Redbooks

ibm.com/redbooks

IBM FlashSystem A9000 and A9000R Business Continuity Solutions

Bert Dufrasne

Francesco Anderloni

Roger Eriksson

Lisa Martinez

Storage

IBM

Redpaper

International Technical Support Organization

IBM FlashSystem A9000 and A9000R Business Continuity Solutions

February 2019

REDP-5401-03

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

Fourth Edition (February 2019)

This edition applies to FlashSystem A9000 and A9000R with system software Version 12.3.

Contents

Notices

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

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

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

Trademarks

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

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

AIX®
DS8000®
Global Technology Services®
HyperSwap®
IBM®
IBM FlashSystem®
IBM Spectrum™
IBM Spectrum Accelerate™
Jazz™
Redbooks®
Redpaper™
Redbooks (logo)  ®
System Storage®
XIV®

The following terms are trademarks of other companies:

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

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

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

Preface

IBM® FlashSystem A9000 and IBM FlashSystem® A9000R provide functions suited for various data protection scenarios that enable you to enhance your business continuance, disaster recovery, data migration, and backup solutions. These functions allow point-in-time copies, known as snapshots, and also include remote copy capabilities in either synchronous or asynchronous mode.

Furthermore, IBM Hyper-Scale Mobility enables a seamless migration of IBM FlashSystem A9000 or A9000R volumes to another with no interference to the host.

Starting with software level V12.1, the IBM HyperSwap® feature delivers always-on, high availability (HA) storage service for storage volumes in a production environment. Starting with version 12.2, asynchronous replication between the IBM XIV® Gen3 and FlashSystem A9000 or A9000R is supported.

Starting with Version 12.2.1, Hyper-Scale Mobility is enabled between XIV Gen3 and FlashSystem A9000 or A9000R.

Version 12.3 offers Multi-site replication solution that entails both High Availability (HA) and Disaster Recovery (DR) function by combining HyperSwap and Asynchronous replication to a third site.

This IBM Redpaper™ publication is intended for anyone who needs a detailed and practical understanding of the IBM FlashSystem A9000 and IBM FlashSystem A9000R replication and business continuity functions.

Authors

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

Bert Dufrasne is an IBM Certified Consulting IT Specialist and Project Leader for IBM System Storage® disk products at the International Technical Support Organization (ITSO). He has worked at IBM in various IT areas. He has authored many IBM Redbooks® publications, and has also developed and taught technical workshops. Before joining the ITSO, he worked for IBM Global Services as an Application Architect. He holds a Master's degree in Electrical Engineering.

Francesco Anderloni is an Infrastructure Specialist working for the IBM Global Technology Services® organization in IBM Italy. Since he joined IBM in 2015, he has been working in the Storage Management area, delivering IBM Storage solutions to clients in Italy and Europe. He is a member of the Young Technical Expert Council in IBM Italy. Francesco holds a Bachelor's Degree in Information Engineering and a Master's Degree in Computer Science, both from the University of Padova, Italy.

Roger Eriksson works at IBM Systems Lab Services Nordic, based in Stockholm, Sweden. He is a Senior Accredited IBM Product Service Professional. Roger has over 25 years of experience working on IBM servers and storage, including Enterprise and Midrange disk, NAS, SAN, IBM x86 and IBM Power. He has done consulting, proof of concepts and education, mainly with the Spectrum Accelerate and Spectrum Virtualize product line, since December 2008. He also works with the Swedish technical sales team for storage solutions

on a daily basis. Working with both clients and various IBM teams worldwide is a normal days work. He holds a Technical Collage Graduation in Mechanical Engineering.

Lisa Martinez has been working in the Washington Systems Center - Storage Team as a storage specialist since January 2012. Her focus has been with pre-sales support for IBM DS8000® and the IBM Spectrum™ Accelerate family of storage products (FlashSystem A9000 and A9000R, IBM XIV, and IBM Spectrum Accelerate™). She is also the lead instructor for FlashSystem A9000 and A9000R, XIV, and IBM Spectrum Accelerate customer-based workshops. Her prior experience includes roles as a storage architect in the Specialty Services Area in GTS and test architect in disk storage, focusing on system-level test for XIV for three years, and copy services for DS8000. Lisa holds degrees in Computer Science from New Mexico Highlands University and Electrical Engineering from the University of New Mexico.

Thanks to the authors of the previous edition:

Deepthi Anne
Mariya Atanasova
Matthew DiVito
Michael Gray
Andrew Greenfield
Detlef Helmbrecht
John Hyams
Peter Kalachev
Markus Oscheka
Bruce Spell
Stephen Solewin
Roey Yeshua
IBM

Special thanks to the following people for their contributions to this project:

Rivka Matosevich
Anat Bar-Natan-Kigel
Yossi Siles
IBM

Now you can become a published author, too

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

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

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us.

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

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

  ibm.com/redbooks

- Send your comments in an email:

  redbooks@us.ibm.com

- Mail your comments:

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

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

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

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

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

- Stay current on recent Redbooks publications with RSS Feeds:

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

1

Business Continuity functions

This chapter presents a high-level description of the business continuity functions available for IBM FlashSystem A9000 and A9000R.

The following concepts are described:

- Mirroring
- Hyperswap
- Multi-site HA/DR
- Migration
- Hyper-Scale Mobility

1.1 Mirroring

Mirroring creates a second set of consistent data at a secondary site, that can be used when there are problems with the production volumes. It can also be used for other purposes such as testing and backup on the secondary site using snapshots of consistent data.

Remote mirroring is independent of applications and operating systems, and does not require host-processor cycle usage.

1.1.1 Synchronous Mirror

Remote mirroring can be a synchronous copy solution whereby a write operation is completed onto both copies (local and remote sites) before an acknowledgment is returned to the host that issued the write. This type of remote mirroring is typically used for geographically close sites to minimize the effect of I/O delays, which are proportional to the distance between the sites. The standard supported distance for synchronous mirror is 100km. If you need more contact your sales representative to file Storage Customer Opportunity REquest (SCORE).

1.1.2 Asynchronous Mirror

Remote mirroring can also be an asynchronous solution. This solution type is similar to above, but differs with the consistent sets of data being copied to the remote location at predefined intervals at the same time the host I/O operations are acknowledged directly after they are written on the primary site alone. This configuration is typically used for longer distances and latencies, between sites.

Note: A reliable, dedicated network bandwidth is preferred for mirroring. Links can be shared, but require available and consistent network bandwidth. The specified minimum bandwidth (50 Mbps for iSCSI) is a functional minimum and might not meet the replication speed that is required for a customer environment and workload.

Also, minimum bandwidths are *not* time-averaged, as typically reported by network monitoring packages. They are instantaneous, constant requirements, typically achievable only through network quality of service (QoS).

RPO/RTO (Restore Point Objective / Restore Time Objective)

The following preferred practices are advised for cross-gen asynchronous mirroring:

- When configuring the asynchronous mirroring, consider the I/O rate that can be handled by the secondary system, and configure the volumes on the primary system to handle a load that is not generally exceeding this limit. Note that it is not feasible to guarantee that the I/O rate *never* exceeds the limit.
- The target sync rate should be set to a reasonable level. The default setting of the target sync rate (300 MBps) is a valid setting. Increasing from this limit should be done with care. Setting the sync rate can be sufficient to ensure that work load spikes do not overwhelm the secondary system. If the host workload is normally low, there might be a period of RPO lagging after a spike, but the mirror recovers over time. If the workload is often higher than the limit, the mirror might not have enough time to recover between spikes and the system might get to an extreme RPO lagging state.
- If the host I/O load is too high and the mirror state is RPO lagging with the sync job taking longer and longer to complete, QoS can be used to limit the host I/O rate. This limitation

ensures that the host is unable to create a load higher than defined. It also ensures that if the configuration is healthy, the recovery point on the secondary system is within the defined RPO.

MRS and LRS (internal snapshots)

When replicating, the storage system creates internal snapshots.

The last-replicated snapshot (LRS) ensures that there is a consistent copy of the data for recovery purposes. This means either in the event the secondary site must be used to carry on production or resynchronization must be done after the source stopped suddenly, leaving the secondary copy in an inconsistent state (because it was only partially updated with the changes that were made to the source volume). This last-replicated snapshot is preserved until a volume/CG pair is synchronized again through a completed sync job, at which point a new last-replicated snapshot is taken.

The last-replicated snapshot lifecycle is as follows:

- A snapshot of the source volume or CG is taken at the primary, and is named the most-recent snapshot (MRS).
- All data from the most-recent snapshot is sent to the secondary site through a sync job.
- Upon the completion of the sync job, the secondary site takes its last-replicated snapshot and time-stamps it.

Notification is sent from the secondary site to the primary site, and the most-recent snapshot is renamed to last-replicated snapshot.

Scheduler

Asynchronous mirroring is initiated at intervals that are defined by the *sync job schedule*. A sync job entails synchronization of data updates that are recorded on the source since the last successful synchronization. The sync job schedule is defined for both the primary and secondary system peers in the mirror. Having it defined for both entities enables an automated failover scenario, where the destination becomes a source and has a readily available schedule interval.

The system supports numerous schedule intervals ranging from 20 seconds to 12 hours. Determine the optimum schedule interval based on your recovery point objective (RPO) requirements.

A schedule set to `NEVER` means that no sync jobs are automatically scheduled. Thus issuing replication in that case must be done through an explicit manual command. A manual command invocation can be done at any time, in addition to scheduled snapshots. These ad hoc snapshots are issued from the source and trigger a sync job that is queued behind the outstanding sync jobs.

The Hyper-Scale Manager GUI automatically creates schedules based on the RPO selected for the mirror that is being created. The interval can be set in the mirror properties window or explicitly specified through the XCLI.

Note: Typical asynchronous mirror configuration indicates the RPO requirements, and the A9000 FlashSystem automatically assigns an interval schedule that is one-third of that value (rounding down if needed).

Tip: The A9000 FlashSystem allows a specific RPO and schedule interval to be set for each mirror coupling.

Also, be aware that existing destination volumes must be formatted before they are configured as part of a mirror. This means that the volume must not have any snapshots and must be unlocked. Otherwise, a new destination volume can be created, and used, when defining the mirror.

Offline initialization

Offline initialization is also referred to as *trucking*. It is a replication feature that provides the ability for a target volume to be initialized without requiring the contents of the source volume to be replicated over an inter-site link. This feature can avoid long initialization times when data is already available on the target side. Or another scenario can be if intersite link speed is not great, mailing a tape/disk with the data can be faster than transfer over the intersite link.

The initialization phase of either of the IBM A9000 FlashSystems replications methods, namely synchronous and asynchronous. Offline initialization can shorten the IBM A9000 FlashSystems mirror initialization phase significantly.

Offline initialization is accomplished with the following steps:

1. Create a snapshot of the future source volume on the primary IBM A9000 FlashSystem. The volume is a production volume that is not currently in a mirroring relationship. Transferring the data on this snapshot to a volume on the secondary IBM A9000 FlashSystem is the objective of the offline initialization.
2. Map this snapshot to a host system and create a disk image of the volume. This image can be written to a file or to a tape or any other suitable media.

   Important: To create a valid disk image**,** use a backup tool that ensures that the same data will be in the same location on both the source and backup copies on disk. A file-level backup tool will *not* work for that purpose; you need a backup tool that creates a raw copy, reading the entire disk serially, with no concept of files, for example **dd** command in unix.

3. Transport this disk image to the IBM A9000 FlashSystem secondary. The volume can either be moved physically through carrier or electronically (FTP server).
4. Create the IBM A9000 FlashSystem volume on the IBM A9000 FlashSystem secondary that is the same size as the source volume and map this volume to a host. This will be the future target volume, but it is not yet in any mirroring relationship.
5. Copy the disk image to the newly created volume on the IBM A9000 FlashSystem secondary using the same utility that was used to create the disk image.
6. Create the mirror relationship of your choice, being sure *not* to select the Create Destination option, and to explicitly name the destination volume based on the name of the volume created on the secondary site. And most important, select the **Offline Init** check box.
7. Activate the mirror relationship.

The IBM A9000 FlashSystem respective (either asynchronous or synchronous) mirror functions now creates the mirror pair. For an asynchronous mirror, a most-recent snapshot is taken on the primary IBM A9000 FlashSystem. This most-recent snapshot on the primary is then compared to the data-populated target volume on the secondary IBM A9000 FlashSystem using 64 KB checksum exchanges. The new data that have been written to the source volume since the original snapshot was taken are calculated. Only the new data on the source volume will be transferred to the target volume during the offline initialization phase.

1.2 Hyperswap

The HyperSwap feature of FlashSystem A9000 and A9000R delivers always-on, high availability (HA) storage service for storage volumes in a production environment. It is based on an active-active, cross-system, and cross-datacenter configuration. HyperSwap builds upon the synchronous mirroring functionality already included with the FlashSystem A9000 and A9000R. HyperSwap volumes can autonomously and transparently switch between primary and secondary roles, based on the volume's failover state.

1.3 Multi-site HA/DR

Using three FlashSystem A9000 and/or A9000Rs, and combining HyperSwap and Asynchronous replication, Multi-site creates a solution that entails both High Availability (HA) and Disaster Recovery (DR). One side of the HyperSwap pair has an active async link to the third system, and the other side has a standby link. This configuration provides HyperSwap active-active high availability, while keeping data mirrored to a third copy to ensure two levels of business continuity.

1.4 Migration

IBM FlashSystem A9000 and A9000R include a powerful data migration capability.

The Data Migration utility can migrate data from almost any storage system to IBM FlashSystem A9000 and A9000R. The storage system can be an IBM storage system or another storage system, if that storage system supports Linux hosts. The migration process is the same for all storage systems.

At the start of the migration, application hosts are offline for only a short time as they are connected to IBM FlashSystem A9000 or A9000R. The logical volumes, also known as logical unit numbers (LUNs), that are migrated are reallocated from the former storage server to FlashSystem A9000 or A9000R and are then natively presented again to the host. Meanwhile, the data is transparently migrated in the background, in a controlled fashion.

For details, refer to Chapter 8, “Data migration” on page 171.

1.5 Hyper-Scale Mobility

Hyper-Scale Mobility enables clients to move a volume from one FlashSystem A9000 or A9000R to another (over synchronous distances) or from XIV to FlashSystem A9000 or A9000R in a manner that is transparent to host applications before, during, and after the volume migration.

Hyper-Scale Mobility helps you overcome provisioning scenarios that normally challenge traditional systems. It can accommodate several critical client needs in the modern data center and cloud environment, including online data mobility, load balancing, over-provisioning, and storage system repurposing.

This volume migration capability greatly enhances FlashSystem A9000 and A9000R scalability and directly addresses several client storage-related issues:

- Managing storage growth
- Providing more flexibility in capacity forecasting
- Managing costs
- Scaling between FlashSystem A9000 and A9000R systems
- Balancing workloads across systems without service downtime for better performance
- Retiring systems gracefully and upgrading to the latest technology
- Separating storage and host maintenance cycles
- Migrating volumes from XIV to FlashSystem A9000 or A9000R without any host downtime

Hyper-Scale Mobility capabilities also provide FlashSystem A9000 and A9000R with improved total cost of ownership (TCO) and improved service continuity.

Consider how Hyper-Scale Mobility can address the following client situations:

- Migrating all the data from a FlashSystem A9000 and A9000R that will be decommissioned or redeployed for a new purpose.
- Migrating all the data from XIV that will be decommissioned or redeployed.

Hyper-Scale Mobility can be used to rebalance the workload, away from a system that is heavily used to a system that is under utilized. It does not matter if the capacity imbalance is performance-related or data storage-related. Hyper-Scale Mobility can help resolve both situations.

2

Snapshots

The IBM FlashSystem A9000 and A9000R *Snapshot* function provides a point-in-time image that can be used for a recovery, or to provide copies of production data for business or IT purposes.

This chapter explains the characteristics of the Snapshot function and describes its implementation and usage. The following sections are included:

- Snapshots handling
- Consistency Group Snapshot

2.1 Snapshots handling

A *Snapshot* is a point-in-time copy of a volume's data.

Snapshots in IBM FlashSystem A9000 and A9000R use several innovative technologies to ensure minimal impact on system performance. Snapshots are space-efficient (redirect on write), use pointers, and contain only partitions with data that changed from the original volume. If a partition did not change, both the Snapshot and the volume point to the same partition.

Because the source volume and the Snapshot volume differ over time, Snapshots require storage capacity. Space for Snapshots must be set aside when you define a storage pool. The Snapshot reserve space requires a minimum of 400 GB in IBM FlashSystem A9000 and A9000R.

An application can use many volumes on IBM FlashSystem A9000 and A9000R. For example, a database application can span several volumes for application data and transaction logs. In this case, the Snapshot for those volumes must occur at the same moment in time so that the data and logs are consistent. To keep those volumes together they are placed in a Consistency Group. Creating a Snapshot of the Consistency Group ensures that all of the volumes that are assigned to the group are snapped at the same moment, which ensures data consistency throughout the group.

The creation and management of Snapshots with IBM FlashSystem A9000 and A9000R are straightforward. This section guides you through the lifecycle of a Snapshot, providing examples of how to interact with the Snapshots by using the GUI and the CLI.

2.1.1 Creating a Snapshot of a volume

A Snapshot of a volume or Snapshots of multiple volumes can be created by using either the GUI or the CLI. To use the GUI, select the volume (or volumes) that you want. Select **Actions** → **Snapshots** → **Create Snapshot(s)**. You can see an illustration in Figure 2-1.

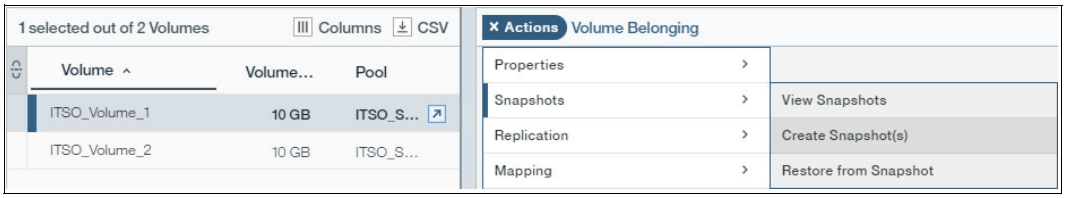


Figure 2-1 Create a volume Snapshot

The view on the right side of the GUI displays the Inspector for this volume and the window to create the Snapshot. If a single volume was selected, you can rename the volume. If multiple volumes were selected for Snapshots, the name is generated by the system, but you can change that name later.

When the Snapshot reserve capacity is exhausted, some Snapshots must be deleted to reclaim space for additional Snapshots. Former Snapshots are deleted according to a preset *deletion priority* (see 2.1.2, "Snapshot deletion priority" on page 11).

The deletion priority can be selected now. An example of multiple Snapshots with deletion priority selection is shown in Figure 2-2.

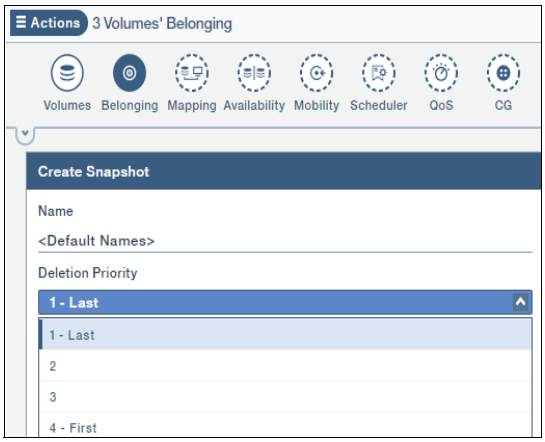


Figure 2-2 Create Snapshots of multiple volumes

For more information on Deletion Priority, refer to section 2.1.2, “Snapshot deletion priority” on page 11.

The new Snapshots can be viewed by clicking the **Sn** element in the Hub, as shown in Figure 2-3.

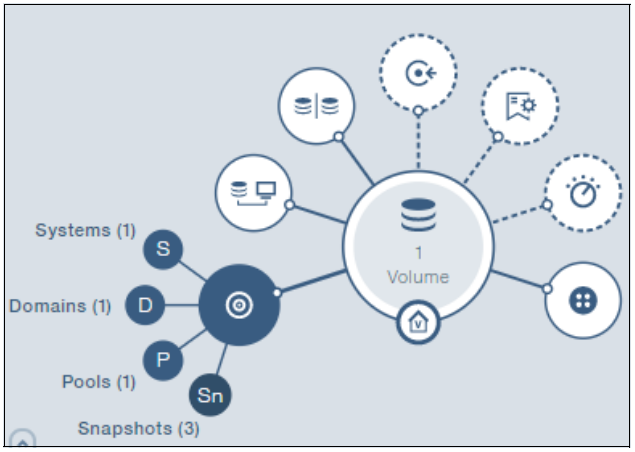


Figure 2-3 Hub view that is expanded for Snapshots

After you click the **Sn** circle, the GUI displays the table view with all of the snapshots and their properties, and the Inspector view, as shown in Figure 2-4.

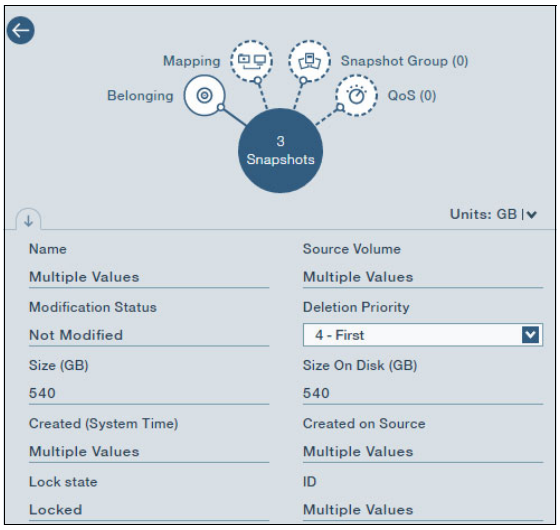


Figure 2-4 Multiple Snapshots Hub view

The deletion priority in this example is set to `4 - First`, but it can be changed with the drop-down list. The deletion priority is the only field that can be changed when multiple items are selected in the table (default if there were multiple Snapshots of a volume) view. When a single Snapshot is selected, the name and size can also be modified, as shown in Figure 2-5.

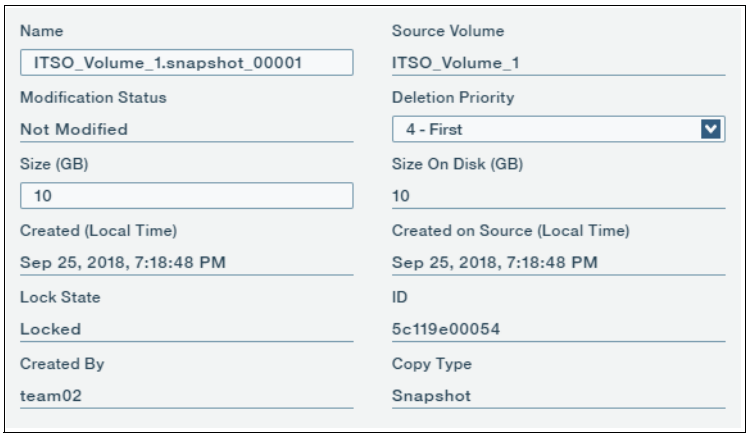


Figure 2-5 Modify Snapshot properties

The table view contains the specific details about each Snapshot as shown in Figure 2-6. The columns view can be fully shown by moving the slider at the bottom of the window or by expanding the table view. The column cell views can be increased to see the entire field (such as the name of the Snapshot) or decreased to see less by hovering over the name of the column to see the dividers and then by moving the divider to the desired width. Columns can be added or removed by right-clicking the column title or by clicking the Columns icon to see the additional fields available or right clicking on the column title area, as shown in Figure 2-6.

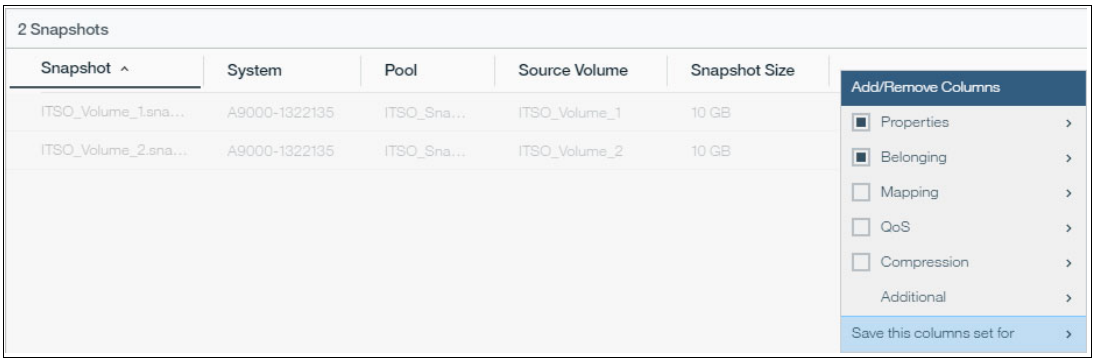


Figure 2-6 Add columns to the Snapshots table

From the Snapshosts list view, as shown in Figure 2-7, you can obtain other details:

- The default name of the Snapshot follows a specific format. The first part is the name of the volume followed by the word `Snapshot` and then a number, or count, of Snapshots for that volume. A Snapshot is the same size as the volume after its creation, although the volume size can change later while the Snapshot retains its original size.
- The `locked` property of the Snapshot. By default, a Snapshot is locked when it is created, which means that it is read-only.
- The modified property is displayed next to the locked field. The value changes to `yes` after a Snapshot is unlocked.

Figure 2-7 Snapshots list view

2.1.2 Snapshot deletion priority

IBM FlashSystem A9000 and A9000R use an automatic Snapshot deletion mechanism to protect against overutilizing the Snapshot space in a pool. Snapshot space overutilization can occur as new data is written to a volume, which means that the Snapshot now must contain the original data from the point in time that the Snapshot was taken. It can also happen as Snapshots are created.

Each Snapshot has a deletion priority property that is set by the user at the time of creation (and it can be modified later). Five deletion priorities from priority 4 to priority 0 (which is also known as the *Golden Snapshot*). Priority 0 is used to protect Snapshots that must *not* be subject to automatic deletion and is only available for Snapshot Groups on FlashSystem A9000 and A9000R. The system uses this priority to determine which Snapshot to delete first.

When the system needs to delete a Snapshot to make room for a new Snapshot (or space in the pool), it deletes the oldest Snapshot with deletion priority 4. The system deletes all of the Snapshots with priority 4 before it deletes Snapshots with priority 3. Then, the system deletes the Snapshots with priority 2. The last Snapshots that are deleted by the system are the deletion priority 1 Snapshots. The default deletion priority in the GUI is priority 1.

IBM FlashSystem A9000 and A9000R provide alerts based on the percentage of the Snapshot space that is used in a pool. As you receive higher-level alerts about Snapshot usage, the Snapshot space of the affected pool can be manually expanded to accommodate more Snapshots, or Snapshots can be manually deleted before the automatic deletion occurs. For more information about viewing and modifying the default Snapshot usage thresholds, see the *Managing storage pools with the GUI* section in the *Storage management and configuration* chapter of *IBM Hyper-Scale Manager for IBM Spectrum Accelerate Family: IBM XIV, IBM FlashSystem A9000 and A9000R, and IBM Spectrum Accelerate*, SG24-8376.

2.1.3 Restoring a volume from a Snapshot

You can restore the data from a Snapshot back to the original volume. This action can be helpful for operations where data was modified incorrectly and the data needs to be restored to the point in time at which the Snapshot was taken.

As shown in Figure 2-8 and Figure 2-9, from the Volume Actions menu select **Snapshot** → **Restore from Snapshot**. The system prompts you to select from a drop-down list the Snapshot to restore from, which is useful when more than one Snapshot exist to choose from.

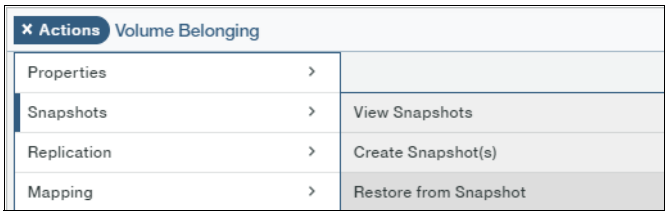


Figure 2-8 Restore a volume from a Snapshot

Figure 2-9 Snapshot restore selection menu

Note: If a Snapshot is taken and the original volume later increases in size, you can still perform the restore operation. The Snapshot has the original volume size, and it will restore the original volume correctly.

2.1.4 Managing Snapshots with the GUI

To manage Snapshots from the Storage Management GUI, select **Pools & Volumes Views** → **Snapshots**. This action lists all of the Snapshots on the systems in a single table view. Selecting any of the Snapshots in the table enables the Actions menu.

The following actions are available:

- Properties: View and modify Snapshot properties, including the lock state
- Mapping: Map Snapshots, unmap Snapshots, and modify Snapshot mappings
- QoS: Set and cancel a performance class for a Snapshot
- Statistics: View statistics for a Snapshot
- Snapshot Data: Format, modify, duplicate, copy, and restore a Snapshot
- Delete: Delete a Snapshot

Properties

The Properties view of a Snapshot also includes the ability to rename a Snapshot, change the deletion priority, resize a Snapshot, and change the lock state of a Snapshot. These options are shown in Figure 2-10.

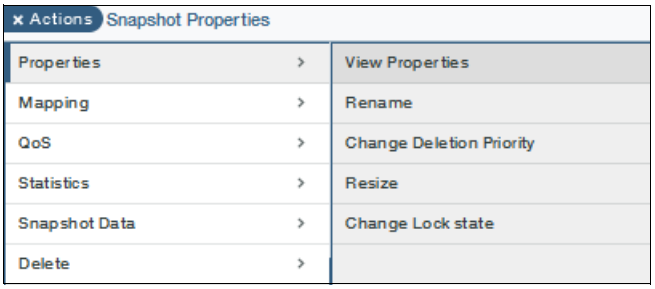


Figure 2-10 Snapshot properties options

Although these options are easy to run, let's look at unlocking a Snapshot. By default, a Snapshot is locked when it is created, and is a read-only Snapshot. By unlocking a Snapshot, you can modify the data in the Snapshot for testing, development, or data mining without affecting the volume.

If the data needs to be maintained in the Snapshot, you can create a duplicate Snapshot for the data while the original Snapshot is unlocked and modified. After the modifications and testing are complete, the Snapshot can be deleted, keeping the duplicate Snapshot that still points to the volume. You can also copy a Snapshot to perform the same activities on the copy instead of a duplicate or the original Snapshot.

To unlock a Snapshot, select a Snapshot from the Snapshots view, then select **Actions** → **Properties** → **Change Lock State** to change the state as shown in Figure 2-11.

Figure 2-11 Change the lock state of a Snapshot

The state of the Snapshot can be toggled between unlocked or locked. The current state of the Snapshot is selected. In this example, the state is locked.

To save changes that were made to a Snapshot while it was unlocked, lock the Snapshot by using the same process as unlocking. The locking process completes immediately, preventing further modification to the Snapshot. In this case, the Snapshot might no longer be a point in time copy of the source volume. A modified Snapshot can be overwritten by a current point in time copy of the volume by selecting **Actions** → **Snapshot Data** → **Overwrite by Volume**.

Note: A Snapshot that is unlocked and then locked again displays `Yes` under the Modified column in the Snapshots view. You might need to add the Modified column to the default view.

Another option is to create a duplicate or copy of the Snapshot to preserve the original Snapshot as a backup of the volume while the duplicate Snapshot is modified after the duplicate Snapshot is unlocked. The option to duplicate or copy a Snapshot is under the Snapshot Data in the Actions menu. Copying a Snapshot requires a volume to copy to. You can specify an existing one or create a new volume.

Mapping

Mapping a Snapshot is the same as mapping a volume. One difference here is that after a Snapshot is mapped to a host, a locked Snapshot is in a read-only state. To use the Snapshot for writing, it must first be unlocked as described in the previous section.

Quality of service (QoS)

A performance class might need to be applied to an unlocked Snapshot that is used for writing or even for backup operations. Select **Actions** → **QoS**, and either create a QoS definition or assign an existing performance class to the Snapshot. The menu option is shown in Figure 2-12.

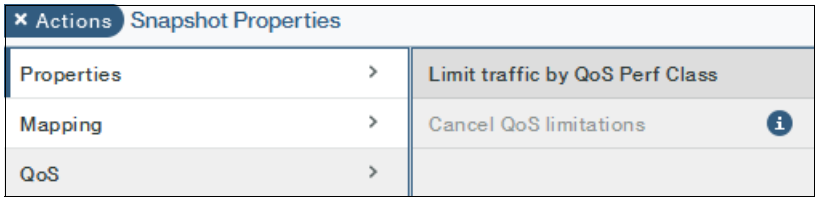


Figure 2-12 Setting a performance class for a Snapshot

Statistics

To view the statistics that are associated with a volume Snapshot, select **Actions** → **Statistics** → **Show Performance Statistics** as shown in Figure 2-13.

Figure 2-13 Performance statistics for a Snapshot

This action opens the Statistics view under the Snapshot table view.

Snapshot Data

Other actions that you can perform on a Snapshot are listed under Snapshot Data. These options include formatting a Snapshot, overwriting the Snapshot from the original volume, duplicating the Snapshot (which is taking a Snapshot of the Snapshot), copying the Snapshot, and restoring a volume from a Snapshot. These options are shown in Figure 2-14.

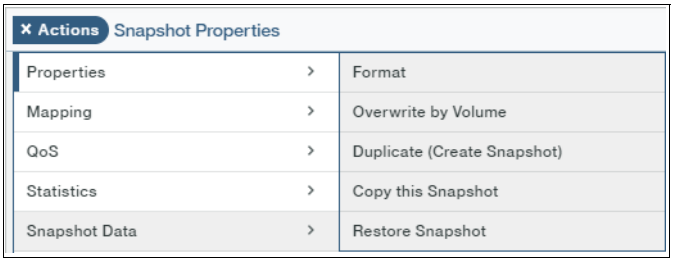


Figure 2-14 Snapshot data options

Consider overwriting a Snapshot. For regular backup jobs, you can decide to create Snapshots, letting the system delete the old Snapshots, or overwriting the existing Snapshots with the latest changes to the data. For instance, a backup application requires the latest copy of the data to perform its backup operation.

The overwrite operation modified the pointers to the Snapshot data to be reset to the volume. All of the pointers to the original data in the Snapshot are lost, and the Snapshot appears as new. Storage that was allocated for the data changes between the volume and its Snapshot is released.

To perform this operation, select **Snapshot Data** → **Overwrite by Volume**. The GUI displays the request for your confirmation, as shown in Figure 2-15. Click **Apply**.

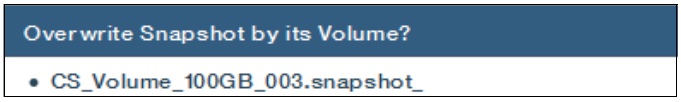


Figure 2-15 Overwrite a Snapshot

You can restore the data from a Snapshot of a Snapshot back to the original Snapshot. This action can be helpful for operations where data was modified incorrectly and the data needs to be restored to the Snapshot. Select **Snapshot Data** → **Restore Snapshot**. The system prompts you to select from a drop-down list the Snapshot to restore from, which is useful when more than one Snapshot exists to choose from.

Select **Apply**, as shown in Figure 2-16.

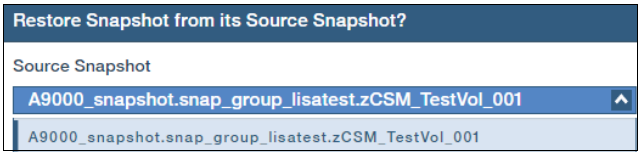


Figure 2-16 Restore a Snapshot

After you restore a Snapshot from its source Snapshot, the process will modify the pointers to the Snapshot so that they are now equivalent to the source Snapshot pointers. This change occurs only for the partitions that are modified from the time that the source Snapshot was taken. The Snapshot pointer does not change and continues to point to the original data. The restore process then frees the modified partition space.

Delete a Snapshot

When a Snapshot is no longer needed, it can easily be deleted. Select the Snapshot in the Snapshots view. Then, click **Actions** → **Delete** → **Delete Snapshot(s)**, as shown in Figure 2-17.

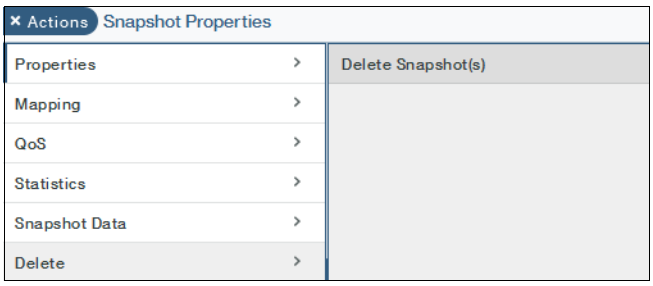


Figure 2-17 Deleting Snapshots

The Snapshots are displayed on the right side of the window. Confirm that these Snapshots are the correct Snapshots to delete and click **Apply**. An example can be seen in Figure 2-18.

Figure 2-18 Delete Snapshots

Reminder: If a volume is deleted, all of the associated Snapshots are also deleted.

2.1.5 Managing Snapshots with the CLI

The CLI commands are straightforward in their functions. For a full listing of commands and usage, see *IBM FlashSystem A9000R Command-Line Interface (CLI) Reference Guide*, SC27-8711. The list of basic commands for a volume Snapshot are displayed in Example 2-1. Additional commands that relate to Snapshots can be listed by issuing the **help** command as shown in Example 2-1:

Example 2-1 Snapshot CLI commands

```
A9000R Demo>>help category=snapshot
Category   Name                      Description
snapshot   snapshot_list             Use the snapshot_list command to list
                                     snapshot information.
snapshot   snap_group_format         Use the snap_group_format command to format
                                     a snapshot group.
snapshot   mirror_create_snapshot    Use the mirror_create_snapshot command to
                                     create a snapshot mirror.
snapshot   mirror_cancel_snapshot    Use the mirror_cancel_snapshot command to
                                     cancel all snapshot mirrors ('ad-hoc'
                                     sync jobs) of a specified master volume or
                                     a master Consistency Group, that have not
                                     run yet.
snapshot   ha_create_snapshot        Use the ha_create_snapshot command to
                                     simultaneously create snapshots on both
                                     peers of a HyperSwap relation.
snapshot   snapshot_delete           Use the snapshot_delete command to delete a
                                     snapshot.
```

```
snapshot   snapshot_format           Use the snapshot_format command to format a
                                     snapshot.
snapshot   snapshot_create           Use the snapshot_create command to create a
                                     snapshot of an existing volume.
snapshot   snapshot_duplicate        Use the snapshot_duplicate command to
                                     duplicate an existing snapshot.
snapshot   snapshot_restore          Use the snapshot_restore command to restore
                                     a master volume or a snapshot from one of
                                     its associated snapshots.
napshot   snapshot_change_priority  Use the snapshot_change_priority command to
                                     change a snapshot's deletion priority.
```

To create a basic Snapshot, use the **snapshot_create** command, as shown in Example 2-2. In this example, we specified the deletion priority. If this option is not used, the default priority is used. The other options for this command are shown:

- name
- overwrite
- ext_id

Example 2-2 Create a Snapshot

```
A9000R Demo>>snapshot_create vol=ITSO_Volume_2 delete_priority=4
Command executed successfully.
```

A Snapshot can also be duplicated for testing and backups. Figure 2-3 illustrates an example of duplicating a Snapshot, which is followed by listing all of the Snapshots that are associated with the same volume.

Example 2-3 Duplicate a Snapshot

```
A9000R Demo>>snapshot_duplicate snapshot=ITSO_Volume_2.snapshot_00001
Command executed successfully.
A9000R Demo>>snapshot_list vol=ITSO_Volume_2
Name                           Size (GB)   Copy type   Master Name
ITSO_Volume_2.snapshot_00001   10          snapshot    ITSO_Volume_2
ITSO_Volume_2.snapshot_00002   10          snapshot    ITSO_Volume_2
```

The CLI also allows a Snapshot to be restored from another Snapshot. Example 2-4 shows a more recent Snapshot (00002) that is restored to a later Snapshot (00001). This process results in the pointers for both Snapshots that now point to the same data.

Example 2-4 Restoring a Snapshot from another Snapshot

```
A9000R Demo>>snapshot_restore snapshot=ITSO_Volume_2.snapshot_00002
target_snapshot=ITSO_Volume_2.snapshot_00001
```

Formatting a Snapshot is also a simple process with the CLI as shown:

```
snapshot_format snapshot=ITSO_Volume_2.snapshot_00001
```

Unlock a Snapshot by using the **vol_unlock** command:

```
vol_unlock vol=ITSO_Volume_2.snapshot_00001
```

Delete a Snapshot by using the **snapshot_delete** command, as shown in Example 2-5.

Example 2-5 Deleting a Snapshot

```
A9000R Demo>>snapshot_delete snapshot=ITSO_Volume_2.snapshot_00001
Command run successfully.
```

2.1.6 Snapshot Scheduler

The Snapshot Scheduler is an option available with Hyper-Scale Manager, starting with V5.3, that allows the system administrator to automate Snapshots in a pool on a defined schedule. The schedule is applied to existing and new volumes and Consistency Groups within the pool. The Snapshot Scheduler is available for the entire IBM Spectrum Accelerate family that is managed by the Hyper-Scale Manager.

To work with the scheduler, select a pool in the pools view. Then, under the **Actions** menu, select **Snapshot Scheduler**. The following options are available:

- View/Modify Snapshot Schedules: Allows you to make change to existing schedules.
- Add Snapshot Scheduler: Allows you to create a new schedule.
- View all the related Snapshots: Lists those Snapshots that were created as a result of the scheduler.
- View all the related Snapshot Groups: Lists those Snapshot Groups that were created as a result of the scheduler.
- Volumes missing automated Snapshots
- CGs missing automated Snapshots
- Remove all Snapshot Schedules

These options are shown in Figure 2-19.

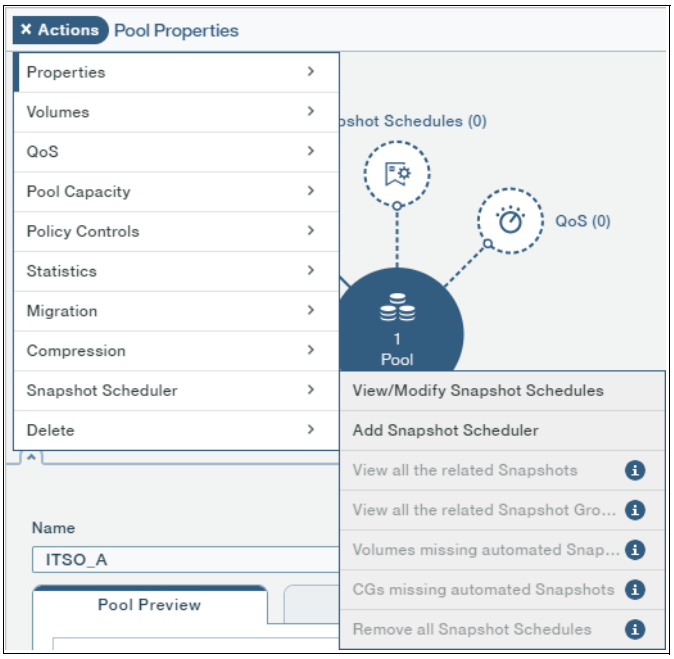


Figure 2-19 Snapshot Scheduler actions

Creating a Snapshot Schedule

This section reviews the steps that are required to create a schedule and some of the options available within adding a new schedule.

To create a schedule, select the **Add Snapshot Scheduler** option for the pool. You need to give the schedule a name and define what it applies to from the following options (as shown in Figure 2-20):

- Volumes & Consistency Groups
- Volumes (only Volumes not in Consistency Groups)
- Consistency Groups (only Volumes in Consistency Groups)

After you create a schedule, it affects all existing and new volumes or Consistency Groups that are created after the schedule is created.

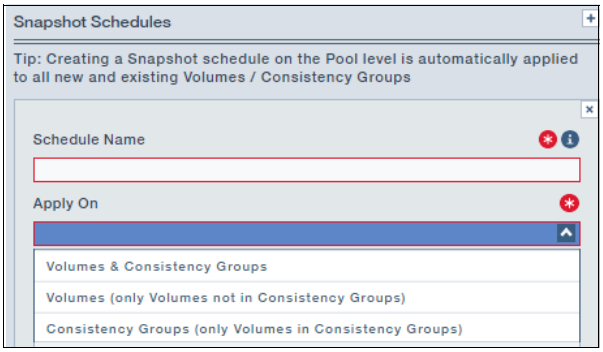


Figure 2-20 Selecting a volume or Consistency Group

Next define the time interval (daily, varying weekly intervals for specific days, monthly, and every other month) and the Time Zone, as shown in Figure 2-21.

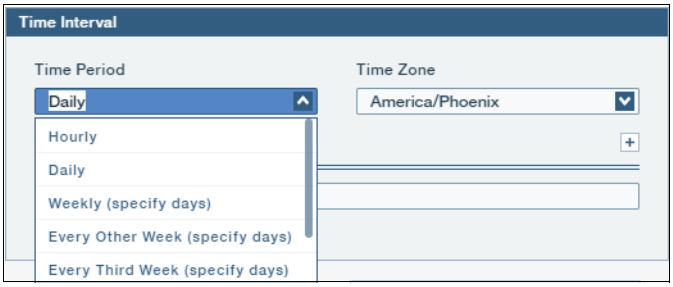


Figure 2-21 Selecting a time period and a time zone

After selecting the time period and the time zone, select the specific time for the Snapshot Scheduler to run. There can be more than one time slot for a time period. Creating an additional time to run in that time period, simply click the plus sign (+) to get a new time box, as shown in Figure 2-22.

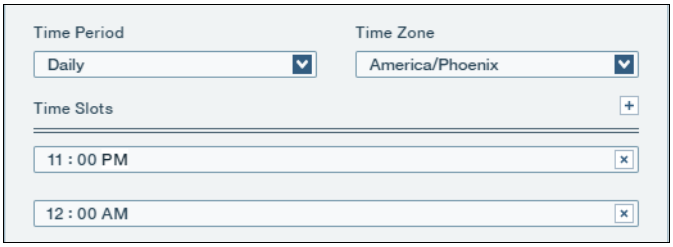


Figure 2-22 Schedule multiple time slots

You also need to define the retention policy. This number indicates how many Snapshots for the volume or Consistency Group that are kept on the system. The HSM displays approximately how long the Snapshot will be retained. If you need Snapshots to stick around for longer, creating a schedule for more Snapshots to be kept might be appropriate. However, remember that the schedule applies to all volumes or Consistency Groups within the pool.

Figure 2-23 shows an example where Snapshots created by a schedule that will be kept for approximately 2 days.

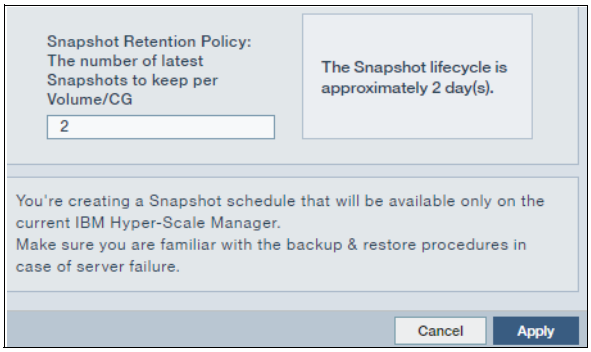


Figure 2-23 Snapshot retention definition

Figure 2-24 shows an example of creating two different types of schedules in the same pool. Notice that the schedule on the left will be taken daily for all volumes and Consistency Groups, and the one on the right is for volumes (not in a Consistency Group) and will be taken Monday through Friday.

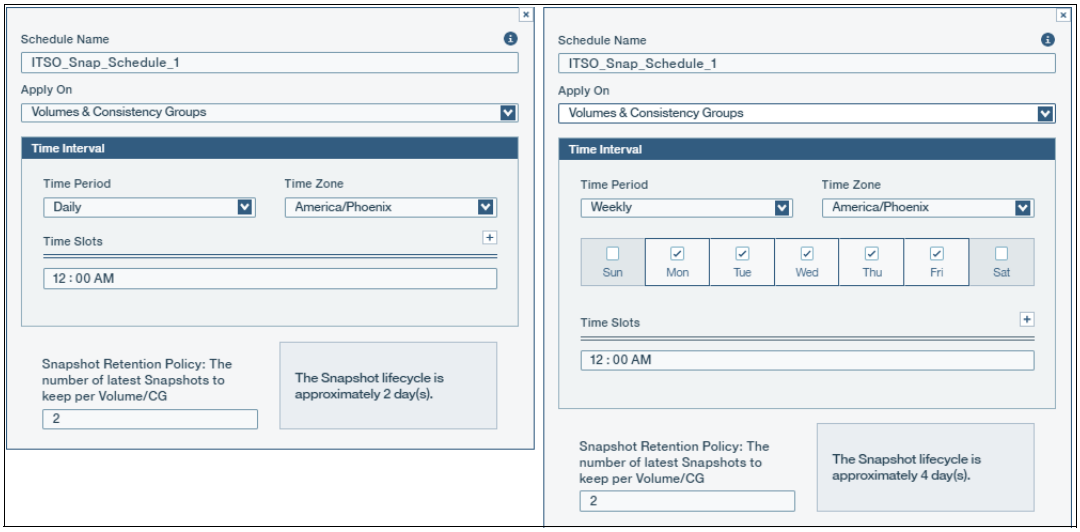


Figure 2-24 Multiple Snapshot schedules

The Snapshot schedules can be modified, removed and viewed by using the Actions menu option (Figure 2-25). You can view missing Snapshots for volumes and Consistency Groups if applicable.

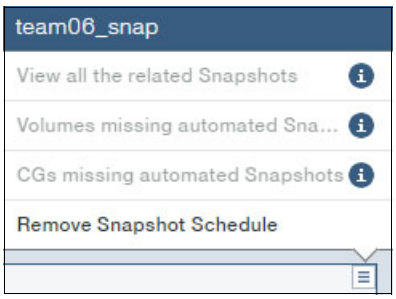


Figure 2-25 Snapshot schedule actions menu

Viewing Snapshot schedules

You can view all the pools containing Snapshot schedules in all the systems managed by the Hyper-Scale Manager by selecting the **Snapshot Scheduled Pools** option under the Pools & Volumes Views menu as shown in Figure 2-26.

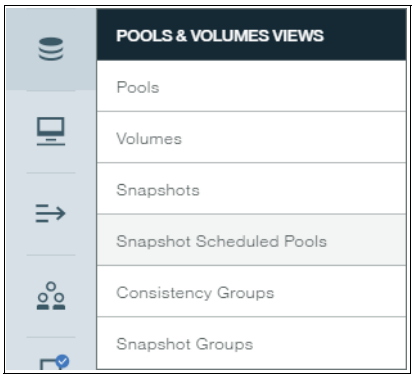


Figure 2-26 Pools with Snapshot schedules

Selecting this option opens a customized filter that lists all the pools with schedules. Selecting one of the pools from the list displays the Snapshot schedules in the inspector area. Figure 2-27 shows the list of pools.

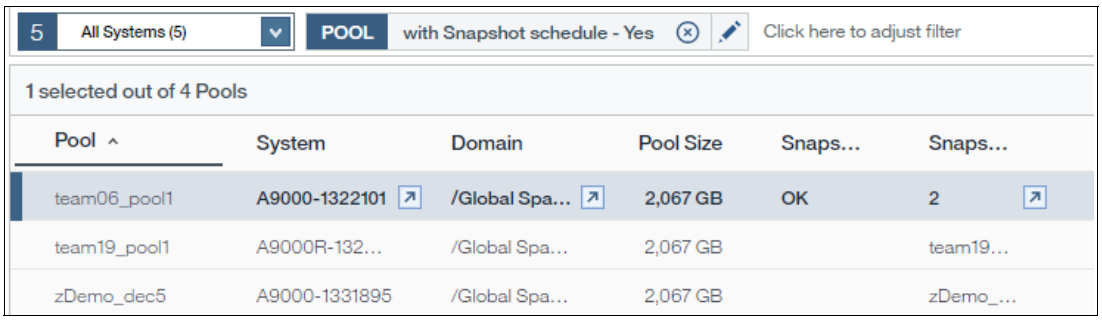


Figure 2-27 List of pools with Snapshot schedules

2.2 Consistency Group Snapshot

A *Consistency Group* is a group of volumes of which a Snapshot can be made at the same point in time. Therefore, a consistent image is made of all volumes within the group at that time. The concept of a Consistency Group is common among storage systems. It is necessary to perform concurrent operations collectively across a set of volumes so that the result of the operation preserves the consistency among the volumes.

For example, effective storage management activities for applications that span multiple volumes, or creating point-in-time backups, is not possible without first employing Consistency Groups.

This consistency among the volumes in the group is critical to maintaining data integrity from the application perspective. By first grouping the application volumes into a Consistency Group, it is possible to later capture a consistent state of all volumes within that group at a specified point-in-time by using a special Snapshot command for Consistency Groups.

When you issue this type of command, the following process results:

1. Complete and destage writes across the constituent volumes.
2. Suspend I/O activity simultaneously across all volumes in the Consistency Group.
3. Create the Snapshots.
4. Resume normal I/O activity across all volumes.

IBM FlashSystem A9000 and A9000R software manage these suspend and resume activities for all volumes within the Consistency Group.

Restriction: A Consistency Group cannot span multiple systems across IBM FlashSystem A9000 and A9000R.

2.2.1 Creating Consistency Groups

You can use the following methods to create a Consistency Group within the GUI:

- Create the Consistency Group and add the volumes to it.
- Choose to move a volume to a Consistency Group and create the Consistency Group then.

We first look at the second method. Under the Volumes view, select the volumes to move. The selection enables the Actions menu. Select **Actions** → **Consistency Group** → **Move to a Group**, as shown in Figure 2-28.

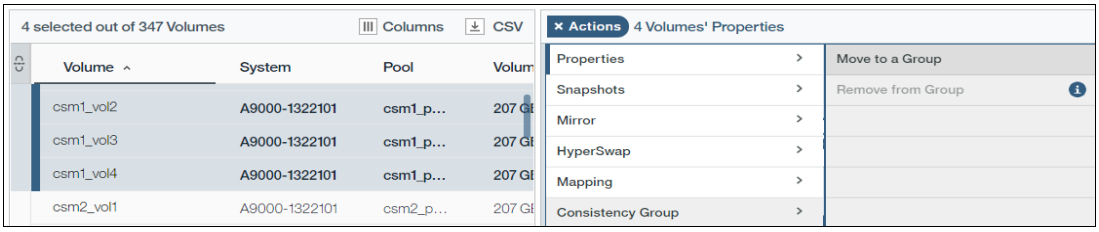


Figure 2-28 Moving volumes to a Consistency Group

This action opens the Volume Consistency Group wizard, as shown in Figure 2-29. The storage administrator can either select an existing Consistency Group or create a Consistency Group by clicking **CREATE CONSISTENCY GROUP**. In this example, chose to create a Consistency Group.

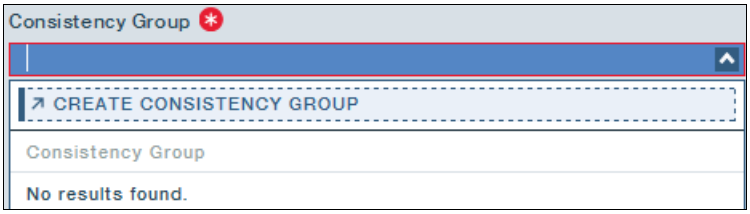


Figure 2-29 Create a Consistency Group from the move volumes to a group option

After the option is selected, a new screen opens that changes the view from volumes to Consistency Groups. The Create Consistency Group wizard is shown in Figure 2-30. Because the option to create was selected from the Volumes view, all of the fields are completed except the name of the Consistency Group. Also, on any of the filled-in lines (System, Domain and Pool), you can optionally navigate to that object's properties by clicking the arrow. The arrow is displayed only when the cursor is on that line.

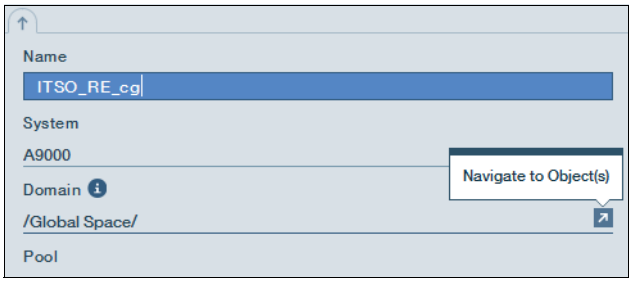


Figure 2-30 New Consistency Group

This action opens a new view. You can get back to the Create Consistency Group view by selecting the CG tab. An example of the tabs is shown in Figure 2-31. The current tab is white. The tab labeled Volume is the Volume Consistency Group tab, which is where we started. The number in red indicates the number of required fields in a tab. You can close any of the tabs to cancel the action.

Figure 2-31 Tabs that are open

After you create the Consistency Group, You will be returned to the volumes view. Select **Apply** to move the volumes to the Consistency Group you just created. The view now shows that the volume or volumes that you selected are in a Consistency Group, similar to Figure 2-32. Four volumes belong to a Consistency Group in the Hub display.

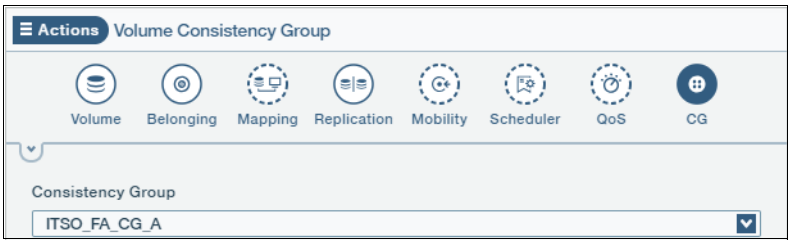


Figure 2-32 Hub view of volumes that belong to a Consistency Group

When you look at the properties of the Consistency Group, you can see the specific items that relate to it, including the four volumes in this example, and any associated Snapshot schedules, Snapshot groups and mirrors, as shown in Figure 2-33.

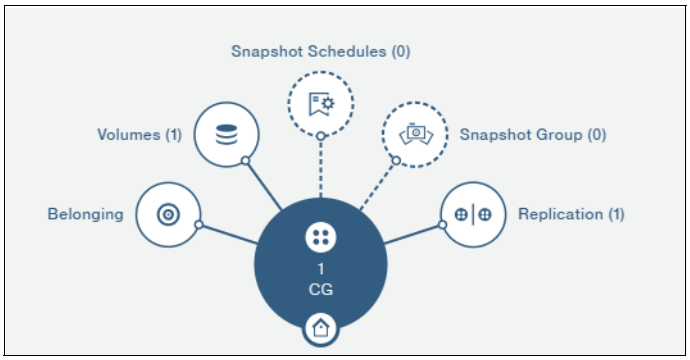


Figure 2-33 Hub view of a Consistency Group that contains volumes

Another option for creating a Consistency Group is to select the **NEW** menu and choosing **Consistency Group** as shown in Figure 2-34.

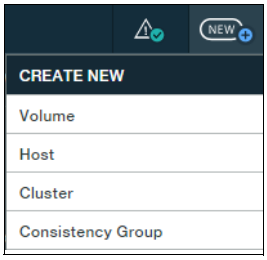


Figure 2-34 Create a Consistency Group

This action opens the Create Consistency Group window. Enter the required information for the name of the Consistency Group and select the system, domain, and pool, as shown in Figure 2-35. Performing the action from the Create New menu does not prepopulate the fields as the previous method did.

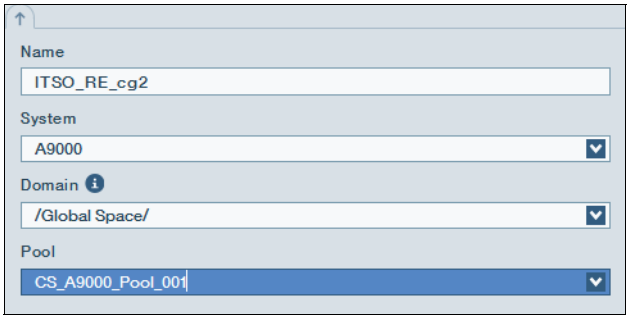


Figure 2-35 Creating a Consistency Group

After all of the information is entered and applied, the Consistency Group is created. The Consistency Group does not contain any volumes yet. The storage administrator can now return to the Volumes view and move volumes to this Consistency Group.

2.2.2 Adding volumes to a Consistency Group

To add volumes to a Consistency Group at any time, select the volume(s) under the Volumes view and select **Actions** → **Consistency Group** → **Move to a Group** as shown in Figure 2-28 on page 22.

You can then select an existing Consistency Group from the drop-down list as shown in Figure 2-36 or create a Consistency Group as we did in the previous section by using the Create Consistency Group option from the list. In this example, we selected the Consistency Group, **ITSO_RE_cg2**, from the list. Click **Apply** (not shown), and the action is complete.

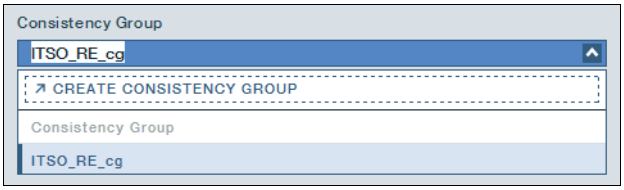


Figure 2-36 Select an existing Consistency Group

Now, the Consistency Group contains members and you can create *crash consistent* Snapshots, either through the GUI or CLI, or by using other techniques and application programming interfaces (APIs).

Note: Adding new volumes to a Consistency Group with Snapshot groups warns you that the existing Snapshot groups will no longer be consistent

2.2.3 Managing Consistency Groups with the GUI

As shown with other configuration tasks, the GUI makes it easy to manage Consistency Groups. You can set up the view in the Consistency Group table or continue with the default view (as described at the beginning of this chapter). To access the Consistency Groups view, select **Pools & Volumes Views** → **Consistency Groups** as shown in Figure 2-37.

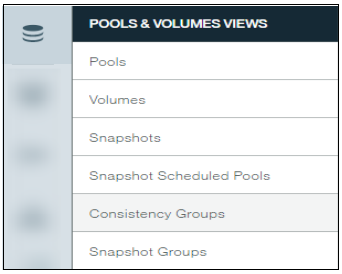


Figure 2-37 Pools & Volumes Views

After the Consistency Groups option is selected, the list of Consistency Groups is displayed in the table view. To view any of the available actions on a Consistency Group, a Consistency Group must first be selected from the list.

Tip: Remember you can filter the view or select a system (or subset by type).

The following actions are available:

- Properties: View and modify the properties of a Consistency Group.
- Pool, System: View and modify the pool that the Consistency Group belongs to.
- Replication: View and modify replication relationships for the Consistency Group.
- Statistics: View the Consistency Group volume and Snapshot performance and statistics.
- Members: View and modify the members of a Consistency Group.
- Snapshot Groups: Create and modify consistency Snapshot groups.
- Snapshot Scheduler: View an associated Snapshot schedule.
- Delete: Delete a Consistency Group.

Let's look at some of the options in more detail.

Properties

After a Consistency Group is selected from the table view, the properties of that Consistency Group are displayed on the right side of the browser window. Through the Properties tab, you can view and modify the name of the Consistency Group. This capability is indicated by the box around the editable fields. For Consistency Groups under properties, the editable field is the name of the group, as shown in Figure 2-38. Editing is a simple task. Place the cursor in the field to edit the name.

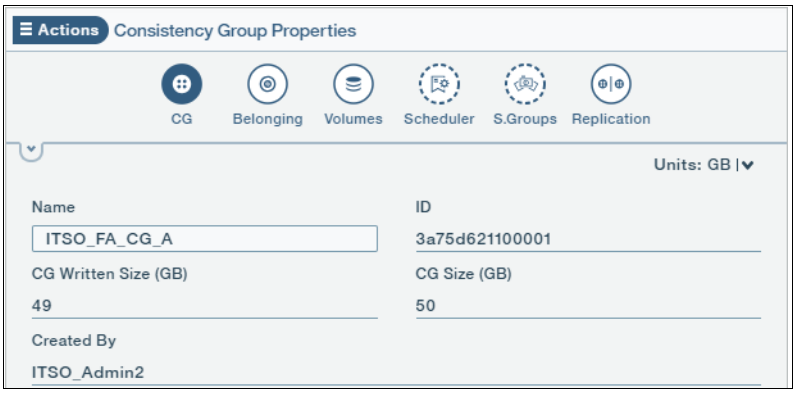


Figure 2-38 Consistency group properties

Another part of the Properties view is the graphical Hub display of more details about the Consistency Group. Clicking any of the solid circles displays details about that object. For example, by clicking the **Belonging** circle, the options for viewing systems, domains, and pools are displayed as shown in Figure 2-39.

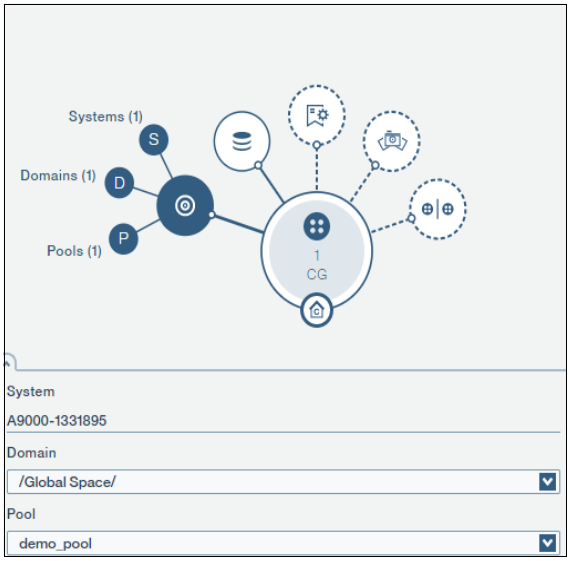


Figure 2-39 Consistency group Hub display

Clicking any of the solid circles displays the Hub details about that object. You can return to the previous window by clicking the back arrow, as shown in Figure 2-40. Starting with HSM V5.4, the back arrow will be on the left side of the filter box. Clicking the main CG circle returns the view to the properties of the Consistency Group. Clicking the lowest level of a circle, such as **Pool**, changes the table and graphical display to that object.

