

IBM System Storage DS5000 Series Hardware Guide

Introduction to IBM System Storage
DS5000 series

Remote Support Manager (RSM)
Configuration

Configuration, Maintenance,
and Troubleshooting



Sangam Racherla
Matus Butora
Antonio Dell'Apa
Mario Ganem
Corne Lottering
Libor Miklas
Hrvoje Stanilovic
Alexander Watson

Redbooks



International Technical Support Organization

IBM System Storage DS5000 Series Hardware Guide

February 2012

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

First Edition (February 2012)

This edition applies to:

- ▶ IBM System Storage® DS5000 series running Firmware V7.77.
- ▶ IBM System Storage DS Storage Manager V10.77.

This document was created or updated on October 3, 2012.

© Copyright International Business Machines Corporation 2012. All rights reserved.

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

Contents

Notices	ix
Trademarks	x
 Preface	 xi
The team who wrote this book	xi
Now you can become a published author, too!	xiv
Comments welcome	xiv
Stay connected to IBM Redbooks	xiv
 Chapter 1. Introduction to IBM System Storage DS5000 series	 1
1.1 Positioning the DS5000 series	2
1.2 IBM Midrange System Storage DS5000 series models	3
1.3 IBM Midrange System Storage DS5000 expansion enclosure	6
1.4 IBM System Storage DS Storage Manager software	7
1.5 IBM Midrange System Storage DS5000 hard disk drives	8
1.6 iSCSI basics	11
1.7 Fibre Channel direct/switch basics	12
1.8 New features with controller firmware version 7.77.	14
1.8.1 Full Disk Encryption capable disk drive modules (DDM)	14
1.8.2 Solid State Drive (SSD) module	15
1.8.3 600 GB FC disk drive module	15
1.8.4 900 GB SAS disk drives	15
1.8.5 2 TB SATA enhanced disk drive module	16
1.8.6 3 TB SATA enhanced disk drive module	16
1.8.7 10 Gbps iSCSI host interface	16
1.8.8 Premium features activation	17
1.8.9 T10 Protection Information	17
1.8.10 8 Gbps FC host interface	17
1.8.11 64 GB cache upgrade for the DS5100 and DS5300	17
1.8.12 Apple Macintosh OS X	18
1.9 More information	18
 Chapter 2. IBM System Storage DS5000 hardware	 19
2.1 DS5100 and DS5300 storage subsystems	20
2.1.1 DS5000 series product comparison	22
2.1.2 DS5100 and DS5300 controller architecture	23
2.1.3 DS5000 storage subsystem chassis design	32
2.1.4 DS5000 storage subsystem front view	32
2.1.5 Interconnect module and battery packs	34
2.1.6 DS5000 storage subsystem rear view	37
2.1.7 DS5000 storage subsystem LED indicator lights	38
2.1.8 DS5000 storage subsystem host-side connections	47
2.1.9 DS5000 storage subsystem drive-side connections	52
2.1.10 DS5000 storage subsystem additional connections	54
2.1.11 DS5000 component locations	55
2.2 DS5020 storage subsystem	57
2.2.1 DS5020 controller architecture	59
2.2.2 DS5020 components	61
2.2.3 DS5020 Storage Subsystem front view	65

2.2.4	DS5020 storage subsystem rear view	66
2.2.5	DS5020 storage subsystem LED indicator lights	69
2.2.6	DS5020 storage subsystem host-side connections	75
2.2.7	DS5020 storage subsystem drive-side connections	76
2.2.8	DS5020 storage subsystem additional connections	77
2.2.9	DS5020 Component Locations	78
2.3	DS5000 series physical specifications	80
2.4	DS5000 supported operating systems	82
2.5	DS5000 storage subsystem disk enclosures	83
2.5.1	EXP5000 and EXP520 Storage Expansion Unit	84
2.5.2	EXP5060 Storage Expansion Unit	89
2.6	DS5000 storage subsystem drive-side cabling	101
2.6.1	EXP5000 storage expansion enclosure cabling rules	101
2.6.2	EXP5060 storage expansion enclosure cabling rules	105
2.6.3	Non-trunked EXP5060 only	107
2.6.4	DS5020 storage subsystem drive-side cabling	112
Chapter 3.	DS5000 storage subsystem configuration	117
3.1	IBM System Storage DS Storage Manager software	118
3.1.1	Storage subsystem management methods	121
3.1.2	Storage Manager client	124
3.1.3	Event Monitor service	127
3.1.4	Storage Manager utilities	128
3.2	Installing IBM System Storage DS Storage Manager	128
3.2.1	Installing DS Storage Manager software on Windows 2008	129
3.2.2	HBA and Multipath device drivers	133
3.3	Preparing the DS5000 storage subsystem	137
3.3.1	Physical installation	138
3.3.2	Powering on the storage subsystem	138
3.3.3	Configuring IP addresses of the controllers	139
3.3.4	Using and configuring the DS Storage Manager client	146
3.3.5	Updating the controller microcode	154
3.4	Step-by-step configuration	155
3.4.1	Configuration planning	155
3.4.2	Enabling the premium features	156
3.5	Methods of configuring	160
3.5.1	Automatic configuration	160
3.5.2	Manual configuration	166
3.5.3	Defining hot spare drives	166
3.5.4	Creating arrays and logical drives	172
3.5.5	Configuring storage partitioning	181
3.5.6	Configuring mapped drives from Windows	199
3.5.7	Monitoring and alerting	202
3.5.8	Saving the configuration	207
3.6	Advanced functions	213
3.6.1	Expanding arrays	213
3.6.2	Changing the RAID array level	215
3.6.3	Unconfiguring a storage subsystem and arrays	216
3.6.4	Performing advanced functions on logical drives (LUNs)	217
3.6.5	Modification priority	223
3.6.6	Controller ownership	226
3.6.7	Cache parameters	228
3.6.8	Logical drive	229

3.6.9 Storage subsystem Cache settings	231
3.6.10 Media scan	232
3.6.11 Failover alert delay	234
3.7 Removing logical drives and arrays	235
3.7.1 Deleting logical drives	236
3.7.2 Defragmenting an array	239
3.7.3 Deleting an array	240
3.7.4 Secure erase	245
3.8 Storage Manager Advanced Monitoring features	249
3.8.1 Persistent reservations	249
3.8.2 Automatic firmware synchronization	250
Chapter 4. Full Disk Encryption with Full Disk Encryption drives	253
4.1 The need for encryption	254
4.1.1 Encryption method used	254
4.2 Disk Security components	256
4.2.1 DS5000 Disk Encryption Manager	256
4.2.2 Full Data Encryption (FDE) drives	257
4.2.3 Premium feature license	257
4.2.4 Security key management	257
4.2.5 Keys	259
4.2.6 Security key identifier	261
4.2.7 Passwords	262
4.3 Setting up and enabling a secure disk	262
4.3.1 FDE and premium feature check	263
4.3.2 Secure key creation	264
4.3.3 Enable Disk Security on array	267
4.4 Additional secure disk functions	268
4.4.1 Changing the security key	268
4.4.2 Save security key file	271
4.4.3 Secure erase	272
4.4.4 FDE drive status	273
4.4.5 Hot spare drive	274
4.5 Migrating secure disk arrays	274
4.5.1 Planning checklist	274
4.5.2 Export the array	275
4.6 Import secure drive array	278
4.6.1 Unlock drives	279
4.6.2 Import array	281
Chapter 5. Advanced maintenance, troubleshooting, and diagnostics	285
5.1 Upgrades and maintenance	286
5.1.1 Displaying installed firmware versions	286
5.1.2 Obtaining updates	288
5.1.3 Planning for upgrades	290
5.1.4 Updating the DS5000 storage subsystem host software	291
5.1.5 Updating controller firmware	292
5.1.6 Updating the ESM board firmware	299
5.1.7 Updating the hard disk drives firmware	303
5.1.8 Updating host bus adapter (HBA) firmware	311
5.2 Handling premium features	315
5.2.1 Listing premium features/feature enabler	316
5.2.2 Enabling a premium feature	319

5.2.3	Disabling a premium feature	323
5.3	Saving and loading the configuration	324
5.3.1	Storage subsystem profile	327
5.4	Migrating arrays between DS storage subsystems	332
5.4.1	Intermixing EXP810 and EXP5000 storage expansion enclosures	332
5.4.2	Intermixing EXP520 and EXP810 storage expansion enclosures	332
5.4.3	Migration prerequisites	333
5.4.4	Exporting an array	335
5.4.5	Importing an array	341
5.5	Upgrading from a DS4700 or DS4800 to a DS5000	345
5.5.1	Planning the upgrade	346
5.5.2	Preparing the new storage subsystem	347
5.5.3	Preparing the original storage subsystem	347
5.5.4	Upgrading the controller firmware	348
5.5.5	Switching from the original to the new storage subsystem	350
5.5.6	Preparing the new storage subsystem for use	351
5.6	Connecting a new storage enclosures to your DS5000	352
5.7	Securing the DS5000 storage subsystem client using remote management	354
5.8	Preventative maintenance and data collection	356
5.8.1	Storage Manager Enterprise Management window	356
5.8.2	Storage Manager Subsystem Management window	358
5.8.3	Storage subsystem profile	359
5.8.4	Recovery Guru	359
5.8.5	Major Event Log	361
5.8.6	Collect All Support Data option	362
5.8.7	Retrieve trace buffers	367
5.8.8	Configuration database validation	369
5.8.9	Database save/restore	371
5.8.10	Media Scan	371
5.8.11	Pre-read redundancy check	373
5.9	Problem determination	373
5.9.1	Diagnosing drive-side problems	374
5.9.2	Diagnosing host-side problems	393
5.9.3	Storage Manager communication problems	407
5.9.4	Connecting to the Controller via the Shell interface	407
5.10	Replacement and maintenance procedures	412
5.10.1	Managing disk failures	412
5.10.2	Managing disks with an impending drive failure error	416
5.10.3	Monitoring Solid State Drives (SSD)	418
5.10.4	Managing battery issues	418
5.11	Replacing adapters (HBA) and storage controllers	419
5.12	HBAs and operating system tools	419
5.12.1	Brocade HBA and Brocade Host Configuration Manager (HCM)	419
5.12.2	Emulex HBA tools	425
5.12.3	Qlogic HBAs and SANsurfer (Windows/Linux)	426
5.12.4	Windows Server 2008	435
5.12.5	Linux	442
5.12.6	AIX	452
Chapter 6.	IBM Remote Support Manager for Storage	455
6.1	IBM Remote Support Manager for Storage	456
6.1.1	RSM for Storage Documentation and installation code	457
6.1.2	Hardware and software requirements	458

6.1.3	How RSM for Storage works.	460
6.1.4	Notification email and events filtering	461
6.1.5	Remote access methods	463
6.1.6	RSM management interface	464
6.1.7	RSM security considerations.	465
6.2	Installing and setting up RSM	467
6.2.1	Installing the host OS	467
6.2.2	Installing RSM.	468
6.2.3	Setting up RSM.	468
6.2.4	Configuring SNMP traps in Storage Manager.	480
6.2.5	Activating RSM	482
6.2.6	Remote access security	484
6.2.7	Managing alerts	489
Chapter 7.	Command-line interface and Script Editor.	495
7.1	Command-line interface (CLI).	496
7.1.1	Using CLI commands	496
7.1.2	CLI parameters	498
7.1.3	Syntax requirements.	503
7.1.4	Error reporting.	504
7.1.5	Commands overview.	505
7.1.6	CLI examples	515
7.2	Script Editor.	522
7.2.1	Using the Script Editor	522
7.2.2	Embedding commands in batch files	526
Appendix A.	Deploying iSCSI with the IBM System Storage DS5000 series.	527
iSCSI technology		528
iSCSI Qualified Name (IQN)		528
iSCSI physical components		529
TCP Offload Engine		530
10 Gigabit iSCSI		530
Network considerations.		531
iSCSI configurations on the DS5000 series.		531
Jumbo frames		531
Virtual Local Area Networks		532
Ethernet priority.		533
Security		534
Internet Storage Name Service.		534
Challenge Handshake Authentication Protocol.		535
iSCSI performance considerations.		536
Multipathing iSCSI		537
Other iSCSI performance considerations		537
Appendix B.	Solid State Drives on the IBM System Storage DS5000 series.	539
SSD technology		540
Solid State Drives in tiered storage		540
Implementing tiered storage		542
Solid State Drives on a DS5000 storage subsystem		542
Identifying SSD in Storage Manager.		543
Wear life		543
SSD performance on DS5000 storage subsystems.		544
A need for high performance disks		544
Initial lab tests of SSDs on a DS5000 storage subsystem		545

SDD summary	546
Related publications	547
IBM Redbooks	547
Other publications	547
Online resources	548
Help from IBM	548

Notices

This information was developed for products and services offered in the U.S.A.

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

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

Any references in this information to non-IBM 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 supply in any way it believes appropriate without incurring any obligation to you.

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.

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


COPYRIGHT LICENSE:

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

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX 5L™	iSeries®	System Storage®
AIX®	Power Systems™	System x®
BladeCenter®	pSeries®	Tivoli®
DS4000®	Redbooks®	XIV®
DS8000®	Redbooks (logo)  ®	zSeries®
FlashCopy®	System p®	
IBM®	System Storage DS®	

The following terms are trademarks of other companies:

Intel Xeon, Intel, Pentium, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

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

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

Preface

This IBM® Redbooks® publication consolidates, in one document, detailed descriptions of the hardware configurations and options offered as part of the IBM System Storage® DS5000 families of products.

This edition covers updates and additional functions available with the IBM System Storage DS® Storage Manager Version 10.77 (firmware level 7.77). This book presents the concepts and functions used in planning and managing the storage servers, such as multipathing and path failover. The book offers a step-by-step guide to using the Storage Manager to create arrays, logical drives, and other basic (as well as advanced) management tasks.

This publication also contains practical information about diagnostics and troubleshooting, and includes practical examples of how to use scripts and the command-line interface.

This publication is intended for customers, IBM Business Partners, and IBM technical professionals who want to learn more about the capabilities and advanced functions of the DS5000® series of storage servers with Storage Manager Software V10.77. It also targets those who have a DS5000 storage subsystem and need detailed advice about how to configure it.

This publication is designed specifically to address the hardware features and configuration of the IBM System Storage DS5000 family and can be used in conjunction with the following IBM Redbooks publications:

- ▶ *IBM System Storage DS5000 Series Implementation and Best Practices Guide*, SG24-8024
- ▶ *IBM System Storage DS Storage Manager Copy Services Guide*, SG24-7822

The team who wrote this book

This book was produced by a team of specialists from around the world working at the International Technical Support Organization, San Jose Center.

Sangam Racherla is an IT Specialist and Project Leader working at the ITSO in San Jose, CA. He has 12 years of experience in the IT field and has been with the ITSO for the past eight years. Sangam has extensive experience in installing and supporting the ITSO lab equipment for various IBM Redbooks projects. He has expertise in working with Microsoft Windows, Linux, IBM AIX®, System x®, and System p® servers, and various SAN and storage products. Sangam holds a degree in electronics and communication engineering.

Matus Butora is an IT Specialist and leader of Storage Support in IBM ITD Delivery Center in Czech Republic. He works with enterprise storage environments providing solutions and support for global strategic customers across the globe. Matus has eight years of experience with Open storage hardware and software including IBM DS8000®, IBM Midrange Storage DS3000/DS4000/DS5000, SVC, NetApp, Tivoli® Storage Management and Tivoli Storage Productivity Center. Matus is a certified IBM Professional and NetApp NCPA certified Administrator.

Antonio Dell'Apa is an IBM Senior Accredited Product Service Specialist and a Team Leader in the MTS Technical Support Team in Rome. He joined IBM in 1989 and spent the first 10 years as Customer Engineer for iSeries®, pSeries® and zSeries® product families. In

2002 he joined the Technical Support group for open systems storage, SAN, and virtualization products. Since 2006 he has been member of Virtual EMEA Team (VET) providing Level 2 support for DS3000, DS4000 and DS5000 products to EMEA region. During the past years, he has been also in charge of deploying education and training to CE and FE specialists to maintain, service, and implement IBM storage products, such as the DS3000, DS5000 and IBM nSeries.

Mario Ganem is an IT professional, specialized in cloud computing and storage solutions. He has 15 years of experience in the IT industry. Mario resides in Buenos Aires, Argentina, where he works as Infrastructure IT Architect in the Delivery Center in Argentina. Prior to starting his career in IBM in 2006, Mario worked in many companies such as Hewlett Packard, Compaq and Unisys. He has developed the internal virtualization products curriculum training which he is teaching nowadays to DCA professionals. He holds, among others, many industry certifications from Microsoft, RedHat, VMWare, Novell, Cisco, CompTIA, HP and Compaq.

Corne Lottering is a Technical Storage Sales Specialist at Saudi Business Machines, the IBM General Marketing and Sales Representative in Saudi Arabia. His job includes customer assessment, planning, design, and delivery of IBM Storage Solutions involving IBM System Storage platforms including IBM San Volume Controller, IBM DS5000 Midrange storage, XIV®, IBM DS8000 Enterprise Storage and IBM N series. His previous experience includes Systems Storage Sales Specialist in the IBM Sub Saharan Africa Growth Market Region for Systems and Technology Group. His primary focus was Sales in the Central African countries but also providing pre-sales support to the Business Partner community. He has more than ten years of experience with IBM working with a wide variety of storage technologies including the DS4000, DS5000, DS8000, IBM XIV. IBM SAN switches, IBM Tape Systems, and storage software.

Libor Miklas is a Team Leader and an experienced IT Specialist working at the IBM Global Services Delivery Center in Czech Republic. He demonstrates ten years of practical experience in the IT industry. During last six years, his main focus has been on backup and recovery and on storage management. He has already written IBM Redbooks related to the IBM storage products and SAN. Libor and his team support midrange and enterprise storage environments for various global and local clients, worldwide. He is an IBM Certified Deployment Professional of the Tivoli Storage Manager family of products and holds a Masters Degree in Electrical Engineering and Telecommunications.

Hrvoje Stanilovic is an IBM Certified Specialist - Midrange Storage Technical Support and Remote Support Engineer working for IBM Croatia. He is a member of CEEMEA VFE Midrange Storage Support team and EMEA PFE Support team, providing Level 2 support for DS3000, DS4000 and DS5000 products in Europe, Middle East and Africa. His primary focus is post-sales Midrange Storage, SAN and Storage Virtualization support, but he is also very active in supporting local projects, mentoring and knowledge sharing. He has been with IBM for 4 years where he has transitioned through various roles, including IBM System p hardware support and Cisco networking support, before working with Midrange Storage systems.

Alexander Watson is a Senior IT Specialist for Storage ATS Americas in the United States. He is a Subject Matter Expert on SAN switches and the DS4000/DS500 products. He has over ten years of experience in planning, managing, designing, implementing, problem analysis, and tuning of SAN environments. He has worked at IBM for ten years. His areas of expertise include SAN fabric networking, Open System Storage IO and the IBM Midrange Storage Subsystems family of products.

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

Jon Tate
Bertrand Dufrasne
Ann Lund
Mary Lovelace
Alex Osuna
Karen Orlando
Larry Coyne

International Technical Support Organization, San Jose Center

Fred Scholten
Joseph F Bacco
Paul Goetz
Harold Pike
Danh Le
Noah J Seller
Reginald Phillips
John Sanner
Joyce Mercado
Barry Haddon
John Fasano
John Murtagh
Roger Bullard
Pete Urbisci
Gene Cullum
James Elliott
Bill Willson
Brenda Robinson
Rebecca C Swingler
Sharyn D Wolfe

IBM

John Bish
Doug Merrill
David Worley

NetApp

Brian Steffler
Steven Tong
Yong Choi

Brocade Communications Systems, Inc.

Thanks to the authors of the current and previous edition of the below Redbooks:

- ▶ *IBM Midrange System Storage Hardware Guide*, SG24-7676
- ▶ *IBM Midrange System Storage Implementation and Best Practices Guide*, SG24-6363
- ▶ *IBM System Storage DS4000 and Storage Manager V10.30*, SG24-7010
- ▶ *VMware Implementation with IBM System Storage DS4000/DS5000*, REDP-4609

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 at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

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

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

ibm.com/redbooks

- Send your comments in an email to:

redbooks@us.ibm.com

- Mail your comments to:

IBM Corporation, 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>



Introduction to IBM System Storage DS5000 series

This chapter introduces the IBM System Storage DS5000 series storage subsystems and positions them within the overall IBM System Storage Disk Systems (DS) family. The current hardware models are briefly described, as well as the Storage Manager software. Detailed information is given in subsequent chapters of this book.

1.1 Positioning the DS5000 series

IBM has brought together into one family, known as the DS family, a broad range of disk systems to help small to large size enterprises select the right solutions for their needs. The DS family combines the high-performance IBM System Storage DS8000 series of enterprise servers with the IBM System Storage DS5000 series of midrange systems, and other line-of-entry systems (IBM System Storage DS3000 series).

The IBM System Storage DS5000 series is composed of products that fit different requirements in terms of performance and scalability, and are ready for multiple environments ranging from departmental to bandwidth-intensive and transaction-heavy. Moreover, these products are designed for business continuity and high availability, are ready for the challenges of IT Optimization (Consolidation, Virtualization, and Adaptability), and are designed for a longer life cycle with investment protection.

The IBM System Storage DS5000 series of disk storage systems that this IBM Redbooks publication addresses is the IBM solution for midrange/departmental storage requirements and controlling change through adaptability. The positioning of the products within the Midrange DS5000 series is shown in Figure 1-1.

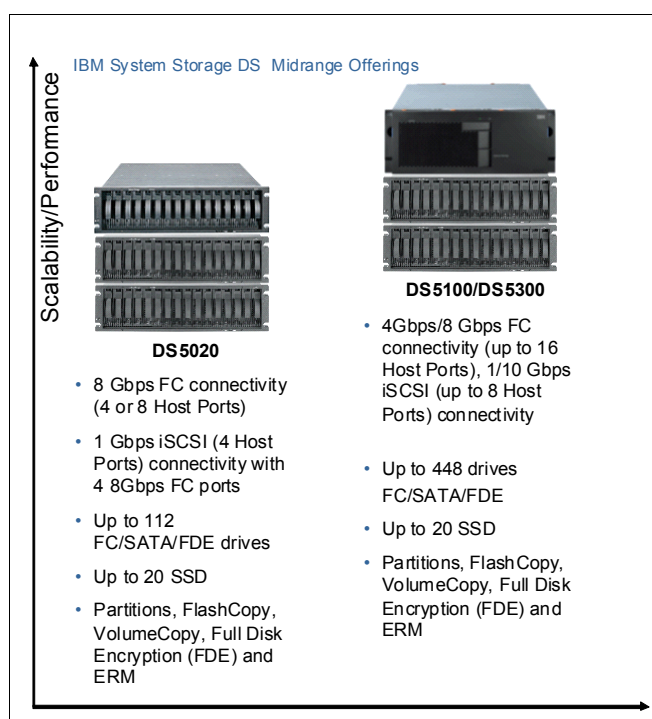


Figure 1-1 Product positioning within the IBM Midrange System Storage DS5000 series

The overall positioning of the DS5000 series within the IBM System Storage DS family is shown in Figure 1-2. It expands the IBM Midrange System Storage offering in terms of performance and scalability.

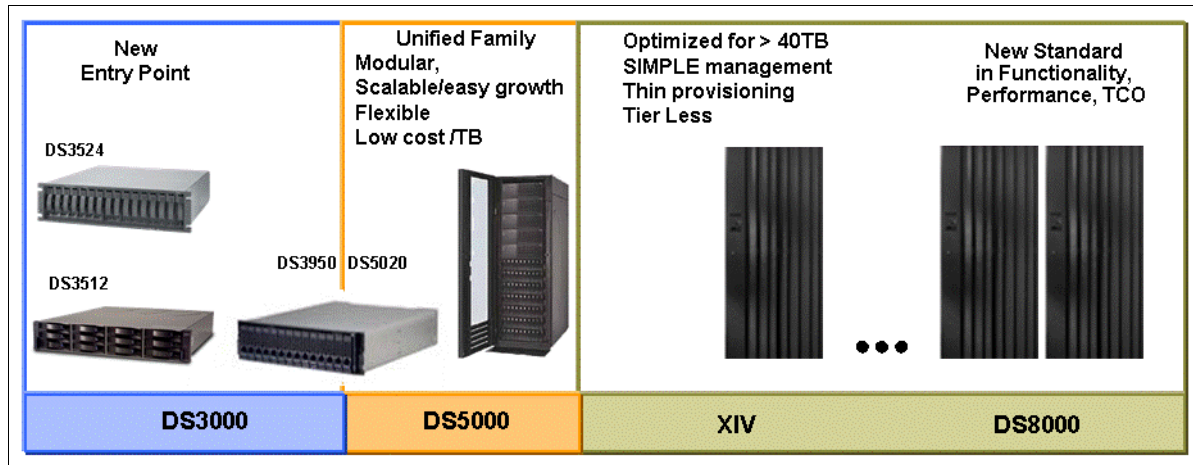


Figure 1-2 DS5000 series positioning within the IBM System Storage family

Within the IBM Midrange storage series, the DS5000 models of storage servers support Fibre Channel (FC), Serial ATA (SATA), Full Disk Encryption (FDE) disk drives, Solid State Drives (SSD), and Serial Attached SCSI (SAS) disk drives through the Fibre Channel (FC) interface.

In terms of capacity, the maximum raw SATA storage capacity is 896TB, using 2TB SATA DDM drives. The maximum raw FC storage capacity is 268.8 TB (using 600 GB 15K 4 Gbps FC DDM).

1.2 IBM Midrange System Storage DS5000 series models

The IBM Midrange System Storage DS5000 series of storage servers uses Redundant Array of Independent Disks (RAID) technology. RAID technology is used to protect the user data from disk drive failures. DS storage subsystems contain Fibre Channel (FC) interfaces to connect the disk drive enclosures, which contain iSCSI or Fibre Channel (FC) interfaces to connect the host systems.

The storage servers in the DS5000 series provide high system availability through the use of hot-swappable and redundant components. This is crucial when the storage server is placed in high-end customer environments, such as server consolidation on Storage Area Networks (SANs).

At the time of writing, the IBM Midrange System Storage DS5000 storage series is composed of three products that are available in specific models. These products are named DS5020, DS5100, and DS5300, which offers balanced performance, and linear IOPS scalability supports workloads ranging from departmental to bandwidth-intensive.

In terms of intermixing among different hard disk drive technologies, we have the following supported configurations:

- ▶ DS5100 and DS5300 storage servers support the intermixing of high performance FC, high capacity SATA drives, Full Disk Encryption (FDE), Solid State Drives (SSD), and Serial Attached SCSI (SAS) within a single expansion units.
- ▶ DS5020 storage servers support the intermixing of high performance FC, high capacity SATA drives, Full Disk Encryption (FDE), Solid State Drives (SSD), and Serial Attached SCSI (SAS) within single expansion units and even within the controller enclosure.

Currently, the DS5000 series supports host connectivity through the following interfaces:

- ▶ 4 Gbps FC host ports (DS5100, and DS5300)
- ▶ 8 Gbps FC host ports (DS5020, DS5100, and DS5300)
- ▶ 1 Gbps iSCSI host ports (DS5020, DS5100, and DS5300)
- ▶ 10 Gbps iSCSI host ports (DS5100, and DS5300)

We briefly describe the characteristics of the three products previously mentioned:

- ▶ IBM System Storage DS5020 server

The DS5020 is designed to help address midrange or departmental storage requirements. The DS5020 has a 3U rack-mountable enclosure, has four 4 Gbps FC drive interfaces, and can consist of a maximum of six EXP520 expansion units for a total of up to 112 disk drives. Through a specific activation feature, six EXP810 expansions can be used in place of the EXP520s.

Note: An RPQ approval from IBM is required for the EXP810 activation with DS5020.

The DS5020 can be configured with 2 or 4 GB of cache memory and different host connectivity options as listed below:

- Two 8 Gbps FC host ports on each of its two controllers
- Four 8 Gbps FC host ports on each of its two controllers
- Two 8 Gbps FC host ports and, optionally, two 1 Gbps iSCSI on each of its two controllers

One model is available:

- Model 20A with 2 GB or 4 GB of cache memory and one of the combinations of host interfaces specified in the list above.

► IBM System Storage DS5100 server

The DS5100 is targeted at high-end customers. This storage subsystem is a 4U rack-mountable enclosure, has sixteen 4 Gbps FC drive interfaces, and can hold a maximum of twenty-eight EXP5000 expansion units, a maximum of twenty-eight EXP810 expansion units or, for migration purposes, up to twenty-eight expansion units composed of a mix of EXP5000 and EXP810 for a total of up to 448 disk drives.

The DS5100 can have up to 64GB of cache memory and different host connectivity options as listed below:

- Four 4 Gbps FC host ports on each of its two controllers
- Four 8 Gbps FC host ports on each of its two controllers
- Two 1 Gbps iSCSI host ports on each of its two controllers
- Two 10 Gbps iSCSI host ports on each of its two controllers
- Eight 4 Gbps FC host ports on each of its two controllers
- Eight 8 Gbps FC host ports on each of its two controllers
- Four 8 Gbps FC host ports and Two 1 Gbps iSCSI host ports on each of its two controllers
- Four 8 Gbps FC host ports and Two 10 Gbps iSCSI host ports on each of its two controllers
- Four 1 Gbps iSCSI host ports on each of its two controllers
- Four 10 Gbps iSCSI host ports on each of its two controllers

One model is available:

- Model 51A with 8 GB, 16 GB, 32 GB, or 64 GB of cache memory and one of the combinations of host interfaces specified in the list above.

► IBM System Storage DS5300 server

The DS5300 server has greater scalability than the DS5100. This storage subsystem is a 4U rack-mountable enclosure, has sixteen 4 Gbps FC drive interfaces, and can hold a maximum of twenty-eight EXP5000 expansion units, a maximum of twenty-eight EXP810 expansion units, or, for migration purposes, up to twenty-eight expansion units composed of a mix of EXP5000 and EXP810 for a total of up to 448 disk drives. It is designed to deliver data throughput of up to 400 MBps per drive port.

The DS5300 can mount up to 64 GB of cache memory and different host connectivity options as listed below:

- Four 4 Gbps FC host ports on each of its two controllers
- Four 8 Gbps FC host ports on each of its two controllers
- Two 1 Gbps iSCSI host ports on each of its two controllers
- Two 10 Gbps iSCSI host ports on each of its two controllers
- Eight 4 Gbps FC host ports on each of its two controllers
- Eight 8 Gbps FC host ports on each of its two controllers
- Four 8 Gbps FC host ports and two 1 Gbps iSCSI host ports on each of its two controllers
- Four 8 Gbps FC host ports and Two 10 Gbps iSCSI host ports on each of its two controllers
- Four 1 Gbps iSCSI host ports on each of its two controllers
- Four 10 Gbps iSCSI host ports on each of its two controllers

One model is available:

- Model 53A with 8 GB, 16 GB, 32 GB, or 64 GB of cache memory and one of the combinations of host interfaces specified in the list above.

1.3 IBM Midrange System Storage DS5000 expansion enclosure

The IBM Midrange System Storage DS5000 expansion enclosures offer a 4 Gbps FC interface, and four models are available:

► EXP810 Expansion Enclosure

This expansion unit is packaged in a 3U rack-mountable enclosure, supports up to 16 FC disk drives or E-DMM SATA drives. It contains 16 drive bays, dual-switched 4 Gbps ESMs, and dual power supplies and cooling components. Fully populated with 600 GB FC disk drive modules, this enclosure offers up to 9.6 TB of raw storage capacity or up to 32 TB when populated with the 2000 GB E-DDM SATA drives. The EXP810 expansion unit is the only one that may be connected to every storage subsystem of the DS5000 family. Through the proper firmware level, this expansion unit is able to host both FC and SATA Drives. Intermix of FC and SATA drives is supported within this expansion enclosure.

► EXP5000 Expansion Enclosure

This expansion unit is packaged in a 3U rack-mountable enclosure, supports up to 16 FC disk drives, E-DMM SATA drives, Full Disk Encryption (FDE) drives, Serial Attached SCSI (SAS) drives, and Solid State Disk drives (SSD). It contains 16 drive bays, dual-switched 4 Gbps ESMs, and dual power supplies and cooling components. Fully populated with 600 GB FC disk drive modules, this enclosure offers up to 9.6 TB of raw storage capacity or up to 32 TB when populated with the 2 TB E-DDM SATA drives. The EXP5000 expansion unit may be connected to the DS5100 or DS5300 storage server. Through the proper firmware level, this expansion unit is able to host both FDE, FC, SATA, SAS and SSD drives. An intermix of FC, SATA, FDE, SAS, and SSD drives is supported within this expansion enclosure.

► EXP520 Expansion Enclosure

This expansion unit is packaged in a 3U rack-mountable enclosure, supports up to 16 FC disk drives, E-DMM SATA drives, Full Disk Encryption (FDE) drives, Serial Attached SCSI (SAS) or Solid State Disk Drives (SSD). It contains 16 drive bays, dual-switched 4 Gbps ESMs, and dual power supplies and cooling components. Fully populated with 600 GB FC disk drive modules, this enclosure offers up to 9.6 TB of raw storage capacity or up to 32TB when populated with the 2 TB E-DDM SATA drives. The EXP520 expansion unit may be connected to the DS5020 storage server. Through the proper firmware level, this expansion unit is able to host both FDE, FC, SATA, SAS and SSD drives. An intermix of FC, SATA, FDE, SAS and SSD drives is supported within this expansion enclosure.

► EXP5060 Expansion Enclosure

The IBM System Storage EXP5060 storage expansion enclosure provides high-capacity SATA disk storage for the DS5100 and DS5300 storage subsystems. The storage expansion enclosure provides continuous, reliable service, using hot-swap technology for easy replacement without shutting down the system and supports redundant, dual-loop configurations. External cables and Small Form-Factor Pluggable (SFP) modules connect the DS5100 or DS5300 storage subsystem to the EXP5060 storage expansion enclosure. The EXP5060 uses redundant 4 Gbps Fibre Channel connections to make connections to the DS5100 or DS5300 storage subsystem, and another EXP5060 storage expansion enclosure in a cascading cabling configuration, offering reliability and performance.

Note: A maximum of eight EXP5060 storage expansion enclosures (with 480 hard drives) can be attached only to the DS5100 and DS5300 storage subsystems and only SATA disks are supported in the EXP5060 expansion.

The EXP5060 is a 4U rack-mountable enclosure that supports up to 60 SATA Disk Drive Modules (DDMs), offering up to 120TB of SATA disk space per enclosure using 2 TB SATA DDMs. The expansion enclosure contains 60 drive bays (arranged on five stacked drawers with twelve drives for each drawer), dual-switched 4 Gbps ESMs, and dual power supplies and cooling components. Coupled with a storage subsystem (DS5100 or DS5300), you can configure RAID-protected storage solutions of up to 960 TB when using 2TB SATA DDMs and eight EXP5060 storage expansion enclosures, providing economical and scalable storage for your rapidly growing application needs. The Attach up to 8 EXP5060s feature pack must be purchased for the DS5100/DS5300 storage subsystem to enable it to be connected to up to eight EXP5060 storage expansion enclosures.

Note: Intermixing of EXP5060 enclosures, EXP5000 enclosures and EXP810 enclosures attached to a DS5100 or DS5300 controller is supported, but limited to a configuration of up to 448 drives or less.

1.4 IBM System Storage DS Storage Manager software

The IBM System Storage DS Storage Manager software (see Figure 1-3) is used to configure, manage, and troubleshoot the DS5000 storage subsystems.

