessary steps to determine why the resource is inconsistent, correct the problem, and resynchronize the resource.

If the resource is inconsistent because an update failed on one or more nodes, information is kept for the MRE that can help you determine the cause of the failure. On the node where the failure occurred, a message is logged with the MRE as to the cause of the failed update. On the other nodes, there is an informational message logged internally, which tells you there was a failure, along with the list of nodes where the update failed. These messages are available through the PowerHA graphical interface or by calling the Retrieve Monitored Resource Information (`QfpadRtvMonitoredResourceInfo`) API. Failure messages are also logged in the job log of the administrative domain job.

After the cause of the inconsistency is determined, the resource can be resynchronized, either as a result of an update operation on the node where the failure occurred, or by ending and restarting the administrative domain. For example, an MRE for a user profile could be inconsistent because you changed the UID for the user profile on one node in the administrative domain, but the UID you specified was already in use by another user profile on one of the nodes. If you change the value of the UID again to something that is not used by another user profile within the administrative domain, the change will be

made by the cluster administrative domain on all nodes and the global status for the user profile MRE is set to consistent. You do not need to take any further action to resynchronize the user profile MRE.

In some cases, you need to end and restart the cluster administrative domain CRG in order for the inconsistent resources to be resynchronized. For example, if you change the UID for a user profile that has an MRE associated with it, but the user profile is active in a job on one of the other cluster nodes in the administrative domain, the global value for the MRE associated with the user profile will be set to inconsistent because the change operation failed on the node where the user profile was active in a job. In order to correct this situation, you need to wait until the job has ended and then end the cluster administrative domain. When the administrative domain is started again, the global value for each attribute that is inconsistent will be used to change the resource to a consistent state.

The global status for a monitored resource is always set to failed if the resource is deleted, renamed, or moved on any node in the domain. If this is the case, the MRE should be removed because the resource is no longer synchronized by the cluster administrative domain.

When you restore a monitored resource on any system that is part of a cluster administrative domain, the resource is resynchronized to the global value currently known in the cluster administrative domain when the cluster administrative domain is active.

The following restore commands result in a resynchronization of system objects: RSTLIB, RSTOBJ, RSTUSRPRF, and RSTCFG. In addition, RSTSYSINF and UPDSYSINF result in a resynchronization of system values and network attributes. To resynchronize system environment variables after running the RSTSYSINF or UPDSYSINF commands, the peer CRG that represents the cluster administrative domain must be ended and started again.

If you want to restore your monitored resources to a previous state, remove the MRE that represents the resource that you want to restore. Then, after restoring the resource, add an MRE for the resource from the system where the restore operation was done. The cluster administrative domain will synchronize the monitored resource across the domain by using the values from the restored resource.

To display a cluster administrative domain using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click **Cluster Administrative Domain**.

Related tasks

[Managing cluster administrative domains](#)

After a cluster administrative domain is created and the appropriate monitored resource entries (MREs) are added, the cluster administrator should monitor the activity within the administrative domain to ensure that the monitored resources remain consistent. Using PowerHA graphical interface or the PowerHA command-line interfaces, you can manage and monitor a cluster administrative domain.

Related information

[Work with Monitored Resources \(WRKCADMRE\) command](#)

Stopping a cluster administrative domain

Cluster administrative domains provide environment resiliency for resources within an IBM i high-availability solution. You might need to stop a cluster administrative domain to temporarily end synchronization of monitored resources.

A cluster administrative domain becomes inactive when it is stopped. While the cluster administrative domain is inactive, all of the monitored resources are considered to be inconsistent because changes to them are not being synchronized. Although changes to monitored resources continue to be tracked, the global value is not changed and changes are not propagated to the rest of the administrative domain. Any changes that are made to any monitored resource while the cluster administrative domain is inactive are synchronized across all active nodes when the cluster administrative domain is restarted.

Note: The cluster administrative domain and its associated exit program are IBM-supplied objects. They should not be changed using the QcstChangeClusterResourceGroup API or the **CHGCRG** command. Making these changes will cause unpredictable results.

To stop a cluster administrative domain using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Administrative Domains**.
5. On the **Cluster Administrative Domains** page, select **Stop** from the context menu of the cluster administrative domain that you want to stop.
6. Click **Yes** on the confirmation panel.

Related tasks

Managing cluster administrative domains

After a cluster administrative domain is created and the appropriate monitored resource entries (MREs) are added, the cluster administrator should monitor the activity within the administrative domain to ensure that the monitored resources remain consistent. Using PowerHA graphical interface or the PowerHA command-line interfaces, you can manage and monitor a cluster administrative domain.

Related information

End Cluster Administrative Domain (ENDCAD) command

Deleting a cluster administrative domain

Using the PowerHA graphical interface, you can delete a cluster administrative domain. Deleting a cluster administrative domain ends synchronization of monitored resources that are defined in the cluster administrative domain. In order to delete a cluster administrative domain, it must be inactive.

To delete a cluster administrative domain using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Administrative Domains**.
5. On the **Cluster Administrative Domains** page, select **Delete** from the context menu of the cluster administrative domain that you want to stop.
6. Click **Yes** on the confirmation panel.

Related tasks

Managing cluster administrative domains

After a cluster administrative domain is created and the appropriate monitored resource entries (MREs) are added, the cluster administrator should monitor the activity within the administrative domain to ensure that the monitored resources remain consistent. Using PowerHA graphical interface or the PowerHA command-line interfaces, you can manage and monitor a cluster administrative domain.

Related information

Delete Cluster Admin Domain (DLTCAD) command

Changing the properties of a cluster administrative domain

Using the PowerHA graphical interface, you can change properties to an existing cluster administrative domain. These properties control synchronizations of monitored resource entries that are defined in the cluster administrative domain.

To change the properties of a cluster administrative domain using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.

3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Administrative Domains**.
5. On the **Cluster Administrative Domains** page, select **Properties...** from the context menu of the cluster administrative domain of which you want to change the properties.
6. On the **Properties** page, click **Edit**.
7. Make changes to the properties and click **Save**.

Related tasks

Managing cluster administrative domains

After a cluster administrative domain is created and the appropriate monitored resource entries (MREs) are added, the cluster administrator should monitor the activity within the administrative domain to ensure that the monitored resources remain consistent. Using PowerHA graphical interface or the PowerHA command-line interfaces, you can manage and monitor a cluster administrative domain.

Managing monitored resource entries

The PowerHA graphical interface allows you to manage monitored resource entries in your cluster administrative domain. A cluster administrative domain ensures that changes made to these monitored resources remain consistent on each node within the high-availability environment.

Related tasks

Managing cluster administrative domains

After a cluster administrative domain is created and the appropriate monitored resource entries (MREs) are added, the cluster administrator should monitor the activity within the administrative domain to ensure that the monitored resources remain consistent. Using PowerHA graphical interface or the PowerHA command-line interfaces, you can manage and monitor a cluster administrative domain.

Working with monitored resource entry status

The PowerHA graphical interface provides status messages for monitored resource entries within a cluster administrative domain.

After an MRE is added to the cluster administrative domain, the resource is monitored for changes on all administrative domain nodes so that the values of the resource attributes can be synchronized across the nodes in the cluster administrative domain. The synchronization behavior is dependent on a number of factors:

- Status of the cluster
- Status of the cluster administrative domain
- Status of the node
- Particular actions on the resource

To work with monitored resource entry status using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Administrative Domains**.
5. On the **Cluster Administrative Domains** page, select **Monitored Resource ...** from the context menu of the cluster administrative domain to which you want to add the monitored resource.

The following status information is available from the **Monitored Resources** page.

- The status of each monitored resource is shown in the **Global Status** column.
- The status of each individual attribute of a monitored resource is shown by selecting **Attributes...** from the context menu of the monitored resource of interest.
- The reason a monitored resource is inconsistent is shown by selecting **Node Details...** from the context menu of the monitored resource of interest.

Related information

[Work with Monitored Resources \(WRKCADMRE\) command](#)

Removing monitored resource entries

Monitored resource entries (MREs) are resources that are currently used within the high-availability environment and are monitored for changes through a cluster administrative domain. You might want to remove MREs when you no longer need them to be monitored. You can remove monitored resource entries (MREs) by using the PowerHA graphical interface.

To remove a monitored resource entry using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Administrative Domains**.
5. On the **Cluster Administrative Domains** page, select **Monitored Resource ...** from the context menu of the cluster administrative domain to which you want to remove the monitored resource.
6. On the **Monitored Resource Entries** page, select **Remove** from the context menu of the monitored resource that you want to remove.
7. Click **Yes** on the confirmation panel.

Related information

[Remove Admin Domain MRE \(RMVCADMRE\) command](#)

[Remove Monitored Resource Entry \(QfpadRmvMonitoredResourceEntry\) API](#)

Listing monitored resource entries

Monitored resource entries are resources, such as user profiles and environment variables, that have been defined in a cluster administrative domain. You can use the PowerHA graphical interface to list monitored resource entries that are currently defined in a cluster administrative domain.

To list monitored resource entries using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Administrative Domains**.
5. On the **Cluster Administrative Domains** page, select **Monitored Resource ...** from the context menu of the cluster administrative domain to which you want to add the monitored resource.

Selecting attributes to monitor

After you have added monitored resource entries, you can select attributes associated with that resource to be monitored by the cluster administrative domain.

To select attributes to monitor for a monitored resource entry (MRE), follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Administrative Domains**.
5. On the **Cluster Administrative Domains** page, select **Monitored Resource ...** from the context menu of the cluster administrative domain to which you want to add the monitored resource.
6. In the list of monitored resource types, click the context icon next to the monitored resource type, and select **Monitored Resource Entries....** The MRE object list is shown.
7. Click the context icon next to the MRE object, such as user profile or system value, and select **Work with Attributes**. The MRE Attributes List is shown.

8. In the MRE Attribute List window, select the attributes that you want to monitor, and then click **Close**. For example, if you want to monitor Ethernet line description for changes to its resource name attribute, you would select resource name as the attribute.

Related tasks

Adding monitored resource entries

You can add a monitored resource entry (MRE) to a cluster administrative domain. Monitored resource entries define critical resources so that changes made to these resources are kept consistent across a high-availability environment.

Attributes that can be monitored

A monitored resource entry can be added to the cluster administrative domain for various types of resources. This topic lists the attributes that each resource type can be monitored.

Resource types

- Authorization lists (*AUTL)
- Classes (*CLS)
- Ethernet line descriptions (*ETHLIN)
- Independent disk pools device descriptions (*ASPDEV)
- Job descriptions (*JOB)
- Network attributes (*NETA)
- Network server configuration for connection security (*NWSCFG)
- Network server configuration for remote systems (*NWSCFG)
- Network server configurations for service processors (*NWSCFG)
- Network server descriptions for iSCSI connections (*NWSD)
- Network server descriptions for integrated network servers (*NWSD)
- Network server descriptions for integrated network servers (*NWSD) (server operating system *AUX)
- Network server storage spaces (*NWSSTG)
- Network server host adapter device descriptions (*NWSHDEV)
- Optical device descriptions (*OPTDEV)
- Printer device descriptions for LAN connections (*PRTDEV)
- Printer device descriptions for virtual connections (*PRTDEV)
- Subsystem descriptions (*SBSD)
- System environment variables (*ENVVAR)
- System values (*SYSVAL)
- Tape device descriptions (*TAPDEV)
- Token-ring line descriptions (*TRNLIN)
- TCP/IP attributes (*TCPA)
- User profiles (*USRPRF)

<i>Table 16. Attributes that can be monitored for authorization lists (*AUTL)</i>	
Attribute name	Description
AUT	Authority
OBJAUTE	Authority entry
OBJPGP	Primary group
OBJOWNER	Object owner

Table 16. Attributes that can be monitored for authorization lists (*AUTL) (continued)

Attribute name	Description
TEXT	Text description

Table 17. Attributes that can be monitored for classes (*CLS)

Attribute name	Description
CPUTIME	Maximum CPU time
DFTWAIT	Default wait time
MAXTHD	Maximum threads
MAXTMPSTG	Maximum temporary storage
OBJAUTE	Authority entry
OBJAUTL	Authorization list
OBJOWNER	Object owner
OBJPGP	Primary group
RUNPTY	Run priority
TEXT	Text description
TIMESLICE	Time slice

Table 18. Attributes that can be monitored for Ethernet line descriptions (*ETHLIN)

Attribute name	Description
ASSOCPORT	Associated port resource name
AUTOCTRL	Autocreate controller
AUTODLTCTL	Autodelete controller
CMNRCYLMT	Recovery limits
COSTBYTE	Relative cost per byte for sending and receiving data on the line
COSTCNN	Relative cost of being connected on the line
DUPLEX	Duplex
GENTSTFRM	Generate test frames
GRPADR	Group address
LINESPEED	Line speed
LINKSPEED	Link speed
MAXFRAME	Maximum frame size
MAXCTL	Maximum controllers
MSGQ	Message queue
OBJAUTE	Authority entry
OBJAUTL	Authorization list

Table 18. Attributes that can be monitored for Ethernet line descriptions (*ETHLIN) (continued)

Attribute name	Description
OBJOWNER	Object owner
OBJPGP	Primary group
ONLINE	Online at IPL
PRPDLY	Propagation delay
RSRCNAME	Resource name
SECURITY	Security level of the physical line
SSAP	Source service access point (SSAP) information list
TEXT	Text description
USRDFN1	First user-defined
USRDFN2	Second user-defined
USRDFN3	Third user-defined
VRYWAIT	Vary on wait

Table 19. Attributes that can be monitored for independent disk pools device descriptions (*ASPDEV)

Attribute name	Description
MSGQ	Message queue
OBJAUTE	Authority entry
OBJAUTL	Authorization list
OBJOWNER	Object owner
OBJPGP	Primary group
RDB	Relational database
RSRCNAME	Resource name
TEXT	Text description

Table 20. Attributes that can be monitored for job descriptions (*JOBDD)

Attribute name	Description
ACGCDE	Accounting code
ALWMLTTHD	Allow multiple threads
DDMCNV	DDM conversation
DEVRCYACN	Device recovery action
ENDSEV	End severity
HOLD	Hold on job queue
INLASPGRP	Initial ASP group
INLLIBL	Initial library list
INQMSGRPY	Inquiry message reply

Table 20. Attributes that can be monitored for job descriptions (*JOBDB) (continued)

Attribute name	Description
JOBMSGQFL	Job message queue full action
JOBMSGQMX	Job message queue maximum size
JOBPTY	Job priority (on JOBQ)
JOBQ	Job queue
LOG	Message logging
LOGCLPGM	Log CL program commands
OBJAUTE	Authority entry
OBJAUTL	Authorization list
OBJOWNER	Object owner
OBJPGP	Primary group
OUTPTY	Output priority (on OUTQ)
OUTQ	Output queue
PRTDEV	Print device
PRTTXT	Print text
RQSDTA	Request data or command
RTGDTA	Routing data
SPLFACN	Spoiled file action
SWS	Job switches
SYNTAX	CL syntax check
TEXT	Text description
TSEPOOL	Time slice end pool
USER	User

Table 21. Attributes that can be monitored for network attributes (*NETA)

Attribute name	Description
ALWADDCLU	Allow add to cluster
DDMACC	DDM/DRDA request access
NWSDOMAIN	Network server domain
PCSACC	Client request access
Note: Each network attribute is treated as its own monitored resource entry. For these, the resource type and attribute names are identical.	