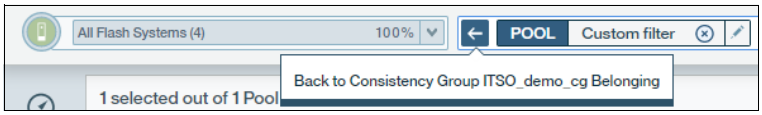


Figure 2-40 Use the back arrow option after you investigate an object to return to the previous view

Note: A circle with a dashed line indicates that no objects exist to display. You can click this to create a new object or association.

Pool and system

To view the Pool, System information that relates to a Consistency Group, you can also select the option from the Actions menu, as shown in Figure 2-41.

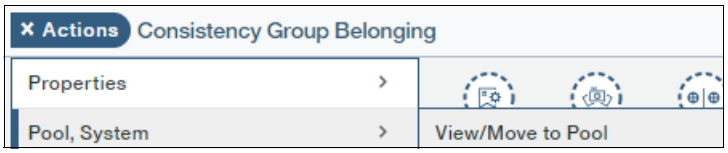


Figure 2-41 View the Consistency Group pool association

The Consistency Group pool and domain view in Figure 2-42 is then displayed. The storage administrator can view and move the Consistency Group with all its volumes and Snapshots to a different domain or pool, assuming that adequate space is available. Each field has a drop-down list of the available domains and pools in the system.

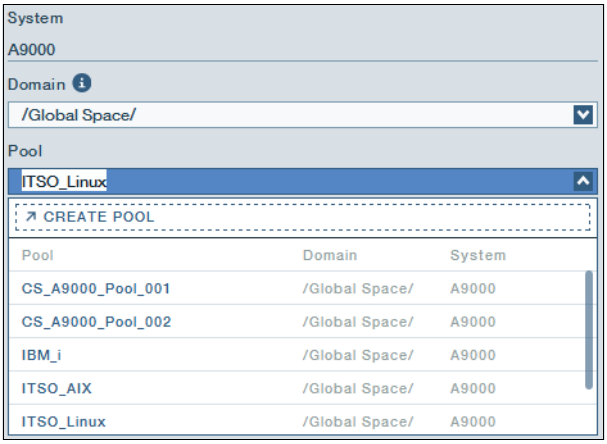


Figure 2-42 Move a Consistency Group to another pool

Statistics

You can use the Statistics view for Consistency Groups to view the performance and capacity statistics for volumes and Snapshots within a Consistency Group. To view the performance statistics, under the Consistency Groups view, select a Consistency Group and select either **Actions** → **Statistics** → **Show Snapshots Performance Statistics** or **Actions** → **Statistics** → **Show Volumes Performance Statistics**, as shown in Figure 2-43.

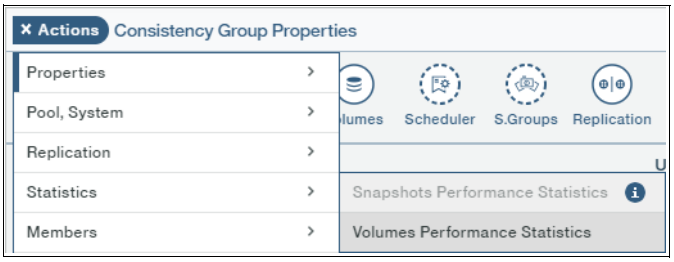


Figure 2-43 View statistics that are associated with Consistency Group members

Members

Members are the volumes and Snapshots that make up a Consistency Group. The storage administrator uses this option under the Consistency Group Actions menu to view the volumes in a Consistency Group, add volumes and remove all members of a Consistency Group, as shown in Figure 2-44.

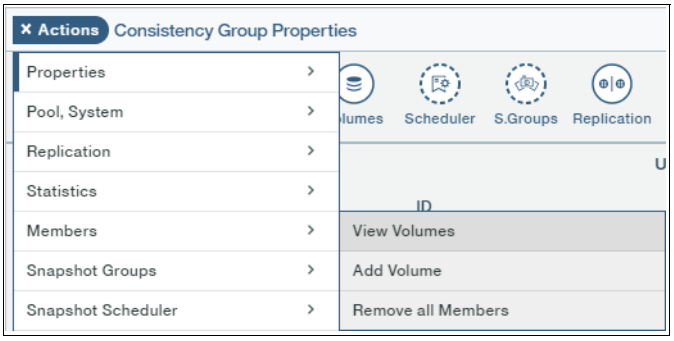


Figure 2-44 Members of a Consistency Group

Snapshot groups

A Consistency Group, which consists of multiple volumes, allows a Snapshot to be taken of all of the volumes at the same time. This action creates a synchronized Snapshot of all of the volumes in the Consistency Group, and it is suited for applications that span multiple volumes, for example, a database application that stores its data files on multiple volumes.

After the Consistency Group contains volumes, Snapshots can be created by selecting a Consistency Group in the Consistency Group view and then selecting **Actions** → **Snapshot Groups** → **Create Snapshot Group**, as shown in Figure 2-45. The other available options are viewing, restoring from, deleting and overwriting a Snapshot group.

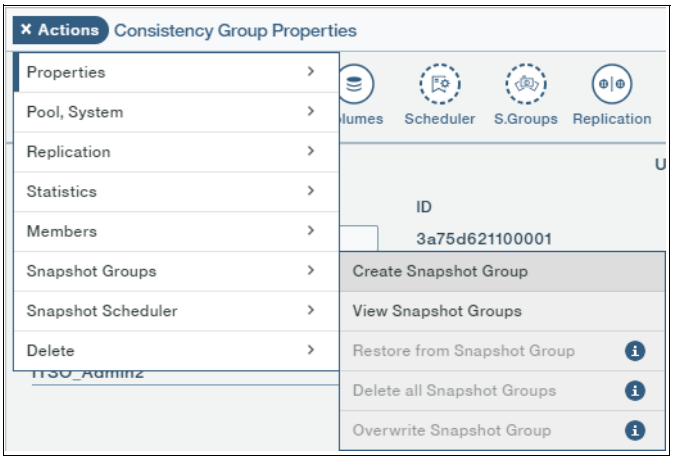


Figure 2-45 Consistency group Snapshot groups

After the Create Snapshot Group option is selected, you will see a window that is similar to Figure 2-46. The name of the Snapshot group and the deletion priority are the only required fields. The name is prepopulated (in this case, `ITSO_RE_cg.snap_group_`), and can be changed. The default deletion priority is set to `1 - Last`, but it can also be changed, depending on your requirements.

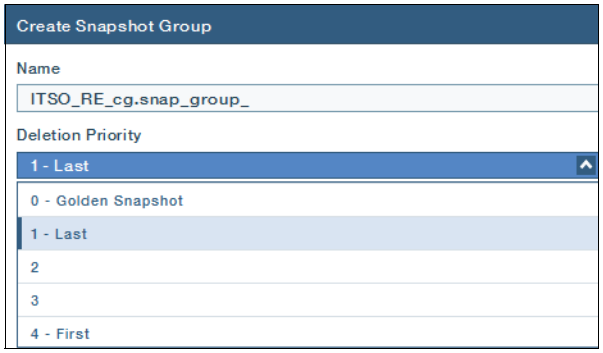


Figure 2-46 Create a Snapshot group

The FlashSystem A9000 and A9000R allow a *Golden Snapshot* on a Consistency Group basis. This means that the system will not automatically delete a Snapshot group with priority 0 when it is trying to free up space.

Important: The system uses the deletion priority when the system needs to remove Snapshots and Snapshot Groups to clear space.

After the Snapshots are created, you can see the Snapshots on the Snapshots view. Multiple paths exist in the GUI to perform actions on objects. For example, for Snapshot groups, by selecting the Snapshot Group circle from the Consistency Group Properties view, you can see the Snapshot Group menu, as shown in Figure 2-47.

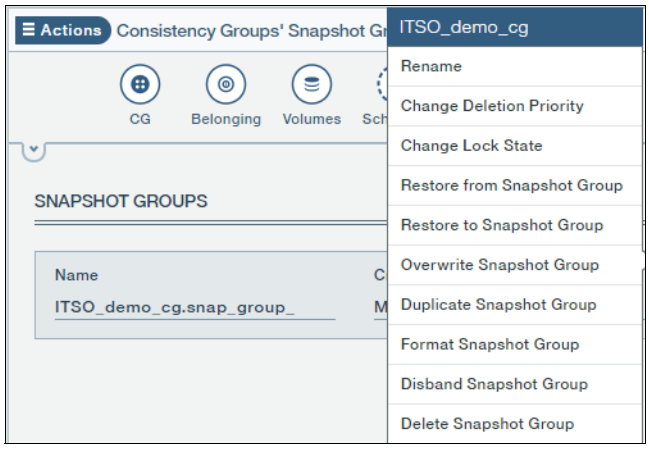


Figure 2-47 Snapshot group menu

Tip: Multiple ways to perform the same action on an object are available in the GUI.

Delete

The storage administrator can also remove a Consistency Group by selecting the Consistency Group and then by selecting **Actions** → **Delete** → **Delete Consistency Group(s)**, as shown in Figure 2-48. Multiple Consistency Groups can be selected at the same time for deletion.

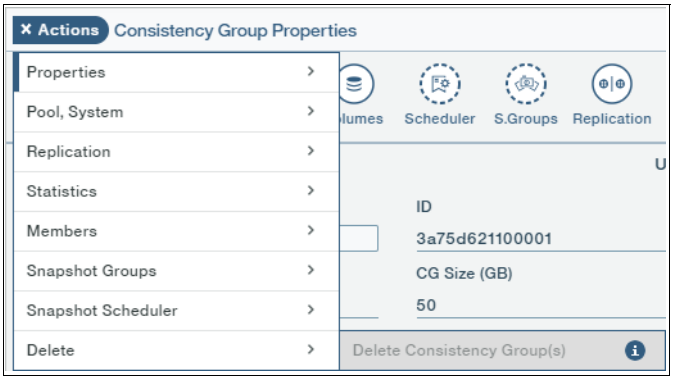


Figure 2-48 Delete a Consistency Group

Before you delete a Consistency Group, you must first move all of the volumes and associated Snapshots out of the Consistency Group. If the storage administrator attempts to delete active members, the system prevents the task from completing, as shown in Figure 2-49.

Figure 2-49 Unable to delete a Consistency Group with members

To remove the members, select the Consistency Group and select **Actions** → **Members** → **Remove all members**.

The system prompts you for confirmation, as shown in Figure 2-50.

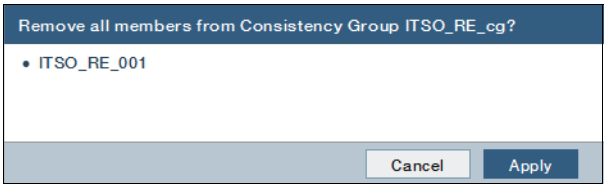


Figure 2-50 Remove members from a Consistency Group

After all of the members are removed, the Consistency Group can successfully be deleted.

2.2.4 Managing Consistency Groups with the CLI

By using the CLI session (or CLI commands), you can also perform the preceding processes. We first look at the commands that relate to Consistency Groups in the CLI by issuing the following command:

```
help category=consistency-group
```

The output of this command is shown in Example 2-6.

Example 2-6 Listing all available Consistency Group commands in the CLI

```
A9000R-Site_A>>help category=consistency-group
Category           Name                       Description
consistency-group  cg_list                    Use the cg_list command to list
                                              consistency groups.
consistency-group  xcg_list                   Use the xcg_list command to list
                                              cross-system consistency group
                                              definitions together with the
                                              contained consistency groups.
consistency-group  xcg_create                 Use the xcg_create command to create
                                              a cross-system consistency group
                                              (XCG) definition.
consistency-group  xcg_add_cg                 Use the xcg_add_cg command to
                                              associate an existing consistency
                                              group to a cross-system consistency
                                              group definition.
consistency-group  xcg_remove_cg              Use the xcg_remove_cg command to
                                              remove an existing consistency group
                                              from a cross-system consistency group
                                              definition.
consistency-group  xcg_add_remote_system      Use the xcg_add_remote_system command
                                              to add a remote system name to a
                                              cross-system consistency group
                                              definition.
consistency-group  xcg_remove_remote_system   Use the xcg_remove_remote_system
                                              command to remove a remote system
                                              name from a cross-system consistency
                                              group definition.
consistency-group  xcg_delete                 Use the xcg_delete command to delete
                                              a cross-system consistency group
                                              (XCG) definition.
consistency-group  xcg_get_local_cgs          Use the xcg_get_local_cgs command to
                                              list cross-system consistency group
                                              definitions together with the
                                              contained consistency groups.
consistency-group  xcg_get_remote_systems     Use the xcg_get_remote_systems
                                              command to retrieve the names of
                                              remote systems that are a part of the
                                              specified cross-system consistency
                                              group.
consistency-group  cg_create                  Use the cg_create command to create a
                                              consistency group.
consistency-group  cg_add_vol                 Use the cg_add_vol command to add a
                                              volume to a consistency group.
```

```
consistency-group  cg_remove_vol            Use the command cg_remove_vol to
                                            remove a volume from a consistency
                                            group.
consistency-group  cg_rename                Use the cg_rename command to rename
                                            consistencygroups.
consistency-group  cg_delete                Use the cg_delete command to delete a
                                            consistencygroup.
consistency-group  cg_snapshots_create      Use the cg_snapshots_create command
                                            to create a snapshot group of a
                                            consistency group.
```

To display all of the Consistency Groups in the system, issue the **cg_list** command, as shown in Example 2-7.

Example 2-7 List the Consistency Groups

```
ITSO_2_A9000R>>cg_list
Name       Pool Name
itso_cg1   itso_pool1
itso_cg2   itso_pool1
itso_cg3   itso_pool2
```

To create a Consistency Group, use the **cg_create** command and specify the name of the Consistency Group with the pool name, as shown in Example 2-8.

Example 2-8 Create a Consistency Group with the CLI

```
ITSO_2_A9000R>>cg_create cg=itso_cg4 pool=itso_pool2
Command run successfully.
```

The next step, after you create a Consistency Group, is to add volumes to the group. Use the **cg_vol_add** command. You must specify the Consistency Group and the volume to add. An example is shown in Example 2-9.

Example 2-9 Add a volume to a Consistency Group with the CLI

```
ITSO_2_A9000R>>cg_add_vol cg=itso_cg4 vol=itso_vol7
Command run successfully.
```

The storage administrator can also remove a volume from a Consistency Group by using the command **cg_remove_vol**. In this case, only the volume must be specified. The CLI prompts for confirmation before it removes the volume from the Consistency Group as shown in Example 2-10.

Example 2-10 Remove a volume from a Consistency Group with the CLI

```
ITSO_2_A9000R>>cg_remove_vol vol=itso_vol7

Warning:  Are you sure you want to remove volume 'itso_vol7' from its Consistency
Group? y/n: y
Command run successfully.
```

Alternatively, the command can be run by using **-y** to avoid the prompt. This option is useful when the command is run within a script.

To create a Snapshot group, issue the command as shown in Example 2-11. Additional options can be used with this command, including specifying a name for the Snapshot group and the deletion priority. By issuing this command, you create all of the Snapshots for all of the volumes within the group at the same time.

Example 2-11 Create a Snapshot group

```
ITSO_2_A9000R>>cg_Snapshots_create cg=itso_cg1
Command run successfully.
```

To get an application crash consistent Snapshot group, first pause I/O from the application before you create the Snapshot. Certain applications can perform this action. In the CLI, you can include commands, such as **`io_pause`** and **`io_resume`**.

You can also create a single volume Snapshot of a volume within a Consistency Group. However, this single volume Snapshot will not be consistent across all of the volumes in the Consistency Group.

2.2.5 Snapshot Groups

Beginning with HSM V5.4, you can now view and perform actions on Snapshot groups. This is accessed from the left side menu options under **Pools & Volumes View** → **Snapshot Groups**. This will display all the Snapshot Groups existing on the system(s) you are filtered for. While this shows all the groups you have created, it will also display internal Snapshot Groups associated with asynchronously mirrored Consistency Groups. An example of this display is shown in Figure 2-51.

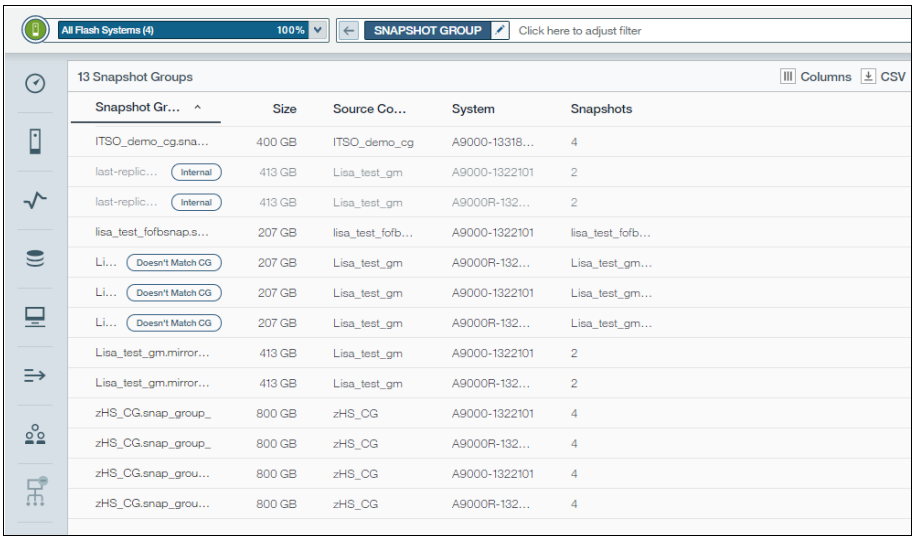


Figure 2-51 Snapshot Groups

You are able to perform actions on the Snapshot Group as well as modify, view the individual Snapshots and delete as shown in Figure 2-52.

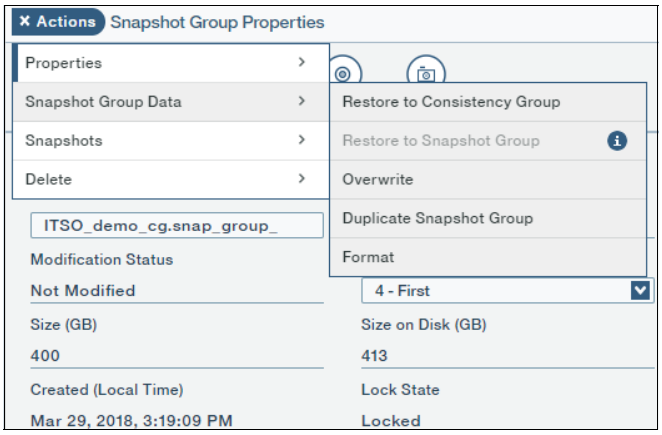


Figure 2-52 Snapshot group action

3

Remote connectivity

Remote system connectivity is the connection between two systems for mirroring or data migration. This chapter provides the information that is required for defining and managing remote target connectivity by using IBM Hyper-Scale Manager and the command-line interface (CLI).

This chapter includes the following sections:

- IBM FlashSystem A9000 and A9000R remote mirror scenarios
- Planning and prerequisites
- Remote mirroring configuration using GUI or CLI

3.1 IBM FlashSystem A9000 and A9000R remote mirror scenarios

The remote system actions that are described in this section are the fundamental building blocks of IBM FlashSystem A9000 and A9000R remote mirroring solutions and usage scenarios.

3.1.1 Defining remote mirror roles

To connect two systems for remote mirroring, each system must be defined to be a mirroring target of the other. This connection and definition allows for either FlashSystem A9000, A9000R, or XIV Gen3 to become the source, which is needed for switching roles. A mirroring target is a FlashSystem A9000, A9000R, or XIV Gen3 with volumes that receive data copied through remote mirroring.

Note: Volumes between a FlashSystem A9000 or A9000R and XIV Gen3 can be mirrored only in an asynchronous manner.

Defining a mirroring target for a FlashSystem A9000, A9000R, or XIV Gen3 involves giving the target a name and specifying whether Fibre Channel (FC) or iSCSI protocol is used to copy the data. For a practical illustration, see 3.3.2, “Remote mirror target configuration through Hyper-Scale Manager” on page 53.

Remote mirroring copies data from a volume on one FlashSystem A9000, A9000R, or XIV Gen3 to a peer on another FlashSystem A9000, A9000R, or XIV Gen3 (that is, the mirroring target system). Whereas the basic underlying mirroring relationship is a one-to-one relationship between two peers, the two mirrored systems can be connected in several ways:

- FlashSystem A9000, A9000R, or XIV Gen3 remote mirror configuration: One-to-one

  The most typical remote mirroring configuration is a one-to-one relationship between a local system (production system) and a remote system (disaster recovery system), as shown in Figure 3-1. This configuration is usually implemented when there is a single production site and a single disaster recovery (DR) site.

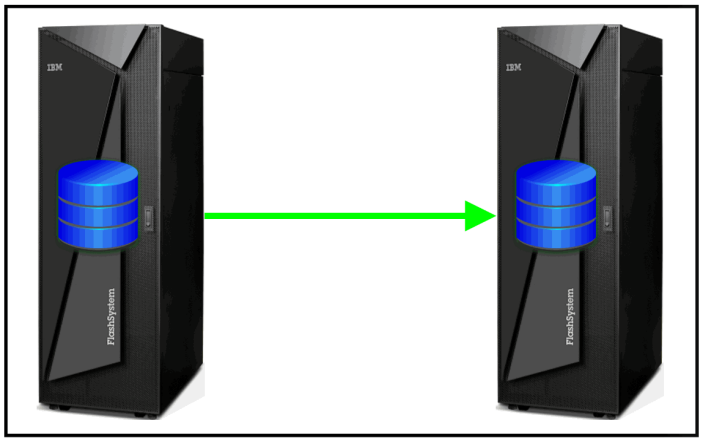


Figure 3-1 One-to-one remote mirror configuration

IBM FlashSystem A9000, A9000R, and XIV Gen3 support both synchronous and asynchronous mirroring (for different mirror couplings) on the same system. A single local FlashSystem A9000 or A9000R can have certain volumes synchronously mirrored to a remote FlashSystem A9000 or A9000R.

Other volumes are asynchronously mirrored to the same remote FlashSystem A9000 or A9000R, as shown in Figure 3-2. Volumes between a FlashSystem A9000 or A9000R and XIV Gen3 can be mirrored only in an asynchronous manner.

Mirroring mode (synchronous or asynchronous) is typically chosen based on the required recovery point objective (RPO) for a given volume, which is the maximal allowed time that the source and target can be unsynchronized. Volumes requiring recovery point objective (RPO) of 0 should be mirrored synchronously. Data that can allow an RPO greater than 0 can be mirrored asynchronously to a remote system.

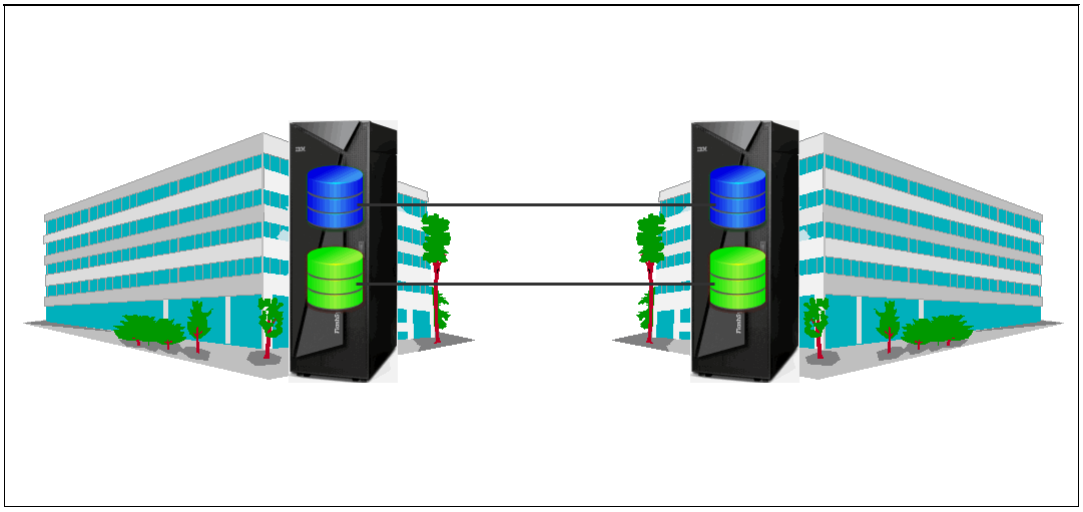


Figure 3-2 Synchronous and asynchronous remote mirror peers

During normal remote mirroring operation, one system (at the DR site) is active as a mirroring target. The other system (at the local production site) is active as a mirroring target only when it becomes available again after an outage, and when changing roles between the production and the DR site. During a failback, data changes made when production is running on the remote (DR) site are copied back to the original production site, as shown in Figure 3-3.

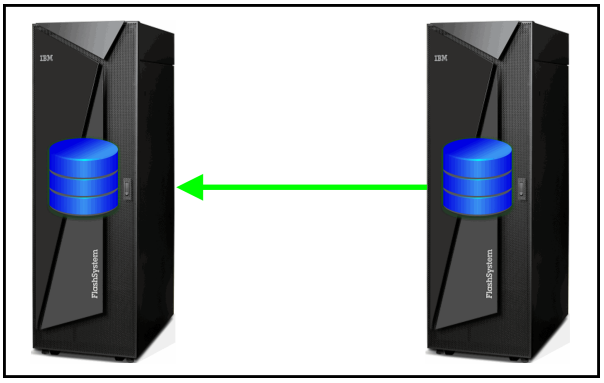


Figure 3-3 Copying changes back to production site

In a configuration with two identically provisioned sites, production might be periodically switched from one site to another as part of normal operation. The FlashSystem A9000, A9000R, or XIV Gen3 system that is the active mirroring target is switched at the same time. The **`mirror_switch_roles`** command allows for switching roles in both synchronous and asynchronous mirroring. There are special requirements for doing so with asynchronous mirroring. See 4.3.1, “Peer designations and roles” on page 73.

- FlashSystem A9000, A9000R, and XIV Gen3 remote mirror configuration: Fan-out

  A single local (production) FlashSystem A9000, A9000R, or XIV Gen3 can be connected to two remote (DR) FlashSystem A9000, A9000R, or XIV Gen3 systems in a fan-out configuration, as shown in Figure 3-4. Both remote systems can be at the same location, or each of the targets can be at a different location. FlashSystem A9000, A9000R, and XIV Gen3 support both synchronous and asynchronous mirroring (for different mirror couplings) on the same system.

  Therefore, a single local FlashSystem A9000 or A9000R can have certain volumes synchronously mirrored to a remote FlashSystem A9000 or A9000R at a metro distance, whereas other volumes are asynchronously mirrored to a remote system at a global distance. Volumes between a FlashSystem A9000 or A9000R and XIV Gen3 can only be mirrored asynchronously. This configuration can be used when data with required RPO of 0 is synchronously mirrored to another system within the metro area, and data with RPO greater than 0 is asynchronously mirrored to a system within or outside the metro area.

  The fan-out configuration is applicable when each system at the DR site has less available capacity than the system at the local site.

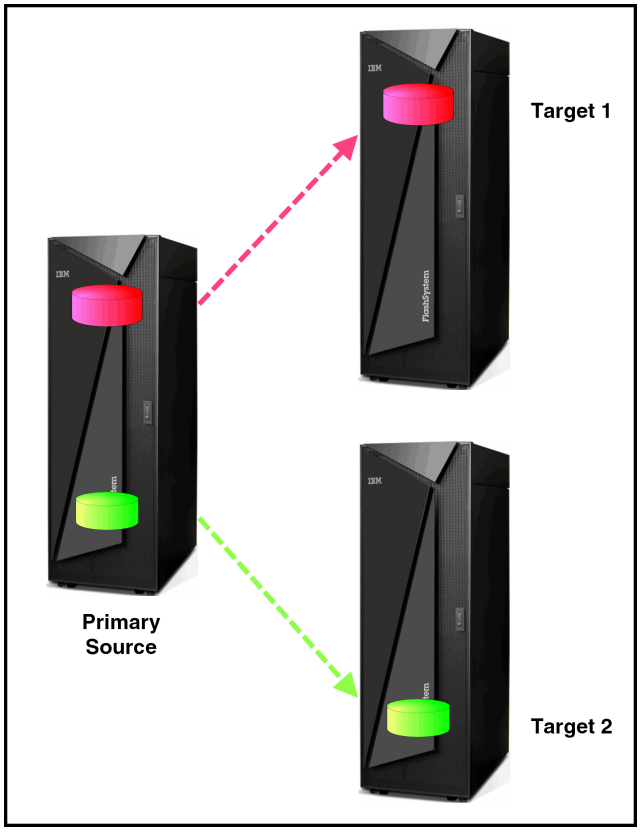


Figure 3-4 Fan-out remote mirror configuration

- FlashSystem A9000, A9000R, and XIV Gen3 remote mirror configuration: Fan-in

  Two or more local FlashSystem A9000, A9000R or XIV Gen3 systems can have peers mirrored to a single remote FlashSystem A9000, A9000R, or XIV Gen3 in a fan-in configuration, as shown in Figure 3-5. This configuration must be evaluated carefully and used with caution, because there is a risk of overloading the single remote system, affecting performance.

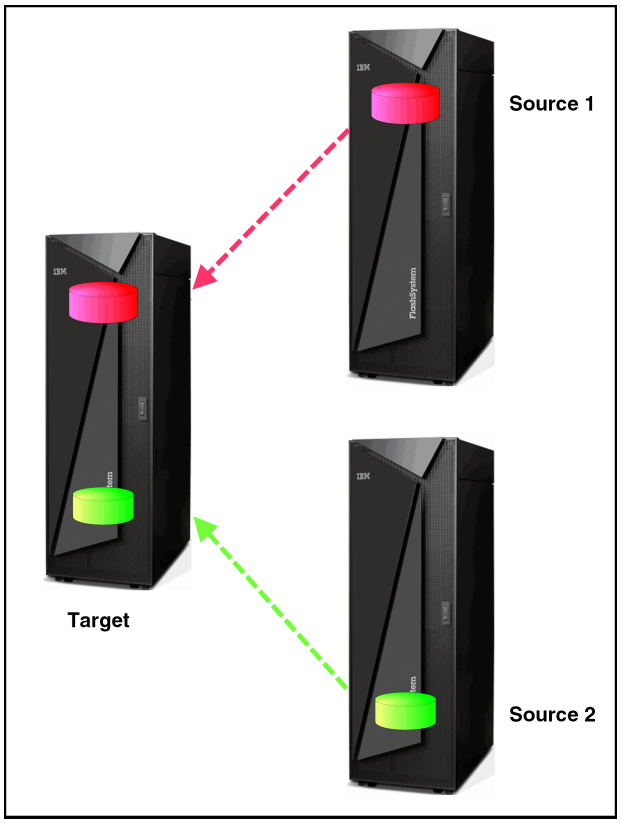


Figure 3-5 Fan-in configuration

  This configuration can be used in situations where there is a single DR data center supporting multiple production data centers. It can also be used when multiple FlashSystem A9000, A9000R, or XIV Gen3 systems are mirrored to a single FlashSystem A9000, A9000R, or XIV Gen3 at a service provider.

- FlashSystem A9000, A9000R, and XIV Gen3 remote mirror configuration: Bidirectional

  Two different FlashSystem A9000, A9000R, or XIV Gen3 systems can have different volumes mirrored in a bidirectional configuration, as shown in Figure 3-6 on page 42. This configuration can be used for situations where there are two active production sites, and each site provides a DR solution for the other. Each FlashSystem A9000, A9000R, or XIV Gen3 is active as a production system for certain peers, and as a mirroring target for other peers.

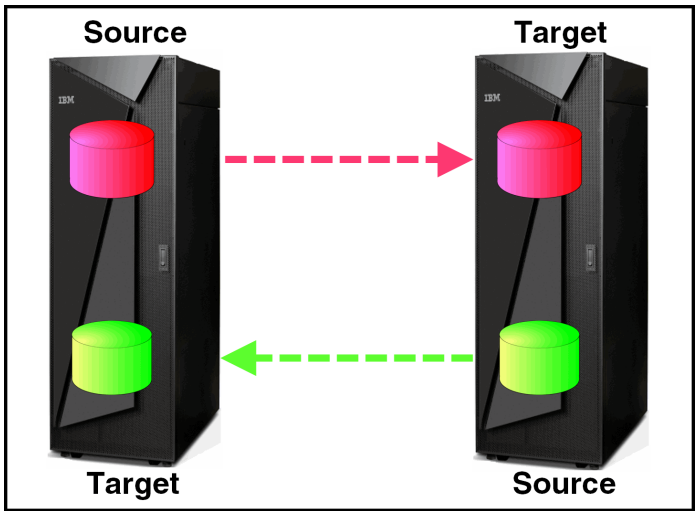


Figure 3-6 Bidirectional configuration

3.1.2 Connecting mirroring ports

After selecting the correct remote mirror scenario and defining which system or systems will be designated as the remote mirror target or targets, one-to-one connections must be made between ports on each FlashSystem A9000, A9000R, or XIV Gen3. For a description of these actions using the Hyper-Scale Manager or the CLI, see 3.3, “Remote mirroring configuration using GUI or CLI” on page 48.

- FC ports

  For the FlashSystem A9000, A9000R, or XIV Gen3 FC ports, connections are unidirectional. An example is a connection from an initiator port (FlashSystem A9000 or A9000R grid controller or XIV Gen3 module Port 4 configured as an FC initiator by default) on the source system to a target port (typically grid controller or module Port 2) on the target system.

  Tip: Use a minimum of four connections (two connections in each direction, from ports in different grid controllers and modules). A minimum of four ports provides availability protection. Using additional ports helps improve performance. We suggest using a minimum of eight ports.

  In Figure 3-7 on page 43, the solid lines represent mirroring connections that are used during normal operation (the mirroring target system is on the right). The dotted lines represent mirroring connections that are used when production is running at the disaster recovery site and changes are being copied back to the original production site (the mirroring target is on the left). FlashSystem A9000, A9000R, and XIV Gen3 FC ports can be easily and dynamically configured as initiator or target ports.

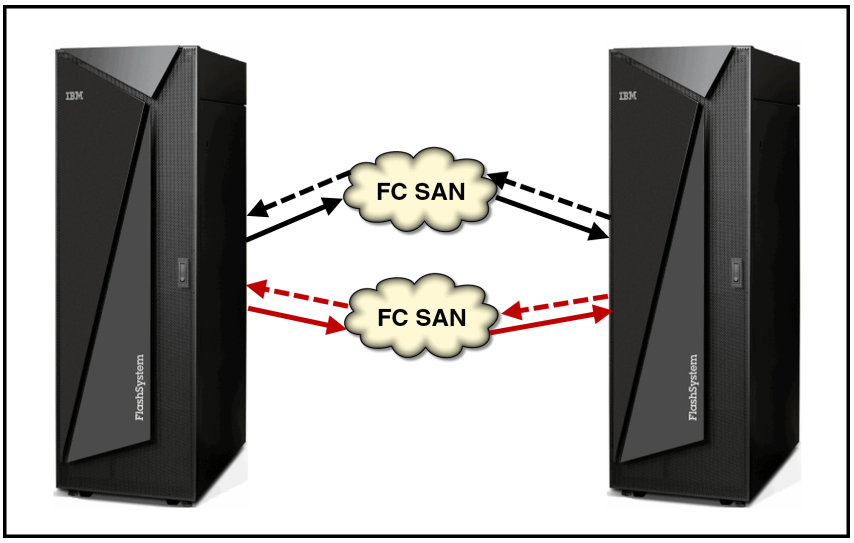


Figure 3-7 Connecting FlashSystem A9000 and A9000R mirroring ports (FC connections)

Note: Each Grid Controller in the FlashSystem A9000 and A9000R is configured with interface ports. Figure 3-8 shows the rear view of a grid controller with feature code 5001 (4 x 16 Gb FC ports + 2 x 10 GbE iSCSI ports). All grid controllers in FlashSystem A9000 or A9000R must have the same feature code.

XIV Gen3 uses a patch panel at the rear of the rack for all external connectivity. The FC ports on the interface modules are connected to the patch panel, and all external connections must be made through it. Figure 3-9 on page 44 shows an example of a patch panel with both FC and either 1 Gb or 10 Gb iSCSI ports.

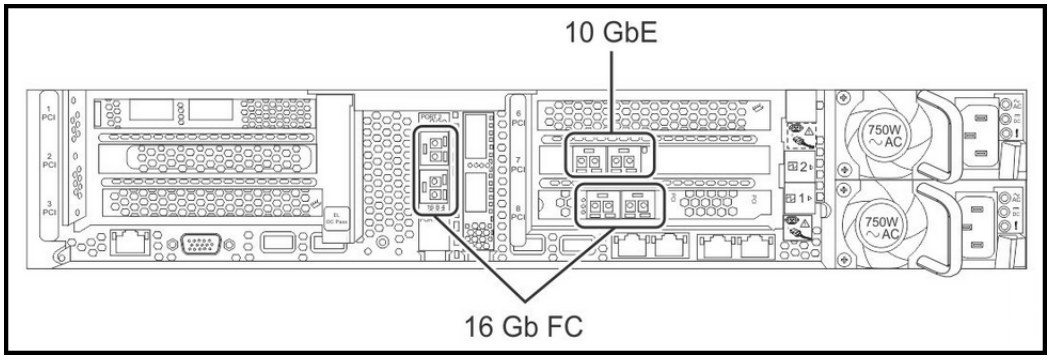


Figure 3-8 FlashSystem A9000 and A9000R grid controller with feature code 5001

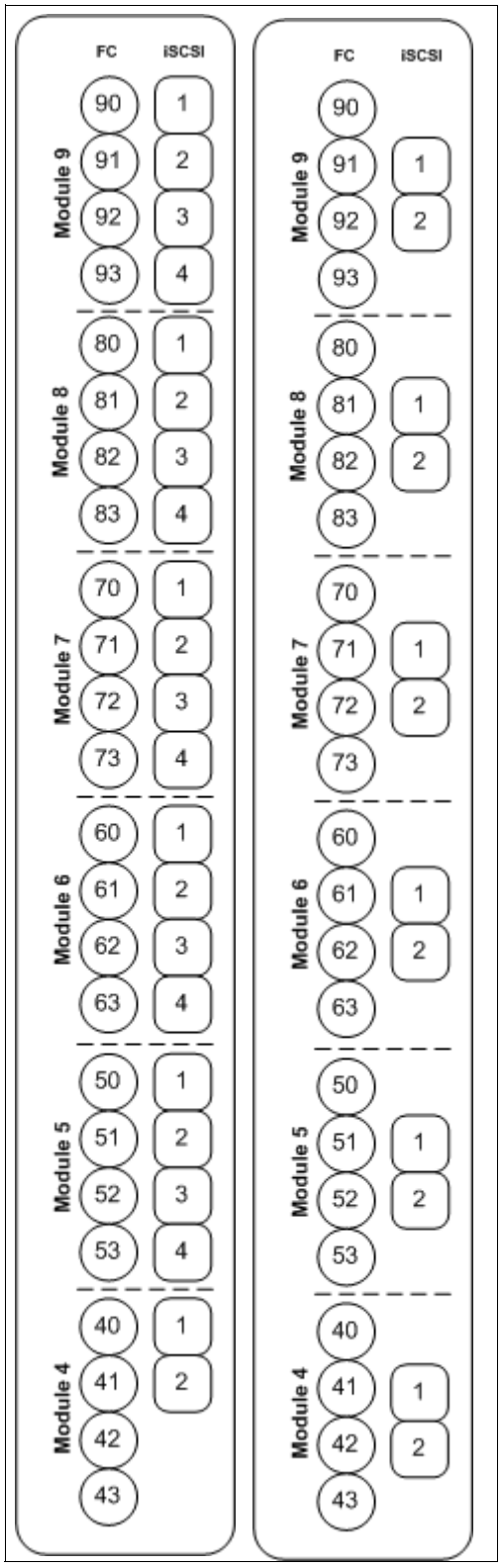


Figure 3-9 XIV Gen3 patch panel with both 1 Gb and 10 Gb iSCSI option

- iSCSI ports

  For iSCSI ports, connections are bidirectional.

Important: If the IP network includes firewalls between the mirrored FlashSystem A9000, A9000R, or XIV Gen3 systems, TCP port 3260 (iSCSI) must be open within firewalls so that iSCSI replication can work.

Tip: Use a minimum of two connections, with each of these ports in a different grid controller or module to provide redundancy. Using additional ports helps improve performance. We suggest using a minimum of four ports.

In Figure 1-10, during normal operation, the data flow starts from the production system (on the left) and goes towards the mirroring target system (on the right). The data flow is reversed when production is running at the disaster recovery site (on the right) and changes are being copied back to the original production site (the mirroring target is on the left).

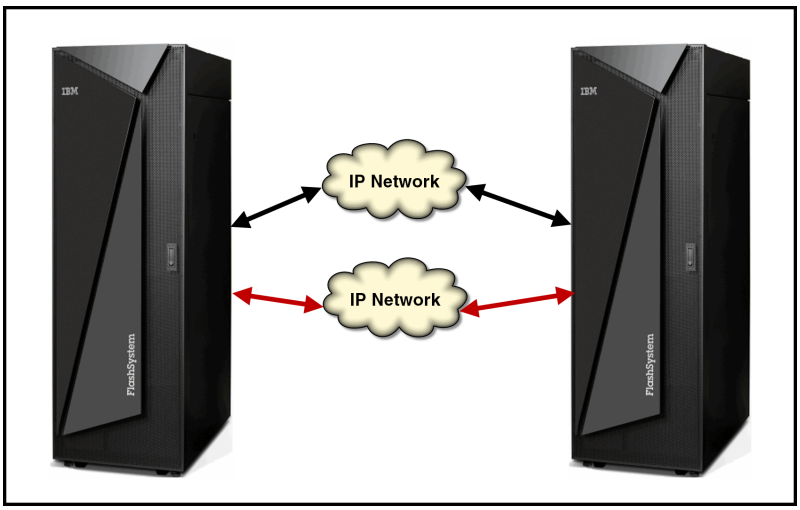


Figure 3-10 Connecting FlashSystem A9000 and A9000R mirroring ports (Ethernet connections)

Note: For asynchronous mirroring over iSCSI links, a reliable, dedicated network must be available. It requires consistent network bandwidth and a non-shared link.

Figure 3-11 shows the rear view of a FlashSystem A9000 and A9000R grid controller with feature code 5002 (4 x 10 GbE iSCSI ports). All grid controllers in FlashSystem A9000 or A9000R must be of the same feature code.

Figure 3-9 on page 44 shows the XIV Gen3 patch panel with both 1 Gb and 10 Gb iSCSI options.

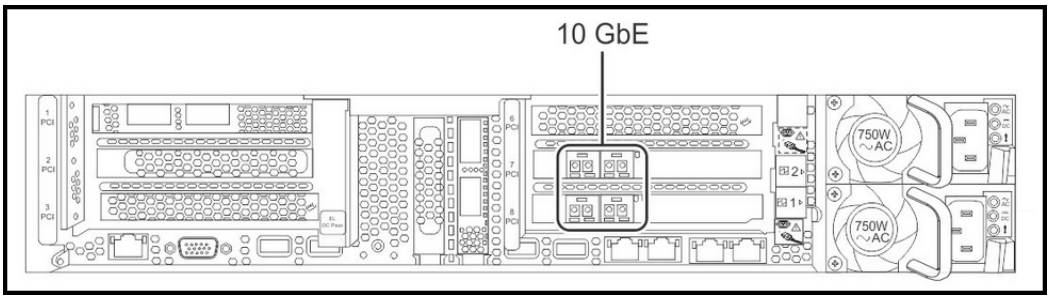


Figure 3-11 FlashSystem A9000 and A9000R grid controller with feature code 5002

3.2 Planning and prerequisites

The most important planning considerations for FlashSystem A9000, A9000R, and XIV Gen3 remote mirroring are those related to ensuring availability and performance of the mirroring or online mobility connections between the systems. Planning for snapshot capacity usage is also important.

To optimize availability, FlashSystem A9000, A9000R, and XIV Gen3 remote mirroring connections must be spread across multiple ports, on different system cards, in different FlashSystem A9000 or A9000R grid controllers and XIV Gen3 modules, and must be connected to different networks. Minimum network bandwidth requirements must be maintained to ensure a stable environment. Adequate bandwidth must also be allocated to ensure that the anticipated amount of changed data can be transported across the network between the systems within the require RPO.

Note: Network bandwidths are typically expressed in megabits per second (Mbps), and disk array bandwidths are expressed in megabytes per second (MBps). Although not exact, a factor of eight between the two gives an acceptable approximation.

3.2.1 Cross-Gen mirroring with XIV Gen3 considerations

For mirroring between FlashSystem A9000 or A9000R and XIV Gen3, the following additional prerequisites should be fulfilled:

- The FlashSystem A9000 or A9000R system is on software 12.2.0 or later.
- The XIV Gen3 system is running software 11.6.2.a or later.
- Volumes that are mirrored between XIV Gen3 and FlashSystem A9000 or A9000R must be decompressed on the XIV Gen3 peer. Mirroring of XIV Gen3 compressed volumes to FlashSystem A9000 or A9000R is not supported.
- Only asynchronous replication is available. All asynchronous mirror functionalities are supported: change mirror, switch role, mirrored snapshots, and so on.
- The volume size in *blocks* must be identical on both systems. Rounding up rules might be different and result in different volume size in GB on the different systems. Remember that volume granularity is 17 GB in XIV Gen3, while it is 1 GB for FlashSystem A9000 and A9000R. A small volume mirrored from FlashSystem A9000 to A9000R could be small in blocks, but will still use at least 17 GB on XIV Gen3. Consequently, mirroring a lot of small volumes can have a substantial impact on the XIV Gen3 usable capacity.
- Maximum volume size that can be mirrored is 161 TiB (an XIV Gen3 limit).
- Maximum consistency group size is 128 volumes.
- All other normal system limitations, such as maximum number of mirrors or targets, apply to cross-gen mirroring.

Note: Remember that mirroring volumes between a FlashSystem A9000 or A9000R and XIV Gen3 is only supported in an asynchronous manner.

When planning for asynchronous mirroring, there are several considerations to be able to handle the I/O load:

- The primary system (source) must be able to handle the host I/O.

- The mirroring connectivity, interval, and sync rate must be sufficient to transfer the modified data within the RPO.
- The secondary system (target) must be able to process the mirrored data.

Hosts typically have limited queue depth, so their I/O rate cannot exceed the rate at which the storage system processes the I/O requests. In asynchronous mirroring, the I/O is acknowledged to the host after the primary system processed it, and before the data is sent to the target and processed there. As a result, the host I/O is limited only by the primary system I/O processing ability.

When the host I/O rate exceeds the ability of the mirror connectivity, we can expect that the rate of data transfer will be slower than the rate of new I/Os. As a result, each synchronization job has more content and therefore takes longer to complete than the last, resulting eventually in an RPO lagging condition (effective RPO being larger than the required one). As time goes on and the synchronization jobs grow, the target falls behind the source and the achieved RPO is much longer than the user-defined one.

If the mirroring connection bandwidth is sufficient but the I/O rate exceeds the ability of the secondary system to process the I/Os, we can expect that the secondary system cache will fill up faster than it can destage the data. Again the RPO will be lagging and the recovery point much further than planned. In this case, in addition to the impact to the mirror, the secondary system performance deteriorates considerably for unrelated I/Os.

When setting up asynchronous mirroring between a FlashSystem A9000 or A9000R system and an XIV Gen3 system, this issue comes to the front because there is a significant difference in the abilities of FlashSystem A9000 or A9000R and XIV Gen3 systems to process I/O. You should note that this setting must be considered for any asynchronous mirror between cross-gen systems, even if initially the XIV Gen3 system is the primary one because a planned maintenance or disaster scenario can lead FlashSystem A9000 or A9000R to assume the primary role.

See 4.5.2, “Cross-Generational Mirroring with XIV Gen3” on page 95 for detailed instructions on how to set up asynchronous replication between XIV Gen3 and FlashSystem A9000 or A9000R

To ensure that the mirror is configured in a balanced way where all the components are able to process the load, the following three mechanisms can be used to control the workload:

- Planning

  The mirror configuration should be planned to ensure that the expected I/O load matches the capabilities of the systems and connectivity.

- Controlling the target sync rate

  Setting a relatively low value to the target sync rate ensures that FlashSystem A9000 or A9000R does not overwhelm the XIV Gen3 system. Alternatively, setting a value too low runs the risk that FlashSystem A9000 or A9000R is not able to transfer all of the modified data to XIV Gen3. This might lead to an RPO lagging state or even an extreme RPO lagging state.

Note: The following value range applies for RPO and sync job interval:

- RPO value can be between a minimum of 1 minute (if using XCLI) or 2 minutes (if using HSM GUI) and a maximum of 24 hours.
- Sync job intervals can be configured between a minimum 30 seconds (if using XCLI) or 60 seconds (if using HSM GUI) and a maximum of 10 minutes. The interval must be less than the RPO.

- Creating a shared quality of service (QoS) performance class for all volumes mirrored to the same XIV Gen3 target

  A QoS performance class limits the I/O the hosts can send to FlashSystem A9000 or A9000R and that must be sent to the XIV Gen3 system. The drawback is that QoS limits all I/O and not just writes that eventually need to be sent to the XIV Gen3 system.

  When setting up the QoS rate, the user must consider the proportion of read I/O to write I/O and set the QoS rate to achieve the wanted write rate. The write rate is an approximation to the rate of data that must be transferred between the mirror peers.

3.2.2 Gross-Gen Mirroring with XIV Gen3 best practices

The following preferred practices are advised for cross-gen asynchronous mirroring with XIV Gen3:

- When configuring the asynchronous mirroring, consider the I/O rate that can be handled by the secondary system, and configure the volumes on the primary system to handle a load that is not generally exceeding this limit. Note that it is not feasible to guarantee that the I/O rate *never* exceeds the limit.
- The target sync rate should be set to a reasonable level. The default setting of the target sync rate (300 MBps) is a valid setting. Increasing from this limit should be done with care. Setting the sync rate can be sufficient to ensure that work load spikes do not overwhelm the secondary system, especially when this is an XIV Gen3 system. If the host workload is normally low, there might be a period of RPO lagging after a spike, but the mirror recovers over time. If the workload is often higher than the limit, the mirror might not have enough time to recover between spikes and the system might get to an extreme RPO lagging state.
- If the host I/O load is too high and the mirror state is RPO lagging with the sync job taking longer and longer to complete, QoS can be used to limit the host I/O rate. This limitation ensures that the host is unable to create a load higher than defined. It also ensures that if the configuration is healthy, the recovery point on the secondary system is within the defined RPO.

  The user should create a shared performance class and add all the volumes mirrored to the same target system to that performance class. The limit of the performance class should be set to limit the write I/O to the target system capability. Because a QoS performance class limits all I/O, the limit should be set depending on the host read/write I/O ratio. For example, if the XIV Gen3 system limit is 300,000 I/O operations per second (IOPS) and the host I/O read/write ratio is 70% reads and 30% writes, the QoS limit y should be:

  $$y = 300{,}000 / 30\% = 300{,}000 * 100/30 = 1{,}000{,}000 \text{ IOPS}$$

Important: The XIV Gen3 system capability depends on the system configuration. A 6-module system can process fewer I/Os than a 15-module system. The limits should be set according to the configuration of the XIV Gen3 system participating in the mirror relation.

3.3 Remote mirroring configuration using GUI or CLI

This section illustrates remote-mirroring definition actions through the Hyper-Scale Manager GUI and the CLI.

3.3.1 Initial setup

When preparing to set up remote mirroring, consider the following questions:

- Will the paths be configured for FC or for iSCSI?
- Is the FC port that you want to use configured as an initiator or a target?
  - Port 4 default configuration is initiator.
  - Port 2 is suggested as the target port for remote mirror links.
  - Port designations can be changed as needed.
- How many mirror pairs will be established?

  FlashSystem A9000 or A9000R supports a maximum of 1536 synchronous volume mirrors and 512 pairs for asynchronous volume mirrors. The write change rate to the source volumes in the mirrored pair relationship dictates the required bandwidth and number of ports needed between sites.
- How many secondary systems will be used for a single primary?

Remote mirroring can be set up on paths that are using SAN-attached FC or iSCSI protocols.

Reminder: If the IP network includes firewalls between the mirrored FlashSystem A9000, A9000R, and XIV Gen3 systems, TCP port 3260 must be open within firewalls so that iSCSI replication can work.

Think about bandwidth considerations when planning the infrastructure to support the remote mirroring implementation. Knowing when the peak write rate occurs for systems attached to the storage helps with the planning for the number of paths needed to support the remote mirroring function and any future growth plans.

When the protocol is selected, determine which ports on FlashSystem A9000, A9000R, or XIV Gen3 are used. The port settings are easily displayed by using the XCLI session environment and the **`fc_port_list`** command for FC or the **`ipinterface_list`** command for iSCSI.

There must always be a minimum of two paths configured within remote mirroring for FC connections, and these paths must be dedicated to remote mirroring. These two paths also must be considered a set. Generally, FC port 4 and FC port 2 in the selected FlashSystems A9000 and A9000R grid controller and XIV Gen3 module are used for this purpose. For redundancy, configure extra sets of paths in different grid controllers and modules.

FC paths for remote mirroring have slightly more requirements for setup (versus iSCSI), which is the method that is described here first.

As Example 3-1 shows in the Role column, each FC port is identified as a target or an initiator. A target in a remote mirror configuration is the port that receives data from the other system, whereas an initiator is the port that sends the data. In this example, five initiators are configured. Initiators, by default, are configured on `1:FC_Port:`*`X`*`:4` (*`X`* is the grid controller or module number). In this example, port 4 on all four grid controllers is configured as an initiator, as is port 3 in grid controller 4.

Example 3-1 The fc_port_list output command

```
A9000R>>fc_port_list
Component ID    Status   Currently Functioning   WWPN               Port ID    Role
1:FC_Port:1:1   OK       yes                     5001738051A60110   007EE680   Target
1:FC_Port:1:2   OK       yes                     5001738051A60111   00011000   Target
1:FC_Port:1:3   OK       yes                     5001738051A60112   00011400   Target
```

```
1:FC_Port:1:4   OK       yes                 5001738051A60113   00042400   Initiator
1:FC_Port:2:1   OK       yes                 5001738051A60120   007FC400   Target
1:FC_Port:2:2   OK       yes                 5001738051A60121   00011100   Target
1:FC_Port:2:3   OK       yes                 5001738051A60122   00011500   Target
1:FC_Port:2:4   OK       yes                 5001738051A60123   00042500   Initiator
1:FC_Port:3:1   OK       yes                 5001738051A60130   00042200   Target
1:FC_Port:3:2   OK       yes                 5001738051A60131   00011200   Target
1:FC_Port:3:3   OK       yes                 5001738051A60132   007FC440   Target
1:FC_Port:3:4   OK       yes                 5001738051A60133   00011600   Initiator
1:FC_Port:4:1   OK       yes                 5001738051A60140   00042300   Target
1:FC_Port:4:2   OK       yes                 5001738051A60141   00011300   Target
1:FC_Port:4:3   OK       yes                 5001738051A60142   007EE6C0   Initiator
1:FC_Port:4:4   OK       yes                 5001738051A60143   00011700   Initiator
```

The iSCSI connections are shown in Example 3-2 using the **`ipinterface_list`** command. The output is truncated to show only the iSCSI connections that are of interest here. The command also displays all other Ethernet connections and settings. In this example, four connections are displayed for iSCSI: One connection in each grid controller.

Example 3-2 The ipinterface_list command

```
A9000R>>ipinterface_list
Name          Type        IP Address      Network Mask    Default Gateway MTU    Module       Port
iSCSI_M1_P1   iSCSI       9.155.116.205   255.255.240.0   9.155.112.1     9000   1:Module:1   1
iSCSI_M2_P1   iSCSI       9.155.116.206   255.255.240.0   9.155.112.1     9000   1:Module:2   1
iSCSI_M3_P1   iSCSI       9.155.116.207   255.255.240.0   9.155.112.1     9000   1:Module:3   1
iSCSI_M4_P1   iSCSI       9.155.116.208   255.255.240.0   9.155.112.1     9000   1:Module:4   1
```

Alternatively, you can query for the existing port settings among the managed FlashSystem A9000, A9000R, and XIV Gen3 systems by selecting a system in the Hyper-Scale Manager, followed by selecting the **System Ports** spoke in the Hub view on the right (Figure 3-12).

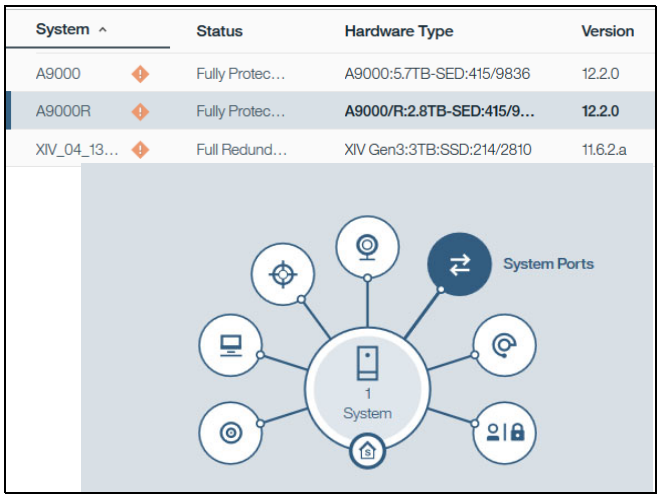


Figure 3-12 Selecting System Ports spoke from the Hyper-Scale Manager Hub View

After selecting the **System Ports** spoke, the ports are displayed beneath the Hub. Figure 3-13 shows some of the ports for FlashSystem A9000R (rack system).

Figure 3-13 Port listing from the System Ports spoke in the Hub view (FlashSystem A9000R)

Click the action menu for a specific port and select **View/Edit**. The output is shown in Figure 3-14. This FC port is configured as a target, as indicated by the radio button on the right.

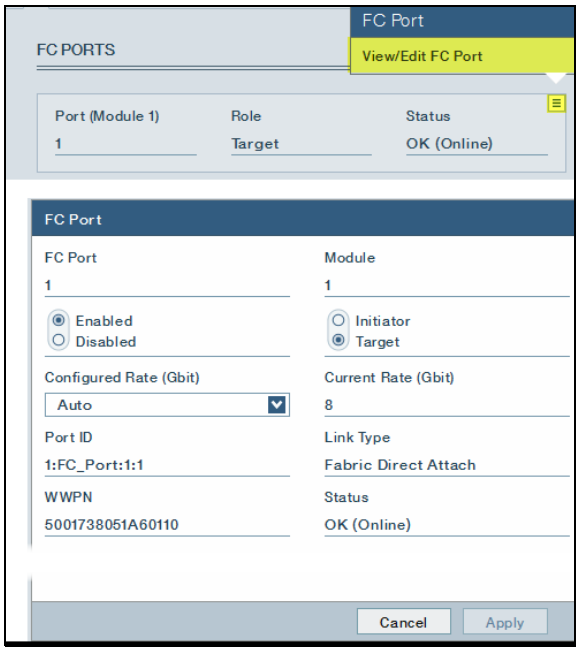


Figure 3-14 FC Port properties displayed with Hyper-Scale Manager

Similar information can be displayed for the iSCSI connections using the Hyper-Scale Manager, as shown in Figure 3-15. This view can be seen by clicking the action menu for an IP Interface and selecting **View/Update IP Interface** (similar to the FC port shown in Figure 3-14 on page 51). This sequence displays the same iSCSI definitions that are shown with the **XCLI ipinterface_list** command.

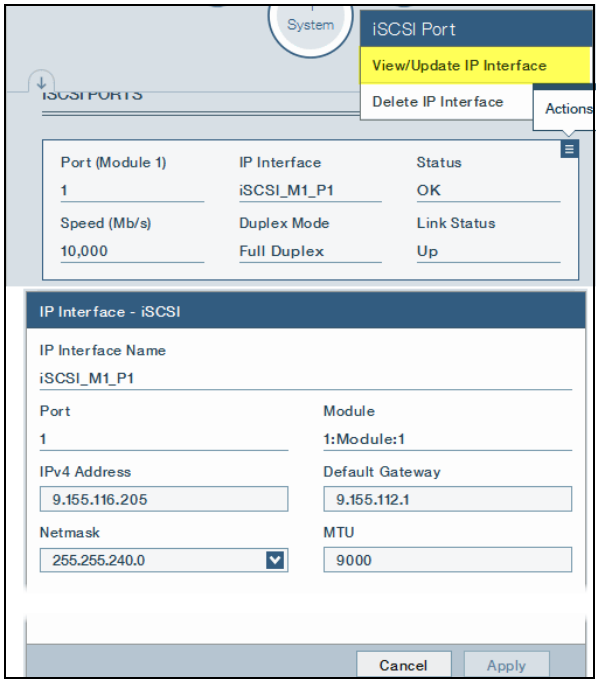


Figure 3-15 iSCSI Port properties displayed with Hyper-Scale Manager

Most commonly, Fibre Channel ports 2 and 4 (target and initiator) from every FlashSystem A9000 or A9000R grid controller and XIV Gen3 module are used for remote mirroring. For example, port 4 in FlashSystem A9000 or A9000R grid controller 3 (initiator) on the local system is connected to port 2 in FlashSystem A9000 or A9000R grid controller 3 (target) on the remote system. XIV Gen3 uses modules 4 - 9 for interface connections, depending on the overall configuration.

When setting up a new system, plan for any remote mirroring and reserve these ports for that purpose. However, different ports can be used if wanted or as needed.

If a port role does need changing, you can change the port role with either the XCLI or the Hyper-Scale Manager.

Use the XCLI **fc_port_config** command to change a port, as shown in Example 3-3. Using the output from **fc_port_list**, you can get the fc_port name to be used in the command, changing the port role to be either initiator or target, as needed.

Example 3-3 XCLI command to configure an FC port

```
A9000R>>fc_port_config fc_port=1:FC_Port:4:3 role=initiator
Command executed successfully.
A9000R>>fc_port_list fcport=1:FC_Port:4:3
Component ID    Status   Currently Functioning   WWPN               Port ID    Role
1:FC_Port:4:3   OK       yes                     5001738051A60142   007EE6C0   Initiator
```

To perform the same function with the Hyper-Scale Manager, select the FC port action menu as shown in Figure 3-14 on page 51, then click **View/Edit FC Port**, which displays the FC port properties, as shown in Figure 3-16.

The settings are displayed and the port can be **Enabled** (or **Disabled**), its role defined as Target or Initiator, and the speed configured. The options are **Auto**, **2**, **4**, **8**, and **16 Gbps**.

After any changes, click **Apply**.

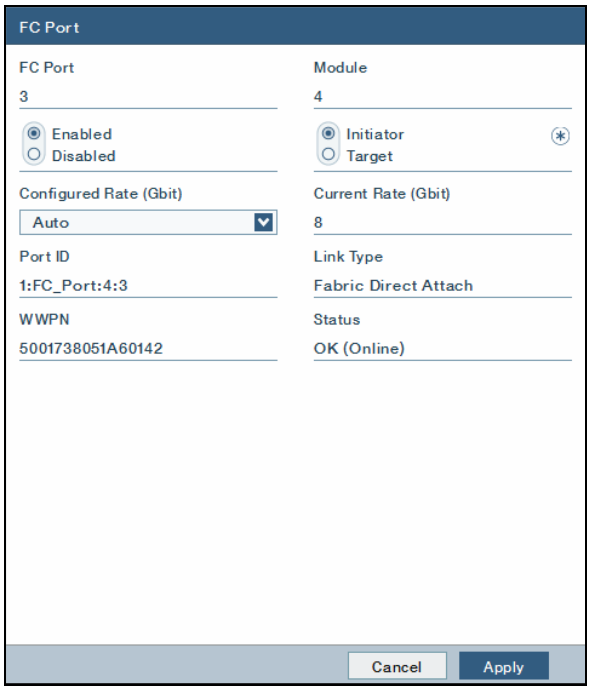


Figure 3-16 Configure FC port with the Hyper-Scale Manager

Note: As iSCSI ports are bidirectional, there is no need to specify a port role. An iSCSI port always acts as both an initiator and a target.

Planning for remote mirroring is important when determining how many mirror pairs will exist. All volumes defined in the system can be mirrored. A single primary system is limited to a maximum of 10 secondary systems.

Volumes cannot be part of a Hyper-Scale Mobility online migration and a remote mirror relationship at the same time. Chapter 7, “Hyper-Scale Mobility” on page 135 describes Hyper-Scale Mobility.

Similarly, volumes cannot be part of a data migration and a remote mirror relationship at the same time. Data migration information is in Chapter 8, “Data migration” on page 171.

3.3.2 Remote mirror target configuration through Hyper-Scale Manager

The connections to the target (secondary) FlashSystem A9000, A9000R, or XIV Gen3 must be defined. The assumption here is that the physical connections and zoning (if using FC) have already been established.

Target configuration is done from the Targets spoke of the Hub display by completing the following steps:

1. Add the target system by selecting the **Targets** spoke from the System Hub display and clicking the plus sign (**+**) to ADD a new target, as shown in Figure 3-17.