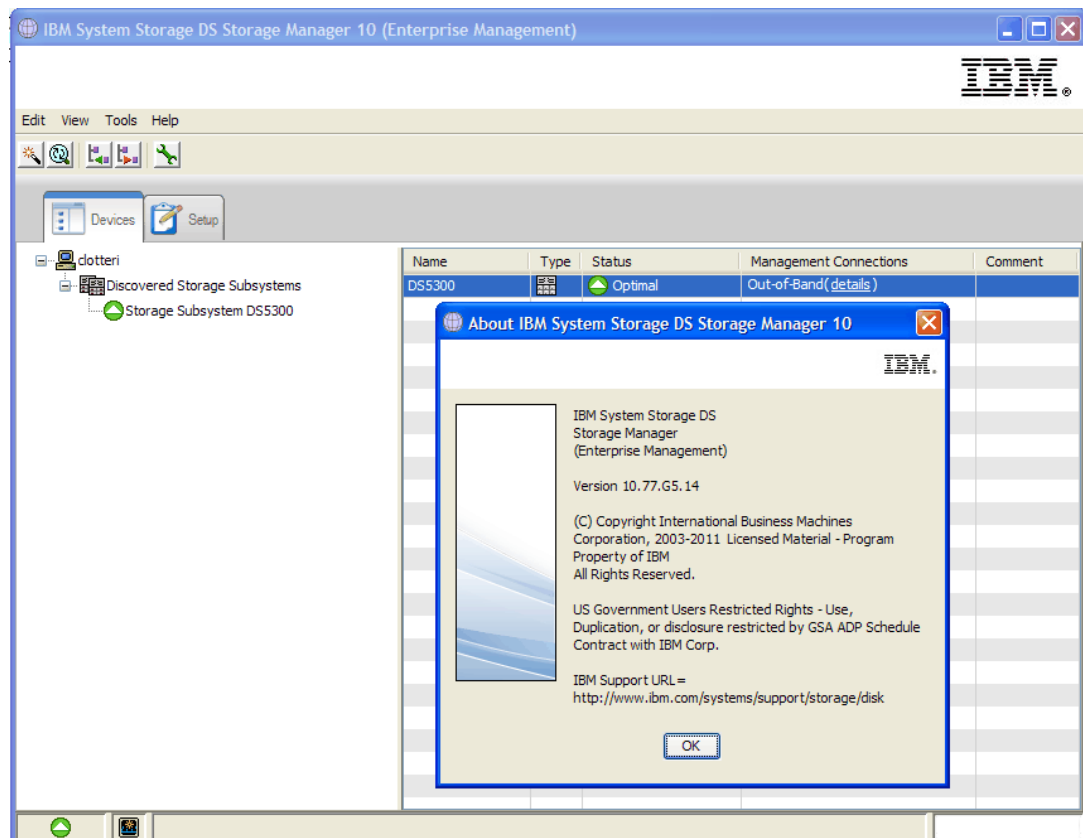


Figure 1-3 IBM System Storage DS Storage Manager

It is used primarily to configure RAID arrays and logical drives, assign logical drives to hosts, replace and rebuild failed disk drives, expand the size of the arrays and logical drives, and convert from one RAID level to another. It allows for troubleshooting and management tasks, such as checking the status of the storage server components, updating the firmware of the RAID controllers, and managing the storage server. Finally, it offers advanced functions, such as FlashCopy®, Volume Copy, Enhanced Remote Mirroring, and Disk Encryption.

The Storage Manager software is now packaged as the following combinations:

► *Host-based software*

– Storage Manager Client (SMclient)

The SMclient component provides the graphical user interface (GUI) for managing storage systems through the Ethernet network or from the host computer.

– Storage Manager Runtime (SMruntime)

The SMruntime is a Java runtime environment that is required for the SMclient to function. It is not available on every platform as a separate package, but in those cases, it has been bundled into the SMclient package.

– Storage Manager Agent (SMagent)

The SMagent package is an optional component that allows in-band management of the DS5000 storage subsystems.

– Storage Manager Utilities (SMutil)

The Storage Manager Utilities package contains command-line tools for making logical drives available to the operating system.

– Failover driver support

Storage Manager host based software includes an optional failover driver. It is a multipath driver built on MPIO technology.

► *Controller-based software*

– DS5000 storage subsystem controller firmware and NVSRAM

The controller firmware and NVSRAM are always installed as a pair and provide the “intelligence” of the Midrange System Storage server.

– DS5000 storage subsystem Environmental Service Modules (ESM) firmware

The ESM firmware controls the interface between the controller and the drives.

– DS5000 storage subsystem drive firmware:

The drive firmware is the software that instructs the Fibre Channel (FC) drives about how to operate on the FC loop.

The Storage Manager functions are reviewed in detail in 3.4, “Step-by-step configuration” on page 155.

1.5 IBM Midrange System Storage DS5000 hard disk drives

Every storage subsystem within the IBM Midrange System Storage DS5000 series is a multi-tiered storage server that is capable of supporting multiple disk drive technologies even within the single expansion unit. This capability enables you to have a Total Cost of Ownership (TCO) reduction and storage consolidation by putting together different workloads with different performance requirements. Figure 1-4 shows a possible hard disk drive (HDD) layout within four expansion units.

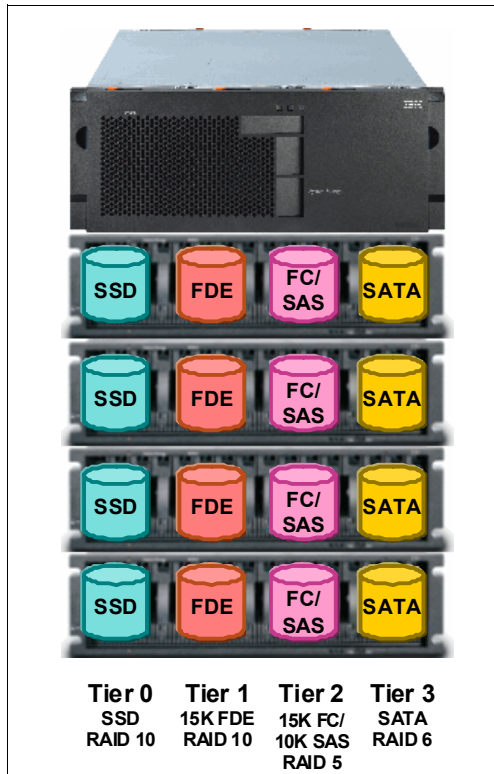


Figure 1-4 Multi-Tier HDD layout

The currently supported HDD technologies are briefly described below:

► Solid State Drives (SSDs)

Solid State Drives use semiconductor devices (solid state memory) to store data and have no moving parts. An SSD is a flash memory device mimicking a disk drive. SSDs are available with the same interfaces used by hard disk drives (for example, SAS, SATA, and Fibre Channel) and they are packaged in the same form factors as hard disk drives (3.5-in., 2.5-in., and 1.8-in.). SSDs are designed to plug into the same environments as those supported by hard disk drives. As already mentioned, the simple fact that there are no moving parts (disk platters, magnetic heads, or motor) in an SSD results in:

- Faster data access and throughput: The access to the data with an SSD is faster because again, there is no read/write head to move and no magnetic platters need to spin up (no latency). On an SSD, the data can be read almost immediately.
- Better reliability: Again, the lack of moving and rotating parts almost eliminates the risk of mechanical failure. SSDs have the ability to tolerate extreme shocks, higher altitudes, vibration, and extremes of temperature. However, they can still fail and must be RAID protected like traditional drives.
- Less power consumption: Because there is no power for the motor required to spin up the magnetic platters and to move the heads, the drive uses less energy than a traditional hard disk drive. Each SSD uses about half of the power of a 15K RPM HDD. The savings can be substantial if a few SSDs can replace many HDDs to deliver the same performance. This is particularly true for applications that were forced, for performance reasons, to use large quantities of HDDs to get as many spindles as they can, though they were only using a small portion of the disk capacity. Besides power consumption savings, the overall system will weigh much less because SSDs are already much lighter than HDDs.

SDD is supported in an EXP5000 expansion unit behind a DS5020, DS5100 or a DS5300 storage server. At the time of writing, two SSD models; 200 GB and 400 GB capacity are supported.

► Full Disk Encryption Hard Disk Drives (FDE HDD)

FDE is a technology that performs encryption on the hard disk drive at the hardware level. The Fibre Channel hard drive contains a custom chip or application specific integrated circuit (ASIC) that is used to encrypt every bit of data as it is written and also decrypts data as it is being read. ASIC requires a security key to allow encryption and decryption to begin.

FDE disk drives encrypt all the data on the disk. The secured drive requires that a security key be supplied before read or write operations can occur. The encryption and decryption of data is processed entirely by the drive and is not apparent to the storage subsystem.

FDE HDDs are supported on DS5000 models (DS5020, DS5100, and DS5300).

The FDE HDDs that are currently supported include:

- 4 Gbps FC, 146.8 GB/15k rpm
- 4 Gbps FC, 300 GB/15k rpm
- 4 Gbps FC, 450 GB/15k rpm
- 4 Gbps FC, 600 GB/15k rpm
- 4 Gbps FC-SAS, 600 GB/10k rpm

► Fibre Channel Hard Disk Drives (FC HDD)

Fibre Channel is an industry-standard interface that supports very high data rates as well as many more devices than traditional SCSI or ATA/IDE technologies. It is also a serial interface, and uses a loop topology. FC HDDs feature a full-duplex dual-port active/active 4 Gbps Fibre Channel interface. The DS5000 series storage servers can mount different types of FC HDDs in terms of size and revolutions per minute (RPM):

- 4 Gbps FC, 146.8 GB/15k rpm
- 4 Gbps FC, 300 GB/15k rpm
- 4 Gbps FC, 450 GB/15k rpm
- 4 Gbps FC, 600 GB/15k rpm

► Serial Attached SCSI Drives (SAS)

SAS is a computer bus used to move data to and from computer storage devices such as hard drives and tape drives. SAS depends on a point-to-point serial protocol that replaces the parallel SCSI bus technology, and uses the standard SCSI command set.

The SAS drives are connected to the DS5000 series storage system via an FC-interposer card to deliver throughput of up to 4 Gbps full duplex.

The DS5000 series can mount the following SAS HDDs in terms of size and revolutions per minute (RPM):

- 4 Gbps FC-SAS, 300 GB/10k rpm FC-SAS
- 4 Gbps FC-SAS, 600 GB/10k rpm FC-SAS
- 4 Gbps FC-SAS, 900 GB/10k rpm FC-SAS

► Serial ATA Hard Disk Drives (SATA HDD)

Serial ATA is the hard disk standard created to replace the parallel ATA interface (also called IDE). Serial ATA transmits data in serial mode and implements two separated datapaths, one for transmitting and another for receiving data. The standard transfer rate is 1.5 Gbps for Serial ATA standard, although Serial ATA II (second generation) provides new features, such as Native Command Queuing (NCQ), plus a higher speed rate of 3 Gbps. NCQ increases the hard disk drive performance by reordering the commands send by the host. Through the speed-matching technology provided by the expansion enclosures mentioned in 1.3, “IBM Midrange System Storage DS5000 expansion enclosure” on page 6, SATA hard disk drives are able to work with a transfer rate of 4 Gbps, enabling the intermixing of high performance FC and high capacity SATA drives.

The DS5000 series can mount different types of FC HDDs in terms of size and revolutions per minute (RPM):

- 500 GB/7.2k rpm SATA
- 750 GB/7.2k rpm SATA II (all the models)
- 1000 GB/7.2k rpm SATA II (all the models)
- 2000 GB/7.2k rpm SATA II (only EXP5000)

1.6 iSCSI basics

All the DS5000 series models now support iSCSI host connectivity and in this section we briefly describe the basics of the iSCSI protocol. Consult Appendix A, “Deploying iSCSI with the IBM System Storage DS5000 series” on page 527 for more detailed information.

iSCSI is an industry standard developed to enable transmission of SCSI block commands over the existing IP network by using the TCP/IP protocol. The TCP/IP protocol provides iSCSI with inherent reliability along with byte by byte, in order delivery, built-in security, and no interoperability barriers.

When a user or application sends a request, the operating system generates the appropriate SCSI commands and data request, which then go through encapsulation. A packet header is added before the resulting IP packets are transmitted over an Ethernet connection. When a packet is received, it is disassembled, separating the SCSI commands and request. The SCSI commands are sent on to the SCSI controller, and from there to the SCSI storage device. Because iSCSI is bi-directional, the protocol can also be used to return data in response to the original request.

The logical link that carries the commands and data to and from TCP/IP endpoints is called an *iSCSI session*. A session is made up of at least one TCP/IP connection from an *initiator* (host) to a *target* (storage device), as shown in Figure 1-5. The iSCSI initiator can be either an iSCSI HBA inside a host server, or you can define a software iSCSI initiator by using an iSCSI stack and an Ethernet network adapter. An example of an iSCSI stack is the Microsoft iSCSI Software Initiator, which runs on Windows Server 2003 and Windows Server 2008.

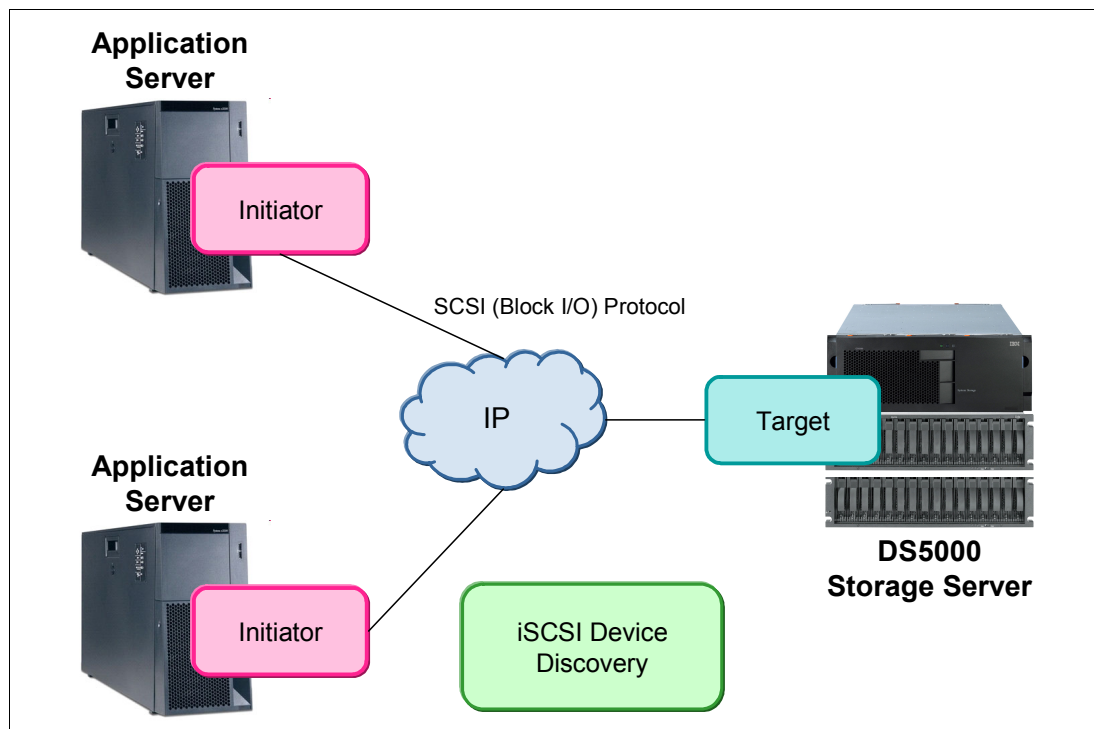


Figure 1-5 iSCSI components

iSCSI SANs might not be a solution for everyone, given that iSCSI SANs might not deliver the same performance that Fibre Channel SANs can deliver. However, there are ways to address iSCSI performance:

- ▶ While the host servers can use almost any Ethernet network interface card for iSCSI traffic, this does mean that the CPUs on the host server have to run the iSCSI stack (to perform encapsulation of SCSI commands and data). This causes increased CPU and memory processing, which can impact performance. For increased performance, it is better to use dedicated iSCSI HBAs to process the TCP/IP stack. This technology is known as TCP Offload Engine (TOE). TOE technology relieves the CPUs on the host server from having to process the SCSI encapsulation, which can lead to better performance.
- ▶ To avoid excessive traffic, but mainly to ensure that only valid initiators connect to storage servers, it is better to run iSCSI over dedicated network segments or virtual LANs (VLAN).

1.7 Fibre Channel direct/switch basics

Fibre Channel (FC) is a high-speed disk attachment technology, designed to connect a large number of storage devices to a number of host servers across a Storage Area Network (SAN). Fibre Channel Protocol (FCP) transfers SCSI commands and data across physical FC links.

FC supports a much higher number of devices and much longer cable lengths than SCSI. It has become the preferred disk attachment technology in midrange and large scale data center solutions.

At the time of writing, the IBM Midrange System Storage DS5000 series' maximum FC throughput is 8 Gbps.

Host servers contain one or more FC Host Bus Adapters (HBA). The HBAs provide connectivity to the storage devices using FC cabling and SAN Switch.

For more information about Fibre Channel and SANs, see *Introduction to Storage Area Networks*, SG24-5470.

FC topologies

FC supports several connectivity topologies:

- ▶ Point-to-point

This is the simplest topology and provides a direct link between an FC HBA inside a host server and a storage device.

- ▶ Arbitrated loop

This topology can be used to interconnect several FC devices. A typical example is to attach a certain number of host servers to an FC storage subsystem. A loop can consist of up to 126 devices.

Devices on the loop use one-way ring communication. In any given moment, only two devices on the loop can communicate. This means the devices share bandwidth, so the arbitrated loop topology is not suitable for high performance requirements.

Arbitrated loops were commonly implemented with the use of an FC hub. Even though this is physically a star topology, logically it will be a loop. Alternatively, devices can be connected in a daisy chain manner. Arbitrated loops are rarely seen these days, as switched fabrics have become the norm.

- ▶ Switched fabric

The most commonly used topology in a typical SAN today is switched fabric. SAN switches are used to provide FC connectivity between the host servers and storage devices. Switched fabrics can become very complex in large scenarios, connecting hundreds of host servers to a very large number of storage subsystems.

SAN switches provide optimized traffic flow and increased performance by allowing concurrent data transfers between many connected hosts and storage devices. Switched fabrics can provide dedicated bandwidth, as opposed to arbitrated loop technology, where the bandwidth is shared among all the devices in the loop.

FC protocol layers

The FC protocol is split into five layers, named FC0 through FC4. Let us look briefly at them:

- ▶ FC0 is the physical layer, which describes cabling, connectors, signalling, and so on. This layer defines the physical media implementation.
- ▶ FC1 is the data link layer. This layer contains the 8b/10b encoding and decoding of signals for transmission across the physical media.
- ▶ FC2 is the network layer and defines the main FC protocols. This layer defines how the frames are transferred.
- ▶ FC3 is the common services layer. This layer provides services such as multi-casting and striping.

- FC4 is the application protocol mapping layer. In storage connectivity applications, FCP protocol is used to encapsulate SCSI data into FC frames.

FC cable types

FC implementations can utilize either single-mode or multi-mode FC cables. The name multi-mode fiber indicates that multiple modes, or rays of light, can travel through the cable core simultaneously. The multi-mode fiber cable uses a larger diameter core, which makes it easier to couple than the single-mode fibre cable. With a throughput of 8 Gbps, the length of the cable can be up to 150 m.

Single-mode fiber transfers a single ray of light. The core diameter is much smaller than the core of a multi-mode cable. Therefore, coupling is much more demanding and tolerances for single-mode connectors and splices are very low. However, single-mode fiber cables can be much longer. The cable length can exceed 50 km.

Multi-mode cabling is much more common, as it is easier to work with and meets the requirements of most customer scenarios. However, in situations where very long cable lengths are needed, single-mode cabling will be required.

FC world wide names (WWN)

FC devices are presented with a unique identifier called world wide name (WWN). The WWNs are somewhat similar to the MAC addresses in Ethernet terms. For example, each FC HBA has its own WWN, which is hardcoded (or burned-in) during manufacturing. The HBA will be uniquely identified by the storage subsystem using its WWN.

1.8 New features with controller firmware version 7.77

This section provides a brief description of new features that are part of controller firmware version (CFW) 7.77 and other IBM System Storage DS5000 announcements.

Apart of the newest enhancements and functionalities that are not covered yet in the previous editions of this publication, we repeat some of the options that we consider as important to mention again and to provide readers the comprehensive overview about DS5000 features.

1.8.1 Full Disk Encryption capable disk drive modules (DDM)

Disk Security is a new feature introduced with the DS5000 that complements the newly available Full Disk Encryption (FDE) drives. It is supported by the latest level of DS5000 firmware (Version 7.60) and Storage Manager V10.60. This new feature can add a greater level of security to data that resides on disk.

The Full Disk Encryption (FDE) disk is used in conjunction with IBM Disk Encryption Storage Manager on the DS5000 storage subsystem. IBM Disk Encryption Storage Manager will generate encryption and decryption keys that are used to lock each FDE drive so that all data that resides on a disk is fully encrypted.

The FDE disks of capacity of 146, 300, 450, and 600 GB disks at a speed of 15k rpm are available for DS5000 storage subsystems.

See Chapter 4, “Full Disk Encryption with Full Disk Encryption drives” on page 253 for details about how FDE works and how to set it up.

1.8.2 Solid State Drive (SSD) module

The need for higher IOPS in enterprise storage led to a new storage type known as Solid State Drive (SSD). SSDs have existed for some time, and were built in the past by using volatile DRAM memory that was supplemented with battery backup. However, these were enormously expensive and were often up to 1,000 times the cost of a high-performance disk drive with an equivalent capacity.

Some applications require very high IOPS rates, and there are specific military or industrial use cases that benefit from insensitivity to shock and vibration. But the vast majority of applications cannot justify the extra cost, so SSDs have remained a rarity.

A new storage device type based on non-volatile flash memory is now available for enterprise workloads that require high IOPS. Flash memory is less than 10 percent of the cost of DRAM, and expected innovations should lower the cost by another order of magnitude in the next 2-3 years. By itself, however, flash memory is too slow to perform WRITE operations and has an unacceptably short life. Clever engineering has been applied to use flash memory in combination with DRAM and embedded software to create a device for enterprise applications, one that is interface and function compatible with an HDD, but has substantially higher IOPS performance. These devices made their appearance in 2008, and will be widely available as optional devices in disk arrays. Flash-based SSDs are still more costly than HDDs of equivalent capacity, but for high IOPS workloads, they can cost less.

SAS SSD (with FC-SAS interposer) are available in the following sizes:

- ▶ 200 GB 4Gbps FC-SAS E-DDM 2.5 inch
- ▶ 400 GB 4Gbps FC-SAS E-DDM 2.5 inch

1.8.3 600 GB FC disk drive module

The DS5000 offers a 600 GB FC enhanced disk drive module (E-DDM). The dual port FC DDM operates at 4 Gbps FC speed. It is designed to fit into the EXP810, EXP5000, and EXP520. However, the drive requires a certain enclosure service module (ESM) firmware and controller firmware (CFW) version to be recognized by the DS5000 subsystem. See the latest ESM readme to verify compatibility with your subsystem.

The drive is also available as an FDE Drive.

The DDM characteristics are:

- ▶ 600 GB capacity
- ▶ 15,000 RPM (15K)
- ▶ Hot swappable
- ▶ Dual FC interface to EXP

1.8.4 900 GB SAS disk drives

The DS5000 offers a 900 GB Serial Attached SCSI (SAS) disk drives modules. These 6 Gbps SAS disk modules are equipped with 4 Gbps Fibre Channel interposer, therefore show the characteristics of 4 Gbps FC disks. The firmware version 7.60 or higher is needed for the storage subsystem to recognize these disk drives, the DS Storage Manager 10.60 or higher to manage them.

The DDM characteristics are:

- ▶ 900 GB capacity

- ▶ 10,000 RPM (10K)
- ▶ Hot swappable
- ▶ Dual FC interface to EXP using the FC-SAS interposer

1.8.5 2 TB SATA enhanced disk drive module

The DS5000 offers a 2000 GB (2 TB) SATA enhanced disk drive module (E-DDM). The disk drive operates at 6 Gbps SATA speed. The ATA interposer card on the DDM converts the ATA protocol of the drive to the 2 or 4 Gbps Fibre Channel protocol, so that the DDM module fits in every EXP810, EXP5000, and EXP520. However, the drive requires a certain enclosure service module (ESM) firmware and controller firmware version (CFW) to be recognized by the DS5000 subsystem. See the latest ESM readme to verify the compatibility with your subsystem.

The DDM characteristics are:

- ▶ 2000 GB capacity
- ▶ 7200 RPM
- ▶ Hot swappable
- ▶ Dual FC interface to EXP
- ▶ 2 and 4 Gbps FC speed (1 Gbps not supported)

1.8.6 3 TB SATA enhanced disk drive module

The DS5000 in configuration with enclosures EXP5060 offers a 3000 GB (3 TB) SATA enhanced disk drive module (E-DDM). The 3.5" disk drive operates at 6 Gbps SATA speed and interconnect with the EXP5060 using SATA interface. There is no FC-SAS interposer being used.

The DDM characteristics are:

- ▶ 3000 GB capacity
- ▶ 7200 RPM
- ▶ Hot swappable
- ▶ 6Gbps SATA interface
- ▶ EXP5060 compatibility only

1.8.7 10 Gbps iSCSI host interface

The DS5100 and DS5300 storage subsystems support 10 Gbps iSCSI connectivity. You must determine how the host systems will connect to the storage subsystem.

The iSCSI ports support IPv4 and IPv6 TCP/IP addresses, CHAP, and iSNS. Use either Cat6 Ethernet cable types for iSCSI port connections (Cat5E can be used for 1 Gbps iSCSI). The Cat6 Ethernet cable provides optimal performance and reliability.

You can choose between and iSCSI host interface cards (HICs) or 8 Gbps FC interfaces when initially purchasing the IBM DS5020. iSCSI HICs for the DS53100 and DS5300 are available as field replaceable upgrades (MES) that will be installed by trained IBM service personnel. Do not intermix 1 Gbps and 10 Gbps HICs in one storage subsystem.

Figure 1-6 on page 17 shows the 10 Gbps iSCSI host interface card.

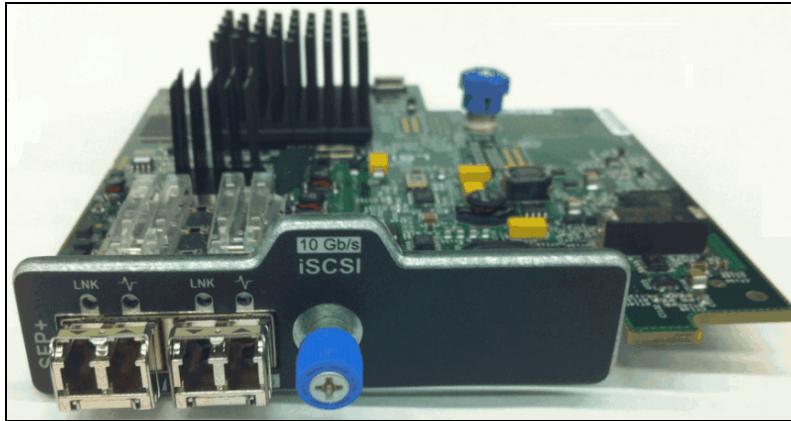


Figure 1-6 10 Gbps iSCSI host interface card

1.8.8 Premium features activation

The latest version of DS5000 introduces the non-disruptive installation and activation of premium features. This option is valid for all models of DS5000 family - DS5020, DS5100, and DS5300.

1.8.9 T10 Protection Information

The DS5000 family supports AIX and Linux platforms to offer T10 Protection Information (T10PI, formerly known as T10-DIF), that helps to prevent silent data corruption and ensures data integrity and regulatory compliance as it is transferred from the application to the SAN. The implementation of the T10PI standard ensures that data is validated as it moves through the data path using Cyclic Redundancy Check (CRC), from the application, to the HBA, to the storage, enabling seamless end-to-end integrity.

1.8.10 8 Gbps FC host interface

The DS5000 offers 8 Gbps Fibre Channel (FC) host attachment. Upon purchase of the DS5000, you must determine how many host ports you will need.

The DS5100 and DS5300 storage subsystems are field upgradable to 8 Gbps by installing the quad-port HIC.

There are up to four (two per controller) quad-port 8 Gbps FC host interface cards (HICs) available per DS5100 and DS5300 storage subsystem. They will be installed in pairs of two (one in each controller).

A DS5020 storage subsystem is not upgradable. Host attachment must be ordered with the initial purchase of the DS5020.

1.8.11 64 GB cache upgrade for the DS5100 and DS5300

With controller firmware version (CFW) 7.60, the DS5300 allows a cache size of 32 GB per controller. There are field upgrade options in different configurations available.

These options are available:

- 8 GB to 16 GB

- ▶ 8 GB to 32 GB
- ▶ 8 GB to 64 GB
- ▶ 16 GB to 32 GB
- ▶ 16 GB to 64 GB
- ▶ 32 GB to 64 GB

1.8.12 Apple Macintosh OS X

The DS5000 storage subsystems with the controller firmware version 7.77 or higher support Apple Macintosh OS X operating system.

1.9 More information

Refer to *IBM System Storage DS5000 Series Implementation and Best Practices Guide*, SG24-8024 for the actual implementation procedures.

The additional details and features of DS5000 family of products is available at <http://www.ibm.com/systems/storage/disk/midrange/>

2



IBM System Storage DS5000 hardware

This chapter describes the hardware and features of the current IBM System Storage DS5000 family. This section details the DS5000 products, which include the DS5100, DS5300, and the DS5020. The DS4000 products are not covered in this book.

The chapter also includes a description of additional hardware components that are essential for a complete storage solution. These include the EXP5000, EXP5060, and the EXP520, with cabling considerations.

The IBM System Storage DS5000 series is designed to meet today's and tomorrow's demanding open-systems requirements while establishing a new standard for life cycle longevity. Building on many decades of design expertise, the DS5000 storage system's architecture delivers industry-leading performance, real reliability, multidimensional scalability and unprecedented investment protection.

2.1 DS5100 and DS5300 storage subsystems

DS5100 and DS5300 offer increased performance and additional features when compared to their predecessors, the DS4000 family. Both machines can hold up to 448 drives if using EXP5000 expansions or up to 480 drives if using 8 EX5060 expansions. With that, you can store up to 960TB of data with the second option (8 EXP5060 expansions). With the introduction of SSD in DS5000 family, machines can be customized for both performance-oriented and capacity-oriented solutions.

Figure 2-1 shows a front view of the DS5000 storage subsystem.



Figure 2-1 DS5100 storage subsystem

The following two models are available:

- ▶ DS5100 (1818-51A)
- ▶ DS5300 (1818-53A)

The two models differ in the number of host ports, amount of cache for data, and performance in the initial package. DS5100 can be upgraded with all the features DS5300 has.

Models DS5100 (1818-51A) and DS5300 (1818-53A) have these features:

- ▶ Compact 4U rack-mountable enclosure.
- ▶ Utilizes new seventh generation dedicated ZIP ASIC engines on RAID controllers.
- ▶ Features Intel Xeon 2.8 GHz processor.
- ▶ Dual, redundant controllers.
- ▶ PCI Express x8 bus technology.
- ▶ Dedicated cache for data (base model has 8 GB cache) with enhanced diagnostics. Upgradeable to 32 GB per controller for a total of 64 GB per storage subsystem
- ▶ Dedicated processor memory of 2 GB per controller.
- ▶ Hot-swappable lithium-ion battery for backup and destaging data.
- ▶ Flash memory to store dirty data from cache during power outage.
- ▶ Two dedicated PCI Express buses for cache mirroring.

- ▶ Redundant, hot-swappable power supplies and fans.
- ▶ Hot-swappable interconnect module acts as midplane and houses the batteries.
- ▶ Supports RAID 0, 1, 3, 5, 6, and 10 (RAID 1+0).
- ▶ Supports RAID 1 and 10 dedicated mirrored drive pairs configurations.
- ▶ The ability to create a RAID 10 or 0 group on all available drives to maximize performance for a LUN.
- ▶ Host interface module selection now also includes dual-port 10Gbps iSCSI Host Interface Cards (HIC). This complements already available quad-port 4Gbps Fibre Channel (FC) HIC, quad-port 8Gbps FC HIC, and 1Gbps iSCSI HIC. They are all available as part of Miscellaneous equipment specification (MES) upgrade process.
- ▶ Supports an unlimited number of Global Hot Spare drives with the ability to enable/disable the copy back function (important for SATA drives).
- ▶ Supports eight host-side connections (two HICs) per controllers on both models.
- ▶ Host-side connections support
 - Fibre Channel Switched Fabric
 - Arbitrated Loop and Fibre Channel Direct Connections
 - Ethernet Direct Connection and Ethernet Switched Network (with iSCSI HIC)
- ▶ Supports sixteen 4 Gbps drive-side connections for both controllers. This allows a total of eight dual-redundant drive channel pairs to be implemented to support expansion enclosure additions.
- ▶ Redundant drive-side connections are designed to avoid any single-point of failure and maintain high availability.
- ▶ Supports up to 28 EXP5000s (or a mix of EXP5000s and EXP810s for migration purposes) for a total of 448 disks.
- ▶ Support up to eight EXP5060s for a total of 480 drives.
- ▶ Supports FC, SATA, FDE, SSD and SAS drives (with FC-SAS interposer).
- ▶ Supports a maximum of 20 Solid State Drives (SSDs) within EXP5000.
- ▶ Fully supports Fibre Channel/SATA intermix by allowing the simultaneous usage of SATA and Fibre Channel behind one DS5000 controller, allowing user flexibility and increased storage capacity utilization. It is also possible to mix disks of different size and technology inside one enclosure.
- ▶ Supports up to 512 host storage partitions that isolate LUNs for different servers or groups of servers.
- ▶ Supports up to 2048 volumes.
- ▶ Supports up to 2048 host logins.
- ▶ Supports 4096 command queue depth (maximum drive queue depth is 16).
- ▶ Supports logical volumes greater than 2 TB (when required and supported by the operating system).
- ▶ Supports shortwave Fibre Channel 4 and 8 Gbps host attachment.
- ▶ Supports 1 Gbps copper iSCSI host attachment.
- ▶ Support 10 Gbps optical iSCSI host attachment.

Note: 10 Gbps iSCSI uses optical SFP+ connectors and it needs a 10 Gbps Ethernet switch to connect to the host infrastructure.

1 Gbps host connections are supported via Switch and network infrastructure, but speed needs to be set to 1 Gbps in Storage Manager.

- ▶ Multiple heterogeneous server and operating system support (host kits required).
- ▶ Powerful On Demand functions: Dynamic Volume Expansion, Dynamic Capacity Expansion, and Dynamic RAID Level Migration. Dynamic Segment Size allows users to modify storage configurations on-the-fly without incurring any downtime.
- ▶ Remote Service Manager notifies IBM if there is an issue. Refer to Chapter 6, “IBM Remote Support Manager for Storage” on page 455 for more details.
- ▶ Dual 10/100/1000 Ethernet for out-of-band management to separate out-of-band management from service diagnostics for each controller.
- ▶ FlashCopy (premium feature) for up to 16 copies per base volume. There are two FlashCopies per default (without premium feature).
- ▶ VolumeCopy (premium feature).
- ▶ Remote Volume Mirroring: Metro Mirror, Global Mirror, and Global Copy (premium features) for up to 128 pairs.
- ▶ Standard DB-9 serial connection for service purposes.

Additionally, the DS5100 offers further value in flexibility, scalability, and investment protection by providing the ability to upgrade to a DS5300. The DS5100 provides excellent performance for dynamic storage consolidation solutions in the deployment stage, with the full assurance that this model can be upgraded to a DS5300 performance level if required.

2.1.1 DS5000 series product comparison

Figure 2-2 compares the DS5100 and DS5300. There is no difference between these models except for the internal front side bus speed. In earlier versions of code, there were restrictions on cache upgrade and number host channels, which no longer apply with the newest code. The DS5100 can be upgraded to the DS5300 by using the Performance Upgrade premium feature.

<i>Dual-controller system (unless noted)</i>	DS5100	DS5300
Number of host channels	Two (iSCSI only), Eight, or Sixteen	
Host channel topologies	4 Gbps FC, 8 Gbps FC, 1 Gbps iSCSI, 10 Gbps iSCSI	
Redundant drive channels	Sixteen 4 Gbps	
Max drives	448 FC/SATA, 480 SATA (with 8 EXP5060)	
Processor	Intel Xeon 2.8 GHz	
Processor memory (per controller)	2 GB	
XOR technology	Dedicated ZIP ASIC	
Internal Frontside Bus Speed	Reduced clock speed through internal code	Full clock speed
Internal controller bandwidth (per controller)	4 GB/s	
Data cache (min/max)	8 / 16 / 32 / 64 GB	
Cache Hold-up	Permanent	
Cache Mirroring	Two dedicated busses	
Cache bandwidth (single controller)	17 GB/s	

Figure 2-2 DS5100 / DS5300 comparison chart

Note: To attach 480 SATA drives to DS5000, 480 Drive Upgrade Premium Feature Pack is required.