Table 22. Attributes that can be monitored for network server configurations for service processors (*NWSCFG)

Attribute name	Description
EID	Enclosure identifier

*Table 22. Attributes that can be monitored for network server configurations for service processors (*NWSCFG) (continued)*

Attribute name	Description
INZSP	Initialize service processor
OBJAUTE	Authority entry
OBJAUTL	Authorization list
OBJOWNER	Object owner
OBJPGP	Primary group
SPAUT	Service processor authority
SPCERTID	Service processor certificate identifier
SPINTNETA	Service processor Internet address
SPNAME	Service processor name
TEXT	Text description

*Table 23. Attributes that can be monitored for network server configuration for remote systems (*NWSCFG)*

Attribute name	Description
BOOTDEVID	Boot device identifier
CHAPAUT	Target CHAP authentication
DELIVERY	Delivery method
DYNBOOTOPT	Dynamic boot options
INRCHAPAUT	Initiator CHAP authentication
OBJAUTE	Authority entry
OBJAUTL	Authorization list
OBJOWNER	Object owner
OBJPGP	Primary group
RMTIFC	Remote interfaces
RMTSYSID	Remote system identifier
SPNWSCFG	Service processor network server configuration that is used to manage the remote server
TEXT	Text description

*Table 24. Attributes that can be monitored for network server configuration for connection security (*NWSCFG)*

Attribute name	Description
IPSECRULE	IP security rules
OBJAUTE	Authority entry
OBJAUTL	Authorization list
OBJOWNER	Object owner

*Table 24. Attributes that can be monitored for network server configuration for connection security (*NWSCFG) (continued)*

Attribute name	Description
OBJPGP	Primary group
TEXT	Text description

*Table 25. Attributes that can be monitored for Network server descriptions for integrated network servers (*NWSD)*

Attribute name	Description
ALWDEVRSC	Allowed device resources
CFGFILE	Configuration file
CODEPAGE	ASCII code page representing the character set to be used by this network server
EVTLOG	Event log
MSGQ	Message queue
NWSSTGL	Storage space links
OBJAUTE	Authority entry
OBJAUTL	Authorization list
OBJOWNER	Object owner
OBJPGP	Primary group
PRPDMNUSR	Propagate domain user
RSRCNAME	Resource name
RSTDDEVRSC	Restricted device resources
SHUTDTIMO	Shut down time out
SYNCTIME	Synchronize date and time
TCPDMNNAME	TCP/IP local domain name
TCPHOSTNAM	TCP/IP host name
TCPPORTCFG	TCP/IP port configuration
TCPNAMSVR	TCP/IP name server system
TEXT	Text description
VRYWAIT	Vary on wait
WINDOWSNT	Windows network server description

*Table 26. Attributes that can be monitored for Network server descriptions for integrated network servers (server operating system *AUX) (*NWSD)*

Attribute name	Description
CODEPAGE	ASCII code page representing the character set to be used by this network server
DSBUSRPRF	Disable user profiles

Table 26. Attributes that can be monitored for Network server descriptions for integrated network servers (server operating system *AUX) (*NWSD) (continued)

Attribute name	Description
EVTLOG	Event log
MSGQ	Message queue
OBJAUTE	Authority entry
OBJAUTL	Authorization list
OBJOWNER	Object owner
OBJPGP	Primary group
PRPDMNUSR	Propagate domain user
RSRCNAME	Resource name
SHUTDTIMO	Shut down time out
SRVOPT	Serviceability options
SYNCTIME	Synchronize date and time
TCPDMNNAME	TCP/IP local domain name
TCPHOSTNAM	TCP/IP host name
TCPPORTCFG	TCP/IP port configuration
TEXT	Text description
VRYWAIT	Vary on wait

Table 27. Attributes that can be monitored for network server descriptions for iSCSI connections (*NWSD)

Attribute name	Description
ACTTMR	Activation timer
ALWDEVRSC	Allowed device resources
CFGFILE	Configuration file
CMNMSGQ	Communications message queue
CODEPAGE	ASCII code page representing the character set to be used by this network server
DFTSECRULE	Default IP security rule
DFTSTGPTH	Default storage path
EVTLOG	Event log
MLTPHGRP	Multi-path group
MSGQ	Message queue
NWSCFG	Network server configuration
NWSSTGL	Storage space links
OBJAUTE	Authority entry
OBJAUTL	Authorization list

*Table 27. Attributes that can be monitored for network server descriptions for iSCSI connections (*NWSD) (continued)*

Attribute name	Description
OBJOWNER	Object owner
OBJPGP	Primary group
PRPDMNUSR	Propagate domain user
RMVMEDPTH	Removable media path
RSRCNAME	Resource name
RSTDDEVRSC	Restricted device resources
SHUTDTIMO	Shut down time out
STGPTH	iSCSI storage paths of the network server
SVROPT	Serviceability options
SYNCTIME	Synchronize date and time
TCPDMNNAME	TCP/IP local domain name
TCPHOSTNAM	TCP/IP host name
TCPNAMSVR	TCP/IP name server system
TCPPORTCFG	TCP/IP port configuration
TEXT	Text description
VRTETHCTLP	Virtual Ethernet control port
VRTETHPTH	Virtual Ethernet path
VRYWAIT	Vary on wait

*Table 28. Attributes that can be monitored for network server storage spaces (*NWSSTG)*

Attribute name	Description
OBJAUTE	Authority entry
OBJAUTL	Authorization list
OBJOWNER	Object owner
OBJPGP	Primary group
RSCALCPTY	Resource allocate priority
SIZE	Size
TEXT	Text description
TOTALFILES	Total files

*Table 29. Attributes that can be monitored for network server host adapter device descriptions (*NWSHDEV)*

Attribute name	Description
CMNRCYLMT	Recovery limits
LCLIFC	Associated local interface

*Table 29. Attributes that can be monitored for network server host adapter device descriptions (*NWSHDEV) (continued)*

Attribute name	Description
MSGQ	Message queue
OBJAUTE	Authority entry
OBJAUTL	Authorization list
OBJOWNER	Object owner
OBJPGP	Primary group
ONLINE	Online at IPL
RSRCNAME	Resource name
TEXT	Text description

*Table 30. Attributes that can be monitored for optical device descriptions *OPTDEV)*

Attribute name	Description
MSGQ	Message queue
OBJAUTE	Authority entry
OBJAUTL	Authorization list
OBJOWNER	Object owner
OBJPGP	Primary group
ONLINE	Online at IPL
RSRCNAME	Resource name
TEXT	Text description

*Table 31. Attributes that can be monitored for printer device descriptions for *LAN connections (*PRTDEV)*

Attribute name	Description
ACTTMR	Activation timer
ADPTADR	LAN remote adapter address
ADPTTYPE	Adapter type
ADPTCNNTYP	Adapter connection type
AFP	Advanced function printing
CHRID	Character identifier
FONT	Font
FORMFEED	Formfeed
IMGCFG	Image configuration
INACTTMR	Inactivity timer
LNGTYPE	Language type
LOCADR	Location location address

Table 31. Attributes that can be monitored for printer device descriptions for *LAN connections (*PRTDEV) (continued)

Attribute name	Description
MAXPNDRQS	Maximum pending request
MFRTYPMDL	Manufacturer type and model
MSGQ	Message queue
OBJAUTE	Authority entry
OBJAUTL	Authorization list
OBJOWNER	Object owner
OBJPGP	Primary group
ONLINE	Online at IPL
PORT	Port number
PRTERMSG	Print error message
PUBLISHINF	Publishing information
RMTLOCNAME	Remote location
SEPDRAWER	Separator drawer
SEPPGM	Separator program
SWTLINLST	Switched line list
SYSDRVPGM	System driver program
TEXT	Text description
TRANSFORM	Host printer transform
USRDFNOBJ	User-defined object
USRDFNOPT	User-defined options
USRDRVPGM	User-defined driver program
USRDTATFM	Data transform program
WSCST	Workstation customizing object

Table 32. Attributes that can be monitored for printer device descriptions for *VRT connections (*PRTDEV)

Attribute name	Description
CHRID	Character identifier
FORMFEED	Form feed
IGCFEAT	DBCS FEATURE
IMGCFG	Image configuration
MAXLENRU	Maximum length of request unit
MFRTYPMDL	Manufacturer type and model
MSGQ	Message queue
OBJAUTE	Authority entry

Table 32. Attributes that can be monitored for printer device descriptions for *VRT connections (*PRTDEV) (continued)

Attribute name	Description
OBJAUTL	Authorization list
OBJOWNER	Object owner
OBJPGP	Primary group
ONLINE	Online at IPL
PRTERMSG	Print error message
PUBLISHINF	Publishing information
SEPDRAWER	Separator drawer
SEPPGM	Separator program
TEXT	Text description
TRANSFORM	Host print transform
USRDFNOBJ	User-defined object
USRDFNOPT	User-defined options
USRDRVPGM	User-defined driver program
USRDTAFM	Data transform program
WSCST	Workstation customizing object
SEPPGM	Separator program
SWTLINLST	Switched line list
SYSDRVPGM	System driver program
TEXT	Text description
TRANSFORM	Host printer transform
USRDFNOBJ	User-defined object
USRDFNOPT	User-defined options
USRDRVPGM	User-defined driver program
USRDTAFM	Data transform program
WSCST	Workstation customizing object

Table 33. Attributes that can be monitored for subsystem descriptions (*SBSD)

Attribute name	Description
AJE	Autostart job entry
CMNE	Online at IPL
JOBQE	Job queue
MAXJOBS	Maximum number of jobs
OBJAUTE	Authority entry
OBJAUTL	Authorization list

Table 33. Attributes that can be monitored for subsystem descriptions (*SBSD) (continued)

Attribute name	Description
OBJOWNER	Object owner
OBJPGP	Primary group
PJE	Prestart job entry
RMTLOCNAME	Remote location name
RTGE	Routing entry
SGNDSPF	Sign on display
SYSLIBLE	Subsystem library
TEXT	Text description
WSNE	Workstation name entry
WSTE	Workstation type entry

Table 34. Attributes that can be monitored for system environment variables (*ENVVAR)

Attribute name	Description
	Any *SYS level environment variable can be monitored. The attribute and resource name are both the same as the environment variable's name.
	Note: Each environment variable is treated as its own monitored resource entry. For these, the resource type and attribute names are identical.

Table 35. Attributes that can be monitored for system values (*SYSVAL)

Attribute name	Description
QACGLVL	Accounting level
QACTJOBTP	Allow jobs to be interrupted
QALWOBJRST	Prevents anyone from restoring a system-state object or an object that adopts authority
QALWUSRDMN	Allows user domain objects
QASTLVL	Assistance level
QATNPGM	Attention program
QAUDCTL	Audit control
QAUDENDACN	Audit journal error action
QAUDFRCLVL	Auditing force level
QAUDLVL	Auditing level
QAUDLVL2	Auditing level extension
QAUTOCFG	Automatic device configuration
QAUTORMT	Remote controllers and devices

Table 35. Attributes that can be monitored for system values (*SYSVAL) (continued)

Attribute name	Description
QAUTOVRT	Automatic virtual device configuration
QCCSID	Coded character set identifier
QCFGMSGQ	Message queue for lines, controllers, and devices
QCHRID	Default graphic character set and code page used for displaying or printing data
QCHRIDCTL	Character identifier control for the job
QCMNRCYLMT	Automatic communications error recovery
QCNTRYID	Country or region identifier
QCRTAUT	Authority for new objects
QCRTOBJAUD	Auditing new objects
QCTLSBSD	Controlling subsystem or library
QCURSYM	Currency symbol
QDATFMT	Date format
QDATSEP	Date separator
QDBRCVYWT	Wait for database recovery before completing restart
QDECFMT	Decimal format
QDEVNAMING	Device naming convention
QDEVRCYACN	Device recovery action
QDSCJOBIV	Time out interval for disconnected jobs
QDSPSGNINF	Controls the display of sign-on information
QENDJOBLMT	Maximum time for immediate end
QFRCCVNRST	Force conversion on restore
QHSTLOGSIZ	History log file size
QIGCCDEFNT	Coded font name
QIGCFNTSIZ	Coded font point size
QINACTIV	Inactive job time-out interval
QINACTMSGQ	Timeout interval action
QIPLTYPE	Type of restart
QJOBMSGQFL	Job message queue full action
QJOBMSGQMX	Job message queue maximum size
QJOBMSGQSZ	Initial size of job message queue in kilobytes (KB)
QJOBMSGQTL	Maximum size of job message queue (in KB)
QJOBSPLA	Initial size of spooling control block for a job (in bytes)

Table 35. Attributes that can be monitored for system values (*SYSVAL) (continued)

Attribute name	Description
QKBDBUF	Keyboard buffer
QKBDTYPE	Keyboard language character set
QLANGID	Default language identifier
QLIBLCKLVL	Lock libraries in a user job's library search list
QLMTDEVSSN	Limit device sessions
QLMTSECOFR	Limit security officer device access
QLOCALE	Locale
QLOGOUTPUT	Produce printer output for job log
QMAXACTLVL	Maximum activity level of the system
QMAXJOB	Maximum number of jobs that are allowed on the system
QMAXSGNACN	The system's response when the limit imposed by QMAXSIGN system value is reached
QMAXSIGN	Maximum number of not valid sign-on attempts allowed
QMAXSPLF	Maximum printer output files
QMLTTHDACN	When a function in a multithreaded job is not threadsafe
QPASTHRSVR	Available display station pass-through server jobs
QPRBFTR	Problem log filter
QPRBHLDTV	Minimum retention
QPRTDEV	Default printer
QPRTKEYFMT	Print key format
QPRTTXT	Up to 30 characters of text that can be printed at the bottom of listings and separator pages
QPWDCHGBLK	Minimum time between password changes
QPWDEXPITV	Number of days for which a password is valid
QPWDEXPWRN	Password expiration warning interval system
QPWDLMTACJ	Limits the use of adjacent numbers in a password
QPWDLMTCHR	Limits the use of certain characters in a password
QPWDLMTREP	Limits the use of repeating characters in a password
QPWDLVL	Password level
QPWDMAXLEN	Maximum number of characters in a password
QPWDMINLEN	Minimum number of characters in a password
QPWDPOSDIF	Controls the position of characters in a new password

Table 35. Attributes that can be monitored for system values (*SYSVAL) (continued)

Attribute name	Description
QPWDRQDDGT	Require a number in a new password
QPWDRQDDIF	Controls whether the password must be different from the previous passwords
QPWDRULES	Password rules
QPWDVLDPGM	Password approval program
QPWRDWNLMT	Maximum time for immediate shutdown
QRCLSPLSTG	Automatically clean up unused printer output storage
QRETSVRSEC	Retain server security data indicator
QRMTSIGN	Remote sign-on
QRMTSRVATR	Remote service attribute
QSCANFS	Scan file systems
QSCANFCTL	Scan control
QSCPFCONS	Console problem occurs
QSECURITY	System security level
QSETJOBATR	Set job attributes
QSFWERRLOG	Software error log
QSHRMEMCTL	Allow use of shared or mapped memory with write capability
QSPCENV	Default user environment
QSPLFACN	Spooled file action
QSRTSEQ	Sort sequence
QSRVDMP	Service log for unmonitored escape messages
QSSLCSL	Secure Sockets Layer cipher specification list
QSSLCSLCTL	Secure Sockets Layer cipher control
QSSLPCL	Secure Sockets Layer protocols
QSTRUPPGM	Set startup program
QSTMSG	Display status messages
QSYSLIBL	System library list
QTIMSEP	Time separator
QTSEPOOL	Indicates whether interactive jobs should be moved to another main storage pool when they reach time slice end
QUPSMGQ	Uninterruptible power supply message queue
QUSEADPAUT	Use adopted authority
QUSRLIBL	User part of the library list

Table 35. Attributes that can be monitored for system values (*SYSVAL) (continued)

Attribute name	Description
QVFOBJRST	Verify object on restore
Note: Each system value is treated as its own monitored resource entry. For these, the resource type and attribute names are identical.	

Table 36. Attributes that can be monitored for tape device descriptions (*TAPDEV)

Attribute name	Description
ASSIGN	Assign device at vary on
MSGQ	Message queue
OBJAUTE	Authority entry
OBJAUTL	Authorization list
OBJOWNER	Object owner
OBJPGP	Primary object
ONLINE	Online at IPL
RSRCNAME	Resource name
TEXT	Text description
UNLOAD	Unload device at vary off

Table 37. Attributes that can be monitored for token-ring descriptions (*TRNLIN)

Attribute name	Description
ACTLANMGR	Activate LAN manager
ADPTADR	Local adapter address
AUTOCRTCTL	Autocreate controller
AUTODLTCTL	Autodelete controller
CMNRCYLMT	Recovery limits
COSTBYTE	Relative cost per byte for sending and receiving data on the line
COSTCNN	Relative cost of being connected on the line
DUPLEX	Duplex
ELYTKNRLS	Early token release
FCNADR	Functional address
LINESPEED	Line speed
LINKSPEED	Link speed
LOGCFGCHG	Log configuration changes
MAXCTL	Maximum controllers
MAXFRAME	Maximum frame size
MSGQ	Message queue

Table 37. Attributes that can be monitored for token-ring descriptions (*TRNLIN) (continued)

Attribute name	Description
OBJAUTE	Authority entry
OBJAUTL	Authorization list
OBJOWNER	Object owner
OBJPGP	Primary group
ONLINE	Online at IPL
PRPDLY	Propagation delay
RSRCNAME	Resource name
SECURITY	Security for line
SSAP	Source service access point (SSAP) information list
TRNINFBDN	Token-ring inform of beacon
TRNLOGLVL	TRLAN manager logging level
TRNMGRMODE	TRLAN manager mode
TEXT	Text description of the token-ring line
USRDFN1	First user-defined
USRDFN2	Second user-defined
USRDFN3	Third user-defined
VRYWAIT	Vary on wait

Table 38. Attributes that can be monitored for TCP/IP attributes (*TCPA)

Attribute name	Description
ARPTIMO	Address resolution protocol (ARP) cache timeout
ECN	Enable explicit congestion notification (ECN)
IP6TMPAXP	IPv6 temporary address excluded prefix
IPDEADGATE	IP dead gateway detection
IPDTGFWD	IP datagram forwarding
IPPATHMTU	Path maximum transmission unit (MTU) discovery
IPQOSBCH	IP QoS datagram batching
IPQOSEN	IP QoS enablement
IPQOSTMR	IP QoS timer resolution
IPRSBTIMO	IP reassembly timeout
IPSRCRTG	IP source routing
IPTTL	IP time to live (hop limit)
LOGPCLERR	Log protocol errors
NFC	Network file cache
TCPCLOTIMO	TCP time-wait timeout

Table 38. Attributes that can be monitored for TCP/IP attributes (*TCPA) (continued)

Attribute name	Description
TCPCNNMSG	TCP close connection message
TCPKEEPALV	TCP keep alive
TCPMINRTM	TCP minimum retransmit time
TCPR1CNT	TCP R1 retransmission count
TCPR2CNT	TCP R2 retransmission count
TCPRCVBUF	TCP receive buffer size
TCPSNDBUF	TCP send buffer size
TCPURGPTR	TCP urgent pointer
UDPCKS	UDP checksum
Note: Each TCP/IP attribute is treated as its own monitored resource entry. For these, the resource type and attribute names are identical.	

Table 39. Attributes that can be monitored for user profiles (*USRPRF)

Attribute name	Description
ACGCDE	Accounting code
ASTLVL	Assistance level
ATNPGM	Attention program
CCSID	Coded character set ID
CHRIDCTL	Character identifier control
CNTRYID	Country or region ID
CURLIB	Current library
DLVRY	Delivery
DSPSGNINF	Display sign-on information
GID	Group ID number
GRPAUT	Group authority
GRPAUTYP	Group authority type
GRPPRF	Group profile
HOMEDIR	Home directory
INLMNU	Initial menu
INLPGM	Initial program to call
JOB	Job description
KBDBUF	Keyboard buffering
LANGID	Language ID
LCLPDMGT	Local password management
LMTCPB	Limit capabilities

Table 39. Attributes that can be monitored for user profiles (*USRPRF) (continued)

Attribute name	Description
LMTDEVSSN	Limit device sessions
LOCALE	Locale
MAXSTG	Maximum allowed storage
MAXSTGLRG	Maximum allowed storage large
MSGQ	Message queue
OBJAUTE	Authority entry
OBJOWNER	Object owner
OBJPGP	Primary group
OUTQ	Output queue
OWNER	Owner
PASSWORD	User password
PRTDEV	Print device
PTYLMT	Highest schedule priority
PWDEXP	Set password to expired
PWDEXPITV	Password expiration interval
SETJOBATR	Locale job attributes
SEV	Severity code filter
SPCAUT	Special authority
SPCENV	Special environment
SRTSEQ	Sort sequence
STATUS	Status
SUPGRPPRF	Supplemental groups
TEXT	Text description
UID	User ID number
USRCLS	User class
USREXPDATE	User expiration date
USREXPITV	User expiration interval
USROPT	User options

Displaying monitored resource entry messages

Using the PowerHA graphical interface, you can display messages that are associated with monitored resource entries. These messages can help explain why a particular monitored resource entry is inconsistent.