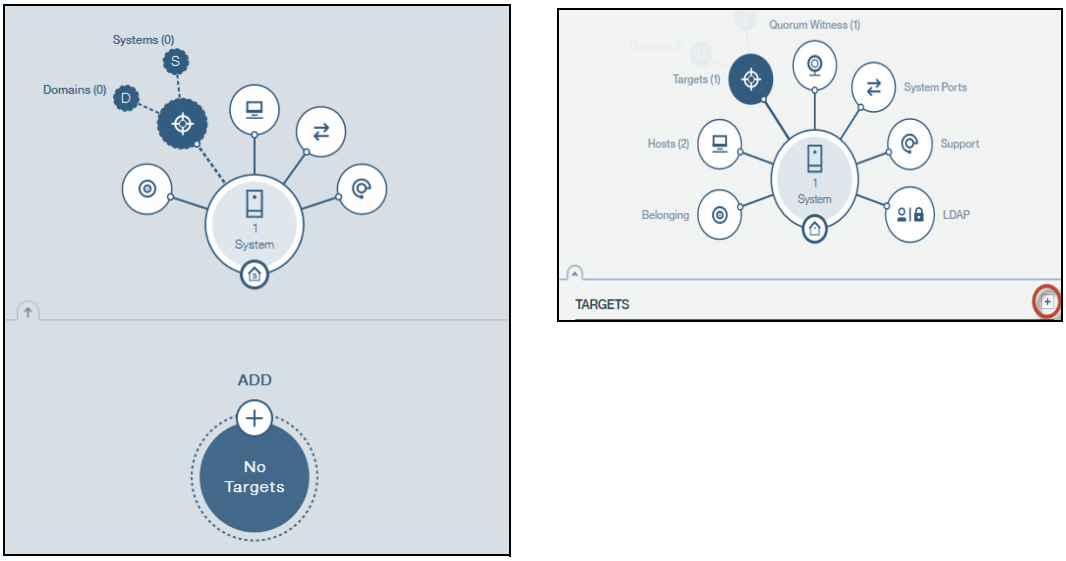


Figure 3-17 Create target

Important: FlashSystem A9000 does not support using more than one mirroring target between two systems in a mirroring relation, or in IBM Hyper-Scale Mobility, because it can compromise the data on the destination.

The Hyper-Scale Manager (assuming it has a connection to the systems involved) prevents you from defining more than one target between two systems.

Depending on the version that you use, the CLI might not prevent that action or give you a warning.

2. Select the Remote System from the drop-down box, select the Remote Domain, define the type of connectivity to be used (**Mirroring** or **Migration**) and select the protocol (**iSCSI** or **FC**), as shown in Figure 3-18.

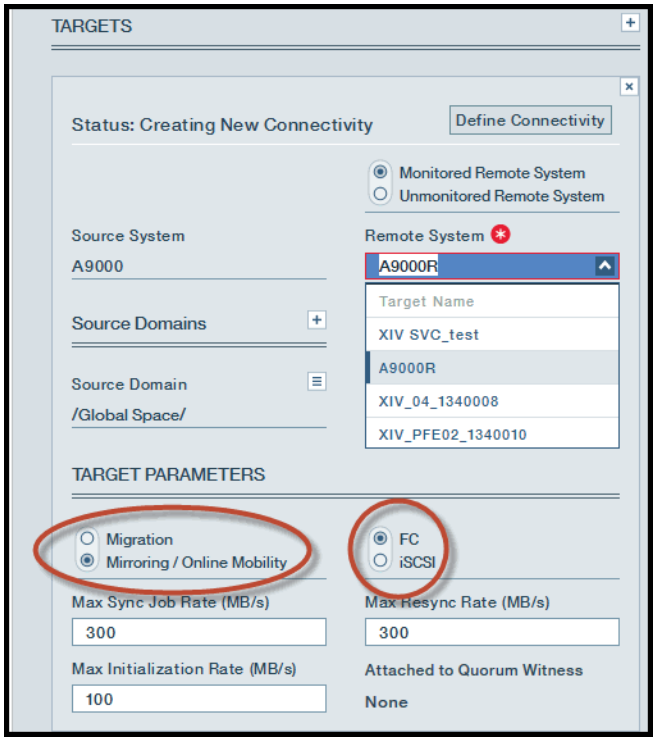


Figure 3-18 Target type and protocol

If you select **iSCSI** for the target connection, also provide the **iSCSI Name**. If the target is monitored by the Hyper-Scale Manager, the iSCSI Name is completed automatically, as shown in Figure 3-19.

Figure 3-19 iSCSI Target Parameters

3. Optionally, modify the **Max Sync Job Rate**, **Max Resync Rate**, and **Max Initialization Rate**.

   FlashSystem A9000, A9000R, and XIV Gen3 allow an adjustable maximum rate (in MBps) for remote mirroring coupling initialization, a different adjustable maximum rate for normal sync jobs, and another for resynchronization.

   The initialization rate, sync job rate, and resynchronization rate are specified for each mirroring target by using the XCLI **`target_config_sync_rates`** command or through the Hyper-Scale Manager, as shown in Figure 3-20 on page 57. These rates are used in order to prevent a situation where synchronization utilizes too much of the system's or of the communication line's resources.

   The actual effective initialization or synchronization rate also depends on the number and speed of connections between the systems. The maximum initialization rate must be less than or equal to the maximum sync job rate (asynchronous mirroring only), which must be less than or equal to the maximum resynchronization rate.

   Important: In normal mirror operations, the rates are cumulative. For example, if initialization, synchronous, and asynchronous operations are all active, the amount of data that the system attempts to send is the sum of those three values.

   The defaults are as follows:

   – Maximum initialization rate: 100 MBps
   – Maximum sync job: 300 MBps
   – Maximum resync rate: 300 MBps

4. Click **Apply,** as shown in Figure 3-20, to create the new Target.

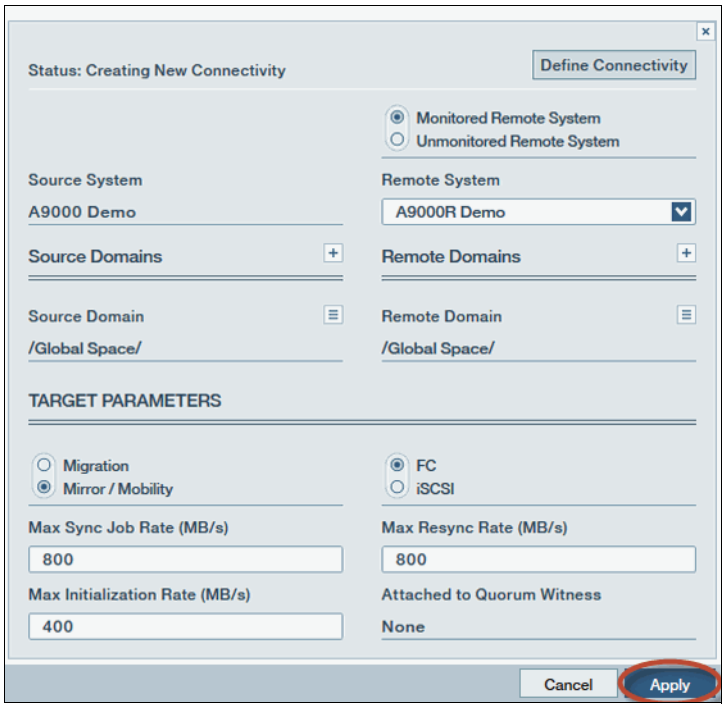


Figure 3-20 Click Apply to create Target

5. As shown in Figure 3-21, define connections by clicking **Define Connectivity** in the Targets window to open the detail window.

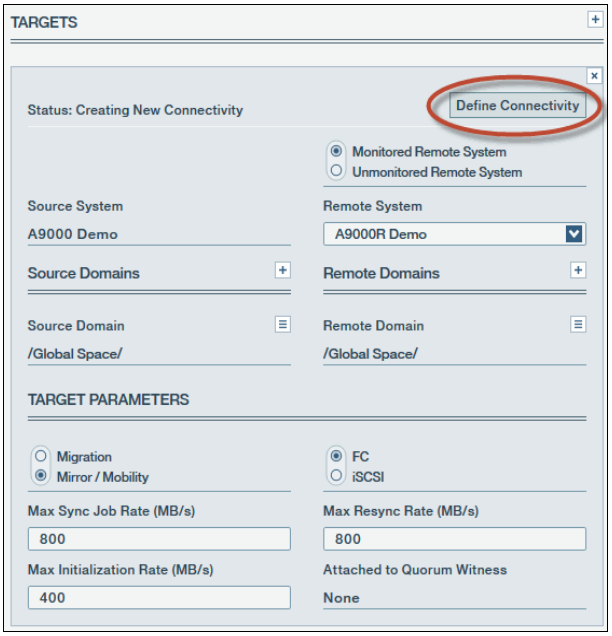


Figure 3-21 Define connectivity

Connections are easily defined by clicking **Auto Connect**. For FC ports, remember that an initiator must be connected to a target, and the proper zoning must be established, for the connections to be successful (as shown in Figure 3-22).

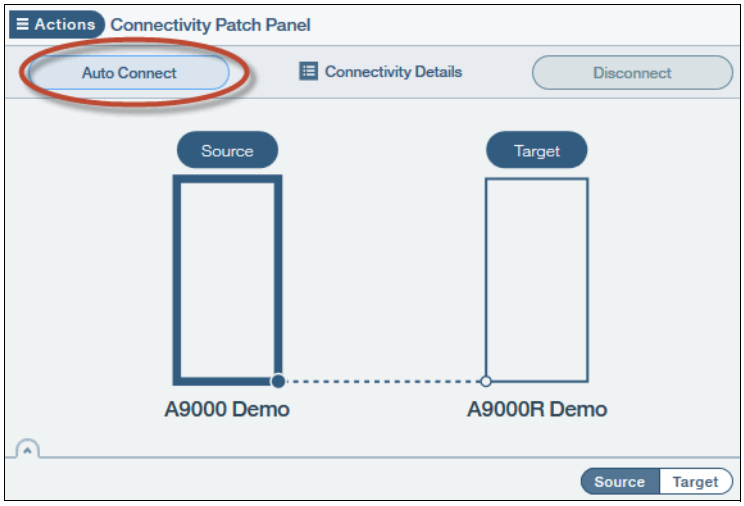


Figure 3-22 Define Connectivity Detail Display

When completed, the Source to Target connection in the diagram displays changes from a dashed line to a solid line with a check mark, as depicted in Figure 3-23.

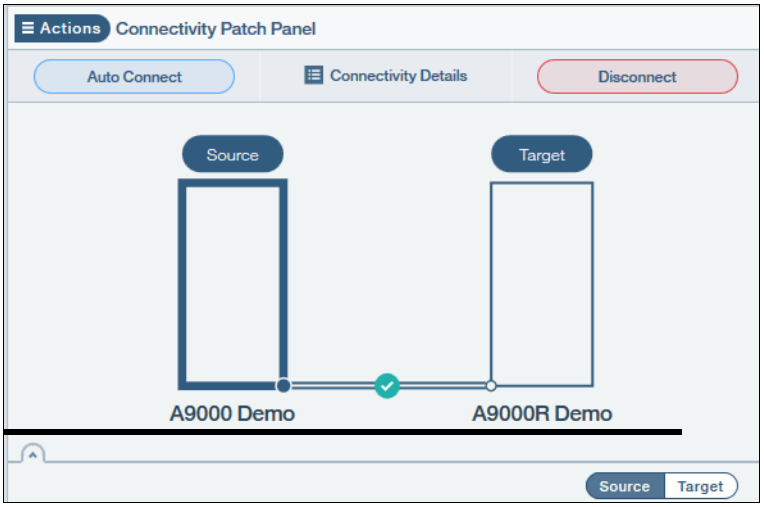


Figure 3-23 Connectivity Patch Panel window after Auto Connect

6. Click **Connectivity Details** to open the Connectivity Patch Panel window that shows the active connections between Source and Target, as shown in Figure 3-24. This example shows FC connections.

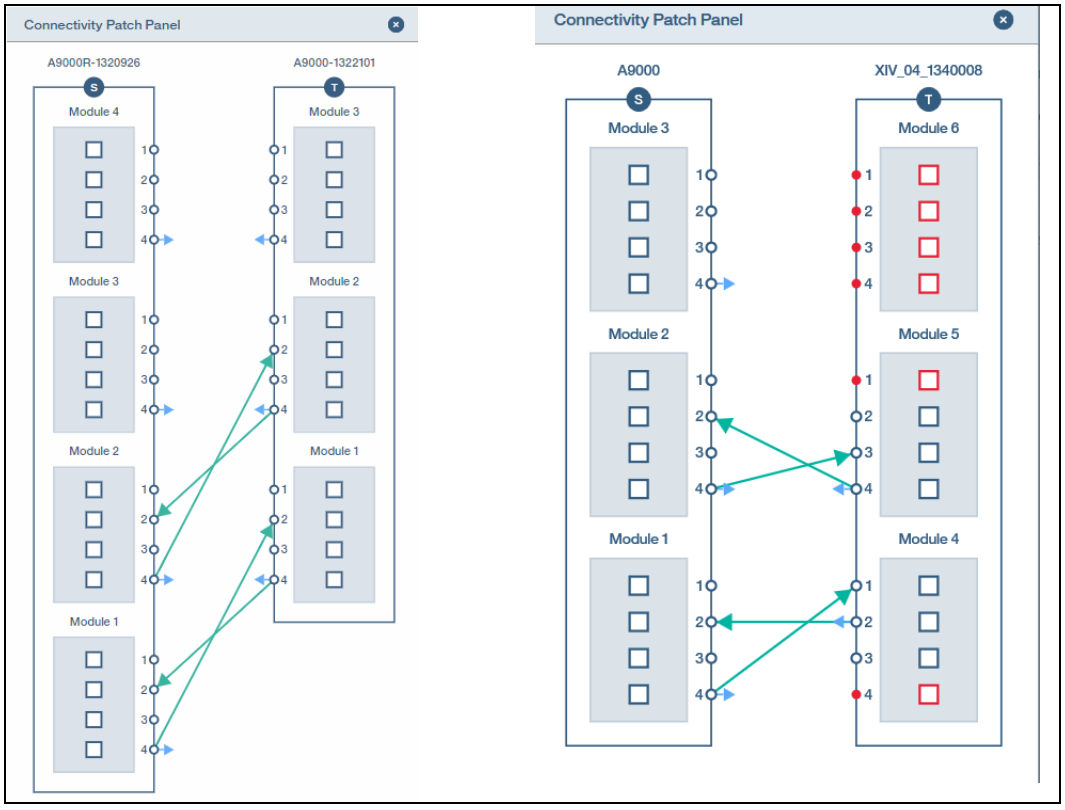


Figure 3-24 Connectivity Patch Panel (FC) in Hyper-Scale Manager between FlashSystem A9000 and A9000R on the left and FlashSystem A9000 and XIV Gen3 on the right

Note: The connectivity shown in Figure 1-24 (right side) is an example of FC connections and is not intended to reflect connectivity best practices. As previously stated, the preferred practice is to use ports 2 and 4 for replication, which leaves port 1 and 3 available for host use.

Similarly, Figure 3-25 shows the auto-connected Source and Target connections for an iSCSI-connected mirroring target system.

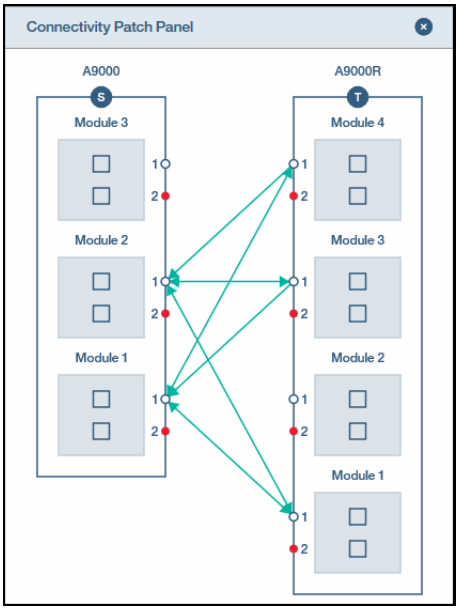


Figure 3-25 Connectivity Patch Panel (iSCSI) in Hyper-Scale Manager

Note: The connectivity shown in Figure 3-25 is an example of iSCSI connections, and is *not* intended to reflect best practice connectivity.

To delete the connections between two mirrored systems, complete the following steps:

1. Click **Disconnect** in the Connectivity Patch Panel window, as shown in Figure 3-26, and click **Apply** in the resulting confirmation window.

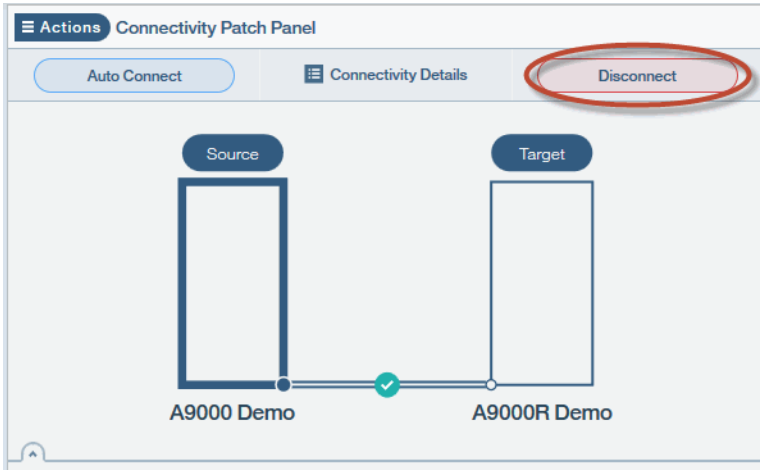


Figure 3-26 Target Connectivity Disconnect

2. From the **Targets** spoke in the Systems Hub display, click the **Actions** menu and select **Remove Target**, as shown in Figure 3-27. Click **Apply** in the resulting confirmation window.

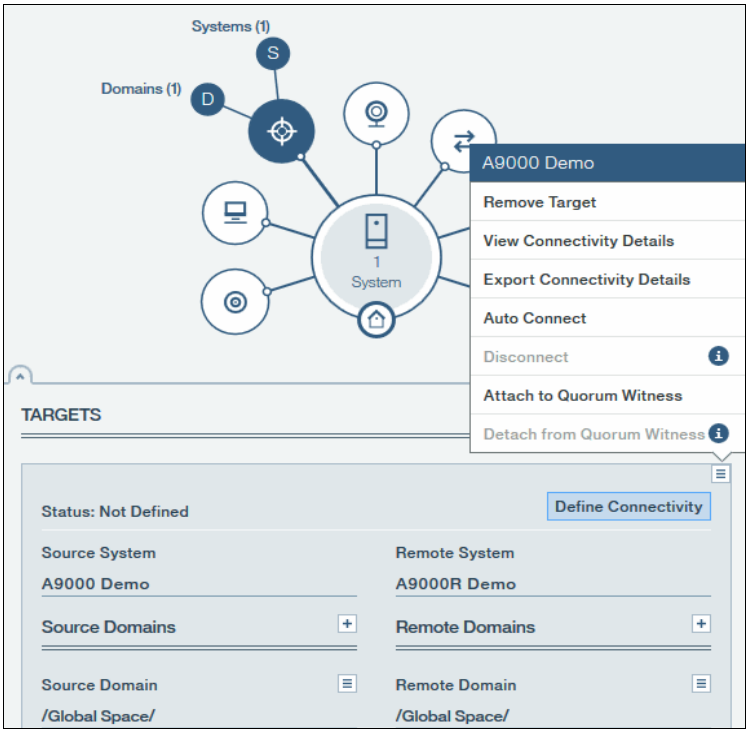


Figure 3-27 Remove Target (links have already been removed)

3.3.3 CLI examples

The following **CLI** commands can be used to configure connectivity between the primary FlashSystem A9000, A9000R, or XIV Gen3 and the target or secondary FlashSystem A9000, A9000R, or XIV Gen3 (Example 3-4):

- **target_define**
- **target_list**
- **target_mirroring_allow**
- **target_config_sync_rates**
- **target_port_add**
- **target_port_list**
- **target_connectivity_define**
- **target_connectivity_list**

Example 3-4 Define Target CLI commands

Source:

```
A9000>>target_define target="A9000R" protocol=FC
A9000>>target_list
Name     SCSI Type   Connected   Max Initialization Rate   Max Resync Rate   Max Syncjob Rate
A9000R   FC          no          100                       300               300
A9000>>target_mirroring_allow target=A9000R
A9000>>target_config_sync_rates target="A9000R" max_initialization_rate=400 max_resync_rate=800
max_syncjob_rate=800
A9000>>target_list
```

```
Name     SCSI Type   Connected   Max Initialization Rate   Max Resync Rate   Max Syncjob Rate
A9000R   FC          no          400                       800               800
A9000>>target_port_add target=A9000R fcaddress=5001738051A60142
A9000>>target_port_add target=A9000R fcaddress=5001738051A60120
A9000>>target_port_add target=A9000R fcaddress=5001738051A60132
A9000>>target_port_list
Target Name   Port Type   Active   WWPN               iSCSI Address   iSCSI Port
A9000R        FC          yes      5001738051A60142                   0
A9000R        FC          yes      5001738051A60120                   0
A9000R        FC          yes      5001738051A60132                   0
A9000>>target_connectivity_define target="A9000R" fcaddress=5001738051A60132
local_port=1:FC_Port:1:4
A9000>>target_connectivity_define target="A9000R" fcaddress=5001738051A60120
local_port=1:FC_Port:3:4
A9000>>target_connectivity_list
Target Name   Remote Port        FC Port         IP Interface   Active   Up
A9000R        5001738051A60132   1:FC_Port:1:4                  yes      yes
A9000R        5001738051A60120   1:FC_Port:3:4                  yes      yes
```

Target:

```
A9000R>>target_define target="A9000" protocol=FC system_id=22131

Warning:   Defining more than one target to the same remote system is not supported, and may
compromise the data on the slave system. Are you sure the remote system is not already defined
as a target? y/n: y
A9000R>>target_list
Name         SCSI Type   Connected   Max Initialization Rate   Max Resync Rate   Max Syncjob
Rate
A9000        FC          no          100                       300               300
A9000R>>target_mirroring_allow target=A9000
A9000R>>target_config_sync_rates target="A9000" max_initialization_rate=400 max_resync_rate=800
max_syncjob_rate=800
A9000R>>target_list
Name         SCSI Type   Connected   Max Initialization Rate   Max Resync Rate   Max Syncjob
Rate
A9000        FC          no          400                       800               800
A9000R>>target_mirroring_allow target=A9000
A9000R>>target_port_add target="A9000" fcaddress=5001738056730133
A9000R>>target_port_add target="A9000" fcaddress=5001738056730131
A9000R>>target_port_add target="A9000" fcaddress=5001738056730113
A9000R>>target_port_list
Target Name   Port Type   Active   WWPN               iSCSI Address   iSCSI Port
A9000         FC          yes      5001738056730133                   0
A9000         FC          yes      5001738056730131                   0
A9000         FC          yes      5001738056730113                   0
A9000R>>target_connectivity_define target="A9000" fcaddress=5001738056730131
local_port=1:FC_Port:4:3
A9000R>>target_connectivity_list
Target Name   Remote Port        FC Port         IP Interface   Active   Up
A9000         5001738056730131   1:FC_Port:4:3                  yes      yes
```

Similarly, the XCLI **target_connectivity_delete**, **target_port_delete**, and **target_delete** commands can be used to delete the connectivity between the primary FlashSystem A9000, A9000R, or XIV Gen3 and the secondary FlashSystem A9000, A9000R, or XIV Gen3, as shown in Example 3-5.

Example 3-5 Delete Target CLI commands

```
Source:
A9000>>target_connectivity_delete target="A9000R" fcaddress=5001738051A60132 local_port=1:FC_Port:1:4
A9000>>target_connectivity_delete target="A9000R" fcaddress=5001738051A6012O local_port=1:FC_Port:3:4
A9000>>target_port_delete target="A9000R" fcaddress=5001738051A60142
A9000>>target_port_delete target="A9000R" fcaddress=5001738051A60120
A9000>>target_port_delete target="A9000R" fcaddress=5001738051A60132
A9000>>target_delete target="A9000R"

Target:
A9000R>>target_connectivity_delete target="A9000" fcaddress=5001738056730131 local_port=1:FC_Port:4:3
A9000R>>target_port_delete target="A9000" fcaddress=5001738056730133
A9000R>>target_port_delete target="A9000" fcaddress=5001738056730131
A9000R>>target_port_delete target="A9000" fcaddress=5001738056730113
A9000R>>target_delete target="A9000"
```

4

Remote mirroring

The remote mirroring function provides a real-time copy between two or more IBM FlashSystem A9000 and A9000R systems, or asynchronously with an XIV Gen3. This feature provides a method to protect data from site failures.

New features:

IBM FlashSystem A9000 and A9000R running code 12.2 or later can use cross-generational asynchronous mirroring with XIV Gen3 systems running code 11.6.2.a or later.

With software V12.2.1, the maximum number of mirroring pairs is raised to 3072 for synchronous mirroring and 1024 for asynchronous mirroring

This chapter includes the following sections:

- Mirroring overview
- Boundaries
- Mirroring schemes
- Remote mirroring configurations
- Using remote mirroring
- Migrating data by using remote mirroring
- Recovering from a site failure
- Deleting mirror coupling definitions
- Recovery from a temporary site outage
- Temporary deactivation of mirroring

4.1 Mirroring overview

Mirroring creates a set of consistent data that can be used when there are problems with the production volumes. It can also be used for other purposes such as testing and backup on the remote site using snapshots of consistent data.

Remote mirroring is independent of applications and operating systems, and does not require host-processor cycle usage.

Remote mirroring can be a synchronous copy solution whereby a write operation is completed onto both copies (local and remote sites) before an acknowledgment is returned to the host that issued the write. This type of remote mirroring is typically used for geographically close sites to minimize the effect of I/O delays, which are proportional to the distance between the sites.

Remote mirroring can also be an asynchronous solution. This solution type is similar to above, but differs with the consistent sets of data being copied to the remote location at predefined intervals at the same time the host I/O operations are acknowledged directly after they are written on the primary site alone. This configuration is typically used for longer distances and latencies, between sites.

Note: A reliable, dedicated network bandwidth is preferred for mirroring. Links can be shared, but require available and consistent network bandwidth. The specified minimum bandwidth (50 Mbps for iSCSI) is a functional minimum and might not meet the replication speed that is required for a customer environment and workload.

Also, minimum bandwidths are *not* time-averaged, as typically reported by network monitoring packages. They are instantaneous, constant requirements, typically achievable only through network quality of service (QoS).

Unless otherwise noted, this chapter describes the basic concepts, functions, and terms that are common to both synchronous and asynchronous mirroring available with IBM FlashSystem A9000 and A9000R.

The following list defines the mirroring-related terms that are used in this document:

- Local site: This site consists of the primary storage system and the servers running applications that are stored on that storage system. The local site normally has the role of production site.
- Remote site: This site holds the mirror copy of the data and usually also has standby servers. The remote site has normally the role of Disaster Recovery (DR). A remote site can become the active production site using a consistent data copy.
- Primary System: This term denotes the FlashSystem A9000, A9000R, or XIV Gen3 system used for production, during typical business workloads, to serve hosts and have its data replicated to a secondary FlashSystem A9000, A9000R, or XIV Gen3. You might also refer to it as the source system.
- Secondary System: This term denotes the FlashSystem A9000, A9000R, or XIV Gen3 system used during normal circumstances to act as the mirror (backup) for the primary system. You might also refer to it as the target system.
- Consistency group (CG): This is a set of related volumes on a single system that are treated as one logical unit. Thus, all CG data reflects correctly ordered writes across all respective volumes within the CGs. Consistency groups are supported within remote mirroring.

- Coupling: This is the pairing of volumes or CGs, between the primary system (source) and secondary system (target), to form a mirror relationship.
- Peer: This is one side of a coupling. It can be either a volume or a consistency group. However, peers must be of the same type (that is, both volumes or both CGs). Whenever a coupling is defined, a role is specified for each peer. One peer is designated as the source and the other peer is designated as the target.
- Role: This term denotes the actual role that the peer is fulfilling:
  - Primary Role: A role that indicates that the peer serves host requests and acts as the source for replication.
  - Secondary Role: A role that indicates that the peer does not serve host write requests (it can be used in read-only mode) and acts as the target for replication.

  Changing a peer's role might be necessary after the peer is recovered from a site or system failure, or due to a link failure or disruption.
- Designation: This term denotes the preferred role that the peer is to fulfill. This is seen in the GUI under a volume or CG Availability Role column when the roles are switched, for example: **Primary (not as designated)** or **Secondary (not as designated)**.
- Sync job: This term applies to asynchronous mirroring only. It denotes a synchronization procedure that is run by the source storage system at user-configured time intervals corresponding to the asynchronous mirroring definition. Alternatively, it is run on manual execution of the XCLI command **`mirror_create_snapshot`**, which is also used for synchronous mirroring, but not as part of a scheduled job.

  The resulting job is referred to as snapshot mirror sync job, ad hoc sync job, or manual sync job in contrast with a scheduled sync job. The sync job entails synchronization of data updates recorded on the source since the creation time of the most-recent snapshot that was successfully synchronized.
- Offline initialization (offline init): A mechanism whereby FlashSystem A9000 and FlashSystem A9000R, using HASH values, compares respective source and target 64 KB data blocks. It then copies over only the parts that have different data. Offline initialization expedites the synchronization of mirror pairs that are known to be inherently similar (for example, when an asynchronous pair is changed to a synchronous pair).

  This feature of FlashSystem A9000 and FlashSystem A9000R can be used when the data links do not have adequate speed or capacity to transmit the entire volume in a timely fashion. In that case, the pair is first created when the systems are at close proximity and can use fast links. Then, when the storage system that hosts the remote mirror is placed at its final physical destination, only the changed data since those volumes were identical must be copied over the wire.
- Asynchronous schedule interval: This term applies only to asynchronous mirroring. It represents how often the source automatically runs a new sync job. The default interval and the minimum possible is 20 seconds.
- Recovery point objective (RPO): The RPO is a setting that is applicable to asynchronous mirroring. It represents an objective set by the user, implying the maximal time difference considered acceptable between the mirror peers (the actual difference between mirror peers can be shorter or longer than the RPO set).

  An RPO of zero indicates that no difference between the mirror peers can be tolerated, and that implies that sync mirroring is required. An RPO that is greater than zero indicates that the replicated volume is less current or lags somewhat behind the source volume. In this case, there is a potential for certain transactions that have been run against the production volume to be rerun when applications start to use the replicated volume.

For asynchronous mirroring, the required RPO is user-specified. The storage system then reports effective RPO and compares it to the required RPO.

Connectivity, bandwidth, and distance between the systems directly impact RPO. More connectivity, greater bandwidth, and less distance typically enable a lower RPO.

4.1.1 Remote mirroring modes

As mentioned earlier, FlashSystem A9000 and A9000R supports both synchronous mirroring and asynchronous mirroring:

- Synchronous mirroring

  Synchronous mirroring is designed to accommodate a requirement for zero RPO.

  To ensure that primary system (also referred to as source) data is also written to the secondary system (also referred to as target), an acknowledgment of the write operation to the host is issued only after the data is written to both storage systems. This process ensures that mirroring peers always contain the same data. This configuration is depicted in Figure 4-1.

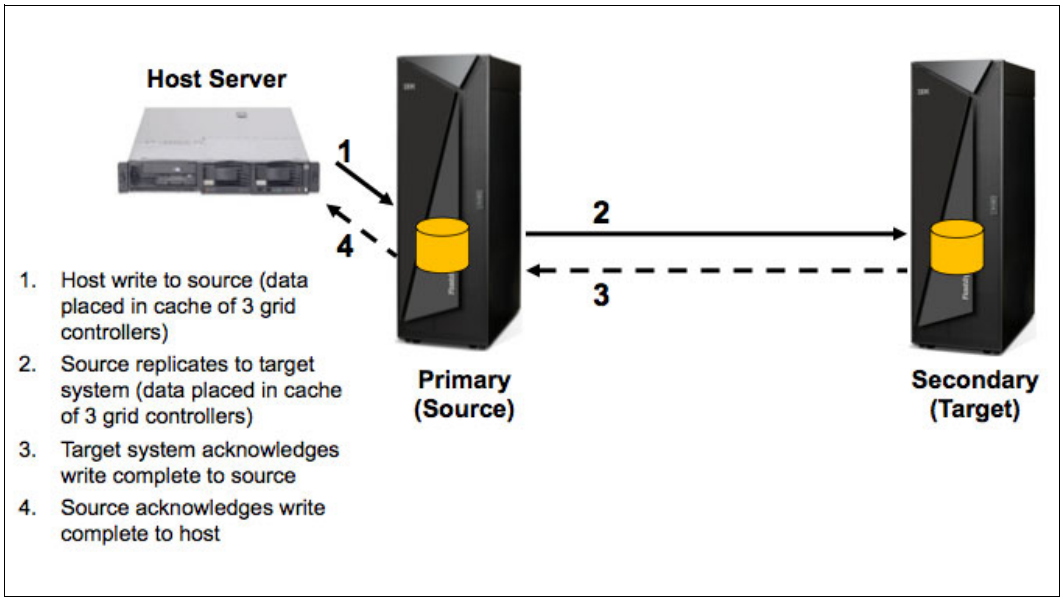


Figure 4-1 Synchronous mirroring

Host read operations are handled by the primary (source), whereas writing is handled at the primary (source) and replicated to the secondary (target) systems.

- Asynchronous mirroring

  Asynchronous mirroring is designed to provide a consistent replica of data on a target peer through timely replication of data changes recorded on a source peer.

  Asynchronous mirroring uses the snapshot function, which creates a point-in-time image. In asynchronous mirroring, successive snapshots (point-in-time images) are made and used to create consistent data on the target peers. The system sync job copies the data corresponding to the differences between two designated snapshots on the source (most-recent and last-replicated).

  For asynchronous mirroring, acknowledgment of *write complete* is returned to the host as soon as the write data is received at the local storage system, as shown in Figure 4-2 on page 69.

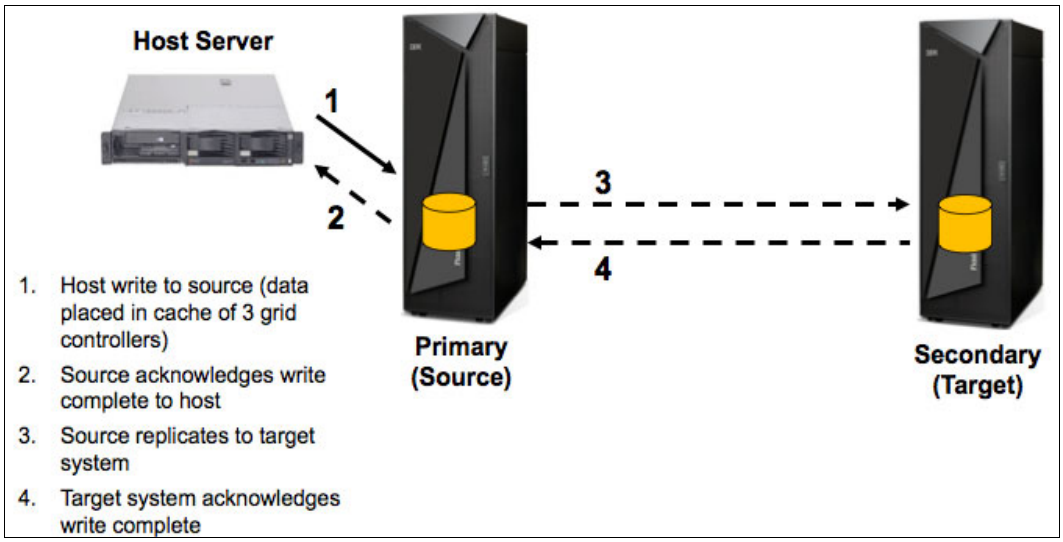


Figure 4-2 Asynchronous mirroring

- HyperSwap

  HyperSwap is designed to automatically and transparently switch between primary and secondary roles, and have the read/write permission assignments depending on their automated role (primary or secondary), based on the failover situation and state. Figure 4-3 illustrates a simple example of a HyperSwap configuration during normal operations.

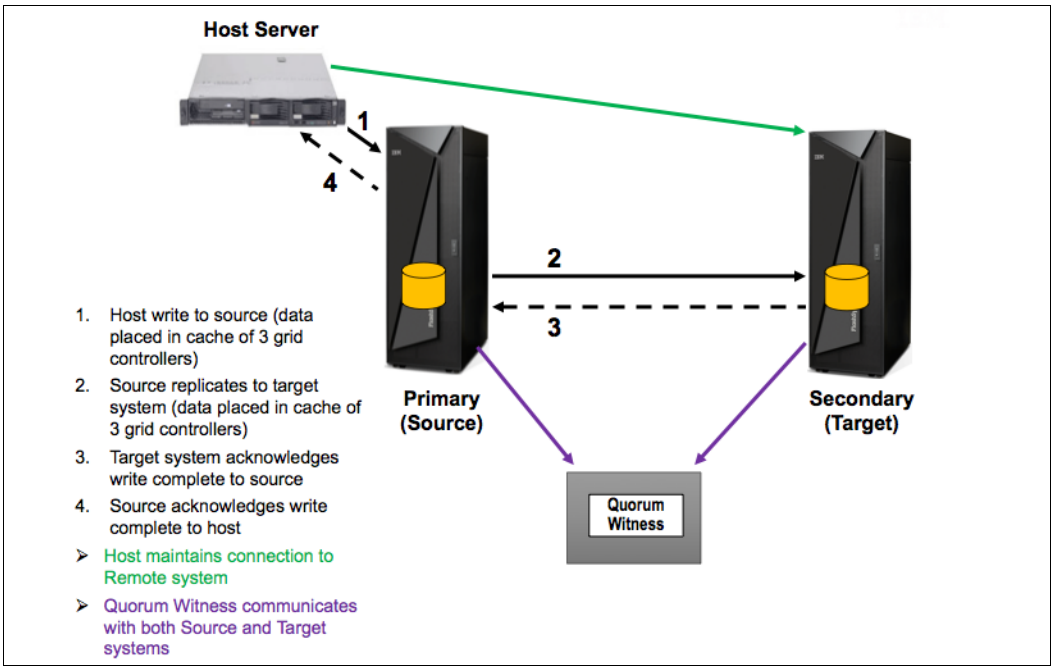


Figure 4-3 HyperSwap mirroring

For more information about HyperSwap, see *IBM HyperSwap and Multi-site HA/DR solution for IBM FlashSystem A9000 and A9000R*, REDP-5434.

Note: The data replicated between two FlashSystem A9000 and A9000R systems is not data reduced. Data reduction is done at the system level.

4.2 Boundaries

IBM FlashSystem A9000 and A9000R have the following boundaries or limitations:

- Maximum remote systems: The maximum number of remote systems that can be attached to a single primary system (source) is 10, with a maximum number of 32 ports on the target.
- Number of remote mirrors:

  Mirroring relationships consume internal system resources, that we refer to as as couplings. The system can provide a maximum of 3072 couplings and applies to volumes and Consistency Groups (CG) in mirroring or Hyperswap relationships

  - Each synchronous replication of one volume or one CG consumes one coupling
  - Each asynchronous mirror consumes 3 couplings, so the maximum number of asynchronous mirrors on a system is (3072 / 3) = 1024.
  - Except in asynchronous mirroring, and the asynchronous leg of a Multi-site HA/DR configuration, any use of data replication is synchronous.
  - In a Multi-site HA/DR relation, the standby async relation does not consume any coupling.

  For example, out of the 3072 maximum number of couplings:

  - Two source volumes in synchronous mirroring with two target volumes consume two couplings (1+1).
  - Two source volumes in synchronous mirroring with two target volumes contained in a Consistency Group, consume for three couplings (1+1+1).
  - Two source volumes in asynchronous mirroring with two target volumes contained in a Consistency Group, count for seven couplings (3+3+1).

  Here are some additional illustrations:

  - Assume a system currently configured with exactly one asynchronous relation of a CG containing 5 volumes. This relation consumes 18 couplings: 3 pairs for the async CG relation plus 15 pairs (3 pairs for each of the 5 volumes)

    In this case, we have remaining of one of the following three options:

    - 3072 - 18 = 3054 synchronous mirroring volume relationships
    - 3054/3 = 1018 asynchronous mirroring relationships
    - 190 CGs, each with 3 volumes, in a multi-site HA/DR configuration.

      Each multi-site HA/DR contains one HyperSwap relation, one active asynchronous relation and one standby asynchronous relation. Therefore a single multi-site HA/DR entity consumes 4 couplings (1 coupling for the HyperSwap relation, 3 couplings for the asynchronous relation, and 0 coupling for the standby async relation). Each CG consisting of 3 volumes, therefore consumes 16 couplings (4 couplings for the CG itself and 4 couplingss for each of the 3 volumes). Thus 3054/16 = 190.

Note the round-down of the result. In this example, 14 couplings are left unused, since 16 couplings are the minimum for a single multi-site HA/DR CG with 3 volumes (14 = 3054 - 190 x 16).

- Distance: Distance is limited only by the response time of the medium used. Use asynchronous mirroring when the distance causes unacceptable delays to the host I/O in synchronous mode. HyperSwap is supported up to synchronous mirroring distances.
- Consistency groups are supported within remote mirroring. The maximum number of consistency groups is 1024. The maximum number of Volumes in a CG is 512.
- The destination storage pool for a remote mirroring configuration must contain enough free space to accommodate the destination volume. Consideration must also be given for any possible increase in snapshot space that might be required on the target system.
- Snapshots: Snapshots are allowed with either the primary or secondary volumes without stopping the mirror. There are also special-purpose snapshots that are used in the mirroring process. Space must be available in the storage pool for snapshots.
- Source and target peers cannot be the target of a copy operation and cannot be restored from a snapshot. Peers cannot be deleted or formatted without deleting the relationship first.
- For Synchronous mirroring, resizing volumes while mirroring is active is supported. For Asynchronous mirroring, volumes cannot be resized when mirroring is active.

Cross-Gen mirroring with XIV Gen3 has the following additional boundaries or limitations:

- XIV Gen3 volumes must be uncompressed.
- Minimum firmware version required for XIV Gen3 is 11.6.2.a.
- Minimum firmware version required for FlashSystem A9000 or A9000R is 12.2.
- Minimum Hyper-Scale Manager Version is 5.3.
- Minimum XCLI is 5.2.
- Maximum volume size is 170 TB (XIV Gen3 limit).
- Maximum CG size is 128 volumes.
- All other normal system limitations, such as maximum number of mirrors or targets, apply to Cross-Gen mirroring.

4.3 Mirroring schemes

Mirroring, whether synchronous or HyperSwap, requires two or more FlashSystem A9000 or A9000R systems. Any combination of FlashSystem A9000 and A9000R is possible for the source and target systems.

Asynchronous mirroring requires two or more source and target systems, which can be any combination of FlashSystem A9000, A9000R or XIV Gen3. The source and target of the asynchronous mirroring can be at the same site and form a local mirroring. Alternatively, they can be at different sites and facilitate a disaster recovery plan. Figure 4-4 shows how peers can be spread across multiple storage systems and sites. Any system that is depicted can be a FlashSystem A9000, A9000R, or XIV Gen3.

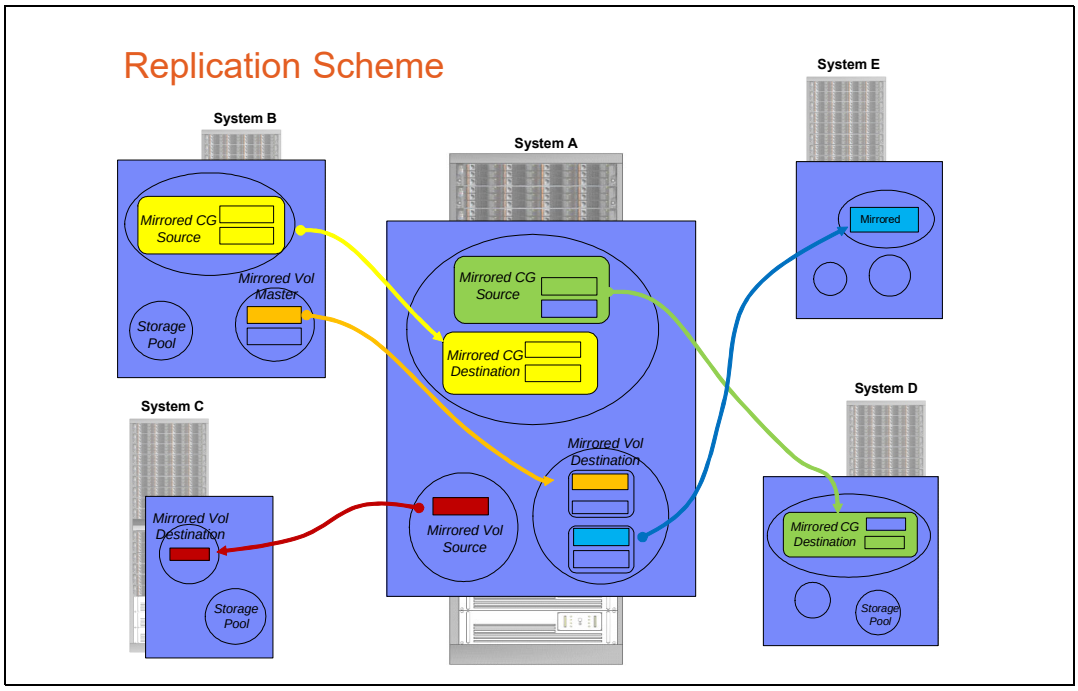


Figure 4-4 Mirroring replication schemes

The only time this will be different is when Multi-site High Availability/Disaster Recovery (HA/DR) is set up. More information on this configuration can be found in *IBM HyperSwap and Multi-site HA/DR solution for IBM FlashSystem A9000 and A9000R*, REDP-5434. This chapter covers stand alone synchronous or asynchronous topics.

A system can be connected to up to 10 other FlashSystem A9000, A9000R, or XIV Gen3 targets for mirroring purposes. Any system can be used simultaneously as a replication source and replication target (for different volumes).

In a bidirectional configuration, a system concurrently functions as the replication source (primary) for one or more couplings, and as the replication target (secondary) for other couplings. Figure 4-4 illustrates possible schemes for how mirroring can be configured.

Figure 4-5 shows connectivity among systems and groups of systems, as shown in the Hyper-Scale Manager GUI.

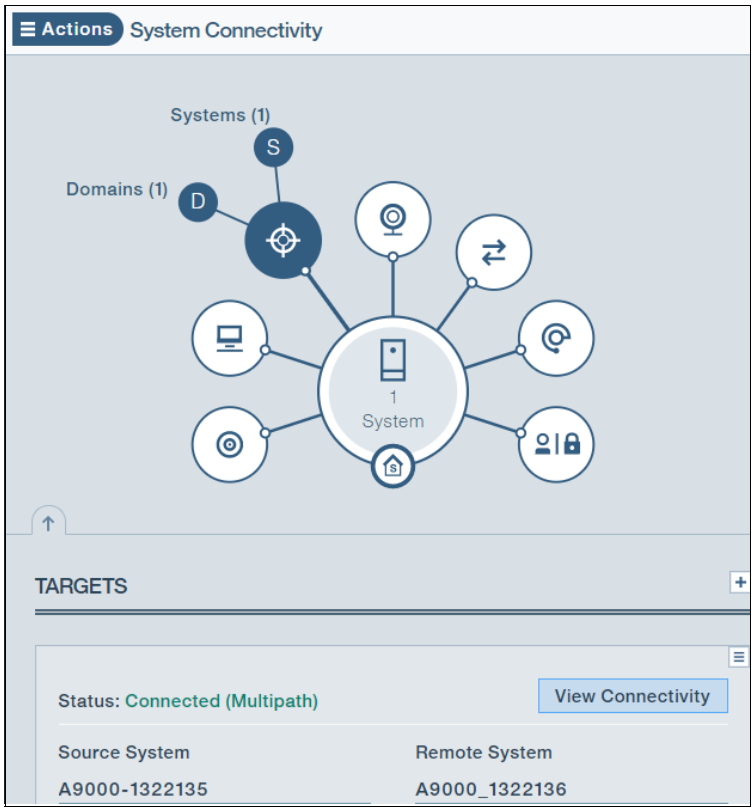


Figure 4-5 Connectivity among systems and group of systems in Hyper-Scale Manager

Figure 4-5 shows the target information. The target systems are listed beneath the TARGETS header in the Hyper-Scale Manager GUI. This example has one target system. The names of the source system and the target system are shown. The remote system is the target system.

4.3.1 Peer designations and roles

A peer (volume or consistency group) is assigned either a primary role or a secondary role when the mirror is defined. An active mirror must have exactly one primary role and exactly one secondary role when configured as synchronous or asynchronous replication.

Important: A single system can contain both source volumes and consistency groups (mirroring to another system) and target volumes and consistency groups (mirroring from another system). Peers in a source role and peers in a target role on the same system must belong to different mirror couplings.

The various mirroring role status options are as follows:

- Designations:
  - Primary designation: The designation of the local peer, which is initially assigned the primary role.
  - Secondary designation: The designation of the remote peer, which initially plays the secondary role.

- Role status:
  - Primary Role: Denotes the peer with the source data in a mirror coupling. Such peers serve host requests and are the source for synchronization updates to the target peer. Primary and secondary roles can be switched by using the **`mirror_switch_roles`** command or in the HyperScale Manager. if the status is synchronized for synchronous mirror and it is in an RPO OK state for an asynchronous mirror. For both synchronous and asynchronous mirroring, the primary can be changed (**`mirror_change_role`** command) to a secondary if the status is inactive. This is typically done as part of a recovery procedure when one of the systems is unavailable. Otherwise the switch roles option is used so that both primary and secondary are changed together.
  - Secondary Role: Denotes the remote peer in a mirror. Such peers do not serve host write requests and accept synchronization updates from a corresponding source. A target logical unit number (LUN) can be accessed in read-only mode by a host. HyperSwap and HA/DR handle this situation somewhat differently with host access to both primary and secondary volumes. If the host happens to send writes to the secondary, the secondary passes the writes to the primary, and the primary replicates the data back to the secondary. For more information about how HyperSwap works, see *IBM HyperSwap and Multi-site HA/DR solution for IBM FlashSystem A9000 and A9000R*, REDP-5434.

Consistency group within an IBM FlashSystem A9000 and A9000R

With mirroring (synchronous, asynchronous, HyperSwap, or HA/DR), the major reason for consistency groups (CGs) is to handle many mirror pairs as a *group* (mirrored volumes are crash consistent). Instead of dealing with many mirror pairs individually, consistency groups simplify the handling of those related pairs.

Important: If your mirrored volumes are in a mirrored consistency group, you cannot do mirroring operations such as *deactivate* or *change_role* on a single volume basis. If you want to do mirroring operations on a mirrored volume, you must remove the volume from the consistency group.

Mirrored volumes in a consistency group must be in the same pool.

Consistency groups also play an important role in the recovery process. If mirroring was suspended (for example, because of complete link failure), data on different target volumes at the remote system are consistent. However, when the links are up again and the resynchronization process is started, data spread across several target volumes is not consistent until the source state has reached the *synchronized* state.

To preserve the consistent state of the target volumes, the system automatically creates a snapshot of each target volume and keeps it until the remote mirror volume pair is synchronized. In other words, the snapshot is kept until all pairs are synchronized to enable restoration to the same consistent point in time. If the remote mirror pairs are in a consistency group, the snapshot is taken for the whole group of target volumes and the snapshot group is preserved until *all* pairs are synchronized. Then, the snapshot group is deleted automatically.

4.3.2 Operational procedures

Mirroring operations involve configuration, initialization, ongoing operation, handling of communication failures, and role switching activities.

The following list defines the mirroring operation activities:

- Configuration

  Local and remote replication peers are defined by an administrator who specifies the primary and secondary roles. These peers can be volumes or consistency groups. The secondary peer provides a backup of the primary.

- Initialization

  Mirroring operations begin with a primary volume that contains data and a formatted secondary volume. The first step is to copy the data from the primary volume to the secondary volume. This process is called *initialization*.

  Initialization is performed one time in the lifetime of a mirror. After it is performed, both volumes are considered to be synchronized to a specific point in time. The completion of initialization marks the first point-in-time that a consistent source replica on the target is available. Details of the process differ depending on the mirroring mode (synchronous or asynchronous) however regardless of the mirroring mode, the initialization phase is performed asynchronously with no impact to host latency.

- Offline initialization

  Offline initialization operation begins with a primary volume that contains data and a secondary volume, which also contains data and is related to this same primary volume. At this step, only different blocks of data are copied from the primary to its secondary. Offline initialization can be run whenever a mirror pair was suspended or when the mirror type changes from asynchronous to synchronous or by restoring an image (or backup) from the primary volume. This may also be used if a significant amount of data is to be copied the first time. The data can be offloaded to backup media (such as tape) at the primary site, then restored to the secondary site without any disruption to the host or application. Selecting the offline initialization option will then only need to copy the differences between the primary and secondary.

- Mirror mode switching

  The toggling between synchronous and asynchronous modes implies the deactivation of the current mirror mode, the deletion of the mirror pair and the respective snapshots on both ends, and unlocking of the target mirror. Then the new mode is selected and a new mirror relationship is created between the peers. Using the offline initialization, only the new data that was written to the primary since the deletion of the original mirror is copied over. Thus, the toggling between the two operational modes does not require a full copy.

- Ongoing operation

  After the initialization process is complete, normal mirroring operations begin.

  In synchronous mirroring, normal ongoing operation means that all data written to the primary volume or CG is first mirrored to the secondary volume or CG. At any point in time, the primary and source volumes or CGs are identical except for any unacknowledged (pending) writes.

  HyperSwap follows the same operations as synchronous mirroring.

  In asynchronous mirroring, ongoing operation means that data is written to the primary volume or CG, and is replicated to the secondary volume or CG at specified intervals.

- Monitoring

The storage system effectively monitors the mirror activity and places events in the event log for error conditions. Alerts can be set up to notify the administrator of such conditions. You must have set up SNMP trap monitoring tools or email notification to be informed about abnormal mirroring situations. For more information, refer to *IBM FlashSystem A9000 and IBM FlashSystem A9000R Architecture and Implementation,* SG24-8345, section 7.1.

- Handling of communication failures

  Sometimes the communication between the sites might break down. The primary continues to serve host requests as the synchronous mirroring is based on best effort to minimize any impact to the host write operations. Upon recovery from a link down incident, the changed data is copied to the secondary site and mirroring is resumed. Events are generated for link failures.

- Role switching

  If required, mirror peer roles of the target and source can be switched. Role switching should always be initiated at the source site. Usually, this process is done for maintenance operations or because of a test drill that verifies the disaster recovery (DR) procedures. Use role switching cautiously, especially with asynchronous mirroring. When roles are switched for an asynchronous mirror, data can be lost for an interval up to the RPO time because the remote site is typically lagging, in time, for a given asynchronous pair.

  Role switching in synchronous mirror is designed so that no data loss occurs. Use role switching only for specific cases, such as a catastrophic host failure at the source site when the pairing is intact, but there have been no write operations to the source since the last sync job was completed.

- Role changing

  In a disaster at the primary site, the source peer might fail. To allow read/write access to the volumes at the remote site, the volume's role must be changed from secondary to primary. A *role change* changes only the role of the system volumes or CGs to which the command was addressed. Original primary volumes or CGs are not automatically reassigned to their original role. That is why changing roles on both mirror sides if mirroring is to be restored is important (if possible).

- Convert to HyperSwap and Synchronous mirror

  It is possible to convert HyperSwap pairs to Synchronous mirrors, and to convert Synchronous mirrors to HyperSwap. This process is possible because HyperSwap is based on synchronous mirroring. It is a simple task in the Hyper-Scale Manager or command-line interface to convert in either direction as needed.

- Extend to Multi-site

  This option allows an existing mirror or HyperSwap to be extended to a multi-site configuration for HA/DR. For more information on this topic, see *IBM HyperSwap and Multi-site HA/DR solution for IBM FlashSystem A9000 and A9000R*, REDP-5434.

4.3.3 Mirroring status

The status of a mirror is affected by several factors, such as the links between the FlashSystem A9000 and A9000R systems or the initialization state.

Link status

The link status reflects the connection from the source to the target volume or CG. A link has a direction (from local site to remote or vice versa). A failed link or a failed secondary system both result in a link error status. The link state is one of the factors determining the mirror operational status. Links can be in one of the following states:

- Connected: Link is up and is functioning.
- Connectivity Failure

Figure 4-6 depicts how the link status is displayed from the System Connectivity window for a specific Target System. The status **Connected (Multipath)** is shown in green letters.

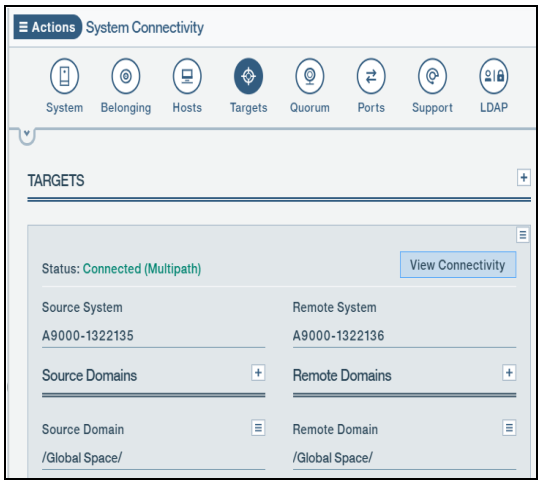


Figure 4-6 Red indicates link down, green indicates link up

Figure 4-7 depicts how the link status is reflected in the Hyper-Scale Manager GUI when the Target Connectivity Details is selected. Click **View Connectivity** for Target Connectivity Details.

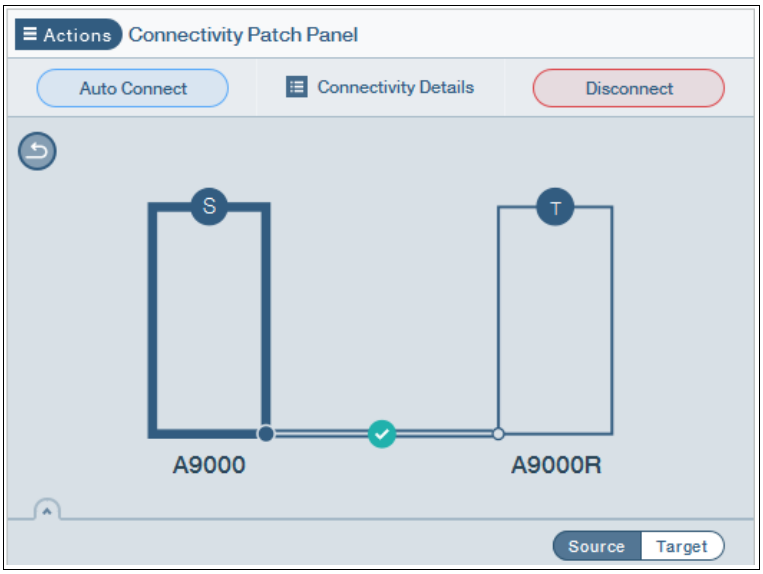


Figure 4-7 Connectivity details

If several links (at least two) are in one direction and one link fails, it usually does not affect mirroring if the bandwidth of the remaining link is high enough to keep up with the data traffic. Clicking on **Connectivity Details** will show a graphical representation of the connections between the systems.

Monitoring the link usage

The mirroring bandwidth of the links must be high enough to cope with the data traffic generated by the changes on the source volumes. During the planning phase, before setting up mirroring, monitor the write activity to the local volumes. Ideally, the bandwidth of the links for mirroring should be as large as the peak write workload.

The physical link between the source and target can also be used for other traffic. This link between the source and target must sustain the maximal peak workload of all workloads that use the link. If peak bandwidth is not available, there may be primary host performance impacts in synchronous mirroring or elongated (lagging) RPO with asynchronous mirroring.

Note: Check the physical link utilization to ensure bandwidth capacity for the peak write workload.

Starting with Hyper-Scale Manager Version 5.1, statistics can be viewed on an interface level. Starting with Hyper-Scale Manager Version 5.2 the ability to see port statistics in historical data at a system level was added. To see live statistics at a port level, you can check the physical link utilization by using the SAN components, for example an FC switch for FC connections. Using the volume view of the Hyper-Scale Manage gives you the current bandwidth of the selected volumes.

Figure 4-8 shows the current write bandwidth of one target volume. The volume source is on the system A9000R and the target volume is on system A9000.

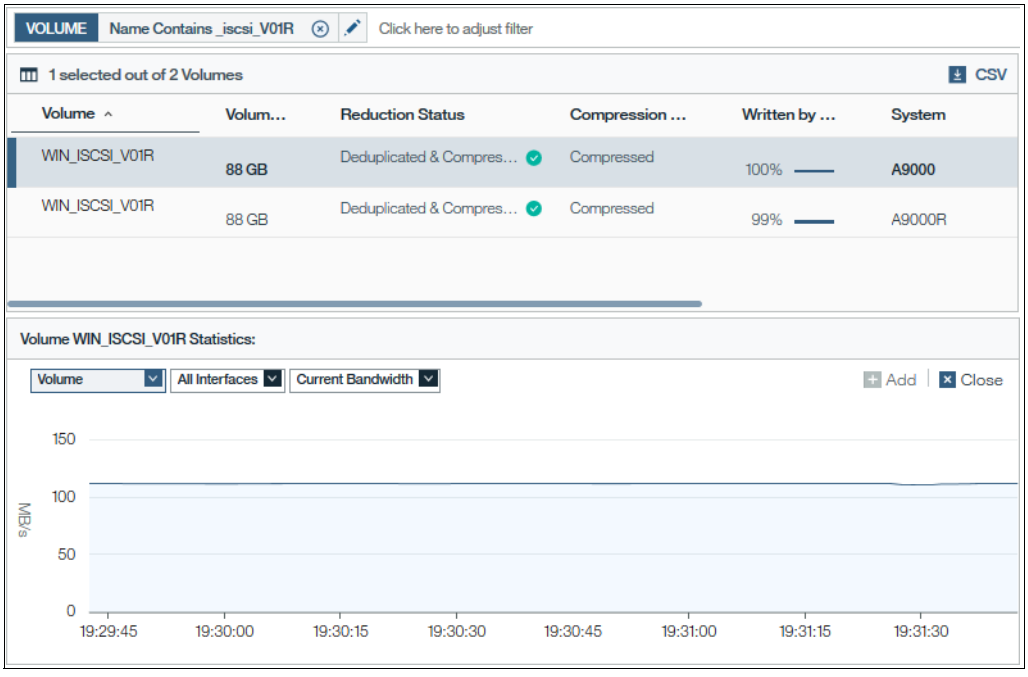


Figure 4-8 Monitoring bandwidth of the target volume

Figure 4-9 shows the option to select specific port statistics when viewing historical data for a single system.

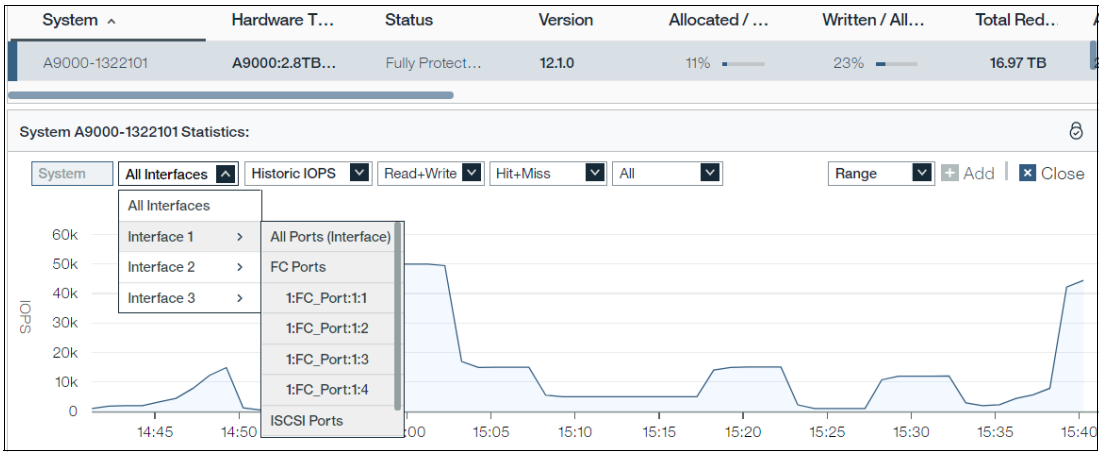


Figure 4-9 Viewing historical port statistics

Mirror operational status

In this section, the mirroring status is defined as either *operational* or *non_operational*:

- Mirroring is `operational` in the following situations:
  - The mirror is *active*.
  - The link is up.
  - Both peers have different roles (primary or secondary).
- Mirroring is `non_operational` in the following situations:
  - The mirror is inactive.
  - The link is in an error state or deactivated (link down).
  - Both peers have the same roles (such as both being primary) resulting in a role conflict.

Synchronous mirroring states

The synchronization status reflects whether the data of the target volume is identical to the source volume. Because the purpose of the remote mirroring feature is to ensure that the target volume is an exact copy of the source volume. This status indicates whether this objective is being achieved. The following states or statuses are possible:

- Initializing

  The first step in remote mirroring is to create a copy of all the data from the source volume to the target volume. During this initial copy phase, the status remains *initializing*.

- Synchronized (source volume or CG) and consistent (target volume or CG)

  This status indicates that all data that has been written to the source volume or CG has also been written to the target volume or CG. Ideally, the source and target volumes or CGs must always be synchronized. Note that write operations that have not yet been acknowledged to the respective hosts are known as *pending writes* or *data in flight*.

- Unsynchronized (source volume) and inconsistent (target volume)

  After a volume or CG has completed the initializing stage and achieved the synchronized status, it can become *unsynchronized* (source) and *inconsistent* (target). This state occurs when it is not known whether all the data that has been written to the source volume has also been written to the target volume.

This status can occur in the following cases:

- The communications link is down and, as a result, certain data might have been written to the source volume, but was not yet written to the target volume.
- Secondary system is down. This is similar to communication link errors because in this state the Primary system is updated, whereas the secondary system is not.
- Remote mirroring is deactivated. As a result, certain data might have been written to the source volume and not to the target volume. The volumes or CGs will be in an inactive state in this case.

The system tracks the partitions that have been modified on the source volumes. When the link is operational again or the remote mirroring is reactivated, these changed partitions are sent to the remote system and applied to the respective targets volumes.

Note: HyperSwap has the same states at synchronous mirroring and some additional information, such as the Quorum Witness. For more information about HyperSwap, see*IBM HyperSwap and Multi-site HA/DR solution for IBM FlashSystem A9000 and A9000R*, REDP-5434.

Asynchronous mirroring states

Note: This section applies only to asynchronous mirroring and Cross-Generation mirroring with XIV Gen3.

The mirror state can be either inactive or initializing:

- Inactive: The synchronization process is disabled. It is possible to delete a mirror in this state.
- Initializing: The initial copy is not done. Synchronization does not start until the initialization completes. The mirror cannot be deleted during this state.