2.1.2 DS5100 and DS5300 controller architecture

The DS5100 uses the same hardware as the DS5300. Both machines use two controllers connected through the interconnect module and there is no backplane. Only difference between the DS5100 and DS5300 is that, DS5100 has reduced internal bus speed controlled by controller firmware and lower amount of base cache (which can be upgraded to maximum amount). Both machines will be referred to as DS5000 in this chapter.

This section describes the architecture of a single controller. The DS5000 controller uses a seventh generation dedicated ZIP application-specific integrated circuit (ASIC) chip, which is designed and customized for a particular use, rather than intended for general purpose use. The ZIP ASIC is designed to support I/O operations and has a built-in hardware assist for RAID operations. The parity calculation is done by hardware which results in much greater performance compared to software solutions.

The ZIP ASIC chip calculates parity for data in cache and it uses a fast 17 Gbps bus to access it. The ZIP ASIC chip is one of the most important components in the architecture, so all disk and host chips are directly connected to it using fast PCI Express x8 2Gbps buses to achieve high performance. With the ZIP ASIC, there is also an Intel Xeon 2.8 GHz processor with dedicated 2 GB of memory for I/O control, management, and other general purposes.

There are two quad-port 4 Gbps FC chips, each controlling 4 drive channels. They are connected to the ZIP ASIC through two PCI Express x8 buses. One chip connects to four loop switches in the same controller and each loop switch has two 4 Gbps drive interfaces. The other one is connected to four loop switches in the other controller through the interconnect

module. Internal loop switches are used to have a switched connection to each disk channel port from both controllers.

Each controller has two host card interfaces which can connect to a variety of HICs including 4/8 Gbps FC HIC and 1/10 Gbps iSCSI HIC.

DS5000 uses two dedicated PCI Express buses for cache mirroring. The buses connect the ZIP ASICs on both controllers directly through the interconnect module.

Figure 2-3 shows the main components of the DS5000 controller.

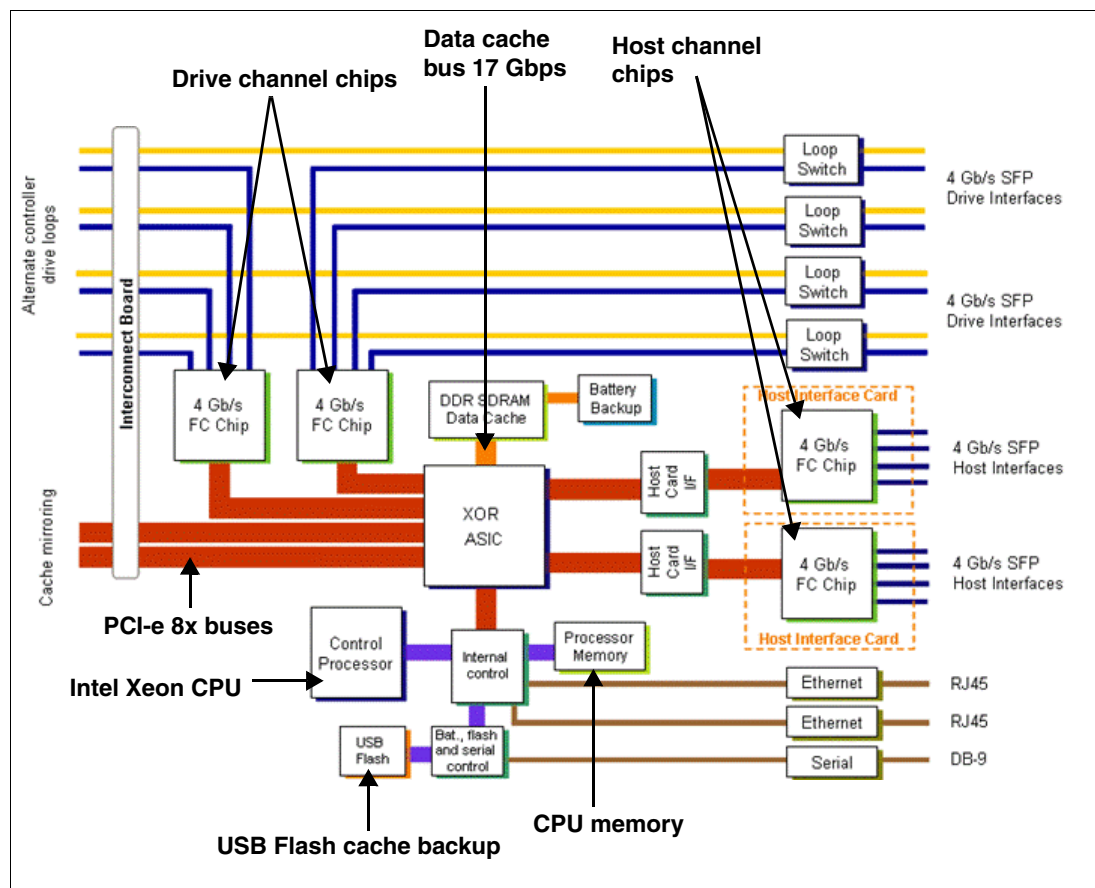


Figure 2-3 DS5000 controller's main components

Figure 2-4 shows the DS5000 controller with the top lid removed.

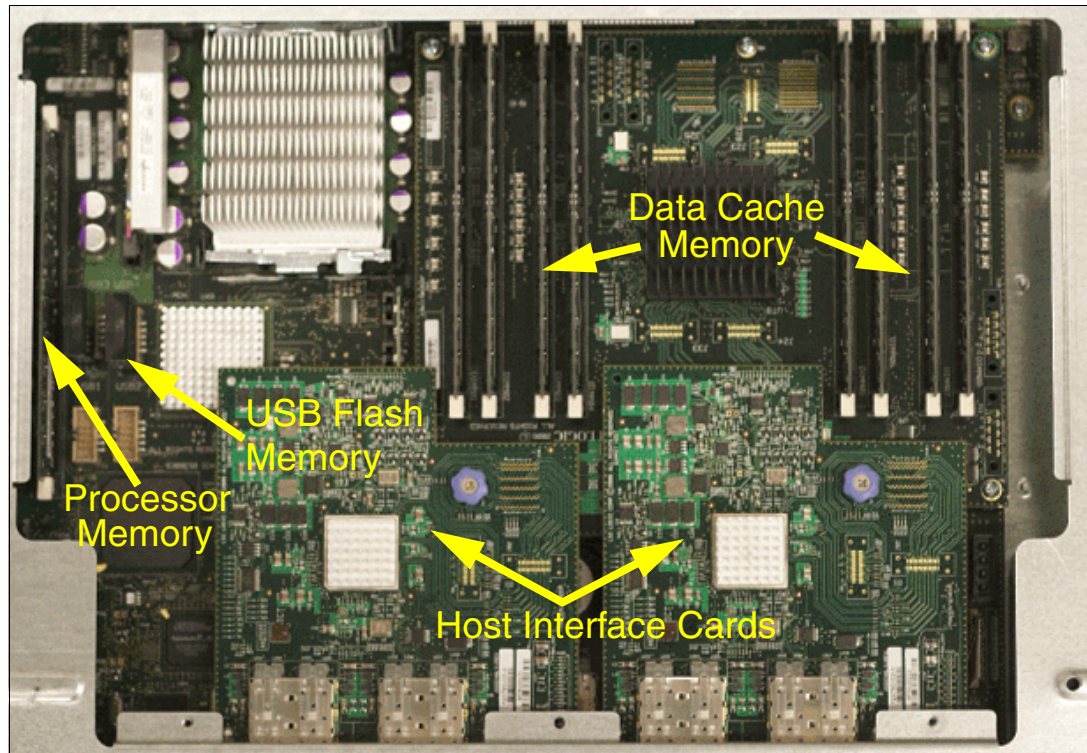


Figure 2-4 DS5000 controller with top lid removed

Figure 2-5 shows a DS5000 controller without the memory board and Host Interface Cards.

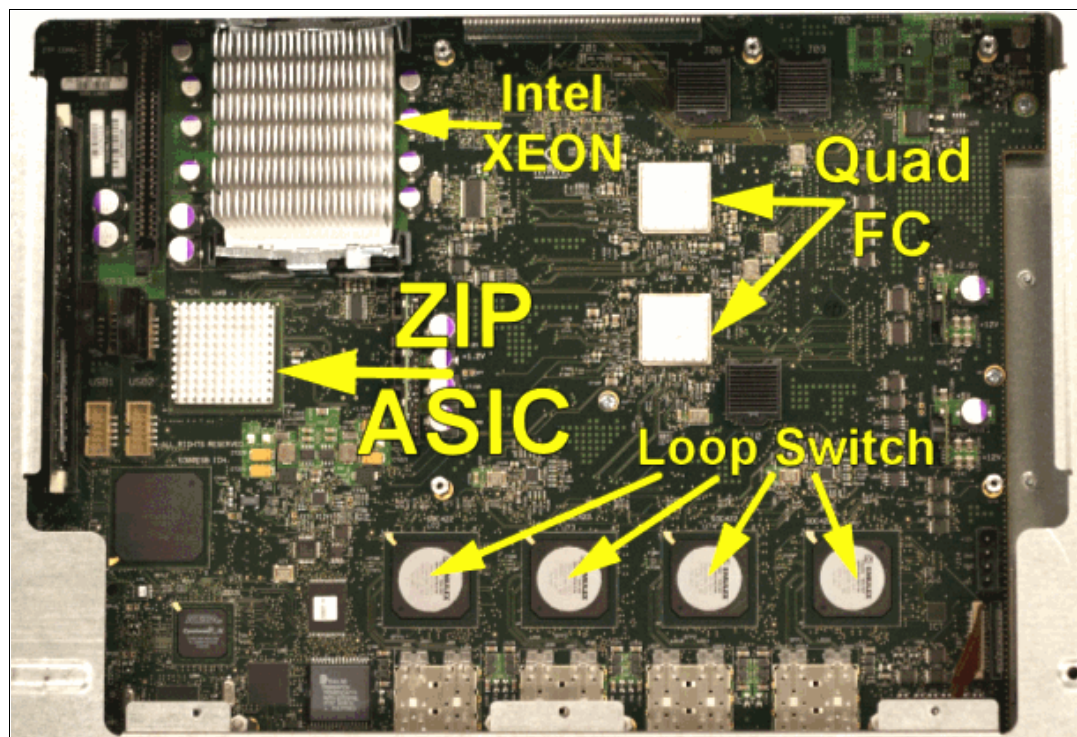


Figure 2-5 DS5000 controller without the memory board and Host Interface Cards

Data cache memory

The controller cache has a large amount of physical memory dedicated to I/O operations between the controller and hosts and between the controller and disk drives. It is logically and physically separate from the controller processor's memory and can participate in Direct Memory Access (DMA) operations with both host side and drive side physical channel adapters, as shown in Figure 2-6. Consequently, the controller's processor is not required to execute the data movement in and out of the cache memory. The controller cache is a significant contributor to the overall performance of the storage array. The use of the cache increases controller performance in several ways:

- ▶ The cache acts as a buffer so that host and drive data transfers do not need to be synchronized.
- ▶ If write-back caching is used, the host can send subsequent write commands before the data from a previous write operation has been written to a drive.
- ▶ The data for a read or write operation from the host may already be in the cache from a previous operation, thus eliminating the need to access the drive. This is referred to as "Reach Cache".
- ▶ If cache pre-fetch is enabled, sequential read access is optimized as cache pre-fetch, which makes it much more likely that a read operation will find its data in cache rather than have to read it from a disk drive. This is also referred to as "Read Ahead".

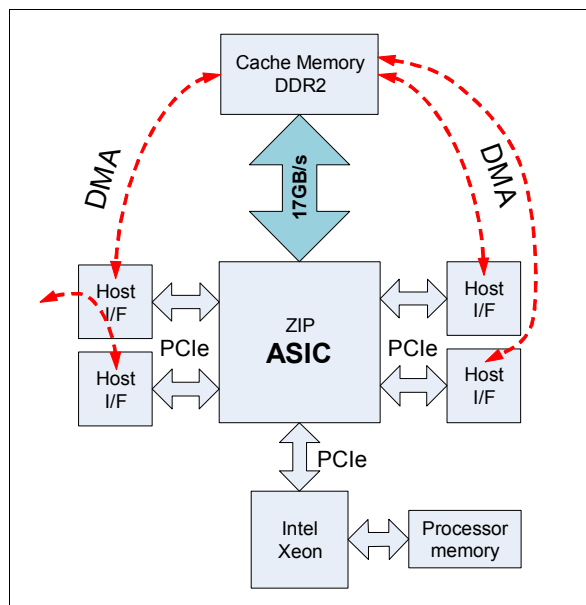


Figure 2-6 Cache memory access

Dirty data: A cache block that contains new data, which is not consistent with data on disk, is called dirty. The cache block holding the write data is dirty until the data is written to disk and the cache block becomes clean.

The cache may have dirty data in it. The cache memory is RAM, so if there is a power failure, the contents of the cache will be lost, including all the dirty data. There is no way for an application using the storage subsystem to tell exactly how many writes were lost in a case like this, so recovery can be very difficult or impossible. This severely limits the applicability of write caching to non-essential data like scratch data, temporary files, and so on. To circumvent this limitation, the controller can make the cache contents persist through power failures by using persistent cache backup devices.

Persistent cache backup devices is a new method implemented in the DS5000 family. The controller has persistent cache backup devices (USB flash memory) into which cache contents can be stored for an indefinite period of time. In this case, the controller also has a battery with enough capacity to let it save the full contents of the cache memory to the persistent cache backup devices in case of a power failure. The controller firmware turns off the batteries when the backup has been completed.

The state of the cache persistence mechanism is tied to the cache management subsystem and affects write caching directly. If the cache persistence mechanism fails for some reason, for example, the battery is missing in a battery-backed cache memory controller, write caching will be disabled for all volumes, except those that have the “cache without batteries” attribute set to true (see 3.6.7, “Cache parameters” on page 228 for more information).

When the controller loses power and dirty data is in the cache, the backup process starts (copying data from cache to flash memory). If power is restored by the time the backup is complete, normal operations continue. If power is *not* restored by the time the backup is complete, the controller disables the batteries and powers off. When it powers on, any dirty data in flash memory will be copied back to cache. Host I/O is supported while backup data is being restored. Normal power up continues as well. Restored data is immediately scheduled to be flushed to drives.

Note: Both data cache as well as flash memory are CRC protected.

Data flow

Figure 2-7 shows simplified data flow from host port to disk drive (not covering the data cache flow). This diagram shows the configuration where an array is built on one disk enclosure and two drive ports are used for I/O operations to one volume. If there are two volumes in the same array, the second one can be managed by controller B. For each volume you set, the default controller will manage it, which allows you to evenly load both controllers and all ports. In this example, there is a RAID 5 array group using five drives and one volume with the default controller A (preferred ownership) and a segment size of 256 KB. Host issues a 1 MB write request. Drives 1, 3, and p (parity) use port 8 in controller A and drives 2 and 4 use port 1 in controller B.

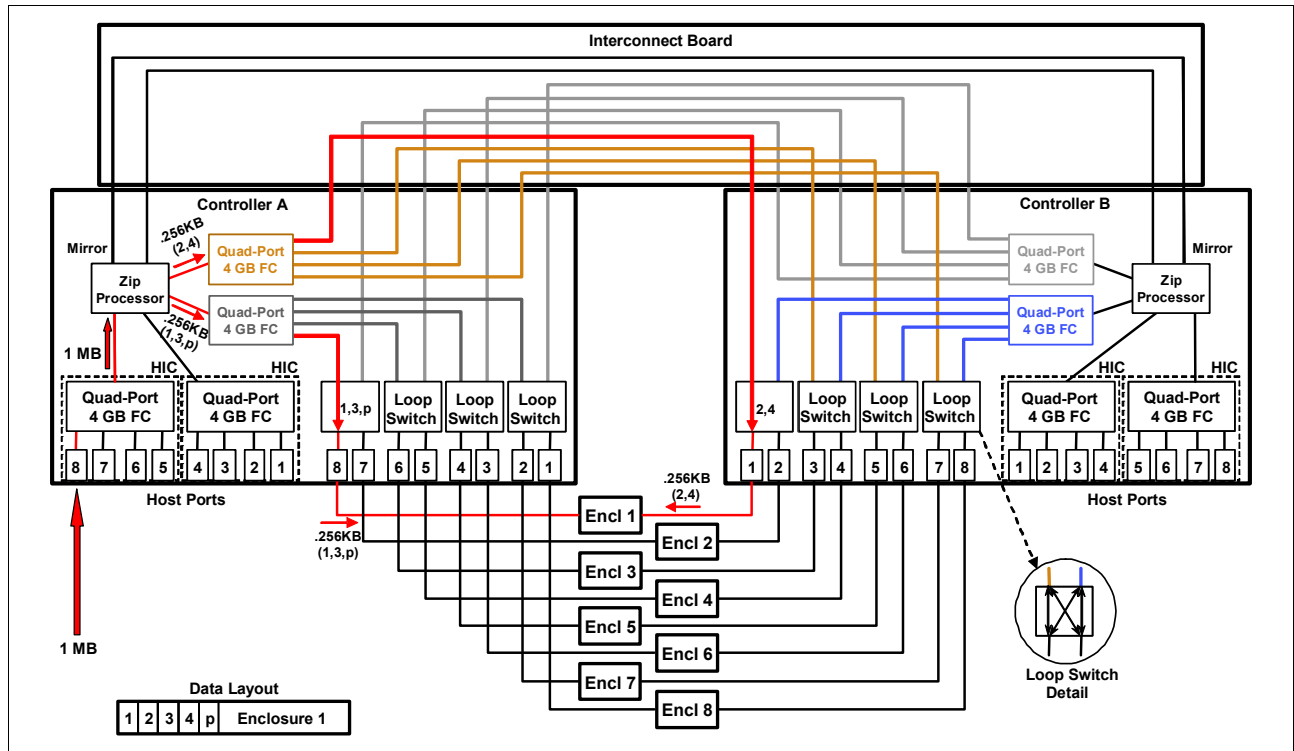


Figure 2-7 Data flow with one enclosure

In the example shown in Figure 2-8, the array is built using five enclosures and uses five drive ports to communicate. Note that drive number 2 is placed in the second enclosure in the second position in the enclosure, and so on ("barber pole" volume). If all drives are placed vertically (on multiple enclosures), but in the same position, for example, the first slot, five drive ports are used, but all in the same controller, using one (of two) quad disk port chips.

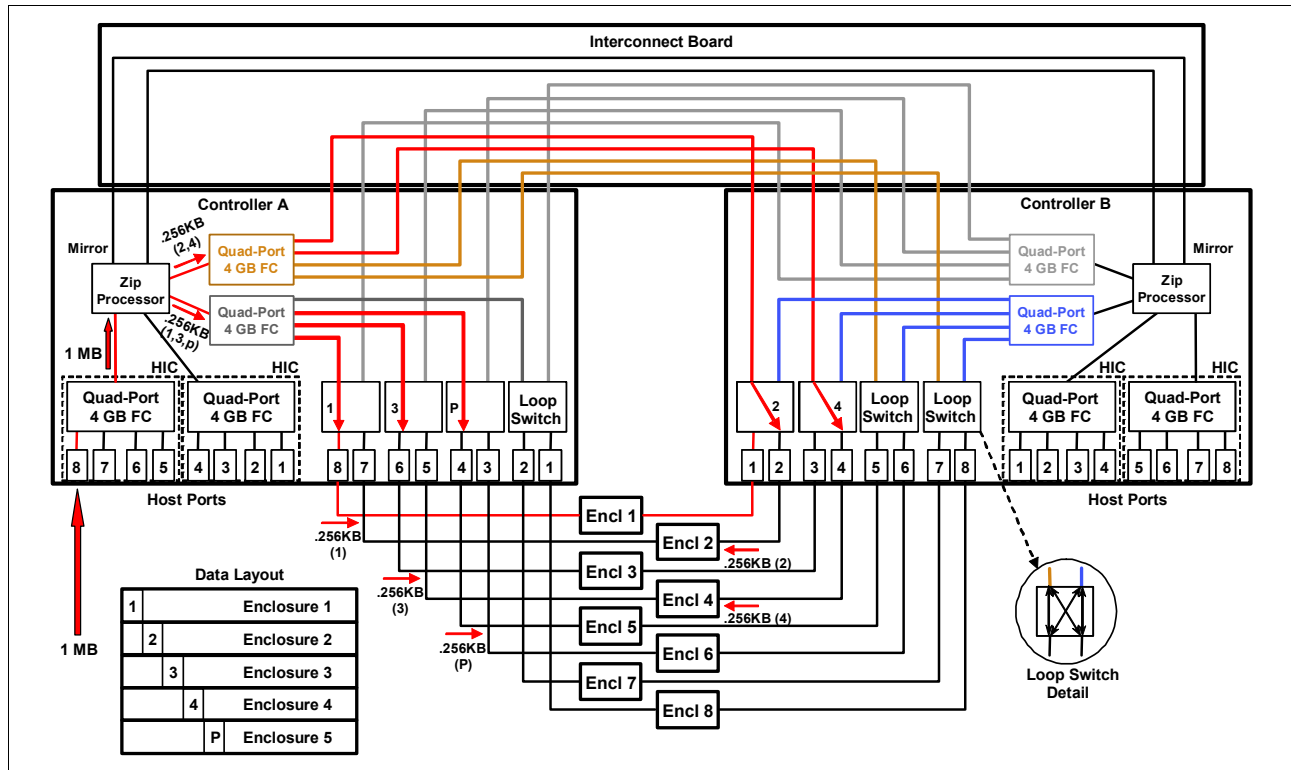


Figure 2-8 Data flow with more expansions

Note: Normally, when both controllers are running, loop switch ports in controller A access odd drives in each drive enclosure. Loop switch ports in controller B access even drives in each drive enclosure. Each controller has connections to all drive ports in both controllers and can communicate to all drives. When the controller fails, the running one uses its ports to communicate to all drives.

Write operation steps

Here are the write operation steps:

1. Data comes through the host port of the preferred controller for the volume.
2. Data is written to cache.
 - a. If cache mirroring is enabled, cache without battery is disabled, the battery state is okay (or just cache without battery is enabled), data is also copied to the cache of the second controller.
 - b. If Enhanced Remote Mirroring is established for the volume, the remote copy procedure starts. If synchronous mode is used, data is copied to a remote DS5000.
 - c. If write caching is enabled, the host receives the message stating I/O is completed.
3. Data is written to drives of the array.
4. Depending on the number of drives, the local or second controller's ports are used for writing.
5. The cache block status is set to Clean.
6. The host receives the message stating I/O is completed (if it did not receive this message before).

Read operation steps

The read operation steps are:

1. A host requests data.
2. If data is in the cache, the data is sent to the host and I/O is completed.
3. Data is read from drives.
4. Data is copied into the cache.
5. The host receives the required data and I/O is completed.
6. If sequential reading is discovered, the next n segments are read and copied into the cache.

Cache block states

The cache block states are:

- ▶ **Empty:** During the start-of-day processing, the controller firmware will partition the cache memory into cache blocks (except for the part of cache memory reserved for various cache metadata). All these cache blocks will be put on the Free list and their state will be Empty.
- ▶ **Clean:** A cache block that contains data that is consistent with the data on disk drive is Clean.
- ▶ **Dirty Write-Through (Dirty WT):** A cache block that contains new data that is not consistent with data on a disk drive is Dirty. In the write-through cache mode, status is not returned to the host until the data has been written to the drives. The cache block holding the write data is Dirty Write-Through until the data is written to the disk drive and the cache block becomes Clean.
- ▶ **Dirty Write-Back (Dirty WB):** In the write-back cache mode, the status is returned to the host as soon as the data has been inserted into the cache. The cache block holding the write data is Dirty Write-Back until the data is written to the disk drive and the cache block becomes Clean.
- ▶ **Dirty Write-Back Mirrored (Dirty WBM):** If cache mirroring is enabled for the volume, the dirty cache block will be replicated to the cache memory in the other controller, and when the replication is completed, the cache block transitions from Dirty Write-Back to Dirty Write-Back Mirrored.

Figure 2-9 shows a simplified cache data flow for a DS storage subsystem. It does not cover remote mirror operations and parity calculations for RAID 3, 5, or 6. In the example, I/O size is equal or smaller than segment size.

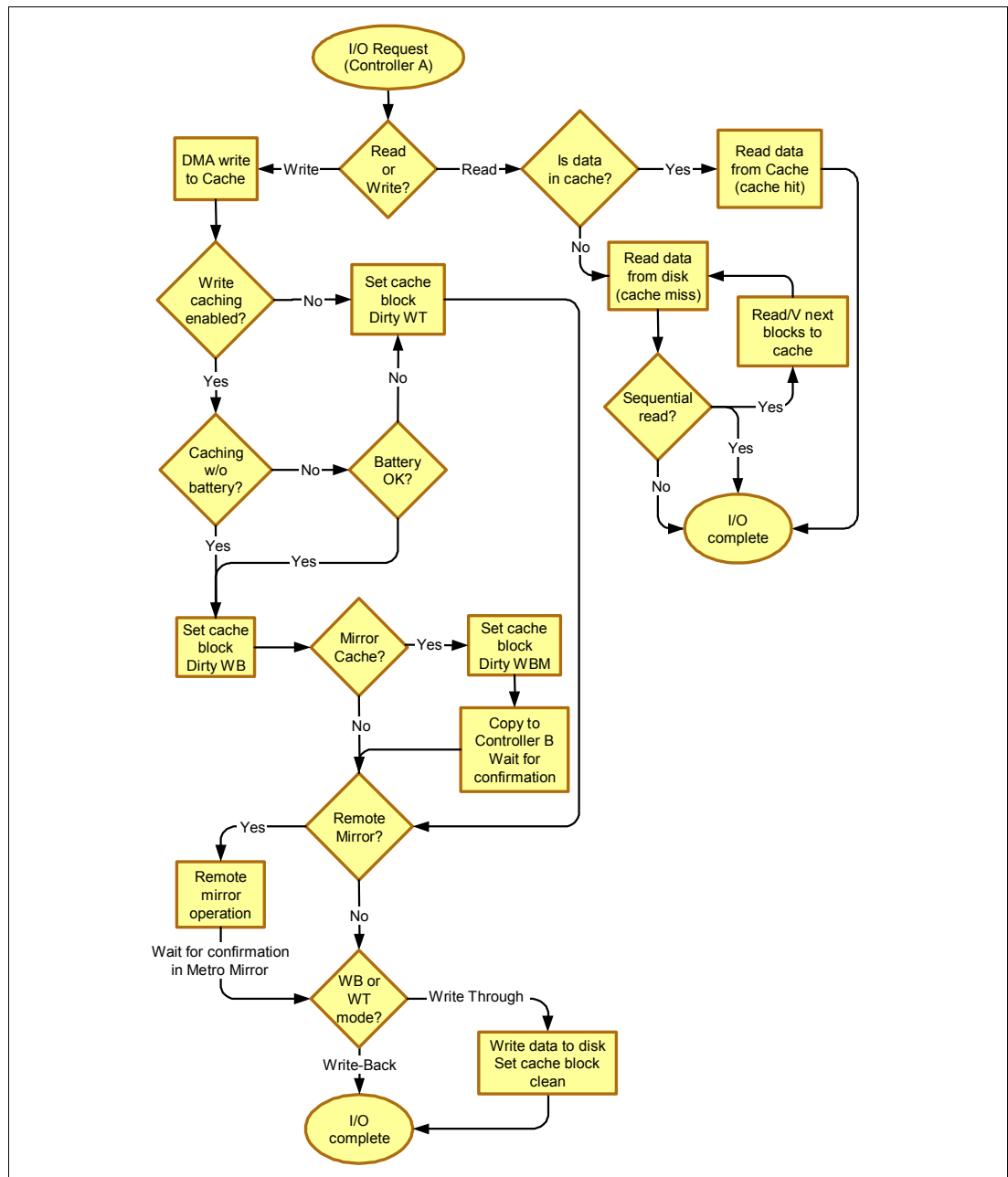


Figure 2-9 Simplified data cache flow diagram

2.1.3 DS5000 storage subsystem chassis design

In Figure 2-10, we show a diagram of the DS5000 modules.

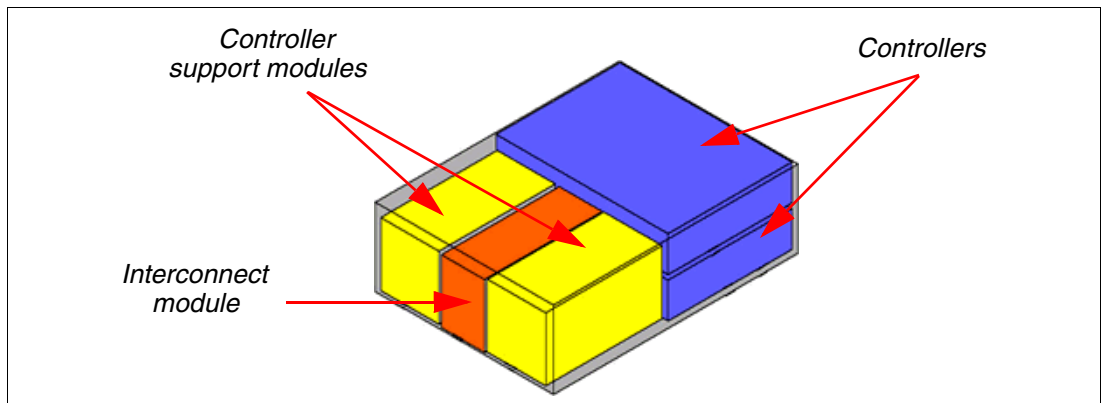


Figure 2-10 DS5000 modules

The DS5000 base controller unit is broken down into five primary Field Replaceable Units (FRUs). These FRUs are: two controller modules, two controller support modules, and one interconnect module:

- ▶ The controller modules contain the ASIC engines, the processors, cache memory, processor memory, flash memory for cache backup, and additional electronics that allow the DS5000 to process I/O.
- ▶ The controller support modules contain the power supplies, battery charging, and fans.
- ▶ The interconnect module holds the batteries and functions as a hot-swappable midplane. Controllers use this module to mirror the data cache and share disk loops ports.

All of the five FRUs and their individual components are hot-swappable and can be replaced while the system is online, allowing DS5000 users to maximize their uptime. See the corresponding service guide for specific replacement instructions that take place for the different FRUs. The latest service guide can be found at:

http://download.boulder.ibm.com/ibmdl/pub/systems/support/system_x_pdf/94y8393.pdf

Note: A DS5000 storage subsystem has no single point of failure; each module, including the midplane, is hot-swappable. When any single module fails, I/O operations continue.

2.1.4 DS5000 storage subsystem front view

The front section of the DS5000 storage subsystem contains the two controller support modules and the interconnect module.

The controller support modules are the units (FRUs) on the left and right. They each house a fan and a power supply. In order to replace the fan or power supply, it is necessary to remove the controller support module and replace the broken or defective part.

The interconnect module is the unit (FRU) between the two controller support modules. The interconnect holds the cache batteries and the hot-swappable midplane. When the interconnect module is removed, the DS5000 storage subsystem automatically suspends controller B, fails over all the LUNs to controller A, and continues to operate. The midplane has batteries, so write caching is disabled for the default settings of the LUNs. If you still want to use cache for writing, open Storage Manager, select a volume, and select **Logical Drive** → **Change** → **Cache settings** → **Enable write caching without batteries**. You can find more details about this topic in 3.6.7, “Cache parameters” on page 228.

Possible loss of data: When you use the feature Enable write caching without batteries, you can lose data in a cache when the batteries are removed or discharged and power fails.

When the interconnect module is put back in place, the DS5000 storage subsystem can revert back to normal operation. If the operating system uses non-AVT path failover drivers, you have to manually redistribute the LUNs to their respective owning controller (A or B). All the components depicted in Figure 2-11 are hot-swappable and can be replaced on-the-fly to ensure that users do not experience any downtime.

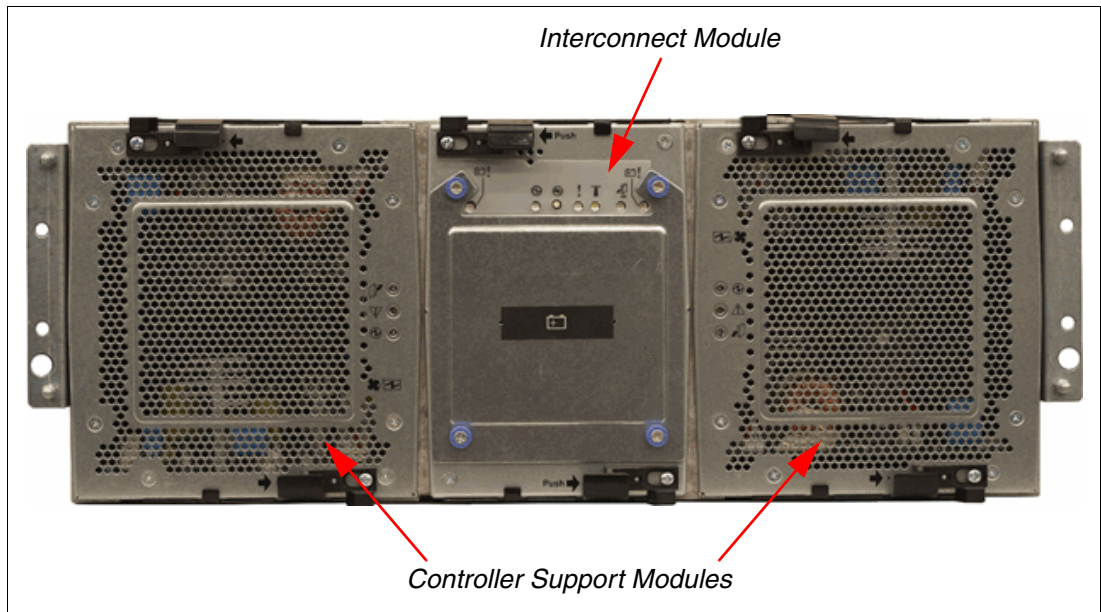


Figure 2-11 Front view of the DS5000 storage subsystem

2.1.5 Interconnect module and battery packs

The interconnect module provides the electrical communication path between the power supply fan units and allows their power supplies to load-share and to charge the cache-backup battery packs. It houses two cache-backup battery packs. Each battery pack contains batteries for both controllers (Figure 2-12). An interconnect module also works as a midplane, connecting disk loops and buses to mirror cache data between controllers.

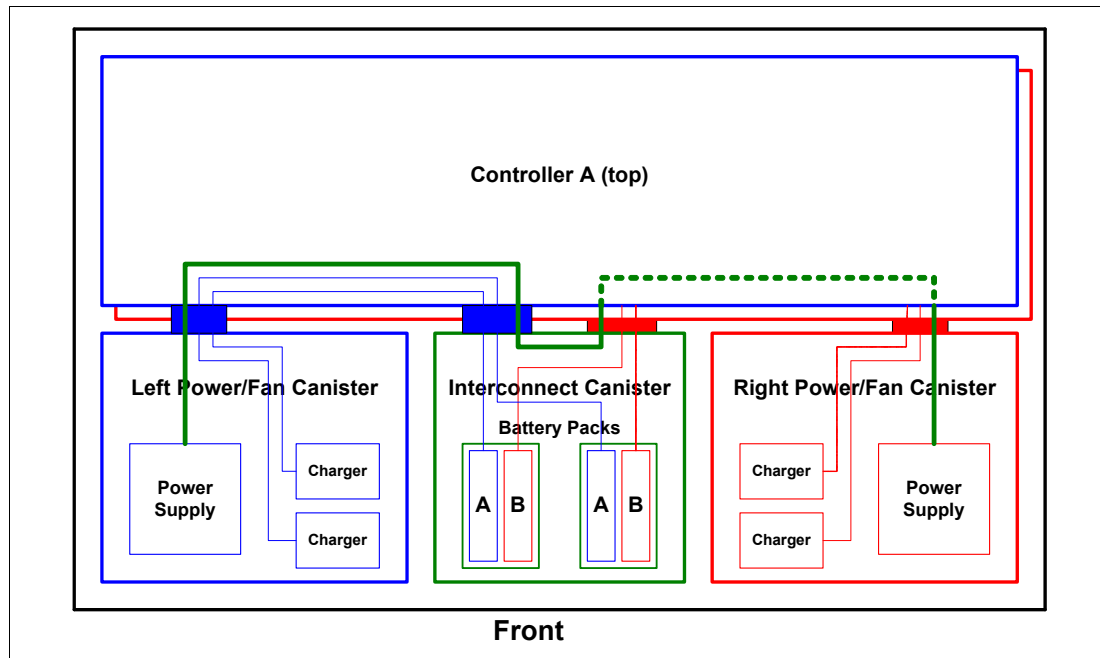


Figure 2-12 Power distribution

The DS5000 storage subsystem battery packs do not have expiration dates. Only replace a battery pack when the LEDs have indicated that they have failed (see 2.1.6, “DS5000 storage subsystem rear view” on page 37). You only have to replace the battery pack that failed, not both battery packs.