To view monitored resource entry messages using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.

4. On the **PowerHA** page, click on **Cluster Administrative Domains**.
5. On the **Cluster Administrative Domains** page, select **Monitored Resource ...** from the context menu of the cluster administrative domain to which you want to add the monitored resource.
6. On the **Monitored Resources** page, select **Node Details ...** from the context menu of the monitored resource entry of which you want to see messages.

Managing independent disk pools

In a high-availability environment, it is necessary that the application and its data remain consistent among the nodes that participate in high availability. An independent disk pool, also called an independent auxiliary storage pool (IASP), is a disk pool that contains objects, the directories, or libraries that contain the objects, and other object attributes such as authorization and ownership attributes. An independent disk pool can be used to help in this situation. Ownership of data and applications that are stored in an independent disk pool can be switched to other systems that are defined in the device CRG. PowerHA technology provides high availability during planned and some unplanned outages.

Related information

[IBM eServer iSeries Independent ASPs: A Guide to Moving Applications to IASPs](#)

Quiescing an independent disk pool

In an IBM i high-availability solution, independent disk pools are used to store resilient data and applications. Some system functions, such as performing backups, require that you temporarily suspend changes to that data while the operation occurs.

To decrease the amount of time it takes to quiesce an independent disk pool, you might want to hold batch job queues, end some subsystems, or send a break message to interactive users, advising them to postpone new work.

To quiesce an independent disk pool, complete these steps.

In a command line interface, enter the following command: **CHGASPACT ASPDEV(name) OPTION(*SUSPEND) SSPTIMO(30) SSPTIMOACN(*CONT)**, where *name* is the name of the independent disk pool that you want to suspend. In this command you are specifying to suspend the independent disk pool with a 30-second timeout, and to continue with the next step even if the timeout limit has been exceeded.

Resuming an independent disk pool

After you have quiesced an independent disk pool in an IBM i high availability environment for backup operations, you will need to resume the independent disk pool to ensure changes that are made to the data during the quiesce are updated.

Complete these steps to resume an independent disk pool:

In a command-line interface, enter the following command: **CHGASPACT ASPDEV(name) OPTION(*RESUME)**, where *name* is the name of the independent disk pool that you want to resume.

Managing copy descriptions

Manage and maintain PowerHA copy descriptions

Copy descriptions are used in IBM PowerHA SystemMirror for i to store information used in Geographic Mirror, Metro Mirror, Global Mirror, and FlashCopy copy sessions. The copy descriptions provide an auxiliary storage pool (ASP) session with the information such as specific disk units or access credentials that the session needs to perform its operations.

After adding a copy description, you can:

- display the description information.
- change the copy description information.
- remove the copy description.

Copy descriptions content varies depending on the type of storage your system uses and the type of copy session the description supports.

Displaying an ASP copy description

The Display ASP Copy Description (**DSPASPCPYD**) command shows the current properties of a copy description.

The Display Auxiliary Storage Pool Copy Description (**DSPASPCPYD**) command displays an auxiliary storage pool (ASP) copy description. This information is useful to determine the current properties of the copy description such as the device domain, storage units, and volumes associated with the copy.

The Display ASP Copy description screen can be accessed by using:

- the Work with Cluster (**WRKCLU**) command menu. Select option 10, Work with ASP copy descriptions and use option 5, Display copy to show the current information contained in the selected copy description.
- entering the **WRKASPCPYD** command that opens the Work with ASP Copy Descriptions screen. Locate the copy description and use option 5, Display copy to show the current information contained in the selected copy description.
- typing the **DSPASPCPYD** command and pressing F4.

To display an ASP copy description with the **DSPASPCPYD** command, follow these steps:

1. Type **DSPASPCPYD** on the command line and press Enter.
2. Enter the name of the ASP copy description to display.
3. Type in the name of the device domain, or * to indicate the device domain for the current node.
4. Enter * to display the ASP copy description information on the screen or *PRINT to print the output in a spool file.
5. Press Enter to display or print the copy description.

As a command sequence, type in:

```
DSPASPCPYD ASPCPY(copy description-name) DEVDMN(*|device domain-name) OUTPUT(*|*PRINT)
```

to display a particular ASP copy description in a particular way.

Verify that the entries in the copy description are configured correctly. If changes are required, they are made with the **CHGASPCPYD** command.

For details about the **DSPASPCPYD** or **CHGASPCPYD** commands and specific fields, consult the F1 Help or visit the [DSPASPCPYD](#) and [CHGASPCPYD](#) pages.

Displaying a SVC copy description

The Display SVC Copy Description (**DSPSVCCPYD**) command shows the current properties of a copy description.

The Display SAN Volume Controller Copy Description (**DSPSVCCPYD**) command displays Storage Area Network Volume Controller (SVC) ASP copy descriptions. This information is useful to determine the current properties of the copy description such as the device domain, storage units, and volumes associated with the copy.

The Display SVC Copy description screen can be accessed by using:

- the Work with Cluster (**WRKCLU**) command menu. Select option 10, Work with ASP copy descriptions and use option 5, Display copy to show the current information contained in the selected copy description.
- entering the **WRKSVCCPYD** command that opens the Work with ASP Copy Descriptions screen. Locate the copy description and use option 5, Display copy to show the current information contained in the selected copy description.
- typing the **DSPSVCCPYD** command and pressing F4.

To display an SVC copy description with the **DSPSVCCPYD** command, follow these steps:

1. Type **DSPSVCCPYD** on the command line and press Enter.
2. Enter the name of the SVC copy description to display.
3. Type in the name of the device domain, or * to indicate the device domain for the current node.
4. Enter * to display the SVC copy description information on the screen or *PRINT to print the output in a spool file.
5. Press Enter to display or print the copy description.

As a command sequence, type in:

```
DSPSVCCPYD ASPCPY(copy description-name) DEVDMN(*|device domain-name) OUTPUT(*|*PRINT)
```

to display a particular SVC copy description in a particular way.

Verify that the entries in the copy description are configured correctly. If changes are required, they are made with the **CHGSVCCPYD** command.

For details about the **DSPSVCCPYD** or **CHGSVCCPYD** commands and specific fields, consult the F1 Help or visit the [DPSVCCPYD](#), and [CHGSVCCPYD](#) pages.

Changing an ASP copy description

Make modifications to an ASP copy description using the Change ASP Copy Description (**CHGASPCPYD**) command

The Change Auxiliary Storage Pool (ASP) Copy Description (**CHGASPCPYD**) command displays the Change Copy Description panel. Here you can make changes to the ASP copy description to reflect changes to the PowerHA environment.

A common use of the **CHGASPCPYD** is to update the disk units of the IASP. When users add or remove disk units, the copy description needs to be updated to reflect the change for the copy session to work.

The Change ASP Copy description screen can be accessed by using:

- the Work with Cluster (**WRKCLU**) command menu. Select option 10, Work with ASP copy descriptions and use option 2, Change copy to go to the Change Copy description screen.
- entering the **WRKASPCPYD** command that opens the Work with ASP Copy Descriptions screen. Locate the copy description and use option 2, Change copy to open the Change Copy description screen for the selected ASP copy description.
- typing the **CHGASPCPYD** command and pressing F4.

To access the Change ASP copy description with the (**CHGASPCPYD**) command, do the following:

1. Type CHGASPCPYD on the command line and press Enter.
2. On the Change ASP Copy description panel enter the copy description name and the device domain in the respective fields and press Enter.
3. Locate the fields that require changes.
4. Make the changes to the fields and press Enter.

You will be returned to your previous menu page.

As a command sequence, type in:

```
CHGASPCPYD ASPCOPY(copy description-name) SVCHOST(*SAME | user-name *SAME | 'file-path' *SAME | 'network address')DEVDMN(* | device domain-name)
```

to change an ASP copy description parameter.

To verify that the changes to the copy description, use the **DSPASPCPYD** command or select option 5 on the Work with ASP copy descriptions menu page.

For details about the **CHGASPCPYD** command and specific fields, consult the F1 Help or visit the [CHGASPCPYD](#) page.

Changing a SVC copy description

Make modifications to an SVC copy description using the Change SVC Copy Description (**CHGSVCCPYD**) command

The Change SVC Copy Description (**CHGSVCCPYD**) command displays the Change Copy Description panel. Here you can make changes to the SVC copy description to reflect changes to the PowerHA environment.

A common use of the **CHGSVCCPYD** is to update the disk units of the IASP. When users add or remove disk units, the copy description needs to be updated to reflect the change for the copy session to work.

The Change ASP SVC Copy description screen can be accessed by using:

- the Work with Cluster (**WRKCLU**) command menu. Select option 10, Work with ASP copy descriptions and use option 2, Change copy to go to the Change Copy description screen.
- entering the **WRKSVCCPYD** command that opens the Work with ASP Copy Descriptions screen. Locate the copy description and use option 2, Change copy to open the Change Copy description screen for the selected SVC copy description.
- typing the **CHGSVCCPYD** command and pressing F4.

To access the Change SVC copy description screen with the (**CHGSVCCPYD**) command do the following:

1. Type **CHGSVCCPYD** in the command line and press Enter.
2. The Change SVC Copy Description screen opens. Type in the name of the copy description to change and press Enter to show the copy description.
3. Locate the fields that require changes.
4. Make the changes to the fields and press Enter.

You will be returned to your previous page.

As a command sequence, type in:

```
CHGSVCCPYD ASPCOPY(copy description-name) SVCHOST(*SAME | user-name *SAME | 'file-path' *SAME | 'network address')DEVDMN(* | device domain-name)
```

to change an SVC copy description parameter.

To verify that the changes to the copy description, use the **DSPSVCCPYD** command or select option 5 on the Work with ASP copy descriptions menu page.

For details about the **CHGSVCCPYD** command and specific fields, consult the F1 Help or visit the **CHGSVCCPYD** page.

Removing an ASP copy description

Remove an ASP copy description with the Remove ASP Copy Description (**RMVASPCPYD**) command

The Remove Auxiliary Storage Pool (ASP) Copy Description (**RMVASPCPYD**) command removes an ASP copy description.

The Remove ASP Copy description screen can be accessed by using:

- the Work with Cluster (**WRKCLU**) command menu. Select option 10, Work with ASP copy descriptions and use option 4, Remove copy to remove the selected copy description.
- entering the **WRKASPCPYD** command that opens the Work with ASP Copy Descriptions screen. Locate the copy description and use option 4, Remove copy to remove the selected copy description.
- typing the **RMVASPCPYD** command and pressing F4.

To remove an ASP copy description with the **WRKASPCPYD** screen, follow these steps:

1. On the **WRKASPCPYD** screen, select option 4 Remove copy. In the ASP Device field, type the name of the device description associated with the ASP copy description, and supply the copy description name in the ASP Copy field. Then press Enter.
2. The Confirm Action screen opens showing the command that was made that requires a confirmation.

- Select F16 (Shift + F4) to confirm the removal.
 - Press F12 to cancel the remove copy description request.
3. The system returns to the Work with ASP Copy Descriptions screen.
If you confirmed the command, the copy description you selected for removal no longer appears in the list.

As a command sequence, type in:

```
RMVASPCPYD ASPCPY(copy description-name) DEVDMN(*|device-domain)
```

to remove a particular ASP copy description.

For details about the **RMVASPCPYD** command, consult the F1 Help or visit the [RMVASPCPYD](#) page.

Removing a SVC copy description

Remove an SVC copy description with the Remove SVC Copy Description (**RMVSVCCPYD**) command

The Remove SVC Copy Description (**RMVSVCCPYD**) command removes an SVC copy description.

The Remove SVC Copy description screen can be accessed by using:

- the Work with Cluster (**WRKCLU**) command menu. Select option 10, Work with ASP copy descriptions and use option 4, Remove copy to remove the selected copy description.
- entering the **WRKSVCCPYD** command that opens the Work with SVC ASP Copy Description screen. Locate the copy description and use option 4, Remove copy to remove the selected copy description.
- typing the **RMVASPCPYD** command and pressing F4.

To remove an SVC copy description with the **RMVSVCCPYD** command, follow these steps:

1. Type in the **RMVSVCCPYD** command in the command line and press Enter.
2. On the Remove ASP Copy Description screen, supply the copy description name and device domain and press enter.
3. The system returns to the previous screen.
The copy description entered for removal will not appear in the list of available copy descriptions on the **WRKASPCPYD** screen.

As a command sequence, type in:

```
RMVSVCCPYD ASPCPY(copy description-name) DEVDMN(*|device-domain)
```

to remove a particular SVC copy description.

For details about the **RMVSVCCPYD** command, consult the F1 Help or visit the [RMVSVCCPYD](#) page.

PowerHA configuration description types

PowerHA configuration descriptions define system and storage device associations

PowerHA configuration descriptions are another method of defining the association between systems and storage devices. Each PowerHA description configuration has a name for identification, an associated cluster where the configuration description resides and a configuration type and configuration subtype.

There are two HA configuration types, each with a unique configuration subtype:

HYSSTG

A HyperSwap storage description, used to define affinity between a system and its preferred IBM System Storage device. The system is identified by the system serial number specified on the **SERIAL** parameter. The name of the IBM System Storage device is specified using the **STGDEV** parameter. This configuration type uses the *DS configuration subtype to designate a HyperSwap storage description for an IBM System Storage device.

STGCTL

A storage controller description, used to allow PowerHA to access, communicate with, and manage a storage controller by providing connection and authentication information. This configuration type uses the *CSM configuration subtype to indicate an IBM Copy Services (CSM) storage controller. Connect to the storage device like any network component.

PowerHA configuration description functions can be accessed through the command line or with the **WRKHACFGD** command group.

Adding an HA configuration description

Create an HA configuration description to provide specific configuration information about the storage components to your system

PowerHA uses configuration descriptions to connect to servers to access and manage copy service functions of key external storage components by providing connection and authentication information.

You create HA configuration descriptions using the Add HA Configuration Description (**ADDHACFGD**) command.

The Add HA Configuration Description screen can be accessed by using:

- The Work with Cluster (**WRKCLU**) command menu. Select option 11, Work with HA Config Desc., and use option 1, Add to go to the Add HA Configuration Desc. panel.
- Type the **WRKHACFGD** command that opens the Work with HA Config Desc. screen. Use option 1, Add to open the Add HA Configuration Desc. panel.
- Entering the **ADDHACFGD** command.

To add an HA configuration description using the **ADDHACFGD** command, follow these steps:

1. Type **ADDHACFGD** on the command line and press Enter.
2. On the Add HA Configuration Desc. (**ADDHACFGD**) panel, enter the name of the cluster to add the HA configuration description to, or enter * to indicate the current cluster.
3. Type a name for the new HA configuration description in the Configuration name field.
4. In the Configuration type field, enter the type of configuration description.

Enter one of two options depending on your network setup:

***HYSSTG**

A HyperSwap storage description, used to define affinity between a system and its preferred IBM System Storage device. The system is identified by the system serial number specified on the **SERIAL** parameter. The name of the IBM System Storage device is specified using the **STGDEV** parameter. This configuration type uses the *DS configuration subtype to designate a HyperSwap storage description for an IBM System Storage device.

***STGCTL**

A storage controller description, used to allow PowerHA to access, communicate with, and manage a storage controller by providing connection and authentication information. This configuration type uses the *CSM configuration subtype to indicate an IBM Copy Services (CSM) storage controller. Connect to the storage device like any network component.

5. You must enter a configuration subtype in the Configuration subtype field.
 - If using a ***HYSSTG** configuration type, enter *DS in the subtype field.
 - If using a ***STGSTL** configuration type, enter *CSM as the subtype.
- a) If you are using a ***HYSSTG** configuration type with the *DS subtype, enter the serial number of the storage system in the System serial number field and in the IBM System Storage device, type in the name of your device.

- b) If you are using the ***STGCTL** configuration type with the ***CSM** subtype, you must supply connection authentication information in the Host section including a User name, the primary, and secondary internet addresses.

6. Press Enter to create the HA configuration description.

As a command sequence type in the following:

```
ADDHACFGD CLUSTER(cluster-name) NAME(configuration-name) TYPE(*HYSSTG|*STGCTL) SUBTYPE(*DS|*CSM) STGDEV(storage device-name)
```

to add a HA configuration description to the cluster.

The HA configuration description is ready to use. To verify the parameters of the description, use the Display HA Configuration Description (**DSPHACFGD**) command. The parameters of the configuration description can be changed with the Change Configuration Description (**CHGCACFGD**) command.

For additional information about the **ADDHACFGD** command and specific fields consult the **F1** help or visit the [ADDHACFGD](#) page.

Displaying an HA configuration description

The Display HA Configuration Description (**DSPHACFGD**) command shows the current properties of the HA configuration description

The Display HA Configuration Description command displays the current properties of the HA configuration description. This information is useful to determine the connection methods to the system storage, affinity with storage units and network location of storage units.