Important: In cases of an unstable data link, it is possible for the initialization to restart. In this case, the progress bar returns to the left side of the display. This change does not mean that the initialization is starting again from the beginning. On the restart of a mirror initialization, the initialization resumes where it left off, and the progress bar displays the percent complete of the remaining data to copy, not the percentage of the full volume.

When initialization is complete, the synchronization process is enabled. Then, it is possible to run sync jobs and copy data between source and target. This does not mean that the data is copied as it is in synchronous mirroring. Synchronization states are as follows:

- RPO_OK: Synchronization completed within the specified sync job interval time (RPO).
- RPO_Lagging: Synchronization completed but took longer that the specified interval time (RPO).

4.3.4 Link failure and last consistent snapshot

A synchronous mirror relationship has, by its nature, identical data on both local and remote with zero RPO. This principle is not maintainable if the link between the two sites is broken. The so-called coupling defines what synchronous mirroring does in a connection line failure. The coupling works in a “Best-Effort” method.

Best-Effort means that remote mirroring is changed to an unsynchronized state. Then, all the writes to the source volume continue. These writes are updates that need to be recorded, and must be written to the target volume later. The process of copying these changes or “Uncommitted Data” to the target is called resynchronization.

Resynchronizing the data will happen only after the link down incident is recovered. During the time of resynchronization, data on both sites is not consistent. That is why you must take precautions to protect against a failure during the resynchronization phase. To preserve consistency, a last-consistent snapshot (LCS) is automatically created on the target system after the link is regained and before resynchronization of any new data.

The following scenarios are examples:

- Resynchronization can be run in any direction if one peer has the primary role and the other peer has the secondary role. If there was only a temporary failure of all links from the primary system to the secondary system, reestablish mirrors with the original direction after links are operational again.
- If there was a disaster at your primary site and production was moved to the secondary site, mirroring must be established first from the secondary site to the primary site. This assures that changes to the secondary volumes during the outage are synchronized back to the primary site. Thereafter the direction can be changed again from the primary to the secondary site.
- A disaster recovery drill on the secondary site often requires resetting the changes applied there during the test and then resynchronizing the mirror from primary to secondary.

Last-consistent snapshot (LCS)

Before a resynchronization process is initiated, the system creates a snapshot of the target volumes/CGs. A snapshot is created to ensure the usability of the target volume/CG if the primary site experiences a disaster during the resynchronization process.

If the source volume/CG is damaged before resynchronization is completed, the target volume/CG might be inconsistent because it might have been only partially updated with the changes that were made to the source volume. To handle this situation, the secondary system always creates a snapshot of the last consistent target volumes/CGs after reconnecting to the primary system and before starting the resynchronization process. This special snapshot is called the last-consistent snapshot (LCS).

No LCS is created for couplings that are in an initialization state. The snapshots are preserved until the volume/CG is synchronized. Then, it is deleted automatically, unless the target peer role has changed during resynchronization.

If there is a disaster at the primary (source) site, the snapshot taken at the secondary (target) site can be used to restore the target volume/CG to a consistent state for production.

Important: The mirror relation at the secondary site must be deleted before the last consistent snapshot can be restored to the target volume/CG.

Tips:

- The last consistent snapshot can be deleted manually by using the **`vol_delete_mirror_snapshots`** CLI command (by IBM support team only).
- Mirroring can be configured so that no last consistent snapshot is generated. This is useful when the system that contains the secondary volume is fully used and an extra snapshot cannot be created. The CLI command to be used for this is **`pool_config_snapshots`** (by IBM support team only).

Last-consistent snapshot time stamp

A time stamp is taken when the coupling between the primary and secondary volumes becomes non-operational. This time stamp specifies the last time that the secondary volume was consistent with the primary volume.

This status has no meaning if the coupling's synchronization state is still Initialization. For synchronized couplings, this time stamp specifies the current time. Most important, for unsynchronized couplings, this time stamp denotes the time when the coupling became non-operational.

Tip: Some options in the HSM GUI might not show by default. In the **SNAPSHOT** view, right-click the column header to add/remove columns, and under the **Additional** menu you can add several columns that can be useful to help determine snapshot creation time. Some examples include: **Created (Local Time)**, **Created (System Time)**, **Created on Source (Local Time)**, and **Created on Source (System Time)**.

Snapshot	System	Pool	Source Volume	Created (Local Time)	Created on Sour...	Created (Syste...	Created on Sour...
itso_HA_cg.mirror_s...	A9000-1322135	ITSO_list	HA_test_002	Sep 25, 2018, 5:58:58 PM	Sep 25, 2018, 5:58...	Sep 25, 2018, 5:...	Sep 25, 2018, 5:58...
itso_HA_cg.mirror_s...	A9000-1322136	ITSO_list2	HA_test_002	Sep 25, 2018, 5:58:58 PM	Sep 25, 2018, 5:58...	Sep 25, 2018, 5:...	Sep 25, 2018, 5:58...

Figure 4-10 Snapshots showing column headings with different creation times

External last consistent snapshot (ELCS)

Before the introduction of the external last consistent snapshot (ELCS), whenever a volume's role was changed back to secondary and whenever a new resynchronization process had started, the system detects an LCS on the peer and does not create one. If during such an event the peer was not part of a mirrored consistency group (mirrored CG), not all volumes have the same LCS time stamp. If the peer was part of a mirrored consistency group, you have a consistent LCS but not as current as expected. This situation is avoided with the introduction of the ELCS.

Whenever the role of a destination with an LCS is changed to primary while mirroring resynchronization is in progress (in the system/target not specific to this volume), the LCS is renamed external last consistent snapshot (ELCS). The ELCS retains the LCS deletion priority of 0. If the peer's role is later changed back to secondary and sometime later a new resynchronization process starts, a new LCS is created.

Later, changing the secondary role again renames the existing ELCS to external last consistent *x* (where *x* is the first available number starting from 1) and renames the LCS to external last consistent. The deletion priority of external last consistent is 0 (zero), but the deletion priority of the new external last consistent *x* is the system default (1), and can thus be deleted automatically by the system upon pool space depletion

It is crucial to validate whether the LCS or an ELCS (or even ELCSx) should serve as a restore point for the target peer volume if resynchronization cannot be completed. Although snapshots with deletion priority 0 are not automatically deleted by the system to free space, the external last consistent and external last consistent x snapshots can be manually deleted by the administrator if required.

Because the deletion of such snapshots might leave an inconsistent peer without a consistent snapshot from which to be restored (in case the resynchronization cannot complete as a

result of source unavailability), avoid it even when pool space is depleted, unless the volume is ensured to be consistent.

4.4 Remote mirroring configurations

Remote mirroring solutions can be used to address multiple types of failures and planned outages. The failure scenarios vary. They can be a result of events that affect a single system. The failure can stem from events that affect an entire data center or campus. Worse, they can be caused by events that affect a whole geographical region.

Several configurations are possible:

- Single-site high-availability remote mirroring configuration

  Protection for the event of a failure or planned outage of a system (single-system failure) can be provided by a *zero-distance* high-availability (HA) solution, including another storage system in the same location (zero distance). Typical usage of this configuration is a synchronous mirroring solution that is part of a high-availability clustering solution that includes both servers and storage systems. HyperSwap is also a high-availability solution implemented with synchronous mirroring.

  Figure 4-11 shows a single-site high-availability configuration where both systems are in the same data center.

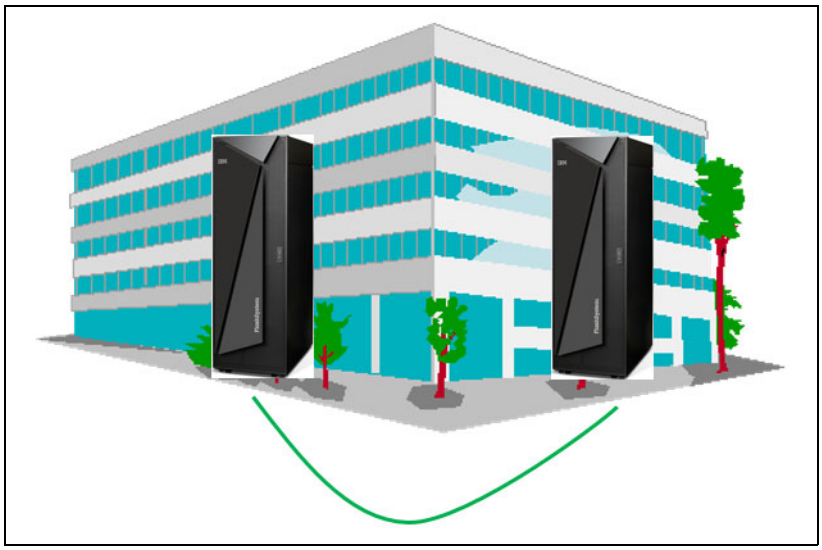


Figure 4-11 Single site HA configuration

- Metro region remote mirroring configuration

  Protection during a failure or planned outage of an entire location (*local disaster*) can be provided by a metro distance disaster recovery solution, including another system in a different location within a metro region. The two systems might be in different buildings on a corporate campus or in different buildings within the same city (typically up to approximately 100 km apart).

  FlashSystem A9000 and A9000R deliver the lowest response time to the host. The added latency due to the distance of the mirrored systems must be tolerated by the host if you are using synchronous mirroring. HyperSwap distances can be shorter than synchronous mirroring distances, depending on host latencies that can be impacted in a failover state.

Note: The SAN infrastructure must be fast enough to handle the speed of FlashSystem A9000 and A9000R.

Typical usage of this configuration is a synchronous mirroring solution or a HyperSwap solution. Figure 4-12 shows a metro region disaster recovery configuration.

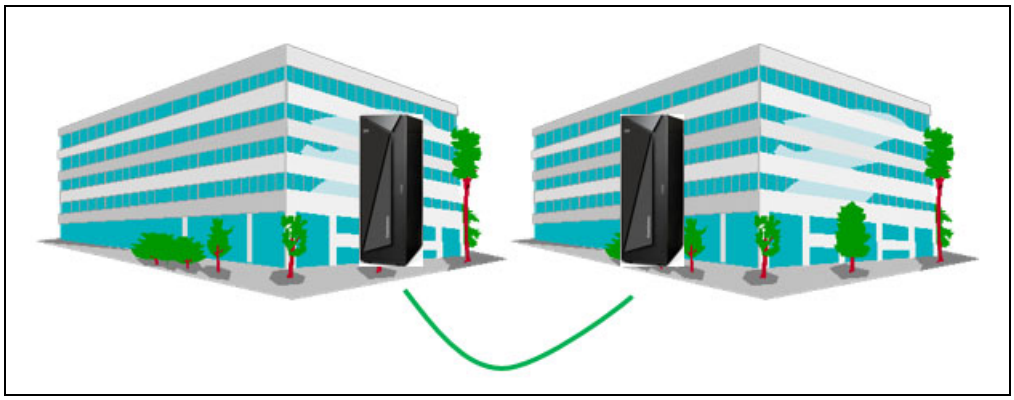


Figure 4-12 Metro region disaster recovery configuration

- Out-of-region remote mirroring configuration

  Protection during a failure or planned outage of an entire geographic region (*regional disaster*) can be provided by a global distance disaster recovery solution that includes another system in a different location outside the metro region. The two locations might be separated by up to a global distance. Typical usage of this configuration is an asynchronous mirroring solution. Figure 4-13 shows an out-of-region disaster recovery configuration.

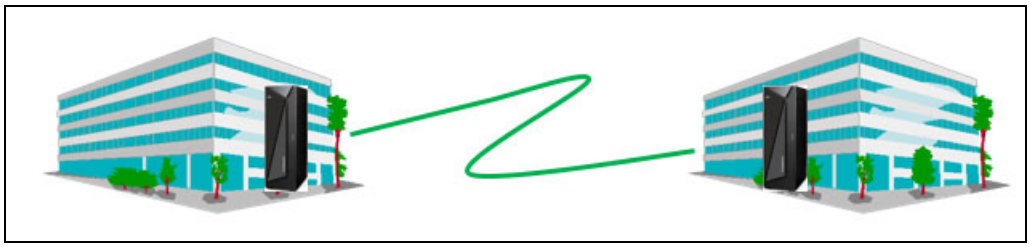


Figure 4-13 Out-of-region disaster recovery configuration

4.4.1 Using snapshots

Snapshots can be used with remote mirroring to provide copies of production data for business or IT purposes. Moreover, when used with remote mirroring, snapshots provide protection against data corruption. Like any continuous or near-continuous remote mirroring solution, remote mirroring cannot protect against software data corruption because the corrupted data is copied as part of the remote mirroring solution.

However, the snapshot function provides a point-in-time image that can be used for a rapid recovery if software data corruption occurs after the snapshot was taken. The snapshot can be used in combination with remote mirroring, as illustrated in Figure 4-14.

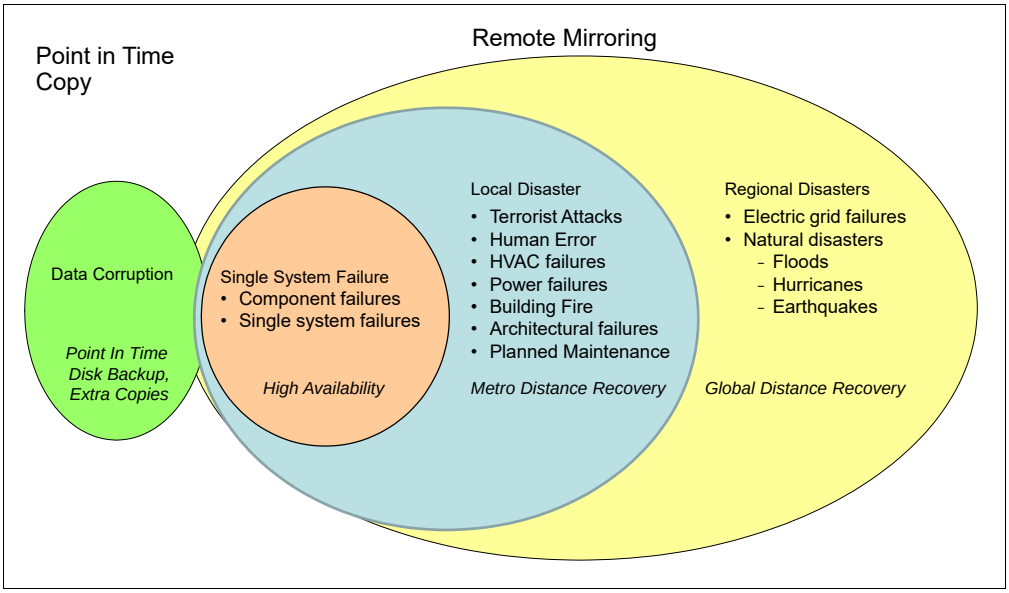


Figure 4-14 Combining snapshots with remote mirroring

Recovery using a snapshot requires deletion and re-creation of the mirror:

- Snapshot (within a single system)

  Protection for the event of software *data corruption* can be provided by restoring the volume to a healthy point-in-time snapshot. The snapshot can be backed up if needed.

- Local snapshot plus remote mirroring configuration

  A snapshot of the production (local) volume can be used in addition to remote mirroring of the production volume when protection from logical data corruption is required in addition to protection against failures and disasters. The extra snapshot of the production volume provides a quick restoration to recover from data corruption. An extra snapshot of the production (local) volume can also be used for other business or IT purposes such as reporting, data mining, development, and testing.

  Figure 4-15 shows a local snapshot plus remote mirroring configuration.

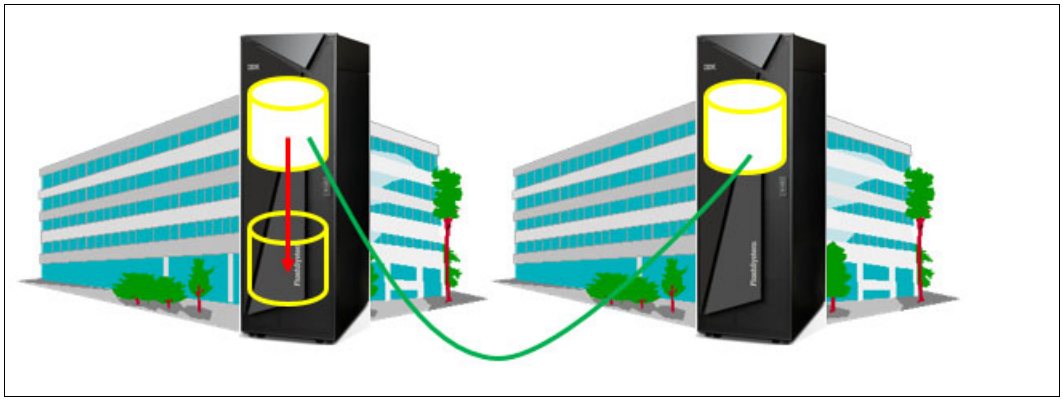


Figure 4-15 Local snapshot plus remote mirroring configuration

- Remote snapshot plus remote mirroring configuration

  A snapshot of the consistent replicated data at the remote site can be used in addition to remote mirroring to provide an extra consistent copy of data. This copy can be used for business purposes, such as data mining and reporting, and for IT purposes, such as remote backup to tape or development, test, and quality assurance. Figure 4-16 shows a remote snapshot plus remote mirroring configuration.

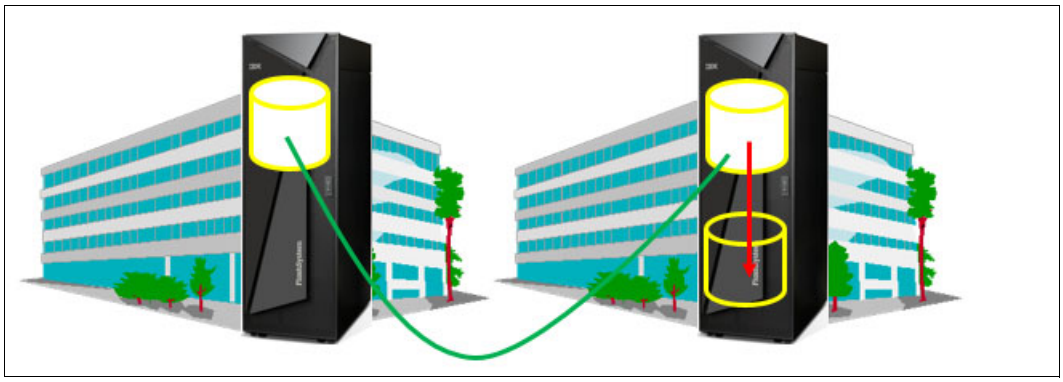


Figure 4-16 Remote snapshot plus remote mirroring configuration

- Mirrored snapshots

  Snapshots from both the primary and secondary replicated volumes can be created, given that the data is consistent across the mirrored pair. These copies can be used for development and testing purposes, in addition to backups, data mining, and reporting. Figure 4-17 shows an example of a mirrored snapshot of both the primary and secondary volumes in a mirrored relationship.

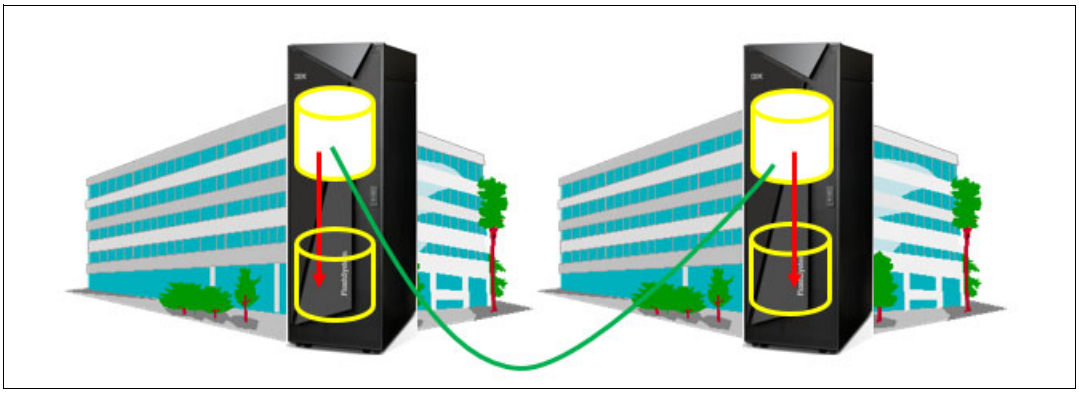


Figure 4-17 Mirrored snapshots

4.5 Using remote mirroring

The following sections show the basic steps used to set up mirrored volumes and mirrored consistency groups. The remote mirroring setup is described in 3.3, “Remote mirroring configuration using GUI or CLI” on page 48.

4.5.1 Defining volume and consistency group mirroring

The two peers in the mirror can be either two volumes (volume peers) or two consistency groups (CG peers). Each of the two peers in the mirroring relationship is given a designation and a role. The designation indicates the original or *normal* function of each of the two peers: Primary or secondary. The peer designation does not change with operational actions or commands. If necessary, it can be changed by explicit user command or action.

The role of a peer indicates its current operational function (either primary or secondary). The operational role of a peer can change as the result of user commands or actions. Peer roles typically change during DR testing or a true disaster recovery and production site switch. When a mirror coupling is created, the first peer specified is the source for data to be replicated to the target system, so it is given the primary designation and the primary role. The first peer can be, for example, the volumes or consistency group (CG) at site 1, as shown in Figure 4-18.

Important: A consistency group to be mirrored must not contain any volumes when the CG coupling is defined. Mirrored volumes can be added after the mirrored CG has completed initialization.

The second peer specified (or automatically created by the storage system) when the mirroring coupling is created is the target of data replication, so it is given the target designation and the secondary role.

Defining synchronous volume mirroring in Hyper-Scale Manager GUI

To define synchronous volume mirroring, complete these steps:

1. Select the volumes in the **Volume** view and select **Replication** in the Hub view, followed by clicking on **+ Sync Mirror**, as shown in Figure 4-18.

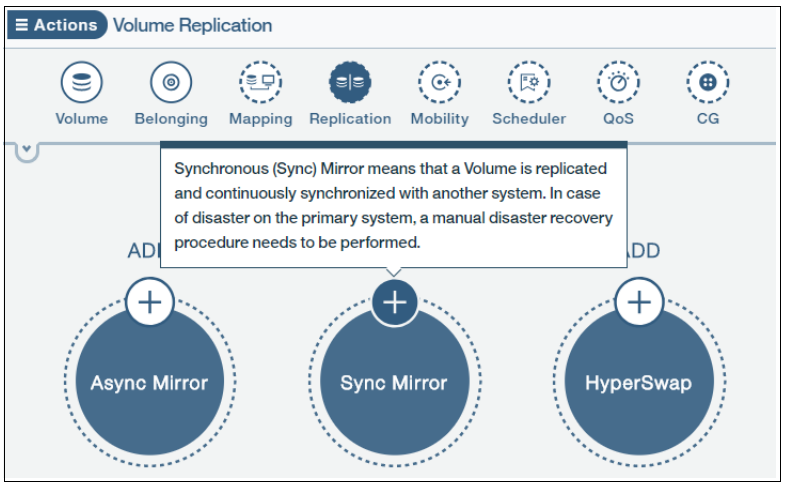


Figure 4-18 Selecting volumes for sync mirroring

2. Then add the details of the **Secondary** system. The target volumes are created automatically when two or more volumes are selected for mirroring. When setting up a mirror for one volume, you can select the target volume name and decide if a new volume is created or an existing volume is used. Figure 4-19 shows the parameters for synchronous mirroring for one volume. Note that you can choose to create the volume on the secondary system automatically or select an existing volume.

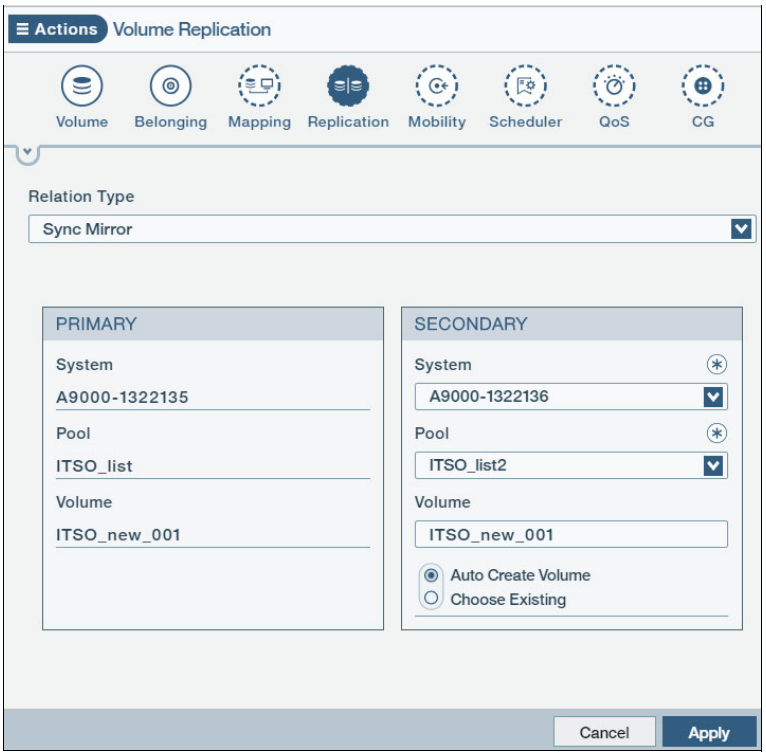


Figure 4-19 Volume sync mirror parameters

3. Click **Apply** to establish the volume mirrors. Because **Activation State: Active** is selected, the synchronization starts immediately and will become synchronized when all the data from the primary volume has been copied to the secondary. The mirror state is shown in Figure 4-20.

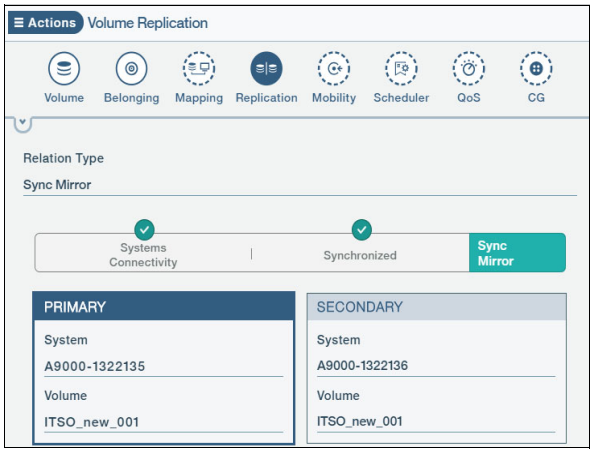
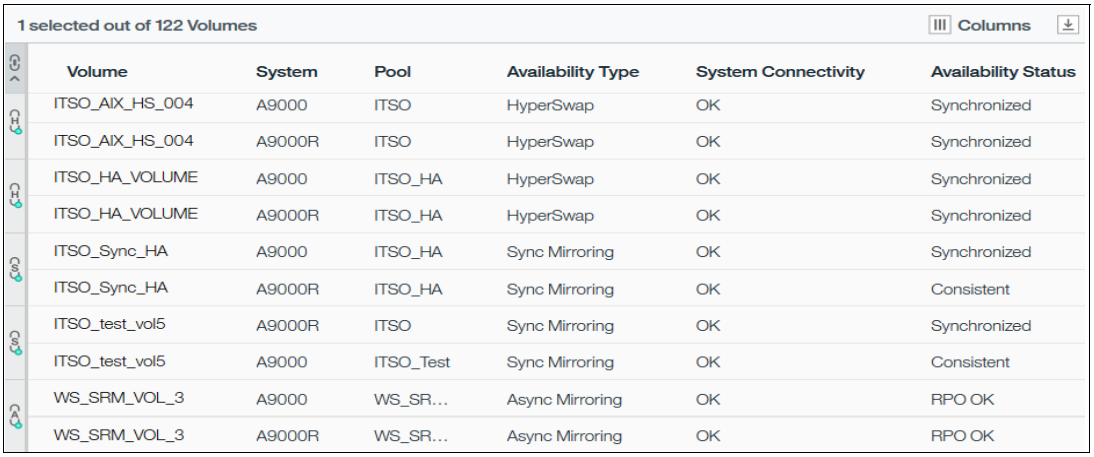


Figure 4-20 Mirroring status

You can check the mirroring initialization progress in the **Volumes** window. One volume after the other is synchronized. Figure 4-21 shows the **Availability Type** and the **Availability Status** and displays an icon on the left side of the table indicating **H** for HyperSwap, **S** for Synchronous mirroring, and **A** for Asynchronous mirroring.


1 selected out of 122 Volumes

Columns

Volume	System	Pool	Availability Type	System Connectivity	Availability Status
ITSO_AIX_HS_004	A9000	ITSO	HyperSwap	OK	Synchronized
ITSO_AIX_HS_004	A9000R	ITSO	HyperSwap	OK	Synchronized
ITSO_HA_VOLUME	A9000	ITSO_HA	HyperSwap	OK	Synchronized
ITSO_HA_VOLUME	A9000R	ITSO_HA	HyperSwap	OK	Synchronized
ITSO_Sync_HA	A9000	ITSO_HA	Sync Mirroring	OK	Synchronized
ITSO_Sync_HA	A9000R	ITSO_HA	Sync Mirroring	OK	Consistent
ITSO_test_vol5	A9000R	ITSO	Sync Mirroring	OK	Synchronized
ITSO_test_vol5	A9000	ITSO_Test	Sync Mirroring	OK	Consistent
WS_SRM_VOL_3	A9000	WS_SR...	Async Mirroring	OK	RPO OK
WS_SRM_VOL_3	A9000R	WS_SR...	Async Mirroring	OK	RPO OK

Figure 4-21 Replication status

You can check the initializing status of one volume by selecting the **Replication** icon in the hub, for information of a volume, as shown in Figure 4-20 on page 88.

When a mirror coupling is first activated, all actual data on the source is either copied to the target (online initialization) or verified to be on the target, and only changed data is copied (offline initialization). This process is referred to as *initialization*. Remote mirroring copies volume identification information (that is, physical volume ID/PVID) and any actual data on the volumes. Space that has not been used is not copied.

Initialization might take a significant amount of time if a large amount of data exists on the source when a mirror coupling is activated. As discussed earlier, the rate for this initial copy of data can be specified by the user as described in 3.3, “Remote mirroring configuration using GUI or CLI” on page 48. The speed of this initial copy of data is also affected by the connectivity and bandwidth (number of links and link speed) between the primary and secondary systems.

As an option to remove the impact of distance on initialization, mirroring can be initialized with the target system installed locally. The target system can then be disconnected after initialization, shipped to the remote site, reconnected, and the mirroring reactivated.

Defining synchronous mirroring using XCLI

Tip: When working with the XCLI from a command line, the storage system that the XCLI commands are dedicated to is not necessarily visible. Commands can inadvertently be run against the wrong FlashSystem A9000 and A9000R. A good idea is to issue a **`config_get`** command to verify that the intended IBM system is being addressed.

To set up sync volume mirroring using XCLI, complete the following steps. The examples shown might have some rows of output deleted to it easier to see the information.

1. Open an XCLI session for the primary IBM FlashSystem A9000 or A9000R and run the **`mirror_create`** command shown in Example 4-1 on page 90.

Example 4-1 XCLI mirror create

```
A9000>>mirror_create target="A9000R" vol="ITSO_Test_Vol1" slave_vol="ITSO_Test_Vol1" remote_pool="ITSO_Test_R"
create_slave=yes
Command executed successfully.
```

2. To list the couplings on the primary IBM FlashSystem A9000 or A9000R, run the **mirror_list** command shown in Example 4-2. The Initializing status is used when the coupling is in standby, inactive, or initializing state.

Example 4-2 XCLI mirror list on primary

```
A9000>>mirror_list
Name           Mirror Type       Mirror Object   Role    Remote System   Remote Peer     Active   Standby   Status
Link Up
ITSO_Test_Vol1   sync_best_effort   Volume          Master   A9000R           ITSO_Test_Vol1   no       no
Initializing   yes
```

3. To list the couplings on the secondary IBM FlashSystem A9000 or A9000R, run the **mirror_list** command shown in Example 4-3.

Example 4-3 XCLI mirror list on secondary

```
A9000R>>mirror_list
Name           Mirror Type       Mirror Object   Role    Remote System   Remote Peer     Active   Standby   Status
Link Up
ITSO_Test_Vol1   sync_best_effort   Volume          Slave    A9000           ITSO_Test_Vol1   no       no
Initializing   yes
```

4. Repeat steps 1-3 to create extra mirror couplings.

To activate the mirror, complete these steps:

1. On the primary IBM FlashSystem A9000 or A9000R, run the **mirror_activate** command, as shown in Example 4-4.

Example 4-4 XCLI mirror activate

```
A9000>>mirror_activate vol=ITSO_Test_Vol1
Command executed successfully.
```

2. On the primary IBM FlashSystem A9000 or A9000R, run the **mirror_list** command to see the status of the couplings, as shown in Example 4-5.

Example 4-5 XCLI mirror list on primary

```
A9000>>mirror_list
Name           Mirror Type       Mirror Object   Role    Remote System   Remote Peer     Active   Standby   Status
Link Up
ITSO_Test_Vol1   sync_best_effort   Volume          Master   A9000R           ITSO_Test_Vol1   yes      no
Synchronized   yes
```

3. On the secondary IBM FlashSystem A9000 or A9000R, run the **mirror_list** command to see the status of the couplings, as shown in Example 4-6.

Example 4-6 XCLI mirror list on secondary

```
A9000R>>mirror_list
Name           Mirror Type       Mirror Object   Role    Remote System   Remote Peer     Active   Standby   Status
Link Up
ITSO_Test_Vol1   sync_best_effort   Volume          Slave    A9000           ITSO_Test_Vol1   yes      no
Consistent     yes
```

4. Repeat steps 1-3 to activate more couplings.

Defining asynchronous volume mirroring in Hyper-Scale Manager GUI

To define asynchronous volume mirroring, complete these steps:

1. Select the volumes in the **Volume** view and right-click or use the **Actions** menu to select **Mirror** → **Define/View Mirror relation**, as shown in Figure 4-22.

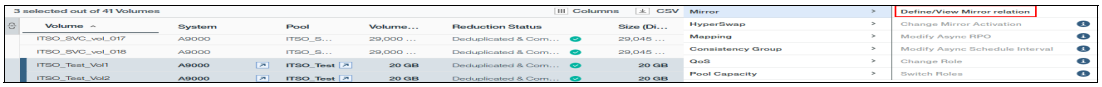


Figure 4-22 Selecting volumes for mirroring

2. Then add the details of the **Secondary** system. The target volumes are created automatically when two or more volumes are selected for mirroring.

   When setting up a mirror for one volume, you can select the target volume name and decide if a new volume is created or an existing volume is used.

3. Enter an **RPO (seconds)** time. Other options you can choose include to activate the mirror, choose between online/offline init if available, or to automatically/manually set a schedule.

4. Click **Apply** to establish the volume mirrors.

   Figure 4-23 shows the parameters for asynchronous mirroring.

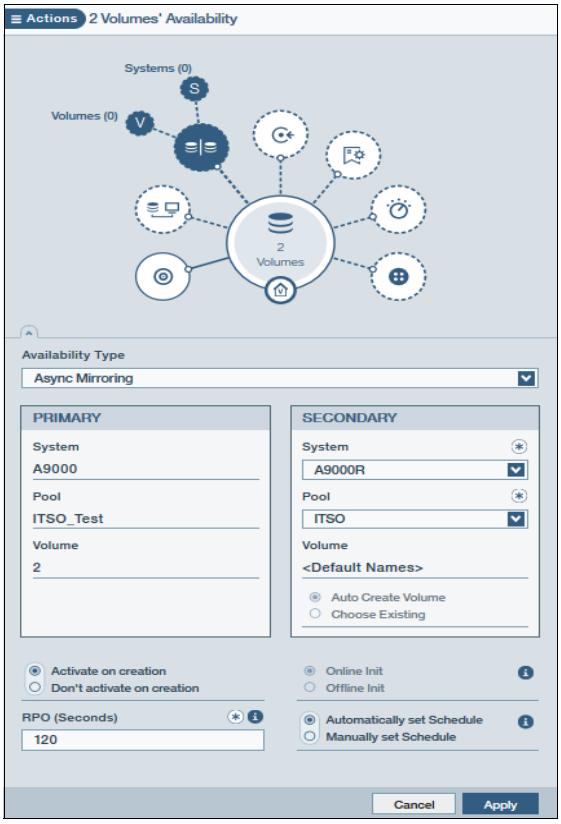


Figure 4-23 Volume asynchronous mirroring settings

5. You can check the mirroring initialization progress of one volume in the **Volumes** window. You can change the listing header, by right-clicking the header, to show the **Availability Type** and **Availability Status**. Figure 4-24 shows the source and target volumes. The value **RPO OK** in the Availability Status column means that the synchronization runs within the defined RPO.

Volume	System	Pool	Availability Type	Availability Status	System Con...	Availability Role	RPO
ITSO_Test_Vol1	A9000	ITSO_Test	Async Mirroring	RPO OK	OK	Primary	00:02:00
ITSO_Test_Vol1	A9000R	ITSO_T...	Async Mirroring	RPO OK	OK	Secondary	00:02:00
ITSO_Test_Vol2	A9000	ITSO_Test	Async Mirroring	RPO OK	OK	Primary	00:02:00
ITSO_Test_Vol2	A9000R	ITSO_T...	Async Mirroring	RPO OK	OK	Secondary	00:02:00
ITSO_Test_vol3	A9000	ITSO_Test	Async Mirroring	RPO OK	OK	Primary	00:02:00
ITSO_Test_vol3	A9000R	ITSO_T...	Async Mirroring	RPO OK	OK	Secondary	00:02:00

Figure 4-24 Asynchronous mirroring progress

6. You can check the status of one volume by selecting the **Availability** hub icon of a volume, as shown in Figure 4-25.

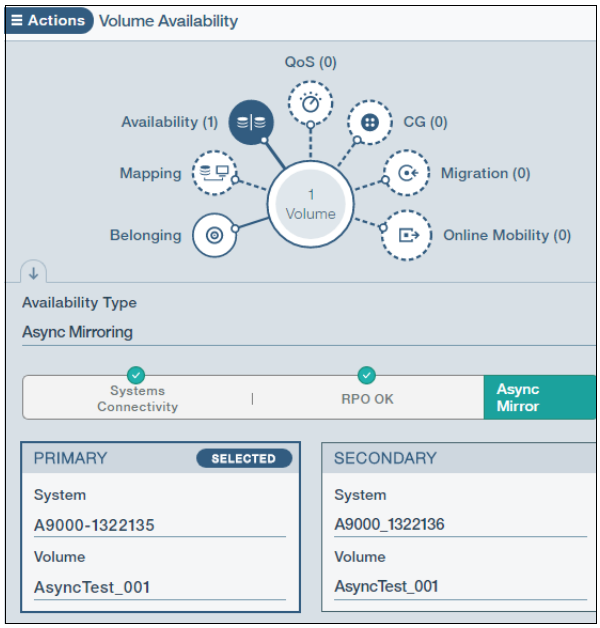


Figure 4-25 Mirroring status

You can see the snapshots associated with the mirrored volumes, which are created by the system, in the **Snapshots** view of the Hyper-Scale Manager, as shown in Figure 4-26.

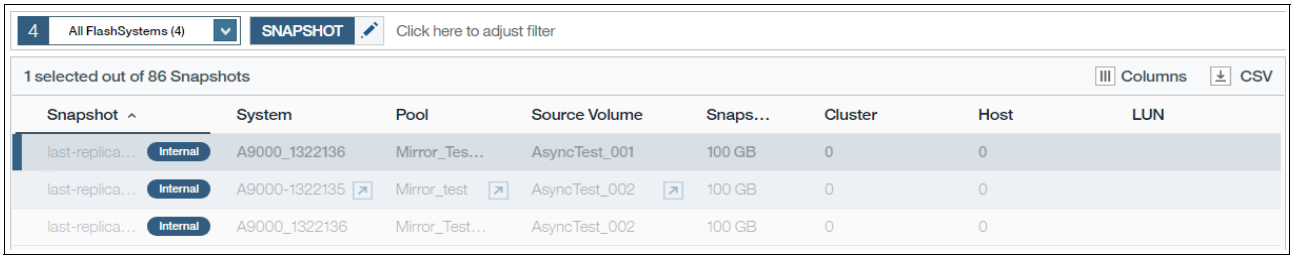


Figure 4-26 Snapshots associated with asynchronously mirrored volumes

The Snapshot Properties windows shows the details of an internal snapshot on the secondary, as shown in Figure 4-27.

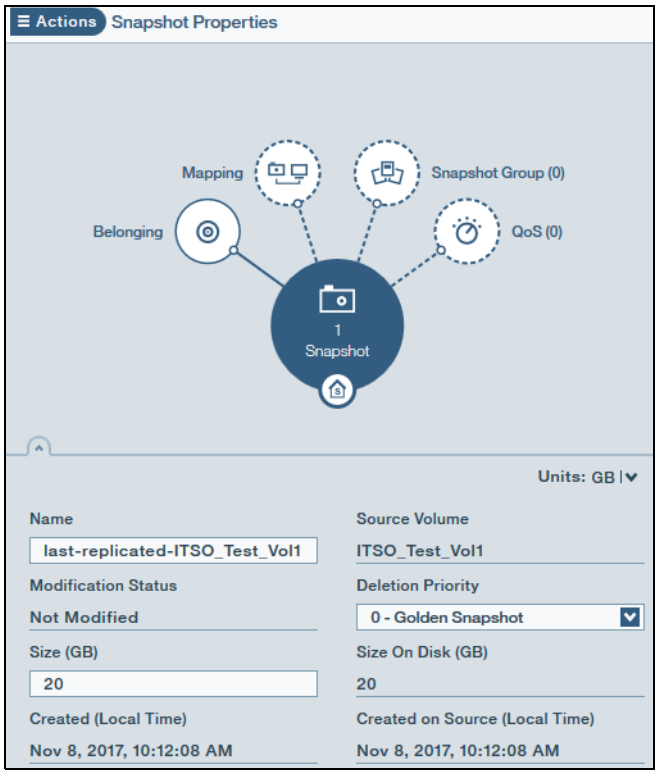


Figure 4-27 Snapshot detail

Defining asynchronous mirroring using XCLI

To set up async volume mirroring using XCLI, complete the following steps. The examples shown might have some rows of output deleted to aid in showing the examples:

1. Open an XCLI session for the primary and the secondary FlashSystem A9000 or A9000R and issue the identical **schedule_create** commands on each. Example 4-7 shows the syntax.

Example 4-7 XCLI schedule create on primary and secondary systems with a 5 min schedule interval

```
# On the primary
A9000>>schedule_create schedule=five_min interval=00:05:00
Command executed successfully.
# On the secondary
A9000R>>schedule_create schedule=five_min interval=00:05:00
Command executed successfully.
```

2. On the primary system, issue the **mirror_create** command, as shown in Example 4-8.

Example 4-8 XCLI mirror create with 1 hour RPO

```
A9000>>mirror_create vol=ITSO_Test_vol3 create_slave=yes remote_pool=ITSO_Test_R slave_vol=ITSO_Test_vol3
type=async_interval target="A9000R" schedule=five_min remote_schedule=five_min rpo=3600 remote_rpo=3600
Command executed successfully.
```

3. To list the couplings on the primary IBM FlashSystem A9000 or A9000R, issue the **mirror_list** command shown in Example 4-9. Note that the status of `Initializing` is used in the XCLI when the coupling is in standby, inactive, or is initializing.

Example 4-9 XCLI mirror list on primary

```
A9000>>mirror_list
Name           Mirror Type       Mirror Object   Role    Remote System   Remote Peer     Active   Standby   Status
Link Up
ITSO_Test_vol3   async_interval     Volume          Master   A9000R           ITSO_Test_vol3   no       no
Initializing   yes
```

4. To list the couplings on the secondary IBM FlashSystem A9000 or A9000R, run the **mirror_list** command, as shown in Example 4-10.

Example 4-10 XCLI mirror list on secondary

```
A9000R>>mirror_list
Name           Mirror Type       Mirror Object   Role    Remote System   Remote Peer     Active   Standby   Status
Link Up
ITSO_Test_vol3   async_interval     Volume          Slave    A9000           ITSO_Test_vol3   no       no
Initializing
```

5. Repeat steps 1-3 to create more mirror couplings.

To activate the mirroring, complete the following steps:

1. On the primary IBM FlashSystem A9000 or A9000R, run the **mirror_activate** command, as shown in Example 4-11.

Example 4-11 XCLI mirror activate on primary

```
A9000>>mirror_activate vol=ITSO_Test_vol3
Command executed successfully.
```

2. On the primary IBM FlashSystem A9000 or A9000R, run the **mirror_list** command. Example 4-12 shows the status of the couplings.

Example 4-12 XCLI mirror list on primary

```
A9000>>mirror_list
Name           Mirror Type       Mirror Object   Role    Remote System   Remote Peer     Active   Standby   Status
Link Up
ITSO_Test_vol3   async_interval    Volume         Master   A9000R          ITSO_Test_vol3   yes     no       RPO OK
yes
```

3. On the secondary IBM FlashSystem A9000 or A9000R, run the **mirror_list** command to see the status of the couplings, as shown in Example 4-13.

Example 4-13 Status of the couplings

```
A9000R>>mirror_list
Name           Mirror Type       Mirror Object   Role    Remote System   Remote Peer     Active   Standby   Status
Link Up
ITSO_Test_vol3   async_interval    Volume         Slave    A9000          ITSO_Test_vol3   yes     no       RPO OK
yes
```

4. Repeat steps 1-3 to activate more couplings.

4.5.2 Cross-Generational Mirroring with XIV Gen3

Cross-Generational (Cross-Gen) mirroring is a new asynchronous replication option that uses XIV Gen3 with FlashSystem A9000 or A9000R. To support Cross-Gen mirroring, XIV Gen3 firmware version 11.6.2.a or later and FlashSystem A9000 or A9000R firmware version 12.2.0 or later are required. The Cross-Gen mirroring functionality setup is supported in Hyper-Scale Manager Version 5.3 and XCLI 5.2.

Note: Cross-Gen mirroring is only supported with asynchronous replication with XIV Gen3.

The steps outlined previously in , “Defining asynchronous volume mirroring in Hyper-Scale Manager GUI” on page 91 are applicable for Cross-Gen mirroring definition.

Cross-Gen mirroring volumes must be in a decompressed reduction state on the XIV Gen3 to set up the mirroring relationship. Obviously, this restriction only applies for XIV Gen3 volumes and not for FlashSystem A9000 or A9000R volumes, which are always compressed. See Figure 4-28 showing the error message for a volume that is compressed on XIV Gen3 and cannot be mirrored in that state.

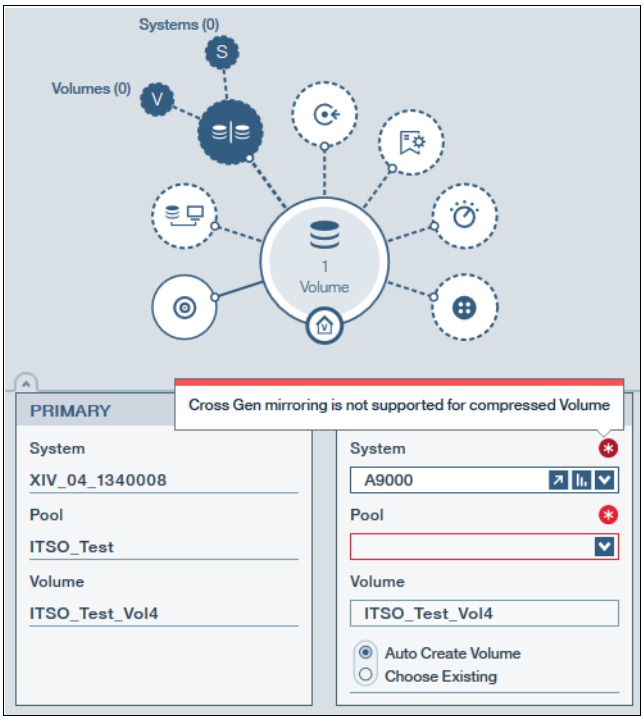


Figure 4-28 Warning message when trying to use XIV Gen3 compressed volume.

When an XIV Gen3 volume is already in a Cross-Gen mirroring relationship, the volume cannot be compressed. Figure 4-29 shows the error that you get if you try to compress an XIV Gen3 volume in a Cross-Gen mirror.

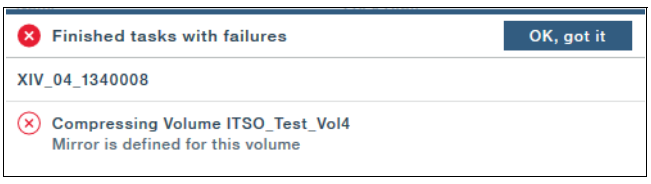


Figure 4-29 Error message seen when you try to compress a XIV Gen3 volume in Cross-Gen mirror

Defining Cross-Gen mirroring using XCLI

To set up asynchronous Cross-Gen volume mirroring between IBM FlashSystem A9000 or A9000R, and XIV Gen3 using XCLI, start by creating the target volumes as usual for any mirroring, then complete the following steps:

1. Open an XCLI session for the primary and the secondary FlashSystem A9000 or A9000R and XIV Gen3, and issue the identical **schedule_create** commands on each. Example 4-14 shows the syntax.

Example 4-14 XCLI schedule create for both primary and secondary systems with 5 min interval

```
# On the primary
A9000>>schedule_create schedule=five_min interval=00:05:00
Command executed successfully.
# On the secondary
XIV_04_1340008>>schedule_create schedule=five_min interval=00:05:00
Command executed successfully.
```

2. On the primary system, issue the **mirror_create** command, as shown in Example 4-15.

Example 4-15 XCLI mirror create on primary

```
A9000>>mirror_create vol=ITSO_test_vol5 create_slave=yes remote_pool=ITSO_Test slave_vol=ITSO_Test_vol5
type=async_interval target="XIV_04_1340008" schedule=five_min remote_schedule=five_min rpo=3600 remote_rpo=3600
Command executed successfully.
```

3. To list the couplings on the primary IBM FlashSystem A9000 or A9000R, or XIV Gen3, issue the **mirror_list** command shown in Example 4-16. Note that the status of `Initializing` is used in the XCLI when the coupling is in standby, inactive or is initializing.

Example 4-16 XCLI mirror list on primary

```
A9000>>mirror_list
Name           Mirror Type       Mirror Object   Role    Remote System   Remote Peer     Active   Standby   Status
Link Up
ITSO_test_vol5   async_interval     Volume          Master   XIV_04_1340008   ITSO_Test_vol5   no       no
Initializing   yes
```

4. To list the couplings on the secondary IBM FlashSystem A9000 or A9000R, run the **mirror_list** command, as shown in Example 4-17.

Example 4-17 XCLI mirror list on secondary

```
XIV_04_1340008>>mirror_list
Name            Mirror Type     Mirror Object   Role    Remote System   Remote Peer     Active   Standby   Status
Link Up
ITSO_Test_vol5   async_interval   Volume          Slave    A9000           ITSO_test_vol5   no       no
Initializing   yes
```

5. Repeat steps 1-3 to create more mirror couplings.

To activate the mirroring, complete the following steps:

1. On the primary IBM FlashSystem A9000, A9000R, or XIV Gen3, run the **mirror_activate** command, as shown in Example 4-18.

Example 4-18 XCLI mirror activate on primary

```
A9000>>mirror_activate vol=ITSO_test_vol5
Command executed successfully.
```

2. On the primary IBM FlashSystem A9000, A9000R, or XIV Gen3, run the **mirror_list** command (Example 4-19) to see the status of the couplings.

Example 4-19 XCLI mirror list on primary

```
A9000>>mirror_list
Name           Mirror Type      Mirror Object  Role    Remote System   Remote Peer      Active Standby Status Link Up
ITSO_Test_vol5 async_interval   Volume         Master  A9000R          ITSO_Test_vol5   Yes    no      RPO OK yes
```

3. On the secondary IBM FlashSystem A9000, A9000R, or XIV Gen3, run the **mirror_list** command (Example 4-20) to see the status of the couplings.

Example 4-20 XCLI mirror list on secondary

```
XIV_04_1340008>>mirror_list
Name           Mirror Type      Mirror Object  Role    Remote System   Remote Peer      Active Standby Status Link Up
ITSO_Test_vol5 async_interval   Volume         Slave   A9000           ITSO_Test_vol5   Yes    no      RPO OK yes
```

4. Repeat steps 1-3 to activate more couplings.

Note: The XCLI command line prevents you from creating an asynchronous mirroring relationship using a compressed XIV Gen3 volume (see Example 4-21).

Example 4-21 XCLI error when trying to do Cross-Gen mirroring with an XIV compressed volume

```
XIV_04_1340008>>mirror_create vol=ITSO_XIV_Vol1 create_slave=yes remote_pool=ITSO_Test slave_vol=ITSO_XIV_Vol1
type=async_interval target="A9000" schedule=five_min remote_schedule=five_min rpo=3600 remote_rpo=3600
Error:   COMPRESSION_NOT_SUPPORTED_IN_TARGET
Details: Compressed volume is not supported by the specified Target.
```

4.5.3 Using offline initialization

To avoid the impact of distance on initialization, you can use offline initialization. The peers can be synchronized locally and the secondary system moved to its remote site. Or, if the target system is already at a remote location with limited WAN capabilities, you can apply an image backup of the source volume onto the target. You can then activate the offline mirroring initialization. If a backup tape is physically transported to the remote site, it must be a volume image backup.

The mirror pairing is defined normally, with the addition of specifying the `offline init` option when making the definition of the pairing, as shown in Figure 4-30 on page 98. The target volume must be entered manually. The activation state is automatically set to *inactive* when using the `offline init` option.

If a remote mirroring configuration is set up when a volume is first created (that is, before any application data is written to the volume), initialization is fast.

When a consistency group mirror coupling is created, the CG must be empty so there is no data movement and the initialization process is fast.

The mirror coupling status at the end of initialization differs for synchronous mirroring and asynchronous mirroring. In either case, when initialization is complete, a consistent set of data exists at the remote site.

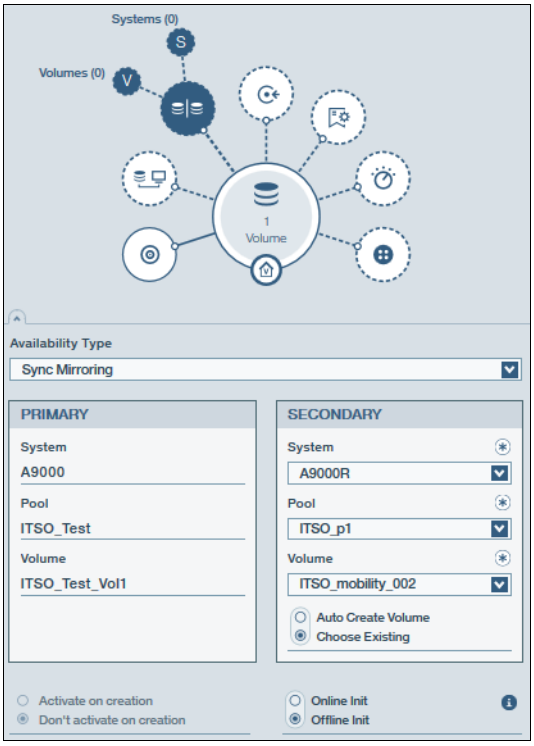


Figure 4-30 Offline init selected

4.5.4 Defining consistency group mirroring

Consistency group mirroring uses one CG on the source system and one CG on the target system. Both CGs must be empty, meaning they do not contain any volumes, before defining the CG mirroring.

1. Select an existing CG in the **Consistency Groups** view, and select **Availability** in the Hub view. Then select the type of availability (**Async Mirror**, **Sync Mirror**, or **HyperSwap**) to create, as shown in Figure 4-31.

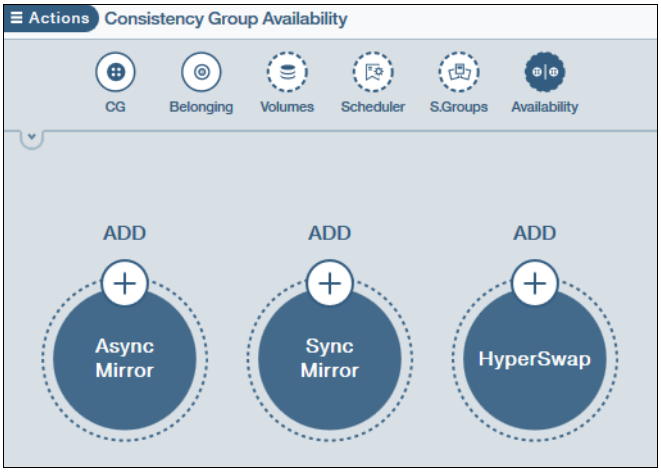


Figure 4-31 Mirroring options for Consistency Group

2. Then add the details of the **Secondary** system and any of the parameters for your selected mirror type. Figure 4-32 shows the parameters for Sync mirroring.

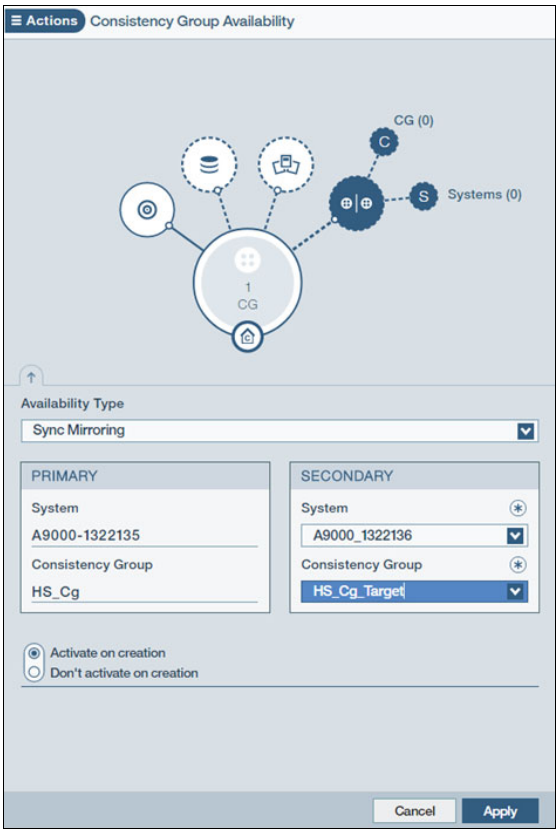


Figure 4-32 Consistency group mirror parameters for Sync mirroring

3. Click **Apply** to immediately establish the volume mirrors. Because there are no volumes in the CGs, the mirroring status is synchronized, as shown in Figure 4-33.

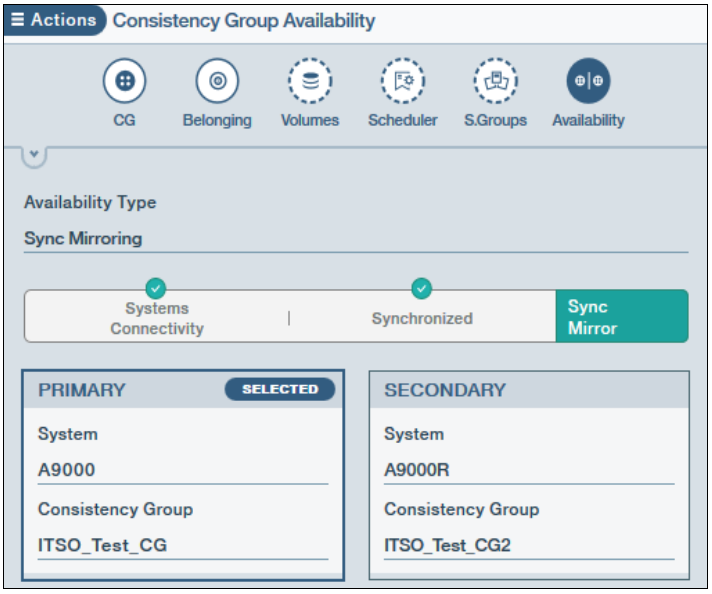


Figure 4-33 Consistency group mirroring status for Sync Mirror

4.5.5 Adding a mirrored volume to a mirrored consistency group

Before adding a volume to the CG, these prerequisites must be met:

- Volume and CG must be associated with the same primary pool and secondary pool.
- Both volume synchronization status and mirrored CG synchronization status are either `RPO OK` for asynchronous mirroring or `Synchronized` for synchronous mirroring.
- The volume mirroring settings must be identical to those of the CG:
  - Mirroring type
  - Mirroring role
  - Mirroring status
  - Mirroring secondary
  - Target pool

After a mirrored volume has completed initialization, the source volume can be added to a pre-existing mirrored CG. Only mirrored volumes can be added to a mirrored consistency group.

1. Select a mirrored volume (or more than one mirrored volume) in the **Volume** view and select **CG** in the Hub view, click **Add CG** beneath the Hub view.
2. Select the Consistency Group and click **Apply** to add the volume to the chosen consistency group as shown in Figure 4-34. All volumes have the same mirrored synchronization state in a mirrored consistency group. In this example consistency group, the volume mirror is RPO OK, so all volumes that are added to this consistency group must be RPO OK.

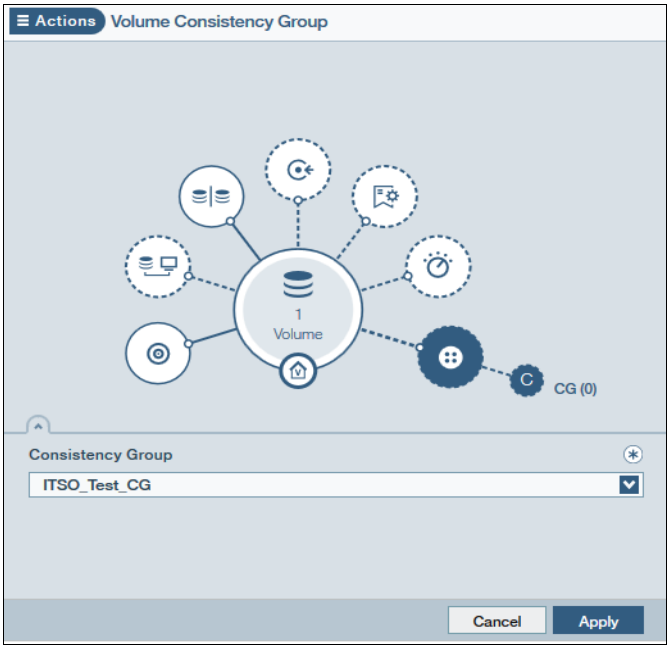


Figure 4-34 Adding a mirrored volume to a mirrored consistency group

3. Select the CG in the **Consistency Groups** view and select **Volumes** in the Hub view, as shown in Figure 4-35.

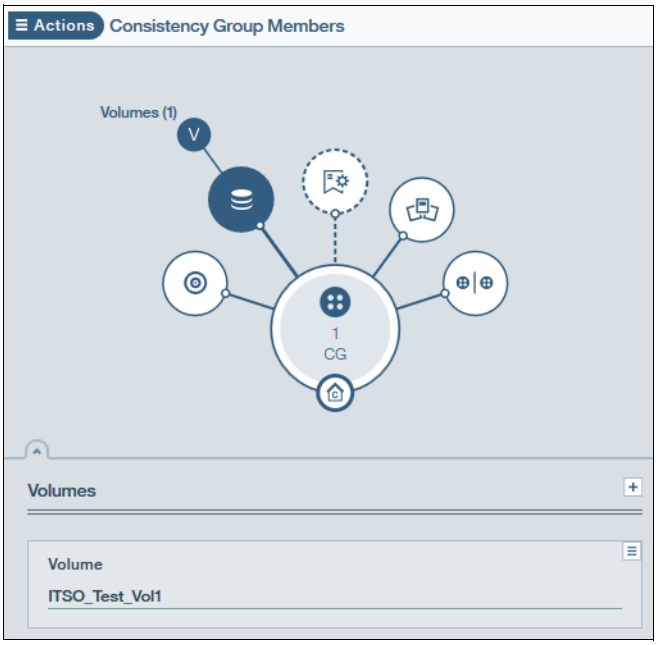


Figure 4-35 Consistency group reference to the mirrored volumes

4. When the **V** icon is selected, from Figure 4-35, the mirrored volumes of the mirrored consistency group are listed, as shown in Figure 4-36.

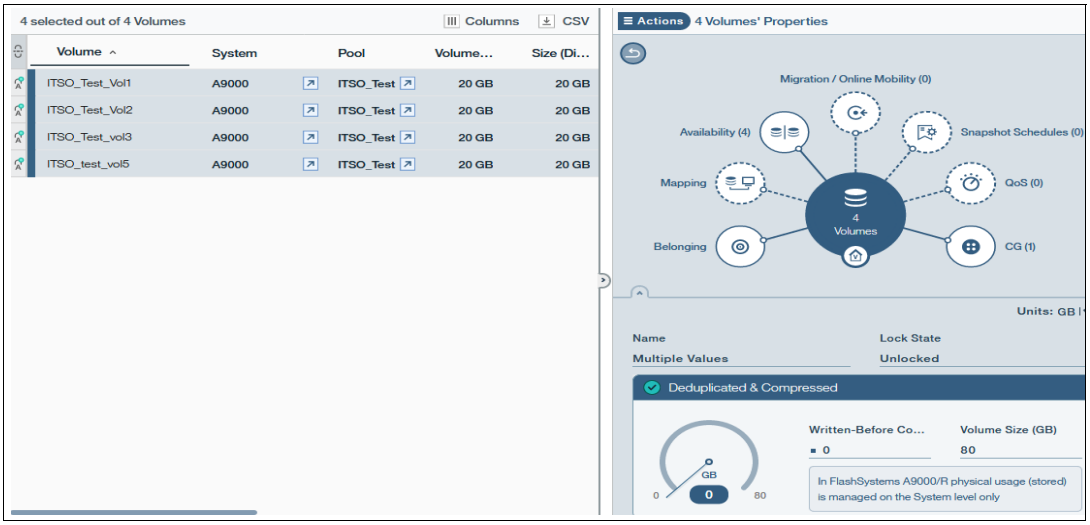


Figure 4-36 Listing of the mirrored volumes in a mirrored consistency group

A mirrored volume can only be in one mirrored CG. Adding a mirrored volume, which is a member of a mirrored CG, to another mirrored CG automatically removes the volume from the previous mirrored CG.