Because write-caching is disabled when either one of the backup battery packs fails, you should replace the failed battery pack as soon as possible to minimize any impact due to the write-caching function being disabled.

Figure 2-13 shows a DS5000 storage subsystem without a chassis (controller A is removed).

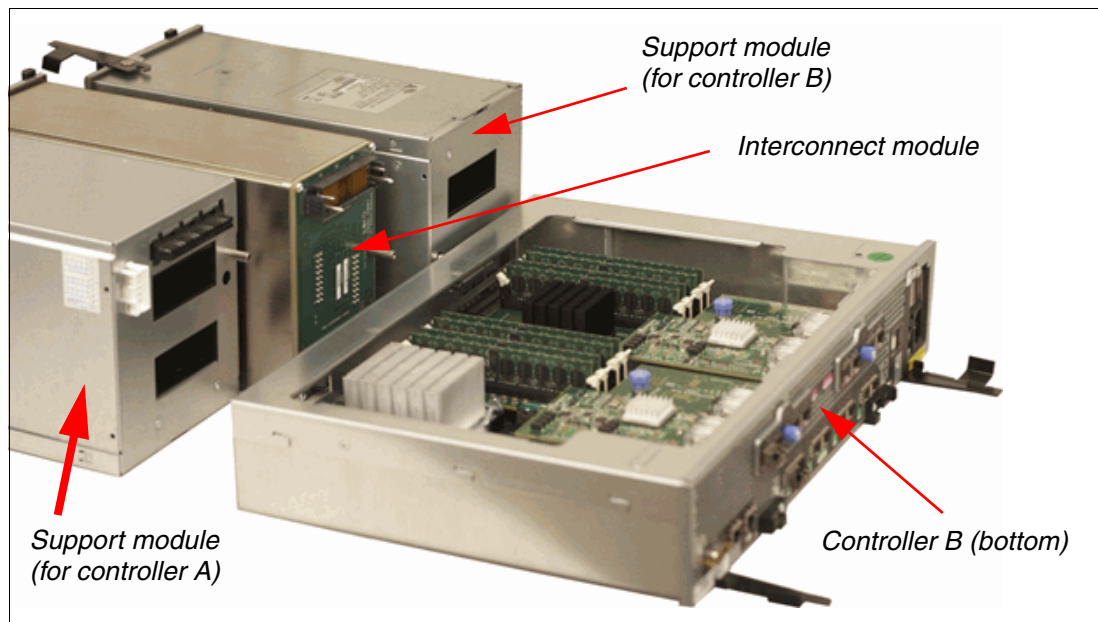


Figure 2-13 DS5000 storage subsystem without a chassis

Figure 2-14 shows the interconnect module with the removed battery.

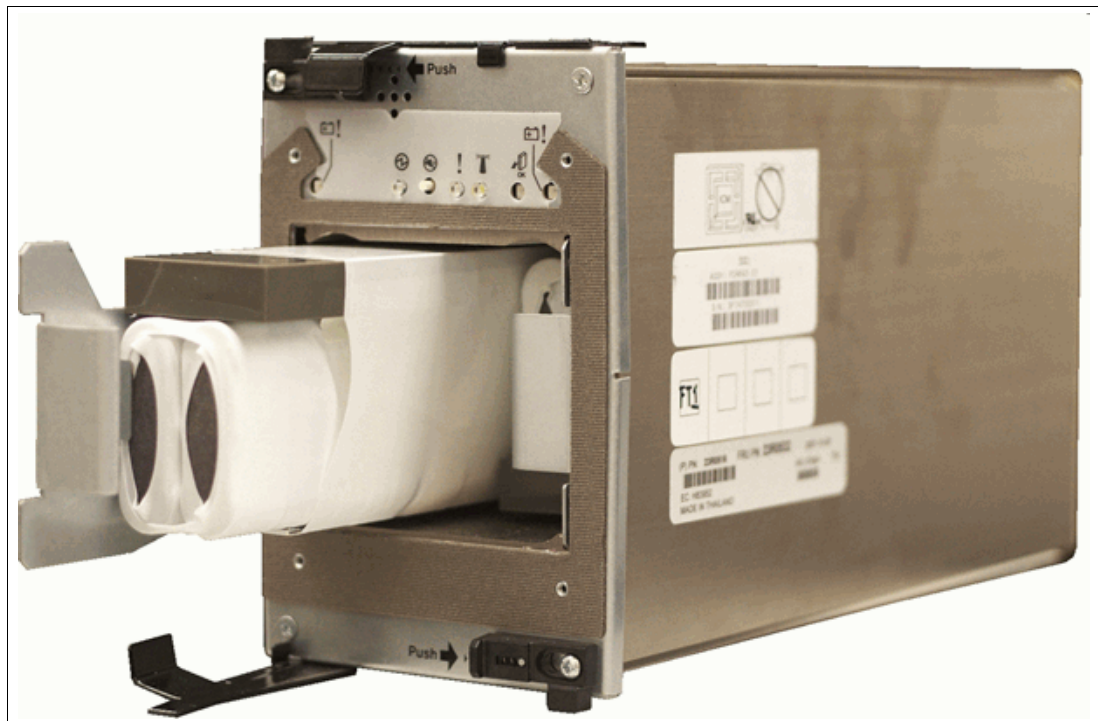


Figure 2-14 Interconnect module with removed battery pack

Smart Battery Backup Units (BBUs)

The Smart Battery Management feature allows the management facilities of the storage subsystem to take advantage of the capabilities provided by a “smart” battery unit. This feature provides a mechanism that enables the controller firmware to accurately determine how much capacity is left in the battery in a battery backup unit (BBU) and to access the battery’s state of health (SOH). This information allows the controller firmware to determine exactly how long the BBU can hold the cache up and take action as needed, for example, disable write-back caching if the battery backup facilities are insufficient.

Batteries are used to hold controller power to destage data from cache to flash memory. Their large capacity allows a load of 150W for a minimum of 30 minutes.

The battery can have three states:

- ▶ Full Charge: The battery is fully charged. The cache is set to Write Caching mode.
- ▶ Maintenance Charge: The battery is “trickle charging”. The cache state is unchanged.
- ▶ Learn Cycle (for Smart Battery): The battery is testing itself for capacity. The battery will retain enough charge to flush the cache. The cache state is unchanged.

Learn cycles

To properly calibrate the battery gas gauge, a fully charged smart battery unit must periodically be taken through a controlled discharge into the discharge load. The battery gas gauge is properly calibrated when the charge level decreases to a predetermined threshold. The threshold varies with the specific hardware design of the smart battery unit. Once the battery is discharged to the predetermined threshold, it is then fully recharged, following any required rest period. This controlled discharge, followed by a rest period, followed by a charge, is referred to as a *learn cycle*.

Learn cycles occur automatically at scheduled intervals. The time between learn cycles is based on the start time of each learn cycle so that the period remains constant, regardless of the length of each cycle. The learn cycle interval is scheduled in weeks (the default is 8 weeks), so that the start time for each learn cycle will occur on the same day of the week, at the same time of day.

Each controller receives backup power from one or more battery components. The controllers execute learn cycles on their respective set of battery components concurrently. In other words, controller A discharges and recharges its battery components at the same time that controller B discharges and recharges its battery components. If a controller receives backup power from more than one battery component or set of battery cells, the learn cycles for the battery components associated with that controller are executed sequentially. In other words, if there are two sets of battery cells that supply backup power to controller A, one set of cells for that controller is discharged/recharged before the second set of cells is discharged/recharged for that controller. In a duplex configuration, controller B is performing sequential discharges and recharges on its battery components at the same time that controller A is performing sequential discharges and recharges on its battery components.

The batteries are not totally discharged during a learn cycle. There is always power left to supply backup power for destaging data from cache to flash memory.

A controlled discharge begins once the following conditions are true:

- ▶ All batteries are fully charged.
- ▶ No batteries are overheated.

2.1.6 DS5000 storage subsystem rear view

The rear of the DS5000 shows the two controllers stacked on top of each other in a horizontal fashion. Controller A is located on the top and controller B is located on the bottom. The DS5100 and DS5300 system can have two Host Interface Cards in total. Both controllers are hot-swappable (Figure 2-15 and Figure 2-16).

The rear view of the subsystem varies depending on the version of HIC cards you have installed. Host connection is described in more detail in 2.1.8, “DS5000 storage subsystem host-side connections” on page 47.

You can have a:

- ▶ Fibre Channel version, which has one or two FC HICs installed per controller (Figure 2-15).
- ▶ iSCSI Version, which has one or two iSCSI HICs installed per controller (Figure 2-16).
- ▶ Mixed version, which has one FC and one iSCSI HIC installed.

Notice that controller A is positioned upside-down relative to controller B. It is important to keep this in mind when connecting the back-end ports to hosts and drive-side expansion enclosures, as we will discuss later.

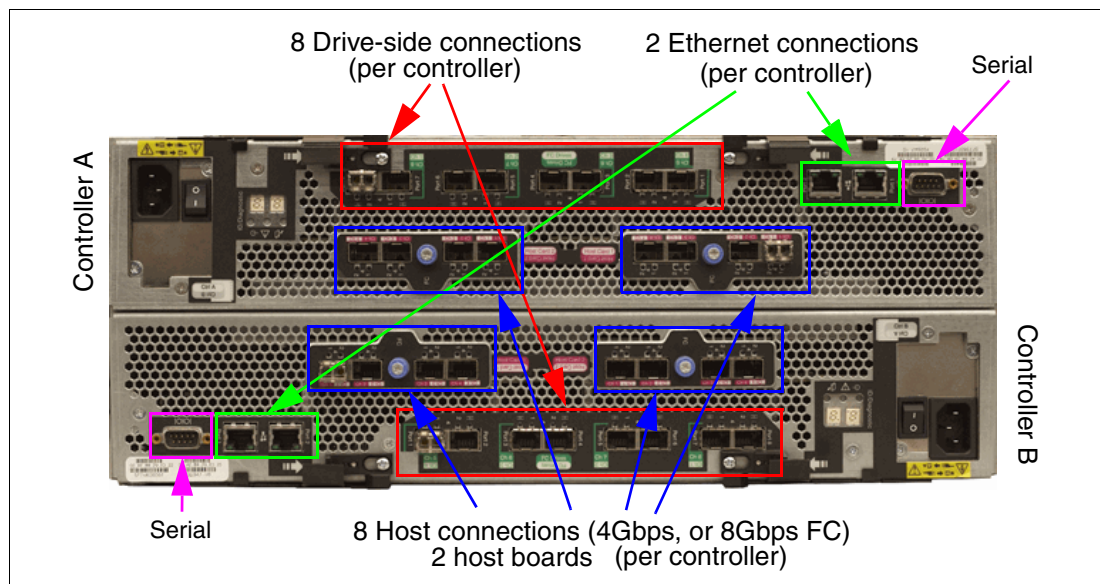


Figure 2-15 Rear view of the DS5000 storage subsystem: FC version

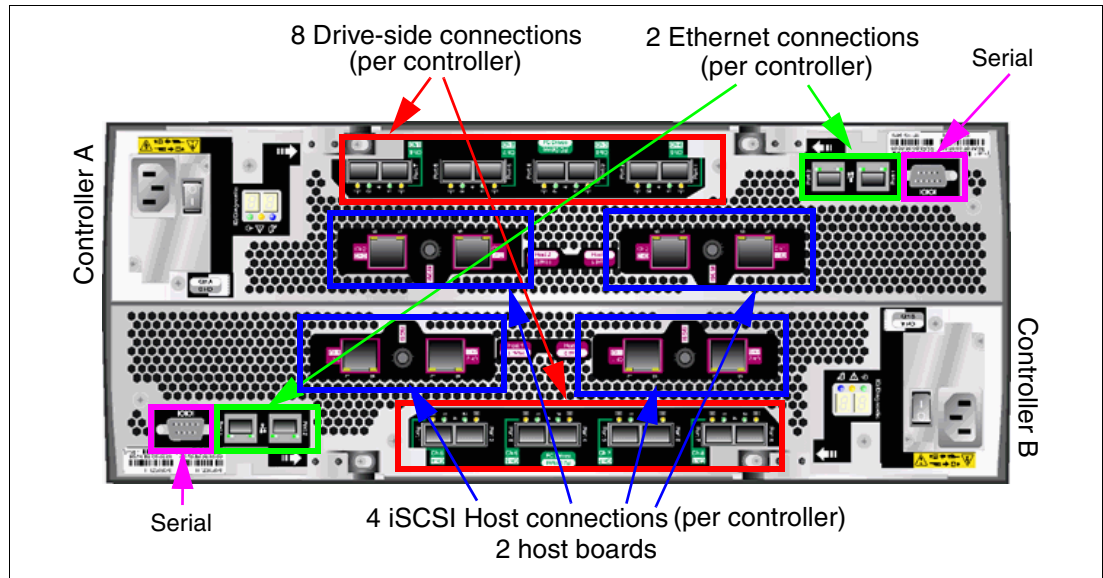


Figure 2-16 Rear view of the DS5000 storage subsystem: iSCSI version

Each controller is also equipped with two Ethernet RJ45 connectors and one DB-9 serial port. These controllers are discussed in 2.1.10, “DS5000 storage subsystem additional connections” on page 54.

2.1.7 DS5000 storage subsystem LED indicator lights

LED indicator lights allow the DS5000 to communicate with the user. There are four main components with LEDs: front bezel panel, RAID controllers, controller support modules, and the interconnect module.

Front bezel LEDs

Figure 2-17 shows the front bezel panel of the DS5000 storage subsystem and its LED indicator lights.

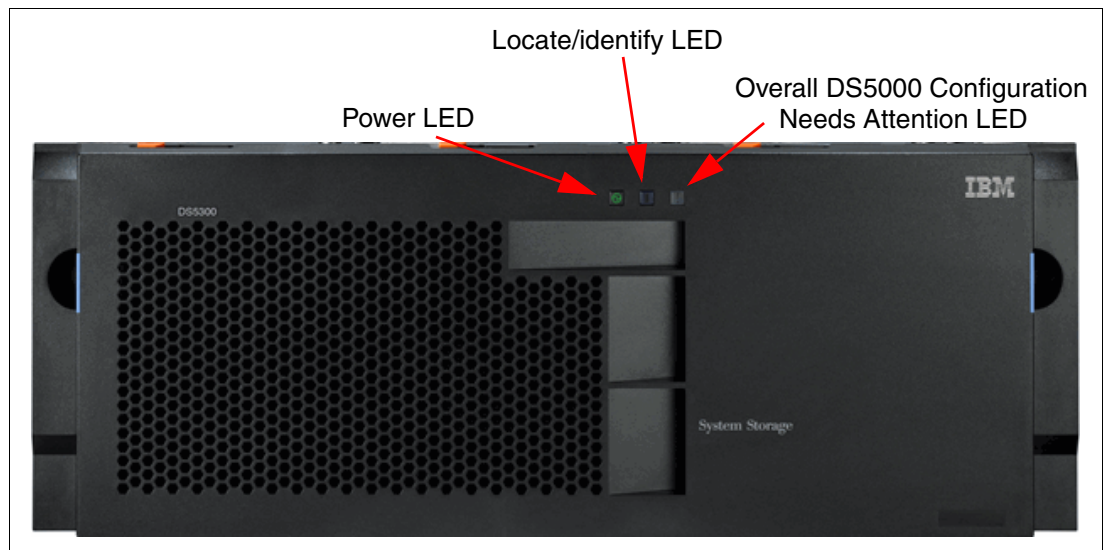


Figure 2-17 Front bezel LEDs

Important: The displayed order of the Overall Configuration Needs Attention and Locate/Identify LEDs on the interconnect-battery unit are reversed when the bezel is removed. See “Interconnect module LEDs” on page 46 for more information.

The LEDs are:

- ▶ Power LED (green):
 - On: Storage subsystem is powered on.
 - Off: Storage subsystem is powered off.
- ▶ Locate/identify (blue):
 - Off: Normal status.
 - On: Storage subsystem locate.

Note: This LED is shown as white (and displayed in a different order) on the interconnect-battery unit when the DS5000 storage subsystem bezel is removed.

- ▶ Overall DS5000 storage subsystem configuration needs attention (amber):
 - Off: Normal status.
 - On: One or more failures exist either in the storage system chassis or expansion enclosures.

RAID controller LEDs

The LEDs on the RAID controllers serve as indicators of key information (Figure 2-18).

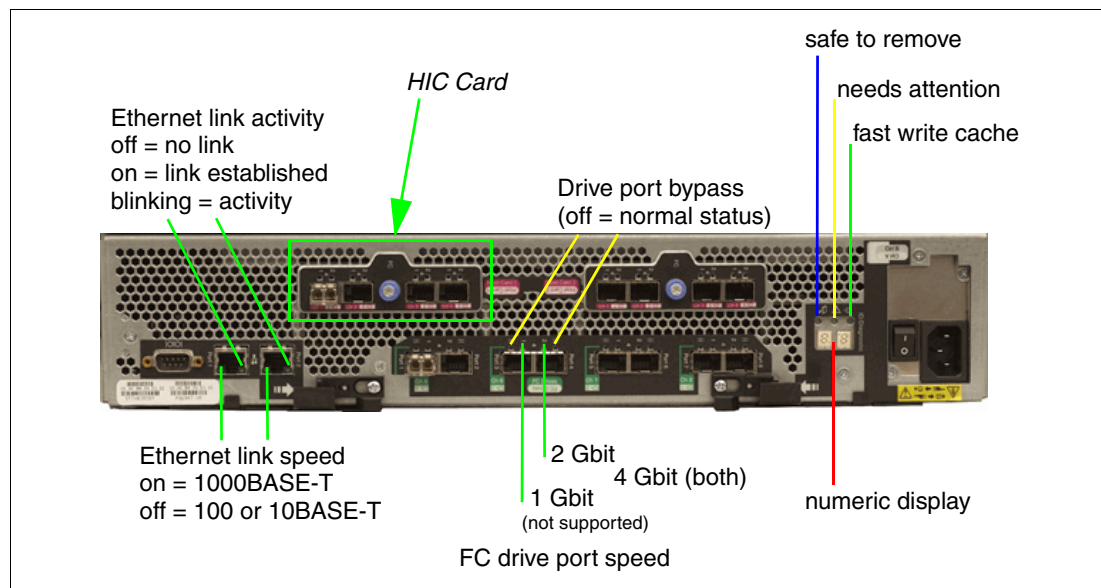


Figure 2-18 RAID controller LEDs (controller B): FC HIC version

Figure 2-23 labels each LED and the descriptions of each LED number are listed in Table 2-1 on page 42 and Table 2-2 on page 43.

There are four different HIC cards available. The following figures illustrate the LEDs and their usage for each host port:

- ▶ Figure 2-19 describes the LEDs for a 4 Gbps FC HIC.
- ▶ Figure 2-20 describes the LEDs for a 8 Gbps HIC.
- ▶ Figure 2-21 describes the LEDs for a 1 Gbps iSCSI HIC.
- ▶ Figure 2-22 describes the LEDs for a 10 Gbps iSCSI HIC.

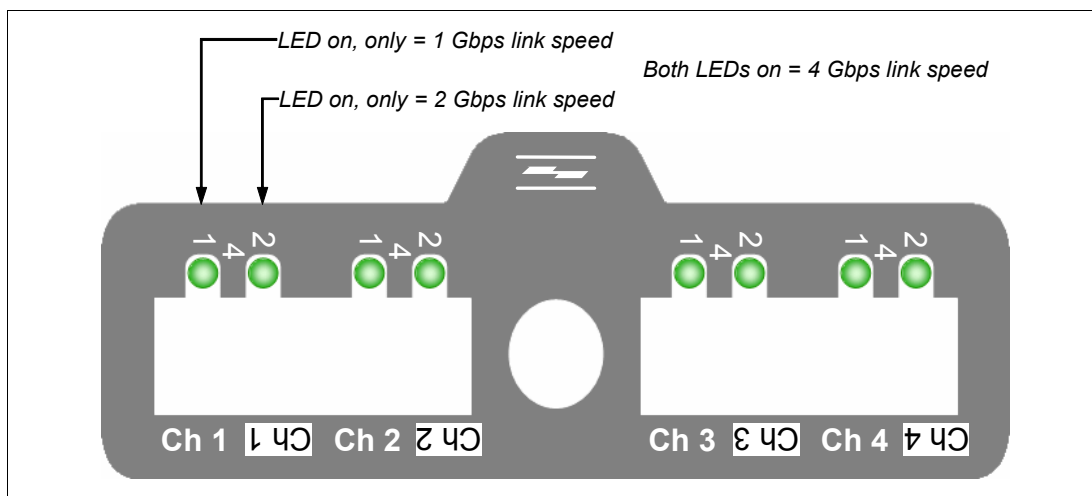


Figure 2-19 4 Gbps HIC faceplate design

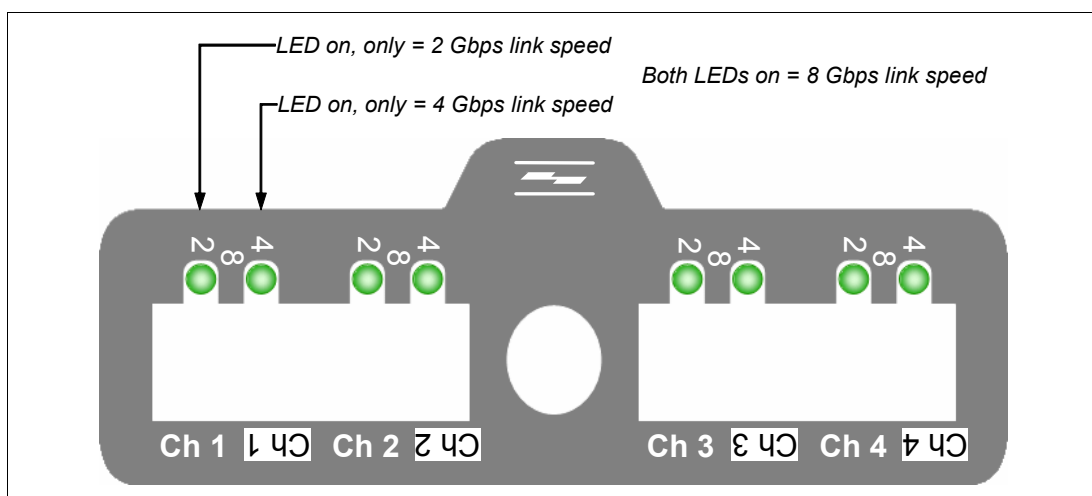


Figure 2-20 8 Gbps faceplate design

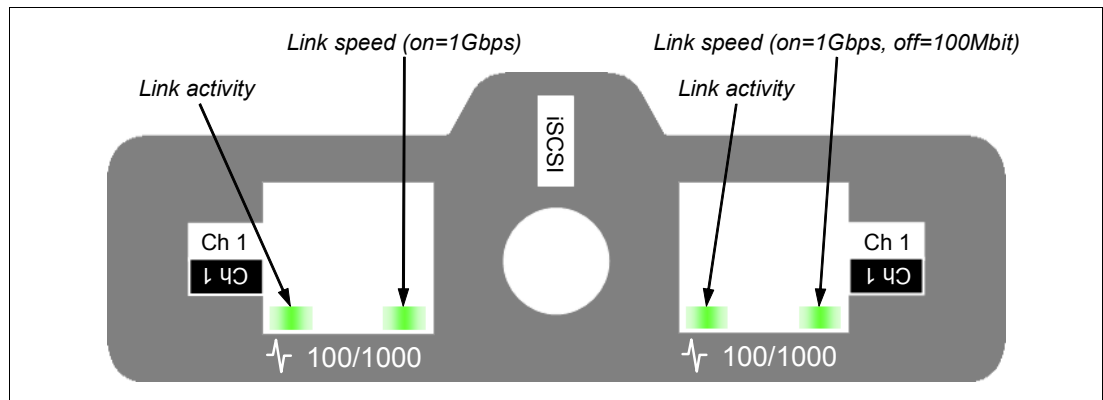


Figure 2-21 1 Gbps iSCSI faceplate design

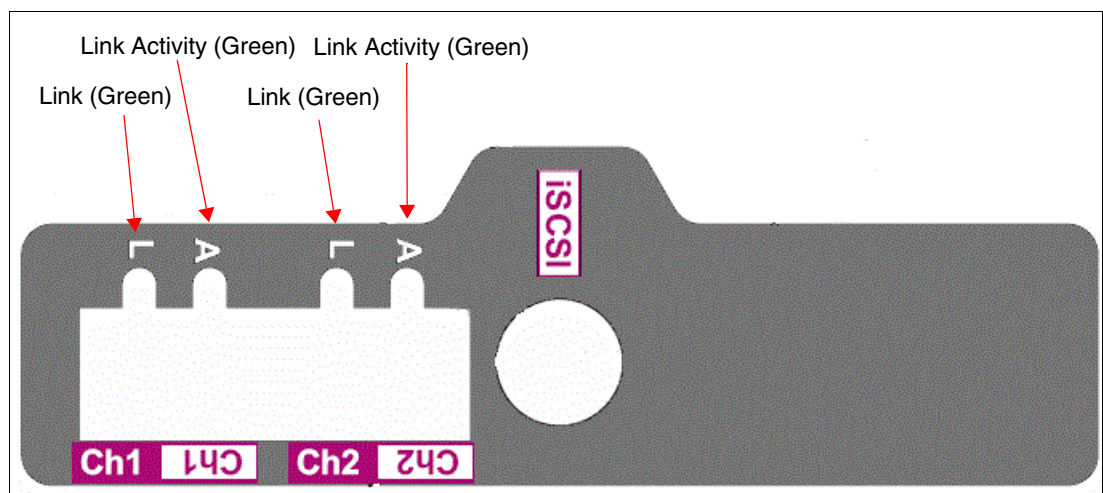


Figure 2-22 10 Gbps iSCSI faceplate design

Note: 10 Gbps iSCSI HIC uses optical SFP+ connectors.

Figure 2-23 shows details about the controller LEDs and their status.

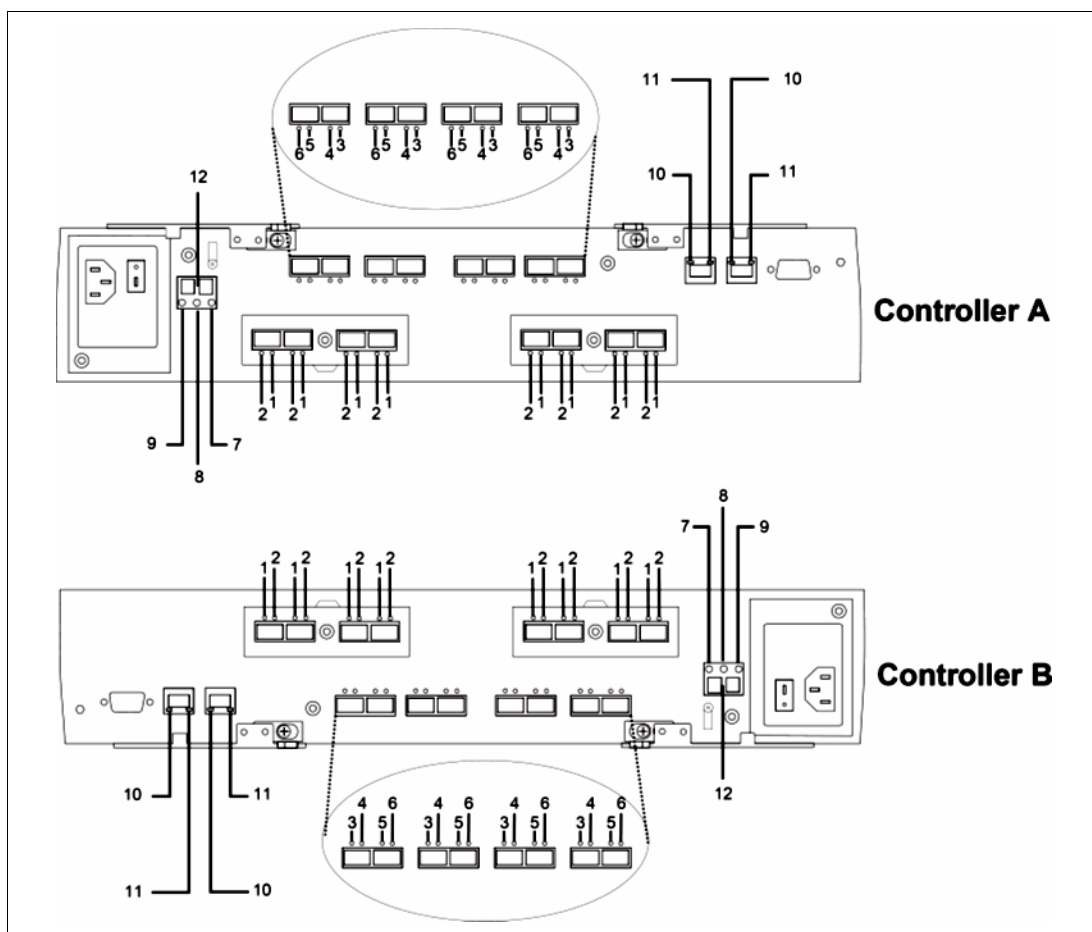


Figure 2-23 DS5000 storage subsystem RAID controller rear LEDs

Descriptions of each LED number shown in Figure 2-23 are listed in Table 2-1 on page 42 and Table 2-2 on page 43.

Table 2-1 DS5000 storage subsystem RAID controller rear LEDs description

Number	LED	Normal Status	Problem Status
1, 2	Host channel LEDs	See Table 4-2 on page 129	
3	Drive port bypass	Off	On (Amber) - Drive port bypass problem
4	Drive channel speed L1	See Table 4-2 on page 129	
5	Drive channel speed L2	See Table 4-2 on page 129	
6	Drive port bypass	Off	On (Amber) - Drive port bypass problem
7	Service Action Allowed (SAA)	Off	On (Blue) - Safe to remove
8	Needs attention	Off	On (Amber) - Controller needs attention (controller fault or controller is offline)
9	Cache active (Green)	On - Data in cache Off - No data in cache	N/A

Number	LED	Normal Status	Problem Status
10	Ethernet link speed (Green)	Off - 100BASE-T or 10BASE-T On - 1000BASE-T	N/A
11	Ethernet link activity	On - Link established Blinking - Activity	Off - No link established
12	Numeric display	Diagnostic LED: On - Diagnostic code is displayed. Diagnostic LED: Flashing - Controller enclosure ID is displayed.	See "Numeric display" on page 44

Table 2-2 Host and drive channel LED definition

HIC version	L1 (Label)	L2 (Label)	Definition
4 Gbps FC	Off (1 Gbps)	Off (2 Gbps)	When both LEDs for a host or drive channel are off, this indicates one or more of the following conditions: <ul style="list-style-type: none"> ► The host or drive channel ports are bad. ► An SFP module is inserted with no Fibre Channel cable attached. ► No SFP module is inserted in one or both of the host or drive ports in the channel.
	On (1 Gbps)	Off (2 Gbps)	The host channel is operating at 1 Gbps.
	Off (1 Gbps)	On (2 Gbps)	The host or drive channel is operating at 2 Gbps.
	On (1 Gbps)	On (2 Gbps)	The host or drive channel is operating at 4 Gbps.
8 Gbps FC	Off (2 Gbps)	Off (4 Gbps)	When both LEDs for a host channel are off, this indicates one or more of the following conditions: <ul style="list-style-type: none"> ► The host channel ports are bad. ► An SFP module is inserted with no Fibre Channel cable attached. ► No SFP module is inserted in one or both of the host ports in the channel.
	On (2 Gbps)	Off (4 Gbps)	The host channel is operating at 2 Gbps.
	Off (2 Gbps)	On (4 Gbps)	The host channel is operating at 4 Gbps.
	On (2 Gbps)	On (4 Gbps)	The host channel is operating at 8 Gbps.
1 Gbps iSCSI	Off (Link)	Off (Speed)	When both LEDs for a host channel are off, this indicates one or more of the following conditions: <ul style="list-style-type: none"> ► The host channel ports are bad. ► No Ethernet connectivity.
	On/blink (Link)	Off (Speed)	100 Mbps Ethernet connection established, transfer data (blinking).
	On/blink (Link)	On (Speed)	1000 Mbps Ethernet connection established, transfer data (blinking).

HIC version	L1 (Label)	L2 (Label)	Definition
10Gbps iSCSI	Off (Link)	Off (Activity)	When both LEDs for a host channel are off, this indicates one or more of the following conditions: <ul style="list-style-type: none"> ▶ The host channel ports are bad. ▶ No Ethernet connectivity.
	On (Link)	Off (Activity)	10 Gbps Ethernet connection established, no activity.
	On (Link)	On (Activity)	10 Gbps Ethernet connection established, transfer data (blinking).

Numeric display

When the storage subsystem is operating normally, the 7-segment LED display shows the enclosure identification (enclosure ID) of the storage subsystem and the diagnostic LED flashes once every two seconds. The storage subsystem tray ID is normally set at the factory to either values 85 or 00. Verify that the attached storage expansion enclosures are not set to either of these enclosure IDs.

Important: Only use storage expansion enclosure IDs in the following range: 01-80. The rest of the IDs are used for diagnostic purposes and can lead to a misunderstanding.

If an error has occurred and the controller Needs Attention LED is on, the numeric display shows diagnostic information. The numeric display indicates the information is diagnostic by illuminating an LED that appears as a decimal point between the display numbers. The diagnostic LED turns off when the 7-segment LED display shows the storage subsystem enclosure ID. The 7-segment LED display shows various diagnostic codes as the controllers perform the startup process after each power cycle or reset. After diagnostics are complete, the current storage subsystem enclosure ID is displayed.

Diagnostic codes in the form of Lx, where x is a hexadecimal digit, indicate controller state information. In general, these codes are displayed only when the controller is in a non-operational state. The controller might be non-operational due to a configuration problem (such as mismatched controller types), or it might be non-operational due to hardware faults. If the controller is non-operational due to system configuration, the controller Needs Attention LED is off. If the controller is non-operational due to a hardware fault, the controller Needs Attention LED is on. The definitions for Lx diagnostic codes are listed in Table 2-3.

Table 2-3 Numeric display diagnostic codes

Value	Description
L0	Mismatched controller types.
L1	Missing interconnect-battery unit.
L2	Persistent memory errors.
L3	Persistent hardware errors.
L4	Persistent data protection errors.
L5	The alternate controller has incompatible firmware, but the automatic controller firmware synchronization (ACS) cannot be performed.
L7	A controller with a different controller submodel ID is inserted.
L8	Unsupported memory is present or memory is not populated in the correct memory slots.

Value	Description
L9	Link speed mismatch.
LB	Host card is not configured properly.
LC	There is an error in the configuration of the persistent cache backup device.
LD	Mixed cache Dual In-line Memory Modules (DIMMs).
LE	Uncertified cache memory DIMM size.
LF	Lockdown with limited SYMbol support.
LH	Controller firmware mismatch.
LL	Unable to access either midplane SBB EEPROM.
LN	Canister not valid for enclosure.
LP	Drive-port mapping tables not found.
LU	Start-Of-Day (SOD) reboot limit exceeded. Controller will go into this state when it reboots for 5 times to prevent continuous reboot.

Note: Lockdown code **88** can still be present in the older versions of controller firmware and it means that the controller is being held in reset by the other controller.

Controller support module LEDs

The controller support modules are located on the left side and the right side in the front section of the DS5000 storage subsystem, behind the front bezel panel. The two modules each contain the power supplies and fans that are needed to operate the DS5000 storage subsystem. The LED positions on the right and left power supply and fan units are in mirrored positions. The LED indicator lights are shown in Figure 2-24.