The Display HA Configuration Description screen can be accessed by using:

- The Work with Cluster (**WRKCLU**) command menu. Select option 11, Work with HA Config Desc., and use option 5, Display to go to the Display HA Configuration Desc. panel.
- Type the **WRKHACFGD** command to open the Work with HA Config Desc screen. Locate the HA configuration description you want to view and use option 5, Display, to open the Display HA Configuration Desc. panel.
- Entering the **DSPHACFGD** command.

To display an HA configuration description using the **DSPHACFGD** command, follow these steps:

1. Type **DSPHACFGD** on the command line and press Enter.
2. On the Display HA Configuration Desc. (**DSPHACFGD**) panel, enter the name of the cluster the HA configuration description belongs to, or enter * to indicate the current cluster.
3. Type a name of the HA configuration description in the Configuration name field.
4. Enter * to display the HA configuration description information on the screen or *PRINT to print the output in a spool file. After making the selection, press Enter.

As a command sequence type in the following:

```
DSPHACFGD CLUSTER(*|cluster-name) NAME(configuration-name)
```

to display the HA configuration description.

Verify that the entries for the HA configuration are correct. If changes are required, they are made with the **CHGHACFGD** command

For additional information about the **DSPHACFGD** command and specific fields consult the **F1** help or visit the [DSPHACFGD](#) page.

Changing an HA configuration description

Change an existing HA configuration description with the Change HA Communication Description (**CHGHACFGD**) command

The Change HA Configuration Description (**CHGHACFGD**) command displays the current properties of the HA configuration description on the Change HA Configuration Desc. panel. Here you can make changes to the HA configuration description to reflect changes in the network or storage units.

The Change HA Configuration Description screen can be accessed by using:

- The Work with Cluster (**WRKCLU**) command menu. Select option 11, Work with HA Config Desc., and use option 2, Change to go to the Change HA Configuration Desc. panel.
- Type the **WRKHACFGD** command to open the Work with HA Config Desc screen. Locate the HA configuration description you want to change and use option 2, Change, to open the Change HA Configuration Desc. panel.
- Entering the **CHGHACFGD** command.

To change an HA configuration description using the **CHGHACFGD** command, follow these steps:

1. Type **CHGHACFGD** on the command line and press Enter.
2. On the Change HA Configuration Desc. (**CHGHACFGD**) panel, enter the name of the cluster the HA configuration description belongs to, or enter * to indicate the current cluster.
3. Type a name of the HA configuration description in the Configuration name field.
4. In the Configuration type field, enter the type of configuration description.
5. You must enter a configuration subtype in the Configuration subtype field.
You are prompted to supply either the serial number of the storage system or the authentication information for the storage depending on which HA configuration description you are using.
6. The Change HA Configuration Desc. panel opens displaying the current parameters.
7. Make the changes needed and press Enter to return you to the Work with HA Configuration Descriptions screen.

As a command sequence type in the following:

```
CHGHACFGD CLUSTER(cluster-name) NAME(configuration-name) TYPE(*HYSSTG|*STGCTL) SUBTYPE(*DS|*CSM) STGDEV(storage device-name)
```

to make the changes to an HA configuration description to the cluster.

The HA configuration description has been changed. To verify the parameters of the description, use the Display HA Configuration Description (**DSPHACFGD**) command.

For additional information about the **CHGHACFGD** command and specific fields consult the F1 help or visit the [CHGHACFGD](#) page.

Removing an HA configuration description

Using the Remove HA Configuration Description (**RMVHACFGD**) command to delete an HA configuration description

The Remove HA Configuration Description command removes an HA configuration description. This may be necessary if creating a new copy description or moving to a new storage environment.

The Remove HA Configuration Description screen can be accessed by using:

- The Work with Cluster (**WRKCLU**) command menu. Select option 11, Work with HA Config Desc., and use option 4, Remove to go to the Remove HA Configuration Desc. panel.
- Type the **WRKHACFGD** command to open the Work with HA Config Desc screen. Locate the HA configuration description you want to remove and use option 4, Remove, to open the Remove HA Configuration Desc. panel.
- Entering the **RMVHACFGD** command.

To remove an HA configuration description using the **RMVHACFGD** screen, follow these steps:

1. Type **RMVHACFGD** on the command line and press Enter.
2. On the Remove HA Configuration Desc. (**RMVHACFGD**) panel, enter the name of the cluster to add the HA configuration description to, or enter * to indicate the current cluster.
3. Type a name of the HA configuration description in the Configuration name field.
4. In the Configuration type field, enter the type of configuration description.
5. Press Enter.

The PowerHA description configuration is removed and will not appear in the list of available description configurations on the **WRKHACFGD** screen.

As a command sequence type in the following:

```
RMVHACFGD CLUSTER(cluster-name) NAME(configuration-name) TYPE(*HYSSTG|*STGCTL)
```

to remove a HA configuration description to the cluster.

For additional information about the **RMVHACFGD** command and specific fields consult the **F1** help or visit the [RMVHACFGD](#) page.

Managing PowerHA policies

Manage and maintain PowerHA policies for your cluster

PowerHA policies control specific behaviors related to clustering and HA environments.

With instances of any PowerHA policy type in place on a system in a PowerHA cluster environment, users can manage policies with the following commands:

- work with available PowerHA policies and policy instances using the [Work with HA Policy \(WRKHAPCY\) command](#). This command provides access to the other command screens in this list through selection options.
- display the policy contents using the [Display High Availability \(HA\) Policy \(DSPHAPCY\) command](#).
- change the policy values using the [Change High Availability \(HA\) Policy \(CHGHAPCY\) command](#).
- save a policies or instances of a policy type with the [Save High Availability \(HA\) Policy \(SAVHAPCY\) command](#).
- remove the policy with the [Remove High Availability \(HA\) Policy \(RMVHAPCY\) command](#).
- restore a policy instance or many policy instances with the [Restore High Availability \(HA\) Policy \(RSTHAPCY\) command](#).

Work with PowerHA policies

The Work with High Availability (HA) Policies (**WRKHAPCY**) command is used to display and work with HA policies.

In the Work with HA Policies screen you can perform many of the management functions that you could perform in the command line. In addition to the familiar add, change, display, or remove commands associated with other PowerHA topics, users can examine the policy definition of a particular policy, save, and restore individual policies.

The Work with HA Policies command screen opens showing the category and names of the High Availability (HA) policies arranged by category and name. The number of defined policy instances are listed, along with the supported command options available to users. Further information can be found by typing the option 12 in front of a HA policy name and pressing Enter. This opens a second Work with HA Policies screen that contains more details about the individual instances of the HA policy and additional command options.

To use the WRKHAPCY command from the command line, type:

```
WRKHAPCY PCY(QCST_AD_CREATE)
```

and press Enter.

This example opens the Work with HA Policies screen and displays the policy name and number of defined instances of that policy.

For additional information about the **WRKHAPCY** command consult the F1 Help or the [WRKHAPCY](#) page in the Knowledge Center.

Displaying a PowerHA policy

The Display HA Policy (**DSPHAPCY**) command shows the current properties of a PowerHA policy.

The Display HA Policy (**DSPHAPCY**) command displays a PowerHA policy. This information is useful to determine the current qualifiers and values that policy instances manage.

The Display HA Policy command screen can be accessed by:

- using the Work with Cluster (**WRKCLU**) command menu. Select option 12, Work with HA policies. Press Enter to open the Work with HA Policies panel. Locate an HA policy group or policy instance and type 12, Work with and press Enter to show the current list of policies and qualifiers. In the Option space, type 5, Display in front of the policy instance and press Enter.
- entering the **WRKHAPCY** command that opens the Work with HA Policies screen. Locate an HA policy group or policy instance and type 12, Work with and press Enter to show the current list of policies and qualifiers. In the Option space, type 5, Display in front of the policy instance and press Enter.
- typing the **DSPHAPCY** command and pressing Enter.

To display an HA policy from the Work with Cluster (**WRKCLU**) command menu, follow these steps:

1. At the Work with Cluster (**WRKCLU**) command menu select option 12 Work with HA policies. Press Enter to go to the Work with HA Policies screen.
2. On the Work with HA policies screen, locate the particular policy group or policy instance to display and type 12 Work with as the option. Press Enter to open the Work with Policy panel.

The Work with Policy panel shows a list of all defined policies for that policy type.

3. To obtain information about a specific HA policy instance, type 5, Display next to the policy you want to display.

The detailed information about the policy will display on the Display HA Policy screen.

To display the information about an HA policy using a command, for example, the QCST_AD_CREATE policy, enter

```
DSPHAPCY PCY(QCST_AD_CREATE)
```

in command line. This will display the policy information for currently defined instances of the QCST_AD_CREATE policy. To display specific instances of a policy, for example all instances of the QCST_AD_CREATE policy for the CRG policy domain, enter into the command line:

```
DSPHAPCY PCY(*ALL) PCYMN(*CRG)
```

Verify that the entries in the HA policy are configured correctly. If changes are required, they can be made with the **CHGHAPCY** command.

For details about the **DSPHAPCY** or **CHGHAPCY** commands and specific fields, consult the F1 Help or visit the [DSPHAPCY](#) and [CHGHAPCY](#) pages.

Changing a PowerHA policy

Make modifications to a PowerHA policy using the Change HA Policy (**CHGHAPCY**) command

The Change HA Policy (**CHGHAPCY**) command can be used to make changes to currently defined HA policies to reflect changes to the PowerHA environment. **CHGHAPCY** only changes the policy value of an individual instance of PowerHA policy.

The Change HA Policy command screen can be accessed by:

- using the Work with Cluster (**WRKCLU**) command menu. Select option 12, Work with HA policies. Press Enter to open the Work with HA Policies panel. Locate an HA policy group or policy instance and type 12, Work with and press Enter to show the current list of policies and qualifiers. In the Option space, type 2, Change in front of the policy you want to change the qualifier and value of. Press Enter to display the Change HA Policy screen.
- entering the **WRKHAPCY** command that opens the Work with HA Policies screen. Locate an HA policy group or policy instance and type 12, Work with and press Enter to show the current list of policies and qualifiers. In the Option space, type 2, Change in front of the policy instance you want to change the qualifier and value of. Press Enter to display the Change HA Policy screen.
- typing the **CHGHAPCY** command and pressing F4 to open the Change HA Policy (**CHGHAPCY**) screen.

To change an HA policy from the Work with Cluster (**WRKCLU**) command menu, follow these steps:

1. At the Work with Cluster (**WRKCLU**) command menu select option 12 Work with HA policies. Press Enter to go to the Work with HA Policies screen.
2. On the Work with HA policies screen, locate the particular policy group or policy instance to display and type 12 Work with as the option. Press Enter to open the Work with Policy panel.

The Work with Policy panel shows a list of all defined policies for that policy type.

3. To change a specific HA policy instance, type 2, Change next to the policy you want to display.
4. Make the appropriate changes to the PowerHA policy and press Enter.

After pressing Enter, you return to the Work with HA Policies screen. A message informs you of the change and how many policies are correctly functioning.

To change a specific instance of the QHA_COMM_STRICT_CERT_CHECK policy using the **CHGHAPCY** command you enter:

```
CHGHAPCY PCY(QHA_COMM_STRICT_CERT_CHECK) PCYDMN(*NONE) QUAL('cfgd(test1)') VALUE(*NO)
```

This example changes the value of the instance of the QHA_COMM_STRICT_CERT_CHECK PowerHA policy using the configuration description test1 as a qualifier to *NO, indicating that the strict usage of certificates in the cluster is not required.

Verify that the entries in the HA policy are changed correctly using the **DSPHAPCY** command.

For details about the **CHGHAPCY** or **DSPHAPCY** commands and specific fields, consult the F1 Help or visit the [CHGHAPCY](#) and [DSPHAPCY](#) pages.

Saving PowerHA policies

Use the Save HA Policy (**SAVHAPCY**) command to save instances of a PowerHA policy

The Save High Availability (HA) Policy (**SAVHAPCY**) command is used to save HA policies. Users can save all HA policies or specific policy groups and instances.

Policy information is saved in comma separated value (CSV) format in an integrated file system (IFS) file on the local cluster node.

The Save HA Policy command screen can be accessed by:

- using the Work with Cluster (**WRKCLU**) command menu. Select option 12, Work with HA policies. Press Enter to open the Work with HA Policies screen. Locate an HA policy name and type 9, Save and press Enter to open the Save HA Policy (**SAVHAPCY**) screen.
- entering the **WRKHAPCY** command that opens the Work with HA Policies screen. Locate an HA policy name and type 9, Save and press Enter to open the Save HA Policy (**SAVHAPCY**) screen.
- typing the **SAVHAPCY** command and pressing F4 to open the Save HA Policy (**SAVHAPCY**) screen.

Steps 1 and 2 demonstrate how to save an HA policy from the Work with HA Policies (**WRKHAPCY**) command menu.

1. On the **WRKHAPCY** command screen, locate an HA policy name and type 9, Save and press Enter.

The Save HA Policy (**SAVHAPCY**) screen opens with the Policy name, Policy domain, and Policy qualifier fields populated with the selected HA policy name and *ALL.

2. In the Policy file field, enter the path and the name of the file to contain the saved HA policy and press Enter.

All instances of that PowerHA policy are saved to the file name provided.

Steps 3, 4, and 5 show how to save individual instances of a PowerHA policy from the Work with HA Policies (**WRKHAPCY**) command menu.

3. On the **WRKHAPCY** command screen, locate an HA policy name and type 12, Work with, and press Enter.

The Work with HA Policies screen opens containing a list of all the individual instances of the selected PowerHA policy.

4. Locate the HA policy instance to save and type option 9, Save next to the policy name. Press Enter.

The Save HA Policy (**SAVHAPCY**) screen opens with the Policy name, Policy domain, and Policy qualifier fields populated with the selected HA policy name and the respective domain and specific qualifier values the policy instance controls.

5. In the Policy file field, enter the path and the name of the file to contain the saved HA policy instance and press Enter.

The individual instance of that PowerHA policy is saved to the file name provided.

To save the information of all PowerHA policies using a command, enter

```
SAVHAPCY PCYFILE('/home/public/test.csv')
```

to store the settings information of all instances of all PowerHA policies in the cluster to a file called `test.csv`.

Save individual instances of specified policies to a file by entering:

```
SAVHAPCY PCYFILE('/home/public/test1.csv') PCY(QCST_CRG_CANCEL_FAILOVER) QUAL('SCOPE(*SITE)')
```

This saves all instances of the `QCST_CRG_CANCEL_FAILOVER` policy with the qualifier scope of ***SITE** to a file called `test1.csv`.

Verify that the entries in the HA policy are saved correctly in the save file. The CSV formatted file can be used with the Restore HA Policy (**RSTHAPCY**) command to restore saved policies to a cluster.

For details about the **SAVHAPCY** command or specific fields, consult the F1 Help or visit the [SAVHAPCY](#) page.

Restoring PowerHA policies

Use the Restore HA Policy (**RSTHAPCY**) command to restore PowerHA policy groups or instances of a policy to a cluster

The Restore High Availability (HA) Policy (**RSTHAPCY**) command is used to restore HA policies that have been previously saved with the Save HA Policy (**SAVHAPCY**) command.

If a policy is being restored over an existing policy in the cluster, the existing policy value is replaced with the value in the policy file. If a policy is being restored as new, the policy is added as a new policy to the cluster.

The Restore HA Policy command screen can be accessed by:

- using the Work with Cluster (**WRKCLU**) command menu. Select option 12, Work with HA policies. Press Enter to open the Work with HA Policies screen. Locate an HA policy name and type 10, Restore and press Enter to open the Restore HA Policy (**RSTHAPCY**) screen.
- entering the **WRKHAPCY** command that opens the Work with HA Policies screen. Locate an HA policy name and type 10, Restore and press Enter to open the Restore HA Policy (**RSTHAPCY**) screen.
- typing the **RSTHAPCY** command and pressing F4 to open the Restore HA Policy (**RSTHAPCY**) screen.

Steps 1, 2, and 3 demonstrate how to restore an HA policy from the Work with HA Policies (**WRKHAPCY**) command menu.

1. On the **WRKHAPCY** command screen, locate an HA policy name and type 10, Restore and press Enter.
The Restore HA Policy (**RSTHAPCY**) screen opens with the Policy name, Saved policy domain, and Policy qualifier fields populated with the selected HA policy name and *ALL.
2. Specify whether the HA policy or policies are restored to the same policy domain in which they were saved or if they will be restored to another policy domain. Enter either:
 - a policy domain name: the name of the policy domain the HA policies will restore to, or
 - *SAVPCYDMN: to specify that all policies are to be restored in the same policy domain from which they were saved.

Steps 3, 4, and 5 show how to save individual instances of a PowerHA policy from the Work with HA Policies (**WRKHAPCY**) command menu.

3. In the Policy file field, enter the path and the name of the file to contain the saved HA policy and press Enter.
All instances of that PowerHA policy are restored from the file name provided.
4. On the **WRKHAPCY** command screen, locate an HA policy name and type 12, Work with, and press Enter.
The Work with HA Policies screen opens containing a list of all the individual instances of the selected PowerHA policy.
5. Locate the HA policy instance to save and type option 10, Restore next to the policy name. Press Enter.
The Restore HA Policy (**RSTHAPCY**) screen opens with the Policy name, Policy domain, the Restore to policy domain, and Policy qualifier fields populated with the selected HA policy name and the respective domain and specific qualifier values the policy instance controls.
6. In the Policy file field, enter the path and the name of the file that contains the saved HA policy instance to restore and press Enter.
The individual instance of that PowerHA policy is saved to the file name provided.

To restore the information of all PowerHA policies using a command, enter:

```
RSTHAPCY PCYFILE('/home/public/Policy/pcy_cf.csv')
```

to restore policies to the cluster from the file `pcy_cf.csv`.

Restore an instance of a specified policy by entering:

```
RSTHAPCY PCYFILE('/home/public/test1.csv') PCY(QCST_CRG_CANCEL_FAILOVER) QUAL('SCOPE(*SITE)')
```

to restore from the file `test1.csv`, instances of the `QCST_CRG_CANCEL_FAILOVER` PowerHA policy with the qualifier **SCOPE** of ***SITE**.