It is also important to realize that in a CG, all volumes have the same role, the same domain, and the same pool on each site. All volumes in a CG have the same role. CGs are handled as a single entity, and, in asynchronous mirroring, a delay in replicating a single volume affects the status of the entire CG.

4.6 Migrating data by using remote mirroring

Remote mirroring can be used to migrate data to a newly installed FlashSystem A9000 and A9000R system if the source data is on an FlashSystem A9000, A9000R, or XIV Gen3 system. This process is basically the same as described in 4.5, “Using remote mirroring” on page 87:

Note: If XIV Gen3 systems are used for remote mirroring, only asynchronous mirroring is supported.

1. Define the target system connectivity.
2. Define mirror coupling peer volumes.
3. Create a mirrored consistency group.
4. Add volumes to the mirrored consistency group.

   Adding the volumes to a consistency group is optional, but doing so is convenient because the set of volumes can be treated as a group, simplifying the following processes.
5. Wait for synchronization to complete.
6. Switch the roles of the volumes.

   The migrated volumes are then available for Host activity with a backup copy at the original site. When mirroring is active and synchronized (consistent), the source and target roles of mirrored volumes or consistency groups can be switched simultaneously. Role switching is typical for returning mirroring to the normal direction after changes have been mirrored in the reverse direction after a production site switch. Role switching is also typical for any planned production site switch.
7. Host server write activity and remote mirroring activity must be paused briefly before and during the role switch. Additionally, in the case of asynchronous mirroring, at least one sync job must complete before the switch to ensure the expected point-in-time copy of the data exists. Figure 4-37 on page 103 shows the action path for switching the role. Notice that this was done by right-clicking the consistency group to open the **Actions** menu.

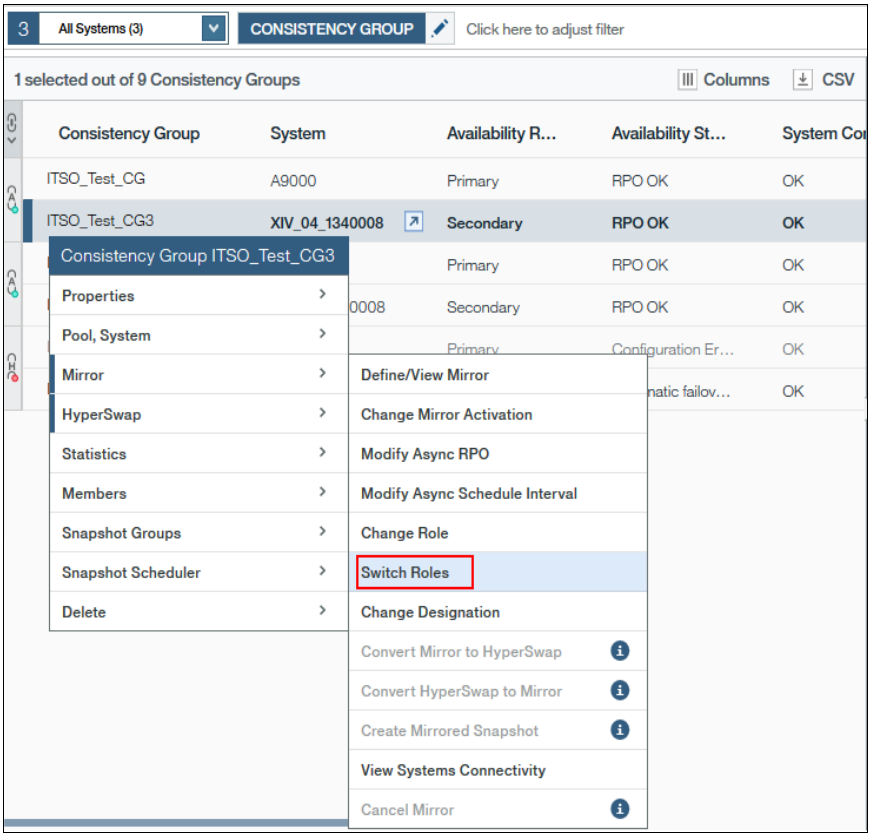


Figure 4-37 Selecting a consistency group to switch roles

8. Select **Switch Roles** for the current and new role information, and optionally set a **Designation** of a volume starting with Hyper-Scale Manager 5.3, as shown in Figure 4-38. The storage administrator can specify a designation in a mirroring relationship that might not be the same as the role. This is a logical setting and has no impact on the role of the volumes and consistency groups in a mirroring relationship.

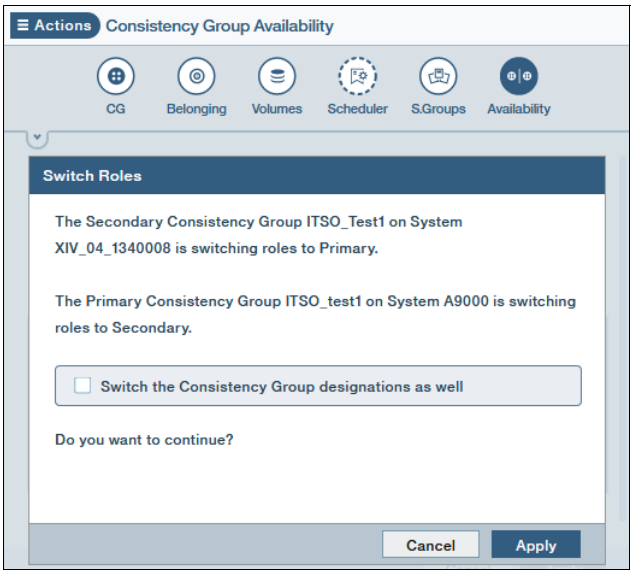


Figure 4-38 Switch roles confirmation prompt with an optional switching of designation

Changing the designation of a volume or consistency group pair in a mirroring relationship enables the user to logically specify if a volume or consistency group should be designated as a primary or secondary despite what the current role is. For example, if a relationship has been defined but the designation of the site changes from a primary to a secondary, then the user can also change the designation of the pair to match, without going through a failover. Making this change does not change the current role of a volume or consistency group.

9. Click **Apply** to switch the roles, which shows the switched role status, as shown in Figure 4-39.

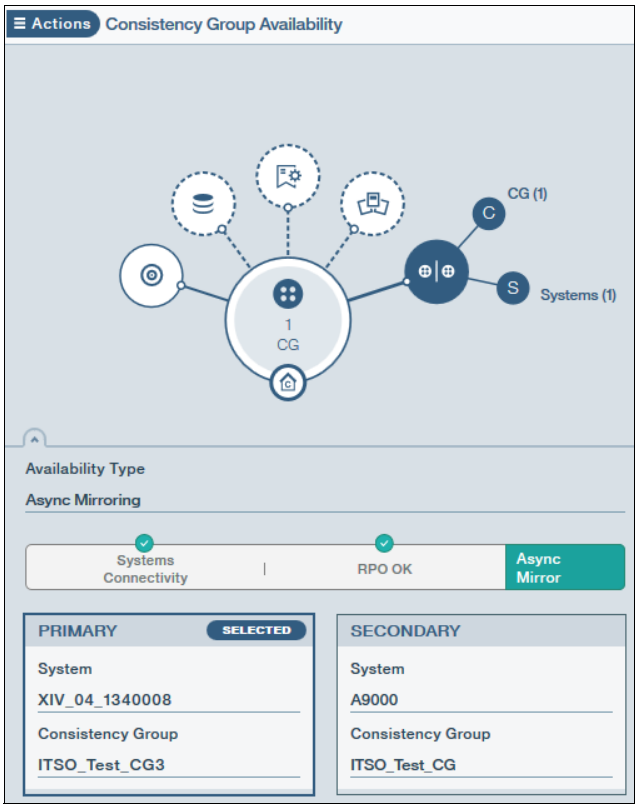


Figure 4-39 Switched roles

The volumes are now active on the secondary IBM FlashSystem A9000 and A9000R system, and mirroring is active to the original source system. Hosts can now access the volumes at the secondary site and any changes are mirrored to the original source volumes.

Note: If continuous availability is required in a synchronous mirroring relationship, consider using HyperSwap to avoid any host downtime when migrating data to the new system.

4.7 Recovering from a site failure

One of the reasons for remote mirroring is to keep a copy of data in a different location in case something happens to the source site. In the case of a real disaster, the systems at the local site might need to be replaced. In such circumstances, the production activity moves to the remote site and, when the local site is restored, data can be migrated back as described in 4.6, “Migrating data by using remote mirroring” on page 102.

4.7.1 System failure at the local site

Figure 4-40 shows a connectivity failure between the source system and the target system. The mirror definitions still exist on the target system and the role of those volumes can be changed to source.

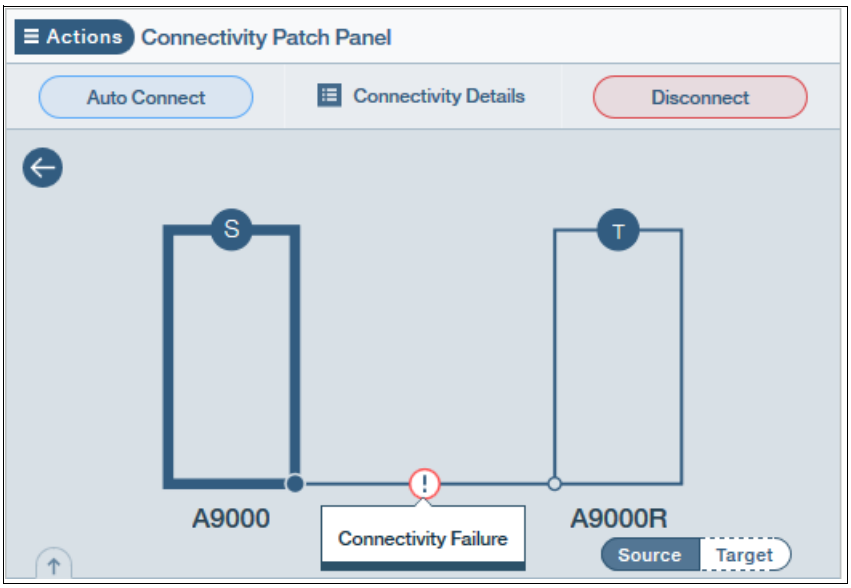


Figure 4-40 Local site system failure

Figure 4-41 shows the details of the mirrored volume status after the connectivity between the source system to the end target system that failed.

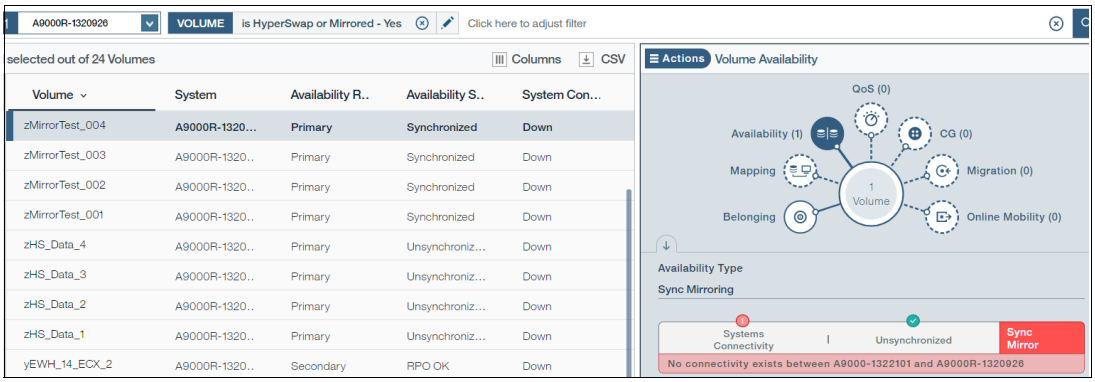


Figure 4-41 Unsynchronized mirrored volume after link failure

Figure 4-42 shows the details of the connectivity between the source and target system. In this example, all connections between the A9000 (source system) and the A9000R (target system) failed.

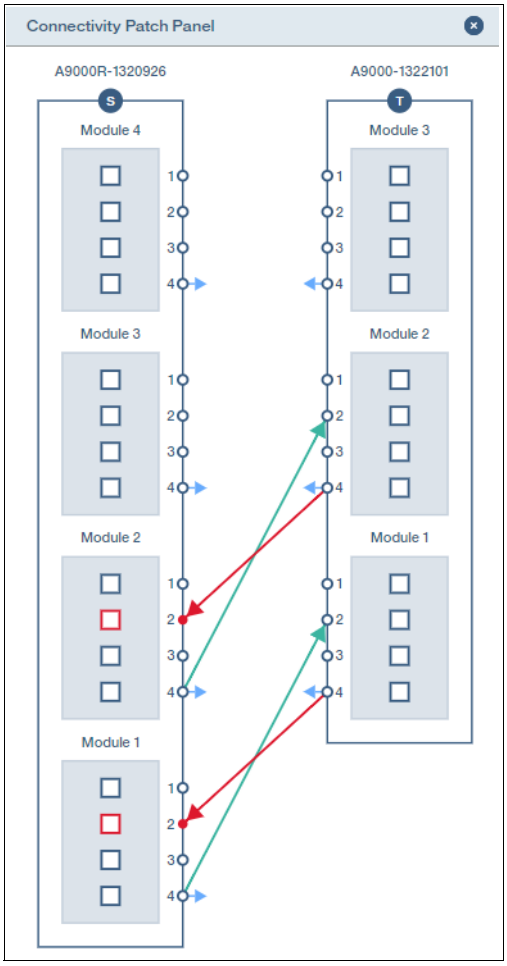


Figure 4-42 Connectivity to the target site has failed

4.7.2 Changing role of target volume or CG

The system at the secondary site needs to be prepared to become the primary system. To make this change, the roles of the target volumes are changed to source volumes, and then host systems are able to access the last consistent copy of the production data.

When mirroring is active, the target volume or CG is locked and write access is prohibited. To allow write access to a target peer in case of failure or unavailability of the source, the target volume role must be changed to the source role. The mirroring status is unsynchronized.

In unsynchronized state, the switch role function, as shown for a CG in Figure 4-38 on page 103, is not available. You must use the change role function as shown in Figure 4-43. In this example, the role of a mirrored volume is changed.

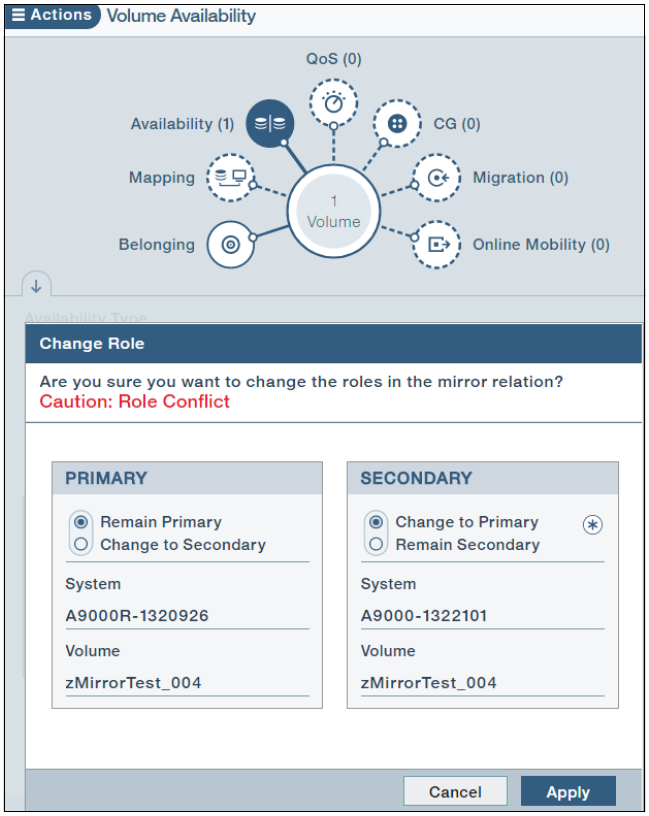


Figure 4-43 Changing role of target volume or CG to become primary

Click **Apply** to change the role of the secondary volume to primary. Changing the role of a volume from secondary to primary allows the volume to be accessed. In synchronous mirroring, changing the role also starts metadata recording for any changes that are made to the volume. This metadata can be used for resynchronization (if the new source volume remains the source when remote mirroring is reactivated). In asynchronous mirroring, changing a peer's role automatically reverts the peer to its last-replicated snapshot.

The volume on the secondary site has changed its role from secondary to primary. The volume is now accessible from a host.

4.8 Deleting mirror coupling definitions

When a mirror coupling is deleted, all metadata and mirroring definitions are deleted, and the peers do not have any relationship at all. However, any volume and consistency group mirroring snapshots remain on the local and remote systems. To restart mirroring, you can use offline initialization instead of a full copy of data.

If you want to delete the existing mirroring between two FlashSystem A9000 or A9000R systems, you must deactivate and delete the volume or CG mirroring and its mirrored volumes first. In case the link between the systems is broken, you must run the procedure on both systems.

Steps to deactivate and delete the mirror volume or CG are shown by using the XCLI in Example 4-22, and by using HSM in Figure 4-44, Figure 4-45 on page 109, and Figure 4-46 on page 109.

Example 4-22 Deactivate and deleting mirroring

```
# Deactivate and delete the mirror on the source system
============================================================
A9000R>>mirror_deactivate vol=P8_DB_001
Warning:   Are you sure you want to deactivate mirroring? y/n: y
Command executed successfully.
A9000R>>mirror_delete vol=P8_DB_001
Warning:   Are you sure you want to delete this mirroring relationship? y/n: y
Command executed successfully.

# Deactivate and delete the mirror on the target system
A9000>>mirror_deactivate vol=P8_DB_001
Warning:   Are you sure you want to deactivate mirroring? y/n: y
Command executed successfully.
A9000>>mirror_delete vol=P8_DB_001
Warning:   Are you sure you want to delete this mirroring relationship? y/n: y
Command executed successfully.
```

1. Select your volume or CG and go to the Actions Menu and select **Mirror > Change Mirror Activation** where you can select **Activation State: Inactive** as shown in Figure 4-44 to change the mirror state.

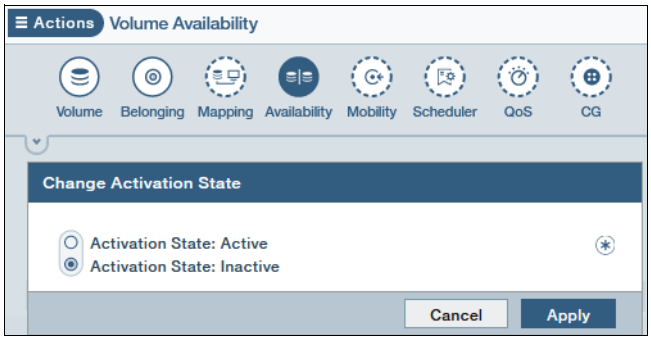


Figure 4-44 Volume Change Activation State

2. Click **Apply** and you see the confirmation page showing the mirror state as Inactive, as shown in Figure 4-45 on page 109.

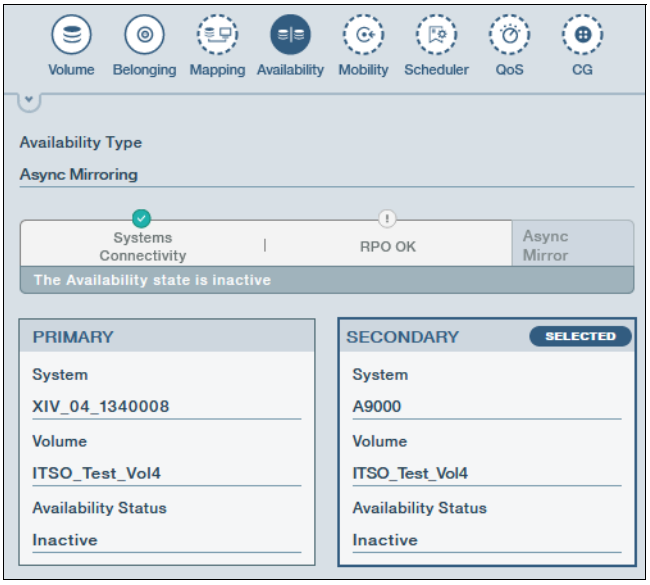


Figure 4-45 Confirmation of mirror set to Inactive.

3. Now you can delete the volume or CG mirror from the Actions Menu **Mirror** → **Cancel Mirror** and confirm by selecting **Apply**, as shown in Figure 4-46.

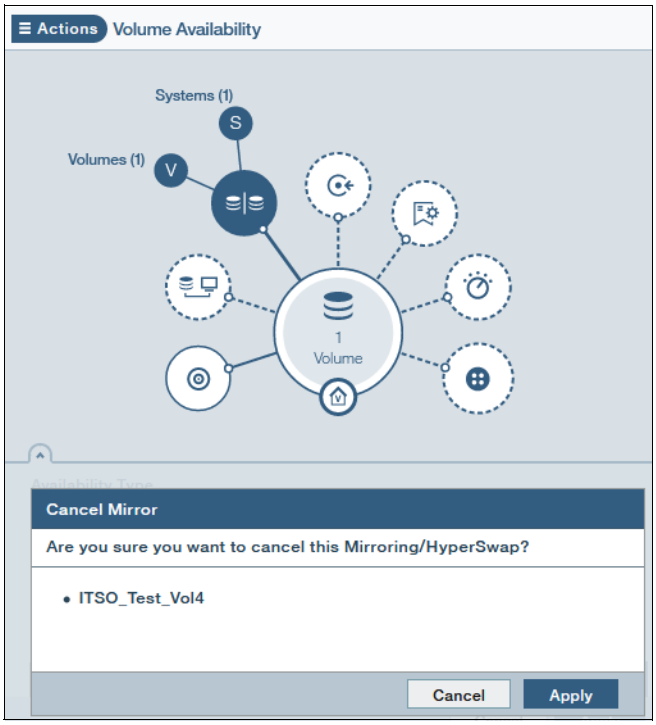


Figure 4-46 Cancel Mirror window

The connectivity can be deleted by using XCLI commands, as shown in Example 4-23.

Example 4-23 Mirroring connectivity deletion

```
# Delete connectivity and ports on the source system
============================================================
A9000R>>target_connectivity_list
```

```
Target Name   Remote Port        FC Port         IP Interface   Active   Up
A9000         5001738056730131   1:FC_Port:4:3                  yes      no
A9000         5001738056730113   1:FC_Port:1:3                  yes      no
A9000R>>target_connectivity_delete target=A9000 fcaddress=5001738056730131
local_port=1:FC_Port:4:3
Command executed successfully.
A9000R>>target_connectivity_delete target=A9000 fcaddress=5001738056730113
local_port=1:FC_Port:1:3
Command executed successfully.

A9000R>>target_port_list
Target Name   Port Type   Active   WWPN              iSCSI Address   iSCSI Port
A9000         FC          yes      5001738056730131                  0
A9000         FC          yes      5001738056730113                  0
A9000R>>target_port_delete target=A9000 fcaddress=5001738056730131
Command executed successfully.
A9000R>>target_port_delete target=A9000 fcaddress=5001738056730113
Command executed successfully.

============================================================
# Delete connectivity and ports on the target system
============================================================
A9000>>target_connectivity_list
Target Name   Remote Port        FC Port         IP Interface   Active   Up
A9000R        5001738051A60132   1:FC_Port:1:4                  yes      yes
A9000R        5001738051A60120   1:FC_Port:3:4                  yes      yes
A9000>>target_connectivity_delete target=A9000R fcaddress=5001738051A60132
local_port=1:FC_Port:1:4
Command executed successfully.
A9000>>target_connectivity_delete target=A9000R fcaddress=5001738051A60120
local_port=1:FC_Port:3:4
Command executed successfully.

A9000>>target_port_list
Target Name   Port Type   Active   WWPN              iSCSI Address   iSCSI Port
A9000R        FC          yes      5001738051A60120                  0
A9000R        FC          yes      5001738051A60132                  0
A9000>>target_port_delete target=A9000R fcaddress=5001738051A60120
Command executed successfully.
A9000>>target_port_delete target=A9000R fcaddress=5001738051A60132
Command executed successfully.
```

The last step is to delete the target definition on the source and the target system, as illustrated in Example 4-24.

Example 4-24 Delete mirror target definition

```
# Delete target on the source system
A9000R>>target_delete target=A9000
Command executed successfully.

# Delete target on the target system
A9000>>target_delete target=A9000R
Command executed successfully.
```

To delete the connections between two mirrored systems by using the GUI, complete the following steps:

1. Click **Disconnect** in the Connectivity Patch Panel window, as shown in Figure 4-47, and click **Apply** in the resulting confirmation window.

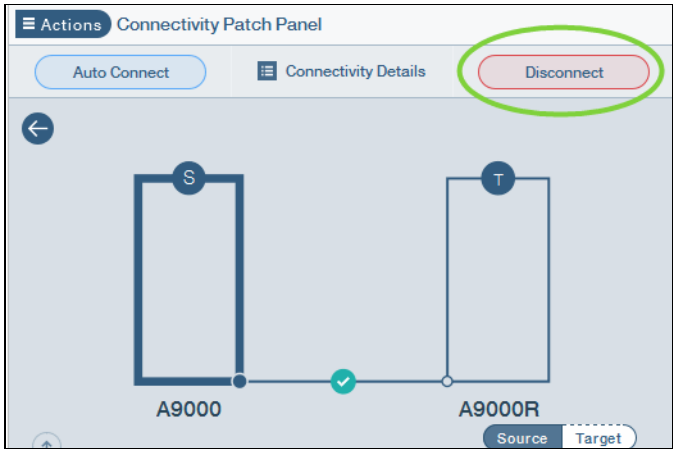


Figure 4-47 Target Connectivity Disconnect

2. From the **Targets** spoke in the Systems Hub display, click the **Targets Actions** menu and select **Remove Target**, as shown in Figure 4-48. Click **Apply** in the resulting confirmation window.

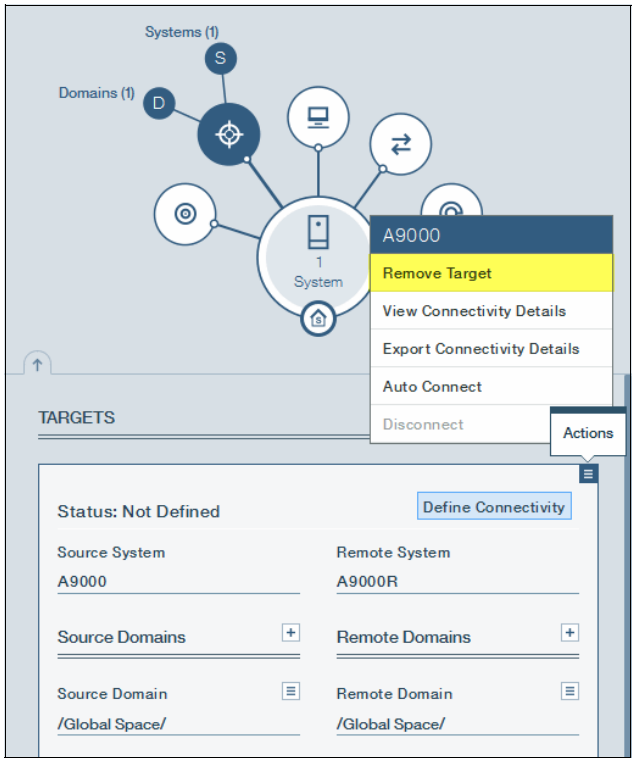


Figure 4-48 Remove Target (links have already been removed)

Typical usage of mirror deletion would be after a one-time data migration using remote mirroring. This process includes deleting the mirror couplings after the migration is complete.

4.9 Recovery from a temporary site outage

In the example described in this chapter, the “local site” is considered the production site, while the “remote site” is considered the original disaster recovery site.

A temporary site outage might require moving production host activity to the disaster recovery location. This move can be accomplished by using the procedure for recovering from a site failure. After the production system is restored, the mirroring can be resumed.

In asynchronous mirroring, changing a peer’s role from secondary to primary automatically reverts the peer to its last-replicated snapshot.

This scenario shows recovery from a temporary failure using a consistency group. The similar scenario without a consistency group follows similar steps:

1. Changing the consistency group mirror of remote site to primary. See 4.9.1, “Enabling production on the remote site”.

   Hosts can then access the volumes of the remote site for reading and writing.

2. Reactivation of the local site and resynchronization of the local site from the data in the remote site. See 4.9.2, “Recovering the local site” on page 114.

   After the local site is recovered, the role of the consistency group mirror on the local site must be changed to secondary to allow the data to be resynchronized from the remote site. The data modified on the remote site during the period it served as production site is mirrored back to the local site (original production site). When the resynchronization completes, the volumes of the mirrored consistency group are synchronized again.

3. After the mirror is synchronized, the original roles of the local and remote sites can be restored by switching the roles of the consistency group mirror (the current source site) back to secondary. See 4.9.3, “Restoring the original DR configuration” on page 117.

   When this step is completed, the local site serves as production site and the remote site as disaster recovery site.

The sections that follow describe the Hyper-Scale Manager commands for a mirrored consistency group. Equivalent Hyper-Scale Manager commands also exist for mirrored volumes, which are not members of a consistency group.

4.9.1 Enabling production on the remote site

After the failure of the local site, the **`change role`** command is used to change the role of the volumes at the remote site to primary role to enable host access to the volumes:

1. Because the volumes are in a mirrored consistency group, the **`change role`** command must be used on the consistency group, as shown in Figure 4-49.

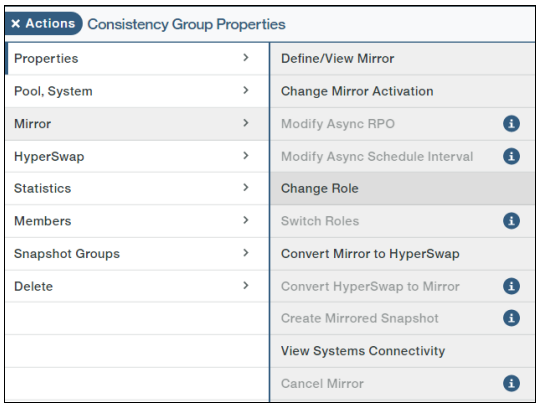


Figure 4-49 Consistency group change role command

2. Change the role of the remote (original disaster recovery) system to **Change to Primary**, as shown in Figure 4-50.

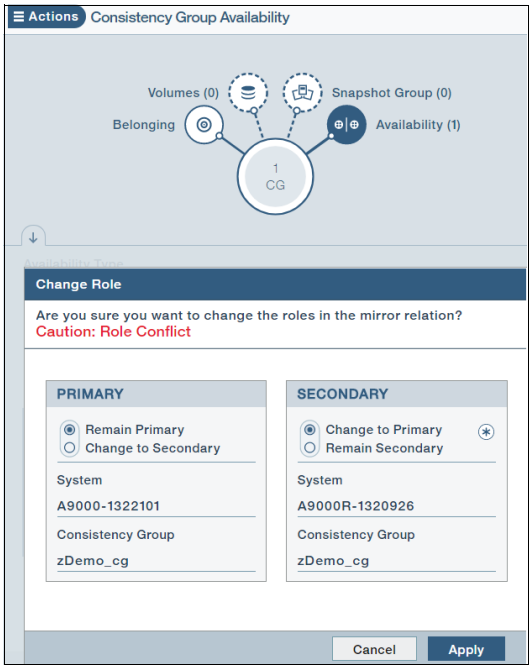


Figure 4-50 Changing the role of the consistency group

3. Click **Apply** to start the role change. Because the primary site is not connected, only the remote (secondary) system's role can be changed.

   At this point in the recovery, both sites have the Primary role.

4. Map the volumes of the remote system to the host. The host can now connect and use the volumes at the remote site that contains the updated data mirrored from the local site before the failure.

4.9.2 Recovering the local site

When the local site becomes available again, recovery of the two-site DR configuration can commence and restore a configuration where the remote site holds the role of Primary and the local site holds the role of Secondary. The first step in the recovery is a change in the role of the consistency group in the local site to Secondary. After the link between the sites is reestablished and the local site consistency group role is changed to Secondary, the mirror relation can be activated to start resynchronization of the modified data from the remote site to the local site.

1. In the Consistency Group Availability window, hover over the availability state, circled in Figure 4-51. This action guides you through the steps needed to recover replication from the remote site to the local site. Notice that the connectivity has been recovered and is now reported as a good state.

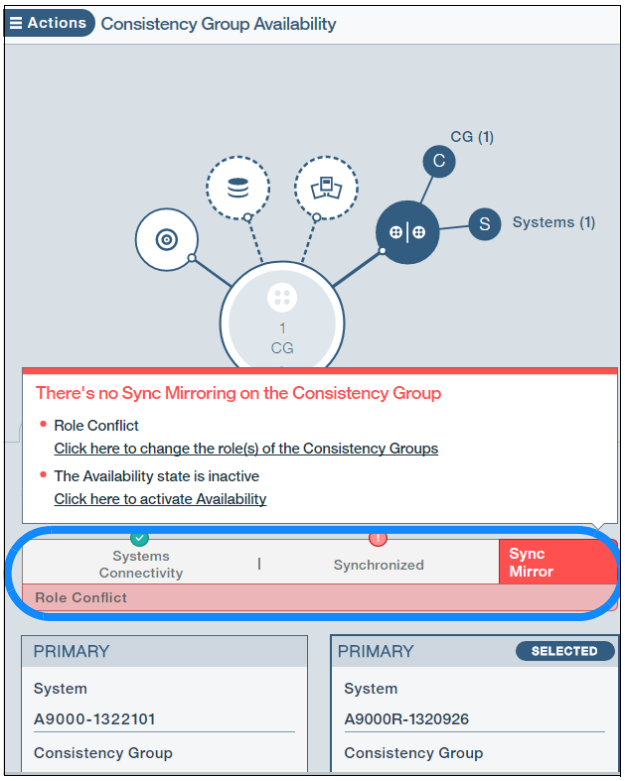


Figure 4-51 Status of CG mirroring with role conflict

2. Click the link under **Role Conflict**, in Figure 4-51 on page 114, to change the roles. This action brings up the role change view. Because you are ready to copy the changes made while mirroring was down back to the local (original production) site, select **Change to Secondary** on the local site as shown in Figure 4-52. Keep track of which system is local (original production) and remote (disaster recovery) site. Click **Apply** to submit the change.

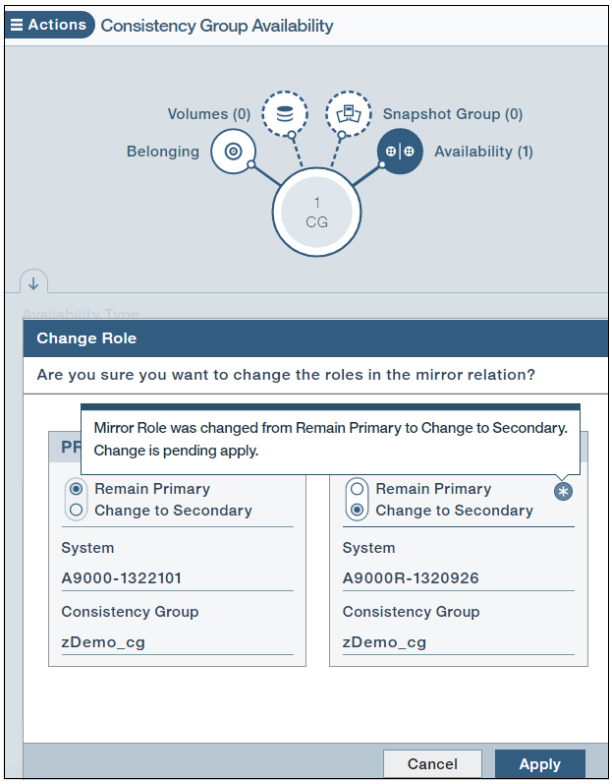


Figure 4-52 Change role of original production system to secondary

3. The next step is to activate the mirror (or consistency group mirror). Use the link **Click here to activate Availability** circled in Figure 4-53. Click the link to open the **Change Activation State** window to activate the mirroring as shown in Figure 4-53.

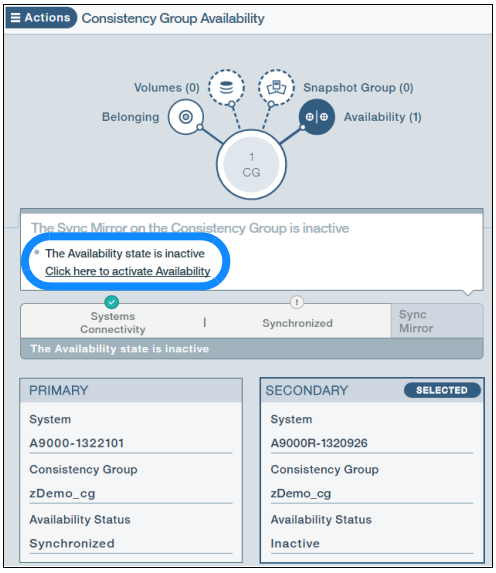


Figure 4-53 Reactivating the consistency group

4. You must select **Activation State: Active** for the state. Click **Apply** to make the change, as shown in Figure 4-54.

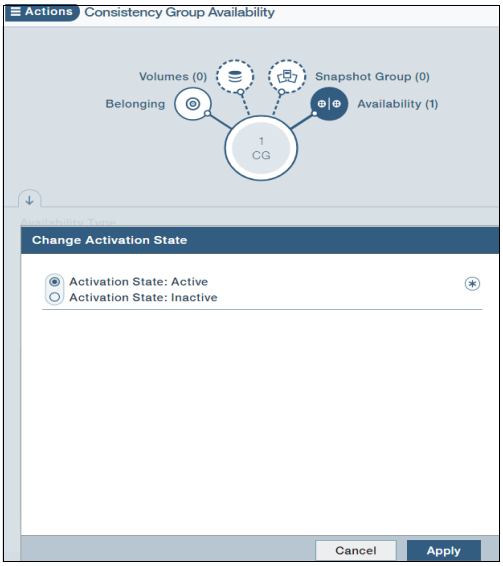


Figure 4-54 Activate mirroring

Note: Review 4.3.4, “Link failure and last consistent snapshot” on page 80 should a failure during resynchronizing, warning on the existence of last consistent snapshot or LCS, occur.

5. After successful resynchronizing of the volumes, the consistency group will show the Availability State as *synchronized*, as shown in Figure 4-55. Notice the icon to the left of the consistency group name is now green, which indicates that this is the primary system in a synchronous mirroring relationship.

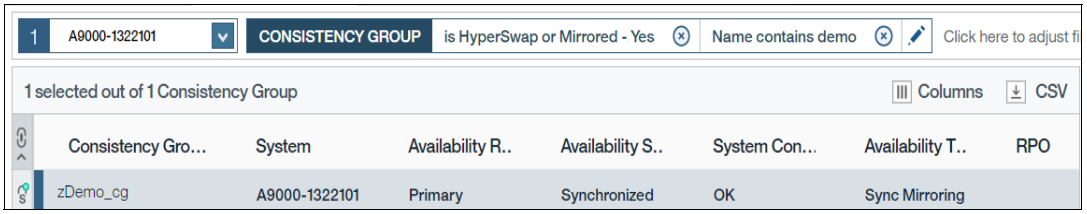


Figure 4-55 CG is synchronized and secondary site is the source site

4.9.3 Restoring the original DR configuration

When the mirror is synchronized it is possible to switch the roles back so that the local site is again the production site and the remote site is the disaster recovery site. To change the local site role back to primary, use the Switch Role action. Note that as part of this procedure, you will need to unmap the hosts from the volumes at the remote site and, after the roles are switched, map them to the volumes at the local site.

1. Open the Switch Roles window by right-clicking the consistency group and selecting **Mirror** → **Switch Roles**, as shown in Figure 4-56. This operation must be carried out on the consistency group holding the Primary role, that is, the consistency group on the system at the remote site.

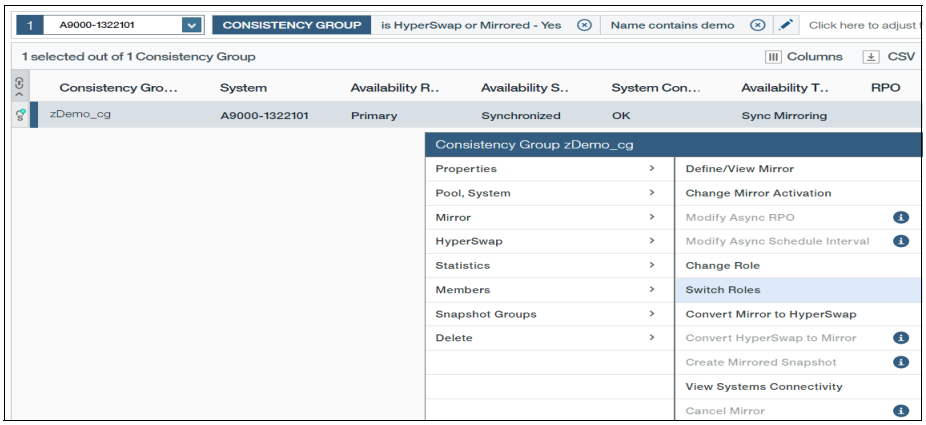


Figure 4-56 Switch role command for consistency group

2. Click **Apply**, as shown in Figure 4-57, to switch the roles of the primary and secondary site.

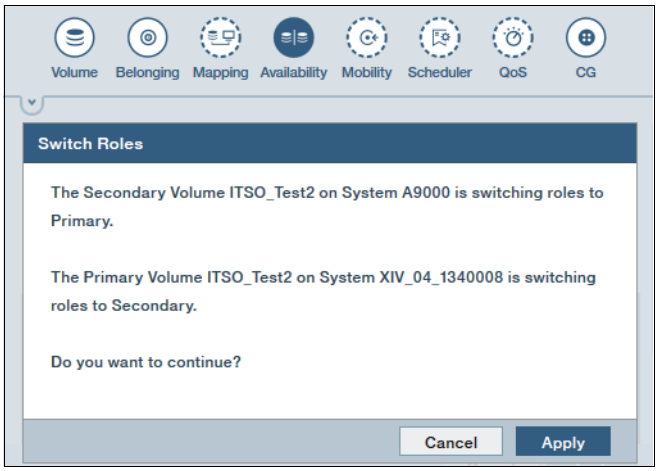


Figure 4-57 Switch role details

3. The local site now has the primary role again, and the remote site has the secondary role, as shown in Figure 4-58.

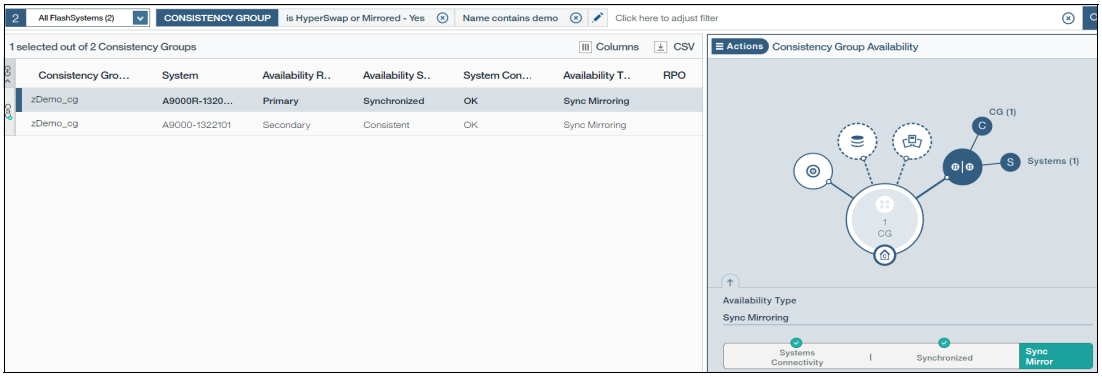


Figure 4-58 The production system has the source role again

The volumes of the consistency group now have the same roles as before the site failure occurred. The local (original production) system has the primary role, as shown in Figure 4-59.

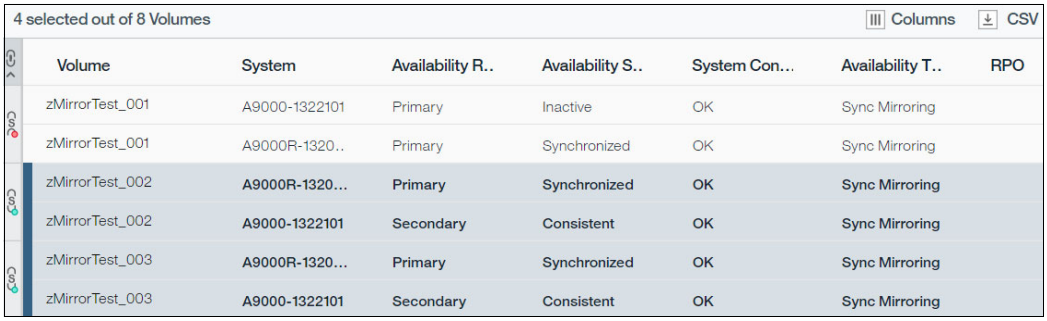


Figure 4-59 Volume mirroring roles back to the roles they had before the site failure

4.10 Temporary deactivation of mirroring

The following examples are of mirror deactivation and reactivation in the same direction:

- Remote mirroring is temporarily deactivated because of a communication failure and then automatically reactivated by the system when communication is restored.
- Remote mirroring is temporarily deactivated to create an extra copy of consistent data at the secondary site.
- Remote mirroring is temporarily deactivated by user action during peak load in an environment with constrained network bandwidth.
- Planned deactivation of remote mirroring can be done to suspend remote mirroring during a planned network outage or DR test.

4.10.1 Consistency group and volume state after link failure

Figure 4-60 shows the mirror status **Unsychronized** of a consistency group after the link between the source and target system failed.

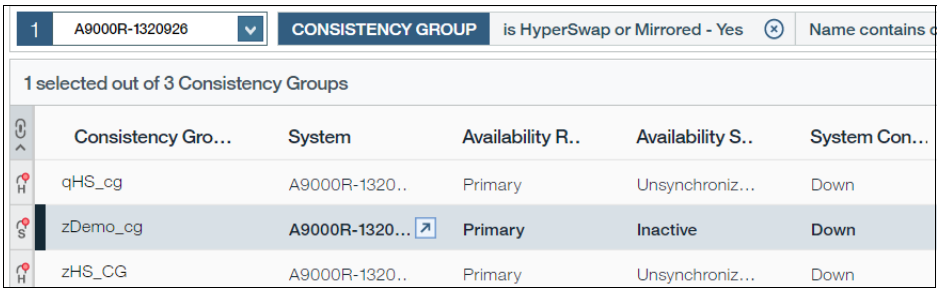


Figure 4-60 Unsynchronized consistency group after link failure

Figure 4-61 shows the mirror status **Unsychronized** for the volume of the consistency group after the link between the source and target system failed.

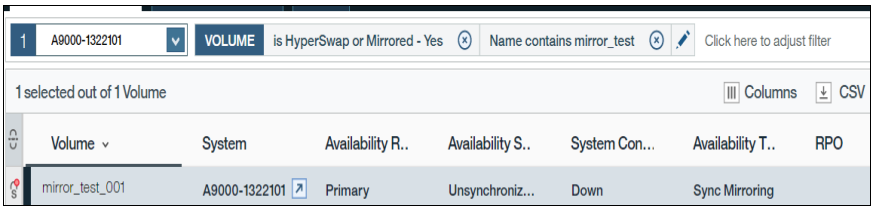


Figure 4-61 Unsynchronized volume after link failure

4.10.2 Consistency group and volume state after the link is restored

After the link is reestablished, the volumes are automatically resynchronized, as shown in Figure 4-62.

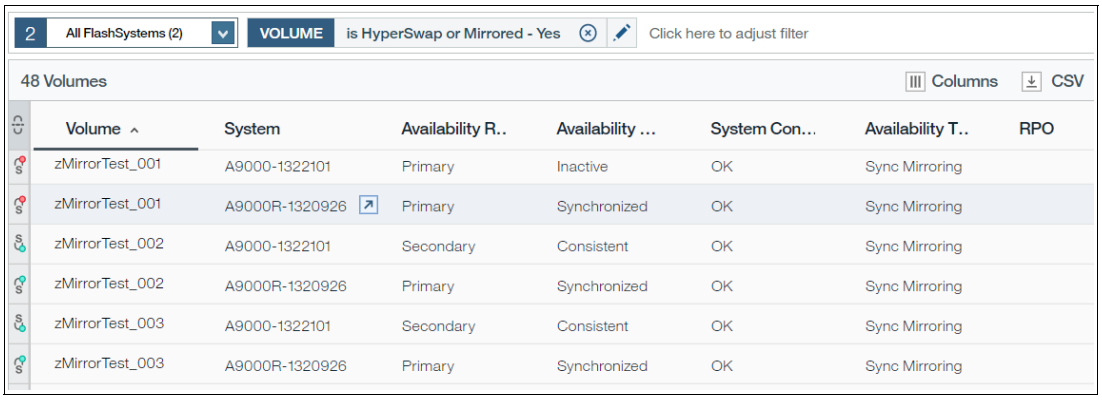


Figure 4-62 Resynchronized mirrored volumes

After the volumes are resynchronized, the consistency group is in the synchronized state again, as shown in Figure 4-63.

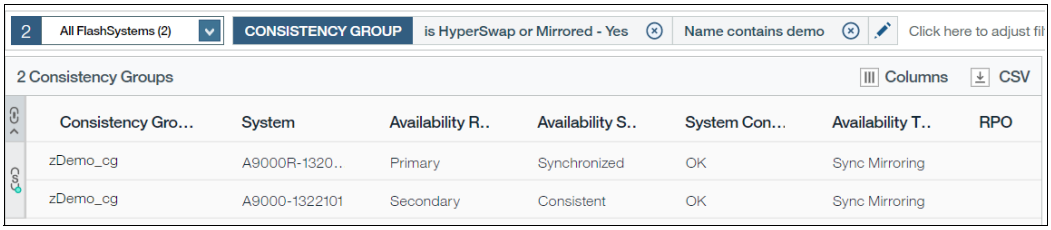


Figure 4-63 Resynchronized consistency group

4.10.3 Deactivating mirror coupling: Change recording

A mirror coupling can be deactivated by a user action:

1. Use the **Mirror** → **Change Mirror Activation** command in the Hyper-Scale Manager, as shown in Figure 4-64.

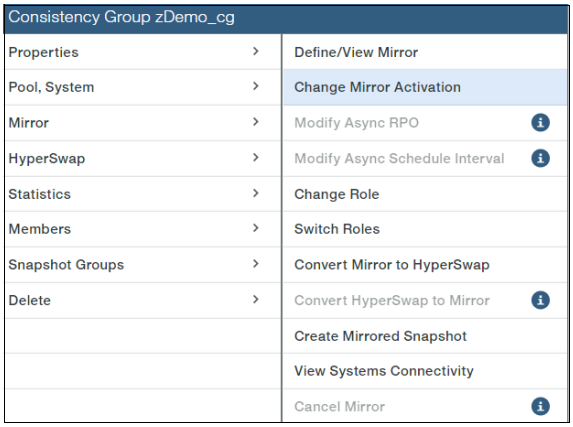


Figure 4-64 Changing the activation state of a mirrored consistency group.

2. Select **Activation State: Inactive**, and click **Apply** to change the state, as shown in Figure 4-65.

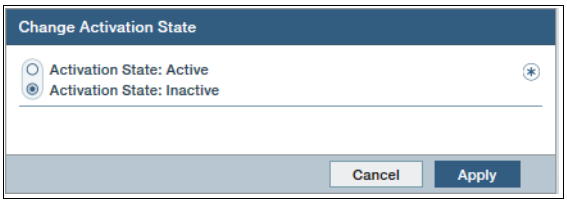


Figure 4-65 Changing the activation state of a CG

In this case, the mirror of the consistency group changes to **Inactive** state, as shown in Figure 4-66. All volumes of this consistency group also have the **Inactive** state.

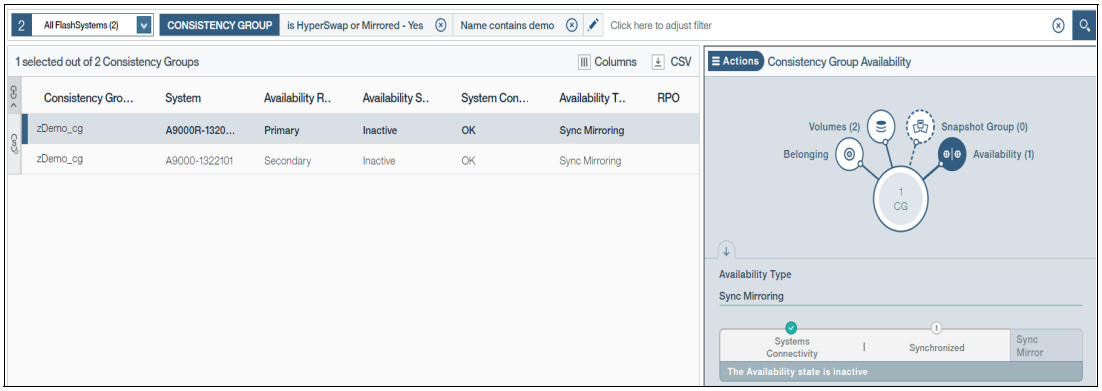


Figure 4-66 Deactivated mirroring of a consistency group

During the inactive state, a consistent set of data is available at the target site. The currency of the consistent data ages in comparison to the source volumes, and the gap increases when mirroring is in standby mode.

In synchronous mirroring, the storage system metadata is used to note which blocks of a source volume are changed but have not yet been replicated to the target volume (because mirroring is not currently active).

When synchronous mirroring is reactivated by a user command or communication is restored, the metadata is used to resynchronize changes from the source volumes to the target volumes. Mirroring records changes for source volumes only. If you want to record changes to both peer volumes when mirroring is in standby mode, change the target volume to a source volume.

In asynchronous mirroring, metadata is not used and the comparison between the most-recent and last-replicated snapshots indicates the data that must be replicated.

4.10.4 Mirror reactivation and resynchronization: Normal direction

In synchronous mirroring, when mirroring has been in standby mode, any changes to volumes with the source role are recorded in metadata. When mirroring is reactivated, changes recorded in metadata for the current source volumes are resynchronized to the current target volumes.

This is the same behavior as the resynchronization after a link failure, as shown in Figure 4-62 on page 120 and Figure 4-63 on page 120. The rate for this resynchronization of changes can be specified by the user in MBps by using the XCLI **`target_config_sync_rates`** command or the **`Max Resync Rate`** command in the Hyper-Scale Manager System Connectivity pane, as shown in Figure 4-67.

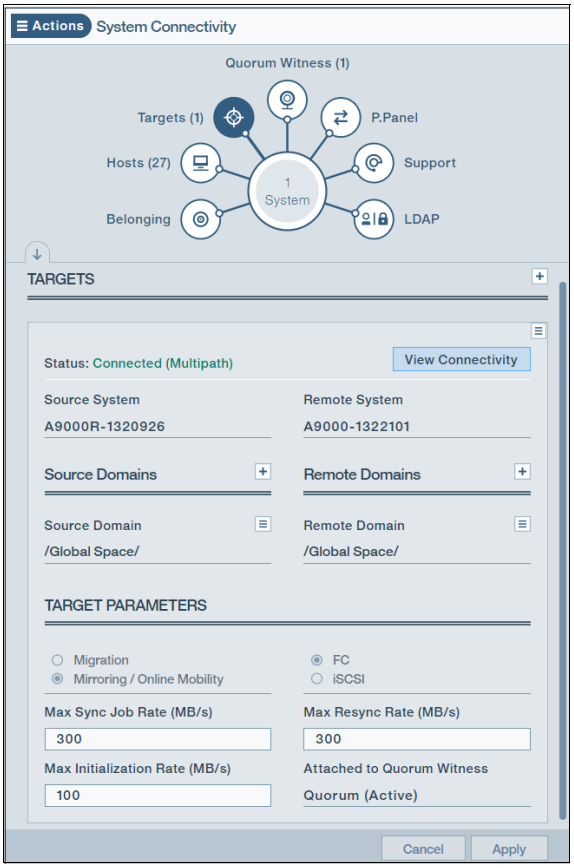


Figure 4-67 Changing the resynchronization rate

When mirroring is reactivated in the normal direction, changes recorded at the primary peers are copied to the secondary peers.

5

HyperSwap

This chapter provides a high-level functional overview of HyperSwap.

Note: For more information about the HyperSwap implementation and usage, see *IBM HyperSwap and Multi-site HA/DR solution for IBM FlashSystem A9000 and A9000R*, REDP-5434.

Some references to HyperSwap are also included in Chapter 4, “Remote mirroring” on page 65.

5.1 HyperSwap feature overview

The HyperSwap feature of IBM FlashSystem A9000 and A9000R, also referred to as *transparent failover*, delivers always-on, HA storage service for storage volumes in a production environment. It is based on an active-active, cross-system, and cross-datacenter configuration, and does not require additional licensing or special hardware.

HyperSwap builds upon the synchronous mirroring functionality that is already included with FlashSystem A9000 and A9000R, together with other advanced replication and stretched-cluster features. HyperSwap volumes can autonomously and transparently switch between *primary* and *secondary* roles, based on the volume failover state. In effect, the pair of mirrored volumes on both mirrored systems constitute a *single HyperSwap volume*, also referred to as *a stretched volume*.

5.1.1 Basic configuration

The basic HyperSwap configuration, shown in Figure 5-1, consists at a minimum of the following components:

- Two storage systems: It can be any combination of FlashSystem A9000 or A9000R. The two systems must be able to interconnect for synchronous mirroring over Fibre Channel.
- Application host: The application host must have read and write access to both storage systems. Host I/Os can be over iSCSI or Fibre Channel.
- Quorum Witness: The Quorum Witness is included with the HyperSwap solution. Its role is to monitor both storage systems health and to arbitrate which storage system owns the primary volume.

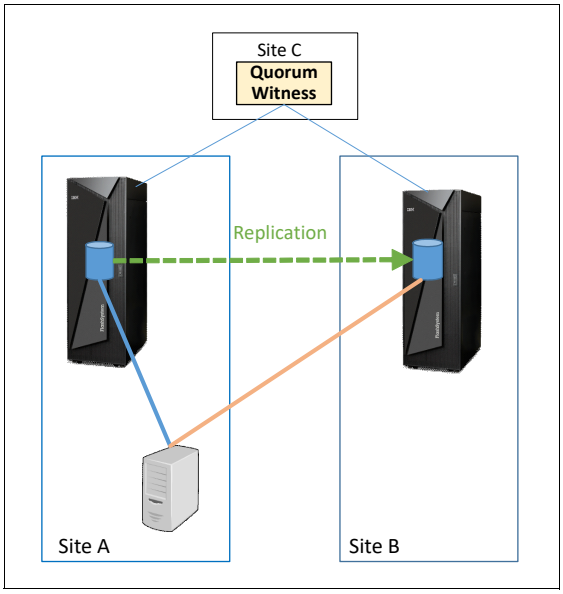


Figure 5-1 HyperSwap volume on peer systems serving host

Note: The basic configuration that is shown in Figure 5-1 represents what is known as a *uniform* configuration where the host can access both the primary and secondary volumes. The uniform configuration is the preferred practice to protect a host from data access problems.

5.1.2 HyperSwap as a critical feature for high availability

The automatic and transparent failover at the volume or Consistency Group level is critical to high availability in partial or complete system failures, and in site disaster scenarios, either in the same data center or between metro-distant data centers serving single or clustered hosts.

HyperSwap protected workloads are not disrupted through most storage, network, server, application, and site failures and disasters. Enterprise IT systems can automatically fail over within seconds, without human intervention and in a straightforward way by using a metro-distance stretch-cluster.

This process protects against loss of access to mission-critical data. Therefore, HyperSwap is a critical feature for high availability, as further described in the following sections:

- Always-on, zero-downtime volume operation
- Simplicity
- Robustness
- Data protection

Always-on, zero-downtime volume operation

The ability to attain always-on flash storage systems is critical to applications (such as time-sensitive financial applications) that require constant operation with availability on a 24 x 7 basis. The active-active pairing per volume or consistency group enables zero downtime operation.

Simplicity

Using active-active systems is a way to greatly simplify failure management. Automation is provided mostly by the solution and does not require complex scripting or procedures. This aspect is especially important for smaller organizations who cannot deal with failover automation complexity.

Robustness

HyperSwap behavior is designed to address the impact of failures and disasters. The HyperSwap function can identify the following failures and recover from them automatically:

- Replication is down
- The Quorum Witness is down
- The Quorum Witness connectivity is down

Data protection

HyperSwap on FlashSystem A9000 and A9000R includes the following functionality:

- Protected hosts and applications continue to benefit from nondisruptive storage service during any of the following failures:
  - Host connectivity to any one of the peer systems is down, for any reason.
  - One of the peer systems does not respond to the host, for any reason.
  - One of the peer systems is completely down, for any reason.
  - A host application or a whole host that is part of a server high-availability cluster fails over to a remote host that is already connected to the peer HyperSwap volume.
- VMware virtual machines can be migrated non-disruptively by using VMware Storage vMotion across vCenter servers and across data centers, supporting VMware vSphere Metro Storage Cluster (vMSC) configurations, and VMware Site Recovery Manager (SRM) 6.1 or later.

5.2 Architecture, design, and components

HyperSwap high availability is based on dual storage systems with active-active pairing per volume, or per consistency group. It is important to note that a HyperSwap relationship is not defined at the storage system level. The HyperSwap function is between peer volumes or peer consistency groups on two separate FlashSystem A9000 or A9000R.

HyperSwap volumes have a copy on one storage system at one site and a copy on the other storage system at another site. Data that is written to the volume is automatically sent to both copies. If one site is no longer available, the other site can provide access to the volume.

Each volume or consistency group pair is using synchronous replication to always keep both systems updated. When certain conditions apply, an autonomous and transparent failover from a volume to its peer is performed so that host applications experience no downtime.

As previously indicated, HyperSwap for FlashSystem A9000 and A9000R builds on the synchronous mirroring functionality. With HyperSwap, volumes can automatically and transparently switch between primary and secondary roles.

As shown in Figure 5-2, each HyperSwap enabled volume exists simultaneously on two FlashSystem A9000 or A9000R peer systems (depending on the specific deployment), in an active-active relationship, synchronously replicated over Fibre Channel (FC).

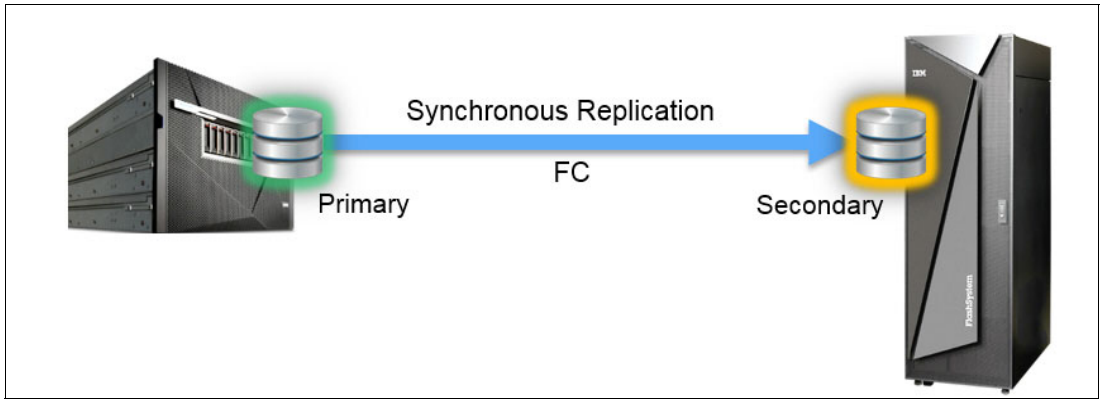


Figure 5-2 HyperSwap volume in synchronous replication over FC

The pair of volumes in a HyperSwap relationship has a unique and identical *SCSI identity* in Network Addressing Authority (NAA) format and the same characteristics relative to I/Os (size, lock state, SCSI reservations). Each storage system with volumes in a HyperSwap configuration has its own volume mapped to the application host, but the application sees them as one LUN.

A HyperSwap stretch volume behaves as a single volume in all SCSI aspects. HyperSwap ensures that the host can use the stretch volume as a single LUN. Storage administrators can non-disruptively and without pausing synchronization, convert synchronously mirrored volumes to HyperSwap volumes, and vice versa. HyperSwap volumes can also be set up using offline initialization.

5.2.1 Host paths

For reliability host operating systems, include a multipath storage driver that allows multiple paths to a storage volume. With recent operating systems, those paths are optimized by using Asymmetric Logical Unit Access (ALUA) support from the multipath driver. ALUA, also known as Target Port Groups Support (TPGS), consists of SCSI concepts and commands that establish path preferences for storage devices.

ALUA allows a storage system to indicate to an operating system the state of the port group. The states include both priority (preferred or non-preferred) and functionality (active or unavailable). When everything is healthy, the port group state conveys only the preference. However, during failure scenarios, it also tells the host which ports cannot be used for I/O.

The HyperSwap function in FlashSystem A9000 and A9000R marks paths to the system that currently owns the primary volume as *active/preferred*. Paths to the system that currently owns the secondary volume are marked as *active/non-preferred*. Therefore, most of the write I/Os go directly to the primary volume because it is the preferred path.

Note: The host experiences a failover as a change in the state of its paths. Therefore, the change is handled by the host multipath driver with no impact to the application (except some delay) and no manual intervention.

Non-preferred paths are used by hosts to balance the load or mitigate disconnects. Occasional write I/Os going over the active, but not preferred path to the secondary volume are redirected to the primary. In this case, the secondary volume acts as a proxy of the primary volume. See Figure 5-3 for the details of the transaction.