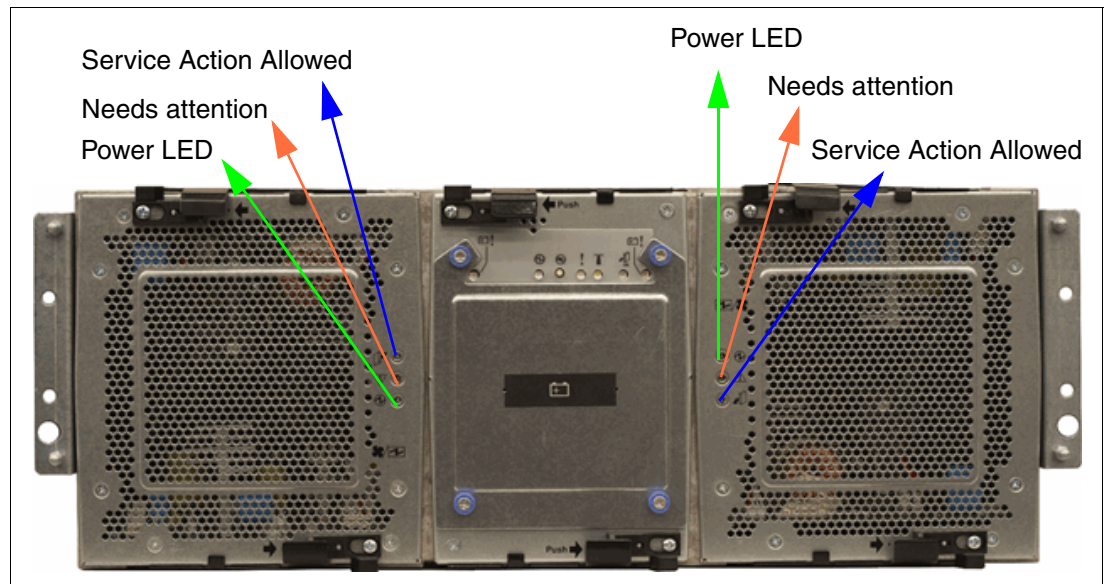


Figure 2-24 Controller support module (power supply/fan) LEDs

Note: The right power supply and fan unit is linked with RAID controller A. The left power supply and fan unit is linked with RAID controller B in the DS5000 storage subsystem.

The LEDs are:

- ▶ Power LED (green):
 - On: Power supply and fan unit is providing power.
 - Off: Power supply and fan unit is not providing power.
- ▶ Needs attention (amber):
 - Off: Normal status.
 - On: Power supply and fan unit need attention.
- ▶ Service action allowed (blue):
 - Off: Normal status.
 - On: Safe to remove.

Interconnect module LEDs

The interconnect module is located in the forward section of the DS5000 storage subsystem, behind the front bezel panel. It is located in between the two controller support modules. It holds the cache batteries and the removable midplane. The LED indicator lights are shown in Figure 2-25.

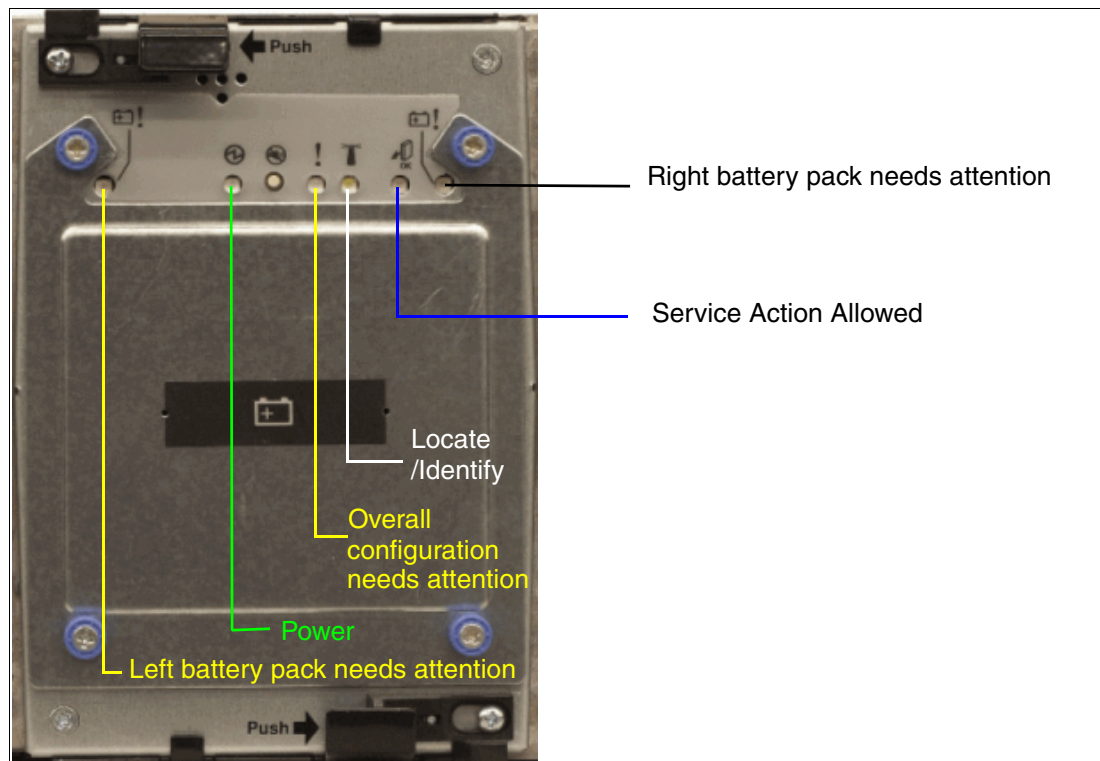


Figure 2-25 Interconnect module LEDs

The LEDs are:

- ▶ Battery needs attention (amber):
 - Off: Normal status.
 - On: Battery failed.
- ▶ Power LED (green):
 - On: Storage subsystem is powered on.
 - Off: Storage subsystem is powered off.
- ▶ Overall DS5000 storage subsystem configuration requires attention (amber):
 - Off: Normal status.
 - On: A component in the storage system has a problem.
- ▶ Locate/Identify (white, appears as blue when front bezel is installed):
 - Off: Normal status.
 - On: Storage subsystem locate/identify.
- ▶ Service action allowed (blue):
 - Off: Normal status.
 - On: Safe to remove.

2.1.8 DS5000 storage subsystem host-side connections

The DS5000 storage subsystem integrates the host-side and drive-side connections into the controller itself. DS5000 models use flexible Host Interface Cards that can be replaced by IBM service personnel only. Each DS5000 controller holds up to two Host Interface Cards (HICs) (see Figure 2-26).

These HICs are currently available:

- ▶ 4 Gbps FC HIC (four ports per HIC)
- ▶ 8 Gbps FC HIC (four ports per HIC)
- ▶ 1 Gbps iSCSI HIC (two ports per HIC)
- ▶ 10 Gbps iSCSI HIC (two ports per HIC)

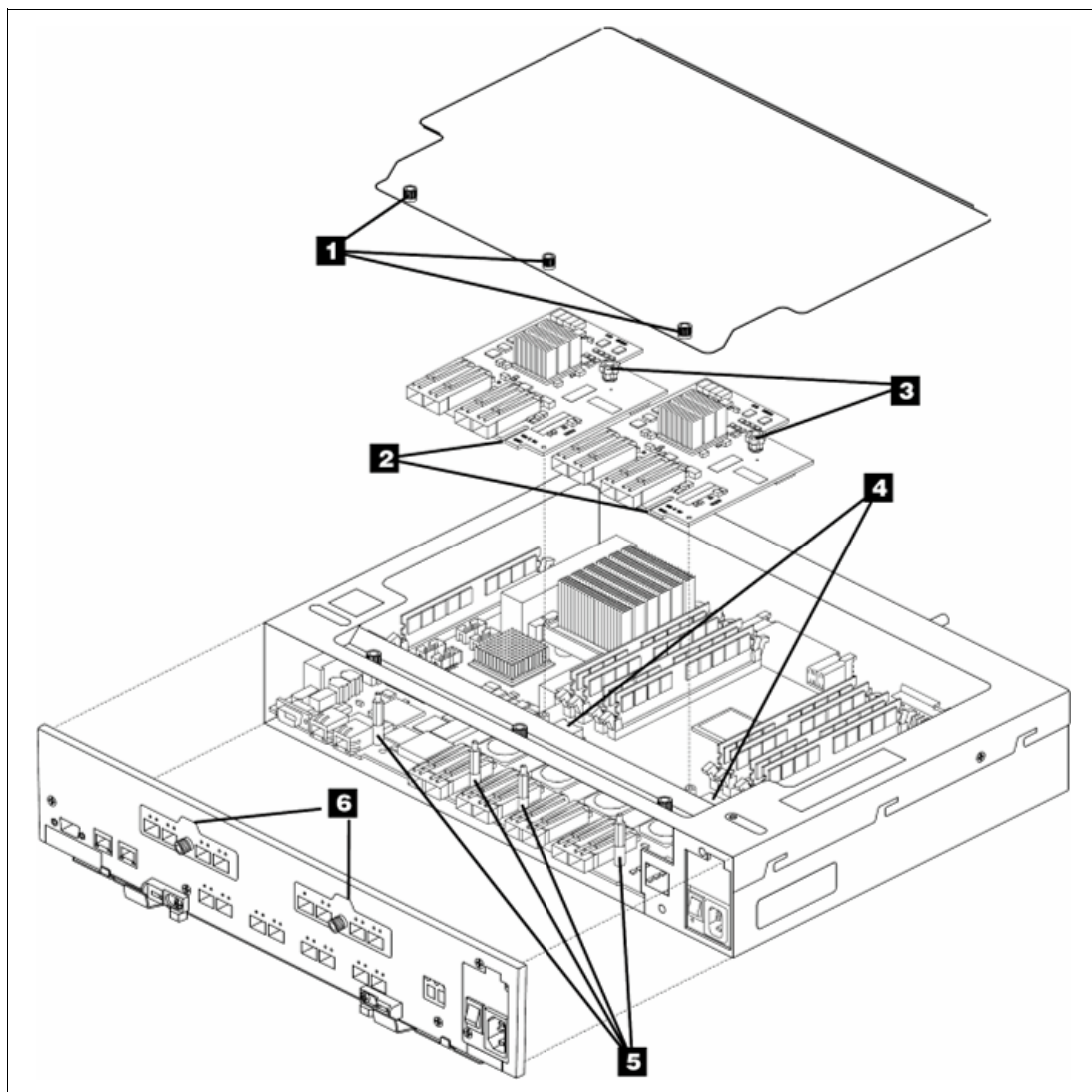


Figure 2-26 Controller exposed

The HICs noted as (2) are shown in Figure 2-26. Thumb screws (3) support easy replacement. Different faceplates (6) are used to describe the LED status of the host port LEDs. The faceplates are described in Figure 2-19, Figure 2-20, Figure 2-21, and Figure 2-22.

The DS5100 and DS5300 can hold up to sixteen host connections.

Host connections support Fibre Channel or iSCSI attachment (depending on the options ordered) through switches and direct connections. The host ports are labeled sequentially from 1 through 4, from left to right, on controller B (bottom) for both host cards. Conversely, they are labeled in reverse order, from 4 to 1, from the left to the right on controller A (top). As previously indicated, this is because controller A is installed “upside-down” relative to controller B.

Having sixteen independent host ports allows us to establish fully redundant direct connections to up to eight hosts.

It is important to match up host or fabric connections to the DS5000 storage subsystem by attaching one connection to each controller. In doing so, you take advantage of the DS5000

storage subsystem's ability to fail over and distribute the workload among the two controllers. For any given host, make sure to connect to the same host port number in the same host card on each controller. Remember that the right most host port on controller A and the left most host port on controller B are both host port #1, as shown in Figure 2-27.

Important: The DS5000 storage subsystem does not support a direct connection to a host if it is only connected to one of the two controllers.

Host ports channels are numbered in the following way (see Figure 2-27 and Figure 2-28):

- ▶ FC HIC 1 ports 1-4 have channel numbers 1-4.
- ▶ FC HIC 2 ports 1-4 have channel numbers 5-8 (in FC only version).
- ▶ FC HIC 2 ports 1-4 have channel numbers 3-6 (in mixed host type version).
- ▶ iSCSI HIC 1 ports 1 and 2 have channel numbers 1 and 2.
- ▶ iSCSI HIC 2 ports 1 and 2 have channel numbers 3 and 4 (in iSCSI only version).
- ▶ iSCSI HIC 2 ports 1 and 2 have channel numbers 5 and 6 (in mixed host type version).

According to Figure 2-27, host ports in controller B have numbers 1-8 from left to right, while the ports in controller A have them from right to left.

The DS5000 storage subsystem also fully supports Fibre Channel switched connections. Figure 2-27 shows how the DS5000 would be connected into dual-redundant fabrics.

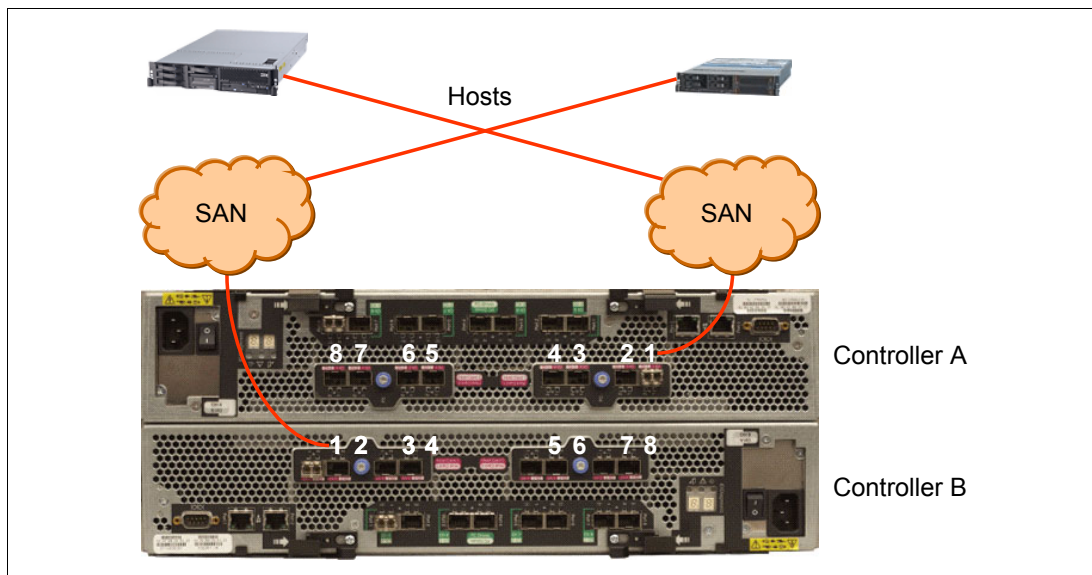


Figure 2-27 SAN connected hosts to DS5000 storage subsystem

According to Figure 2-28, host ports in controller B have numbers 1-6 from left to right, while the ports in controller A have them from right to left.

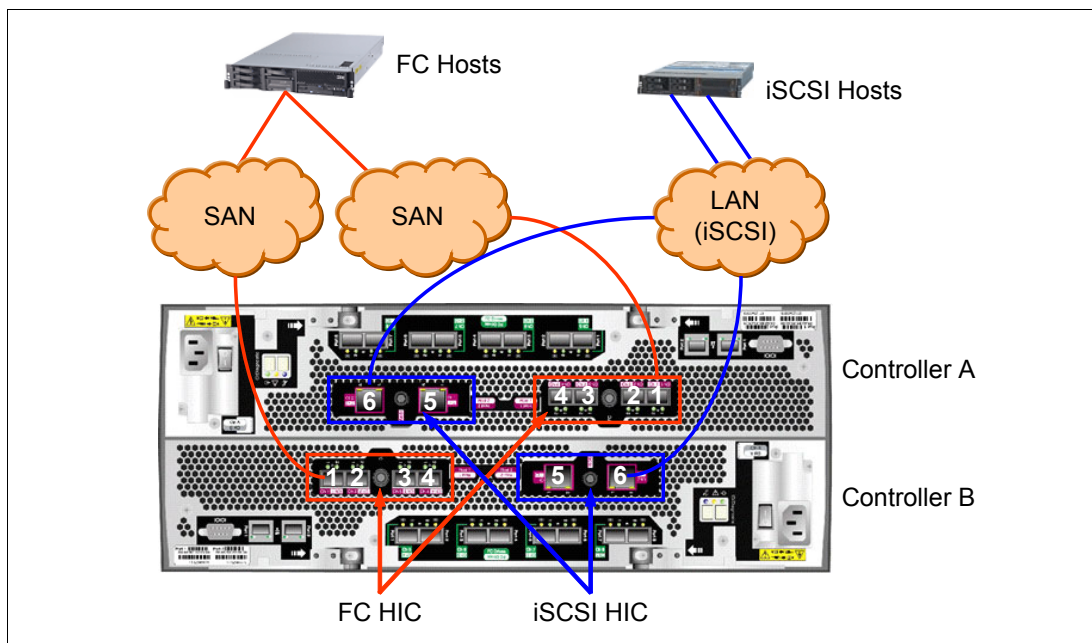


Figure 2-28 Mixed host type HICs

Figure 2-29 shows that the host ports are connected to eight sets of FC host bus adapters (HBAs). You can replace one or all of these sets of FC HBAs with FC switches as required. In our example, HBA 1 of the host AIX is connected to port 1 in the host card 1 in RAID controller A. HBA 2 is connected to the same port and card number in controller B.

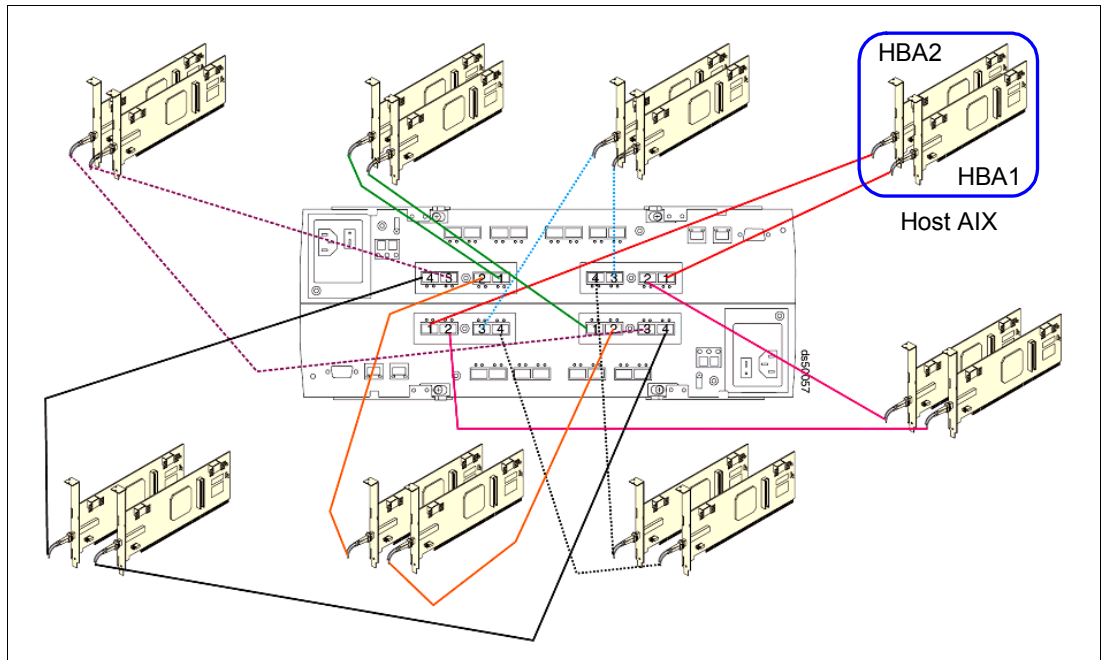


Figure 2-29 Directly connected hosts to the DS5000 storage subsystem

In practice, there is no difference about which ports in which order (in one controller) will be connected to hosts or switches. However, we recommend connecting hosts or switches in the following order:

Models 5100 and 5300 with eight host ports (single Host Interface Card per controller):

1. Controller A, host card 1, port 1 <-> controller B, host card 1, port 1
2. Controller A, host card 1, port 3 <-> controller B, host card 1, port 3
3. Controller A, host card 1, port 2 <-> controller B, host card 1, port 2
4. Controller A, host card 1, port 4 <-> controller B, host card 1, port 4

Models 5100 and 5300 with 16 host ports (two Host Interface Cards per controller):

1. Controller A, host card 1, port 1 <-> controller B, host card 1, port 1
2. Controller A, host card 2, port 1 <-> controller B, host card 2, port 1
3. Controller A, host card 1, port 3 <-> controller B, host card 1, port 3
4. Controller A, host card 2, port 3 <-> controller B, host card 2, port 3
5. Controller A, host card 1, port 2 <-> controller B, host card 1, port 2
6. Controller A, host card 2, port 2 <-> controller B, host card 2, port 2
7. Controller A, host card 1, port 4 <-> controller B, host card 1, port 4
8. Controller A, host card 2, port 4 <-> controller B, host card 2, port 4

In this situation, ports dedicated for Enhanced Remote Mirroring (ERM) (refer to *IBM System Storage DS Storage Manager Copy Services Guide*, SG24-7822 for more details) are used last. Another reason to connect the ports in the suggested order is easier manageability and higher availability (in case of a failure of a host card, you only lose half of the connections to the controller instead of all of them).

Note: When ERM is enabled, the following ports are dedicated for replication (which stops the host I/O):

- Models with eight FC host ports: FC HIC, FC port 4 in both controllers
- Model with 16 FC host ports: Host card 2 and port 4 in both controllers

iSCSI ports are not supported for ERM.

Rule of Thumb: The last FC host port is always dedicated for mirror traffic if ERM is enabled.

2.1.9 DS5000 storage subsystem drive-side connections

The drive-side connections operate at up to 4 Gbps (2 Gbps or 4 Gbps) and allow connection of disk expansion enclosures to the base controller unit.

There are 16 total drive-side connections (eight on each controller). The numbering scheme for the drive connections is structured like the host connections. Because controller A is upside-down, the left-to-right numbering of the drive connection ports is reversed. This means controller A is numbered left to right, 8 through 1, in reverse sequential order. Controller B is numbered left to right, 1 through 8, in forward sequential order (see Figure 2-30).

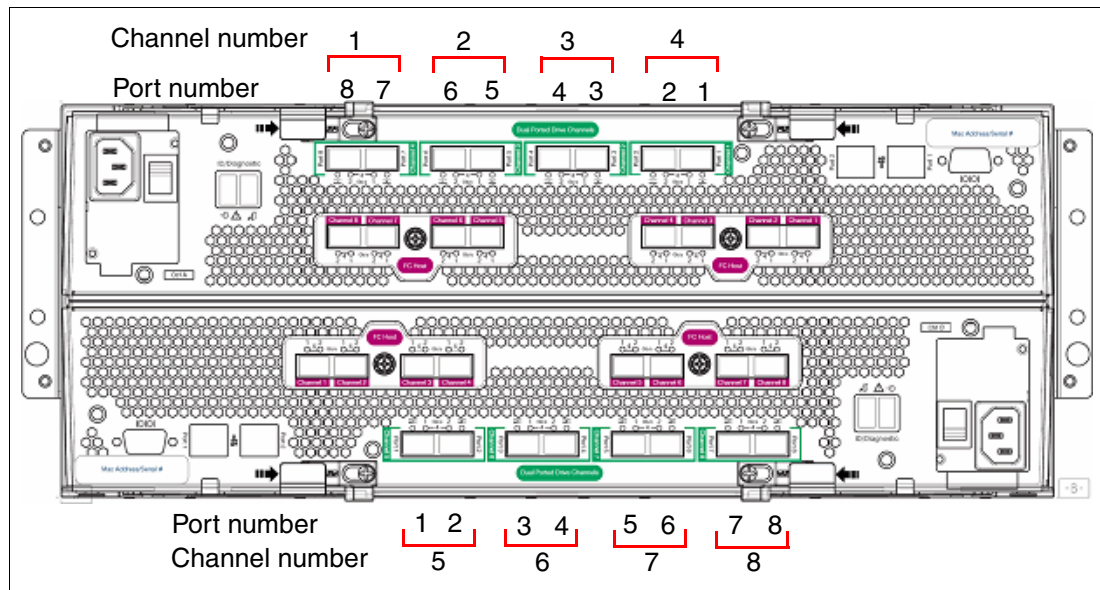


Figure 2-30 Disk drive channel and port numbering

The DS5000 storage subsystem supports eight redundant drive channel pairs on which to place expansion enclosures. Having so many drive channel pairs allows you to achieve high bandwidth and linear scalability. The Arbitrated Loop (FC-AL) standard allows you to connect 127 devices together into a loop. It is important not to have a fully utilized FC-AL to fulfill the linear performance scalability requirement. The DS5000 storage subsystem allows attachment of 448 FC/SAS drives or 480 SATA drives. Having so many drive loops brings the DS5000 system to an unprecedented level of availability, with the ability to spread out drive enclosures over eight back-end drive channels. With EXP5000, you can attach up to 128 drives for each drive enclosure to have a dedicated drive loop. EXP5060 expands that, so in a non-trunked configuration, you can attach up to 480 drives, and each disk enclosure has a dedicated drive loop.

Ports 1 and 2 on each controller are grouped together in one drive channel group. Similarly, ports 3 and 4, 5 and 6, and 7 and 8 are grouped together in other drive channel groups. If you look at the rear of a properly installed DS5000 storage subsystem, you will see them clearly labeled. In this case:

- ▶ Ports 8 and 7 on controller A are channel group 1.
- ▶ Ports 6 and 5 on controller A are channel group 2.
- ▶ Ports 4 and 3 on controller A are channel group 3.
- ▶ Ports 2 and 1 on controller A are channel group 4.
- ▶ Ports 1 and 2 on controller B are channel group 5.
- ▶ Ports 3 and 4 on controller B are channel group 6.
- ▶ Ports 5 and 6 on controller B are channel group 7.
- ▶ Ports 7 and 8 on controller B are channel group 8.

The two ports on each drive channel group must run at the same speed. There is no blocking between the two adjacent ports at the drive channel group level. It is best to spread out the drive-side channel pairs among the channel groups to ensure maximum availability. Each channel (two ports) is internally connected to a 4 Gbit FC port in Controller A and Controller B. Each controller has two quad ports drive chips for drive connections. One chip is dedicated for local ports, with one link per channel. The second one for remote ports (in the second controller) has one link per channel. Refer to Figure 2-3 and Figure 2-7 for architectural details.

A drive-side channel pair is made up of one port from each controller, going left to right. For example, drive channel pair 1 is composed of controller A, port 8, and controller B, port 1. Drive channel pair 2 is composed of controller A, port 7, and controller B, port 2, and so on.

The recommended pairing is driven by the connections between FC loop switches within controllers A and B. For attaching the first four enclosures, we recommend using one port of each channel. Because of easier management, performance, and availability, we propose connecting channel pairs in the following order (refer to Figure 2-31):

1. Disk port 8 controller A <-> disk port 1 controller B
2. Disk port 6 controller A <-> disk port 3 controller B
3. Disk port 4 controller A <-> disk port 5 controller B
4. Disk port 2 controller A <-> disk port 7 controller B
5. Disk port 7 controller A <-> disk port 2 controller B
6. Disk port 5 controller A <-> disk port 4 controller B
7. Disk port 3 controller A <-> disk port 6 controller B
8. Disk port 1 controller A <-> disk port 8 controller B

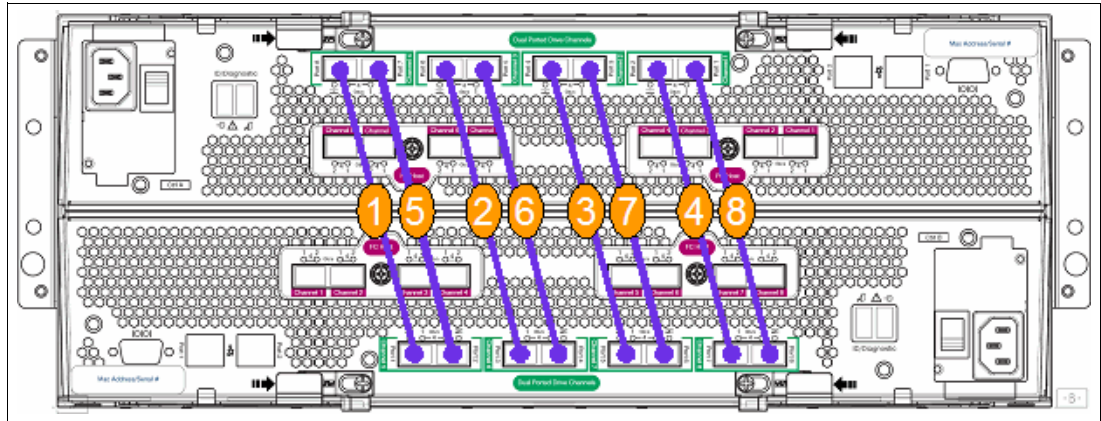


Figure 2-31 Enclosure connections order

Note: The numbering in Figure 2-31 is to help with the growth of a subsystem by adding enclosures. It is not indicative of channel or port numbers.

For cabling configurations, refer to 2.6, “DS5000 storage subsystem drive-side cabling” on page 101.

2.1.10 DS5000 storage subsystem additional connections

In addition to host and drive connections, the DS5000 storage subsystem’s rear also has connections for Ethernet and serial ports. You can manage and service the DS5000 storage subsystem through these ports. The ports are:

- Two RJ-45 Ethernet connectors

These connectors are for an RJ-45 10/100/1000BASE-Tx Ethernet connection. There are two connections per controller. One port is designed for out-of-band management and the other port is meant for serviceability. The logic behind adding an extra port was to introduce additional isolation and to separate management and service traffic from one another. Because of the extra port, you need to have two IP addresses per controller in order to manage and service the DS5000 storage subsystem appropriately. However, you cannot attach this port to a routed network, because you can not set up a gateway for it. You can still operate the DS5000 storage subsystem with only one IP port active per controller. The best practice is to set Port 1 into customer network for out-of-band management and leave the Port 2 as the default in order to let IBM service personnel connect using the default IP addresses.

The default IP addresses for the controllers are shown in the Table 2-4. The default subnet mask for all four Ethernet ports is 255.255.255.0.

Table 2-4 Default IP addresses for the controllers

	Controller A	Controller B
Port 1	192.168.128.101	192.168.128.102
Port 2	192.168.129.101	192.168.129.102

► DB9 Serial port

This serial port is used for management and diagnostic purposes. You can use a PC with a terminal emulation utility, such as Hyper Terminal, to access the command set

Note: We do not recommend the terminal program PuTTY, because certain versions of PuTTY send characters to the controller that can cause the controller to reboot.

The maximum baud rate is 115,200 bps. The default baud rate setting from the factory is 38,400 bps, N-8-1, with no flow control.

Attention: Managing the DS5000 storage subsystem through the serial interface has potential risks. Using certain commands, you can initialize the RAID controller, and therefore lose all your data. You should only use this interface when instructed to do so by IBM Support.

2.1.11 DS5000 component locations

This section will show all DS5000 storage subsystem component locations as displayed in Storage Manager (SM) software. Figure 2-32 shows all the DS5000 storage subsystem component locations and Table 2-5 on page 56 describes how they relate to locations shown in Storage Manager software.

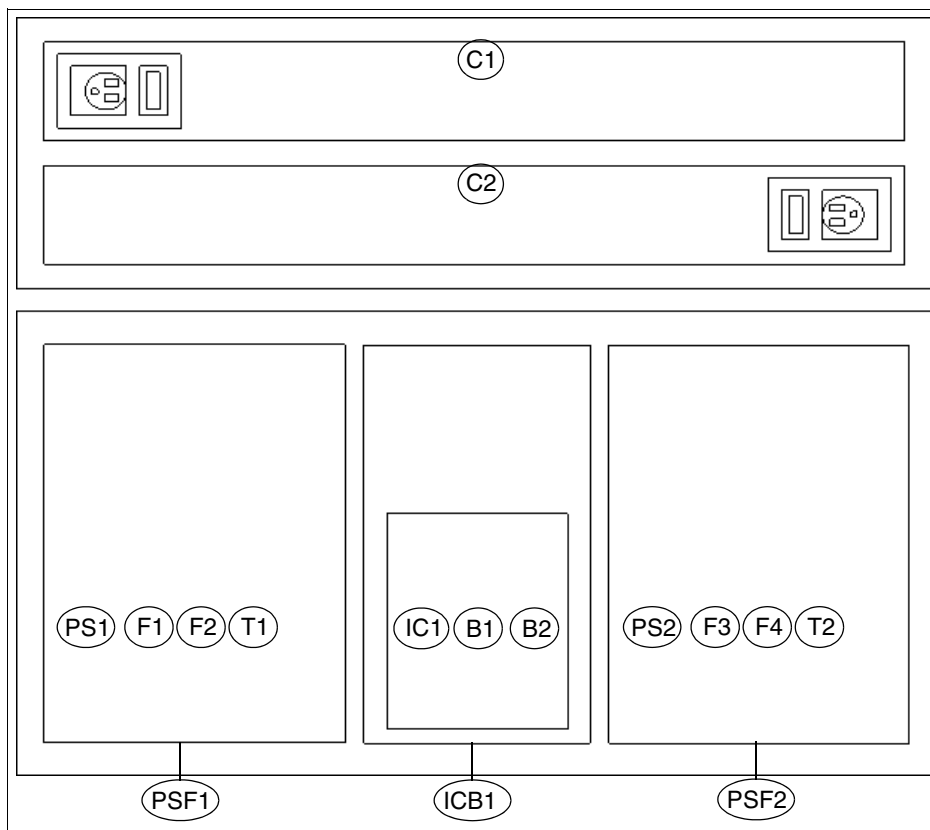


Figure 2-32 DS5000 component locations

Table 2-5 Storage Manager references to DS5000 component locations

Reference	Parent	Slot	Name
C1	Enclosure	1	Controller A
C2	Enclosure	2	Controller B
ICB1	Enclosure	1	Interconnect-Battery canister
IC1	ICB1	N/A	Not represented in SM
B1	ICB1	1	Battery Pack ^a (left)
B2	ICB1	2	Battery Pack ^a (right)
PSF1	Enclosure	1	Power-Fan Canister ^b (left)
PSF2	Enclosure	2	Power-Fan Canister ^b (right)
PS1	PSF1	1	Power Supply (left)
PS2	PSF2	1	Power Supply (right)
F1	PSF1	1	Fan (left)
F2	PSF1	2	Fan (left)
F3	PSF2	1	Fan (right)
F4	PSF2	2	Fan (right)
T1	PSF1	1	Temperature Sensor (left)

Reference	Parent	Slot	Name
T2	PSF2	1	Temperature Sensor (right)

- a. Each battery pack contains two batteries but they are not represented separately and cannot be replaced separately.
- b. Power supply and fans are part of a Power-Fan Canister. They cannot be replaced separately. If any of them fails, whole Power-Fan Canister will need to be replaced.

Important: The DS5000 storage subsystem battery packs do not have expiration dates. Only replace a battery pack when the LEDs have indicated that they have failed (see 2.1.6, “DS5000 storage subsystem rear view” on page 37). You only have to replace the battery pack that failed, not both battery packs

2.2 DS5020 storage subsystem

The IBM System Storage DS5020 disk system, shown in Figure 2-33, is designed to provide low total cost of ownership, high performance, advanced functionality, high availability, and modular and scalable storage capacity.

The DS5020 disk system is designed to deliver up to a two-fold IOP performance increase over its predecessor, the DS4700, and represents the eighth generation architecture within the midrange disk family.