Verify that the entries in the HA policy have been restored correctly using the **DSPHAPCY** command.

Removing PowerHA policies

Remove a PowerHA policy with the Remove HA Policy (**RMVHAPCY**) command

The Remove HA policy (**RMVHAPCY**) command will remove a PowerHA policy that is no longer required in your PowerHA cluster environment.

The Remove HA Policy screen can be accessed by:

- using the Work with Cluster (**WRKCLU**) command menu. Select option 12, Work with HA policies. Press Enter to open the Work with HA Policies panel. Locate an HA policy group or policy instance and type 12, Work with and press Enter to show the current list of policies and qualifiers. In the Option space, type 4, Remove in front of the policy instance you want to remove. When performing a remove operation this way, PowerHA will open a Confirm Action panel asking you to confirm your removal command.
- entering the **WRKHAPCY** command that opens the Work with HA Policies screen. Locate the copy description and use option 12, Work with to show the current list of policies.

- typing the **RMVHAPCY** command and pressing F4.

To display an HA policy from the Work with Cluster (**WRKCLU**) command menu, follow these steps:

1. At the Work with Cluster (**WRKCLU**) command menu select option 12 Work with HA policies. Press Enter to go to the Work with HA Policies screen.
2. On the Work with HA policies screen, locate the particular policy to remove and type 12 Work with as the option. Press Enter to open the Work with Policy panel.

The Work with Policy panel shows a list of all defined policies for that policy type.

3. To remove a specific HA policy, type 4, Remove next to the policy you want to remove and press Enter.
4. A Confirm Action screen opens and displays the command to remove the selected policy.
 - Press F12 to cancel the request.
 - Press F16 (Shift+F4) to confirm the remove of the policy.

When confirmed, the HA policy will be removed and the user returned to the Work with HA Policies screen.

To remove a specific QCST_AD_RESTORE policy from your list of policies using the command line enter:

```
RMVHAPCY PCY(QCST_CRG_CANCEL_FAILOVER) PCYDMN(CRG) QUAL('SCOPE(*SITE)')
```

This will remove the policy managing the job descriptor resources in the HA domain of your PowerHA environment. When using the **RMVHAPCY** command through the command line, a Confirm Action panel does not open to request any confirmation.

For details about the **RMVHAPCY** command, consult the F1 Help or visit the [RMVHAPCY](#) page.

Managing geographic mirroring

Use the following information to help you manage geographic mirroring. Geographic mirroring is a sub-function of cross-site mirroring, where data is mirrored to independent disk pools in an IBM i environment.

Suspending geographic mirroring

If you need to end TCP communications for any reason, such as placing your system in restricted state, you should suspend geographic mirroring first. This action temporarily stops mirroring between systems in a high-availability solution.

When you suspend mirroring, any changes that are made on the production copy of the independent disk pool are not being transmitted to the mirror copy.

Note: When you resume geographic mirroring, synchronization is required between the production and mirror copies. If geographic mirroring was suspended without tracking, then full synchronization occurs. This can be a lengthy process.

Suspending geographic mirroring when IBM PowerHA for i is installed

To use the PowerHA graphical interface to suspend geographic mirroring, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to suspend geographic mirroring.
6. On the **Independent ASP Details** page, select **Suspend Mirroring** from the **Select Action** menu below the mirroring status.
7. Click **Yes** on the confirmation panel.

Suspending geographic mirroring with command line interface when IBM PowerHA SystemMirror for i licensed program is installed

To suspend a geographic mirroring by using the command line interface, issue the following command:

- CHGASPSSN SESSION(session-name) OPTION(*SUSPEND) where session-name is the name of your geographic mirroring session.

Suspending geographic mirroring when IBM PowerHA for i is not installed

To suspend geographic mirroring with IBM Navigator for i, follow these steps:

1. In IBM Navigator for i, expand **My Connections** (or your active environment).
2. Expand the system that owns the production copy of the geographically mirrored disk pool that you want to suspend.
3. Expand **Configuration and Service > Hardware > Disk Units > Disk Pools**.
4. Right-click the production copy of the **Disk Pool** you want to suspend and select **Geographic Mirroring > Suspend Geographic Mirroring**.

If you suspend with tracking, the system attempts to track changes that are made to those disk pools. This might shorten the length of the synchronization process by performing partial synchronization when you resume geographic mirroring. If tracking space is exhausted, then when you resume geographic mirroring, complete synchronization is required.

Note: If you suspend geographic mirroring without tracking changes, then when you resume geographic mirroring, a complete synchronization is required between the production and mirror copies. If you suspend geographic mirroring and you do track changes, then only a partial synchronization is required. Complete synchronization can be a lengthy process, anywhere from one to several hours, or longer. The length of time it takes to synchronize is dependent on the amount of data being synchronized, the speed of TCP/IP connections, and the number of communication lines that are used for geographic mirroring.

Related information

[Change ASP Session \(CHGASPSSN\) command](#)

[Change SVC Session \(CHGSVCSSN\) command](#)

Resuming geographic mirroring

If you suspend geographic mirroring, you must resume it in order to reactivate mirroring between the production and mirrored copies again.

Note: When you resume geographic mirroring, the production and mirror copies are synchronized concurrent with performing geographic mirroring. Synchronization can be a lengthy process. If a disk pool becoming unavailable interrupts synchronization, then synchronization continues from where it was interrupted when the disk pool becomes available again. When an interrupted synchronization is continued, the first message (CPI0985D) states that the synchronization is 0% complete.

Resuming geographic mirroring when PowerHA is installed

To use the PowerHA graphical interface to resume geographic mirroring, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to resume geographic mirroring.
6. On the **Independent ASP Details** page, select **Resume Mirroring** from the **Select Action** menu below the mirroring status.
7. Click **Yes** on the confirmation panel.

Resuming geographic mirroring with command line interface when IBM PowerHA SystemMirror for i licensed program is installed

To resume a geographic mirroring session by using the command line interface, issue the following command:

- CHGASPSSN SESSION(session-name) OPTION(*RESUME) where session-name is the name of your geographic mirroring session.

Resuming geographic mirroring when PowerHA is not installed

To resume geographic mirroring using PowerHA, follow these steps:

1. In IBM Navigator for i, expand **My Connections** (or your active environment).
2. Expand the system that owns the production copy of the disk pool for which you want to resume geographic mirroring.
3. Expand **Configuration and Service > Hardware > Disk Units > Disk Pools**.
4. Right-click the **Disk Pool** you want to resume and select **Geographic Mirroring > Resume Geographic Mirroring**.

Related information

[Change ASP Session \(CHGASPSSN\) command](#)

[Change SVC Session \(CHGSVCSSN\) command](#)

Detaching mirror copy

If you are using geographic mirroring and want to access the mirror copy to perform save operations or data mining, or to create reports, you must detach the mirror copy from the production copy.

Detaching the mirror copy when IBM PowerHA for i is installed

To use the PowerHA graphical interface to detach the mirror copy, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to detach the mirror copy.
6. On the **Independent ASP Details** page, select **Detach** from the context menu of the mirror copy.
7. Click **Yes** on the confirmation panel.

Detaching the geographic mirroring with command line interface when IBM PowerHA SystemMirror for i licensed program is installed

To detach geographic mirroring using the command line interface, issue the following command:

- CHGASPSSN SESSION(session-name) OPTION(*DETACH) where session-name is the name of your geographic mirroring session.

Detaching the mirror copy when IBM PowerHA for i is not installed

It is recommended, but not required, that you make the independent disk pool unavailable to ensure that the production copy is not altered while the detachment is being performed.

To detach the mirror copy by using IBM Navigator for i, follow these steps:

1. In IBM Navigator for i, expand **My Connections** (or your active environment).
2. Expand the system that owns the production copy of the disk pool from which you want to detach the mirror copy.
3. Expand **Configuration and Service > Hardware > Disk Units > Disk Pools**.

4. Right-click the production copy of the **Disk Pool** you want to detach and select **Geographic Mirroring > Detach Mirror Copy**.

If **Geographic Mirroring > Detach Mirror Copy** cannot be clicked because it is disabled, the mirror copy is not in sync with the production copy, Geographic mirroring must be resumed, the disk pool varied on, and production and mirror copies that are synchronized before the mirror copy can be detached.

Related information

[Change ASP Session \(CHGASPSN\) command](#)

[Change SVC Session \(CHGSVCSSN\) command](#)

Reattaching mirror copy

If you detached the mirror copy and have completed your work with the detached mirror copy, you must reattach the detached mirror copy to resume using geographic mirroring.

The detached mirror copy must be unavailable when you reattach it to the production copy.

Note: When you reattach the detached mirror copy, as of V6R1, there is the option to detach with tracking, which only requires a partial synchronization on reattach. Changes that are made on the Production Copy will be applied to the Mirror Copy, and all changes that are made on the Detached Mirror copy will be overwritten with the contents from the Production Copy.

Reattaching the mirror copy when IBM PowerHA SystemMirror for i licensed program is installed

To use the PowerHA graphical interface to reattach the mirror copy, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to reattach the mirror copy.
6. On the **Independent ASP Details** page, select **Reattach** from the context menu of the mirror copy.
7. Click **Yes** on the confirmation panel.

Reattaching geographic mirroring with command line interface when IBM PowerHA SystemMirror for i licensed program is installed

To reattach geographic mirroring using the command line interface, issue the following command:

- `CHGASPSN SESSION(session-name) OPTION(*REATTACH)` where `session-name` is the name of your geographic mirroring session.

Reattaching the mirror copy when IBM PowerHA SystemMirror for i is not installed

To reattach the mirror copy using IBM Navigator for i, follow these steps:

1. In IBM Navigator for i, expand **My Connections** (or your active environment).
2. Expand the system that owns the production copy of the disk pool to which you want to reattach the detached mirror copy.
3. Expand **Configuration and Service > Hardware > Disk Units > Disk Pools**.
4. Right-click the production copy of the **Disk Pool** you want to reattach and select **Geographic Mirroring > Reattach Mirror Copy**.

Related information

[Change ASP Session \(CHGASPSN\) command](#)

[Change SVC Session \(CHGSVCSSN\) command](#)

Deconfiguring geographic mirroring

If you no longer want the capability to use geographic mirroring for a specific disk pool or disk pool group, you can select to **Deconfigure Geographic Mirroring**. If you deconfigure geographic mirroring, the system stops geographic mirroring and deletes the mirror copy of the disk pools on the nodes in the mirror copy site.

The disk pool must be offline to deconfigure geographic mirroring and the cluster resource group (CRG) must have a status of INACTIVE.

Deconfigure geographic mirroring when IBM PowerHA SystemMirror for i licensed program is installed

To use the IBM Navigator for i deconfigure geographic mirroring with, follow these steps:

1. In a web browser, enter **http://mysystem:2001**, where **mysystem** is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to deconfigure geographic mirroring.
6. On the **Independent ASP Details** page, select **Deconfigure Geographic Mirroring...** from the **Select Action** menu below the mirroring status.
7. Click **OK** on the confirmation panel.

Deconfiguring geographic mirroring with command line interface when IBM PowerHA SystemMirror for i licensed program is installed

To deconfigure geographic mirroring using the command line interface, issue the following command:

- CHGASPSSN SESSION(session-name) OPTION(*DELETE) where session-name is the name of the independent ASP to deconfigure geographic mirroring on.

Deconfigure geographic mirroring when IBM PowerHA SystemMirror for i licensed program is not installed

1. In IBM Navigator for i, expand **My Connections** (or your active environment).
2. Expand the system that you want to examine, **Configuration and Service > Hardware > Disk Units > Disk Pools**.
3. Right-click the production copy of the **Disk Pool** you want to deconfigure and select **Geographic Mirroring>Deconfigure Geographic Mirroring**.
4. Update your cluster configuration, as follows:
 - a) Remove the nodes that are associated with the mirror copy from the device cluster resource group (CRG) recovery domain.
 - b) Remove the site name and data port IP addresses from the remaining nodes in the cluster.

Related tasks

Removing nodes

You might need to remove a node from a cluster if you are performing an upgrade of that node or if the node no longer needs to participate in the IBM i high-availability environment.

Related information

[Change ASP Session \(CHGASPSSN\) command](#)

Changing geographic mirroring properties

All geographic mirroring properties can be changed when the production copy of the independent disk pool is varied off. The Synchronization Priority property can be also changed with the independent disk pool is Available and geographic mirroring is Suspended.

Changing geographic mirroring properties with IBM PowerHA SystemMirror for i licensed program

To change the geographic mirroring properties by using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to change the geographic mirroring properties.
6. On the **Independent ASP Details** page, select **Mirroring Properties...** from the **Select Action** menu below the mirroring status.
7. On the **Properties** page, click **Edit**.
8. Make changes to the properties and click **Save**.

Changing geographic mirroring with command line interface when IBM PowerHA SystemMirror for i licensed program is installed

To change the geographic mirroring session using the command line interface, issue the following command:

- `CHGASPSN SESSION(session-name) OPTION(*CHGATTR)` where `session-name` is the name of your geographic mirroring Mirror session. You need to list the attributes that should be changed.

Changing geographic mirroring properties with IBM Navigator for i

To change the geographic mirroring properties by using IBM Navigator for i, follow these steps:

1. In IBM Navigator for i, expand **My Connections** (or your active environment).
2. Expand the system that owns the production copy of the geographically mirrored disk pool associated with the geographic mirror session for which you want to edit the attributes, **Configuration and Service > Hardware > Disk Units > Disk Pools**.
3. Right-click the production copy of the **Disk Pool** for which you want to edit the attributes and select **Sessions > Open**.
4. Right-click the production copy of the **Session** for which you want to edit the attributes and select **Properties**. To change an associated copy description, select the copy description and click **Edit**.

Managing Metro Mirror

In PowerHA environment that use IBM System Storage Metro Mirror technology, you must configure a metro mirroring session between the IBM i systems and the external disk units with Metro Mirror configured. From the system, you can manage these sessions.

Suspending Metro Mirror

You might need to suspend Metro Mirror sessions to perform maintenance on the system.

Suspending metro mirroring with PowerHA graphical interface

To suspend a Metro Mirror session by using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.

4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to suspend Metro Mirror.
6. On the **Independent ASP Details** page, select **Suspend Mirroring** from the **Select Action** menu below the mirroring status.
7. Click **Yes** on the confirmation panel.

Suspending metro mirroring with command-line interface

To suspend a Metro Mirror session by using the command-line interface, use the following command:

- CHGASPSSN SESSION(session-name) OPTION(*SUSPEND) where session-name is the name of your DS8000 Metro Mirror session.
- CHGSVCSSN SESSION(session-name) OPTION(*SUSPEND) where session-name is the name of your SAN Volume Controller(SVC) Metro Mirror session.

Related information

[Change ASP Session \(CHGASPSSN\) command](#)

[Change SVC Session \(CHGSVCSSN\) command](#)

Resuming Metro Mirror sessions

After you have completed routine operations, such as performing maintenance on your system, you need to resume a suspended Metro Mirror session to re-enable high availability.

Resuming metro mirroring with PowerHA graphical interface

To resume a Metro Mirror session by using the PowerHA graphical interface, follow these steps:

1. In a web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to resume geographic mirroring.
6. On the **Independent ASP Details** page, select **Resume Mirroring** from the **Select Action** menu below the mirroring status.
7. Click **Yes** on the confirmation panel.

Resuming metro mirroring with command-line interface

To resume a Metro Mirror session by using the command-line interface, issue the following command:

- CHGASPSSN SESSION(session-name) OPTION(*RESUME) where session-name is the name of your DS8000 Metro Mirror session.
- CHGSVCSSN SESSION(session-name) OPTION(*RESUME) where session-name is the name of your SAN Volume Controller (SVC) Metro Mirror session.

Related information

[Change ASP Session \(CHGASPSSN\) command](#)

[Change SVC Session \(CHGSVCSSN\) command](#)

Detaching Metro Mirror copy

If you are using Metro Mirror and want to access the target copy to perform save operations or data mining, you must detach the target copy from the source copy.

Detaching the mirror copy with PowerHA graphical interface

To use the PowerHA graphical interface to detach the mirror copy, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to detach the mirror copy.
6. On the **Independent ASP Details** page, select **Detach** from the context menu of the mirror copy.
7. Click **Yes** on the confirmation panel.

Detaching the mirror copy with command-line interface

To detach the mirror copy using the command-line interface, issue the following command:

- `CHGASPSSN SESSION(session-name) OPTION(*DETACH)` where `session-name` is the name of your DS8000 Metro Mirror session.
- `CHGSVCSSN SESSION(session-name) OPTION(*DETACH)` where `session-name` is the name of your SAN Volume Controller (SVC) Metro Mirror session.

Reattaching Metro Mirror

If you detached the target copy and have completed your work with the detached target copy, you must reattach the detached target copy to resume using Metro Mirroring.

The detached target copy must be unavailable when you reattach it to the source copy.

Note: When you reattach the detached mirror copy, as of V6R1, there is the option to detach with tracking, which only requires a partial synchronization on reattach. Changes that are made on the source copy will be applied to the target copy, and all changes that are made on the detached target copy will be overwritten with the contents from the source copy.

Reattaching the target copy with PowerHA graphical interface

To use the PowerHA graphical interface to reattach the mirror copy, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to reattach the mirror copy.
6. On the **Independent ASP Details** page, select **Reattach** from the context menu of the mirror copy.
7. Click **Yes** on the confirmation panel.

Reattaching the target copy with command-line interface

To reattach metro mirroring using the command-line interface, use the following command:

- `CHGASPSSN SESSION(session-name) OPTION(*REATTACH)` where `session-name` is the name of your DS8000 Metro Mirror session.
- `CHGSVCSSN SESSION(session-name) OPTION(*REATTACH)` where `session-name` is the name of your SAN Volume Controller (SVC) Metro Mirror session.