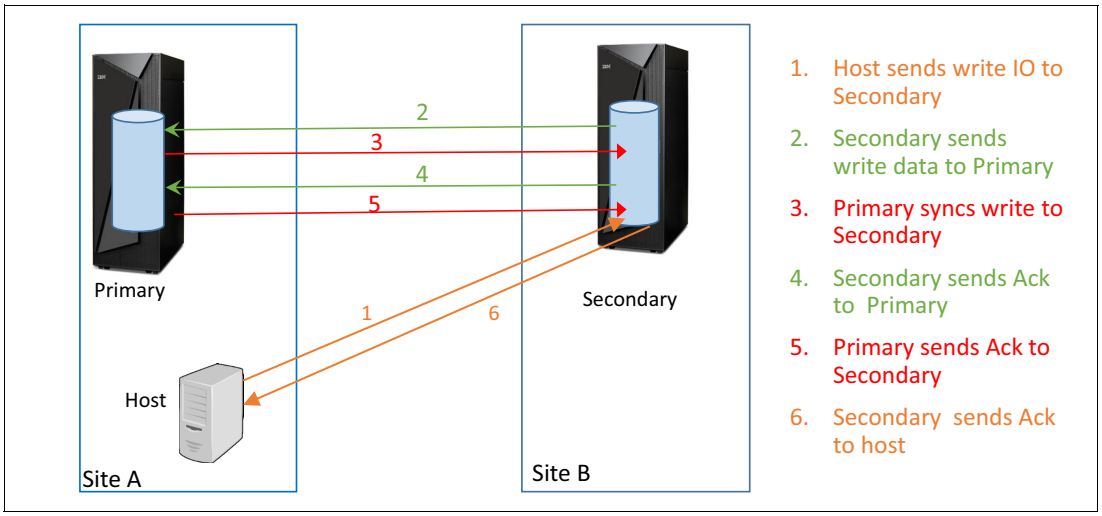


Figure 5-3 Write I/O to secondary

Read I/Os requests on the non-preferred path are normally served directly by the secondary. However, if the relationship was just activated and the secondary is not yet fully synchronized, read requests are also redirected to the primary volume until synchronization is complete.

Important: HyperSwap requires the IBM Storage Host Attachment Kit Version 2.8 or later. Follow this link for the download:

`https://www.ibm.com/support/knowledgecenter/en/SSEPRF/landing/HAK_welcome_page.html`

5.2.2 Failure domains

For the best protection against different types of possible failures, each of the two storage systems and the Quorum Witness must be located in distinct failure domains. The failure domains must be defined by the failures that must be overcome. For example, three physical sites can be considered as three failure domains with regard to failures that affect the physical site but not in case of a major power failure.

Typically, you want to be protected from any type of disaster that might either affect both storage systems at the same time or that would simultaneously disable one of the storage systems and the quorum witness application. However, remember that the physical sites must still be within distances that allow synchronous mirroring between the storage systems, and acceptable latency.

5.2.3 Connection with host stretch-cluster configurations

HyperSwap in stretch-cluster configurations includes the following properties (Figure 5-4):

- Protected hosts are connected to both systems locally and remotely.
- I/O path priorities are assigned for minimum latency, by default. The two systems assign a preferred or non-preferred ALUA state to the port groups, which are translated by the host multipath driver to path priorities, resulting in optimized I/O latency.
- Multiple HyperSwap volumes can exist on each pair of peer systems.

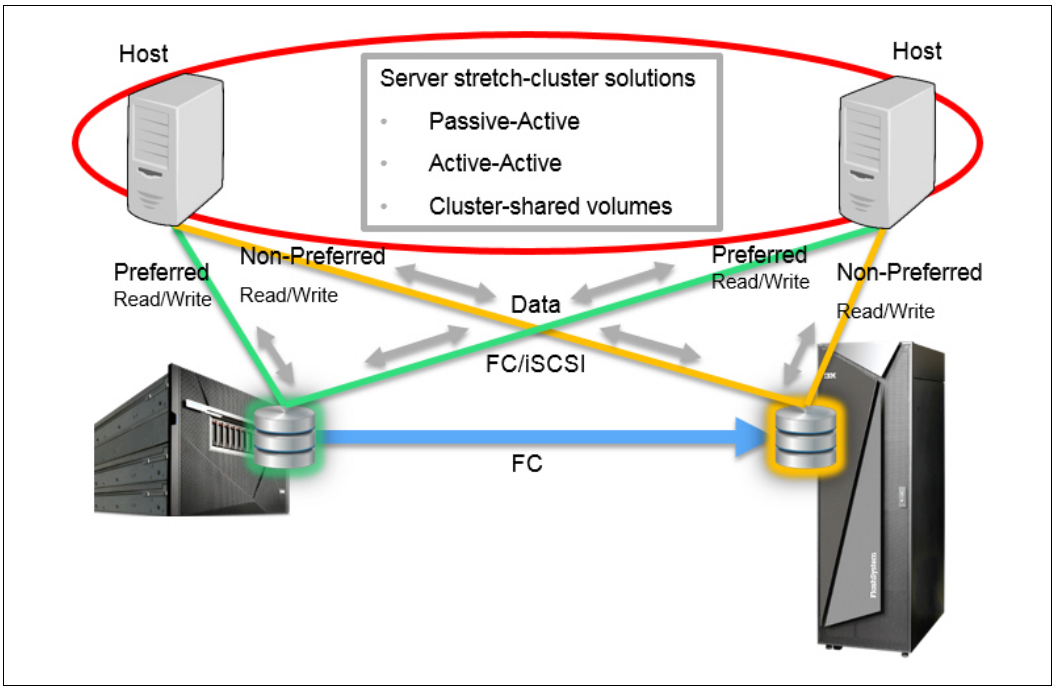


Figure 5-4 Stretch-cluster server configurations

5.3 Independent Quorum Witness

An independent Quorum Witness software component is used as part of the HyperSwap solution to enable transparent failover and facilitate coordination between two storage systems with volumes in a HyperSwap relationship. The Quorum Witness role is to continuously monitor the systems health by using dedicated heartbeat messages. When needed, it serves as a tie-breaker or ruler in possible split-brain scenarios.

Note: The most fundamental function of Quorum Witness is to determine during failure, per HyperSwap volume, which system should own the primary volume and which system should own the secondary volume.

Whenever a failure is detected at the system level, the Quorum Witness is used immediately by the storage systems to resolve any potential contention and to determine which system should own each primary volume or Consistency Group. Therefore, the Quorum Witness component is critical for the complete always-on HyperSwap functionality.

The two systems send keepalive messages to report their health to the Quorum Witness, as illustrated in Figure 5-5. The systems also retrieve the information pertaining to the health of their peer systems from the Quorum Witness. The communication with the Quorum Witness is performed over Ethernet using TCP/IP.

A system can detect the failure of its peer system through the mirroring connectivity between them. If the peer failure is verified through the Quorum Witness information, the system then takes over as owner of primary volumes or Consistency Groups, provided that it has a synchronized copy of the volume or Consistency Group data.

Some rare failure scenarios might result in both systems attempting to take over the primary role. Quorum Witness is used to tie-break these cases and make sure that a single system wins and becomes the primary for the volume.

The automatic recovery ensures that, upon failure, the protected host can access at least one of the volume instances.

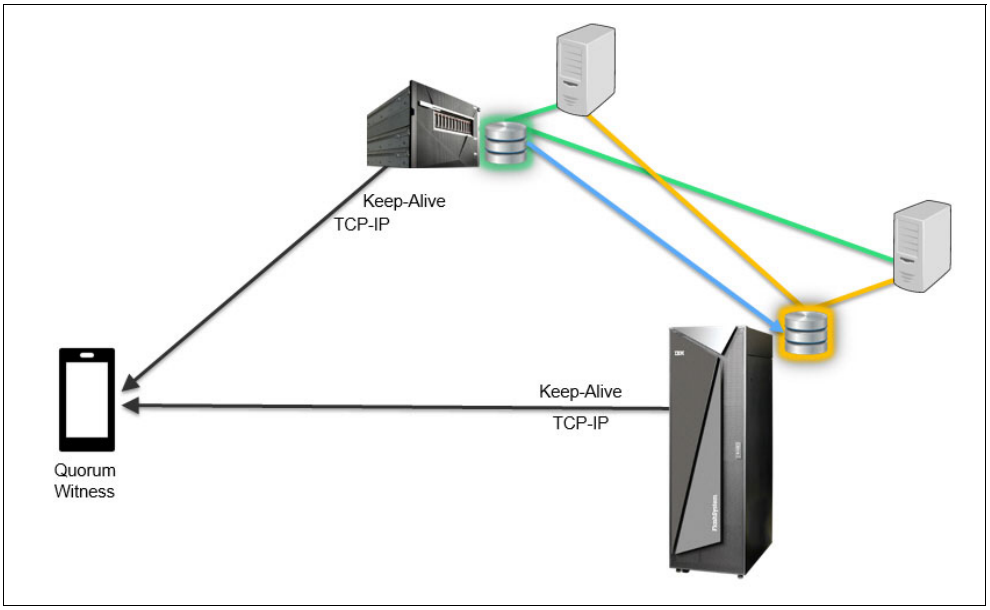


Figure 5-5 Using a keepalive connection with a Quorum Witness node

The Quorum Witness node consists of a small-footprint software application, typically deployed separately at a third site.

Note: The Quorum Witness is preferably deployed as a highly available virtual machine on a VMware vSphere 6.1 (or later) cluster, using VMware HA. For more information, see the following document:

https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.avail.doc/GUID-63F459B7-8884-4818-8872-C9753B2E0215.html

Figure 5-6 illustrates a typical configuration of hosts, storage systems, and a Quorum Witness node in a HyperSwap high availability solution. Typically, the hosts and the storage systems with primary volumes are located at the same site, and the Quorum Witness is deployed at a separate third site.

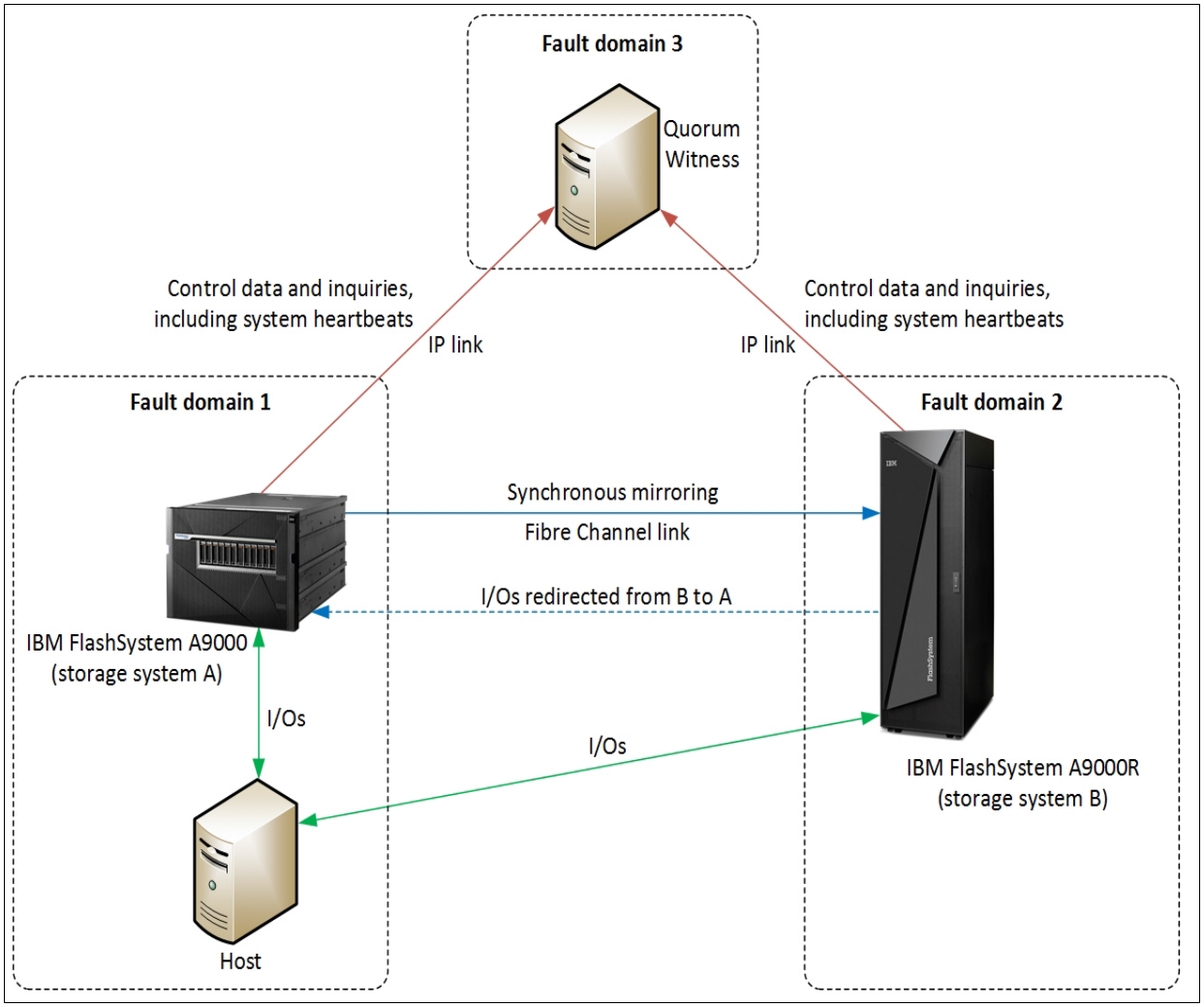


Figure 5-6 FlashSystem A9000 and A9000R with Quorum Witness deployment in separate fault domains

6

Multi-site HA/DR

This chapter provides a high-level functional overview of the Multi-site HA/DR feature, available on FlashSystem A9000 and A9000R systems, starting with software version 12.3.

This chapter covers the following topics:

- IBM Hyper-Scale Manager provides special management for the Multi-site HA/DR solution.
- Architecture, design, and components
- Multi-site HA/DR advantages

Note: For more information about the Multi-site HA/DR implementation and usage, see *IBM HyperSwap and Multi-site HA/DR solution for IBM FlashSystem A9000 and A9000R*, REDP-5434.

6.1 Multi-site HA/DR feature overview

Introduced with the IBM FlashSystem A9000 and A9000R storage system software version 12.3.0, the Multi-site HA/DR feature allows customers to deploy field-proven high availability (HA) and disaster recovery (DR) solutions over multiple sites, keeping three concurrent copies of data.

As shown in Figure 6-1, a Multi-site HA/DR configuration is composed of three IBM FlashSystem A9000 or A9000R systems in a multi-star topology. It comprises:

- One HyperSwap relationship between systems A and B
- One active asynchronous mirroring relationship between systems A and C
- Optionally, one standby asynchronous mirroring relationship between systems B and C

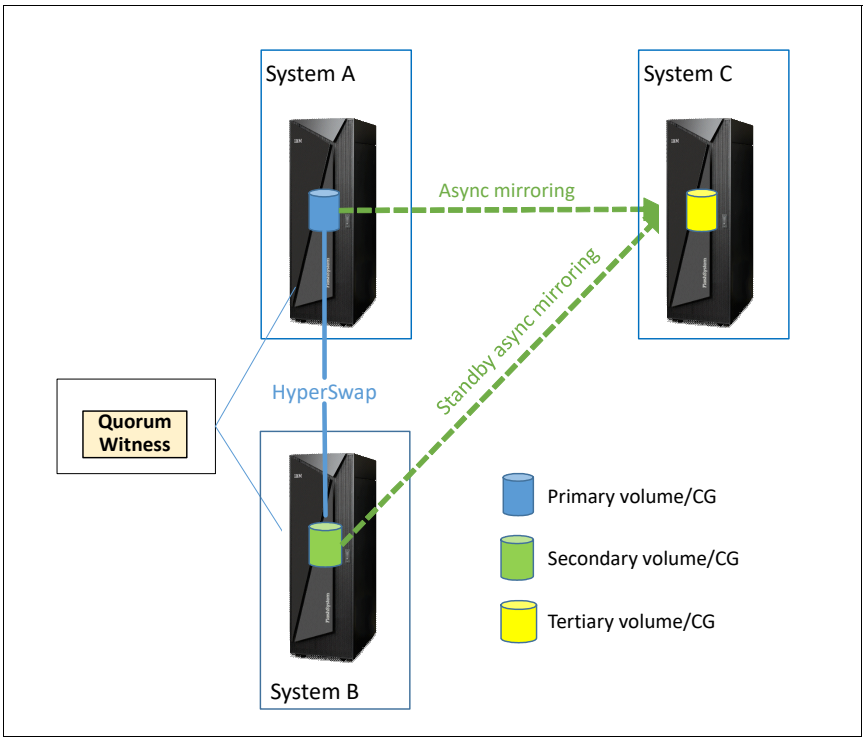


Figure 6-1 Basic Multi-site HA/DR configuration

This configuration provides HyperSwap active-active high availability, while keeping data mirrored to a third copy to ensure two levels of business continuity.

The Multi-site HA/DR feature is able to operate with volumes and consistency groups.

Any storage system in a multi-site relation can have multiple multi-site relations with volumes and consistency groups (CG) in different roles.

6.2 Architecture, design, and components

A multi-site configuration is defined by *extending* a HyperSwap relationship or an asynchronous mirror. In other words, defining the multi-site relationship assumes that at least there already exists a fully initialized two-way HyperSwap or asynchronous mirroring relationship.

The multi-site relationship runs on system A (see Figure 6-1 on page 132) by activating the A-B and A-C relationships. If one of these is already active, no further changes to that existing relation are required.

Important:

- Running the same multi-site configuration on system B or C is not allowed.
- The destination storage pool for the multi-site HA/DR feature must contain enough free space to accommodate the destination volume. Consideration must also be given for any possible increase in snapshot space that might be required on the target systems.

6.2.1 Roles in a multi-site relationship

The Multi-site HA/DR feature introduces some new terms in addition to the familiar HyperSwap and asynchronous mirroring terminology.

As shown in Figure 6-1 on page 132, the volume/CG roles are defined as follows:

Primary volume The primary volume in a HyperSwap relationship with the secondary volume, and in an asynchronous mirroring relationship with the tertiary volume. Normally, the primary volume resides on system A.

Secondary volume The secondary volume in a HyperSwap relationship between A and B. This volume also acts as the primary volume in the optional standby asynchronous mirroring relationship between B and C. Normally, the secondary volume resides on system B.

Tertiary volume The secondary volume in two asynchronous mirroring relationships, between A and C (active) and B and C (standby). Normally, the tertiary volume resides on system C.

In a regular, properly operating multi-site relationship, the role of each volume is as indicated above.

6.2.2 Standby asynchronous mirror

The standby asynchronous mirror between systems B and C can be defined either in advance, at the time of the multi-site relationship assembly, or when needed for data recovery.

Defining the standby mirror in advance requires that the target connectivity between the systems B and C (or at least its definitions) be in place when the multi-site relationship is assembled. When defined, the B-C asynchronous mirror remains on standby under normal conditions and only becomes active, by request, when a disaster occurs on system A, making the primary volume inaccessible and triggering a failover in the A-B HyperSwap relationship.

6.3 Multi-site HA/DR advantages

As implemented in IBM FlashSystem A9000 and A9000R, the Multi-site HA/DR solution offers the following advantages, as discussed hereafter.

6.3.1 Flexibility

Any of the three peer systems participating in a multi-site relationship can be either IBM FlashSystem A9000 and A9000R. System models do not have to be identical. In other words, a multi-site relationship peer system can be model 415 or 425.

The Multi-site HA/DR feature does not require separate licensing.

6.3.2 Non-disruptiveness

The Multi-site HA/DR solution is designed to maintain non-disruptive host data access and recover data in case of a disaster.

The administrator assembles it from existing relationships. Any existing two-way relationship (HyperSwap or asynchronous) can be extended to a multi-site relationship without disrupting the existing relation.

6.3.3 Ease of use

Multi-site HA/DR is easy to configure and monitor, because its administration and management are based on existing features.

IBM Hyper-Scale Manager provides special management for the Multi-site HA/DR solution.

7

Hyper-Scale Mobility

Hyper-Scale Mobility is a powerful function for moving volumes between IBM FlashSystem A9000 and A9000R systems or from an XIV Gen3, in a manner that is transparent to host applications.

New: Starting with System software V12.2.1, Hyper-Scale Mobility also allows you to migrate volumes from XIV Gen3 (with software V11.6.2.a) to FlashSystem A9000 or A9000R.

This chapter includes the following sections:

- Introduction to Hyper-Scale Mobility
- Hyper-Scale Mobility design considerations
- Hyper-Scale Mobility requirements
- Hyper-Scale Mobility process description
- Usage prerequisites and considerations
- Management software support for Hyper-Scale Mobility
- Using Hyper-Scale Mobility

7.1 Introduction to Hyper-Scale Mobility

Hyper-Scale Mobility enables clients to move a volume from one IBM FlashSystem A9000 or A9000R to another (over synchronous distances) or from XIV to FlashSystem A9000 or A9000R in a manner that is transparent to host applications before, during, and after the volume migration.

Note: Hyper-Scale Mobility is a no-charge feature that is included with FlashSystem A9000 Version 12.0.1 and the FlashSystem A9000R Version 12.2 and later.

Hyper-Scale Mobility helps you overcome provisioning scenarios that normally challenge traditional systems. It can accommodate several critical client needs in the modern data center and cloud environment, including online data mobility, load balancing, over-provisioning, and storage system repurposing.

This volume migration capability greatly enhances FlashSystem A9000 and A9000R scalability and directly addresses several client storage-related issues:

- Managing storage growth
- Providing more flexibility in capacity forecasting
- Managing costs
- Scaling between FlashSystem A9000 and A9000R systems
- Balancing workloads across systems without service downtime for better performance
- Retiring systems gracefully and upgrading to the latest technology
- Separating storage and host maintenance cycles
- Migrating volumes from XIV to FlashSystem A9000 or A9000R without any host downtime

Hyper-Scale Mobility capabilities also provide FlashSystem A9000 and A9000R with improved total cost of ownership (TCO) and improved service continuity.

Consider how Hyper-Scale Mobility can address the following client situations:

- Migrating all the data from a FlashSystem A9000 and A9000R that will be decommissioned or redeployed for a new purpose.
- Migrating all the data from XIV that will be decommissioned or redeployed.
- Hyper-Scale Mobility can be used to rebalance the workload, away from a system that is heavily used to a system that is underused. It does not matter if the capacity imbalance is performance-related or data storage-related. Hyper-Scale Mobility can help resolve both situations.

7.2 Hyper-Scale Mobility design considerations

Hyper-Scale Mobility is designed to provide a process to move volumes between one FlashSystem A9000 and A9000R to another FlashSystem A9000 or A9000R as well as moving off XIV Gen3 to FlashSystem A9000 or A9000R with little host effect.

Moving volumes usually requires defining a volume on the destination (or target) FlashSystem A9000 or A9000R, porting data, and disrupting host applications when the new volume is activated. The Hyper-Scale Mobility architecture enables these basic steps to be completed with minimum host involvement and with no disruption to host applications.

The objective is to move the data to a new volume that is on another FlashSystem A9000 or A9000R at the same time, enabling the host to view this new volume as though it is the original. This task is accomplished by redirecting input/output (I/O) activity automatically (by using a proxy method) from the source FlashSystem A9000, A9000R or XIV to the destination system without needing changes to the host configuration.

The new volume must look to the host as though it is the original, which is accomplished by duplicating the volume characteristics of the original volume (for example, the worldwide name of the two volumes is identical).

The final steps of the migration require some host intervention to establish paths directly to the new volume and to remove the paths to the original volume. However, this task does not significantly disrupt host application activity. The host I/Os never need to be interrupted during the whole migration process.

For a detailed, step-by-step illustration of the online migration process, using either the Hyper-Scale Manager or the XCLI, see 7.7, “Using Hyper-Scale Mobility” on page 142.

7.3 Hyper-Scale Mobility requirements

To cause minimal disruption to the host, and to enable uninterrupted I/O operations, these requirements must be met:

- Multi-path driver

  The process of moving a volume concurrently with host access requires that the host operating system uses a multi-path driver to access the volume that is being moved. During the migration, new paths are added, and the old paths to the original volume are eventually removed.

- Switch zoning

  The source and the destination FlashSystem A9000 or A9000R must both be accessible to the host system concurrently. This configuration might require changes to the zoning in use by the host that is involved. The two FlashSystem A9000 and A9000R systems also need zoning between each other to enable connections for the volume data migration.

- SAN boot

  If using SAN boot, make sure that in the adapter BIOS, targets (WWPNs) from both storage systems are defined. The adapter BIOS may be changed during boot time or by using tools from the HBA vendor running on the operating system.

- FlashSystem A9000 and A9000R systems

  There must be two FlashSystem A9000 and A9000R systems: One system is the source, and the other system is the target (destination).

  The new volume is automatically created on the destination system in a specified storage pool, so sufficient space must be available for this action. Consideration must also be given for any possible increase in snapshot space that might be required on the destination system. Hyper-Scale Mobility, in any combination, between FlashSystem A9000 and FlashSystem A9000R requires system software V12.2.0 or later and Hyper-Scale Manager V5.3 or XCLI V5.2 or later.

- XIV as source system

  XIV systems running storage Software V11.6.2.a can be used as the source system to move data to a FlashSystem A9000 or A9000R system on V12.2.1 or later using Hyper-Scale Manager V5.4 or XCLI V5.2.0.a or later.

7.4 Hyper-Scale Mobility process description

From a design standpoint, the Hyper-Scale Mobility process that is used to move a volume between XIV, FlashSystem A9000 and A9000R systems can be summarized in a sequence of stages. The process is characterized by phases and the corresponding states of the migrated volume. The phases and states are depicted in Figure 7-1.

Volume mobility between the source system and the destination system does not interrupt host activity. It is not disrupted by rebuild, redistribution, phase-out, or failover on the destination.

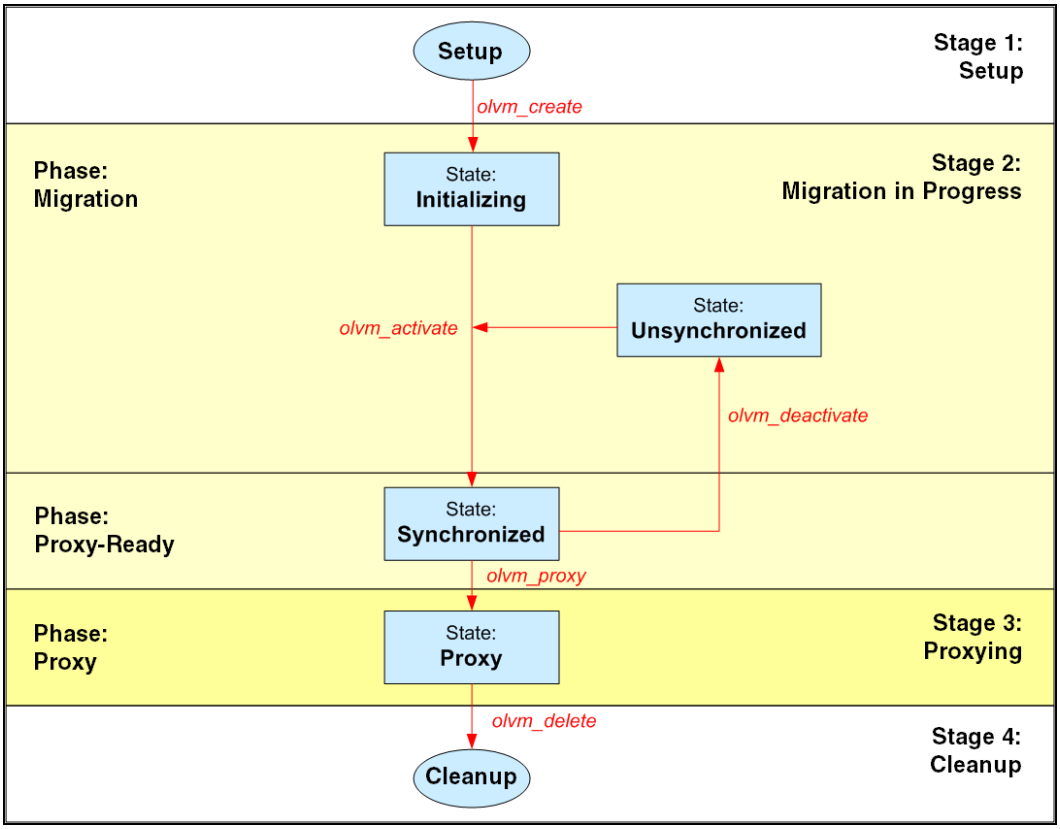


Figure 7-1 Volume migration flow of the IBM Hyper-Scale Mobility

7.4.1 Stage 1: Setup

The first stage of the Hyper-Scale Mobility is to create the volume on the destination FlashSystem A9000 or A9000R. Also, you need to set up the relationship between the two volumes that are needed for migration by running the **`olvm_create`** command or equivalent Hyper-Scale Manager option.

7.4.2 Stage 2: Migration in progress

Data migration can begin by running the **`olvm_activate`** (or **Activate** in the Hyper-Scale Manager) command and must complete successfully before the host can access the new volume. This process is part of the Migration phase. During migration, new data is written by the host to the source and ported (copied) to the destination.

The source volume state goes from initializing to synchronized if the migration is successful (Proxy_Ready phase). The source volume can enter the unsynchronized state if there is a link disruption or deactivation. You can also set it to this state by running the **`olvm_deactivate`** (or **Deactivate** in the Hyper-Scale Manager) command.

7.4.3 Stage 3: Proxying

At this point, the administrator can instruct the source storage system to redirect host I/O to the new volume on the destination storage system by running the **`olvm_proxy`** command. This stage corresponds to the Proxy phase.

In proxy mode, the source (now the proxy) no longer functions as a regular volume, and the source XIV, FlashSystem A9000 or A9000R communicates host requests to the destination. The migration is no longer reversible.

In proxy mode, the host can remain connected to the source without a need to zone and move it to the destination. The host can be moved after the ported volume data is on the destination.

7.4.4 Stage 4: Cleanup

The final stage of the migration involves connecting the host directly to the new volume. This stage might require zoning changes, and the multi-path device driver must discover the new path to the ported volume.

Finally, the original paths can be removed, and the Hyper-Scale Mobility relationship can be deleted by running the **`olvm_delete`** command.

7.5 Usage prerequisites and considerations

In addition to the general requirements for using Hyper-Scale Mobility that are described in 7.3, “Hyper-Scale Mobility requirements” on page 137, there are additional prerequisites and considerations.

7.5.1 Volume and storage pool considerations

There are specific considerations and conditions regarding volume and storage pools selection when you use Hyper-Scale Mobility:

- Volumes that are already part of a mirroring relationship cannot be selected as the source volume with Hyper-Scale Mobility.
- Volumes that are already part of a consistency group cannot be selected as the source volume with Hyper-Scale Mobility.
- Any snapshots that exist on a volume are *deleted* when the Hyper-Scale Mobility process is moved to the Proxy phase.
- The destination storage pool for a Hyper-Scale Mobility relationship must contain enough free space to accommodate the destination volume. Consideration must also be given for any possible increase in snapshot space that might be required on the target system.

7.5.2 Management workstation connectivity

To perform the online migration of an XIV, FlashSystem A9000 or A9000R volume by using the GUI or XCLI, you must verify that both the source and destination systems are configured and accessible by the GUI or XCLI.

7.5.3 Connectivity between the source and destination systems

To effectively use Hyper-Scale Mobility, there must be adequate connectivity between the source and destination systems. The Hyper-Scale Mobility process uses the same mechanism as remote mirroring to synchronize source and destination volumes. Fundamentally, Hyper-Scale Mobility acts similarly to synchronous remote mirroring during the migration and proxy-ready phases.

When planning Hyper-Scale Mobility activities, follow the same guidelines and leading practices regarding connectivity between source and destination systems as those that you follow with synchronous remote mirroring. For more information, see Chapter 3, “Remote connectivity” on page 37. The same information applies if the source system is an XIV.

Beginning with FlashSystem A9000 and A9000R Version 12.2.1 Hyper-Scale Mobility is also possible with an XIV Gen3 at Version 11.6.2.a as the source. With FlashSystem A9000 and A9000R Version 12.2, Hyper-Scale Mobility is available between any combination of FlashSystem A9000 and A9000R systems. Prior to Version 12.2, support is available on FlashSystem A9000 only. The systems must be connected over Fibre Channel (FC) and be at a short distance from each other. This requirement is similar to Synchronous Remote Mirroring. Internet Small Computer System Interface (iSCSI) is not currently supported.

7.5.4 Host system connectivity

Before you use Hyper-Scale Mobility, you must confirm that any host that has mappings to the source volume on the source XIV, FlashSystem A9000 or A9000R has the appropriate access to the destination system:

- If you are migrating an iSCSI logical unit number (LUN), ensure that the host can access the destination system over the Internet Protocol (IP) network.
- If you are migrating an FC LUN, ensure that the host is correctly zoned to the destination system.

7.6 Management software support for Hyper-Scale Mobility

Hyper-Scale Manager v5.3 and XCLI enable support for the Hyper-Scale Mobility feature for the FlashSystem A9000 and A9000R. Either tool can be used to perform the tasks that are related to Hyper-Scale Mobility. Hyper-Scale Manager v5.3 is used for the examples and illustrations in this publication. To migrate a source volume from XIV to FlashSystem A9000 or A9000R, Hyper-Scale Manager v5.4 or later is required. An example of migration between XIV and FlashSystem A9000 is shown in 7.7.3, “Migrating volumes from XIV to FlashSystem A9000 or A9000R using Hyper-Scale Manager” on page 164.

7.6.1 Hyper-Scale Manager features

The Hyper-Scale Manager options for Hyper-Scale Mobility are found under the Remote View side menu, as shown in Figure 7-2 on page 141.

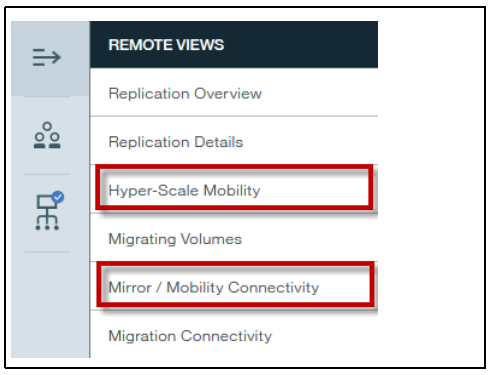


Figure 7-2 Volume Mobility menu options

Several filters are included in the default filters available when selecting **Volumes** from the left navigation pane, as shown in Figure 7-3.

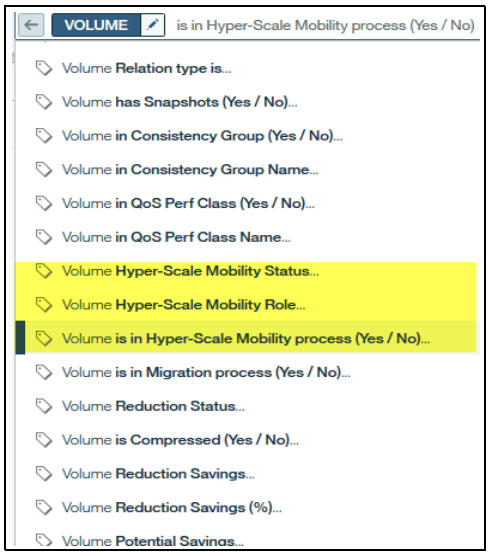


Figure 7-3 Mobility filters in the Volumes menu

7.6.2 XCLI functions that support Hyper-Scale Mobility

The XCLI includes a series of commands to support Hyper-Scale Mobility:

`olvm_list`	Displays details for Hyper-Scale Mobility relationships on a local system.
`olvm_create`	Defines an Hyper-Scale Mobility configuration.
`olvm_activate`	Activates (starts) an Hyper-Scale Mobility migration for a defined mobility relationship.
`olvm_proxy`	Moves the Hyper-Scale Mobility source volume to a proxy state.
`olvm_deactivate`	Deactivates the Hyper-Scale Mobility migration for a defined relationship.
`olvm_abort`	Aborts a defined or activated Hyper-Scale Mobility process.
`olvm_delete`	Deletes an Hyper-Scale Mobility relationship and attributes.

7.7 Using Hyper-Scale Mobility

The following examples depict an online volume migration of a volume by using Hyper-Scale Manager and the XCLI. In these examples, the volume that is being migrated is mapped over Fibre Channel to a Red Hat Enterprise Linux (RHEL) host, and the host is actively generating I/Os to the volume throughout the migration.

In this example, the source and destination FlashSystem A9000 systems are connected through Fibre Channel according to the connectivity described and outlined in Chapter 3, “Remote connectivity” on page 37.

A later example will be shown using XIV as source and a FlashSystem A9000 system as destination along with a Windows host with Fibre Channel connections with active I/Os will be used.

Note: The process is the same for any combination of FlashSystem A9000 and A9000R.

7.7.1 Using Hyper-Scale Mobility with Hyper-Scale Manager GUI

This section illustrates how to prepare and use Hyper-Scale Mobility from the Hyper-Scale Manager UI. We have decomposed the process into a series of six tasks.

Task 1: Planning and preparation

To complete planning and preparation, follow these steps:

1. Confirm that both the source and destination are configured and accessible in the Hyper-Scale Manager and that there is FC connectivity between these systems. Figure 7-4 shows the source (A9000) and destination (A9000R) systems with confirmed connectivity between them.

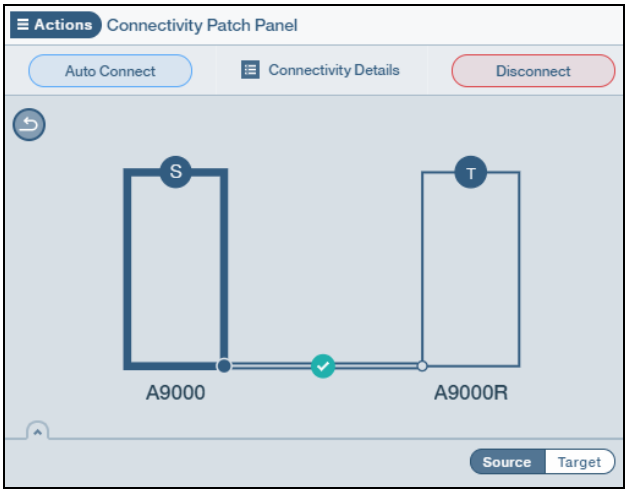


Figure 7-4 Connectivity between two A9000 systems

2. Validate the host multipath connectivity to the source volume by running the **xiv_devlist** command of the Host Attachment Kit (HAK), as shown in Example 7-1.

Example 7-1 Check multipath connectivity

```
[root@mcnode81 ~]# xiv_devlist
IBM Devices
------------------------------------------------------------------------------
                                                                 Storage Storage
Device               Size (GB)  Paths  Vol Name          Vol ID  ID      Host
------------------------------------------------------------------------------
/dev/mapper/mpathaqd 1033.6     8/8    HS_Mob_6003310_01 13443   6003310 mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaqe 1033.6     8/8    HS_Mob_6003310_02 13444   6003310 mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaqf 1033.6     8/8    HS_Mob_6003310_03 13445   6003310 mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaqg 1033.6     8/8    HS_Mob_6003310_04 13446   6003310 mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaqi 1033.6     8/8    HS_Mob_6003310_05 13447   6003310 mcnode81
```

Note the Vol ID of 13444 and ID of 6003310 of volume HS_Mob_6003310_02, indicating that the volume is presented to the host from the FlashSystem A9000.

As part of the preparation, it is also possible to define the host on the target system. This action can also be completed when the migration is taking place. In this example, the host definition and port definitions are created for the host on the destination system.

3. From the Hyper-Scale Manager Dashboard, mouse over the **New** icon, click **New Item**, and select **Host** from the menu, as shown in Figure 7-5. This illustration applies to a FC-connected host. For an iSCSI-connected host, see the procedure that is explained in *IBM FlashSystem A9000, IBM FlashSystem A9000R, and IBM XIV Storage System: Host Attachment and Interoperability*, SG24-8368.

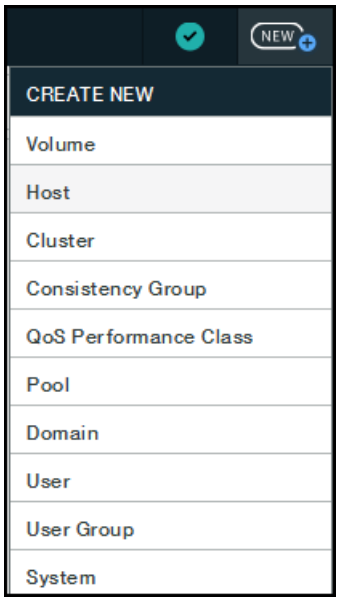


Figure 7-5 Defining a new host

4. In the Add Host window, enter the details for the host, as shown in Figure 7-6. Ensure that the details match the corresponding host details from the source FlashSystem A9000. In this example, the Name of the host is `mcnode81`, the Type is **Default**, and the Cluster value is empty. The System value is chosen from the drop-down menu and set to the destination FlashSystem A9000 (**A9000 6003308 Jazz** (IBM Jazz™) in this example).

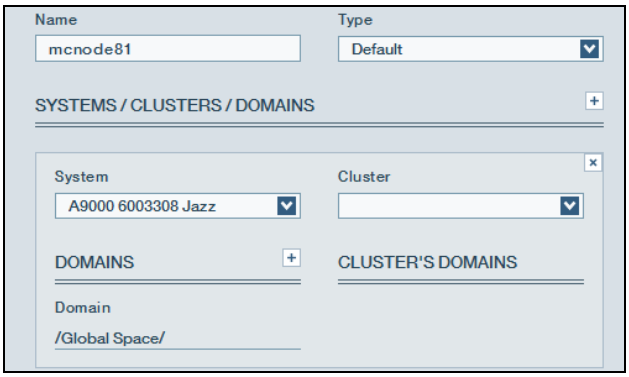


Figure 7-6 Host details

5. Add the ports for the host. Click the plus icon (**+**) and complete the port information, as shown in Figure 7-7. For this example, two ports are added using the WWPN addresses zoned to this host. When completed, click **Create**.

   Ensure that the details match the corresponding port details from the source system. In this example, choose **FC** for the **Port Type**. The Port Addresses are **10000090FA731D36** and **10000090FA731D37**.

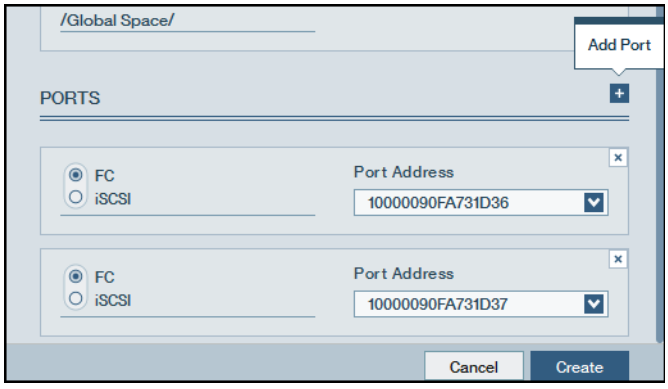


Figure 7-7 Add host ports on the destination system

6. The new host and port definitions are now visible in the Hosts tab of the Hyper-Scale Manager display, as shown in Figure 7-8.

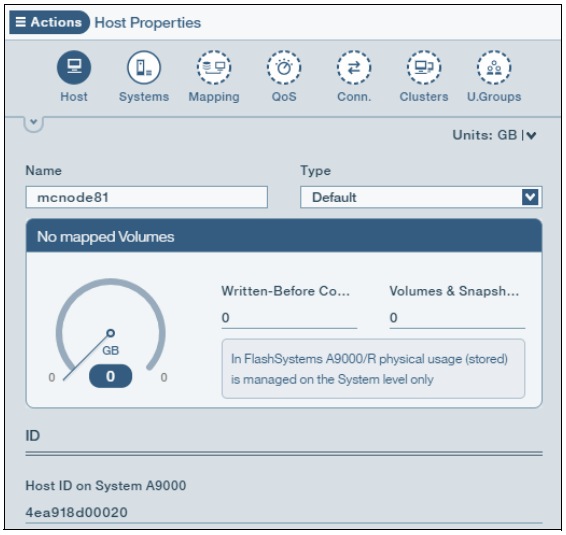


Figure 7-8 Host properties

Task 2: Setup

For setup, complete the following steps:

1. To create the Hyper-Scale Mobility relationship, select the source volumes in the Volumes view and select **Hyper-Scale Mobility** → **Move Volume to other System**, as shown in Figure 7-9.

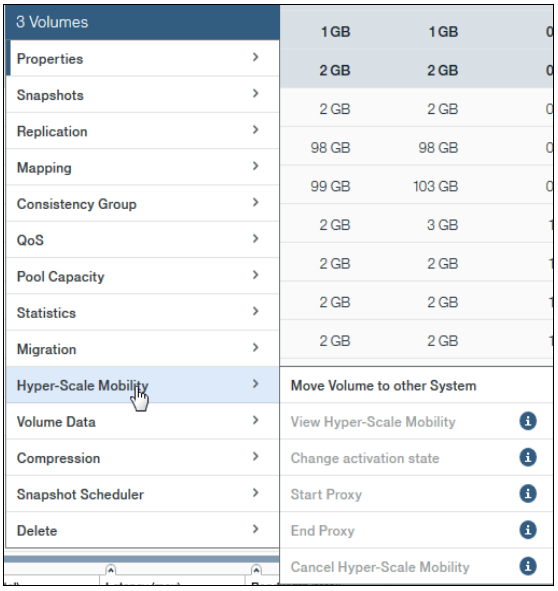


Figure 7-9 Online volume mobility menu

2. After selecting the mobility option, enter the information for the Destination System and pool, as shown in Figure 7-10. In this example, multiple volumes have been selected so the system will automatically name the volumes as they are created on the destination system.

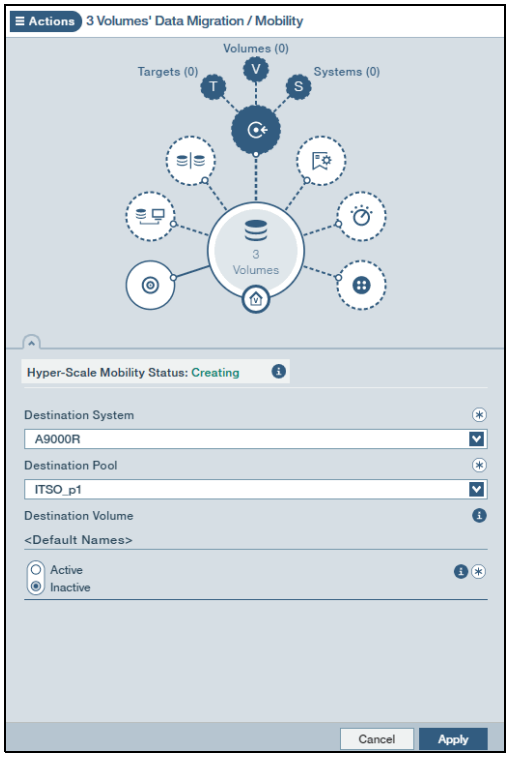


Figure 7-10 Creating an Online Volume Migration

Note: Destination volumes are created automatically on the destination system with the same name as the source volumes.

3. To immediately activate the Hyper-Scale Mobility relationship upon creation, select **Active**. In this example, **Inactive** is selected because the next step explicitly activates the relationship.

   Click **Create** to create the relationship.

Consideration: A volume that is part of an availability relationship cannot be used as the source volume for Hyper-Scale Mobility without first removing that relationship.

4. By opening a new tab and selecting **Hyper-Scale Mobility**, as shown in Figure 7-11, the source and destination volumes can be seen for the newly created migration relationship, as shown in Figure 7-12.

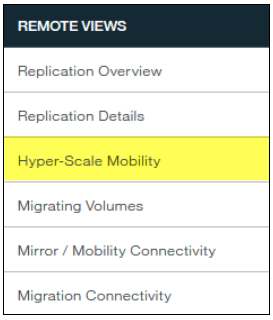
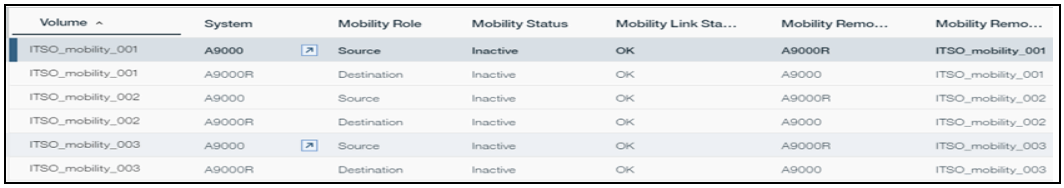


Figure 7-11 Remote Views: Hyper-Scale Mobility

Notice that the Mobility Status for the volumes is showing as **Inactive**. Notice the volumes in this view are shown for both the source and destination systems (A9000 and A9000R).



Volume	System	Mobility Role	Mobility Status	Mobility Link Sta...	Mobility Remo...	Mobility Remo...
ITSO_mobility_001	A9000	Source	Inactive	OK	A9000R	ITSO_mobility_001
ITSO_mobility_001	A9000R	Destination	Inactive	OK	A9000	ITSO_mobility_001
ITSO_mobility_002	A9000	Source	Inactive	OK	A9000R	ITSO_mobility_002
ITSO_mobility_002	A9000R	Destination	Inactive	OK	A9000	ITSO_mobility_002
ITSO_mobility_003	A9000	Source	Inactive	OK	A9000R	ITSO_mobility_003
ITSO_mobility_003	A9000R	Destination	Inactive	OK	A9000	ITSO_mobility_003

Figure 7-12 Source and Destination volumes

Also note that the size of the destination volume will match the size of the source volume, but the **Written (Used capacity)** of the volume will be 0 GB while in this inactive state. This configuration is expected because the Hyper-Scale Mobility relationship has not yet been activated, and the synchronization of the destination volume has not yet begun. When the Hyper-Scale Mobility relationship is in an inactive state, Host I/O continues to only go to the original (source) volume, as described in the information window shown in Figure 7-13.

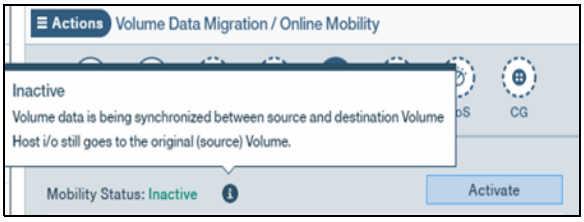


Figure 7-13 Hyper-Scale Mobility: Inactive description

Note: Although the destination volume has been created, it cannot yet be mapped to the host. The destination volume in a Hyper-Scale Mobility relationship cannot be mapped to a host until the Proxy phase. In addition, its Locked Status is `Read Only`. These are the available actions that you can perform on the volume:

- Move to Pool
- Create Snapshot
- Create Snapshot (Advanced)
- Copy this Volume
- Show Statistics
- Properties

Task 3: Migration

To complete the Migration task, perform the following steps:

1. Select the Volumes in the destination system, right-click and select **Online Volume Mobility** → **Change activation state**, as shown in Figure 7-14.

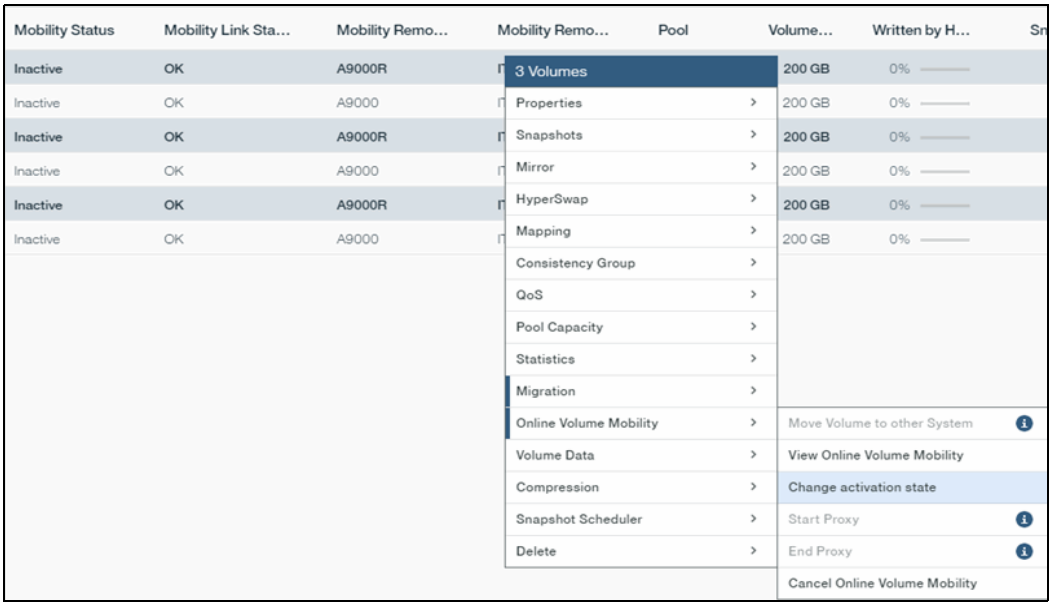


Figure 7-14 Change activation state

2. This provides the option to select **Active**. Click **Apply** to finish the steps. This action activates the relationship and queues the process to synchronize the destination volume on the destination FlashSystem A9000.

Remember: Only one Hyper-Scale Mobility process at a time is synchronized from the source system.

Where there is more than one Hyper-Scale Mobility pair, the synchronization is done serially. The progress of the synchronization can be viewed in the Volumes tab, as shown in Figure 7-15. The status is `Initializing` and the progress is shown as a percentage. Note that the progress is only shown for the Source volume.

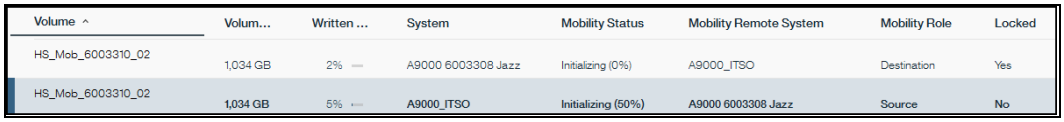


Figure 7-15 Hyper-Scale Mobility status view from the Volumes tab

3. After the synchronization is complete, Mobility Status changes to `Synchronized` for both volumes. Note that both volumes now report the same Written percentage (Used Capacity). Volume data is mirrored and is consistent on both the source and destination volumes. Host I/O is still being sent only to the original (source) volume in this state, as shown in the information window in Figure 7-16.

Figure 7-16 Proxy Ready and Synchronized at the source

Now, the destination FlashSystem A9000R (in this example) contains a consistent copy of the source volume, in addition to the necessary host and port definitions. The next task is to enter the actual migration stage.

Task 4: Proxying

Proxying means that the source FlashSystem A9000 or A9000R starts redirecting host I/O to the volume on the destination system. To start the proxy mode, complete the following steps:

1. In the Hub view to the right of the Volumes tab, select **Start Proxy**, as shown in Figure 7-17.

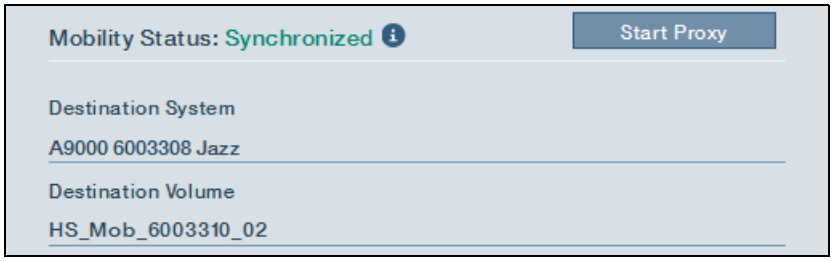


Figure 7-17 Start Proxy for IBM Hyper-Scale Mobility

2. To start multiple volumes at the same time, select the volumes on one system (ctrl+click), right-click to get the Actions menu, then select **Online Volume Mobility** → **Start Proxy**. This is shown in Figure 7-18.

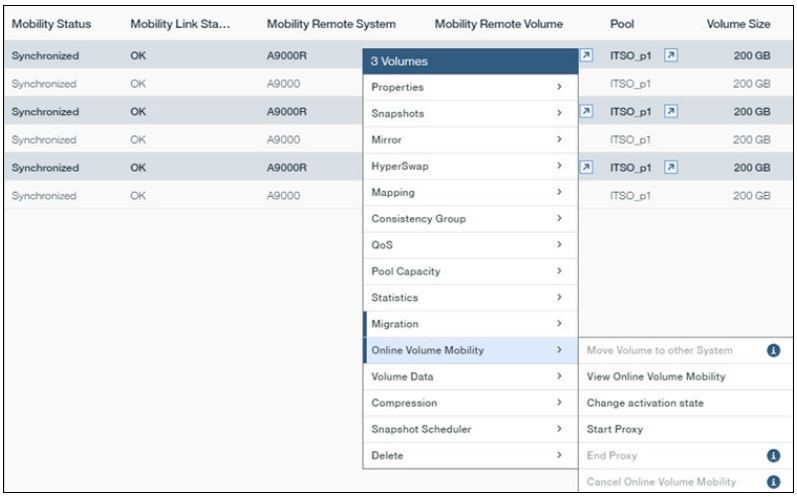


Figure 7-18 Start proxy for multiple volumes

3. As shown in Figure 7-19, a warning message is displayed, indicating that any source volume snapshots that exist are deleted if the proxy is started. It also describes what will be happening during the Proxy phase.

   Click **Apply** to initiate the Proxy phase.

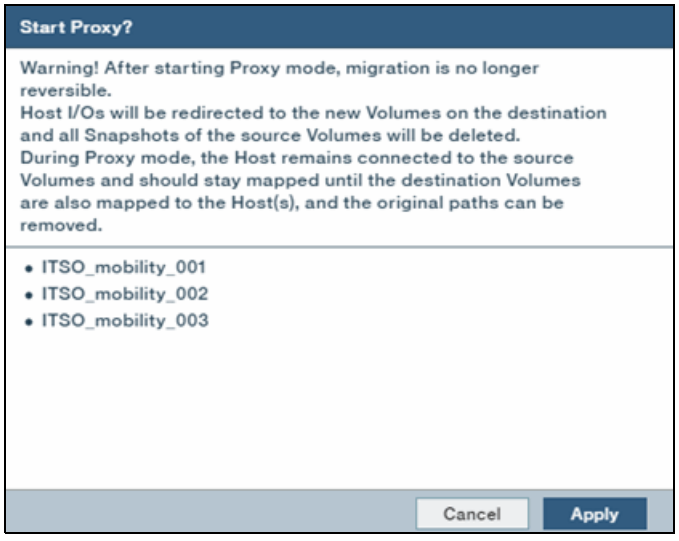


Figure 7-19 Warning on proxy start

Important: Upon initiating the Proxy phase for a volume, it is no longer possible to stop the migration of this volume. Up to this point, the source volume still exists on the source FlashSystem A9000 or A9000R, and any host I/O is still synchronized between both the source and destination volumes.

Clicking **Apply** in this window triggers the source system to proxy all subsequent host I/O to the volume on the destination system only. The source volume becomes inconsistent and unavailable. The source volume is now just a logical placeholder for the original volume. Its size is 0 GB, and its hard (total usable) capacity is returned to the storage pool.

4. The volumes view now changes to show the Hyper-Scale Mobility relationship in the Proxy state, as shown in Figure 7-20.

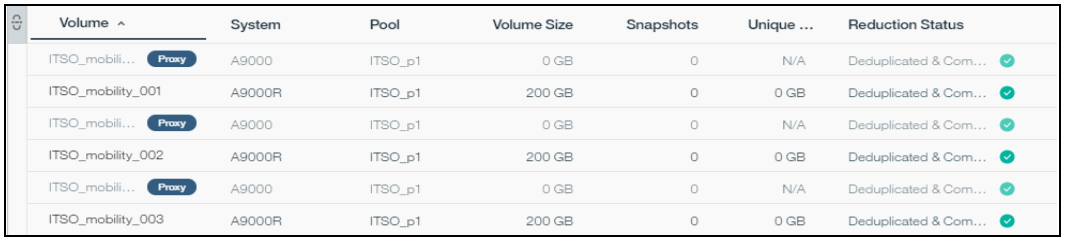


Figure 7-20 Proxy state viewed from the Volumes view

5. Now that the Proxy phase is successfully initiated, the newly created destination volume is ready to map to the host on the destination system. Select the destination volumes in the Volumes tab and choose the Mapping element in the Hub display on the right, as shown in Figure 7-21.

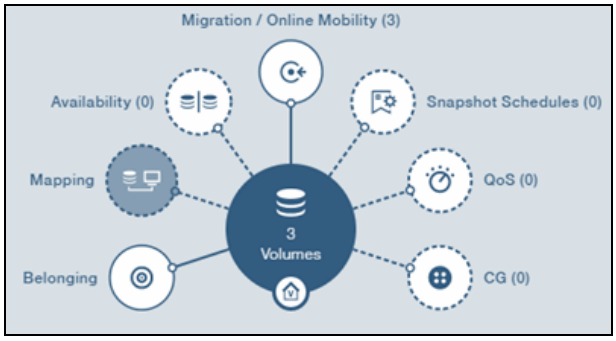


Figure 7-21 Selecting the Mapping element in the Hub

6. Click the Plus sign (**+**) beneath the Hub to add a mapping, as shown in Figure 7-22. You can either map a single host or a cluster.

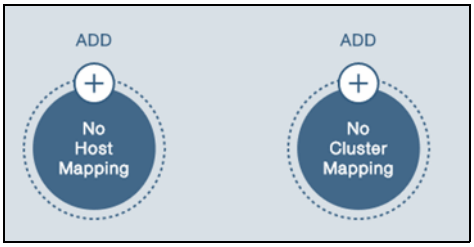


Figure 7-22 Add host mapping to the destination volume

7. In the window that opens, select the new host from the menu and the LUN ID to map it to. Click **Apply** to map the volume, as shown in Figure 7-23.

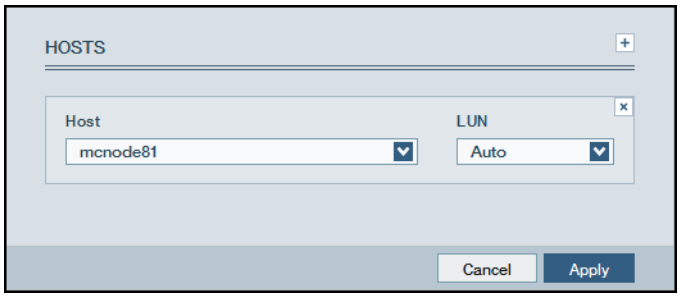


Figure 7-23 Select the host to map

8. After the destination volume is mapped to the host, a rescan of the devices from the host is needed to pick up the new paths to the volume on the destination system. Run the **xiv_fc_admin -R** command, and then run the **xiv_devlist** command from the host, as shown in Example 7-2.

   Note the 14 paths (six additional) for the destination volume, HS_Mob_6003310_02, in the bold row.

Example 7-2 Host rescan

```
[root@mcnode81 ~]# xiv_fc_admin -R
[root@mcnode81 ~]# xiv_devlist
IBM Devices
------------------------------------------------------------------------------
                                                                 System  System
Device               Size (GB)  Paths  Vol Name           Vol ID  ID      Host
------------------------------------------------------------------------------
/dev/mapper/mpathaqf  1033.6     8/8    HS_Mob_6003310_03  13445   6003310  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaql  1033.6     8/8    HS_Mob_6003310_01  13452   6003310  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaqo  1033.6     14/14  HS_Mob_6003310_02  13453   6003310  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaxu  2067.3     6/6    HS_Mob_6003308_01  15857   6003308  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaxv  2067.3     6/6    HS_Mob_6003308_03  15859   6003308  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathayb  2067.3     6/6    HS_Mob_6003308_02  15858   6003308  mcnode81
------------------------------------------------------------------------------
```

Note: The **xiv_fc_admin** and **xiv_devlist** commands are available on the host after installing the HAK.

Task 5: Cleanup

After the host has connectivity to the volume through the new paths to the destination FlashSystem A9000 or A9000R, unmap the volume from the host on the source system. Then remove the paths to the source volume from the host.

To accomplish this task, complete the following steps:

1. Select the source volumes (which are in a `Proxy` state) in the Volumes view of the Hyper-Scale Manager. Right-click and select **Mapping** → **Unmap All**, as shown in Figure 7-24. Click **Apply** to unmap the volumes.

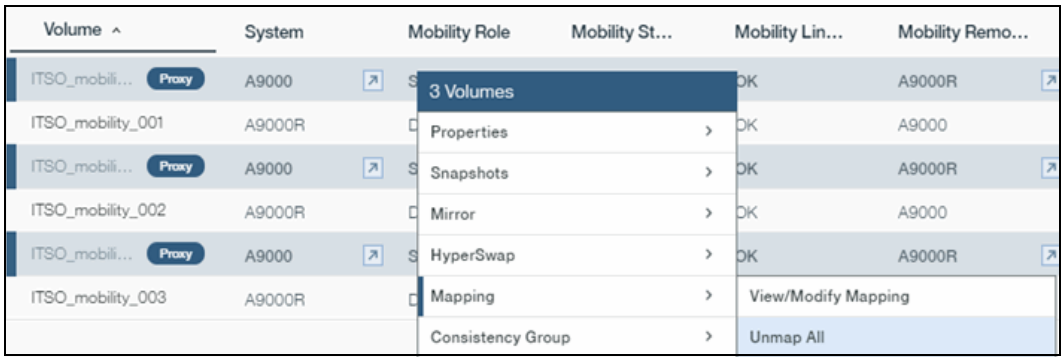


Figure 7-24 Mapping selection for the source volume

2. A confirmation window opens and prompts you to confirm that you want to unmap the selected volume, as shown in Figure 7-25. Click **Apply** to unmap the source volume from the host.

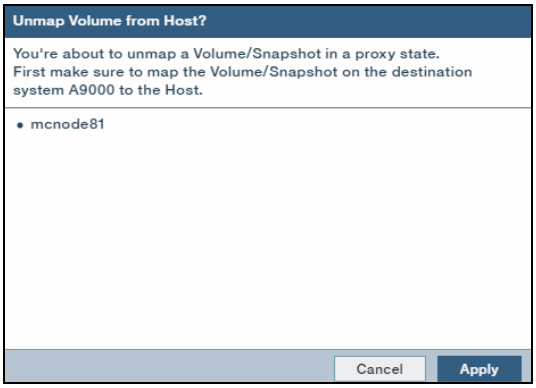


Figure 7-25 Confirm the unmapping of the source volume from the host

3. After the volume is unmapped from the host, only six enabled paths to the volume remain to the host. Run the **`xiv_fc_admin -R`** command, and then run the **`xiv_devlist`** command from the host to remove the unused paths, as shown in Example 7-3.