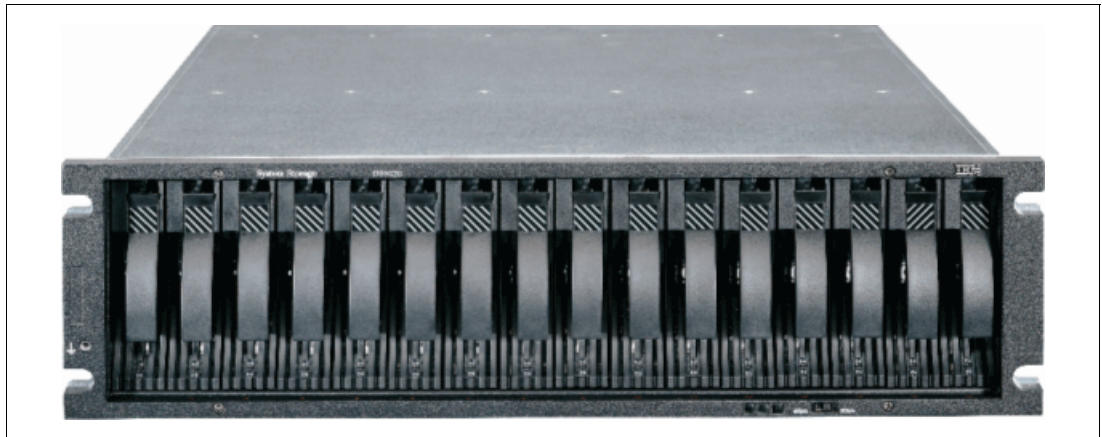


Figure 2-33 IBM System Storage DS5020 storage subsystem

DS5020 disk system members

- ▶ DS5020 Disk Controller (1814-20A)
- ▶ EXP520 Storage Expansion Unit (1814-52A)

Disk drives

- ▶ Up to 224 TB physical storage capacity.
- ▶ Accommodates up to 16 disk drives installed within the DS5020 enclosure.
- ▶ Attachment support for up to six EXP520 expansion enclosures.
- ▶ Attachment support for EXP810 with the *Attach EXP810 to DS5020 Activation feature*.

- ▶ Supports an intermix of SATA drives, FC drives, encryption-capable FC drives (FDE), SAS drives (with FC-SAS interposer), encryption capable SAS drives (with FC-SAS interposer), and SAS SSD drives (with FC-SAS interposer) within the DS5020 and EXP520 enclosures.

Host attachment

Provides SAN-attached 8 Gbps Fibre Channel (FC) host connectivity, as well as optional 1GbE iSCSI host connectivity. All DS5020s have four 8 Gbps FC ports (two per controller).

Additionally you may order initially either:

- ▶ 2-Dual 8 Gbps Host Interface Cards (HIC)
- ▶ 2-Dual 1 Gbps iSCSI HIC

System cache

- ▶ DS5020 comes with 2 GB cache memory (1 GB per internal RAID controller).
- ▶ The 4 GB cache memory (2 GB per RAID controller) feature is available as an initial plant order feature.
- ▶ There are no cache memory upgrades available as field (MES) features for the DS5020.

Drive options

The DS5020 supports RAID 0, 1, 3, 5, 6, and 10 with the following drive options:

- ▶ FC drives without encryption:
 - 146.8 GB/15K 4 Gbps FC E-DDM
 - 300 GB/15K 4 Gbps FC E-DDM
 - 450 GB/15K 4 Gbps FC E-DDM
 - 600 GB/15K 4 Gbps FC E-DDM
- ▶ FC disk with encryption:
 - 146.8 GB/15K 4 Gbps FC encryption-capable E-DDM
 - 300 GB/15K 4 Gbps FC encryption-capable E-DDM
 - 450 GB/15K 4 Gbps FC encryption-capable E-DDM
 - 600 GB/15k 4 Gbps FC encryption-capable E-DDM
- ▶ SATA disks:
 - 750 GB/7.2K SATA E-DDM
 - 1000 GB/7.2K SATA E-DDM
 - 2000 GB/7.2K SATA E-DDM
- ▶ SAS drives (with FC-SAS interposer) without encryption:
 - 300 GB/10k FC-SAS E-DDM
 - 600 GB/10k FC-SAS E-DDM
 - 900 GB/10k FC-SAS E-DDM
- ▶ SAS drives (with FC-SAS interposer) with encryption
 - 300 GB/10k FC-SAS encryption-capable E-DDM
 - 600 GB/10k FC-SAS encryption-capable E-DDM
 - 900 GB/10k FC-SAS encryption-capable E-DDM
- ▶ SAS SSD (with FC-SAS interposer)
 - 200 GB 4Gbps FC-SAS E-DDM
 - 400 GB 4Gbps FC-SAS E-DDM

2.2.1 DS5020 controller architecture

The DS5020 storage subsystem uses almost the same controller architecture as the predecessor DS4700 did (see Figure 2-34) with a few minor differences.

- ▶ Uses a faster XOR engine (1.2 GHz vs. 667 MHz on DS4700).
- ▶ One optional host interface (either dual port iSCSI or dual port 8 Gbps FC).
- ▶ The internal bus is PCI-E x8 (PCI-X on DS4700).
- ▶ Flash drives are used to destage dirty data from the cache in case of a power loss.

The heart of the controller is the 1.2 GHz XOR raid processor, which has improved speed compared to the predecessor's DS4700 667 Mhz Xscale processor. The standard 8 Gbps host port and the optional Host Interface Cards in Figure 2-35 and Figure 2-36 share the same PCI-E x8 bus to transfer their data to the XOR chip. The main FC switch on the controller mainboard processes the FC traffic for the drive channels as well as for the two standard host channels.

The backup battery unit provides power to back up the cache memory of each controller onto the flash drives in the event of a power failure.

To distribute the data to the drives, a chip called “switch-on-chip” (SOC) is used to switch the data directly to their internal destination drive or the external drive channel. Controllers use the drive channel for inter-controller communication.

Figure 2-34 shows the DS5020 storage subsystem controller architecture.

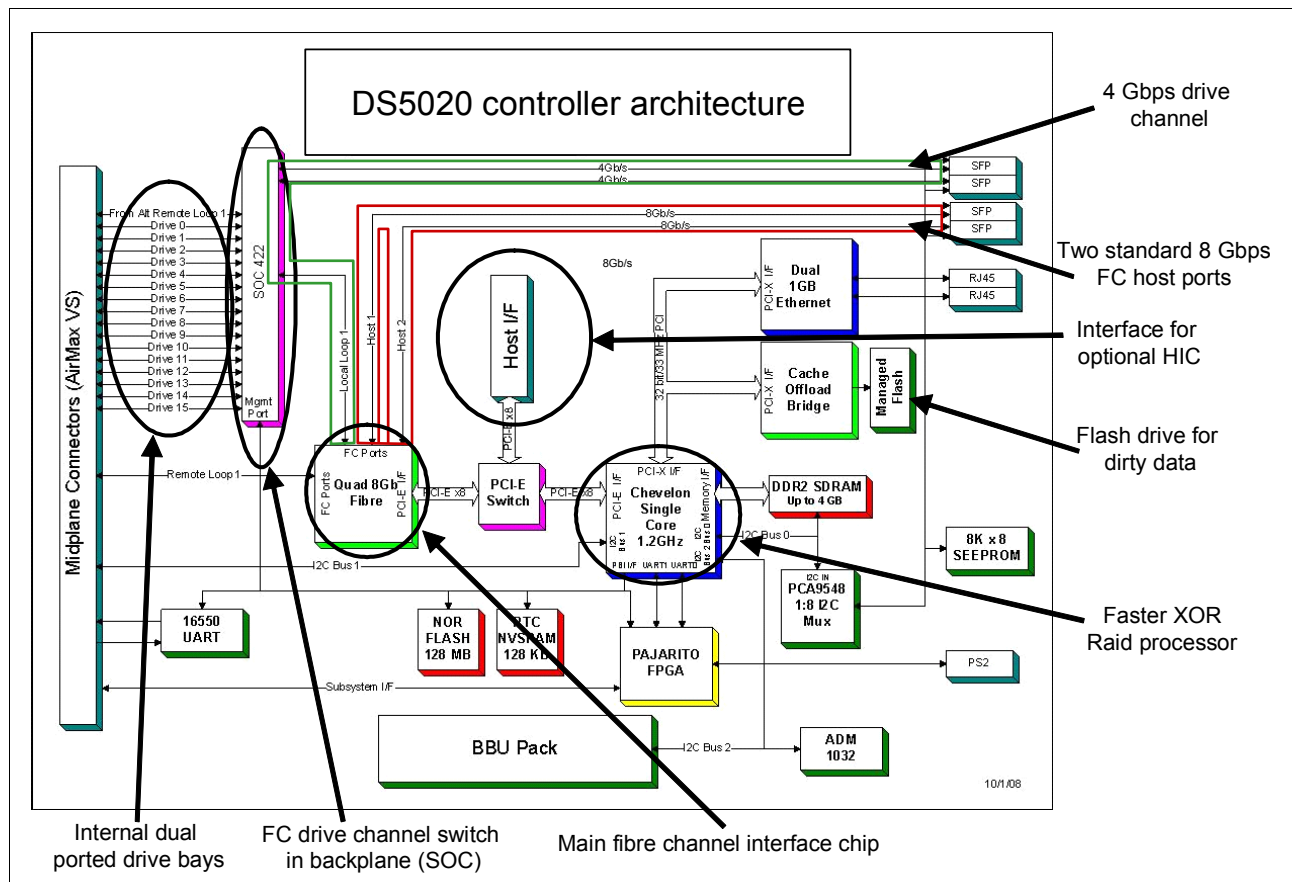


Figure 2-34 DS5020 controller architecture breakdown

The optional dual-ported 8 Gbps Host Interface Card (HIC), shown in Figure 2-35, uses a two port FC chip. This chip connects via PCI-E x8 to the XOR engine.

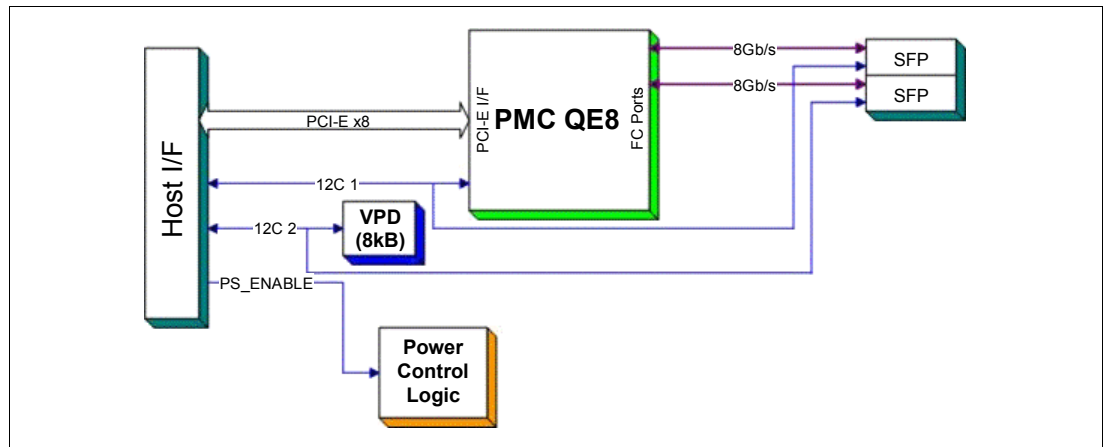


Figure 2-35 DS5020 Dual-Port 8 Gbps HIC architecture

If you have the iSCSI option, as shown in Figure 2-36, there is an QLogic top-off-engine (TOE) build into the DS5020. It will be built in as a daughter card of the controller mainboard. It reduces the workload of the controller CPU by calculating the whole Ethernet traffic and transfers just the SCSI packet through it.

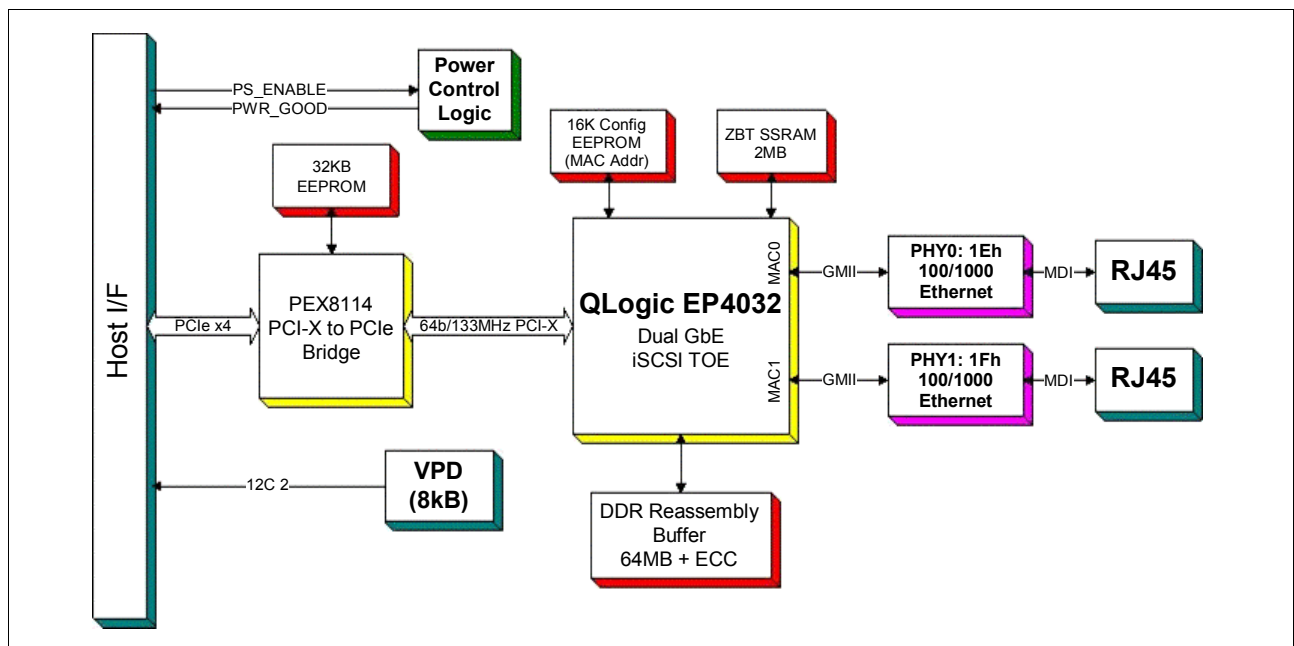


Figure 2-36 DS5020 iSCSI HIC architecture

Because of the similarities between the DS5000 controller models, we refer to 2.1.2, “DS5100 and DS5300 controller architecture” on page 23 for details about write cache, cache handling, write operations, and cache block flow.

2.2.2 DS5020 components

Figure 2-37 shows the components of a DS5020 storage subsystem. All the components shown in this figure are Customer Replaceable Units (CRU).

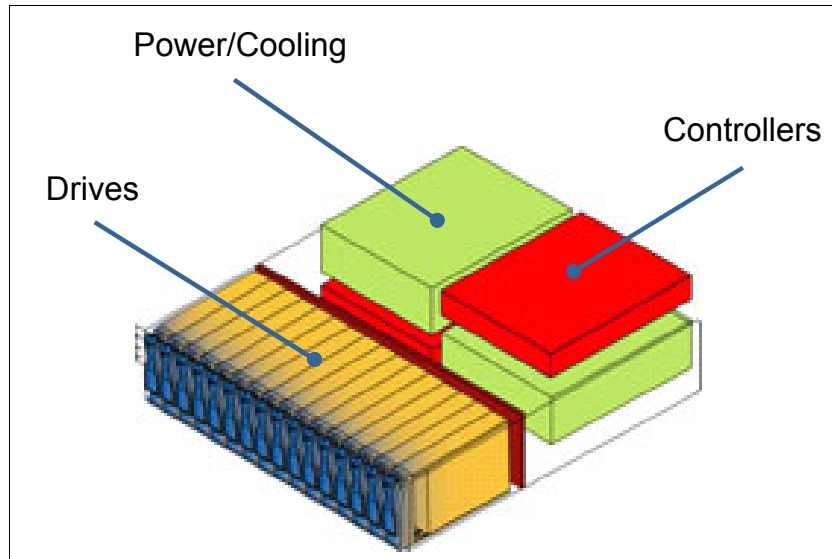


Figure 2-37 DS5020 hardware components

AC power supply and fan unit

Figure 2-38 shows the LEDs on the AC power supply and fan unit.

The LEDs display the status of the storage subsystem and components. The color of the LED is important:

- ▶ Green LEDs indicate a normal operating status.
- ▶ Amber LEDs (Needs Attention) indicate a possible failure.
- ▶ A blue LED on CRU indicates that it is safe to remove the component.

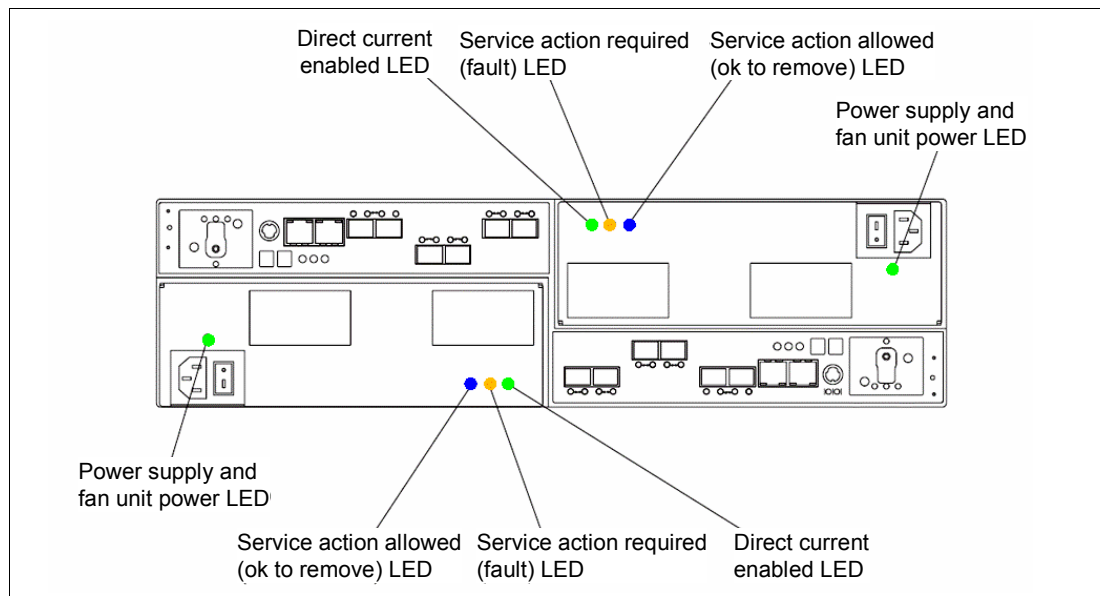


Figure 2-38 DS5020 power supply and fan unit LEDs

In normal operation, only the green LEDs (power LED and DC enabled LED) are on.

Controller

The controllers contain the storage subsystem control logic, interface ports, and LEDs. Depending on the DS5020 configuration you purchased, your controllers are one of the following types:

- ▶ Controllers with 1 GB memory and two standard 8 Gbps FC host ports
- ▶ Controllers with 1 GB memory, two standard 8 Gbps FC host ports, and one optional 2-port 8 Gbps FC host card
- ▶ Controllers with 1 GB memory, two standard 8 Gbps FC host ports, and one optional 2-port 1 Gbps iSCSI host card
- ▶ Controllers with 2 GB memory and two standard 8 Gbps FC host ports
- ▶ Controllers with 2 GB memory, two standard 8 Gbps FC host ports, and one optional 2-port 8 Gbps FC host card
- ▶ Controllers with 2 GB memory, two standard 8 Gbps FC host ports, and one optional 2-port 1 Gbps iSCSI host card

The controllers vary only in the size of the cache (either 1 or 2 GB) and the type of the optional Host Interface Card (either none, FC, or iSCSI).

Figure 2-39, Figure 2-40, and Figure 2-41 show the different DS5020 controller host interface configurations that are available. The DS5020 comes with all SFPs pre-installed.

Figure 2-39 shows the base DS5020 storage subsystem, with two Fibre Channel host ports only. A field upgrade is not possible.

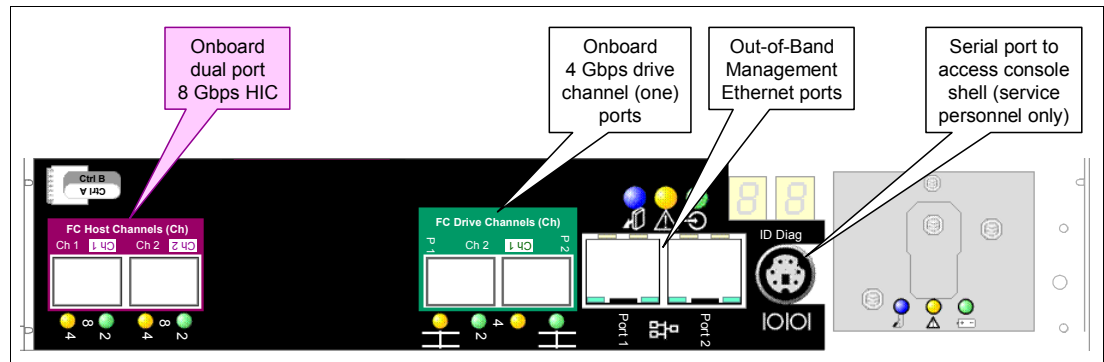


Figure 2-39 DS5020 controller with standard dual 8 Gbps FC host ports: Base model

Figure 2-40 shows the controller with the additional Dual-Port 8 Gbps FC Host Interface Card (HIC). The daughter card will be factory installed only. No field change can be done to this controller.

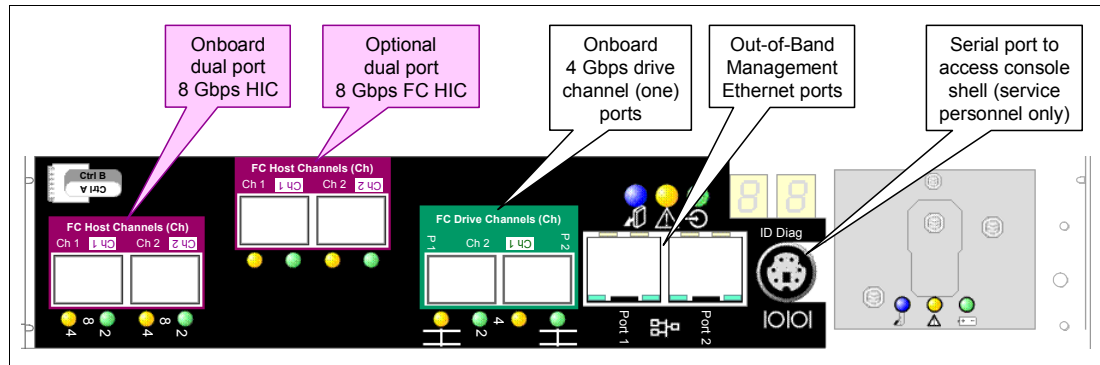


Figure 2-40 DS5020 controller: Additional 8 Gbps daughter card upgrade

The third configuration, shown in Figure 2-41, include a Dual-Port 1 Gbps iSCSI HIC card that will be factory installed as well. There is no field upgrade/change for the HIC cards.

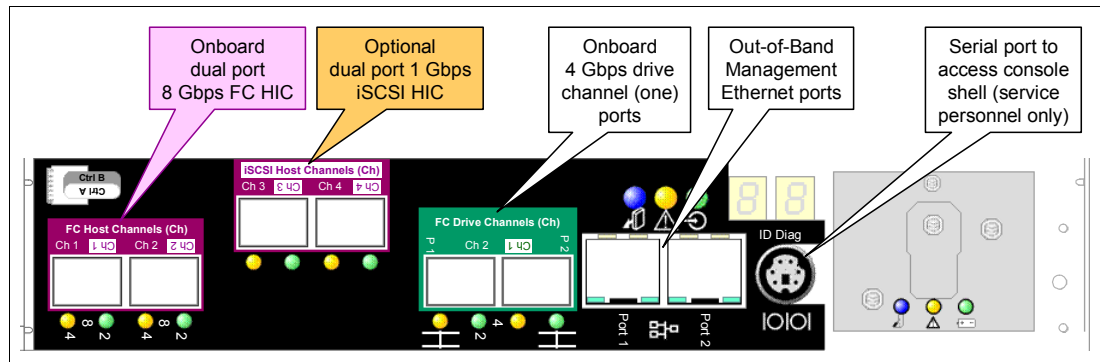


Figure 2-41 DS5020 controller with iSCSI host ports

Enhanced Disk Drive Modules (E-DDMs)

The hot-swap drive bays that are accessible from the front of your storage subsystem are shown in Figure 2-42.

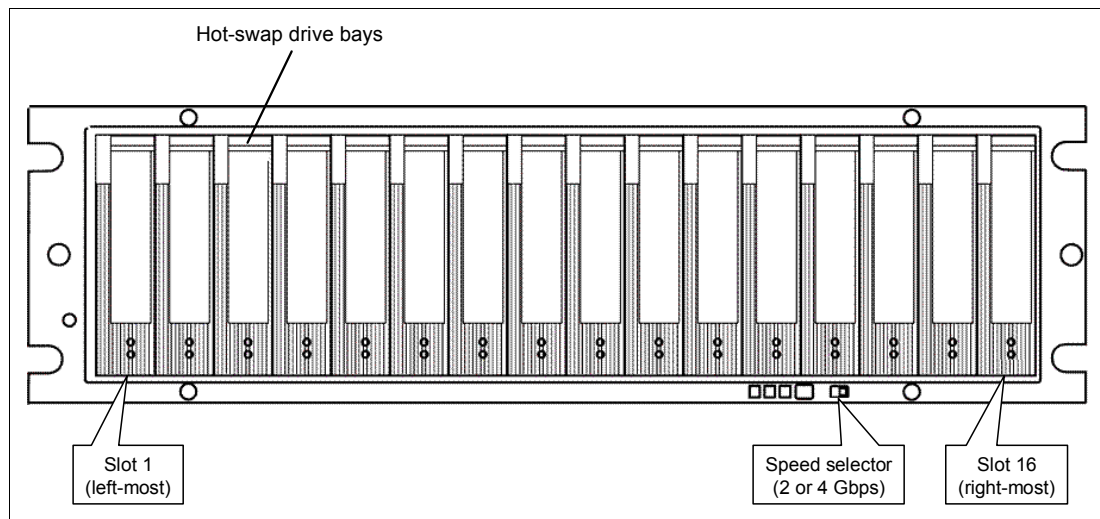


Figure 2-42 DS5020 hot-swap drive bays

The DS5020 supports both Fibre Channel (FC) and SATA E-DDMs intermixed in the storage subsystem drive chassis. The DS5020 supports up to sixteen 4 Gbps FC, 3 Gbps SATA, and 4 Gbps FC-SAS E-DDMs.

SATA E-DDMs have an ATA translator card (interposer card) that converts the Fibre Channel protocol interface of the DS5020 drive channel or loop into the hard drive SATA protocol interface. It also provides dual paths to the SATA drive for drive CRU path redundancy. Each drive, ATA translator card, and carrier assembly is called SATA E-DDM CRU. The Fibre Channel E-DDMs consist of the Fibre Channel and the carrier assembly (drive tray). The FC-SAS E-DDMs have a FC-SAS interposer card that translates the SAS drive interface to a 4 Gbps FC protocol interface of the DS5020 drive channel. Each SAS drive, FC-SAS interposer card (with a 2.5" to 3.5" form factor conversion), and carrier assembly are called FC-SAS E-DDM CRUs.

Install E-DDM CRUs in the 16 drive bays on the front of the storage subsystem from the leftmost slot (slot 1) to the rightmost slot (slot 16). When an E-DDM is installed, the drive and tray slot designation is set automatically. The hardware addresses are based on the enclosure ID, which is set by the controller software, and on the E-DDM physical location in the storage subsystem.

The DS5020 storage subsystem drive channel operates at a 4 Gbps Fibre Channel interface speed. Even the 3 Gbps SATA E-DDMs operate at 4 Gbps Fibre Channel speed.

Note: Even though the DS5020 has a 2 or 4 Gbps Fibre Channel Link Rate switch that can be used to set the drive channel speed at 2 Gbps, the link rate speed must be set to 4 Gbps. The DS5020 supports only 4 Gbps FC speed in the drive channel.

The Link Rate switch on the DS5020 storage subsystem and all storage expansion enclosures connected to it must have the same setting.

There are no serviceable parts in an E-DDM CRU. If it fails, it must be replaced in its entirety (E-DDM, ATA translator card, bezel, and tray). The DS5020 drive tray is not interchangeable with the drive tray of other DS4000 storage subsystems, such as DS4100 or DS4300 storage subsystems. The DS5020 E-DDM option CRUs are not interchangeable with those of the DS4200 Express and EXP420. When replacing an E-DDM CRU, be sure to order and install the correct E-DDM CRU. Using non-supported E-DDM options or FRUs will result in the E-DDM being locked out by the DS5020 controller firmware and might also damage the drive connector in the enclosure midplane.

The following precautions must be taken while replacing the E-DDM CRU.

- ▶ After you remove an E-DDM CRU, wait 70 seconds before replacing or reseating the E-DDM CRU to allow it to properly spin down. Failure to do so might cause undesired events.
- ▶ Never hot-swap an E-DDM CRU when its associated green Activity LED is flashing. Hot-swap an E-DDM CRU only when its associated amber Fault LED lights is not flashing or when the E-DDM is inactive and its associated green Activity LED lights is not flashing.
- ▶ If the E-DDM you want to remove is not in a failed or bypass state, always use the Storage Manager client program either to place it in a failed state or to place the array that is associated with the E-DDM (or E-DDMs) in an offline state before you remove it from the enclosure.

Attention: If you hot-swap an optimal drive without setting it to failed status, drive will become bypassed. If an appropriate hotspare drive is available, reconstruction of the removed drive will start. If a different drive is inserted in the removed slot, copy back will not start and you will need to start it with the *Replace drives* procedure.

The IBM System Storage DS5020 storage subsystem (Machine Type 1814-20A) supports RAID levels 0, 1, 3, 5, and 6 up to over 67.2 TB when using 600 GB Fibre Channel hard drives, up to over 100,8 TB when using 900 GB FC-SAS hard drives and up to 224 TB when using 2 TB Serial Advanced Technology Attachment (SATA) Enhanced Disk Drive Modules (E-DDMs).

The DS5020 supports configurations of FC disks with or without Full Disk Encryption (FDE), or SATA disks, or a mix of disk drives. To install FDE disks in a DS5020, you must purchase the Full Disk Encryption option.

2.2.3 DS5020 Storage Subsystem front view

Figure 2-43 shows the DS5020 from the front side.

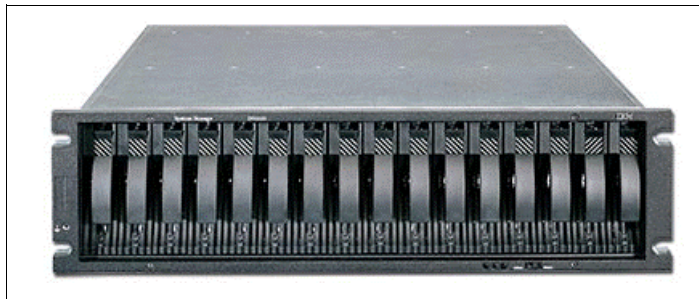


Figure 2-43 DS5020 storage subsystem front view

The hot-swap features of the DS5020 enable you to remove and replace the hard disk drives without turning off the storage expansion enclosure. You can maintain the availability of your system while a hot-swap device is removed, installed, or replaced.

The DS5020 Express supports up to 16 enhanced disk drive modules (E-DDMs). Each drive bay also provides dual paths to each drive for path redundancy. The drives are customer replacement units (CRUs).

Several LED indicators and the FC Link speed selector are also visible from the front of the storage unit. Refer to “Front panel LEDs and FC link speed selector” on page 69 for details about the LEDs.

Attention: Never hot-swap an E-DDM CRU when its associated green activity LED is flashing. Hot-swap a drive CRU only when its associated amber fault LED light is not flashing or when the drive is inactive and its associated green activity LED light is not flashing. Wait 70 seconds before inserting the drive back into the bay.

2.2.4 DS5020 storage subsystem rear view

The rear of the DS5020 appears in different versions depending on what host port configuration has been ordered for the system (Figure 2-44, Figure 2-45, and Figure 2-46).

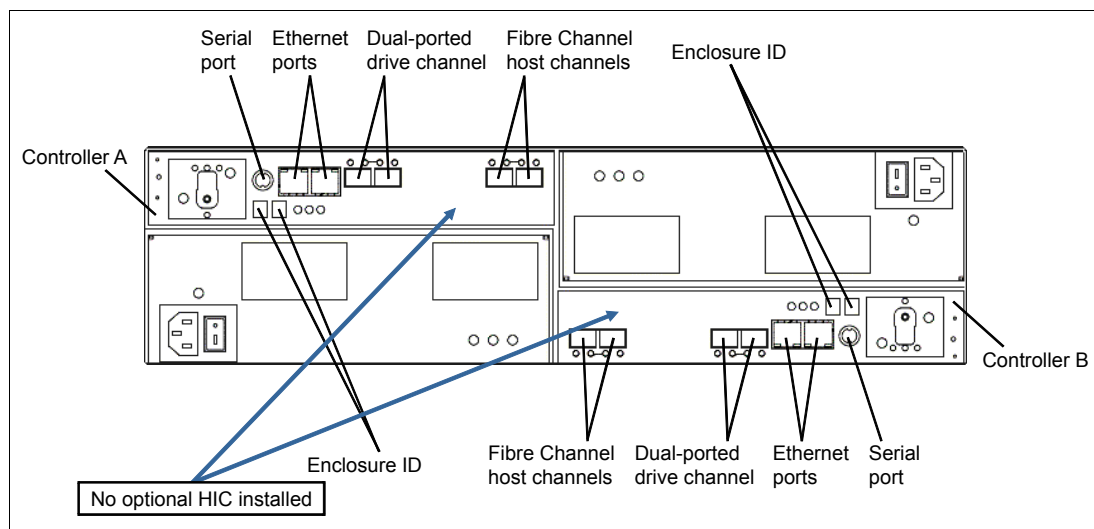


Figure 2-44 DS5020 rear view: Base model

They vary only in host port configurations. The base model does not have the optional Host Interface Cards (HIC). It comes with four 8 Gbps Fibre Channel host ports.

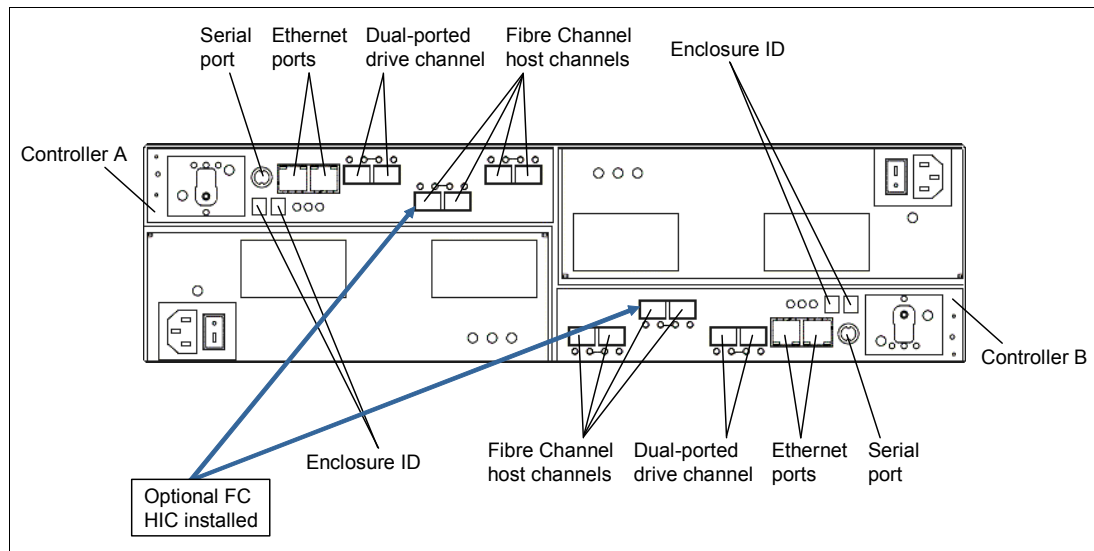


Figure 2-45 DS5020 rear view: 8 FC Port model

Another configuration of the DS5020 has additional four 8 Gbps FC host ports (Figure 2-45) or additional four 1 Gbps iSCSI host ports instead (Figure 2-46).