Ending Metro Mirror

You can end the Metro Mirror session to no longer use the session for high availability and disaster recovery.

Ending the Metro Mirror session does not deconfigure metro mirroring on the IBM System Storage, it just removes our connection to the IBM System Storage.

Ending metro mirroring with PowerHA graphical interface

To end a Metro Mirror session by using the PowerHA graphical interface, follow these steps:

1. In a web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to delete the Metro Mirror session.
6. On the **Independent ASP Details** page, select **Deconfigure Mirroring...** from the **Select Action** menu below the mirroring status.
7. Click **OK** on the confirmation panel.

Ending metro mirroring with command-line interface

To end a Metro Mirror session by using the command-line interface, use the following command:

- `ENDASPSSN SESSION(session-name)` where `session-name` is the name of your DS8000 Metro Mirror session.
- `ENDSVCSSN SESSION(session-name)` where `session-name` is the name of your SAN Volume Controller (SVC) Metro Mirror session.

Deleting metro mirroring configuration

Ending the Metro Mirror session does not deconfigure metro mirroring on the IBM System Storage, it just removes the connection to the IBM System Storage.

To deconfigure Metro Mirror on the IBM i, you should deconfigure the IBM System Storage external storage units. For information about Metro Mirror on IBM System Storage DS8000, see [Copy Services in the IBM](#)

[System Storage DS8000 Information Center](#)



Related information

[End ASP Session \(ENDASPSSN\) command](#)

[End SVC Session \(ENDSVCSSN\) command](#)

Displaying or changing Metro Mirror properties

Display information about a metro mirroring session to change the associated copy descriptions.

Displaying or changing metro mirroring properties with PowerHA licensed program is installed

To change metro mirroring properties by using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to change the metro mirroring properties.
6. On the **Independent ASP Details** page, select **Properties...** from the context menu of either the production or mirror copy.
7. On the **Properties** page, click **Edit** in the Advanced section.
8. Make changes to the properties and click **Save**.

Managing Global Mirror

In IBM i high availability environment that use IBM System Storage Global Mirror technology, you must configure a global mirroring session between the IBM i systems and the external disk units with Global Mirror configured. From the system, you can manage these sessions.

Suspending Global Mirror

You might need to suspend Global Mirror sessions to perform maintenance on the system.

Suspending Global Mirror with PowerHA graphical interface

To suspend a Global Mirror session by using the PowerHA graphical interface, follow these steps:

1. In a web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to suspend Global Mirror.
6. On the **Independent ASP Details** page, select **Suspend Mirroring** from the **Select Action** menu below the mirroring status.
7. Click **Yes** on the confirmation panel.

Suspending Global Mirror with command-line interface

To suspend a Global Mirror session by using the command-line interface, use the following command:

- `CHGASPSN SESSION(session-name) OPTION(*SUSPEND)` where `session-name` is the name of your DS8000 Global Mirror session.
- `CHGSVCSSN SESSION(session-name) OPTION(*SUSPEND)` where `session-name` is the name of your SAN Volume Controller (SVC) Global Mirror session.

Resuming Global Mirror

After you have completed routine operations, such as performing maintenance on your system, you need to resume a suspended Global Mirror session to re-enable high availability.

Resuming Global Mirror with PowerHA graphical interface

To resume a suspended global mirroring session by using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to resume Global Mirror.
6. On the **Independent ASP Details** page, select **Resume Mirroring** from the **Select Action** menu below the mirroring status.
7. Click **Yes** on the confirmation panel.

Resuming Global Mirror with command-line interface

To resume a suspended global mirroring session using the command-line interface, use this command:

- `CHGASPSN SESSION(session-name) OPTION(*RESUME)` where `session-name` is the name of your DS8000 Global Mirror session.

- CHGSVCSSN SESSION(session-name) OPTION(*RESUME) where session-name is the name of your SAN Volume Controller(SVC) Global Mirror session.

Detaching Global Mirror copy

If you are using Global Mirror and want to access the target copy to perform save operations or data mining, you must detach the target copy from the source copy.

Detaching the mirror copy with PowerHA graphical interface

To use the PowerHA graphical interface to detach the mirror copy, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to detach the mirror copy.
6. On the **Independent ASP Details** page, select **Detach** from the context menu of the mirror copy.
7. Click **Yes** on the confirmation panel.

Detaching the mirror copy with command-line interface

To detach the mirror copy using the command-line interface, use the following command:

- CHGASPSSN SESSION(session-name) OPTION(*DETACH) where session-name is the name of your DS8000 Global Mirror session.
- CHGSVCSSN SESSION(session-name) OPTION(*DETACH) where session-name is the name of your SAN Volume Controller (SVC) Global Mirror session.

Reattaching Global Mirror

If you detached the target copy and have completed your work with the detached target copy, you must reattach the detached target copy to resume using Global Mirror.

The detached target copy must be unavailable when you reattach it to the source copy.

Note: When you reattach the detached mirror copy, as of V6R1, there is the option to detach with tracking, which only requires a partial synchronization on reattach. Changes that are made on the source copy will be applied to the target copy, and all changes that are made on the detached target copy will be overwritten with the contents from the source copy.

Reattaching the target copy when PowerHA graphical interface

To use the PowerHA graphical interface to reattach the mirror copy, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to reattach the mirror copy.
6. On the **Independent ASP Details** page, select **Reattach** from the context menu of the mirror copy.
7. Click **Yes** on the confirmation panel.

Reattaching the target copy with command-line interface

To reattach mirror copy using the command-line interface, use the following command:

- CHGASPSSN SESSION(session-name) OPTION(*REATTACH) where session-name is the name of your DS8000 Global Mirror session.

- CHGSVCSSN SESSION(session-name) OPTION(*REATTACH) where session-name is the name of your SAN Volume Controller (SVC) Global Mirror session.

Ending Global Mirror

You can end the Global Mirror session to no longer use the session for high availability and disaster recovery.

Ending global mirroring with PowerHA graphical interface

To delete a global mirroring session by using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to delete the Global Mirror session.
6. On the **Independent ASP Details** page, select **Deconfigure Mirroring...** from the **Select Action** menu below the mirroring status.
7. Click **OK** on the confirmation panel.

Ending global mirroring with the command-line interface


To end a Global Mirror session using the command-line interface, use this command:

- ENDASPCSSN SESSION(session-name) where session-name is the name of your DS8000 Metro Mirror session.
- ENDSVCSSN SESSION(session-name) where session-name is the name of your SAN Volume Controller (SVC) Metro Mirror session.

Deleting Global Mirror configuration

Ending the Global Mirror session does not deconfigure global mirroring on the IBM System Storage, it just removes the connection to the IBM System Storage.

To deconfigure Global Mirror on the IBM i, you should deconfigure the IBMSystem Storage external storage units. For information about Global Mirror on IBMSystem StorageDS8000, see [Copy Services in](#)

[the IBM System Storage DS8000 Information Center](#) .

Changing Global Mirror session properties

Display information about a Global Mirror session to change the associated copy descriptions.

Displaying or changing Global Mirror properties with PowerHA graphical interface

To change Global Mirror properties by using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the IBM Navigator for i window
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to change Global Mirror properties.
6. On the **Independent ASP Details** page, select **Properties...** from the context menu of either the production or mirror copy.
7. On the **Properties** page, click **Edit** in the Advanced section.
8. Make changes to the properties and click **Save**.

Managing switched logical units (LUNs)

Switched logical units are independent disk pools created from logical units created in an IBM System Storage that have been configured as part of a device cluster resource group (CRG).

Ownership of data and applications that stored in a switched logical unit can be switched to other systems that have been defined in the device CRG. Switched disk technology provides high availability during planned and some unplanned outages.

Related concepts

[PowerHA supported storage servers](#)

IBM System Storage provides enhanced storage capabilities.

Making switched logical units (LUNs) available and unavailable

You can select an independent disk pool to make it unavailable or available. You cannot access any of the disk units or objects in the independent disk pool or its corresponding database until it is made available again. The pool can be made available again on the same system or another system in the recovery domain of the cluster resource group.

An independent disk pool can be made unavailable by varying it off. Access to any of the disk units or objects in the independent disk pool or its corresponding database are not available, until they are varied on. The pool can be made available on the same system or another system in the recovery domain of the cluster resource group.

Managing the FlashCopy technology

FlashCopy is an IBM System Storage technology that allows you to take a point-in-time copy of external disk units. In PowerHA solutions that use Metro Mirror or Global Mirror, The FlashCopy technology can be used for backup window reduction by taking a copy of data that then can be backed up to media. To use the FlashCopy technology, a session must be created between the system and the external storage units.

Updating a FlashCopy session

You can update a FlashCopy session when you are performing resynchronization of FlashCopy volumes on your IBM System Storage external storage units. Resynchronization allows you to make a copy without recopying the entire volume. This process is only possible with a persistent relationship, whereby the storage unit continually tracks updates to the source and target volumes. With persistent relationships, the relationship between the source and target volumes is maintained after the background copy has completed. The FlashCopy session that is created on the IBM i provides a means to manage and monitor activity that is related to the FlashCopy session on the IBM System Storage units.

Updating a FlashCopy when IBM PowerHA SystemMirror for i licensed program is installed

To update a FlashCopy session by using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool that has a FlashCopy you want to update.
6. On the **Independent ASP Details** page, select **Update** from the context menu of the FlashCopy you want to update.
7. Click **Yes** on the confirmation panel.

Reattaching a FlashCopy session

Reattach a FlashCopy session.

Reattaching a FlashCopy when IBM PowerHA SystemMirror for i licensed program is installed

To reattach (enable) a FlashCopy session by using the IBM PowerHA for i graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the IBM Navigator for i window
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for that has a FlashCopy you want to reattach (enable).
6. On the **Independent ASP Details** page, select **Enable** from the context menu of the FlashCopy you want to reattach (enable).

Reattaching a FlashCopy when IBM PowerHA SystemMirror for i licensed program is not installed

To reattach a FlashCopy session by using the Configuration and Service graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Select **Configuration and Service** from your IBM Navigator for i window.
4. Select **Disk Pools**.
5. Select the disk pool that is associated with the session that you want to reattach.
6. From the **Select Actions** menu, select **Sessions**.
7. Select the session that you want to reattach.
8. From the **Select Actions** menu, select **Reattach FlashCopy**.

Detaching a FlashCopy session

You can detach the target volumes from the source for a selected FlashCopy session.

Detaching FlashCopy when IBM PowerHA for i is installed

To detach (disable) a FlashCopy session by using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool that has a FlashCopy you want to detach (disable).
6. On the **Independent ASP Details** page, select **Disable** from the context menu of the FlashCopy you want to detach (disable).
7. Click **Yes** on the confirmation panel.

Deleting a FlashCopy session

Delete a FlashCopy session.

Deleting a FlashCopy when IBM PowerHA SystemMirror for i licensed program is installed

To delete a FlashCopy session by using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.

2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool that has a FlashCopy you want to delete.
6. On the **Independent ASP Details** page, select **Delete** from the context menu of the FlashCopy you want to delete.
7. Click **Yes** on the confirmation panel.

Restoring data from a FlashCopy session

After a FlashCopy session has been completed on the IBM System Storage units, you can restore that data from target volume to the source volume in the event of an outage at the source copy of data. To do this, you need to reverse the FlashCopy session that is created on IBM i. However, reversing the session copies data from the target back to the source and returns the source to it an earlier version.

If the FlashCopy source is a member of a cluster resource group, then reverse FlashCopy are not allowed unless the original FlashCopy was performed as a *NOCOPY flash. Full-copy reverse flashes are not supported when the original FlashCopy source is a member of a cluster resource group.



Attention: Reversing a FlashCopy session backs out the changes that are made on the source copy by copying the target's data back to the source. This returns the source to that earlier point in time.

To reverse a FlashCopy session, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Select **Configuration and Service** from your IBM Navigator for i window.
4. Select **Disk Pools**.
5. Select the disk pool of the source copy.
6. From the **Select Actions** menu, select **Open Sessions**.
7. Select the session.
8. From the **Select Actions** menu, select **Reverse FlashCopy**.

Changing FlashCopy properties

Display information about a FlashCopy session to change the associated copy descriptions.

Changing FlashCopy properties when IBM PowerHA SystemMirror for i licensed program is installed

To change information about a FlashCopy session by using the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the IBM Navigator for i window.
4. On the **PowerHA** page, click **Independent ASPs**.
5. On the **Independent ASPs** page, select **Details...** from the context menu of the independent disk pool for which you want to change FlashCopy properties.
6. On the **Independent ASP Details** page, select **Properties...** from the context menu FlashCopy.
7. On the **Properties** page, click **Edit**.
8. Make changes to the properties and click **Save**.

Managing DS8000 Full System HyperSwap

DS8000 Full System HyperSwap is a full system solution that allows logical units that are mirrored between two IBM System Storage DS8000 units to be switched between without an outage, providing a minimal impact high availability solution.

To use DS8000 Full System HyperSwap requires IBM PowerHA for i Express Edition be installed, with a valid license key.

Displaying HyperSwap Status

To display the current HyperSwap Status for the system, use the DSPHYSSTS command. The output from the command indicates the current direction and status of HyperSwap replication.

Related information

[Display HyperSwap Status \(DSPHYSSTS\) command](#)

Perform a Planned HyperSwap

To perform a planned HyperSwap from the primary IBM System Storage unit to the secondary, and start replication in the reverse direction, use the Change HyperSwap Status (CHGHYSSTS) command with the *SWAP option.

Related information

[Change HyperSwap Status \(CHGHYSSTS\) command](#)

Suspend HyperSwap Replication

To suspend HyperSwap replication for the system, use the Change HyperSwap Status (CHGHYSSTS) command with the *STOP option.

Note: When replication is suspended, a HyperSwap cannot be performed. Hourly messages are posted to the QSYSOPR message queue.

Related information

[Change HyperSwap Status \(CHGHYSSTS\) command](#)

Resume HyperSwap Replication

To resume HyperSwap replication that was suspended, use the Change HyperSwap Status (CHGHYSSTS) command with the *START option.

Note: The system is able to perform a HyperSwap as soon as the resynchronization has completed.

Related information

[Change HyperSwap Status \(CHGHYSSTS\) command](#)

Recovering from an unplanned HyperSwap Failover

In the event of an unplanned HyperSwap failover, the system will automatically switch to use the secondary IBM System Storage device as the primary. When the issue that caused the HyperSwap failover has been resolved, the system indicates that there are two primary IBM System Storage devices. The replication direction is indicated on the Display HyperSwap Status (DSPHYSSTS) command output.

To recover perform the following steps:

1. Issue a Change HyperSwap Status (CHGHYSSTS) command with the *START option to resume replication.
2. Display the HyperSwap Status (DSPHYSSTS) command waiting until all units are fully synchronized.
3. To switch back to the original primary, issue a Change HyperSwap Status (CHGHYSSTS) command with the *SWAP option.

Related information

[Change HyperSwap Status \(CHGHYSSTS\) command](#)

[Display HyperSwap Status \(DSPHYSSTS\) command](#)

Managing DS8000 HyperSwap with independent auxiliary storage pools (IASPs)

DS8000 HyperSwap with IASPs is typically used with PowerHA LUN switching technology to provide coverage for planned and unplanned storage and server outages, and can also be used with live partition mobility to further minimize downtime for planned server outages.

The following table contains the recommended technology to use for several outages and scenarios, both planned and unplanned.

Outage type	Recovery type
Planned IBM i OS upgrade or maintenance	CRG switchover. For more information, see “CRG Planned switchover with HyperSwap and LUN switching” on page 176.
Planned server firmware upgrade or outage	LPM switch or CRG switchover. For more information, see “CRG Planned switchover with HyperSwap and LUN switching” on page 176 or “Live partition mobility switch with HyperSwap and affinity” on page 178.
Planned storage upgrade or outage	HyperSwap switchover. For more information, see “HyperSwap planned switchover of SYSBAS” on page 176, “HyperSwap planned switchover of independent auxiliary storage pool (IASP)” on page 176, or “HyperSwap planned switchover with HyperSwap and LUN switching” on page 176.
Planned server hardware upgrade or outage	CRG switchover. For more information, see “CRG Planned switchover with HyperSwap and LUN switching” on page 176.
Unplanned IBM i OS outage	CRG failover. For more information, see “CRG Failover HyperSwap and LUN switching” on page 177.
Unplanned server firmware outage	CRG failover. For more information, see “CRG Failover HyperSwap and LUN switching” on page 177.
Unplanned storage outage	HyperSwap failover. For more information, see “HyperSwap failover with HyperSwap and LUN switching” on page 177.
Unplanned server hardware outage	CRG failover. For more information, see “CRG Failover HyperSwap and LUN switching” on page 177.

Displaying HyperSwap Status

To display the current HyperSwap Status for the system, use the DSPHYSSTS command. The output from the command indicates the current direction and status of HyperSwap replication.

Related information

[Display HyperSwap Status \(DSPHYSSTS\) command](#)

HyperSwap planned switchover of SYSBAS

To do a planned switchover of SYSBAS, enter the following command:

```
CHGHYSSTS OPTION(*SWAP) NODE(*) ASPDEV(*SYSBAS)
```

This command switches primary access of the SYSBAS from one DS8000 storage server to the other DS8000 storage server in the HyperSwap relationship. If an IASP exists on the system, its HyperSwap relationship stays the same.

HyperSwap planned switchover of independent auxiliary storage pool (IASP)

To do a planned switchover of an IASP, enter the following command:

```
CHGHYSSTS OPTION(*SWAP) NODE(*) ASPDEV(<iasp-name>)
```

This command switches primary access of the asp-name IASP from one DS8000 storage server to the other DS8000 storage server in the HyperSwap relationship. It does not change the relationship for SYSBAS or any other IASPs, which exist on the system.