Example 7-3 Only six paths enabled

```
[root@mcnode81 ~]# xiv_fc_admin -R
[root@mcnode81 ~]# xiv_devlist
XIV Devices
------------------------------------------------------------------------------
                                                          System   System
Device               Size (GB)  Paths  Vol Name          Vol ID  ID       XIV Host
------------------------------------------------------------------------------
/dev/mapper/mpathaqf  1033.6     8/8    HS_Mob_6003310_03  13445   6003310  mcnode81
```

```
-------------------------------------------------------------------------------
/dev/mapper/mpathaql  1033.6     8/8    HS_Mob_6003310_01  13452   6003310  mcnode81
-------------------------------------------------------------------------------
/dev/mapper/mpathaqo  1033.6     6/14   HS_Mob_6003310_02  13453   6003308  mcnode81
-------------------------------------------------------------------------------
/dev/mapper/mpathaxu  2067.3     6/6    HS_Mob_6003308_01  15857   6003308  mcnode81
-------------------------------------------------------------------------------
/dev/mapper/mpathaxv  2067.3     6/6    HS_Mob_6003308_03  15859   6003308  mcnode81
-------------------------------------------------------------------------------
/dev/mapper/mpathayb  2067.3     6/6    HS_Mob_6003308_02  15858   6003308  mcnode81
-------------------------------------------------------------------------------
```

Note the unmatching paths for the destination volume, `HS_Mob_6003310_02`, in the bold row. Also, note that the Vol ID is still `13453` and the System ID has changed to `6003308`. These IDs indicate that the host is connected *only* to the destination volume on the destination FlashSystem A9000 or A9000R. The destination FlashSystem A9000 or A9000R keeps the same Vol ID, if possible.

4. Run the **`xiv_fc_admin -R --clean`** command, and then run the **`xiv_devlist`** command from the host to remove the failed paths from the RHEL host, as shown in Example 7-4.

Example 7-4 Path removal and rescan for RHEL

```
[root@mcnode81 ~]# xiv_fc_admin -R --clean
[root@mcnode81 ~]# xiv_devlist
XIV Devices
-------------------------------------------------------------------------------
                                                                 System   System
Device                Size (GB)  Paths  Vol Name           Vol ID  ID       XIV Host
-------------------------------------------------------------------------------
/dev/mapper/mpathaqf  1033.6     8/8    HS_Mob_6003310_03  13445   6003310  mcnode81
-------------------------------------------------------------------------------
/dev/mapper/mpathaql  1033.6     8/8    HS_Mob_6003310_01  13452   6003310  mcnode81
-------------------------------------------------------------------------------
/dev/mapper/mpathaqo  1033.6     6/6    HS_Mob_6003310_02  13453   6003308  mcnode81
-------------------------------------------------------------------------------
/dev/mapper/mpathaxu  2067.3     6/6    HS_Mob_6003308_01  15857   6003308  mcnode81
-------------------------------------------------------------------------------
/dev/mapper/mpathaxv  2067.3     6/6    HS_Mob_6003308_03  15859   6003308  mcnode81
-------------------------------------------------------------------------------
/dev/mapper/mpathayb  2067.3     6/6    HS_Mob_6003308_02  15858   6003308  mcnode81
-------------------------------------------------------------------------------
```

5. To remove the failed paths in IBM AIX®, use the sample script shown in Example 7-5.

Example 7-5 Path removal in AIX

```
for disk in `lsdev -Cc disk | grep 2810 | awk '{ print $1 }'`
do
        for path in `lspath -l $disk -F "status connection" | grep Failed | awk '{ print
$2 }'`
        do
                echo $disk
                rmpath -l $disk -w $path -d
        done
done
```

Task 6: Post-cleanup

The previous example successfully used Hyper-Scale Mobility through the Hyper-Scale Manager to move the volume on the source FlashSystem A9000 to the destination FlashSystem A9000 without incurring any downtime on the host. The final step is to end the proxy and delete the relationship. Although this example is illustrated using the Hub to select items, you can also do this with the Actions menu.

To accomplish this task, complete the following steps:

1. From the Volumes tab in the Hyper-Scale Manager, select the source volume and choose the Migration / Online Mobility element in the Hub view to the right, as shown in Figure 7-26.

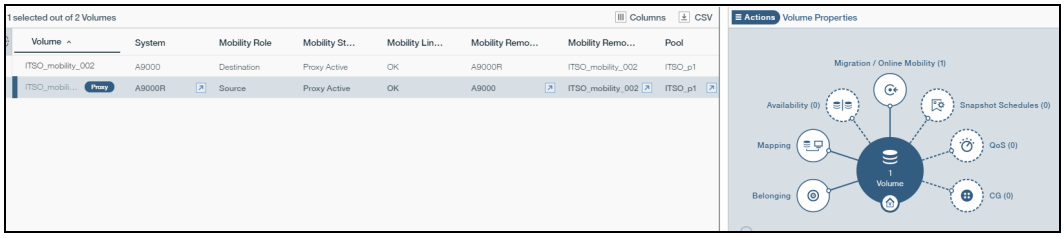


Figure 7-26 Migration/Mobility element for the source volume

2. Select **End Proxy**, as shown in Figure 7-27.

Figure 7-27 End the Hyper-Scale Mobility proxy

3. A confirmation window opens, as shown in Figure 7-28, to ensure that you mapped the host to the destination volume and confirmed access to it. This configuration was confirmed in the Cleanup stage.

   Click **Apply** to end the proxy.

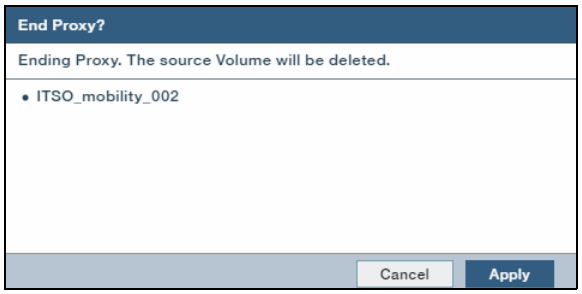
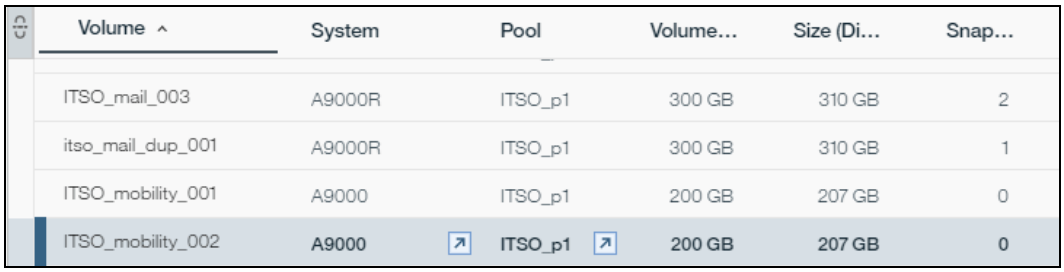


Figure 7-28 Confirm the ending of the IBM Hyper-Scale Mobility proxy

4. The proxy has been removed and the expected end state of the volume on the source FlashSystem A9000 is shown in Figure 7-29.

   On the source system, the volume no longer exists. On the destination FlashSystem A9000, there is a new volume named `ITSO_mobility_02`. This volume has the matching size and Written percentage (Used capacity) as the source volume before the Hyper-Scale Mobility process started.



Volume	System	Pool	Volume...	Size (Di...	Snap...
ITSO_mail_003	A9000R	ITSO_p1	300 GB	310 GB	2
itso_mail_dup_001	A9000R	ITSO_p1	300 GB	310 GB	1
ITSO_mobility_001	A9000	ITSO_p1	200 GB	207 GB	0
ITSO_mobility_002	A9000	ITSO_p1	200 GB	207 GB	0

Figure 7-29 Volume list after clean-up

Confirm that the source volume is no longer on the source FlashSystem A9000 or A9000R and a new volume that matches the source now exists on the destination FlashSystem A9000 or A9000R.

7.7.2 Using the command-line interface with Hyper-Scale Mobility

This section illustrates using the XCLI for Hyper-Scale Mobility. The process consists of the same six tasks that are described and illustrated in 7.7.1, “Using Hyper-Scale Mobility with Hyper-Scale Manager GUI” on page 142.

Task 1: Planning and preparation

To perform an online migration of an FlashSystem A9000 or A9000R volume by using the XCLI, follow these steps:

1. Confirm that both the source and destination FlashSystem A9000 or A9000R are configured and accessible through the XCLI, and that there is Fibre Channel connectivity between these systems.

   Example 7-6 shows the **target_list** and **target_connectivity_list** commands run on the source FlashSystem A9000 or A9000R to confirm the connectivity. The output that is shown in Example 7-6 shows that the destination FlashSystem A9000 or A9000R is connected through only a single active FC connection.

Example 7-6 The target_list and target_connectivity_list commands before migration

```
#Source:
A9000_ITSO>>target_list
Name                SCSI Type   Connected   Max Initialization Rate   Max Resync Rate   Max Syncjob Rate
A9000 6003308 Jazz   FC          yes         100                       300               300
A9000_ITSO>>target_connectivity_list
Target Name          Remote Port        FC Port         IP Interface   Active   Up
A9000 6003308 Jazz   500173800CEC0123   1:FC_Port:3:4                  yes      yes

#Destination:
A9000 6003308 Jazz>>target_connectivity_list
Target Name         Remote Port        FC Port         IP Interface   Active   Up
A9000_ITSO          500173800CEE0123   1:FC_Port:3:4                  yes      yes
```

2. In addition, confirm that any host that has mappings to the source volume on the source FlashSystem A9000 or A9000R has the appropriate access to the destination system.

   Consider the following items:

   – For a migration of an iSCSI LUN, ensure that the host can access the destination system over the IP network.

   – For a migration of an FC LUN, ensure that the host is correctly zoned to the destination system.

3. Validate the host multipath connectivity to the source volume by running the **xiv_devlist** command of the HAK, as shown in Example 7-7.

Example 7-7 The xiv_devlist command before migration

```
[root@mcnode81 ~]# xiv_devlist
IBM Devices
------------------------------------------------------------------------------
                                                                  System  System
Device               Size (GB)  Paths  Vol Name           Vol ID   ID      Host
------------------------------------------------------------------------------
/dev/mapper/mpathaqf 1033.6     8/8    HS_Mob_6003310_03  13445   6003310  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaql 1033.6     8/8    HS_Mob_6003310_01  13452   6003310  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaqo 1033.6     6/6    HS_Mob_6003310_02  13453   6003308  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaxu 2067.3     6/6    HS_Mob_6003308_01  15857   6003308  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaxv 2067.3     6/6    HS_Mob_6003308_03  15859   6003308  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathayb 2067.3     6/6    HS_Mob_6003308_02  15858   6003308  mcnode81
------------------------------------------------------------------------------
```

Note the Vol ID of 13452 and System ID of 6003310, which indicates that the volume is presented to the host from the source FlashSystem A9000 6003310.

Example 7-8 shows the output of the **vol_list** command for the source and destination FlashSystem A9000s before the start of the Hyper-Scale Mobility process.

Example 7-8 The vol_list command on source and destination IBM FlashSystem A9000s before migration

```
#Source:
A9000_ITSO>>vol_list pool=ITSO_HSM
Name               Size (GB)   Master Name   Consistency Group   Pool       Creator   Written (GB)
HS_Mob_6003310_03  1033                                          ITSO_HSM   admin     0
HS_Mob_6003310_11  1033                                          ITSO_HSM   admin     0
HS_Mob_6003310_12  1033                                          ITSO_HSM   admin     0
HS_Mob_6003310_01  1033                                          ITSO_HSM   admin     30

#Destination:
A9000 6003308 Jazz>>vol_list pool=ITSO_HSM
Name               Size (GB)   Master Name   Consistency Group   Pool       Creator   Written (GB)
HS_Mob_6003308_01  2067                                          ITSO_HSM   admin     53
HS_Mob_6003308_02  2067                                          ITSO_HSM   admin     0
HS_Mob_6003308_03  2067                                          ITSO_HSM   admin     0
HS_Mob_6003308_10  2067                                          ITSO_HSM   admin     3
HS_Mob_6003308_11  2067                                          ITSO_HSM   admin     0
HS_Mob_6003308_12  2067                                          ITSO_HSM   admin     0
HS_Mob_6003310_02  1033                                          ITSO_HSM             53
```

Task 2: Setup

To perform the Setup task, complete the following steps:

1. To create the Hyper-Scale Mobility relationship, run the **olvm_create** command, as shown in Example 7-9. The required parameters are **vol=**, **remote_pool=**, and **target=**.

> **Attention:** Any existing snapshot for the Hyper-Scale Mobility source volume is *deleted without explicit warning* from the XCLI when the **olvm_create** command is run.

Example 7-9 The olvm_create command

```
#Source:
A9000_ITSO>>olvm_create vol=HS_Mob_6003310_01 remote_pool=ITSO_HSM target="A9000 6003308 Jazz"
Command executed successfully.
A9000_ITSO>>olvm_list
Volume name         Role     Remote System        Active   Phase       State          Link Up
HS_Mob_6003310_01   source   A9000 6003308 Jazz   no       migration   Initializing   yes

#Destination:
A9000 6003308 Jazz>>olvm_list
Volume name         Role          Remote System   Active   Phase       State          Link Up
HS_Mob_6003310_01   destination   A9000_ITSO      no       migration   Initializing   yes
```

2. As seen in Example 7-9, running the **olvm_create** command accomplishes the following tasks:
   - Creates a volume on the destination FlashSystem A9000 or A9000R with the same name as the source volume, in the specified **remote_pool**.
   - Creates a Hyper-Scale Mobility relationship between the source FlashSystem A9000 or A9000R volume and the destination volume.

   The **olvm_create** command only creates the relationship. The Hyper-Scale Mobility relationship is not activated in this step, and the destination volume is empty.

Task 3: Migration

To complete the migration task, complete the following steps:

1. After the Hyper-Scale Mobility relationship is created, activate it by running the **olvm_activate** command, as shown in Example 7-10 on page 159.

Example 7-10 The olvm_activate command

```
#Source:
A9000_ITSO>>olvm_activate vol=HS_Mob_6003310_01
Command executed successfully.
A9000_ITSO>>olvm_list
Volume name         Role     Remote System        Active   Phase       State          Link Up
HS_Mob_6003310_01   source   A9000 6003308 Jazz   yes      migration   Initializing   yes

#After initialization is complete:
A9000_ITSO>>olvm_list
Volume name         Role     Remote System        Active   Phase   State          Link Up
HS_Mob_6003310_01   source   A9000 6003308 Jazz   yes      ready   Synchronized   yes

#Destination:
A9000 6003308 Jazz>>olvm_list
Volume name         Role          Remote System   Active   Phase       State          Link Up
HS_Mob_6003310_01   destination   A9000_ITSO      yes      migration   Initializing   yes

#After initialization is complete:
A9000 6003308 Jazz>>olvm_list
Volume name         Role          Remote System   Active   Phase   State        Link Up
HS_Mob_6003310_01   destination   A9000_ITSO      yes      ready   Consistent   yes
```

2. The **olvm_activate** command initializes the synchronization of the source and destination volumes. Note that the Hyper-Scale Mobility relationship becomes active (`Active=yes`). The synchronization is queued because only one Hyper-Scale Mobility process is synchronized at a time.

   The time that is required to complete the synchronization depends on numerous factors, including how many migrations are active, and the amount of data that needs to be synchronized per volume. After the synchronization has completed, the Phase changes to `ready` on both the source and destination volumes. Additionally, the State changes to `Synchronized` on the source volume as the State changes to `Consistent` on the destination volume.

Task 4: Proxying

Proxying means that the source FlashSystem A9000 or A9000R starts redirecting host I/O to the volume on the destination system. To start the proxy mode, complete the following steps:

1. During the migration, host and host-port definitions can be created by running the commands that are shown in Example 7-11. Note that these definitions can also be done before, and independently of, the migration process.

   Example 7-11 The host_define and host_add_port commands

   ```
   #Destination:
   A9000 6003308 Jazz>>host_define host=mcnode81
   Command executed successfully.
   A9000 6003308 Jazz>>host_add_port host=mcnode81 fcaddress=10000090FA731D36
   Command executed successfully.
   A9000 6003308 Jazz>>host_add_port host=mcnode81 fcaddress=10000090FA731D37
   Command executed successfully.
   ```

Example 7-12 shows the resulting host definition on the destination FlashSystem A9000.

Example 7-12 The host_list command on the destination FlashSystem A9000

```
A9000 6003308 Jazz>>host_list host=mcnode81
Name       Type      FC Ports                          iSCSI Ports   User Group   Cluster   Performance Class
mcnode81   default   10000090FA731D36,10000090FA731D37                                      none
```

2. Run the XCLI **olvm_proxy** command to start the Proxy phase, as shown in Example 7-13.

Important: Upon initiating the Proxy phase for a volume, it is no longer possible to stop the Hyper-Scale Mobility for this volume. Up to this point, the source volume still exists on the source FlashSystem A9000 or A9000R, and any host I/O is still synchronized between both source and destination volumes.

Answering `y` to confirm the command execution shown in Example 7-13 triggers the source FlashSystem A9000 or A9000R to proxy all subsequent host I/O to the volume on the destination system only. The source volume becomes inconsistent and unavailable. The source volume is now just a logical placeholder for the original volume. Its size is 0 GB, and its hard (total usable) capacity is returned to the storage pool.

Example 7-13 The olvm_proxy command

```
#Source:
A9000_ITSO>>olvm_proxy vol=HS_Mob_6003310_01

Warning:   Are you sure you want to move the volume HS_Mob_6003310_01 to a
Proxy state? Source volume and all volume snapshots will be deleted. y/n: y
Command executed successfully.
A9000_ITSO>>olvm_list
Volume name         Role     Remote System        Active   Phase   State   Link Up
HS_Mob_6003310_01   source   A9000 6003308 Jazz   yes      proxy   Proxy   yes

#Destination:
A9000 6003308 Jazz>>olvm_list
Volume name         Role          Remote System   Active   Phase   State     Link Up
HS_Mob_6003310_01   destination   A9000_ITSO      yes      proxy   Proxied   yes
```

3. To verify the start of the Proxy phase, issue the **olvm_list** command, as shown in Example 7-14 on page 161. The State of the source volume changes to `Proxy`, and the State of the destination volume changes to `Proxied`. All host I/O to the source volume is redirected (proxied) to the destination volume.

In Example 7-14, the output of the **vol_list** command on each FlashSystem A9000 now shows that the volume named HS_Mob_6003310_01 is no longer showing on the source system, but has been moved to the destination system.

Example 7-14 The vol_list command after the Hyper-Scale Process is in State Proxy/Proxied

```
#Source:
A9000_ITSO>>vol_list pool=ITSO_HSM
Name               Size (GB)   Master Name   Consistency Group   Pool       Creator   Written (GB)
HS_Mob_6003310_03  1033                                          ITSO_HSM   admin     0
HS_Mob_6003310_11  1033                                          ITSO_HSM   admin     0
HS_Mob_6003310_12  1033                                          ITSO_HSM   admin     0

#Destination:
A9000 6003308 Jazz>>vol_list pool=ITSO_HSM
Name               Size (GB)   Master Name   Consistency Group   Pool       Creator   Written (GB)
HS_Mob_6003308_01  2067                                          ITSO_HSM   admin     53
HS_Mob_6003308_02  2067                                          ITSO_HSM   admin     0
HS_Mob_6003308_03  2067                                          ITSO_HSM   admin     0
HS_Mob_6003308_10  2067                                          ITSO_HSM   admin     3
HS_Mob_6003308_11  2067                                          ITSO_HSM   admin     0
HS_Mob_6003308_12  2067                                          ITSO_HSM   admin     0
HS_Mob_6003310_02  1033                                          ITSO_HSM             53
HS_Mob_6003310_01  1033                                          ITSO_HSM             30
```

4. After the Proxy phase is successfully initiated, the destination volume can be mapped to the host by running the **map_vol** command, as shown in Example 7-15.

Example 7-15 The map_vol command

```
#Destination:
A9000 6003308 Jazz>>map_vol vol=HS_Mob_6003310_01 host=mcnode81 lun=3
Command executed successfully.
```

5. After mapping, rescan the devices from the host to pick up the new paths to the volume on the destination FlashSystem A9000 or A9000R. Run the **xiv_fc_admin -R** command, and then run the **xiv_devlist** command from the host, as shown in Example 7-16.

Example 7-16 The xiv_fc_admin -R and xiv_devlist commands

```
[root@mcnode81 ~]# xiv_fc_admin -R
[root@mcnode81 ~]# xiv_devlist
IBM Devices
-------------------------------------------------------------------------------
                                                                  System  System
Device               Size (GB)  Paths  Vol Name          Vol ID   ID      Host
-------------------------------------------------------------------------------
/dev/mapper/mpathaqf 1033.6     8/8    HS_Mob_6003310_03 13445   6003310 mcnode81
-------------------------------------------------------------------------------
/dev/mapper/mpathaql 1033.6     14/14  HS_Mob_6003310_01 13452   6003310 mcnode81
-------------------------------------------------------------------------------
/dev/mapper/mpathaqo 1033.6     6/6    HS_Mob_6003310_02 13453   6003308 mcnode81
-------------------------------------------------------------------------------
/dev/mapper/mpathaxu 2067.3     6/6    HS_Mob_6003308_01 15857   6003308 mcnode81
-------------------------------------------------------------------------------
/dev/mapper/mpathaxv 2067.3     6/6    HS_Mob_6003308_03 15859   6003308 mcnode81
-------------------------------------------------------------------------------
/dev/mapper/mpathayb 2067.3     6/6    HS_Mob_6003308_02 15858   6003308 mcnode81
-------------------------------------------------------------------------------
```

Note the 14 paths (six additional) for the destination volume, HS_Mob_6003310_01, in the bold row in Example 7-16 on page 161.

Task 5: Cleanup

To complete the Cleanup task, perform the following steps:

1. After validating that the host has connectivity to the destination volume through the new paths to the destination FlashSystem A9000 or A9000R, unmap the source volume on the source FlashSystem A9000 or A9000R from the host, as shown in Example 7-17.

Example 7-17 The unmap_vol command

```
#Source:
A9000_ITSO>>unmap_vol vol=HS_Mob_6003310_01 host=mcnode81
Command executed successfully.
A9000_ITSO>>olvm_list
Volume name         Role     Remote System        Active   Phase   State   Link Up
HS_Mob_6003310_01   source   A9000 6003308 Jazz   yes      proxy   Proxy   yes

#Destination:
A9000 6003308 Jazz>>olvm_list
Volume name         Role          Remote System   Active   Phase   State     Link Up
HS_Mob_6003310_01   destination   A9000_ITSO      yes      proxy   Proxied   yes
```

2. After unmapping the volume from the host, only six enabled paths to the volume remain to the host. From the host, run the **xiv_fc_admin -R** command followed by the **xiv_devlist** command, as shown in Example 7-18.

Example 7-18 6 out of the 14 paths enabled

```
[root@mcnode81 ~]# xiv_fc_admin -R
[root@mcnode81 ~]# xiv_devlist
IBM Devices
------------------------------------------------------------------------------
                                                                 System  System
Device               Size (GB)  Paths  Vol Name           Vol ID   ID      Host
------------------------------------------------------------------------------
/dev/mapper/mpathaqf  1033.6     8/8    HS_Mob_6003310_03  13445   6003310  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaql  1033.6     6/14   HS_Mob_6003310_01  13452   6003308  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaqo  1033.6     6/6    HS_Mob_6003310_02  13453   6003308  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaxu  2067.3     6/6    HS_Mob_6003308_01  15857   6003308  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaxv  2067.3     6/6    HS_Mob_6003308_03  15859   6003308  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathayb  2067.3     6/6    HS_Mob_6003308_02  15858   6003308  mcnode81
------------------------------------------------------------------------------
```

Note the unmatching paths for the destination volume, HS_Mob_6003310_01, in the bold row. Also, note that the Vol ID is still 13452 and the System ID has changed to 6003308. These IDs indicate that the host is connected *only* to the destination volume on the destination FlashSystem A9000. The destination FlashSystem A9000 keeps the same Vol ID, if possible.

3. Run the **xiv_fc_admin -R --clean** command, and then run the **xiv_devlist** command from the host to remove the failed paths from the RHEL host, as shown in Example 7-19. To remove the failed paths from an AIX host, a sample script is shown in Example 7-5 on page 154.

Example 7-19 Path removal and rescan for RHEL

```
[root@mcnode81 ~]# xiv_fc_admin -R --clean
[root@mcnode81 ~]# xiv_devlist
IBM Devices
------------------------------------------------------------------------------
                                                                 System  System
Device               Size (GB)  Paths  Vol Name          Vol ID   ID      Host
------------------------------------------------------------------------------
/dev/mapper/mpathaqf  1033.6     8/8    HS_Mob_6003310_03  13445   6003310  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaql  1033.6     6/6    HS_Mob_6003310_01  13452   6003308  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaqo  1033.6     6/6    HS_Mob_6003310_02  13453   6003308  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaxu  2067.3     6/6    HS_Mob_6003308_01  15857   6003308  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathaxv  2067.3     6/6    HS_Mob_6003308_03  15859   6003308  mcnode81
------------------------------------------------------------------------------
/dev/mapper/mpathayb  2067.3     6/6    HS_Mob_6003308_02  15858   6003308  mcnode81
------------------------------------------------------------------------------
```

Task 6: Post-cleanup

The previous example successfully used Hyper-Scale Mobility by using the XCLI to move the volume HS_Mob_6003310_01 from FlashSystem A9000 6003310 to FlashSystem A9000 6003308 without incurring any downtime on the host. The final step is to end the proxy and delete the relationship: To accomplish this task, complete the following steps:

1. Run the **olvm_delete** command, as shown in Example 7-20.

Example 7-20 The olvm_delete command

```
#Source:
A9000_ITSO>>olvm_delete vol=HS_Mob_6003310_01

Warning:   Are you sure you want to delete IBM Hyper-Scale Mobility relationship? y/n: y
Command executed successfully.
A9000_ITSO>>olvm_list
No olvms match the given criteria

#Destination:
A9000 6003308 Jazz>>olvm_list
No olvms match the given criteria
```

2. The proxy has been removed and the expected end state of the volumes on both the source and destination FlashSystem A9000s are shown in Example 7-21. On the source FlashSystem A9000, volume HS_Mob_6003310_01 no longer exists. On the destination FlashSystem A9000, there is a new volume named HS_Mob_6003310_01. This volume has the matching size and Written percentage (Used capacity) as the source volume before the Hyper-Scale Mobility process start.

Example 7-21 The vol_list by pool command

```
#Source:
A9000_ITSO>>vol_list pool=ITSO_HSM
Name                Size (GB)   Master Name   Consistency Group   Pool       Creator   Written (GB)
HS_Mob_6003310_03   1033                                          ITSO_HSM   admin     0
HS_Mob_6003310_11   1033                                          ITSO_HSM   admin     0
HS_Mob_6003310_12   1033                                          ITSO_HSM   admin     0

#Destination:
A9000 6003308 Jazz>>vol_list pool=ITSO_HSM
Name                Size (GB)   Master Name   Consistency Group   Pool       Creator   Written (GB)
HS_Mob_6003308_01   2067                                          ITSO_HSM   admin     53
HS_Mob_6003308_02   2067                                          ITSO_HSM   admin     0
HS_Mob_6003308_03   2067                                          ITSO_HSM   admin     0
HS_Mob_6003308_10   2067                                          ITSO_HSM   admin     3
HS_Mob_6003308_11   2067                                          ITSO_HSM   admin     0
HS_Mob_6003308_12   2067                                          ITSO_HSM   admin     0
HS_Mob_6003310_02   1033                                          ITSO_HSM             53
HS_Mob_6003310_01   1033                                          ITSO_HSM             30
```

7.7.3 Migrating volumes from XIV to FlashSystem A9000 or A9000R using Hyper-Scale Manager

This section illustrates how to use Hyper-Scale Mobility by using the Hyper-Scale Manager to move a volume from XIV to FlashSystem A9000. The process is the same regardless of the destination system and follows the same process as described in “Using Hyper-Scale Mobility with Hyper-Scale Manager GUI” on page 142. We have followed the same set if six tasks with the condensed information here for illustration purposes.

Note: IBM Storage Host Attachment Toolkit V2.9.0 or later is required.

Task 1: Planning and preparation

1. Confirm that both the source and destination are configured and accessible in the Hyper-Scale Manager and that there is FC connectivity between these systems. Figure 7-30 shows the source (XIV) and destination (A9000) systems with confirmed connectivity between them.

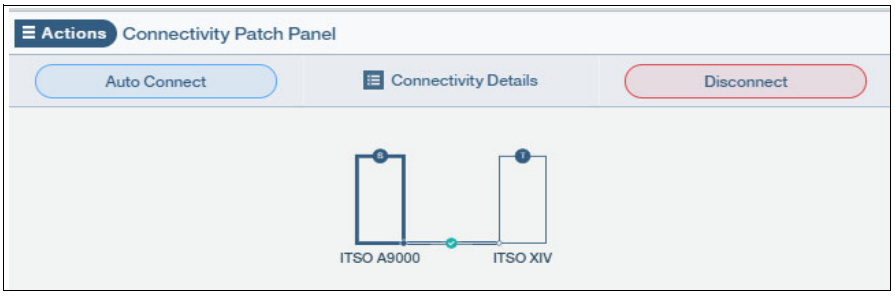


Figure 7-30 Connectivity between A9000 and XIV

2. Validate the host multipath connectivity to the source volume by running the **xiv_devlist** command of the Host Attachment Kit (HAK), as shown for a Windows host in Figure 7-31.

```
PS C:\Users\Administrator> xiv_devlist.exe
IBM storage devices
-------------------------------------------------------------------------------------------------------------
Device             Size (GB)  Paths  Vol Name      Vol ID  Storage ID  Storage Type  Hyper-Scale Mobility
-------------------------------------------------------------------------------------------------------------
\\.\PHYSICALDRIVE1  30.0       4/4    itso_vol_001  7       1310040     XIV           Idle
-------------------------------------------------------------------------------------------------------------
\\.\PHYSICALDRIVE2  30.0       4/4    itso_vol_002  8       1310040     XIV           Idle
-------------------------------------------------------------------------------------------------------------
\\.\PHYSICALDRIVE3  30.0       4/4    itso_vol_003  9       1310040     XIV           Idle
-------------------------------------------------------------------------------------------------------------
```

Figure 7-31 Output on Windows server for xiv_devlist

3. Ensure that the zoning for the host has been done so that it is connected to the destination system. When that is completed, add the host definition to the destination system making sure to define the ports as shown in Figure 7-32. In this example we have zoned and defined the Windows server to the destination system, ITSO A9000. The process is fully documented in “Task 1: Planning and preparation” on page 142.

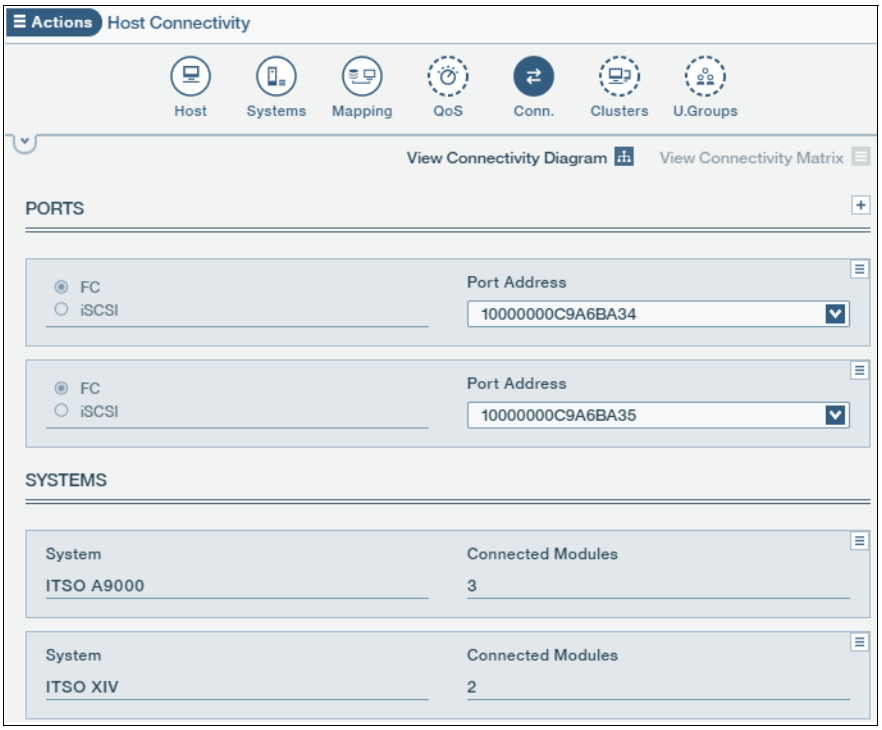


Figure 7-32 Host connectivity ports and systems

Task 2 and 3: Setup and migration

To setup Hyper-Scale Mobility between XIV and FlashSystem A9000 or A9000R, complete the following steps:

1. Create the relationship by selecting the source volume in the Volumes view and select Mobility element in the Hub, as shown in Figure 7-33. Notice that the dashed line indicates Mobility has not been defined for the selected volume. Selecting this option opens a screen as shown in Figure 7-34. Click on the “+” symbol to define the mobility relationship.

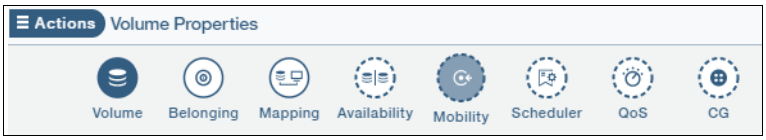


Figure 7-33 Mobility element in the hub

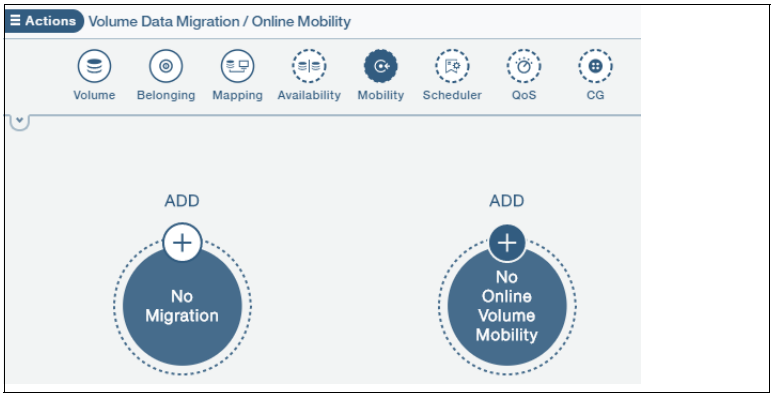


Figure 7-34 Create a new Mobility definition

2. Enter the information for the destination system as shown in Figure 7-35. The volume on the destination side will be created by this process automatically. The name of the destination volume will match the source volume. Click **Create** to create the relationship and activate the process.

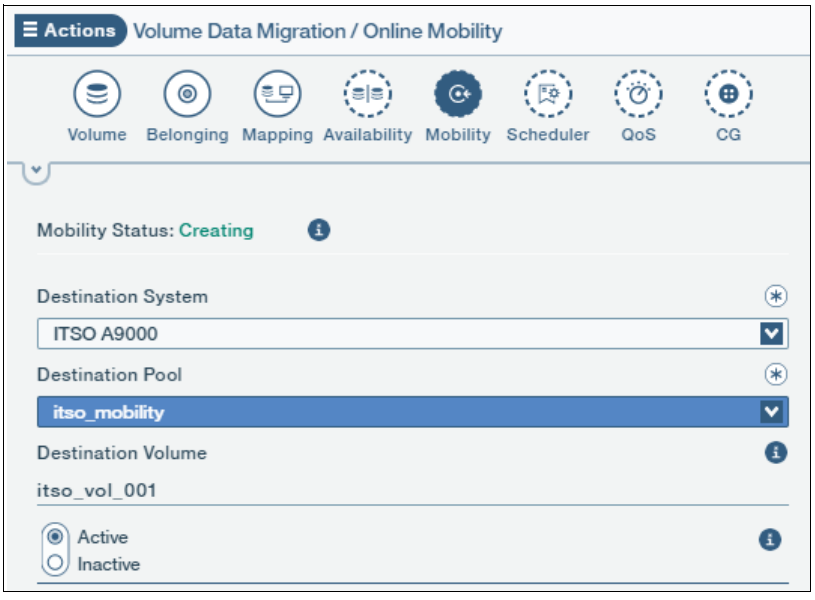


Figure 7-35 Define the destination information

3. By selecting Active when creating the relationship, the initialization phase will begin as soon as Create is selected. The process will run serially if more than one volume is defined. Examples of what can be seen during this phase is shown in Figure 7-36 and Figure 7-37.

Figure 7-36 Initialization from element manager

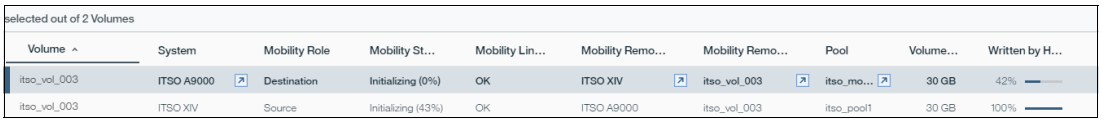


Figure 7-37 Initialization from Online Mobility view

At this point, host writes are going to the XIV system and the data is being copied to the destination FlashSystem A9000. The initialization phase must reach synchronized state before continuing to the proxy task. At this point, volume data is mirrored and consistent on both the source and destination volumes. It is still possible to stop the migration without impact to the source volume. When proceeding to the next step, you will not be able to return.

Task 4: Proxy

Proxy means that the source XIV will start to redirect all host I/O to the destination volume. Again, this is the point of no return so ensure you are ready before moving forward.

1. Validate the Mobility status as shown in Figure 7-38 and Figure 7-39 to ensure that it is ready for Proxy mode.

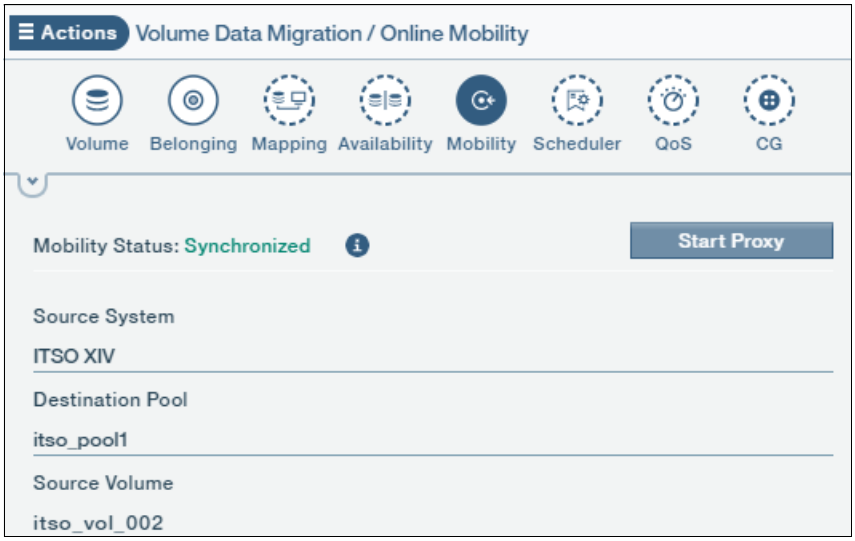


Figure 7-38 Synchronized state

Figure 7-39 Synchronized state from the Volumes view

2. To start proxy, select the source volume (or more than one as needed) and click on the Proxy button. You will get a warning message as shown in Figure 7-40. When in Proxy mode, all the host I/O's will be passed through the source to the destination volume. At this point the host is still connected to the source system.

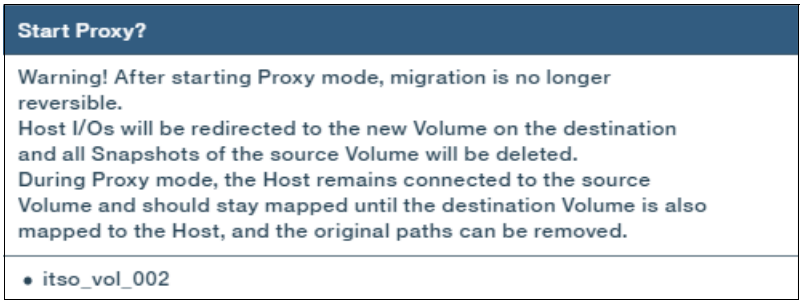


Figure 7-40 Proxy warning message

3. When in the Proxy state, you can now map the destination volume(s) to the host. This mapping was shown in "Task 4: Proxying" on page 149 and does not change when using Mobility from XIV to FlashSystem A9000 or A9000R.

4. When the mapping has been completed, use the HAK command *xiv_fc_admin -R* to rescan for the new paths to the FlashSystem A9000 or A9000R. Then issue the *xiv_devlist* command to view the increased number of paths. An example of this output is shown in Figure 7-41. Note that the storage type has now changed for volume *itso_vol_003* from XIV to FlashSystem A9000. Additionally, the number of paths have gone from 4 to 10 (6 paths to the FlashSystem A9000 in this example).

```
PS C:\Program Files\xiv\host_attach\bin> .\xiv_devlist.exe
IBM storage devices
------------------------------------------------------------------------------------------------------------------
Device              Size (GB)  Paths  Vol Name          Vol ID  Storage ID  Storage Type       Hyper-Scale Mobility
------------------------------------------------------------------------------------------------------------------
\\.\PHYSICALDRIVE1  30.0       6/6    itso_vol_001      7       1322133     FlashSystem A9000  Proxy Disabled
------------------------------------------------------------------------------------------------------------------
\\.\PHYSICALDRIVE2  30.0       6/6    itso_vol_002      8       1322133     FlashSystem A9000  Proxy Disabled
------------------------------------------------------------------------------------------------------------------
\\.\PHYSICALDRIVE3  30.0       10/10  itso_vol_003      9       1322133     FlashSystem A9000  Proxy
------------------------------------------------------------------------------------------------------------------
\\.\PHYSICALDRIVE4  34.0       4/4    itso_win_vol_001  10      1310040     XIV                Idle
------------------------------------------------------------------------------------------------------------------
\\.\PHYSICALDRIVE5  34.0       4/4    itso_win_vol_002  11      1310040     XIV                Idle
------------------------------------------------------------------------------------------------------------------
```

Figure 7-41 Additional paths detected after rescan command

5. If you do not see the additional paths and the storage type changing to FlashSystem A9000 or A9000R, do not proceed to the next task until you do. At this point, the XIV is simply passing the read and write requests on to the FlashSystem A9000 or A9000R.

Task 5 and 6 Cleanup and post cleanup

These tasks are identical to the those shown in “Task 5: Cleanup” on page 153 and “Task 6: Post-cleanup” on page 155 so will not be repeated here in full. Remember that when the server/host has discovered the additional paths you are able to end the proxy and clean up the paths from XIV by running the HAK command *xiv_fc_admin -R -- clean* followed by the HAK command *xiv_devlist* to verify that the paths were removed. In our example, we have 6 paths to the FlashSystem A9000 so the path count will decrease from 10 to 6 as shown in Figure 7-41 for volumes `itso_vol_001` and `itso_vol_002`. These volumes have completed the migration from XIV to the FlashSystem A9000.

8

Data migration

This chapter provides a description of the migration process, which is a built-in feature of IBM FlashSystem A9000 and IBM FlashSystem A9000R. The Data Migration Utility can migrate data from almost any storage system to IBM FlashSystem A9000 and A9000R. The chapter also includes the pre-migration and post-migration steps.

This chapter includes the following sections:

- Migration overview
- Source storage connectivity
- Detailed migration steps for an iSCSI connection
- Detailed migration steps for a Fibre Channel connection

8.1 Migration overview

IBM FlashSystem A9000 and A9000R include, at no extra charge, a powerful data migration capability. The Data Migration utility can migrate data from almost any storage system to IBM FlashSystem A9000 and A9000R.

At the start of the migration, application hosts are offline for only a short time as they are connected to IBM FlashSystem A9000 or A9000R. The logical volumes, also known as logical unit numbers (LUNs), that are migrated are reallocated from the former storage server to FlashSystem A9000 or A9000R and are then natively presented again to the host. Meanwhile, the data is transparently migrated in the background, in a controlled fashion.

The migration overview, which is depicted in Figure 8-1, assumes a migration from another storage system to FlashSystem A9000 or A9000R. The storage system can be an IBM storage system or another storage system, if that storage system supports Linux hosts. The migration process is the same for all storage systems.

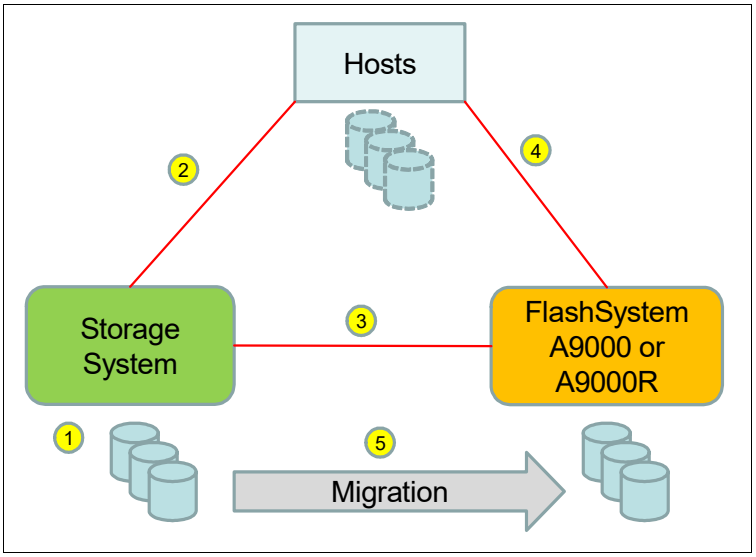


Figure 8-1 Migration overview

Figure 8-1 shows the process (the following numbers correspond to the numbers in the figure):

1. Volumes and pools that are defined in the Storage System are initially used by host systems.
2. Hosts are connected over Fibre Channel (FC) or internet Small Computer System Interface (iSCSI) targets, and the LUNs that are defined in the Storage System are mapped to those hosts.
3. An FC or iSCSI target is defined in IBM FlashSystem A9000 or A9000R for the Storage System, as though it were a host. Target migration volumes in IBM FlashSystem A9000 or A9000R are defined and mapped to the remote LUNs in the Storage System.
4. A new FC or iSCSI host object for the host must be defined in IBM FlashSystem A9000 or A9000R. At this stage, the storage system has two hosts that are defined in the system (the actual host and IBM FlashSystem A9000 or A9000R).

5. The migration feature is now enabled in FlashSystem A9000 or A9000R. Before this enablement starts, the host connectivity to the Storage System must be terminated (apparent downtime for the host), and the volumes being migrated are manually presented by FlashSystem A9000 or A9000R to the host.

8.2 Source storage connectivity

This section describes several considerations regarding the connectivity between IBM FlashSystem A9000 or A9000R and the source storage being migrated.

8.2.1 Multipathing with data migrations

Three types of storage systems controllers can be considered regarding multipathing:

- Active/Active Controllers: With these storage systems, volumes can be active on all of the storage system controllers at the same time (whether there are two controllers or more). These systems support I/O activity to any specific volume through two or more paths. These types of storage systems typically support load balancing capabilities between the paths, with path failover and recovery during a path failure.

  FlashSystem A9000 and A9000R are such devices and can use this technology during data migrations. Examples of IBM products that are active/active storage servers are the DS8000 series of products.

  If your source storage system supports active/active, you can carefully configure multiple paths from IBM FlashSystem A9000 or A9000R to the source storage system. IBM FlashSystem A9000 or A9000R load balances the migration traffic across all paths, and it automatically handles path failures.

- Active/Passive Controllers: With these storage systems, any specific volume can be active on only one controller at a time. These storage devices do not support I/O activity to any specific volume through multiple paths at the same time. Most devices support active volumes on one or more controllers at the same time, but any specific volume can be active on only one controller at a time.

- Asymmetric Logical Unit Access (ALUA) Controllers: These storage systems are essentially active/passive multipathing systems with some intelligence built in. These systems have a preferred path but can switch the owning controller depending on where I/O requests originate. Different implementations of ALUA exist, each with its own nuances.

  When migrating, ALUA should be deactivated and connectivity between IBM FlashSystem A9000 or A9000R and the source storage system be set up as active/passive. Because IBM FlashSystem A9000 or A9000R is an active/active storage system, it requests I/O from all defined paths.

  This activity can lead to a “ping-pong” affect as the source storage system switches the LUN’s owning controller back and forth from controller to controller. This effect, in turn, can lead to severe performance issues during the migration.

Migrating from an active/active storage device

If the source storage system supports active/active LUN access, then you can configure multiple paths from IBM FlashSystem A9000 or A9000R to the source storage system. IBM FlashSystem A9000 or A9000R balances the migration traffic across these paths.

This feature might tempt you to configure more than two connections, or to increase the initialization speed to a large value to speed up the migration. However, IBM FlashSystem A9000 or A9000R can synchronize only one volume at a time per target (with four targets, this feature means that four volumes can be migrated at the same time). Therefore, the speed of the migration from each target is determined by the ability of the source storage system to read from the LUN currently being migrated.

Unless the source storage system has striped the volume across multiple RAID arrays, the migration speed is unlikely to exceed 250 - 300 MBps (and can be much less). This speed is totally dependent on the source storage system.

If the source storage system is used by other servers while migrating the data to IBM FlashSystem A9000 or A9000R, care must be taken not to overwork the source storage system. An overload might lead to an increase in latency on the other servers doing the I/O.

It is best to leave the IBM FlashSystem A9000 or A9000R migration speed set to the defaults and start migrating slowly to see how the existing environment can handle the change. As the comfort levels rise and the migration process in a particular environment is learned, settings can be changed and more server LUNs can be moved.

Important: If multiple paths are created between an IBM FlashSystem A9000 or A9000R and an active/active storage device, the same SCSI LUN IDs to host IDs associations must be used for each LUN on each path, or data corruption occurs.

Configure a maximum of two paths per target. Defining more paths does not increase throughput. With some storage arrays, defining more paths adds complexity and increases the likelihood of configuration issues and corruption.

Migrating from an active/passive storage device

Because of their active/active nature, special considerations must be made when migrating data from an active/passive storage device to IBM FlashSystem A9000 or A9000R. A single path is configured between any source storage system controller and the IBM FlashSystem A9000 or A9000R. Many users decide to run migrations with the host applications offline because of the single path.

Define the target to the IBM FlashSystem A9000 or A9000R for each source storage controller (controller, not port). Define at least one path from that controller to IBM FlashSystem A9000 or A9000R. All of the active volumes on the controller can be migrated using the defined target for that controller (for example, if the source storage system contains two controllers, A and B, as shown in Figure 8-2).

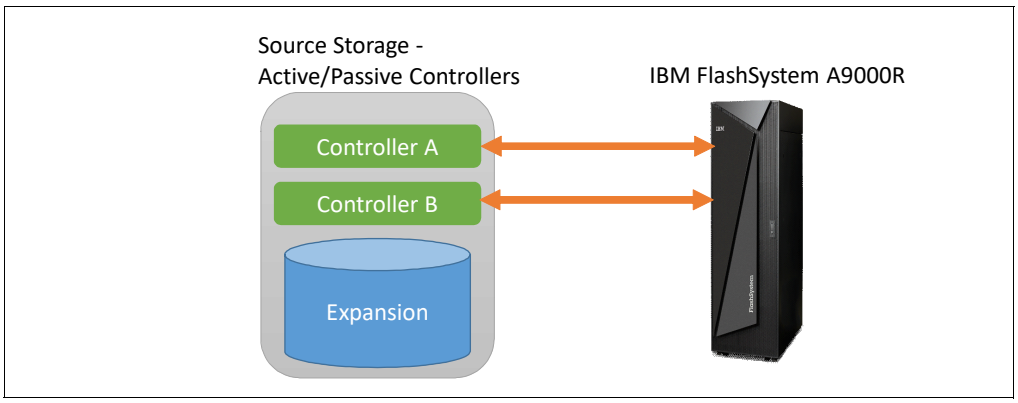


Figure 8-2 Migration between Active/Passive Controllers and IBM FlashSystem A9000R

Complete these steps:

1. Define one target (called controller A, for example) with one path between the IBM FlashSystem A9000 or A9000R and one controller on the source storage system (for example, controller *A*). All active volumes on this controller can be migrated by using this target.

   When defining the IBM FlashSystem A9000 or A9000R initiator to the controller, be sure to define it as *not* supporting failover or ALUA if these options are available on the source storage array. By doing so, volumes that are passive on controller *A* are not presented to the IBM FlashSystem A9000 or A9000R.

   Check the source storage system documentation for information about changing the ALUA or failover configuration on the controllers.

2. Define another target (called controller B, for example) with one path between IBM FlashSystem A9000 or A9000R and controller *B*. All volumes active on controller *B* can be migrated to the IBM FlashSystem A9000 or A9000R by using this target.

   When defining the IBM FlashSystem A9000 or A9000R initiator to the controller, be sure to define it as *not* supporting failover or ALUA if these options are available. By doing so, volumes that are passive on controller *B* are not presented to IBM FlashSystem A9000 or A9000R.

   Check the source storage system documentation for changing the ALUA or failover configuration on the controllers.

Important:

- If a single controller has two target ports, both can be defined as links for that controller target. Make sure that the two target links are connected to separate IBM FlashSystem A9000 or A9000R grid controllers or grid elements for redundancy during a grid controller or grid element failure. However, the migration fails if the LUN being migrated trespasses (ownership transfers) to the other controller.
- If you define an active/passive source storage controller as a target, do not define the alternate controller as a second port on the first target. Doing so causes unexpected issues, such as migration failure, preferred path errors on the source storage, slow migration progress, and corruption.

8.3 Detailed migration steps for an iSCSI connection

Note: We chose to migrate from an IBM XIV Storage System to IBM FlashSystem A9000. These systems were used for illustration because they were available for our experimentation. Migration can be performed from any storage system that can attach to a Linux host. The setup details differ based on the storage system.

At a high level, we used the following steps to migrate volumes from an XIV Storage System (or any iSCSI attached storage system) to IBM FlashSystem A9000:

1. Initial connection and preparation:
   a. Establish connection between the XIV Storage System (or any storage system) and IBM FlashSystem A9000.
   b. Prepare an iSCSI qualified name (IQN) table for all of the systems that are involved.
   c. Assume that the volumes and the host are already defined in the XIV Storage System.

d. Define IBM FlashSystem A9000 as a host object on the XIV Storage System with type **Default**.

e. Define XIV Storage System in IBM FlashSystem A9000 as a migration target.

2. Perform pre-migration tasks for each host that is attached to the XIV that will be migrated:

   a. Back up host data.

   b. Stop all I/O from the host to the LUNs on the XIV storage.

   c. Update the Host Attachment Kit (HAK) to the current version.

   Important: If your migration source is not an IBM XIV, IBM FlashSystem A9000, or IBM FlashSystem A9000R, it is important that you uninstall any specific multipath software (for example IBM SDD) and install the IBM HAK.

   d. A restart of the host might be needed depending on the multipath software changes requirements.

3. Define and test the data migration volume:

   a. On the XIV storage, remap volumes from the old host to IBM FlashSystem A9000.

   b. On IBM FlashSystem A9000, create the data migration tasks and test them.

4. Activate the data migration tasks on IBM FlashSystem A9000.

5. Define the host in IBM FlashSystem A9000 and bring the host and applications online:

   a. Define the host and iSCSI name on IBM FlashSystem A9000.

   b. Map volumes to the host on IBM FlashSystem A9000.

   c. Verify that IBM FlashSystem A9000 storage is visible.

   d. Depending on the host, a rescan on the host for the volumes on IBM FlashSystem A9000 might be necessary. Enable and start the host applications.

6. Complete the data migration on IBM FlashSystem A9000:

   a. Monitor IBM FlashSystem A9000 migration tasks.

   b. On completion, delete the migration tasks.

Tip: Print these overview steps and refer to them as you perform a migration.

The following steps are specific to the example that is mentioned here, and focus only on the iSCSI-attached volumes in an XIV Storage System (or any storage system) and IBM FlashSystem A9000 (or A9000R) with a Windows host.

8.3.1 Initial connection and preparation

For the initial connection setup, start by connecting IBM FlashSystem A9000 to the XIV system that you are migrating from.

Because the migration and the host attachment are through iSCSI, you must ensure that appropriate firewall ports are opened to allow iSCSI communications.

Important: If the Internet Protocol (IP) network includes firewalls, TCP port 3260 must be open for iSCSI host attachment and migration to work.

This is also a good opportunity for you to update the host operating system (OS) patches and drivers to the latest supported levels for the storage system that you are migrating (the XIV Storage System in our scenario).

Prepare an iSCSI qualified name table

A preferred practice is to document all of the IQNs of all of the systems that are involved, as shown in Table 8-1.

Table 8-1 Example of an iSCSI qualified name (IQN) table

Machine type	iSCSI name
Windows host	iqn.1991-05.com.microsoft:windows-ilplid1
XIV Storage System	iqn.2005-10.com.xivstorage:010133
IBM FlashSystem A9000	iqn.2005-10.com.xivstorage:01322131

On a Windows host, click **Control Panel** → **iSCSI initiator**. You can determine the IQNs from the iSCSI initiator System Properties display.

Using the XIV GUI, you can see the iSCSI port address in the Host Connectivity tab under Hosts and Clusters as shown in Figure 8-3.

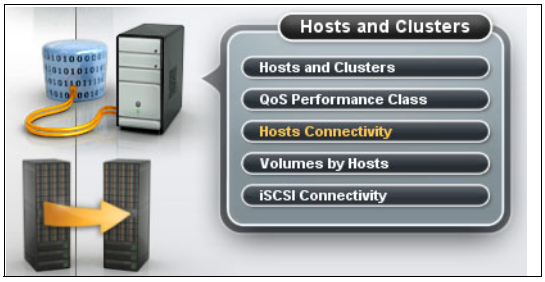


Figure 8-3 iSCSI qualified name in the Host Properties window

Using the Hyper-Scale Manager, you can see the iSCSI port address for the storage system under the **System Properties** → **System Parameters** when a system is selected. An example of this is shown in Figure 8-4.

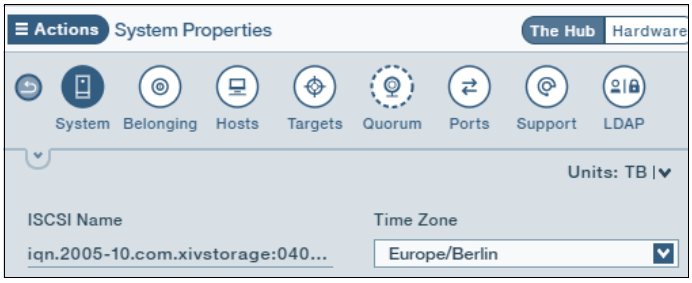


Figure 8-4 iSCSI name in Hyper-Scale Manager

Volumes and host that are defined in the XIV Storage System

The example assumes that the pools and the volumes that you want to migrate exist in the XIV Storage System. This example also assumes that the host that uses the existing volumes in the XIV Storage System.

Define IBM FlashSystem A9000 on the XIV Storage System as host

IBM FlashSystem A9000 must be defined as a Default host on the XIV Storage System:

1. In the XIV Storage System GUI, click **Hosts and Clusters** → **Hosts and Clusters** as shown in Figure 8-5.

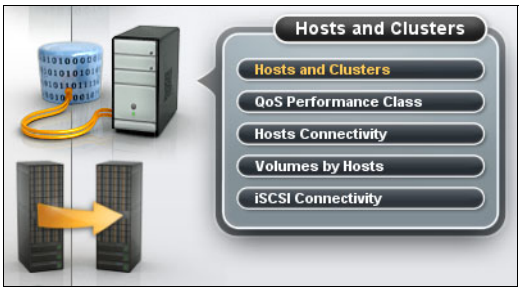


Figure 8-5 Hosts and Clusters in the XIV GUI

2. Select **Add Host** from the top menu bar. Add a default host with the name of the target IBM FlashSystem A9000, as shown in Figure 8-6.

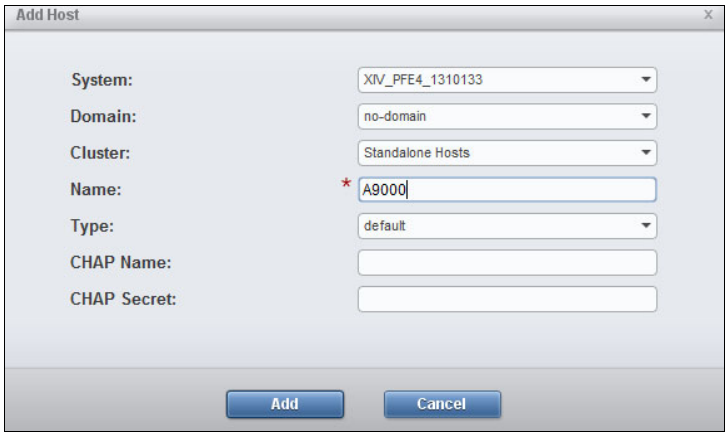


Figure 8-6 Add Host window for the data migration host

3. To add ports, right-click the host as shown in Figure 8-7.

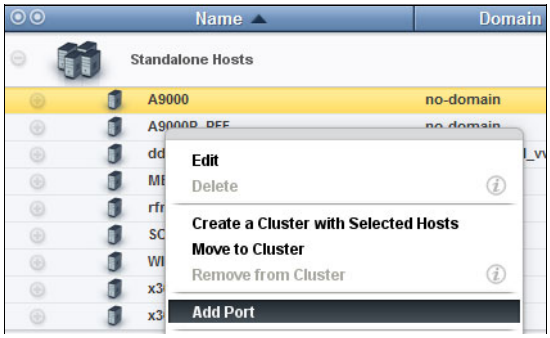


Figure 8-7 Navigating to Add Port

4. On the Add Port window, select **iSCSI** and enter the iSCSI qualified name, as shown in Figure 8-8.

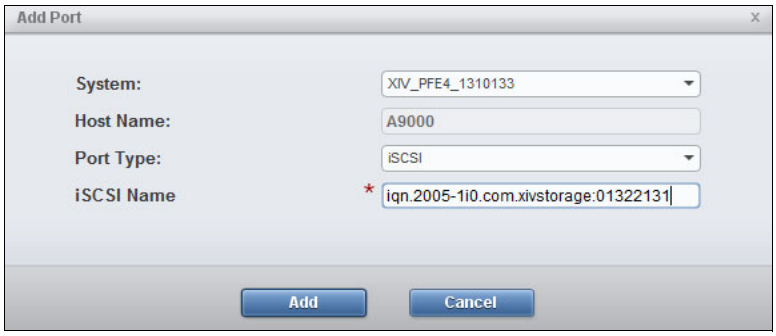


Figure 8-8 Adding the iSCSI port connections for the data migration host

Figure 8-9 shows the iSCSI port listed in Table 8-1 on page 177 added to the host.

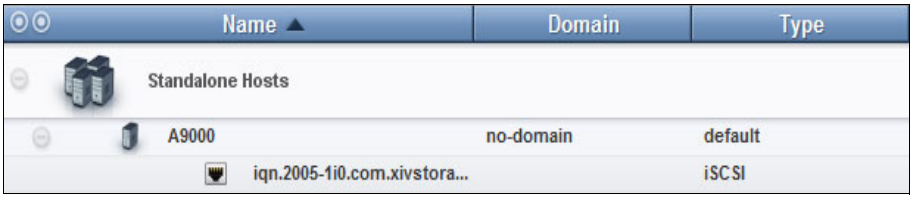


Figure 8-9 Host and associated iSCSI port

Define the XIV being migrated on IBM FlashSystem A9000 as a target

After the physical connectivity is established and IBM FlashSystem A9000 is defined on the XIV Storage System (or any iSCSI-attached storage), you must also define the XIV Storage System on IBM FlashSystem A9000 as a target.

Define the connectivity between IBM FlashSystem A9000 and the XIV Storage System through iSCSI target initiator. Complete these steps:

1. By using the Hyper-Scale Manager GUI, log in to IBM FlashSystem A9000 system with the storage administrator credentials.

2. Click **Actions** → **Targets** → **View/Modify Targets** and click the Plus sign (+) icon to add a target, as shown in Figure 8-10.

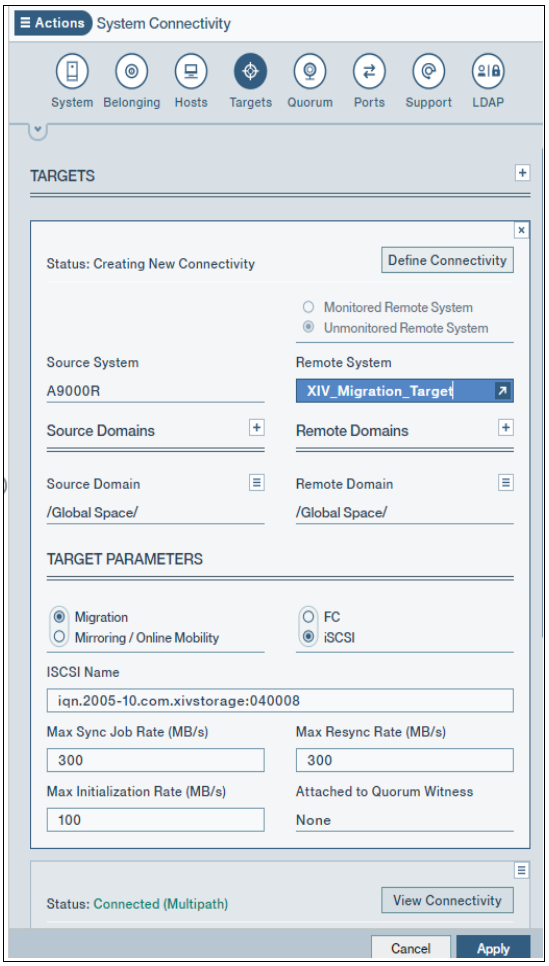


Figure 8-10 Defining a target for migration in IBM FlashSystem A9000

3. Enter the following information and select the following options, as shown in Figure 8-11 on page 181:

Remote System	This field is for the current system, for example, `XIV_Migration_Target`. You must select **Unmonitored Remote System** to be able to enter the name. It is also selected when Migration is chosen under the Target Parameters.
Source Domains	The default is **/Global Space/**, which means *no-domain* unless specified.
Remote Domain	Depending on the previous selection of domain, other options might be available.
Target Type	Two options exist: **Migration** and **Mirroring**. Select **Migration**.
Target Protocol	**Fibre Channel** or **iSCSI**. For this example, **iSCSI** is selected.
iSCSI (Initiator) Name	The iSCSI target that IBM FlashSystem A9000 attaches its volumes from. In this example, XIV is the iSCSI target, so select the corresponding iSCSI name from Table 8-1 on page 177.