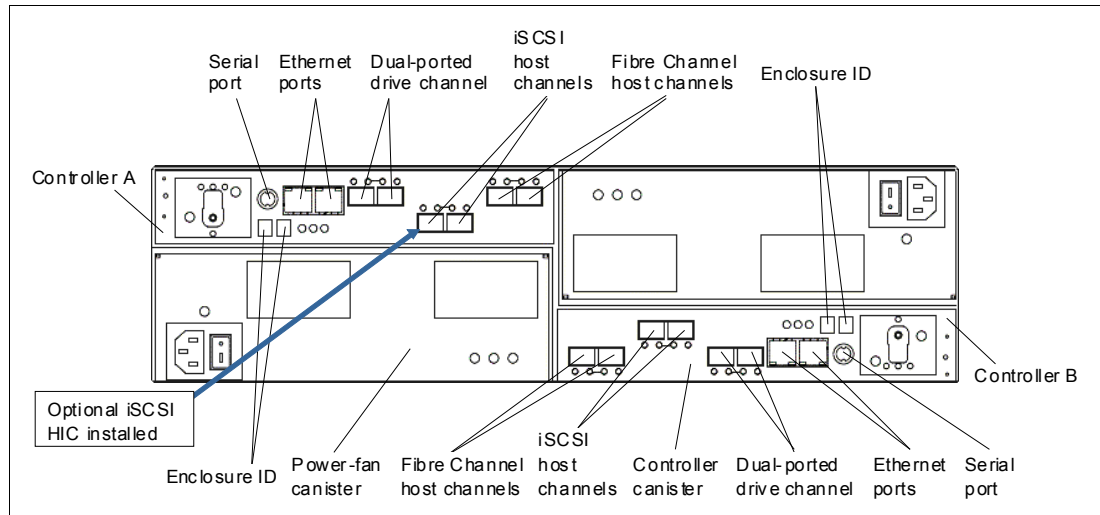


Figure 2-46 DS5020 rear view: 4 FC and 4 iSCSI port model

The DS5020 rear view shows four hot swappable parts:

- ▶ The two controllers with the Backup Battery Unit (BBU)
- ▶ The two Power Supply and Fan Units

The two controllers hold host and drive interfaces as well as the batteries. The left controller is controller A and the right controller is controller B. Note that controller A is upside-down relative to controller B. The same configuration applies to the power supply and fan unit. It is important to keep this information in mind when connecting the back-end ports to hosts and drive-side expansion enclosures. Refer to 2.2.7, “DS5020 storage subsystem drive-side connections” on page 76 for more details.

Figure 2-47 shows a closer view of a DS5020 controller.

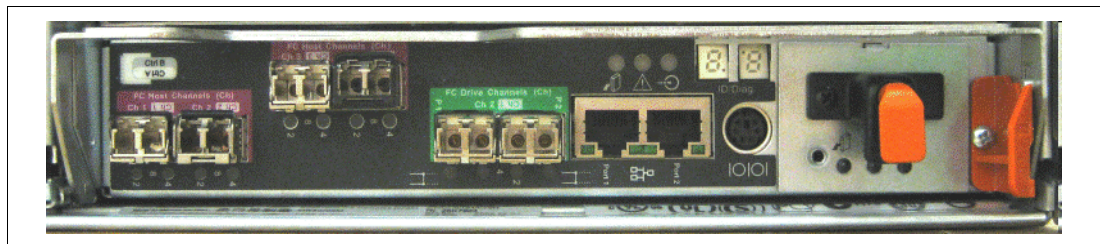


Figure 2-47 DS5020 controller photo rear view

SFP modules

The storage subsystem supports a fiber-optic interface for host and storage expansion enclosure connections. You must install a Small Form-factor Pluggable (SFP) module in each interface connector on the controller where a fiber-optic cable is to be installed.

Note: Remove all unused SFP modules so they don't interfere with the IO operations.

The DS5020 storage subsystem host ports support 2, 4, and 8 Gbps Fibre Channel speeds. The DS5020 storage subsystem drive ports support only 4 Gbps Fibre Channel speeds.

The maximum operating speed of the Fibre Channel port is determined by two factors:

- The speed of the SFP module that is installed
- The speed of the Fibre Channel connection

For example, a 4 Gbps SFP that is plugged into a 8 Gbps-capable port will limit the speed of that port to a maximum of 4 Gbps. Conversely, an 8 Gbps SFP that is plugged into a 4 Gbps-capable port will limit the speed of the port to a maximum of 4 Gbps. Carefully check the SFP IBM part number, option number, and FRU part number to identify its speed. There are no physical features that distinguish an 8 Gbps SFP from a 4 Gbps SFP.

DS5020 ships with all SFP modules included. Figure 2-48 shows an example of SFP module with fiber-optic cable.

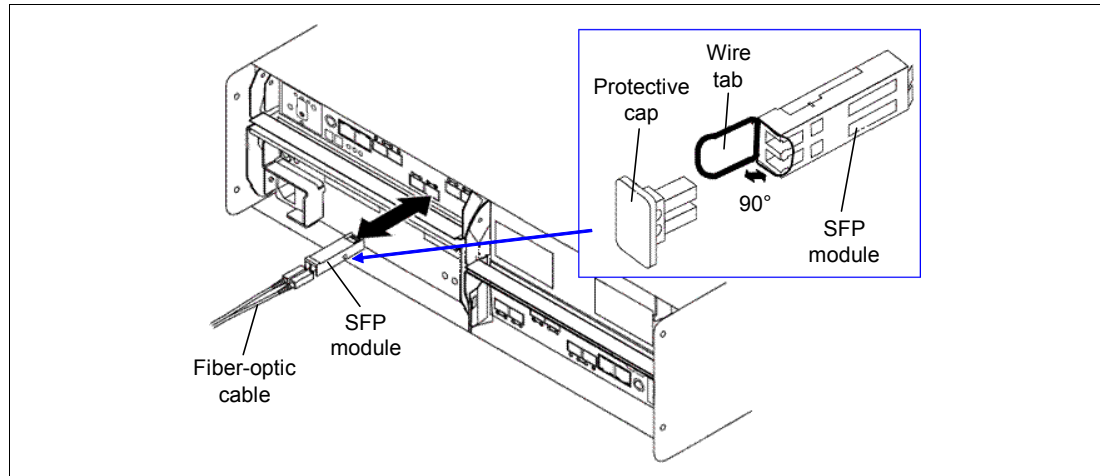


Figure 2-48 DS5020 SFP Module

Backup Battery Unit (BBU)

The Backup Battery Unit provides power to back up the cache memory of each controller onto flash drives in the event of a power failure. Each battery unit contains a sealed, rechargeable SMART lithium ion battery. The battery unit contains enough charge to back up the cached data in each controller to a flash drive in the event of a power failure.

When the unit is powered on the first time or whenever the battery is replaced, the battery chargers will charge the battery to the programmed level. Then, the controller will start a battery learning cycle to determine whether the battery current capacity is sufficient.

Note: Data caching starts after the battery is charged to the programmed level.

During the battery learn cycle, the cache will be active if the battery is in good condition. If the battery fails the learn cycle, it is marked as failed. The battery learning cycle lasts up to three hours. After the first battery learn cycle, the controller will perform a learn cycle every 8 weeks to recalibrate the battery-charging level. The battery unit is hot-swappable. You can remove the battery unit for servicing and then reinsert it while the DS5020 continues to perform I/O operations. The battery should be removed using the Storage Manager: Prepare for Removal procedure (see Chapter 5, “Advanced maintenance, troubleshooting, and diagnostics” on page 285). However, write I/O caching is disabled when the battery is in a failed state or removed from the controller chassis. Replace the failed battery as soon as possible to minimize the time that the write I/O caching is disabled. Information about the condition of the battery unit is conveyed by indicator LEDs on the front of battery unit.

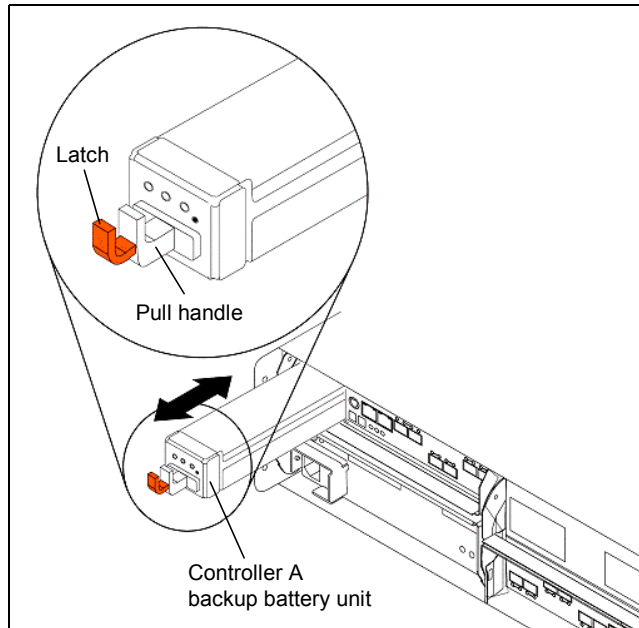


Figure 2-49 Replaceable Backup Battery Unit (BBU)

To physically remove the BBU, just push the latch, as shown in Figure 2-49, and pull out the battery unit.

Important: Unlike the batteries for DS4000 storage subsystems, the DS5020 storage subsystem battery units do not use the expiration dates given in Storage Manager. Do not replace these batteries after a certain usage period.

2.2.5 DS5020 storage subsystem LED indicator lights

LED indicator lights allow the DS5020 to communicate with the user. There are four main components with LEDs:

- ▶ Front panel
- ▶ RAID controllers
- ▶ Battery
- ▶ Power supply fans

Front panel LEDs and FC link speed selector

Figure 2-50 shows the DS5020 front panel and its LED indicator lights.

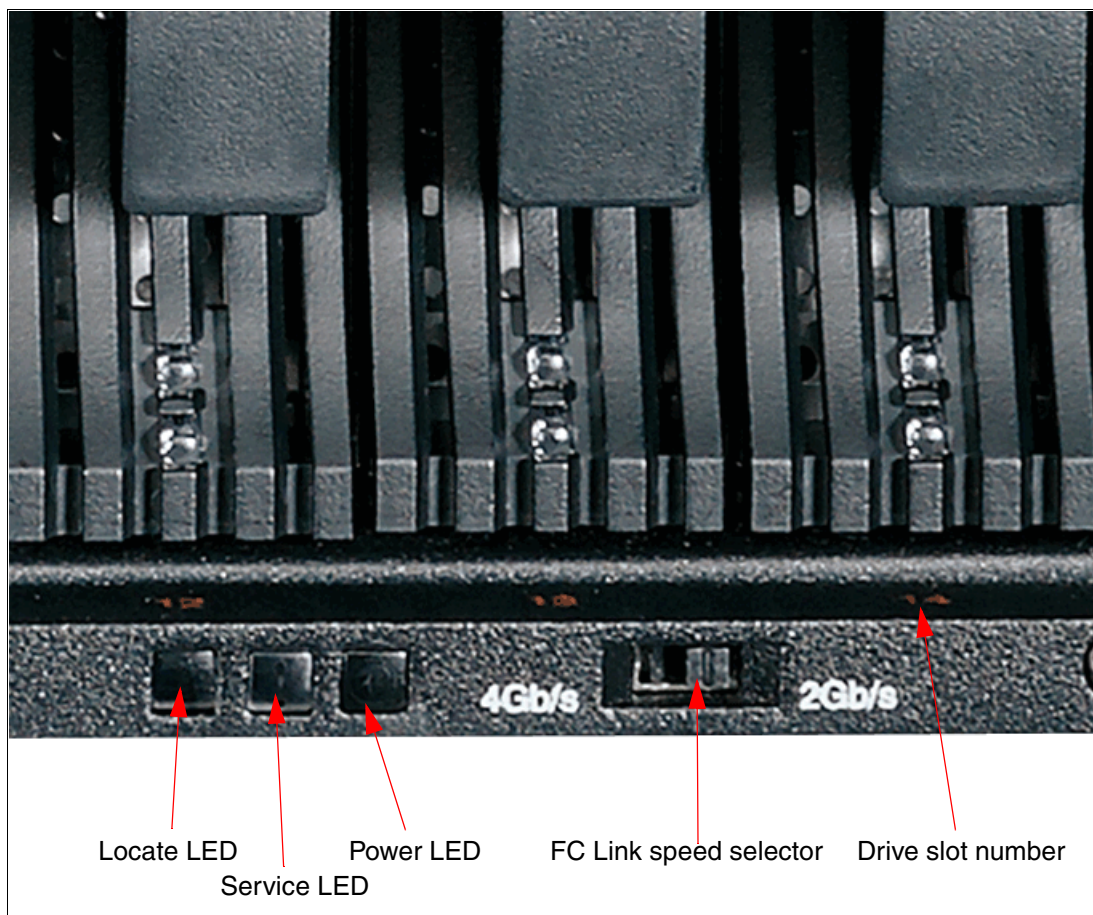


Figure 2-50 DS5020 front panel LEDs

Link speed selector

The FC link speed selector is a physical switch that must be used to set the enclosure speed. The DS5020 Express storage system drive channel operates only at 4 Gbps Fibre Channel interface speed.

Note: Link speed switch always has to be set to 4 Gb/s setting. The DS5020 storage system SATA E-DDM CRUs have an ATA translator card that converts E-DDM 3 Gbps SATA drive interface protocol to 4 Gbps Fibre Channel interface speed and FC-SAS E-DDM CRUs have a FC-SAS interposer that converts 6 Gbps SAS drive interface protocol to 4 Gbps Fibre Channel interface speed.

Front LEDs

These are:

- ▶ Locate LED (blue)
 - On: This indicates storage subsystem locate function is on.
 - Off: This is the normal status.
- ▶ Service action required LED (amber)
 - On: There is a corresponding needs attention condition flagged by the controller firmware. Some of these conditions might not be hardware related.
 - Off: This is the normal status.

- Power LED (green)
 - On: The subsystem is powered on.
 - Off: The subsystem is powered off.

RAID controller LEDs

The LEDs on the RAID controllers serve as indicators of key information as described in Figure 2-51. The LED status details are provided in Table 2-6, and Table 2-7 on page 71.

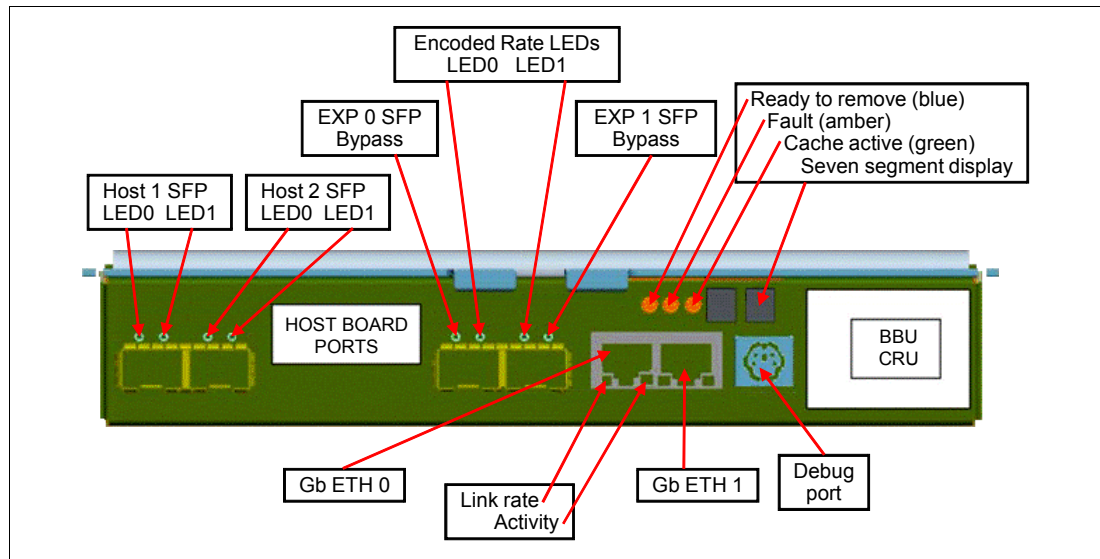


Figure 2-51 DS5020 RAID controller LEDs

Host SFP LEDs

- LED #0 (green): Host channel speed L1
- LED #1 (green): Host channel speed L2

Table 2-6 FC host SFP status LED definitions

LED#0	LED#1	Port status
OFF	OFF	Link down
ON	OFF	Link rate 2 Gbps
OFF	ON	Link rate 4 Gbps
ON	ON	Link rate 8 Gbps

Disk Channel SFPs LEDs

Table 2-7 FC disk expansion port SFP LED definitions

LED#0	LED#1	Port status
OFF	OFF	Link down
ON	OFF	Reserved
OFF	ON	Link rate 2 Gbps
ON	ON	Link rate 4 Gbps

- ▶ Drive channel bypass / EXP bypass (amber)
 - Off: Normal status
 - On: Drive port bypass problem

Other LEDs

- ▶ Serviced action allowed / Ready to remove (blue) (see “Service action allowed (SAA) LEDs” on page 73 for details)
 - Off: Normal status
 - On: Safe to remove
- ▶ Need attention (amber)
 - Off: Normal status
 - On: Controller needs attention (controller fault or controller is offline)
- ▶ Caching active (green)
 - On: Data in cache
 - Off: No data in cache
- ▶ Ethernet link rate
 - Off: 100 Mbps
 - On: 1 Gbps
- ▶ Ethernet link activity
 - Off: No link established
 - On: Link established (blinks off with transmit or receive activity)

Enclosure ID

The enclosure ID, comprised of two seven-segment numbers, is located on the back of each controller next to the indicator lights, as shown in Figure 2-52. It provides a unique identifier for each enclosure in the DS5020 storage subsystem configuration.

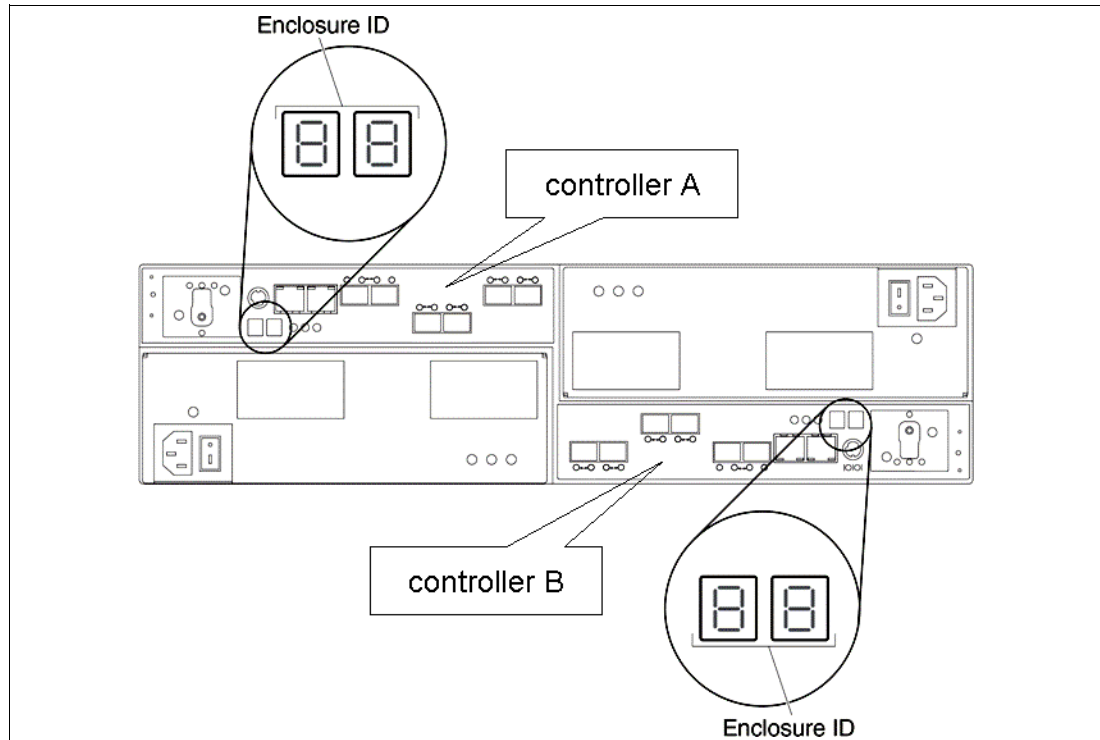


Figure 2-52 DS5020 controller enclosure ID display

The controller automatically sets the enclosure ID number. You can change the setting through the storage management software if necessary. Both controller enclosure ID numbers are identical under normal operating conditions. Each storage expansion enclosure (including the DS5020 storage subsystem itself) in the DS5020 configuration must have a unique storage enclosure ID.

In addition, the single digits (x1) of the enclosure IDs of all storage expansion enclosures and the DS5020 storage subsystem in the redundant drive channel/loop pair must be unique. Because the DS5020 has only one drive channel, all expansion enclosures will have the same single digit (x1).

Although the allowable ranges for enclosure ID settings are 0-99, do not set the enclosure ID to 00 or any number less than 80 for the controller enclosure. For expansions, only use enclosure ID in range from 01 to 80. The DS5020 enclosure ID is usually set to a value of 85 before it is shipped.

Service action allowed (SAA) LEDs

There are few things to talk about regarding the SAA LEDs (Figure 2-53).

Each controller, power supply and fan unit, and battery unit has a blue Service Action Allowed status (SAA) LED. The purpose of the SAA LED is to help make sure that a component is not removed before it is safe to do so. Do not remove any storage subsystem component unless the Service Action Allowed status LED for that component is lit.

Attention: If you do a controller replacement, make sure that the controller that you want to replace is in offline mode or failed before you physically remove it. Using only the Prepare for Removal function will not change the controller state.

Use the Prepare for Removal function in the DS Storage Manager Subsystem Management window or refer to the applicable component replacement instructions for this case. Refer to Chapter 5, “Advanced maintenance, troubleshooting, and diagnostics” on page 285 for detailed information.

Note: Wait at least two minutes after you replace each component for the controller to recognize the new component and update the LED status. If the SAA LED is turned on, you must remove and replace the component in order to get the LED turned off.

In most cases when a single component fails, the Service Action Allowed status LED turns on steadily when the Needs Attention status LED is turned on for the component.

Battery LEDs

Each DS5020 RAID controller has its own battery. There are three LED indicator lights on each battery:

- ▶ Service action allowed (blue) (see “Service action allowed (SAA) LEDs” on page 73 for details)
 - Off: Normal status.
 - On: Safe to remove.
- ▶ Battery charging (green)
 - On: Battery charged and ready.
 - Blinking: Battery is charging.
 - Off: Battery is faulted, discharged, or missing.
- ▶ Needs attention or service action required (amber)
 - Off: Normal status.
 - On: Controller firmware or hardware requires attention.

Figure 2-53 shows the battery LEDs.

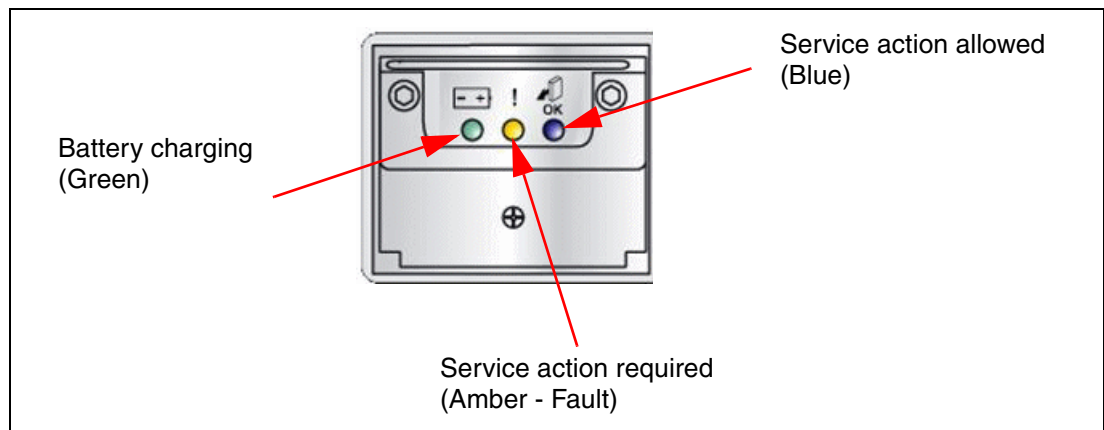


Figure 2-53 Battery LEDs

Power supply and fan unit LEDs

Each power supply fan (Figure 2-54) contains one power supply and two fans.

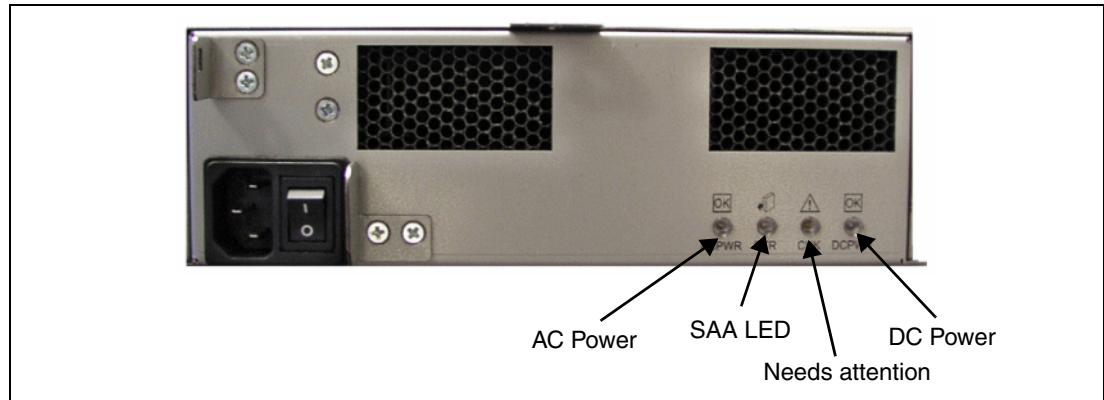


Figure 2-54 Power supply and fan unit LEDs

The LEDs are:

- ▶ Power supply fan LED (AC power) (green)
 - Off: Power supply fan is not providing AC power.
 - On: Power supply fan is providing AC power.
- ▶ Serviced action allowed (blue) (see “Service action allowed (SAA) LEDs” on page 73 for details)
 - On: Safe to remove.
 - Off: Normal status.
- ▶ Needs attention (amber)
 - Off: Normal status.
 - On: Power supply fan requires attention.
- ▶ Power supply fan Direct Current Enabled (DC power) (green)
 - Off: Power supply fan is not providing DC power.
 - On: Power supply fan is providing DC power.

2.2.6 DS5020 storage subsystem host-side connections

The DS5020 integrates the host-side and drive-side connections into the controller itself. The DS5020 has two 8 Gbps host connections by default. They are mounted on the mainboard of the controller. Another two host ports per controller can be added when ordering the DS5020. They can be installed only by factory. No MES field upgrade will be possible. Currently, you can order 1 Gbps iSCSI or 8 Gbps FC Host ports. Refer to “Controller” on page 62 for the configuration options. The FC Host connections support Fibre Channel attachment through SAN switches or direct connections. The iSCSI Host connections support 100 Mbps or 1 Gbps switched Ethernet or iSCSI network and direct connection.

- | | |
|-----------------------|---|
| 8 Gbps FC host ports | These ports auto negotiate with 2 Gbps, 4 Gbps, and 8 Gbps Fibre Channel speed if an 8 Gbps SFP is installed. 1 Gbps FC speed will not be supported. |
| 4 Gbps FC drive ports | The controller has two drive ports that belong to the same drive channel. Both ports must run at 4 Gbps speed because only EXPs and drives running a 4 Gbps are supported to be attached to the DS5020. |

1 Gbps iSCSI host Ports The iSCSI ports support both IPv4 and IPv6 TCP/IP addresses, CHAP, and iSNS. Use either Cat 5E or Cat 6 Ethernet cable types for iSCSI port connections. A Cat 6 Ethernet cable provides optimal performance. The setup of the host ports will be done in the Storage Manager. By default, the iSCSI ports auto negotiate between 100 and 1000 Mbps Ethernet speed.

It is important to match up host or fabric connections to the DS5020 by attaching one connection to each controller. In doing so, you take advantage of the DS5020's ability to fail over and distribute the workload among the two controllers. For any given host, make sure to connect to the same host port number on each controller. The host port layout is shown in Figure 2-57.

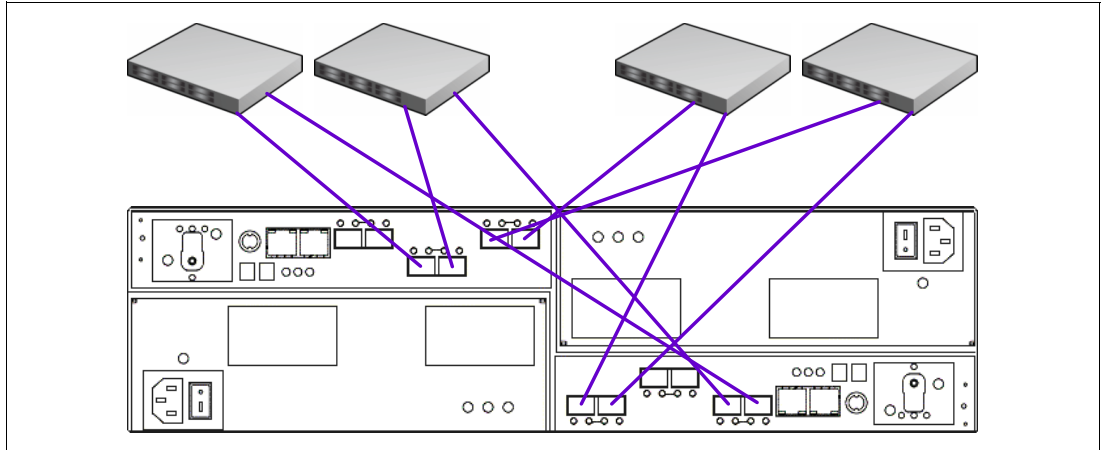


Figure 2-55 DS5020 mixed host connection layout

2.2.7 DS5020 storage subsystem drive-side connections

The DS5020 can attach up to six expansion enclosures. The regular expansion enclosure is the EXP520. However, you can buy a feature that enables you to attach EXP810 as well (refer to “Disk drives” on page 57). Only these two expansion enclosures are currently supported. It is generally best to spread the enclosures evenly between the two drive channel pairs as you scale up the DS5020 in storage capacity. A fully configured DS5020 should have three expansion enclosures on each drive-side channel pair.

Both drive ports on the DS5020 controller belong to the same drive channel, which means that both drive ports must operate at the same Fibre Channel speed. However, only 4 Gbps expansion units supported.

Note: There are three rules for the expansion cabling:

- ▶ With the DS5020, you should only connect a maximum of three enclosures per controller drive port.
- ▶ The DS5020 controller drive port must always be connected to the EXP520 or EXP810 port labelled 1B. Because the left (ESM A) and right (ESM B) enclosure service modules (ESM) are inserted in different orientations, ensure that you use the port labeled 1B before making the Fibre Channel connection to the DS5020 storage subsystem, as shown in Figure 2-56.
- ▶ Spread expansion enclosures among the two drive channel pairs. For example, if you attach four enclosures, it is better to have two enclosures behind each drive port rather than three and one.

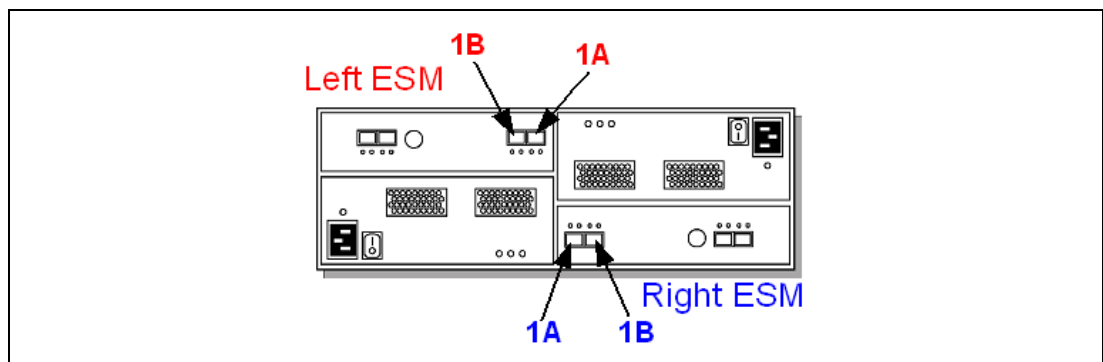


Figure 2-56 Port labels on EXP520 or EXP810

Refer to “Disk Channel SFPs LEDs” on page 71 for more details about the LED status on the disk channels. For cabling configurations, refer to 2.6.4, “DS5020 storage subsystem drive-side cabling” on page 112.

2.2.8 DS5020 storage subsystem additional connections

The DS5020 storage subsystem has various kinds of connectors, as shown in Figure 2-57.

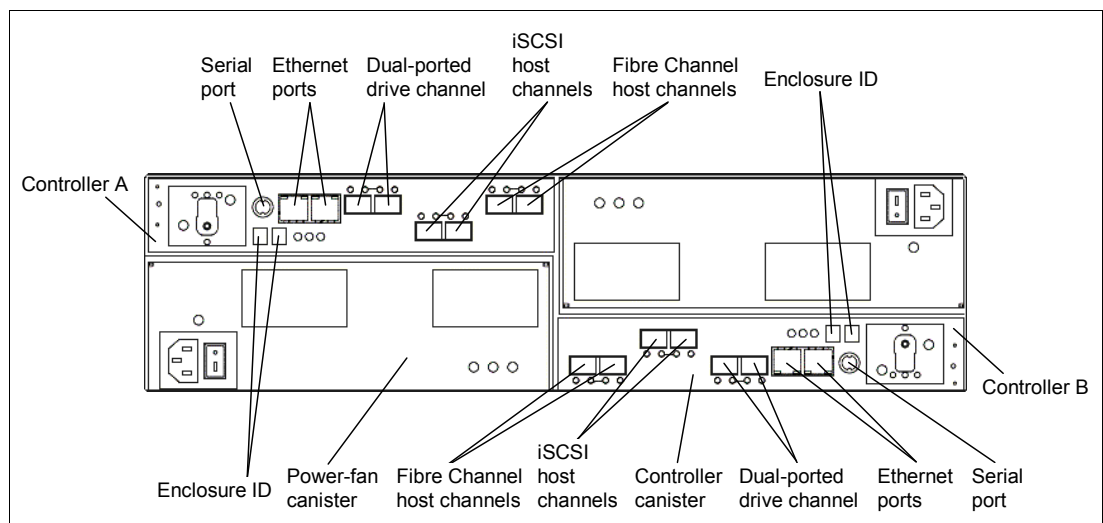


Figure 2-57 DS5020: All connectors

These connectors are:

► Management Ethernet connectors

This connector is for an RJ-45 10/100/1000 BASE-Tx Ethernet connection. There are two connections per controller. One port is designed for out-of-band management and the other port is meant for serviceability. The logic behind adding an extra port was to introduce additional isolation and to separate management and service traffic from one another. Because of the extra port, you need to have two IP addresses per controller in order to manage and service the DS5020 storage subsystem appropriately. However, you cannot attach this port to a routed network, because you cannot set up a gateway for it. You will still operate the DS5020 with only one IP port active per controller. The best practice is to set port 1 in the customer network for out-of-band management and leave the Port 2 as the default in order to let service personnel to connect using the default IP addresses.

The default IP addresses for the controllers are shown in the Table 2-8. The default subnet mask for all four Ethernet ports is 255.255.255.0.

Table 2-8 Default IP addresses for management ports

	Controller A	Controller B
Port 1	192.168.128.101	192.168.128.102
Port 2	192.168.129.101	192.168.129.102

► Serial port

This serial port is used for management and diagnostic purposes. You can use a PC with a terminal emulation utility, such as Hyper Terminal, to access the command set.

Note: We do not recommend the terminal program PuTTY, because certain versions of PuTTY send characters to the controller that can cause the controller to reboot.

The maximum baud rate is 115,200 bps. The default baud rate setting from the factory is 38,400 bps, N-8-1, with no flow control.

Attention: Managing the DS5000 storage subsystem through the serial interface has potential risks. Using certain commands, you can initialize the RAID controller, and therefore lose all your data. You should only use this interface when instructed to do so by IBM Support.

2.2.9 DS5020 Component Locations

This section will show all DS5020 storage subsystem component locations as displayed in Storage Manager (SM) software. Figure 2-58 shows all the DS5020 storage subsystem component locations and Table 2-9 on page 79 describes how they relate to locations shown in Storage Manager software.