HyperSwap planned switchover with HyperSwap and LUN switching

In the case of a planned outage of a storage server, a HyperSwap switchover can be initiated, resulting in near-zero downtime from a user perspective. In the following figure on the left, all disk units in IASP1 are metro mirrored to the second DS8000 to create a HyperSwap relationship. In addition to being configured for HyperSwap, IASP1 is also configured for LUN level switching to a second IBM i partition, named IBM i B in the figure.



For the HyperSwap switchover to be initiated, the following conditions must be met.

1. All disk units in the ASP group must be configured in a HyperSwap relationship.
2. All of the HyperSwap relationships in the ASP group must be fully synchronized.
3. All of the HyperSwap relationships in the ASP group must be going the same direction (some disk units in the ASP group cannot have one DS8000 as the primary while other disk units have the other DS8000 as primary).

When the user wants to initiate a planned HyperSwap switchover of IASP1, the following command must be entered:

```
CHGHYSSTS OPTION(*SWAP) NODE(*) ASPDEV(*ALL)
```

After you enter the command, the primary access for IASP1 and SYSBAS will be the second DS8000, as shown in the figure on the right side.

CRG Planned switchover with HyperSwap and LUN switching

In the case of a planned outage of the system server, a CRG switchover can be initiated.

The following conditions must be met before the switchover can be initiated.


1. Both DS8000s must be accessible by PowerHA through DSCLI.
2. None of the HyperSwap relationships in the IASP can have two primary volumes. This is shown by XXXX for the copy status when a Display HyperSwap Status or Work with HyperSwap Status command is run for the IASP.




The following command must be entered to perform the CRG switchover.

```
CHGCRGPRI CLUSTER(<cluster-name>) CRG(<CRG-name>)
```




The  in the figure shows the configuration after IASP1 is varied on for IBM i B. If affinity was defined by the ADDHACFGD command and the affinity is not correct after the CRG switchover, then PowerHA will

also initiate a HyperSwap switchover of IASP1, shown by  in the figure.

When a HyperSwap switchover cannot be completed, the CRG switchover completes and a diagnostic message is sent indicating that the HyperSwap switchover failed. Examples of why the HyperSwap switchover could not complete are HyperSwap is being suspended, or is not fully synchronized.

HyperSwap failover with HyperSwap and LUN switching

In the case of an unplanned outage of a storage server, a HyperSwap failover is initiated, resulting in near-zero downtime from a user perspective. The figure on the left shows a HyperSwap relationship between all of the disk units in SYSBAS A and SYSBAS B, and in IASP1. The primary access for SYSBAS A and IASP1 is DS8000 M, and the primary access for SYSBAS B is DS8000 N. In addition to being configured for HyperSwap, IASP1 is also configured for LUN level switching to a second IBM i partition, named IBM i B in the figure.

In order for the HyperSwap failover to be initiated, the following conditions must be met.

1. All disk units in the ASP group must be configured in a HyperSwap relationship.
2. All of the HyperSwap relationships in the ASP group must be fully synchronized.
3. All of the HyperSwap relationships in the ASP group must be going the same direction (some disk units in the ASP group can't have one DS8000 as the primary while other disk units have the other DS8000 as primary).



After the HyperSwap failover completes, the primary access for IASP1 and SYSBAS will be the second DS8000, as shown in the figure on the right side. If the HyperSwap failover cannot be completed, the IASP goes into DASD attention.

After the failover occurs and the failed DS8000 comes back online, the HyperSwap relationship must be restarted by entering the following command.

```
CHGHYSSTS OPTION(*START) NODE(*) ASPDEV(*ALL)
```

This will restart replication for all ASP devices. The Display HyperSwap Status and Work with HyperSwap Status commands can then be used to monitor the resynchronization process. After resynchronization is completed, a HyperSwap switchover can be initiated if desired.

Two primary case

After a HyperSwap failover and until the HyperSwap relationship is restarted, each DS8000s reports that it is the primary. If the mirroring relationship is not restarted before the IBM i partition is IPLed, the IPL will fail, requiring the user to manually correct the condition from the DS8000.

The two primary case can be determined in one of the following ways.

1. By entering the **DSPHYSSTS** command, the HyperSwap copy status is shown as XXXX.
2. Hourly messages are posted to QSYSOPR indicating there is a problem with the HyperSwap relationship.

CRG Failover HyperSwap and LUN switching


In the case of a planned outage of the system server, a CRG failover can be initiated.

The following conditions must be met before the failover is initiated.

1. Both DS8000s must be accessible by PowerHA through DSCLI.

2. None of the HyperSwap relationships in the IASP can have two primary volumes. This is shown by **XXXX** for the copy status when a Display HyperSwap Status or Work with HyperSwap Status command is run for the IASP.



In the figure, first the CRG failover takes place, resulting in , where IASP1 is now varied on to IBM i B. If affinity was defined by the **ADDHACFGD** command and the affinity is not correct after the CRG failover,

then PowerHA will also initiate a HyperSwap switchover of IASP1, shown in .

If a HyperSwap switchover cannot be completed due to some reason such as HyperSwap being suspended or not fully synchronized, the CRG failover completes and a diagnostic message is sent indicating that the HyperSwap switchover failed.

Live partition mobility switch with HyperSwap and affinity

Live partition mobility (LPM) allows a running IBM i partition to migrate from one physical server to another server with near-zero downtime. HyperSwap can be combined with live partition mobility to move the data access to the DS8000 storage server with the most affinity to the physical server hosting the IBM i partition. LPM switch with HyperSwap and affinity is illustrated in the figure.



When HyperSwap affinity is configured by using the Add HA Configuration Description (**ADDHACFGD**) command, the HyperSwap switchover can automatically occur when a live partition mobility switch occurs and the current primary DS8000 does not have affinity to the new server.

DS8000 HyperSwap IASP with FlashCopy

In addition to integrating HyperSwap with PowerHA logical unit (LUN) level switching, HyperSwap can also be integrated with the PowerHA FlashCopy technology.

The following rules apply to a configuration that has both HyperSwap and FlashCopy

1. A FlashCopy source can be a HyperSwap IASP (as identified by two storage hosts and LUN ranges that are defined in the source copy description).
2. A FlashCopy target cannot be a HyperSwap IASP. It might have only one storage host and LUN range defined in the target copy description.

Depending on which storage server is currently the primary DS8000 in the HyperSwap relationship, the FlashCopy target might be in the secondary DS8000. In this case, the FlashCopy target gets the data, which is in the target DS8000. If the HyperSwap relationship is not active, then the FlashCopy is stale data as well.

Troubleshooting your high availability solution

After you have configured your IBM i high-availability solution, you may encounter problems with different technologies, including clusters and cross-site mirroring.

Troubleshooting clusters

Find error recovery solutions for problems that are specific to clusters.

At times, it may appear that the cluster is not working properly. This topic covers information about problems that you may encounter with clusters.

Determine if a cluster problem exists

Start here to diagnose your cluster problems.

At times, it may seem that your cluster is not operating correctly. When you think a problem exists, you can use the following to help determine if a problem exists and the nature of the problem.

- **Use the PowerHA graphical interface to examine the cluster.**

To use the PowerHA graphical interface, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** in the IBM Navigator for i window
4. Verify if the status icons indicate a problem and investigate further if needed.

- **Determine if clustering is active on your system.**

To determine if cluster resource services are active, look for the two jobs - QCSTCTL and QCSTCRGM - in the list of system jobs. If these jobs are active, then cluster resource services are active. You can use the Work Management function in IBM Navigator for i or in IBM Navigator for i to View jobs or use the **WRKACTJOB (Work with Active Jobs)** command to do this. You can also use the **DSPCLUINF (Display Cluster Information)** command to view status information for the cluster.

- Additional jobs for cluster resource services may also be active. Cluster jobs provides information about how cluster resource services jobs are formatted.

- **Determine the cause of a CPFBB26 message.**

```
Message . . . . : Cluster Resource Services not active or not responding.  
Cause . . . . . : Cluster Resource Services is either not active or cannot  
respond to this request because a resource is unavailable or damaged.
```

This error can mean that either the CRG job is not active or the cluster is not active. Use the **DSPCLUINF (Display Cluster Information)** command to determine if the node is active. If the node is not active, start the cluster node. If it is active, you should also check the CRG to determine whether the CRG has problems.

Look for the CRG job in the list of system jobs. You can use the Work Management function in IBM Navigator for i or in IBM Navigator for i to View jobs or use the **WRKACTJOB (Work with Active Jobs)** command to do this. You can also use the **DSPCRGINF (Display CRG Information)** command to view status information for the specific CRG, by specifying the CRG name in the command. If the CRG job is not active, look for the CRG job log to determine the cause of why it was ended. Once the problem is fixed, you could restart the CRG job with **CHGCLURCY (Change Cluster Recovery) command** or by ending and restarting cluster on that node.

- **Look for messages indicating a problem.**

- Ensure that you can review all messages associated with a cluster command, by selecting F10, which toggles between "Include detailed messages" and "Exclude detailed messages". Select to include all detailed messages and review them to determine if other actions are necessary.
- Look for inquiry messages in QSYSOPR that are waiting for a response.
- Look for error messages in QSYSOPR that indicate a cluster problem. Generally, these are in the CPFBB00 to CPFBBFF range.
- Display the history log (**DSPLOG CL** command) for messages that indicate a cluster problem. Generally, these are in the CPFBB00 to CPFBBFF range.

- **Look at job logs for the cluster jobs for severe errors.**

These jobs are initially set with a logging level at (4 0 *SECLVL) so that you can see the necessary error messages. You should ensure that these jobs and the exit program jobs have the logging level set appropriately. If clustering is not active, you can still look for spool files for the cluster jobs and exit program jobs.

- **If you suspect some kind of hang condition, look at call stacks of cluster jobs.**

Determine if there is any program in some kind of DEQW (dequeue wait). If so, check the call stack of each thread and see if any of them have getSpecialMsg in the call stack.

- **Check for cluster vertical Licensed Internal Code (VLIC) logs entries.**

These log entries have a 4800 major code.

- **Use NETSTAT command to determine if there are any abnormalities in your communications environment.**

NETSTAT returns information about the status of Internet Protocol network routes, interfaces, TCP connections, and UDP ports on your system.

- Use Netstat Option 1 (Work with TCP/IP interface status) to ensure that the IP addresses chosen to be used for clustering show an 'Active' status. Also ensure that the LOOPBACK address (127.0.0.1) is also active.
- Use **NETSTAT** Option 3 (Work with TCP/IP Connection Status) to display the port numbers (F14). Local port 5550 should be in a 'Listen' state. This port must be opened using the **STRTCPSVR *INETD** command evidenced by the existence of a QTOGINTD (User QTCP) job in the Active Jobs list. If clustering is started on a node, local port 5551 must be opened and be in a '*UDP' state. If clustering is not started, port 5551 must not be opened or it will, in fact, prevent the successful start of clustering on the subject node.
- Use **PING** to verify if there is a communications problem. If you try to start a cluster node and there is a communications problem, you may receive an internal clustering error (CPFBB46). However, **PING** does not work between IPv4 and IPv6 addresses, or if a firewall is blocking it.

Gathering recovery information for a cluster

You can use the **Work with Cluster (WRKCLU)** command to collect information for a complete picture of your cluster. This information can be used to aid in error resolution.

The **Work with Cluster (WRKCLU)** command is used to display and to work with cluster nodes and objects. When you run this command, the Work with Cluster display is shown. In addition to displaying nodes in a cluster and cluster information, you can use this command to view cluster information and to gather data about your cluster

To gather error recovery information, complete these steps:

1. On a character-based interface, type **WRKCLU OPTION(OPTION)**. You can specify the following options to indicate with which cluster status information you want to work with.

- *SELECT**

Display the Work with Cluster menu.

- *CLUINF**

Display cluster information.

- *CFG**

Display the performance and configuration parameters for the cluster.

- *NODE**

Display the Work with Cluster Nodes panel which is a list of nodes in the cluster.

- *DEVDMN**

Display the Work with Device Domains panel which is a list of device domains in the cluster.

- *CRG**

Display the Work with Cluster Resource Groups panel which is a list of cluster resource groups in the cluster.

- *ADMDMN**

Display the Work with Administrative Domains panel which is a list of administrative domains in the cluster.

***SERVICE**

Gathers related trace and debug information for all cluster resource service jobs in the cluster. This information is written to a file with a member for each cluster resource service job. Use this option only when directed by your service provider. It will display a prompt panel for the **Dump Cluster Trace (DMPCLUTRC)**.

Common cluster problems

Lists some of the most common problems that can occur in a cluster, as well as ways to avoid and recover from them.

The following common problems are easily avoidable or easily correctable.

Use the PowerHA graphical interface to identify current or potential problems.

To use the PowerHA graphical interface to identify a current problem, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where *mysystem* is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click on **PowerHA** in the IBM Navigator for iwindow.
4. On the **PowerHA** page, verify if any status icons indicate a problem and investigate further if needed.
- 5.

To use the PowerHA graphical interface to identify a potential problem, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where *mysystem* is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click on **PowerHA** in the IBM Navigator for iwindow.
4. On the PowerHA, select **Check Requirements...** from the **Select Action** menu next to the cluster name.
5. Fix any problems identified on the **Check Requirements** page. Some problems can be fixed immediately by selecting Fix from the context menu of the identified problem.

You cannot start or restart a cluster node

This situation is typically due to some problem with your communications environment. To avoid this situation, ensure that your network attributes are set correctly, including the loopback address, INETD settings, ALWADDCLU attribute, and the IP addresses for cluster communications.

- The ALWADDCLU network attribute must be appropriately set on the target node if trying to start a remote node. This should be set to either *ANY or *RQSAUT depending on your environment.
- The IP addresses chosen to be used for clustering locally and on the target node must show an *Active* status.
- The LOOPBACK address (127.0.0.1) locally and on the target node must also be active.
- Verify that network routing is active by attempting to PING using the IP addresses used for clustering on the local and remote nodes; however, PING does not work between IPv4 and IPv6 addresses, or if a firewall is blocking it. If any cluster node uses an IPv4 address, than every node in the cluster needs to have an active IPv4 address (not necessarily configured as a Cluster IP address) that can route to and send TCP packets to that address. Also, if any cluster node uses an IPv6 address, than every node in the cluster needs to have an active IPv6 address (not necessarily configured as a Cluster IP address) that can route to and send TCP packets to that address.
- INETD must be active on the target node. When INETD is active, port 5550 on the target node should be in a *Listen* state. See INETD server for information about starting the INETD server.
- Prior to attempting to start a node, port 5551 on the node to be started must not be opened or it will, in fact, prevent the successful start of clustering on the subject node.

You end up with several, disjointed one-node clusters

This can occur when the node being started cannot communicate with the rest of the cluster nodes. Check the communications paths.

The response from exit programs is slow.

A common cause for this situation is incorrect setting for the job description used by the exit program. The MAXACT parameter may be set too low so that, for example, only one instance of the exit program can be active at any point in time. It is recommended that this be set to *NOMAX.

Performance in general seems to be slow.

There are several common causes for this symptom.

- The most likely cause is heavy communications traffic over a shared communications line.
- Another likely cause is an inconsistency between the communications environment and the cluster message tuning parameters. You can use the [Retrieve Cluster Resource Services Information \(QcstRetrieveCRSInfo\) API](#) to view the current settings of the tuning parameters and the [Change Cluster Resource Services \(QcstChgClusterResourceServices\) API](#) to change the settings. Cluster performance may be degraded under default cluster tuning parameter settings if using old adapter hardware. The adapter hardware types included in the definition of *old* are 2617, 2618, 2619, 2626, and 2665. In this case, setting of the *Performance class* tuning parameter to *Normal* is desired.
- If all the nodes of a cluster are on a local LAN or have routing capabilities which can handle Maximum Transmission Unit (MTU) packet sizes of greater than 1,464 bytes throughout the network routes, large cluster message transfers (greater than 1,536K bytes) can be greatly speeded up by increasing the cluster tuning parameter value for *Message fragment size* to better match the route MTUs.

You cannot use any of the function of the new release.

If you attempt to use new release function and you see error message CPFBB70, then your current cluster version is still set at the prior version level. You must upgrade all cluster nodes to the new release level and then use the adjust cluster version interface to set the current cluster version to the new level. See [Adjust the cluster version of a cluster for more information](#).

You cannot add a node to a device domain or access the System i Navigator cluster management interface.

To access the System i Navigator cluster management interface, or to use switchable devices, you must have IBM i Option 41, HA Switchable Resources installed on your system. You must also have a valid license key for this option.

You applied a cluster PTF and it does not seem to be working.

You should ensure that you have completed the following tasks after applying the PTF:

1. [End the cluster](#)
2. Signoff then signon

The old program is still active in the activation group until the activation group is destroyed. All of the cluster code (even the cluster APIs) run in the default activation group.

3. [Start the cluster](#)

Most cluster PTFs require clustering to be ended and restarted on the node to activate the PTF.

CEE0200 appears in the exit program joblog.

On this error message, the from module is QLEPM and the from procedure is Q_LE_leBdyPeilog. Any program that the exit program invokes must run in either *CALLER or a named activation group. You must change your exit program or the program in error to correct this condition.

CPD000D followed by CPF0001 appears in the cluster resource services joblog.

When you receive this error message, make sure the QMLTTHDACN system value is set to either 1 or 2.

Cluster appears hung.

Make sure cluster resource group exit programs are outstanding. To check the exit program, use the **WRKACTJOB (Work with Active Jobs)** command, then look in the Function column for the presence of PGM-QCSTCRGEXT.

Partition errors

Certain cluster conditions are easily corrected. If a cluster partition has occurred, you can learn how to recover. This topic also tells you how to avoid a cluster partition and gives you an example of how to merge partitions back together.

A cluster partition occurs in a cluster whenever contact is lost between one or more nodes in the cluster and a failure of the lost nodes cannot be confirmed. This is not to be confused with a partition in a logical partition (LPAR) environment.