Max. Sync Job Rate Depending on the network bandwidth, the default value is set to 300 MBps. Not applicable for migration.

Max. Resync Rate Depending on the network bandwidth, the default value is set to 300 MBps. Not applicable for migration.

Max. Init Rate Depending on the network bandwidth, the default value is set to 100 MBps.

4. After the target is defined, the target appears in the System Connectivity display as shown in Figure 8-11. Select **Define Connectivity** to define the iSCSI connections.

Figure 8-11 Defining target ports in IBM FlashSystem A9000

5. In the window that is displayed, complete the following steps:

   a. Enter the IP addresses for the iSCSI connectivity of XIV to define the connection between the two systems, as shown in Figure 8-12.

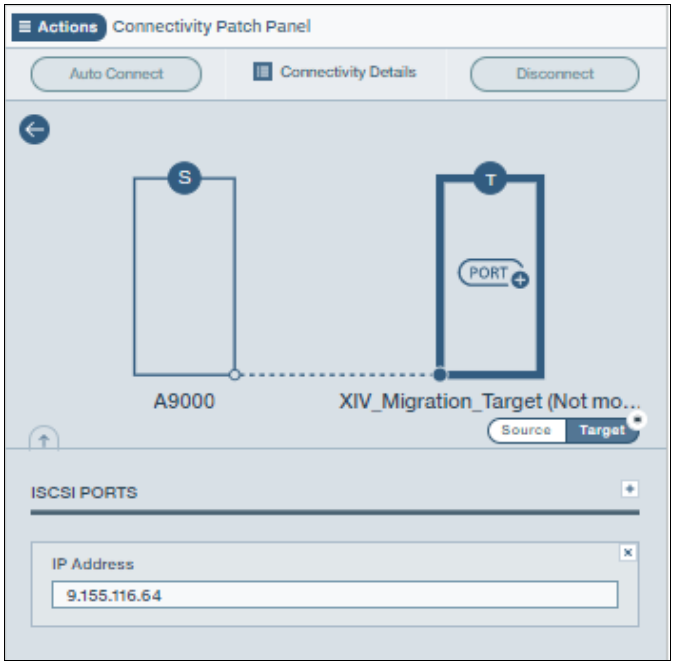


Figure 8-12 Define the IP ports for the target system

   b. Select **Auto Connect** to establish the connections between IBM FlashSystem A9000 and the target system.

   c. If the connection between IBM FlashSystem A9000 and the target system (the XIV Storage System in this example) is successful, the connection is displayed as connected (with a check mark) and you can select **Connectivity Details** to view the connectivity, as shown in Figure 8-13.

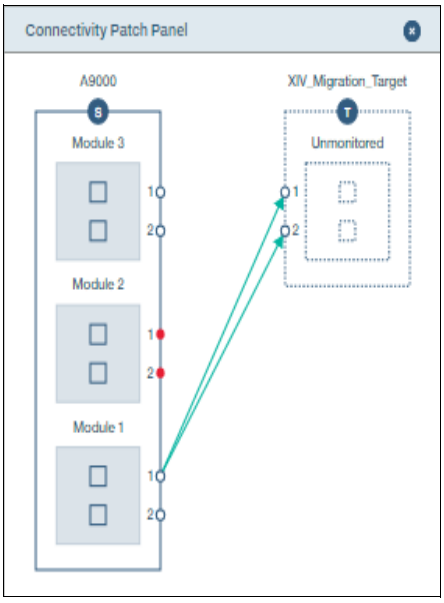


Figure 8-13 Connectivity details

Perform pre-migration tasks for each host that is migrated

Perform the following pre-migration tasks for each host that you are migrating:

1. Back up the volumes that are migrated.
2. Stop all I/O from the host to the LUNs on the storage that is migrated.

Back up the volumes that are migrated

It is a good practice to take a full restorable backup before any data migration activity. Verify that all of the data is restorable from the backup, and that no backup media errors exist.

In addition to a regular backup, a point-in-time copy of the LUNs that are being migrated (if available) is an extra level of protection so that you can perform a rapid rollback, if necessary.

Stop all I/O from the host to the LUNs on the storage that is migrated

Before the actual migration can begin, the application must be quiesced and the file system must be synchronized to ensure that the application data is in a consistent state. Because the host might need to be rebooted several times before the application data becomes available again, the following steps might be required:

1. Set applications to *not* automatically start when the host operating system restarts.
2. Stop file systems from being automatically remounted upon system boot.

Note: In clustered environments, such as Windows or Linux, you might choose to work with only one node until the migration is complete. If so, consider shutting down all other nodes in the cluster.

8.3.2 Define and test data migration volumes

To define and test the data migration volumes, complete these tasks:

1. Remap the volumes to be migrated to the new host in the storage system (XIV in this example).
2. Define migration volumes in the IBM FlashSystem A9000.
3. Test data migration volumes in the IBM FlashSystem A9000.

The volumes being migrated to the IBM FlashSystem A9000 must be allocated through LUN mapping to the IBM FlashSystem A9000. The LUN ID presented to the IBM FlashSystem A9000 must be a decimal value in the range of 0 - 511. However, LUN ID 0 must be avoided.

Note: LUN ID 0 is reserved for in-band communication in IBM FlashSystem A9000 or A9000R. This fact means that the first LUN ID that you normally use is LUN ID 1. SCSI protocol dictates that LUN ID 0 must exist on the target/storage system. All storage systems present a pseudo LUN ID 0 unless a real (actual data LUN) LUN ID 0 is needed.

The Hyper-Scale Manager GUI presents a warning if you attempt to use LUN ID 0, as shown in Figure 8-14.

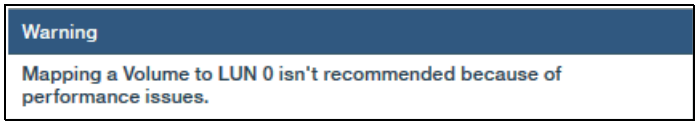


Figure 8-14 LUN 0 is not recommended

Complete the following steps to remap the old volumes to the new host:

Important: Make sure the LUNs that are migrated do not have any mappings to another host, because this can cause data corruption.

1. In the XIV Storage System GUI, log in with the storage administrator credentials.
2. Click **Hosts and Clusters** → **Volumes by Hosts**, select the volumes that you want to migrate, and unmap them from the current host.
3. Click **Hosts and Clusters** → **Hosts and Clusters**.
4. Select the data migration host (FlashSystem A9000) in the XIV Storage System that was defined in “Define the XIV being migrated on IBM FlashSystem A9000 as a target” on page 179.
5. Right-click the selected host, and click **Modify LUN Mapping**.
6. Select the volumes to be mapped (the volumes that were earlier mapped to the actual host), as shown in Figure 8-15, and click **Map**.

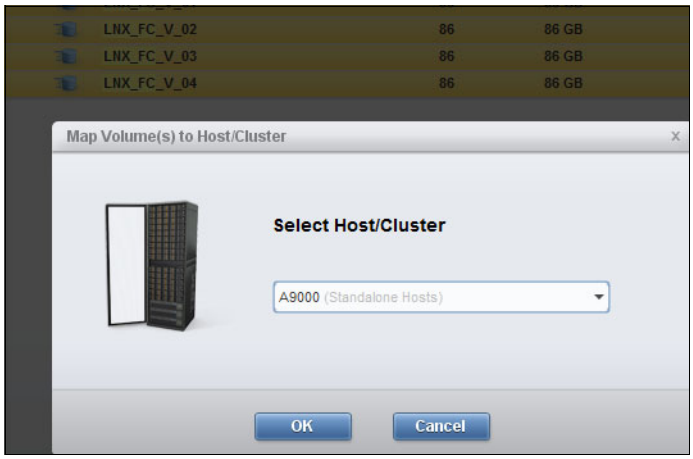


Figure 8-15 Mapping the volumes to IBM FlashSystem A9000

Figure 8-16 shows the selected LUNs mapped to IBM FlashSystem A9000.

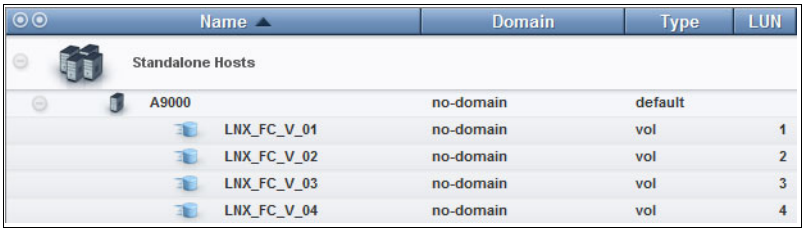


Figure 8-16 LUNs mapped to IBM FlashSystem A9000

Define migration volumes in IBM FlashSystem A9000

IBM FlashSystem A9000 can determine the size of the iSCSI-attached storage volumes and create the corresponding IBM FlashSystem A9000 volumes quickly when the data migration object is defined.

Use this method to help avoid potential problems when you manually calculate the real block size of a volume.

Complete these steps:

1. In the Hyper-Scale Manager GUI, select an existing pool or create a pool to use for the migrated volumes and then select **Actions** → **Migration** → **Migrate remote volume to Pool**, as shown in Figure 8-17.

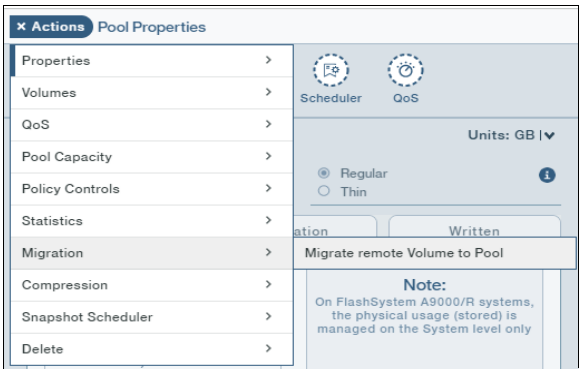


Figure 8-17 Selecting Pool for Migration in IBM FlashSystem A9000

2. Get the LUN IDs of the volumes mapped to host A9000 on the XIV Storage System as shown in Figure 8-18.

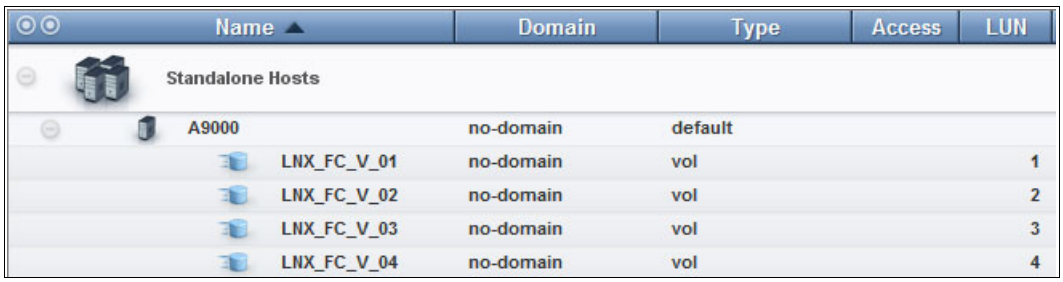


Figure 8-18 XIV Storage System LUN IDs for host A9000

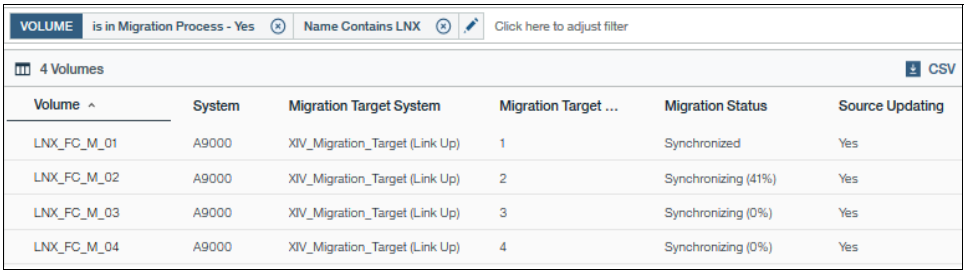
3. Select the settings for the following entries, as shown in Figure 8-19 on page 186:

Target	Select the target system as defined in “Define the XIV being migrated on IBM FlashSystem A9000 as a target” on page 179.
Target LUN	This field needs to match the remote logical unit number (LUN ID), for example, 1, 2, 3, or 4.
Destination Volume	Provide a name for the destination volume, for example, `WIN_ISCSI_M_1`.
Existing Volume	Select this option if the volume has already been created.
Create Volume	Select this option if you want to create the destination volume.
Don’t Update Source	Select this option if you do not want to keep the source volume updated with new host writes.
Update Source	Select this option if you want to update the source volumes when the hosts make changes.
Active	Select this option if you want to activate the migration.
Inactive	Select this option if you do not want to activate the migration right away.

Figure 8-19 Creating migration volumes in IBM FlashSystem A9000

4. Click **Apply**.
5. Repeat steps 2 - 4 for all of the migrated volumes with their respective remote LUNs.

After all of the migrated volumes are created, you can list the migrated volumes by using a migration volume filter, as shown in Figure 8-20.



Volume	System	Migration Target System	Migration Target ...	Migration Status	Source Updating
LNX_FC_M_01	A9000	XIV_Migration_Target (Link Up)	1	Synchronized	Yes
LNX_FC_M_02	A9000	XIV_Migration_Target (Link Up)	2	Synchronizing (41%)	Yes
LNX_FC_M_03	A9000	XIV_Migration_Target (Link Up)	3	Synchronizing (0%)	Yes
LNX_FC_M_04	A9000	XIV_Migration_Target (Link Up)	4	Synchronizing (0%)	Yes

Figure 8-20 Migrated volumes view

Test data migration volumes in IBM FlashSystem A9000

Select the migration volume and then click **Actions** → **Test**.

The test action reads the first block of the volume and can therefore make sure that the system is able to read from the mapped volume. In some active/passive storage systems, it is possible to read the configuration over the passive controller, but not read the data. The test ensures that there is connectivity to the controller that owns the LUN. If any issues exist with the data migration object, the test fails and the issues that are encountered are reported.

8.3.3 Activating data migration on the migrated volumes

If you selected **Inactive** in the Pool Properties window as depicted in Figure 8-19 on page 186 when creating the migration volumes on IBM FlashSystem A9000, you must start the migration process manually. When the data migration is initiated, the data is copied sequentially in the background from the XIV Storage System to IBM FlashSystem A9000.

The host reads and writes data to the new storage system without being aware of the background I/O that is being performed. If a write to a block comes from a host that has not been migrated yet, the source storage system is also updated with this write.

Important: After the data migration is activated, the data migration can be inactivated. However, when the data migration is inactivated, the host is no longer able to read from or write to the source migration volume, and all host I/O stops. *Do not inactivate the migration with host I/O running.*

When migration is finished, select **Disconnect** and not inactivate.

To activate the data migration, complete these steps:

1. Select the Migration volumes by using a volume migration filter.
2. Select **Volumes** → **Actions** → **Migration** → **Change Activation State** → **Activate**.
3. Select **Active**, as shown in Figure 8-21.

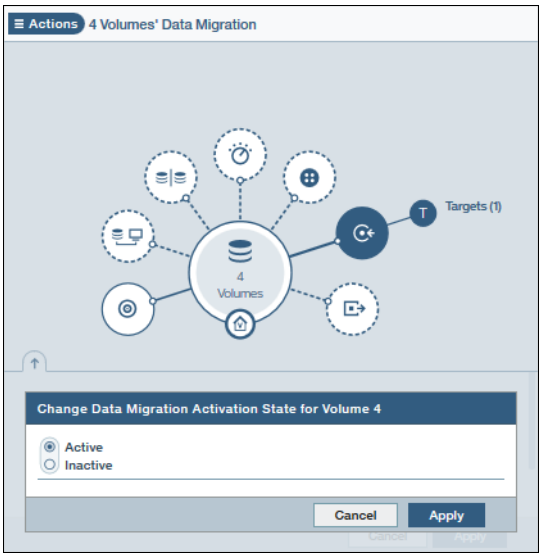


Figure 8-21 Activating migration for the migration volumes

8.3.4 Define the host in IBM FlashSystem A9000 and bring the host online

Before you complete the data migration and allocate the volumes to the host, the host must be defined in IBM FlashSystem A9000. Volumes are then mapped to the hosts or clusters. Upon completion of these steps, the volumes are available to the host for read and write operations. If the host cannot view the volumes, ensure that the HAK is installed and configured, and that no other multipath software is installed on the host.

To attach a host to the volumes that are being migrated, complete these steps:

1. Define the host in IBM FlashSystem A9000.

   Use the **New Item** → **Host** window to create a new host and add ports to the host.

2. Map the LUNs that are being migrated to the host.

   Use the **Volume** → **Actions** → **Mapping** → **View/Modify** window to map volumes to the host.

Note: After the data migration has started, you can use the Hyper-Scale Manager GUI or XCLI to map the migration volumes to the host. When mapping volumes to hosts on the IBM FlashSystem A9000, LUN ID 0 is reserved for IBM FlashSystem A9000 in-band communication.

This configuration means that the first LUN ID that you normally use is LUN ID 1, including boot-from-SAN hosts. You might also choose to use the same LUN IDs as were used on the XIV storage, but this is not mandatory.

For more information about the host attachment, see *IBM FlashSystem A9000, IBM FlashSystem A9000R, and IBM XIV Storage System: Host Attachment and Interoperability*, SG24-8368.

8.3.5 Complete the data migration on IBM FlashSystem A9000

After the volumes and data access are confirmed, you can start the host application and verify the operations. The migration tasks run in the background and allow normal host access to the newly mapped volumes.

Make sure that all of the devices come back online and that the applications can start.

Occasionally, a host might not need to be online during the migration (such as after hours, not in production, or if the migration is completed within the customer change window). It can be offline and be brought back online after the migration is complete.

Note: In clustered environments, the usual recommendation is for only one node of the cluster to be initially brought online after the migration is started, and to have all other nodes stay offline until the migration is complete. After completion, update all other nodes (drivers and HAK) in the same way that the primary node was updated during the initial outage.

Complete the data migration on IBM FlashSystem A9000

To complete the data migration, complete the steps that are described in this section.

Data migration progress

Figure 8-20 on page 186 shows one volume that is migrated, and one volume that is in the process of migrating. The process is sequential, so when one volume completes its migration, the next volume initializes. Figure 8-22 on page 189 shows that all volumes have completed the migration and have the migration status `Synchronized`.

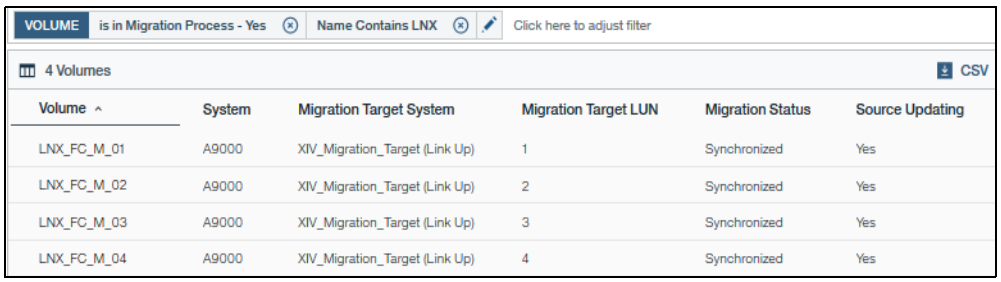


Figure 8-22 Data migration process completed

After all of a volume's data is copied, the data migration achieves synchronization status. After synchronization is achieved, all read requests are served by the new IBM FlashSystem A9000. If source updating was selected, IBM FlashSystem A9000 continues to write data to itself and the storage system that is being migrated from until the data migration is terminated.

Disconnect data migration

After synchronization is achieved, the data migration object can be safely disconnected without host interruption. Verify that the migration is complete before you proceed. Select the volume and verify the migration status as displayed in Figure 8-22.

Important: If this migration is an online migration, do *not* inactivate the data migration before deletion because inactivation causes host I/O to stop, which can cause data corruption.

You can perform this task without host or server interruption if the volume completed synchronization. Select the volumes that you want to disconnect and select **Disconnect**, as shown in Figure 8-23. If the data migration is incomplete, a warning message is displayed.

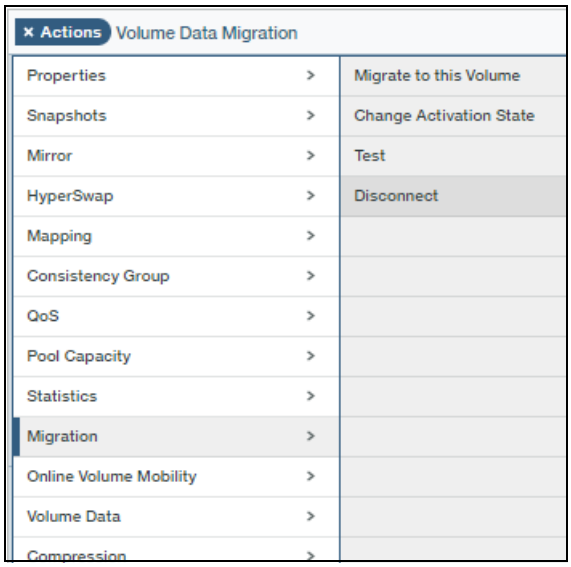


Figure 8-23 Disconnect data migration

Data migration is now completed.

8.3.6 Removing migration connectivity

To remove the FC migration connectivity, complete these steps:

1. Remove migration Target on A9000.
2. Remove the host A9000 used for migration on the XIV Storage System.

Remove migration Target on A9000

Select A9000 in the System view and list the targets in the System Connectivity windows:

1. Select **Actions** → **Targets** → **View/Modify Targets** → **Actions** menu of the migration target `XIV_Migration_Target`, as shown in Figure 8-24.

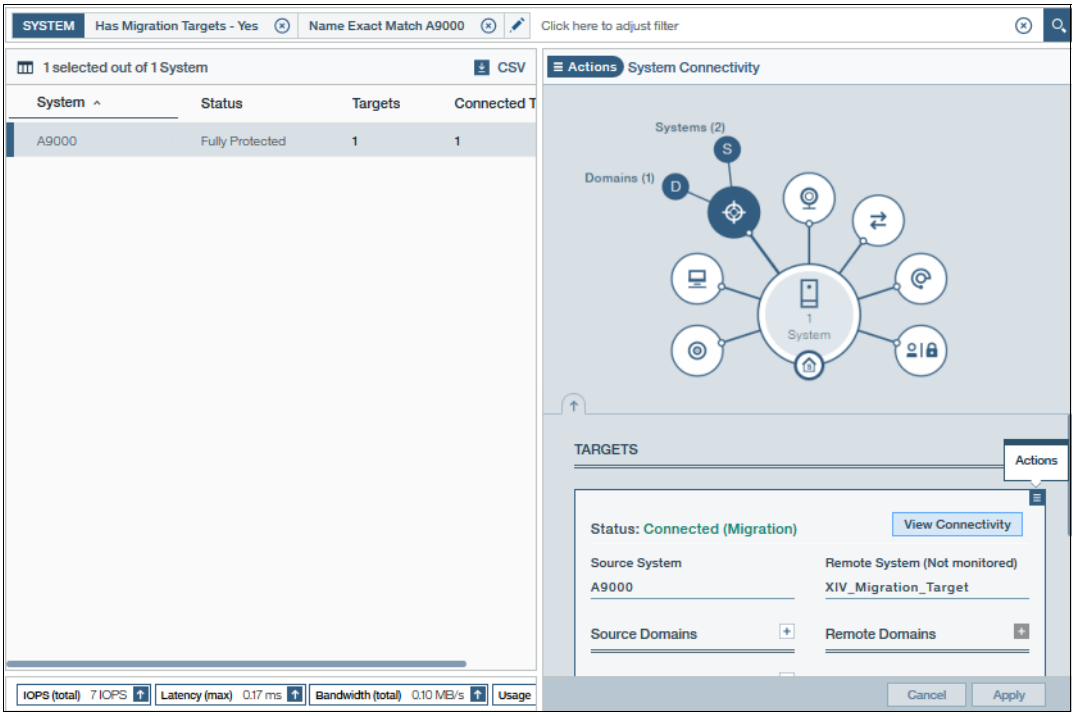


Figure 8-24 Actions menu in the System Connectivity window

2. Select **Disconnect** from the **Actions** menu, as shown in Figure 8-25.

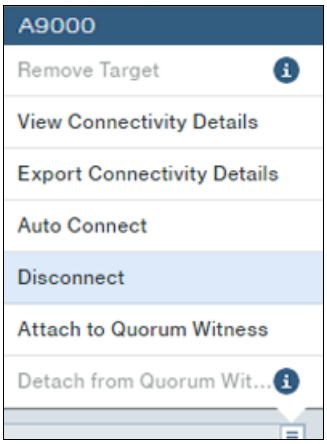


Figure 8-25 Disconnection migration target

3. Using the same menu as shown in Figure 8-25 on page 190, select **Remove Target**, as shown in Figure 8-26.

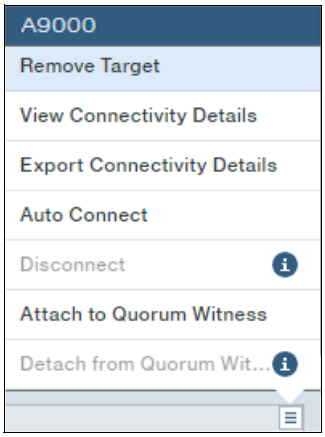


Figure 8-26 Removing migration Target

After successful target removal, the target is not listed anymore in the System Connectivity window.

Remove the host A9000 on the XIV Storage System

To remove the host, complete the following steps:

1. In the XIV GUI, select the volumes mapped to **A9000** and select **Unmap** to unmap the volumes from the host **A9000,** as shown in Figure 8-27.

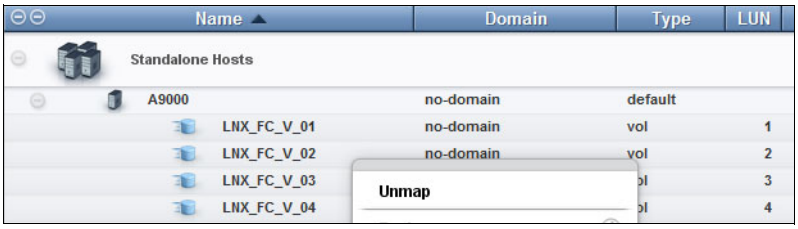


Figure 8-27 Unmap volumes

2. In the XIV GUI, select the host **A9000** and select **Delete** to delete the host used for migration, as shown in Figure 8-28.

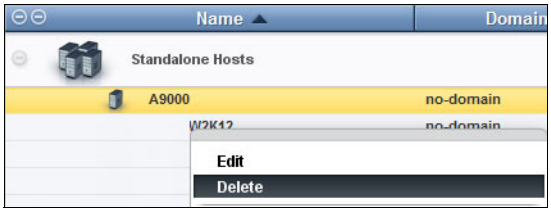


Figure 8-28 Deleting the host used for migration.

The migration connectivity is now deleted.

8.4 Detailed migration steps for a Fibre Channel connection

Note: We chose to migrate from an IBM XIV Storage System to IBM FlashSystem A9000. These systems were used for illustration because they were available for our experimentation. Migration can be performed from any storage system that can attach to a Linux host. The setup details differ based on the storage system.

At a high level, we used the following steps to migrate volumes from an XIV Storage System (or any FC attached storage system) to IBM FlashSystem A9000:

1. Initial connection and preparation:
   a. Establish connection between the XIV Storage System (or any storage system) and IBM FlashSystem A9000.
   b. Prepare a worldwide port name (WWPN) table for all of the systems that are involved.
   c. Assume that the volumes and the host are already defined in the XIV Storage System.
   d. Define IBM FlashSystem A9000 as a host object on the XIV Storage System with the type **Default**.
   e. Define the XIV Storage System in IBM FlashSystem A9000 (as a migration target).
2. Perform pre-migration tasks for each host that is attached to the XIV that will be migrated:
   a. Back up host data.
   b. Stop all I/O from the host to the LUNs on the XIV storage.
   c. Update the HAK to the current version.

      Important: If your migration source is not an XIV, IBM FlashSystem A9000, or IBM FlashSystem A9000R, it is important that you uninstall any specific multipath software (for example IBM SDD) and install the IBM HAK.

   d. A reboot of the host might be needed depending on the multipath software changes requirements.
3. Define and test the data migration volume:
   a. On the XIV storage, remap volumes from the old host to IBM FlashSystem A9000.
   b. On IBM FlashSystem A9000, create the data migration tasks and test them.
4. Activate the data migration tasks on IBM FlashSystem A9000.
5. Define the host in IBM FlashSystem A9000 and bring the host and applications online:
   a. Define the host on IBM FlashSystem A9000.
   b. Map volumes to the host on IBM FlashSystem A9000.
   c. Verify that IBM FlashSystem A9000 storage is visible.
   d. Depending on the host, a rescan on the host for the volumes on IBM FlashSystem A9000 might be necessary. Enable and start the host applications.
6. Complete the data migration on IBM FlashSystem A9000:
   a. Monitor IBM FlashSystem A9000 migration tasks.
   b. On completion, delete the migration tasks.

Tip: Print these overview steps and refer to them as you perform a migration.

The following steps are specific to the example that is mentioned here and focus only on the FC connection between an XIV Storage System (or any storage system) and IBM FlashSystem A9000 (or A9000R).

8.4.1 Initial connection and preparation

For the initial connection setup, start by connecting IBM FlashSystem A9000 to the XIV system that you are migrating from.

Because the migration is through FC, you must ensure a correct storage area network (SAN) configuration between the XIV Storage System and IBM FlashSystem A9000. Also, the data connection between IBM FlashSystem A9000 and the host must be correct.

It is also a good opportunity for you to update the host OS patches and drivers to the latest supported levels for the storage system that you are migrating (the XIV Storage System in our scenario).

Prepare a Fibre Channel WWPN table

A preferred practice is to document all WWPNs of the systems that are involved, as shown in Table 8-2.

Table 8-2 Example of FC ports

System	WWPN	TYPE
IBM FlashSystem A9000	50:01:73:80:56:73.01:13	Initiator
IBM FlashSystem A9000	50:01:73:80:56:73.01:33	Initiator
XIV Storage System	50:01:73:80:9c:4a:01:60	Target
XIV Storage System	50:01:73:80:9c:4a:01:90	Target

Volumes and host that are defined in the XIV Storage System

The example assumes that the pools and the volumes that you want to migrate exist in the XIV Storage System. This example also assumes that the host that uses the volumes exist in the XIV Storage System.

Define IBM FlashSystem A9000 on the XIV Storage System as host

IBM FlashSystem A9000 must be defined as a **Default** host on the XIV Storage System.

Complete the following steps:

1. In the XIV Storage System GUI, click **Hosts and Clusters** → **Hosts and Clusters** (Figure 8-29).

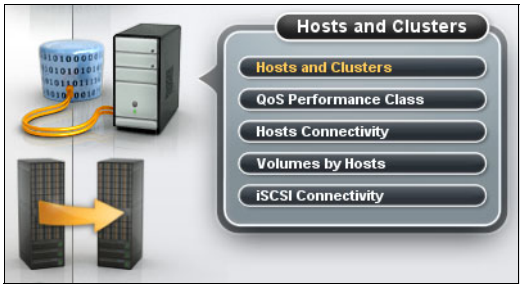


Figure 8-29 Hosts and Clusters in the XIV Storage System GUI

2. Select **Add Host** from the top menu bar. Add a default host (A9000) with the name of the target IBM FlashSystem A9000, as shown in Figure 8-30.

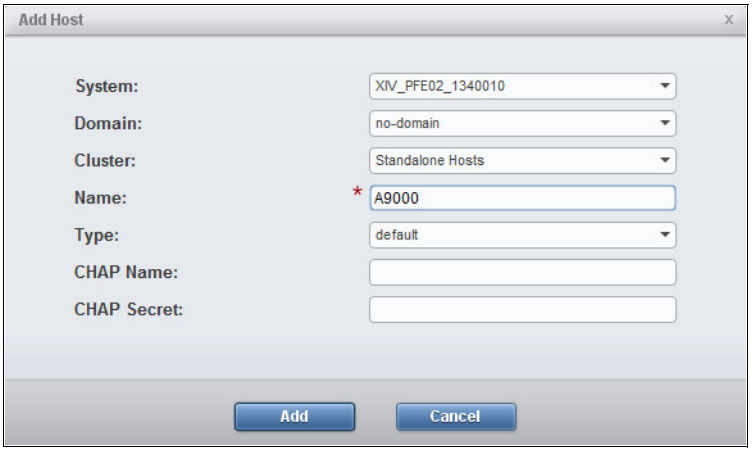


Figure 8-30 Add Host window for the data migration host

3. Right-click the host as shown in Figure 8-31 to add ports.

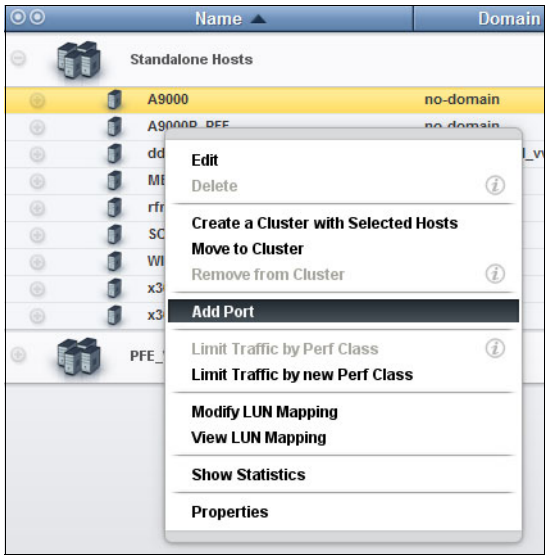


Figure 8-31 Navigating to Add Port

4. On the Add Port window, add the host ports with the WWPNs of the IBM FlashSystem A9000, as shown in Figure 8-32.

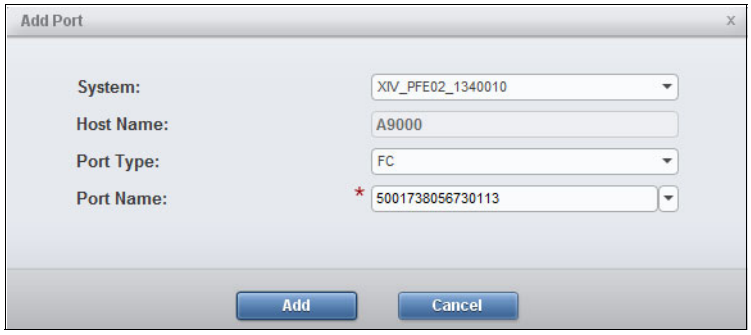


Figure 8-32 Adding the FC port connections for the data migration host

5. Repeat the steps in Figure 8-32 for all IBM FlashSystem A9000 ports listed in Table 8-2 on page 193. Figure 8-33 shows that the two ports of the table have been added to the host.

Figure 8-33 Host and associated FC ports

Define the XIV Storage System on IBM FlashSystem A9000 as a target

After the physical connectivity is established and IBM FlashSystem A9000 is defined on the XIV Storage System (or any FC-attached storage), you must also define the XIV Storage System on IBM FlashSystem A9000 as a target.

Define the connectivity between IBM FlashSystem A9000 and the XIV Storage System through FC. Complete these steps:

1. By using the Hyper-Scale Manager GUI, log in to IBM FlashSystem A9000 system with the storage administrator credentials.
2. Click **Actions** → **Targets** → **View/Modify Targets** and click the Plus sign (+) icon to add a target, as shown in Figure 8-34.

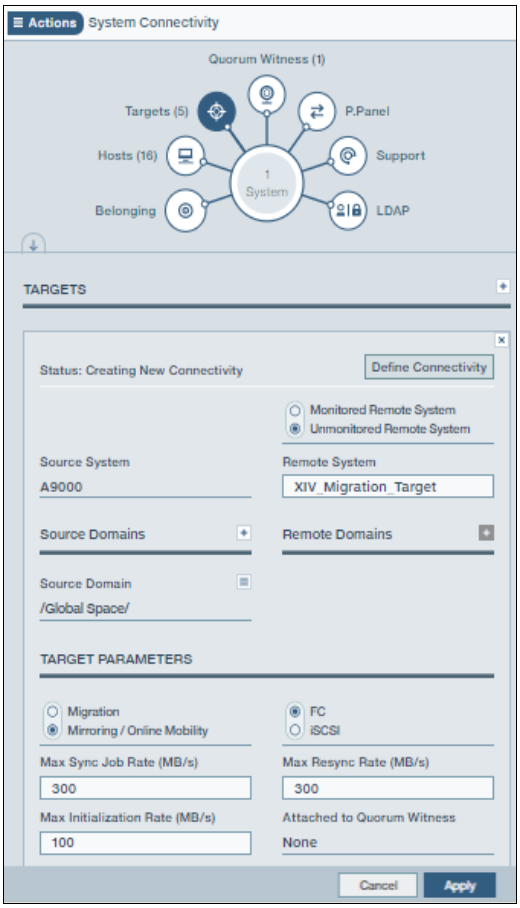


Figure 8-34 Defining a Target in IBM FlashSystem A9000

3. Enter the following information and select the following options, as shown in Figure 8-34:

Remote System	This field is for the current system, for example, `XIV_Migration_Target`. You must select **Unmonitored Remote System** to be able to enter the name.
Source Domains	The default is **/Global Space/**, which means *no-domain* unless specified.
Remote Domain	Depending on the previous selection of domain, other options might be available.
Target Type	Two options exist: **Migration** and **Mirroring**. Select **Migration**.
Target Protocol	**FC** or **iSCSI**. For this example, **FC** is selected.
Max. Sync Job Rate	Depending on the network bandwidth, the default value is set to 300 MBps. Not applicable for migration.

Max. Resync Rate Depending on the network bandwidth, the default value is set to 300 MBps. Not applicable for migration.

Max. Init Rate Depending on the network bandwidth, the default value is set to 100 MBps.

4. After the target is defined, the target appears in the System Connectivity window, as shown in Figure 8-35. Select **Define Connectivity** to define the FC connections.

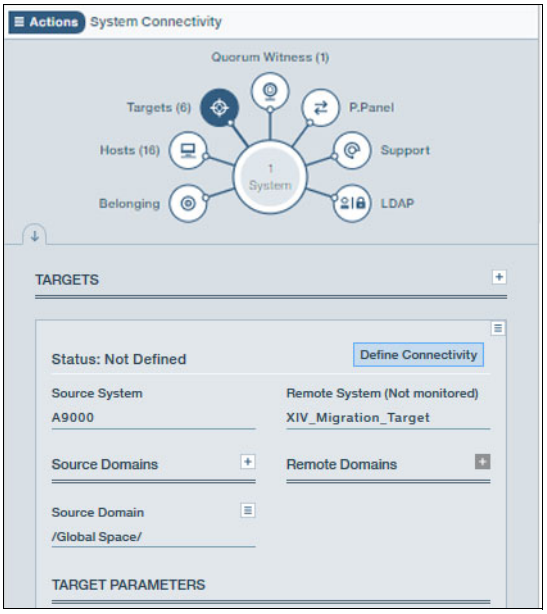


Figure 8-35 Defining connectivity in IBM FlashSystem A9000

5. In the window that is displayed, complete the following steps:
   a. Enter the WWPN as listed in Table Table 8-2 on page 193 of the XIV Storage System to define the connection between the two systems, as shown in Figure 8-36.

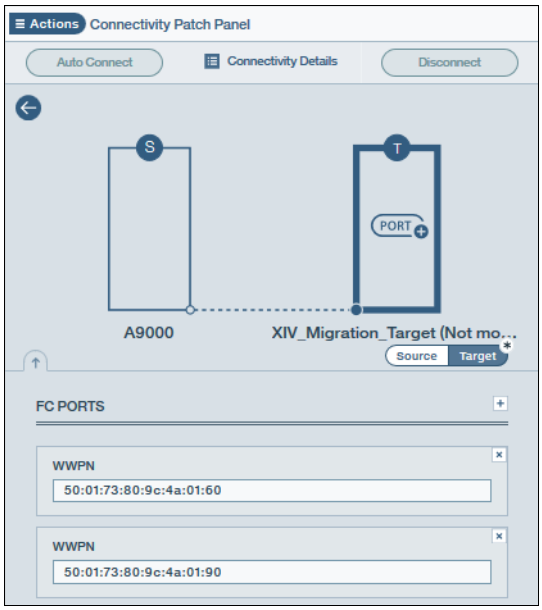


Figure 8-36 Define the FC ports for the target system

b. Select **Auto Connect** to establish the connections between IBM FlashSystem A9000 and the target system.

c. If the connection between IBM FlashSystem A9000 and the target system (the XIV Storage System) is successful, the connection is displayed as connected (with a check mark). You can select **Connectivity Details** to view the connectivity, as shown in Figure 8-37.

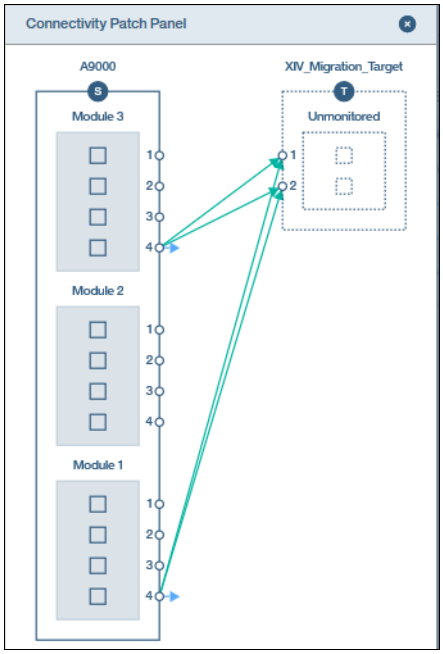


Figure 8-37 Migration connectivity details

8.4.2 Perform pre-migration tasks for each host that is migrated

The following pre-migration tasks are preferred practices to be performed for each host that you are migrating:

1. Back up the volumes that are migrated.
2. Stop all I/O from the host to the LUNs on the storage that is migrated.

Back up the volumes that are migrated

Its good practice to take a full restorable backup before any data migration activity. Verify that all of the data is restorable from the backup and that no backup media errors exist.

In addition to a regular backup, a point-in-time copy of the LUNs that are being migrated (if available) is an extra level of protection so that you can perform a rapid rollback, if necessary.

Stop all I/O from the host to the LUNs on the storage that is migrated

Before the actual migration can begin, the application must be quiesced and the file system must be synchronized to ensure that the application data is in a consistent state. Because the host might need to be rebooted several times before the application data becomes available again, the following steps might be required:

1. Set applications to *not* automatically start when the host operating system restarts.
2. Stop file systems from being automatically remounted on boot.

Note: In clustered environments, such as Windows or Linux, you might choose to work with only one node until the migration is complete. If so, consider shutting down all other nodes in the cluster.

8.4.3 Define and test data migration volumes

To define and test the data migration volumes, complete these tasks:

1. Remapping old volumes to the new host in the XIV Storage System.
2. Define migration volumes in IBM FlashSystem A9000.
3. Test data migration volumes in IBM FlashSystem A9000R.

Remapping old volumes to the new host in the XIV Storage System

The volumes being migrated to the IBM FlashSystem A9000 must be allocated through LUN mapping to the IBM FlashSystem A9000. The LUN ID presented to the IBM FlashSystem A9000 must be a decimal value in the range of 0 - 511. However, LUN ID 0 must be avoided.

Note: LUN ID 0 is reserved for in-band communication in IBM FlashSystem A9000 or A9000R. This requirement means that the first LUN ID that you normally use is LUN ID 1. SCSI protocol dictates that LUN ID 0 must exist on the target/storage system. All storage systems present a pseudo LUN ID 0 unless a real (actual data LUN) LUN ID 0 is needed.

The Hyper-Scale Manager GUI presents a warning if you attempt to use LUN ID 0, as shown in Figure 8-38.

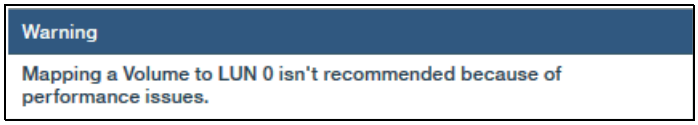


Figure 8-38 LUN 0 is not recommended

Complete the following steps to remap the old volumes to the new host:

Important: Make sure the LUNs that are going to be migrated do not have any mappings to an old host because this can cause data corruption.

1. In the XIV Storage System GUI, log in with the storage administrator credentials.
2. Click **Hosts and Clusters** → **Volumes by Hosts**, select the volumes that you want to migrate, and unmap them from the current host.
3. Click **Hosts and Clusters** → **Hosts and Clusters**.
4. Select the data migration host in the XIV Storage System that was defined in “Define the XIV Storage System on IBM FlashSystem A9000 as a target” on page 195.
5. Right-click the selected host, and click **Modify LUN Mapping**.

6. Select the volumes to be mapped (the volumes that were earlier mapped to the actual host), as shown in Figure 8-39, and click **Map**.

Figure 8-39 LUN mapping to the data migration host

Figure 8-40 shows the selected LUNs mapped to IBM FlashSystem A9000.

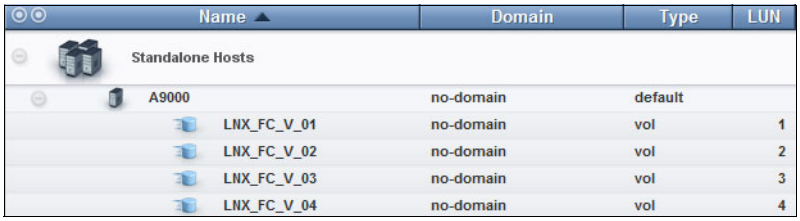


Figure 8-40 LUNs mapped to IBM FlashSystem A9000

Define migration volumes in IBM FlashSystem A9000

IBM FlashSystem A9000 can determine the size of the XIV Storage System (or any iSCSI-attached storage) volumes and create the corresponding IBM FlashSystem A9000 volumes quickly when the data migration object is defined. Use this method to help avoid potential problems when you manually calculate the real block size of a volume.

Complete these steps:

1. In the GUI, select the pool to use for the migrated volumes and then select **Actions** → **Migration** → **Migrate remote Volume to Pool,** as shown in Figure 8-41.

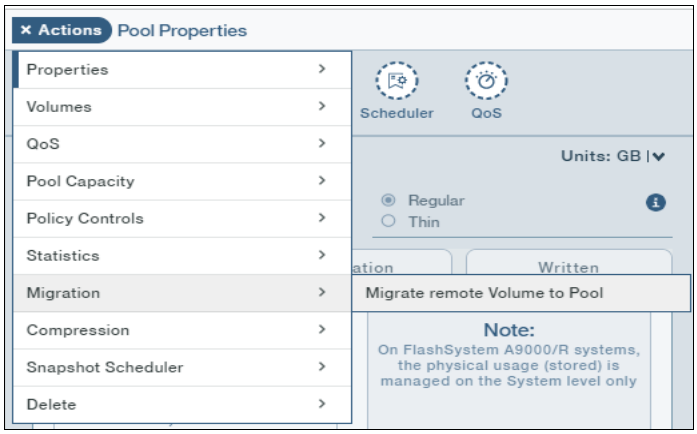


Figure 8-41 Selecting Migration in IBM FlashSystem A9000

2. Get the LUN IDs of the volumes mapped to host A9000 on the XIV Storage System as shown in Figure 8-42.

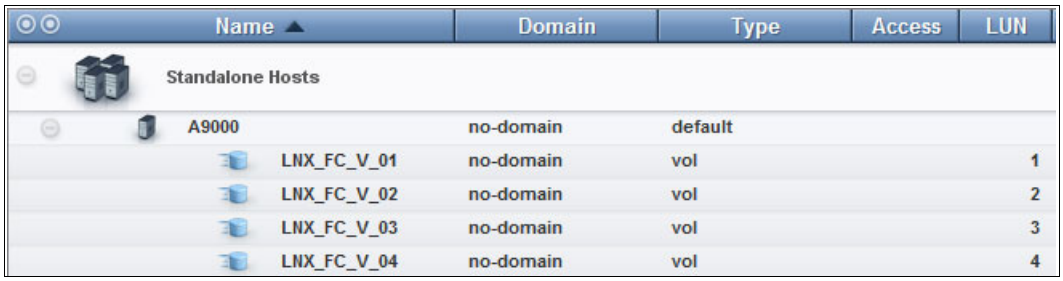


Figure 8-42 XIV Storage System LUN IDs for host A9000

3. Select the settings for the following entries, as shown in Figure 8-43:

Target Select the target system that was defined earlier in the XIV Storage System.

Target LUN This field needs to match the remote logical unit number (LUN ID), for example, 1, 2, 3, and 4.

Destination Volume Provide a name for the destination volume, for example, `LNX_FC_M01`.

Create Volume Select the check box if you want to create destination volumes.

Update Source Select this option if you want to update the source volumes when the hosts make changes.

Active Select this box if you want to activate the migration.

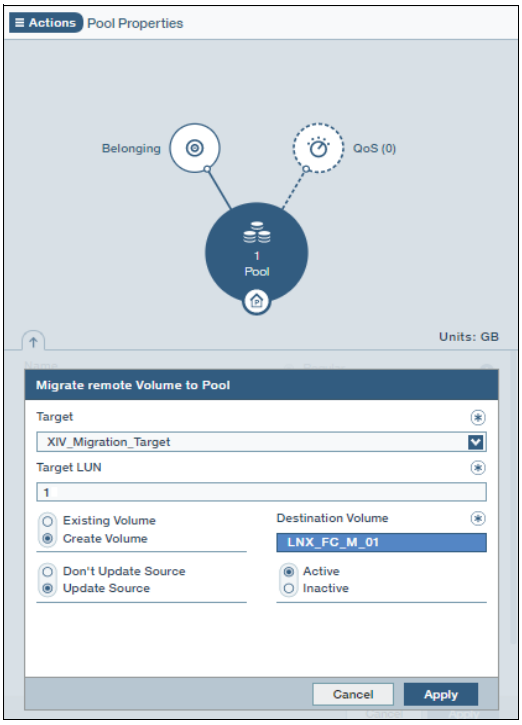


Figure 8-43 Creating migration volumes in IBM FlashSystem A9000

4. Click **Apply**.

5. Repeat steps 2 - 4 for all of the migrated volumes with their respective remote LUNs.

After all of the migrated volumes are created, you can list the migrated volumes by using a migration volume filter, as shown in Figure 8-44.

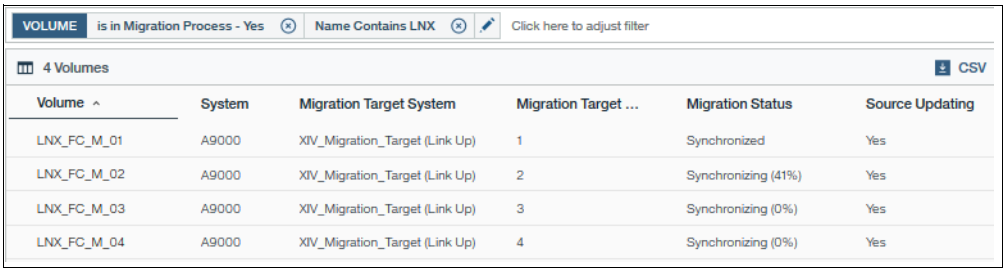


Figure 8-44 Migrated volumes view

Test data migration volumes in IBM FlashSystem A9000R

Select the migration volumes and then click **Actions** → **Test**.

The test action reads the first block of the volume and can therefore make sure that the system is able to read from the mapped volume. In some active and passive storage systems, it is possible to read the configuration over the passive controller, but not read the data. The test ensures that there is connectivity to the controller that owns the LUN. If any issues exist with the data migration object, the test fails and the issues that are encountered are reported.

8.4.4 Activating data migration on the migrated volumes

If you selected **Inactive** in the Pool Properties window when creating the migration volumes on IBM FlashSystem A9000R, you must start the migration process manually. When the data migration is initiated, the data is copied sequentially in the background from the XIV Storage System volume to IBM FlashSystem A9000.

The host reads and writes data to the new storage system without being aware of the background I/O that is being performed. If a write to a block comes from a host that has not been migrated yet, the source storage system is also updated with this write.

Important: After the data migration is activated, the data migration can be inactivated. However, when the data migration is inactivated, the host is no longer able to read or write to the source migration volume and all host I/O stops. *Do not inactivate the migration with host I/O running.*

When migration is finished, select **Disconnect** and not inactivate.

To activate the data migration, complete these steps:

1. Select the Migration volumes by using a volume migration filter.
2. Select **Volumes** → **Actions** → **Migration** → **Change Activation State** → **Activate**.

3. Select **Active** and click **Apply**, as shown in Figure 8-45.

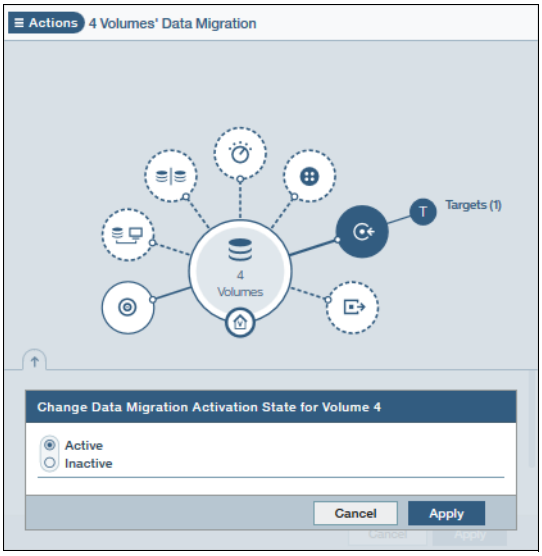


Figure 8-45 Activating migration for the migration volumes

8.4.5 Define the host in IBM FlashSystem A9000 and bring the host online

Before you complete the data migration and map the volumes to the host, the host must be defined in IBM FlashSystem A9000. Volumes are then mapped to the hosts or clusters.

Upon the completion of these steps, the volumes are available to the host for read and write operations. If the host cannot view the volumes, ensure that the HAK is installed and configured and no other multipath software is installed on the host.

To attach a host to the volumes that are being migrated, complete these steps:

1. Define the host to IBM FlashSystem A9000R.

   Use the **New Item** → **Host** window to create a new host and add the ports to the host.

2. Map the LUNs that are being migrated to the host.

   Use the **Volume** → **Actions** → **Mapping** → **View/Modify** window to map volumes to the host.

For more information about the host attachment, see *IBM FlashSystem A9000, IBM FlashSystem A9000R, and IBM XIV Storage System: Host Attachment and Interoperability*, SG24-8368.

8.4.6 Complete the data migration on IBM FlashSystem A9000

After the volumes and data access are confirmed, you can start the host application and verify the operations. The migration tasks run in the background and allow normal host access to the newly mapped volumes.

Make sure that all of the devices come back online and that the applications can start.

Occasionally, a host might not need to be online during the migration (such as after hours, not in production, or if the migration is completed within the customer change window). It can be offline and be brought back online after the migration is complete.

Note: In clustered environments, the usual recommendation is for only one node of the cluster to be initially brought online after the migration is started, and to have all other nodes stay offline until the migration is complete.

After completion, update all other nodes (driver, host attachment package, and so on) in the same way that the primary node was updated during the initial outage.

Complete the data migration on IBM FlashSystem A9000

To complete the data migration, complete the steps that are described in this section.

Data migration progress

Figure 8-44 on page 202 shows one volume that has been migrated, and one volume being migrated. The process is sequential so that when one volume completes its migration, the next volume initializes.

Figure 8-46 shows that all volumes have been migrated and have the migration status `Synchronized`.

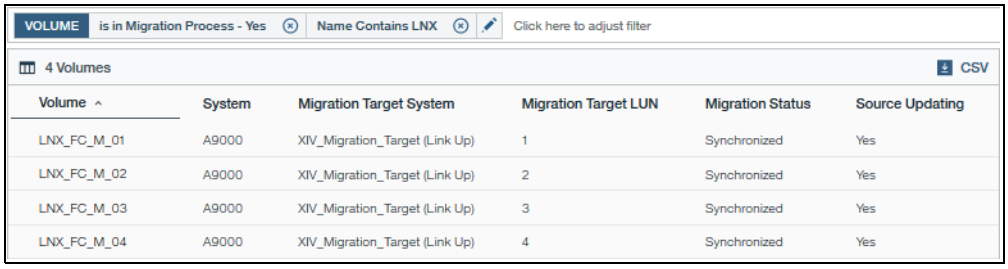


Figure 8-46 Data migration process completed

After all of a volume's data is copied, the data migration achieves synchronization status. After synchronization is achieved, all read requests are served by the new IBM FlashSystem A9000. If source updating was selected, IBM FlashSystem A9000R continues to write data to itself and the storage system that is being migrated until the data migration is terminated.

Disconnect data migration

After synchronization is achieved, the data migration object can be safely disconnected without host interruption. Verify that the migration is complete before you proceed. Select the volume and verify the migration status as shown in Figure 8-46.

Important: If this migration is an online migration, do *not* inactivate the data migration before deletion because inactivation causes host I/O to stop, which can cause data corruption.

You can perform this task without host/server interruption if the volume completed synchronization. Select the volumes that you want to disconnect and select the **Disconnect** action, as shown in Figure 8-47 on page 205. If the data migration is incomplete, a warning message appears.

Data migration is now completed.

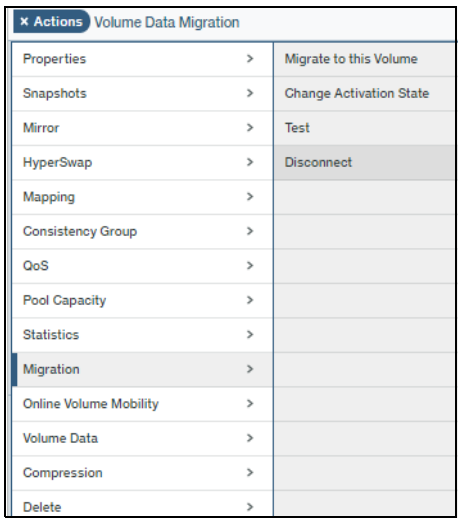


Figure 8-47 Disconnect data migration

8.4.7 Removing Migration Connectivity

To remove the FC migration connectivity, complete these steps:

1. Remove migration Target on A9000.
2. Remove the host A9000 used for migration on the XIV Storage System.

Remove migration Target on A9000

Select A9000 in the System view and list the targets in the System Connectivity windows:

1. Select **Actions** → **Targets** → **View/Modify Targets** → **Actions** menu of the migration target `XIV_Migration_Target`, as shown in Figure 8-48.

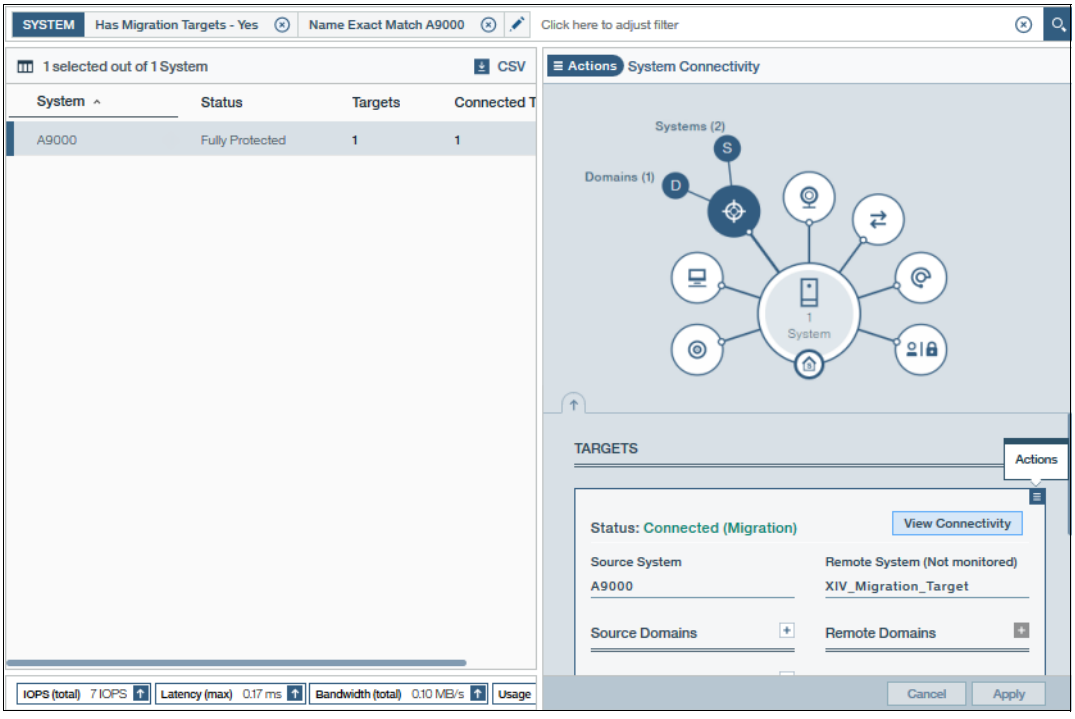


Figure 8-48 Actions menu in the System Connectivity window

2. Select **Disconnect** from the **Actions** menu, as shown in Figure 8-49.

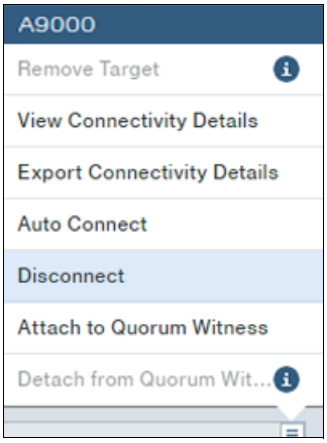


Figure 8-49 Disconnection migration target

3. Using the same action menu as shown in Figure 8-48 on page 205, select **Remove Target**, as shown in Figure 8-50.

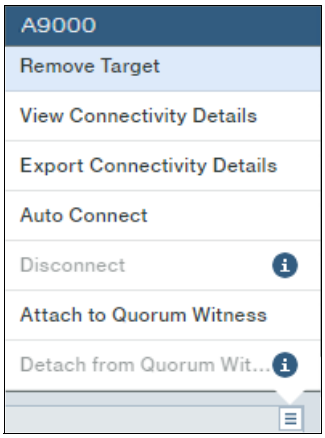


Figure 8-50 Removing migration Target

After successful target removal, the target is not listed anymore in the System Connectivity window.

Remove the host A9000 on the XIV Storage System

The steps to remove the migration connectivity on A9000 for an FC connection are the same steps as for an iSCSI connection as described in 8.3.6, “Removing migration connectivity” on page 190.

Related publications

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

IBM Redbooks

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

- *IBM FlashSystem A9000 and IBM FlashSystem A9000R Architecture and Implementation*, SG24-8345
- *IBM FlashSystem A9000, IBM FlashSystem A9000R, and IBM XIV Storage System: Host Attachment and Interoperability*, SG24-8368
- *IBM HyperSwap and Multi-site HA/DR solution for IBM FlashSystem A9000 and A9000R*, REDP-5434
- *IBM Hyper-Scale Manager for IBM Spectrum Accelerate Family: IBM XIV, IBM FlashSystem A9000 and A9000R, and IBM Spectrum Accelerate*, SG24-8376
- *Using the IBM Spectrum Accelerate Family in VMware Environments: IBM XIV, IBM FlashSystem A9000 and IBM FlashSystem A9000R, and IBM Spectrum Accelerate*, REDP-5425

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

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

Other publications and Online resources

- IBM FlashSystem A9000 on IBM Knowledge Center:

  `http://www.ibm.com/support/knowledgecenter/STJKMM`

  The following publications are at this website:

  - *IBM FlashSystem A9000 Command-Line Interface (CLI) Reference Guide*, SC27-8559
  - *IBM FlashSystem A9000 Models 9836-415, 9838-415, 9836-425, and 9838-425 Deployment Guide,* GC27-8564
  - *IBM FlashSystem A9000 Product Overview,* GC27-8583-00
- IBM FlashSystem A9000R on IBM Knowledge Center:

  `http://www.ibm.com/support/knowledgecenter/STJKN5`

  The following publications are at this website:

  - *IBM FlashSystem A9000R Command-Line Interface (CLI) Reference Guide*, SC27-8711
  - *IBM FlashSystem A9000R Models 9835-415, 9837-415, 9835-425, and 9837-425 Deployment Guide,* GC27-8565

- *IBM FlashSystem A9000R Product Overview,* GC27-8558-00

- IBM FlashSystem A9000 product page:

  http://www.ibm.com/systems/storage/flash/a9000

- IBM FlashSystem A9000R product page:

  https://www.ibm.com/systems/storage/flash/a9000r/

- IBM Fix Central:

  http://www.ibm.com/support/fixcentral/

- For the latest hardware and software requirements, visit the IBM System Storage Interoperation Center (SSIC) website:

  http://www.ibm.com/systems/support/storage/ssic/interoperability.wss

- IBM Offering Information page (announcement letters and sales manuals):

  http://www.ibm.com/common/ssi/index.wss?request_locale=en

  On this page, enter A9000, select the information type, and click **Search**. On the next page, narrow your search results by geography and language.

Help from IBM

IBM Support and downloads

http://www.ibm.com/support

IBM Global Services

http://www.ibm.com/services

REDP-5401-03

ISBN 0738457434

Printed in U.S.A.