If you receive error message CPFBB20 in either the history log (QHST) or the QCSTCTL joblog, a cluster partition has occurred and you need to know how to recover. The following example shows a cluster partition that involves a cluster made up of four nodes: A, B, C, and D. The example shows a loss of communication between cluster nodes B and C has occurred, which results in the cluster dividing into two cluster partitions. Before the cluster partition occurred, there were four cluster resource groups, which can be of any type, called CRG A, CRG B, CRG C, and CRG D. The example shows the recovery domain of each cluster resource group.

Table 41. Example of a recovery domain during a cluster partition

Node A	Node B	x	Node C	Node D
CRG A (backup1)	CRG A (primary)			
	CRG B (primary)		CRG B (backup1)	
	CRG C (primary)		CRG C (backup1)	CRG C (backup2)
CRG D (backup2)	CRG D (primary)		CRG D (backup1)	
Partition 1			Partition 2	

A cluster may partition if the maximum transmission unit (MTU) at any point in the communication path is less than the cluster communications tuneable parameter, message fragment size. MTU for a cluster IP address can be verified by using the **Work with TCP/IP Network Status (WRKTCPSTS)** command on the subject node. The MTU must also be verified at each step along the entire communication path. If the MTU is less than the message fragment size, either raise the MTU of the path or lower the message fragment size. You can use the Retrieve Cluster Resource Services Information (QcstRetrieveCRSInfo) API to view the current settings of the tuning parameters and the Change Cluster Resource Services (QcstChgClusterResourceServices) API to change the settings.

Once the cause of the cluster partition condition has been corrected, the cluster will detect the re-established communication link and issue the message CPFBB21 in either the history log (QHST) or the QCSTCTL joblog. This informs the operator that the cluster has recovered from the cluster partition. Be aware that once the cluster partition condition has been corrected, it may be a few minutes before the cluster merges back together.

Determining primary and secondary cluster partitions

In order to determine the types of cluster resource group actions that you can take within a cluster partition, you need to know whether the partition is a primary or a secondary cluster partition. When a partition is detected, each partition is designated as a primary or secondary partition for each cluster resource group defined in the cluster.

For primary-backup model, the primary partition contains the node that has the current node role of primary. All other partitions are secondary. The primary partition may not be the same for all cluster resource groups.

A peer model has the following partition rules:

- If the recovery domain nodes are fully contained within one partition, it will be the primary partition.
- If the recovery domain nodes span a partition, there will be no primary partition. Both partitions will be secondary partitions.
- If the cluster resource group is active and there are no peer nodes in the given partition, the cluster resource group will be ended in that partition.
- Operational changes are allowed in a secondary partition as long as the restrictions for the operational changes are met.
- No configuration changes are allowed in a secondary partition.

The restrictions for each Cluster Resource Group API are:

Cluster Resource Group API	Allowed in primary partition	Allowed in secondary partitions
Add Node to Recovery Domain	X	
Add CRG Device Entry		
Change Cluster Resource Group	X	
Change CRG Device Entry	X	X
Create Cluster Resource Group		
Delete Cluster Resource Group	X	X
Distribute Information	X	X
End Cluster Resource Group ¹	X	
Initiate Switchover	X	
List Cluster Resource Groups	X	X
List Cluster Resource Group Information	X	X
Remove Node from Recovery Domain	X	
Remove CRG Device Entry	X	
Start Cluster Resource Group ¹	X	
Note:		
1. Allowed in all partitions for peer cluster resource groups, but only affects the partition running the API.		

By applying these restrictions, cluster resource groups can be synchronized when the cluster is no longer partitioned. As nodes rejoin the cluster from a partitioned status, the version of the cluster resource group in the primary partition is copied to nodes from a secondary partition.

When merging two secondary partitions for peer model, the partition which has cluster resource group with status of Active will be declared the winner. If both partitions have the same status for cluster resource group, the partition which contains the first node listed in the cluster resource group recovery domain will be declared the winner. The version of the cluster resource group in the winning partition will be copied to nodes in another partition.

When a partition is detected, the Add Cluster Node Entry, Adjust Cluster Version, and the Create Cluster API cannot be run in any of the partitions. The Add Device Domain Entry API can only be run if none of the nodes in the device domain are partitioned. All of the other Cluster Control APIs may be run in any partition. However, the action performed by the API takes affect only in the partition running the API.

Changing partitioned nodes to failed

Sometimes, a partitioned condition is reported when there really was a node outage. This can occur when cluster resource service loses communications with one or more nodes, but cannot detect if the nodes are still operational. When this condition occurs, a simple mechanism exists for you to indicate that the node has failed.



Attention: When you tell cluster resource services that a node has failed, it makes recovery from the partition state simpler. However, changing the node status to failed when, in fact, the node is still active and a true partition has occurred should not be done. Doing so can cause a node in more than one partition to assume the primary role for a cluster resource group. When two nodes think they are the primary node, data such as files or databases can become disjoint or corrupted if multiple nodes are each independently making changes to their copies of files. In addition, the two partitions cannot be merged back together when a node in each partition has been assigned the primary role.

When the status of a node is changed to Failed, the role of nodes in the recovery domain for each cluster resource group in the partition may be reordered. The node being set to Failed will be assigned as the last backup. If multiple nodes have failed and their status needs to be changed, the order in which the nodes are changed will affect the final order of the recovery domain's backup nodes. If the failed node was the primary node for a CRG, the first active backup will be reassigned as the new primary node.

When cluster resource services has lost communications with a node but cannot detect if the node is still operational, a cluster node will have a status of **Not communicating**. You may need to change the status of the node from **Not communicating** to **Failed**. You will then be able to restart the node.

To change the status of a node from **Not communicating** to **Failed**, follow these steps:

1. In a Web browser, enter `http://mysystem:2001`, where `mysystem` is the host name of the system.
2. Log on to the system with your user profile and password.
3. Click **PowerHA** from the IBM Navigator for i window.
4. On the **PowerHA** page, click on **Cluster Nodes** .
5. On the **Cluster Nodes** page, select **Change Status** from the context menu of the node for which you want to change its status.
6. Click **Yes** on the confirmation panel.

Related information

[Change Cluster Node \(CHGCLUNODE\) command](#)

[Change Cluster Node Entry \(QcstChangeClusterNodeEntry\) API](#)

Partitioned cluster administrative domains

Consider the following information when working with partitioned cluster administrative domains.

If a cluster administrative domain is partitioned, changes continue to be synchronized among the active nodes in each partition. When the nodes are merged back together again, the cluster administrative domain propagates all changes made in every partition so that the resources are consistent within the active domain. There are several considerations regarding the merge processing for a cluster administrative domain:

- If all partitions were active and changes were made to the same resource in different partitions, the most recent change is applied to resource on all nodes during the merge. The most recent change is determined by using Coordinated Universal Time (UTC) from each node where a change initiated.
- If all partitions were inactive, the global values for each resource are resolved based on the last change made while any partition was active. The actual application of these changes to the monitored resources does not happen until the peer CRG that represents the cluster administrative domain is started.
- If some partitions were active and some were inactive prior to the merge, the global values representing changes made in the active partitions are propagated to the inactive partitions. The inactive partitions are then started, causing any pending changes made on the nodes in the inactive partitions to propagate to the merged domain.

Tips: Cluster partitions

Use these tips for cluster partitions.

1. The rules for restricting operations within a partition are designed to make merging the partitions feasible. Without these restrictions, reconstructing the cluster requires extensive work.
2. If the nodes in the primary partition have been destroyed, special processing may be necessary in a secondary partition. The most common scenario that causes this condition is the loss of the site that made up the primary partition. Use the example in recovering from partition errors and assume that Partition 1 was destroyed. In this case, the primary node for Cluster Resource Groups B, C, and D must be located in Partition 2. The simplest recovery is to use Change Cluster Node Entry to set both Node A and Node B to failed. See changing partitioned nodes to failed for more information about how to do this. Recovery can also be achieved manually. In order to do this, perform these operations:
 - a) Remove Nodes A and B from the cluster in Partition 2. Partition 2 is now the cluster.
 - b) Establish any logical replication environments needed in the new cluster. IE. Start Cluster Resource Group API/CL command, and so on.

Since nodes have been removed from the cluster definition in Partition 2, an attempt to merge Partition 1 and Partition 2 will fail. In order to correct the mismatch in cluster definitions, run the Delete Cluster (`QcstDeleteCluster`) API on each node in Partition 1. Then add the nodes from Partition 1 to the cluster, and reestablish all the cluster resource group definitions, recovery domains, and logical replication. This requires a great deal of work and is also prone to errors. It is very important that you do this procedure only in a site loss situation.

3. Processing a start node operation is dependent on the status of the node that is being started:

The node either failed or an End Node operation ended the node:

- a) Cluster resource services is started on the node that is being added
- b) Cluster definition is copied from an active node in the cluster to the node that is being started.
- c) Any cluster resource group that has the node being started in the recovery domain is copied from an active node in the cluster to the node being started. No cluster resource groups are copied from the node that is being started to an active node in the cluster.

The node is a partitioned node:

- a) The cluster definition of an active node is compared to the cluster definition of the node that is being started. If the definitions are the same, the start will continue as a merge operation. If the definitions do not match, the merge will stop, and the user will need to intervene.
- b) If the merge continues, the node that is being started is set to an active status.
- c) Any cluster resource group that has the node being started in the recovery domain is copied from the primary partition of the cluster resource group to the secondary partition of the cluster resource group. Cluster resource groups may be copied from the node that is being started to nodes that are already active in the cluster.

Cluster recovery

Read about how to recover from other cluster failures that may occur.

Recovering from cluster job failures

Failure of a cluster resource services job is usually indicative of some other problem.

You should look for the job log associated with the failed job and look for messages that describe why it failed. Correct any error situations.

You can use the **Change Cluster Recovery (CHGCLURCY) command** to restart a cluster resource group job that was ended without having to end and restart clustering on a node.

1. CHGCLURCY CLUSTER(EXAMPLE) CRG(CRG1) NODE(NODE1) ACTION(*STRCRGJOB) This command will cause cluster resource group job, CRG1, on node NODE1 to be submitted. To start the cluster resource group job on NODE1 requires clustering to be active on NODE1.
2. Restart clustering on the node.

If you are using a IBM Business Partner cluster management product, refer to the documentation that came with the product.

Related information

[Change Cluster Recovery \(CHGCLURCY\) command](#)

Recovering a damaged cluster object

While it is unlikely you will ever experience a damaged object, it may be possible for cluster resource services objects to become damaged.

The system, if it is an active node, will attempt to recover from another active node in the cluster. The system will perform the following recovery steps:

For a damaged internal object

1. The node that has the damage ends.
2. If there is at least one other active node within the cluster, the damaged node will automatically restart itself and rejoin the cluster. The process of rejoining will correct the damaged situation.

For a damaged cluster resource group

1. The node that has a damaged CRG will fail any operation currently in process that is associated with that CRG. The system will then attempt to automatically recover the CRG from another active node.
2. If there is at least one active member in the recovery domain, the CRG recovery will work. Otherwise, the CRG job ends.

If the system cannot identify or reach any other active node, you will need to perform these recovery steps.

For a damaged internal object

You receive an internal clustering error (CPFBB46, CPFBB47, or CPFBB48).

1. End clustering for the node that contains the damage.
2. Restart clustering for the node that contains the damage. Do this from another active node in the cluster.
3. If Steps 1 and 2 do not solve the problem, remove the damaged node from the cluster.
4. Add the system back into the cluster and into the recovery domain for the appropriate cluster resource groups.

For a damaged cluster resource group

You receive an error stating that an object is damaged (CPF9804).

1. End clustering on the node that contains the damaged cluster resource group.
2. Delete the CRG by using the **DLTCRG** command.
3. If there is no other node active in the cluster that contains the CRG object, restore from media.
4. Start clustering on the node that contains the damaged cluster resource group. This can be done from any active node.
5. When you start clustering, the system resynchronizes all of the cluster resource groups. You may need to recreate the CRG if no other node in the cluster contains the CRG.

Recovering a cluster after a complete system loss

Use this information with the appropriate checklist in the *Recovering your system* topic for recovering your entire system after a complete system loss when your system loses power unexpectedly.

Scenario 1: Restoring to the same system

1. In order to prevent inconsistencies in the device domain information between the Licensed Internal Code and IBM i, it is recommended that you install the Licensed Internal Code by using option 3 (Install Licensed Internal Code and Recover Configuration).

Note: For the Install Licensed Internal Code and Recover Configuration operation to succeed, you must have the same disk units -- with exception of the load source disk unit if it has failed. You must also be recovering the same release.

2. After you have installed the Licensed Internal Code, follow the [Recovering Your Disk Configuration](#) procedure in the *Recovering your system* topic. These steps will help you avoid having to reconfigure the disk pools.
3. After you have recovered your system information and are ready to start clustering on the node you just recovered, you must start clustering from the active node. This will propagate the most current configuration information to the recovered node.

Scenario 2: Restoring to a different system

After you have recovered your system information and checked the job log to make sure that all objects have restored, you must perform the following steps to obtain the correct cluster device domain configuration.

1. From the node you just restored, delete the cluster.
2. From the active node, perform these steps:
 - a. Remove the recovered node from the cluster.
 - b. Add the recovered node back into the cluster.
 - c. Add the recovered node to the device domain.
 - d. Create the cluster resource group or add the node to the recovery domain.

Recovering a cluster after a disaster

In the case of a disaster where all your nodes are lost, you will need to reconfigure your cluster.

In order to prepare for such a scenario, it is recommended that you save your cluster configuration information and keep a hardcopy printout of that information.

Restoring a cluster from backup tapes

During normal operations, you should never restore from a backup tape.

This is only necessary when a disaster occurs and all nodes were lost in your cluster. If a disaster should occur, you recover by following your normal recovery procedures that you have put in place after you created your backup and recovery strategy.

Troubleshooting geographic mirroring

This information can help you solve problems related to geographic mirroring that you might encounter.

Geographic mirroring messages

Review the geographic mirroring message descriptions and recoveries to resolve your geographic mirroring problems.

0x00010259

Description: Operation failed because the system did not find the mirror copy.

Recovery: Not all the nodes in the device domain responded. Make sure that clustering is active. If necessary, start clusters on the node. See [“Starting nodes” on page 57](#) for details. Try the request again. If the problem persists, contact your technical support provider.

0x0001025A

Description: Not all of the disk pools in the disk pool group are geographically mirrored.

Recovery: If one disk pool in a disk pool group is geographically mirrored, all of the disk pools in the disk pool group must be geographically mirrored. Take one of the following actions:

1. Configure geographic mirroring for the disk pools which are not geographically mirrored.
2. Deconfigure geographic mirroring for the disk pools that are geographically mirrored.

0x00010265

Description: The detached mirrored copy is available.

Recovery: Make the detached mirrored copy unavailable and then try the reattach operation again.

0x00010380

Description: A disk unit is missing from the configuration of the mirror copy.

Recovery: Find or fix the missing disk unit in the mirror copy. Check the Product Activity Log on destination node. Reclaim IOP cache storage.

0x00011210

Description: The proposed secondary disk pool for the disk pool group is not geographically mirrored.

Recovery: If one disk pool in a disk pool group is geographically mirrored, all of the disk pools in the disk pool group must be geographically mirrored. You must configure geographic mirroring for the proposed secondary disk pool which is not geographically mirrored, either now or after completing this operation.

0x00011211

Description: Duplicate mirror copies exist.

Recovery: Check for locally mirrored disk units that may exist on two systems, Enterprise Storage Server® FlashCopy, or back level independent disk pool copies. See the Product Activity Log on the mirror copy node for more information. Eliminate duplication and try the request again. If the problem persists, contact your technical support provider, or see IBM i Technical Support for information about IBM support and services.

Troubleshooting Metro Mirror, Global Mirror, and FlashCopy

This information can help you solve problems that are related to Metro Mirror, Global Mirror, and FlashCopy mirroring that you might encounter.

For more troubleshooting ideas for Metro Mirror, Global Mirror and FlashCopy, check out the [IBM PowerHA SystemMirror for i wiki](#).

Troubleshooting HyperSwap

Find error recovery solutions for problems that are specific to clusters.

The following are HyperSwap messages and recommended recovery.

- **System fails to IPL with SRC A6005090**
 - Power down the System i and verify that the Metro Mirror replication on the IBM System Storage device is started and running in the correct direction for all logical units. Contact your next level of support if the problem persists.

Related information for Implementing high availability

Related reference

[PDF file for Implementing high availability](#)

You can view and print a PDF file of this information about implementing high availability.

Code license and disclaimer information

IBM grants you a nonexclusive copyright license to use all programming code examples from which you can generate similar function tailored to your own specific needs.

SUBJECT TO ANY STATUTORY WARRANTIES WHICH CANNOT BE EXCLUDED, IBM, ITS PROGRAM DEVELOPERS AND SUPPLIERS MAKE NO WARRANTIES OR CONDITIONS EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, REGARDING THE PROGRAM OR TECHNICAL SUPPORT, IF ANY.

UNDER NO CIRCUMSTANCES IS IBM, ITS PROGRAM DEVELOPERS OR SUPPLIERS LIABLE FOR ANY OF THE FOLLOWING, EVEN IF INFORMED OF THEIR POSSIBILITY:

1. LOSS OF, OR DAMAGE TO, DATA;
2. DIRECT, SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES, OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES; OR
3. LOST PROFITS, BUSINESS, REVENUE, GOODWILL, OR ANTICIPATED SAVINGS.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF DIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, SO SOME OR ALL OF THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU.

Notices

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

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

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

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

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

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

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

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

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

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

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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

COPYRIGHT LICENSE:

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

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. _enter the year or years_.

Programming interface information

This Implementing high availability publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM i.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., 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](http://www.ibm.com/legal/copytrade.shtml)" at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Other product and service names might be trademarks of IBM or other companies.

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.



Product Number: 5770-SS1