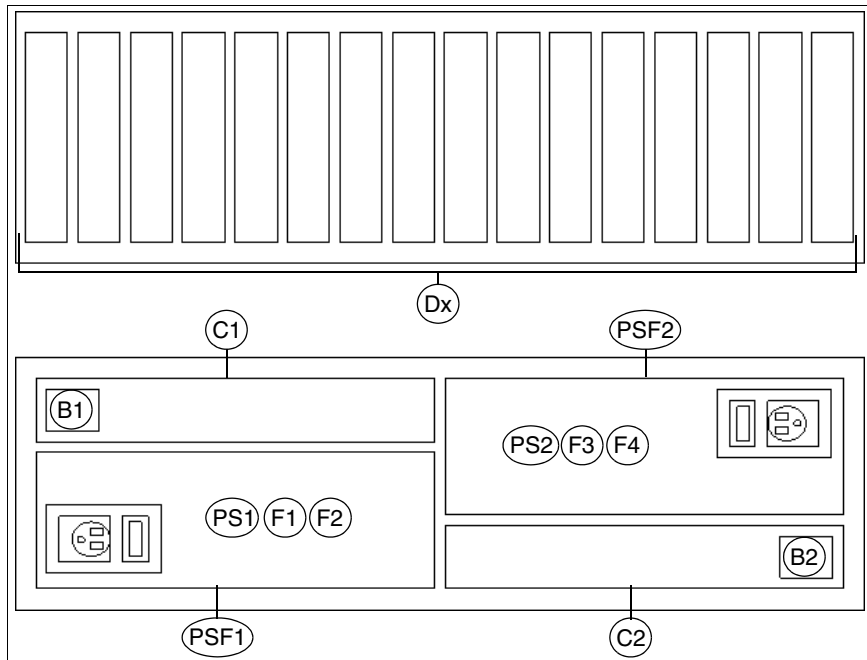


Figure 2-58 DS5020 component locations

Table 2-9 Storage Manager references to DS5020 component locations

Reference	Parent	Slot	Name
Dx (D1-D16)	Enclosure	1-16	Drive 1 - 16
C1	Enclosure	1	Controller A
C2	Enclosure	2	Controller B
B1	C1	1	Battery Pack
B2	C2	2	Battery Pack
T1	C1	1	Temperature Sensor
T2	C2	2	Temperature Sensor
PSF1	Enclosure	1	Power-Fan Canister (left)
PSF2	Enclosure	2	Power-Fan Canister (right)
PS1	PSF1	1	Power Supply (left)
PS2	PSF2	2	Power Supply (right)
F1	PSF1	1	Fan
F2	PSF1	2	Fan
F3	PSF2	3	Fan
F4	PSF2	4	Fan

2.3 DS5000 series physical specifications

This section contains the physical specifications for the DS5020, DS5100, and DS5300 systems and the expansion units.

IBM System Storage DS5020 storage subsystem (1814-20A)

- ▶ Height: 129.5 mm (5.1 in.)
- ▶ Width: 482.6 mm (19.0 in.)
- ▶ Depth: 571.5 mm (22.5 in.)
- ▶ Weight
 - Drive-ready (without drive modules installed): 27.67 kg (61 lbs.)
 - Fully configured (16 drive modules installed): 39.92 kg (88 lbs.)

EXP520 Expansion Unit (1814-52A)

- ▶ Height: 129.5 mm (5.1 in.)
- ▶ Width: 482.6 mm (19.0 in.)
- ▶ Depth: 571.5 mm (22.5 in.)
- ▶ Weight:
 - Drive-ready (without drive modules installed): 26.31 kg (58 lbs.)
 - Fully configured (16 drive modules installed): 38.56 kg (84 lbs.)

IBM System Storage DS5100 (1818-51A) and DS5300 (1818-53A) storage subsystems

- ▶ Height: 174.50 mm (6.87 in.)
- ▶ Width: 481.75 mm (18.97 in.)
- ▶ Depth: 634.92 mm (25.0 in.)
- ▶ Weight: 40.90 kg (90.0 lbs.)

IBM System Storage EXP5000 Expansion Unit (1818-D1A)

- ▶ Height: 132.10 mm (5.20 in.)
- ▶ Width: 482.60 mm (19.0 in.)
- ▶ Depth: 558.80 mm (22.0 in.)
- ▶ Weight:
 - Drive-ready (without drive modules installed): 31.30 kg (69 lbs.)
 - Fully configured (16 drive modules installed): 38.56 kg (85 lbs.)

IBM System Storage EXP5060 Expansion Unit (1818-G1A)

- ▶ Height: 176.0 mm (6.93 in.)
- ▶ Width: 482.6 mm (19.0 in.)
- ▶ Depth: 866.1 mm (34.10 in.)
- ▶ Weight:
 - Drive-ready (without drive modules installed): 56.7 kg (125 lbs.)
 - Fully configured (60 drive modules installed): 102.1 kg (225 lbs.)

Operating environment

This section will cover operating environment specifications.

IBM System Storage DS5020 storage subsystem (1814-20A)

- ▶ Temperature (operating):
 - 10 to 35° C (50 to 95° F) at 0 to 914 m (0-3,000 ft.)
 - 10 to 32° C (50 to 90° F) at 914 to 2,133 m (3,000-7,000 ft.)
- ▶ Relative humidity (operating): 8% to 80%
- ▶ Relative humidity (storage): 5% to 80%
- ▶ Electrical power (per power supply, system rating):
 - Voltage range: 100-240V ac
 - Operating current: 6.0 - 2.5 amperes
 - Power: 600 watts
 - Frequency: 50/60 Hz
- ▶ Heat dissipation: 1529 BTU per hour
- ▶ Noise level (normal operation): 6.4 bels

IBM System Storage EXP520 (1814-52A) Expansion Unit

- ▶ Temperature (operating):
 - 10 to 35° C (50 to 95° F) at 0 to 914 m (0-3,000 ft.)
 - 10 to 32° C (50 to 90° F) at 914 to 2,133 m (3,000-7,000 ft.)
- ▶ Relative humidity (operating): 8% to 80%
- ▶ Relative humidity (storage): 5% to 80%
- ▶ Electrical power (per power supply, system rating):
 - Voltage range: 100-240V ac
 - Operating current: 6.0 - 2.5 amperes
 - Power: 600 watts
 - Frequency: 50/60 Hz
- ▶ Heat dissipation: 1516 BTU per hour (fully configured)
- ▶ Noise level (normal operation): 6.5 bels

IBM System Storage DS5100 (1818-51A) and DS5300 (1818-53A) storage subsystems

- ▶ Temperature (operating):
 - 10 to 35 degrees C (50 to 95 degrees F) at 0 to 914 m (0-3,000 ft.)
 - 10 to 32 degrees C (50 to 90 degrees F) at 914 to 2,133 m (3,000-7,000 ft.)
- ▶ Relative humidity (operating): 8% to 80%
- ▶ Relative humidity (storage): 5% to 80%
- ▶ Electrical power (per power supply, system rating):
 - Voltage range: 100-240V ac
 - Operating current: 5.4 - 2.25 amperes
 - Power: 580 watts

- Frequency: 50/60 Hz
- ▶ Heat dissipation: 804 BTU per hour
- ▶ Noise level (normal operation): 6.75 bels

IBM System Storage EXP5000 (1818-D1A) Expansion Unit

- ▶ Temperature (operating):
 - 10 to 35 degrees C (50 to 95 degrees F) at 0 to 914 m (0-3,000 ft.)
 - 10 to 32 degrees C (50 to 90 degrees F) at 914 to 2,133 m (3,000-7,000 ft.)
- ▶ Relative humidity (operating): 8% to 80%
- ▶ Relative humidity (storage): 5% to 80%
- ▶ Electrical power (per power supply, system rating):
 - Voltage range: 100-240V ac
 - Operating current: 5.4 - 2.25 amperes
 - Power: 580 watts
 - Frequency: 50/60 Hz
- ▶ Heat dissipation: 1570 BTU per hour (fully configured)
- ▶ Noise level (normal operation): 6.75 bels

IBM System Storage EXP5060 (1818-G1A) Expansion Unit

- ▶ Temperature (operating):
 - 10 to 35 degrees C (50 to 95 degrees F) at 0 to 914 m (0-3,000 ft.)
 - 10 to 32 degrees C (50 to 90 degrees F) at 914 to 2,133 m (3,000-7,000 ft.)
- ▶ Relative humidity (operating): 8% to 80%
- ▶ Relative humidity (storage): 5% to 80%
- ▶ Electrical power (per power supply, system rating):
 - Voltage range: 200-240V ac
 - Operating current: 8.62 - 7.19 amperes
 - Power: 1428 watts
 - Frequency: 50/60 Hz
- ▶ Heat dissipation: 4884 BTU per hour (fully configured)
- ▶ Noise level (normal operation): 6.8 bels

2.4 DS5000 supported operating systems

The intent of this section is to list the most popular supported operating system platforms for the DS5000 series. For a complete and up-to-date list, refer to the SSIC website at the following address:

<http://www-03.ibm.com/systems/support/storage/ssic/interoperability.wss>

The supported systems are:

- ▶ IBM Power Systems™
 - IBM AIX V5.3 TL12, V6.1 TL6, and V7.1

- Red Hat Enterprise Linux versions 5.5, 5.6, and 6
- Novell SUSE Linux Enterprise Server versions 10 SP3 and SP4, and version 11 SP1
- ▶ IBM BladeCenter®
 - Microsoft Windows Server 2003 SP2, 2008 R2, 2008 R2 SP1, and 2008 SP2
 - Red Hat Enterprise Linux versions 5.5, 5.6, and 6 (on Intel, AMD, and Power)
 - Novell SUSE Linux Enterprise Server versions 10 SP3 and SP4, and version 11 SP1 (on Intel, AMD, and Power)
 - IBM AIX V5.3 TL12, V6.1 TL6, and V7.1 (on Power)
- ▶ IBM System x, Intel, and AMD
 - Microsoft Windows Server 2003 SP2, 2008 R2, 2008 R2 SP1, and 2008 SP2
 - Red Hat Enterprise Linux versions 5.5, 5.6, and 6
 - Novell SUSE Linux Enterprise Server versions 10 SP3 and SP4, and version 11 SP1
- ▶ VMware V3.5 U5, V4.1 and V4.1 U1, and V5.0
- ▶ Hewlett-Packard: HP-UX 11iV3 (11.31)
- ▶ Solaris: Sun Solaris 10 U8 and 10 U9
- ▶ Apple Mac Pro, Apple Xserve, and MacOS 10.6.x

2.5 DS5000 storage subsystem disk enclosures

DS5000 family has 3 enclosures available. The EXP5000 and the EX5060 can be attached to DS5100 and DS5300, while EXP520 can be attached to the DS5020. EXP810 can still be attached to the DS5000 storage systems for purposes of migrating data from the EXP810 to the DS5000 storage subsystem. However, you will need a license to attach the EXP810 to a DS5020 storage subsystem.

- ▶ EXP5000 Storage Expansion Unit (1818-D1A)
- ▶ EXP5060 Storage Expansion Unit (1818-G1A)
- ▶ EXP520 Storage Expansion Unit (1818-52A)

In this section, we discuss the features of the DS5000 expansion units (EXPs) and how they can be attached and combined to expand the storage capacity of the DS5000 storage systems. The EXP5000 and the EXP520 are very similar, only difference being that the EXP5000 is attached to DS5100 and DS5300, and EXP520 is attached to DS5020. The EX5060 can only be attached to the DS5100 and the DS5300.

As part of the base machine functionality, the DS5000 controllers and EXP5000 are designed to support integration and use of up to 448 high-performance Fibre Channel or high-capacity SATA disk drive modules (DDMs).

With a 480 Drive Upgrade Premium Feature Pack, DS5000 can use up to 480 SATA DDMs with 8 EXP5060 storage expansion enclosures.

Warning: Applying 480 Drive Upgrade Premium Feature Pack will reboot the controllers, so it is necessary to stop all IO before applying it.

2.5.1 EXP5000 and EXP520 Storage Expansion Unit

The EXP5000 (1818-D1A) and EXP520 (1814-52A) Storage Expansion Units are each packaged in a 3U rack-mountable, high-capacity 16-drive bay enclosure containing dual switched 4 Gbps ESMs, dual power supplies, and redundant cooling. EXP5000s connect to DS5100 and DS5300 controllers through high-speed 4 Gbps FC disk expansion ports and have a physical storage capacity of up to 32 TB per enclosure, using 2000 GB SATA DDMs, up to 9.6 TB per enclosure, using 600 GB FC DDMs, and up to 14.4 TB per enclosure using 900 GB FC-SAS DDMs. It is also possible to mix SATA, FC-SAS, and FC drives in the same enclosure. The EXP520 uses the same disk types and sizes, but only connects to DS5020 storage controllers.

The EXP5000 Expansion Unit (1818-D1A) and EXP520 (1814-52A) base model includes a 3U, rack-mount 16-bay disk enclosure, two SFP transceivers, dual power supplies, redundant cooling, rack mounting rails, softcopy documentation, and two rack PDU power cords (36L8886). Any country-specific wall outlet power cord is obtained through feature number 98xx.

Both expansion units support the following drives:

- ▶ FC drives without encryption:
 - 146.8 GB/15K 4 Gbps FC E-DDM
 - 300 GB/15K 4 Gbps FC E-DDM
 - 450 GB/15K 4 Gbps FC E-DDM
 - 600 GB/15K 4 Gbps FC E-DDM
- ▶ FC disk with encryption:
 - 146.8 GB/15K 4 Gbps FC encryption-capable E-DDM
 - 300 GB/15K 4 Gbps FC encryption-capable E-DDM
 - 450 GB/15K 4 Gbps FC encryption-capable E-DDM
 - 600 GB/15k 4 Gbps FC encryption-capable E-DDM
- ▶ SATA disks:
 - 750 GB/7.2K SATA E-DDM
 - 1000 GB/7.2K SATA E-DDM
 - 2000 GB/7.2K SATA E-DDM
- ▶ SAS drives (with FC-SAS interposer) without encryption:
 - 300 GB/10k FC-SAS E-DDM
 - 600 GB/10k FC-SAS E-DDM
 - 900 GB/10k FC-SAS E-DDM
- ▶ SAS drives (with FC-SAS interposer) with encryption
 - 300 GB/10k FC-SAS encryption-capable E-DDM
 - 600 GB/10k FC-SAS encryption-capable E-DDM
 - 900 GB/10k FC-SAS encryption-capable E-DDM
- ▶ SAS SSD (with FC-SAS interposer)
 - 200 GB 4Gbps FC-SAS E-DDM
 - 400 GB 4Gbps FC-SAS E-DDM

Note: The usable disk space is less than the overall disk capacity.

The usable capacities are what the SMclient will report as storage that can be used by the hosts. We arrive at this number through the following steps:

1. Take the listed raw disk amount (listed in decimal, per the storage industry standard), multiply by 1000^3 , and divide by 1024^3 to get a raw binary capacity (1 decimal GB = 1,000,000,000 bytes. 1 binary GB = 1,073,741,824 bytes (2^{30} bytes)).
2. Subtract the 512 MB configuration database, that is, the DACstore (the region that holds controllers and configuration information) after converting to binary.

This gives you the approximate usable binary capacity that can be utilized by hosts and is what the SMclient will report to you as usable capacity.

Front view

The front of the subsystem provides access to the sixteen portable canister contained drives. There are three summary LEDs at the bottom of the front panel, as shown in Figure 2-59:

- ▶ Locate/Identify (White) - This White Locator LED aids in module identification.
- ▶ Summary Fault (Amber) - When there is a fault condition, this LED glows amber.
- ▶ Power (Green) - This LED glows green when at least one power supply is operational.

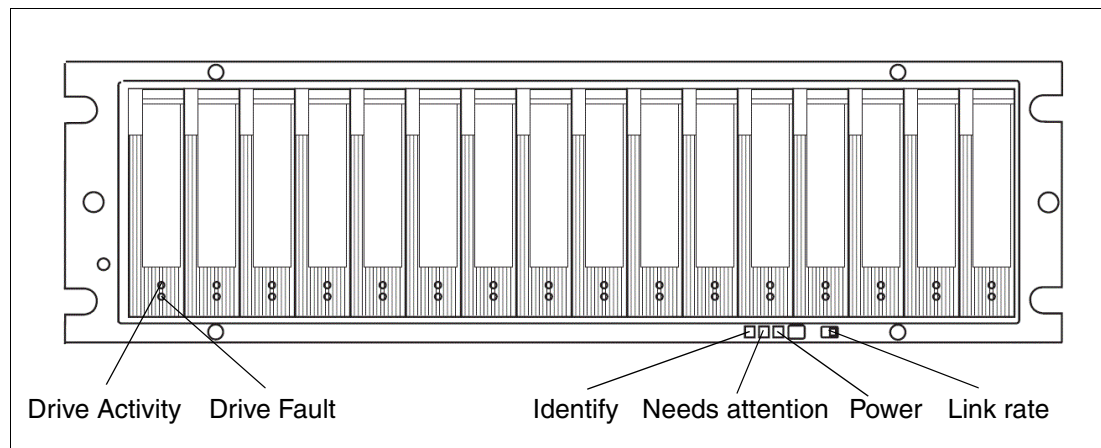


Figure 2-59 EXP5000 and EXP520 front panel

There are two LEDs on each drive tray (see Figure 2-59):

- ▶ Drive Activity
 - On (not blinking): No data is being processed.
 - Blinking: Data is being processed.
- ▶ Drive Fault
 - Blinking: Drive, volume, or storage array locate function.
 - On: A problem has occurred.

The Link Rate switch (number 6) should be set to 4 Gbps (depending on your configuration).

Rear view

This section describes the primary LEDs, controls, and connectors on the rear of the storage expansion enclosure for all models. The back view in Figure 2-60 shows the following components:

- Fans and power supplies: Two removable power supply and fan unit FRUs, each containing one power supply and two fans
- ESMs: Two removable environmental services modules (ESMs)

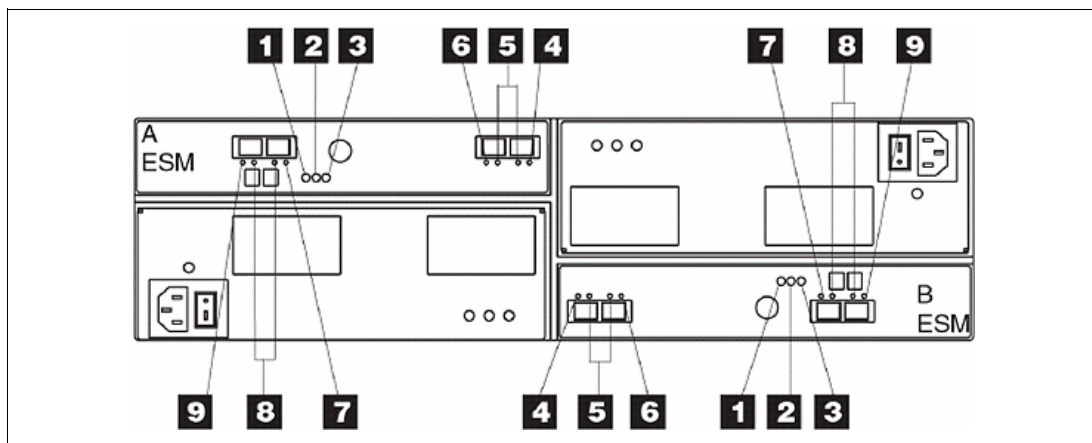


Figure 2-60 EXP5000 and EXP520 rear view

Table 2-10 explains all the LEDs and connectors shown in Figure 2-60.

Table 2-10 Rear LEDs and connectors

Number	LED	Normal Status	Problem Status
1	ESM Power	On	Off
2	ESM Fault	Off	On
3	ESM Service Action Allowed (SAA)	Off	On
4	ESM Port 1 in Bypass (This port is labeled 1A)	Off - Cable connected On - No Cable connected	On - when a FC cable is connected
5	ESM Ports 1 & 2 2 or 4 Gbps Data Rate	One LED is lit if 2 Gbps Both LEDs are lit if 4 Gbps	N/A
6	ESM Port 2 in Bypass (This port is labeled 1B)	Off - Cable connected On - No Cable connected	On - when a FC cable is connected
7	ESM Port 3 in Bypass (This port is labeled 2A)	This port is reserved for future use	On - blinking for 30 seconds
8	ESM Ports 3 & 4 2 or 4 Gbps Data Rate	One LED is lit if 2 Gbps Both LEDs are lit if 4 Gbps	N/A
9	ESM Port 4 in Bypass (This port is labeled 2B)	This port is reserved for future use	On - blinking for 30 seconds

EXP5000 and EXP520 ESM board

The ESMs contain the storage expansion enclosure control logic, interface ports, and LEDs. Each ESM has four SFP module ports that you could use to connect the storage expansion

enclosure to the storage subsystem. However, only the two ESM SFP ports (labeled 1A and 1B) near the center of the storage expansion enclosure are used as shown in Figure 2-61. The SFP ports labeled 2A and 2B are reserved for future use.

Note: Always use port 1B to connect to the controller drive channel ports or previous drive enclosure in a loop. Port 1A is used to connect the next enclosure in the loop. These ports were called In (1B) and Out (1A) in the older drive enclosures and the analogy is still valid.

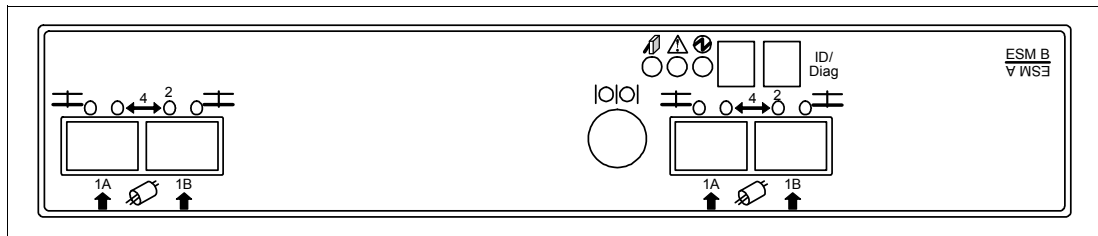


Figure 2-61 EXP5000 and EXP520 ESM ports

The EXP5000 and EXP520 ESM board allows for host based monitoring and control of the subsystem through SCSI-3 Enclosure Services (SES) over the FC link.

The EXP5000 and EXP520 supports two ESM CRUs to help provide system redundancy. Each ESM connects a separate Fibre Channel loop to one of the two Fibre Channel ports on the disk drives, which is designed to provide both loops access to all drives. It is designed to maintain access to all drives through the second loop and ESM. In the event of an FC ESM failure or inoperable loop, access to all drives is still available through the second loop and ESM.

There are switches inside ESM that allow direct access (1 hop) to a required disk from ESM, as shown in Figure 2-62.

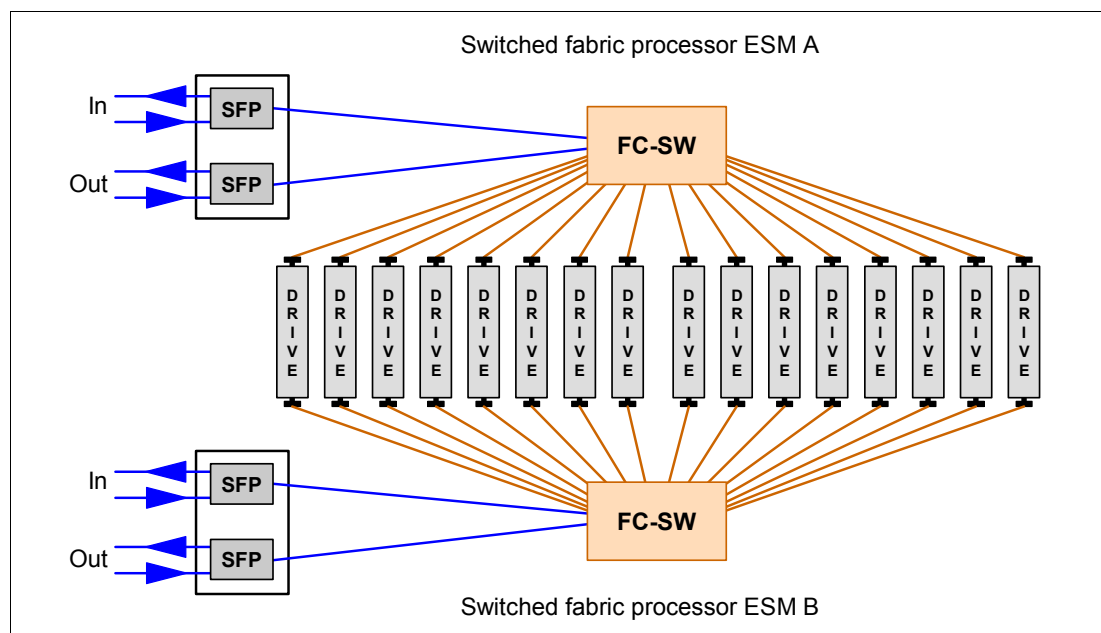


Figure 2-62 EXP5000 and EXP520 switched architecture

EXP5000 and EXP520 component locations

This section will show all EXP5000 and EXP520 storage expansion enclosure component locations as displayed in Storage Manager (SM) software. Figure 2-63 shows all EXP5000 and EXP520 storage expansion enclosure component locations and Table 2-11 describes how they relate to locations shown in Storage Manager software.

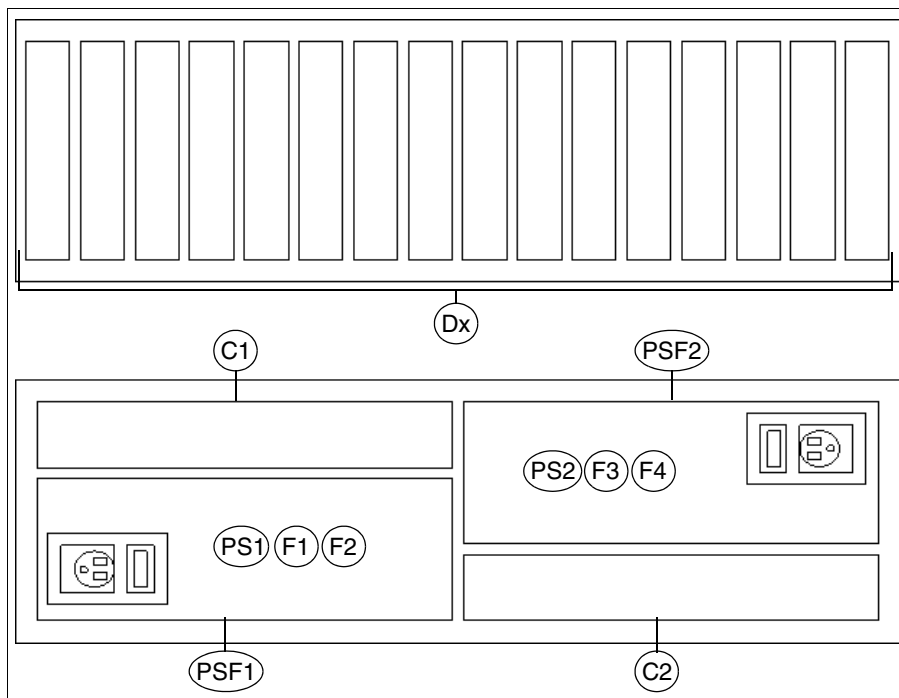


Figure 2-63 EXP5000 and EXP520 component locations

Table 2-11 Storage Manager references to EXP5000 and EXP520 component locations

Reference	Parent	Slot	Name
Dx (D1-D16)	Enclosure	1-16	Drive 1 - 16
C1	Enclosure	1	ESM A
C2	Enclosure	2	ESM B
T1	C1	1	Temperature Sensor
T2	C2	2	Temperature Sensor
PSF1	Enclosure	1	Power-Fan Canister (left)
PSF2	Enclosure	2	Power-Fan Canister (right)
PS1	PSF1	1	Power Supply (left)
PS2	PSF2	2	Power Supply (right)
F1	PSF1	1	Fan
F2	PSF1	2	Fan
F3	PSF2	3	Fan
F4	PSF2	4	Fan

2.5.2 EXP5060 Storage Expansion Unit

The IBM EXP5060 enclosure is a high capacity expansion, capable of holding up to 60 Serial Advanced Technology Attachment (SATA) disk modules. You can have a maximum of eight EXP5060s installed on either the DS5100 or the DS5300 with the proper addition of the necessary feature keys. The maximum configuration is 480 disk modules.

Best practice: For the maximum configuration on the DS5100, include the performance enhancement key as well with the configuration to increase the throughput rate to the maximum.

The design of this expansion is five drawers with 12 disks in each drawer. Supported drives are 1 TB and 2 TB models. The maximum raw capacity of a single EXP5060 is a maximum of 120 TB, or a maximum system capacity of 960 TB. Figure 2-64 shows a front view of the EXP5060 enclosure and an illustration of its front bezel.

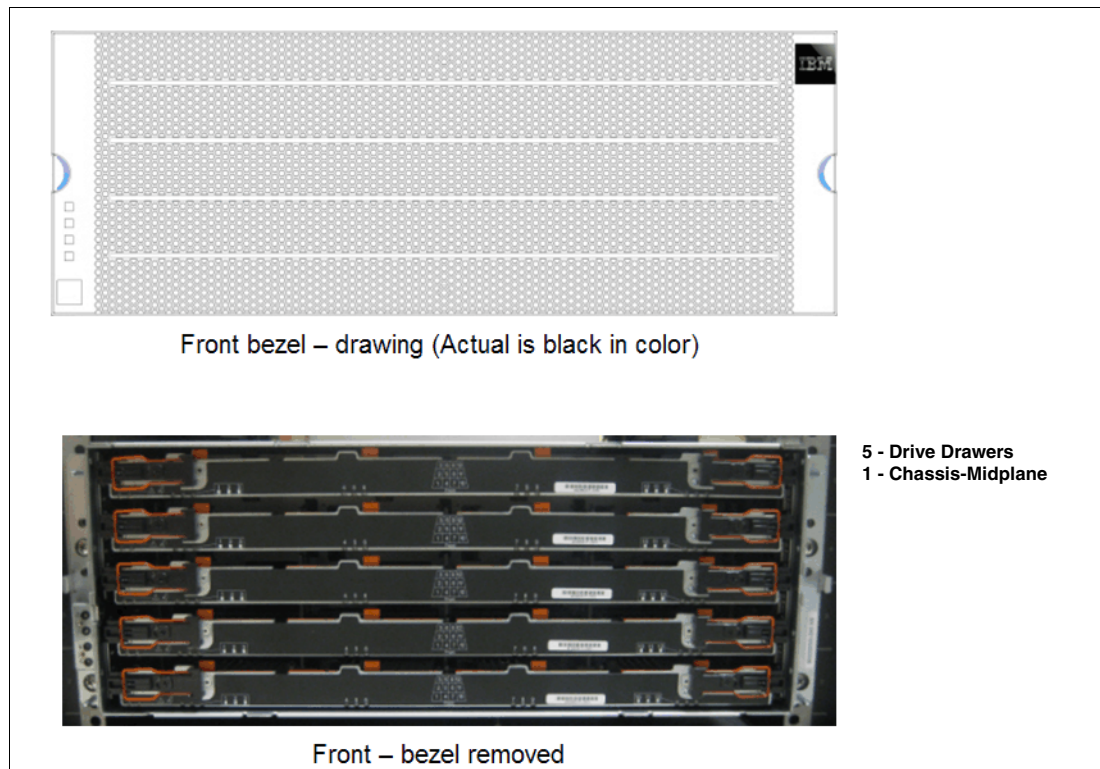


Figure 2-64 EXP5060 front bezel and drive drawers

EXP5060 components

The EXP5060 is a 5U tall chassis that is built with five drawers, and each can hold up to 12 SATA disk drives, for a total of 60 drives. There is an interconnect midplane, which connects the five drawers to the Environmental Service Modules (ESMs). There are service and status LEDs on the front panel for the EXP5060, and drive activity and service LEDs on the front of each drawer for each drive location in the drawer.

The EXP5060 has the following field replaceable units (FRUs). They can be hot-swapped, thus maintaining the availability of your system.

- ▶ Five drive drawers (trays), including the right and left cable chains.
- ▶ 20 (minimum) to 60 (maximum) SATA DDMs

- ▶ Two ESMs
- ▶ Two power supplies
- ▶ Two fan assemblies

Attention: Replacing a drive drawer will cause all the drives in that tray to become unavailable to the controllers in the storage subsystem. To replace the drawer without data access loss, all arrays containing drives in that drawer must have enclosure loss protection. If enclosure loss protection is not active, maintenance window will need to be scheduled.

The EXP5060 is also a heavy chassis with an empty weight of about 56.7 kg (125 lb) and a full chassis weight of 113 kg (250 lb). It is due to this heavy weight that the EXP5060 is not to be installed in any rack over the 32U point. When installing the chassis into the rack, it is a requirement that you use a portable lift tool to install or remove the chassis from the cabinet. Make sure that the lift tool is available on location at the time of these procedures.

Note: The ordering procedures for the lift tool vary depending on your location. Direct questions about these procedures to your regional representative.

The EXP5060s power supplies have higher wattage to handle the increased drive count and therefore require a 208 VAC circuit. Ensure that you order sufficient and proper power distribution units (PDUs) for the rack in which the EXP5060s will be installed.

Important: The EXP5060 does not support 90-136 VAC sources. It supports 180-240VAC sources only.

Drive drawers

The EXP5060 storage expansion enclosure has five removable drive drawers, each containing from 4 to 12 drives. To have an optimum airflow, a minimum of four drives must be installed in each drawer in the front four drive bays (1,4, 7, and 10). This requirement places the minimum configuration of this expansion at 20 drives. Figure 2-65 shows the drive slot locations in the drawer and the location of the four required drives.



Figure 2-65 EXP5060 drawer with required drives shown

Figure 2-66 shows the LEDs present on the front panel of each drawer.

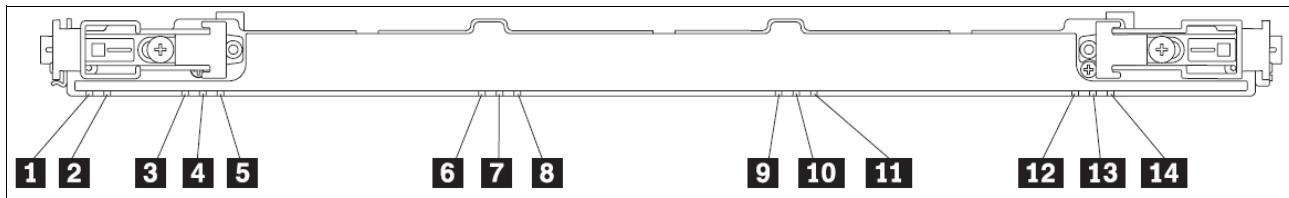


Figure 2-66 EXP5060 Drive drawer LEDs

Table 2-12 explains the LEDs shown in Figure 2-66.

Table 2-12 Drive drawer LEDs

Number	LED	Normal Status	Problem Status
1	Service Action Allowed	Off	On (Blue) - The drive drawer can be removed The drawer Service Action Allowed LED is also lit when a Service Action Allowed LED on one of the drives in the drawer is lit.
2	Service Action Required	Off	On (Amber) - A fault exists within the drive drawer

Number	LED	Normal Status	Problem Status
3-14	Drive Activity (for drives 1 to 12 in the drawer) The associated disk drive is indicated by a number (1 to 12) that is displayed inside the Drive Activity icon.	On (Green) - Power is on, drive is operating normally Blinking (Green) - Indicates drive I/O activity	Off - No power to the drive or a drive is not installed

EXP5060 disk drive modules

The SATA drive modules that are supported by the EXP5060 differ from the SATA drives that are supported by the EXP5000. The EXP5060 has a fiber to Advanced Technology Attachment (ATA) translator built into the ESMs and does not require the use of the interposer card on the disk modules. Additionally, with the horizontal mounting of the drive in the drawer, IBM has introduced a new carrier with these modules. Figure 2-67 shows the drive module and carrier that support the EXP5060. EXP5060 storage expansion enclosure supports two SATA DDMs at the moment: 1 TB SATA DDM and 2 TB SATA DDM.

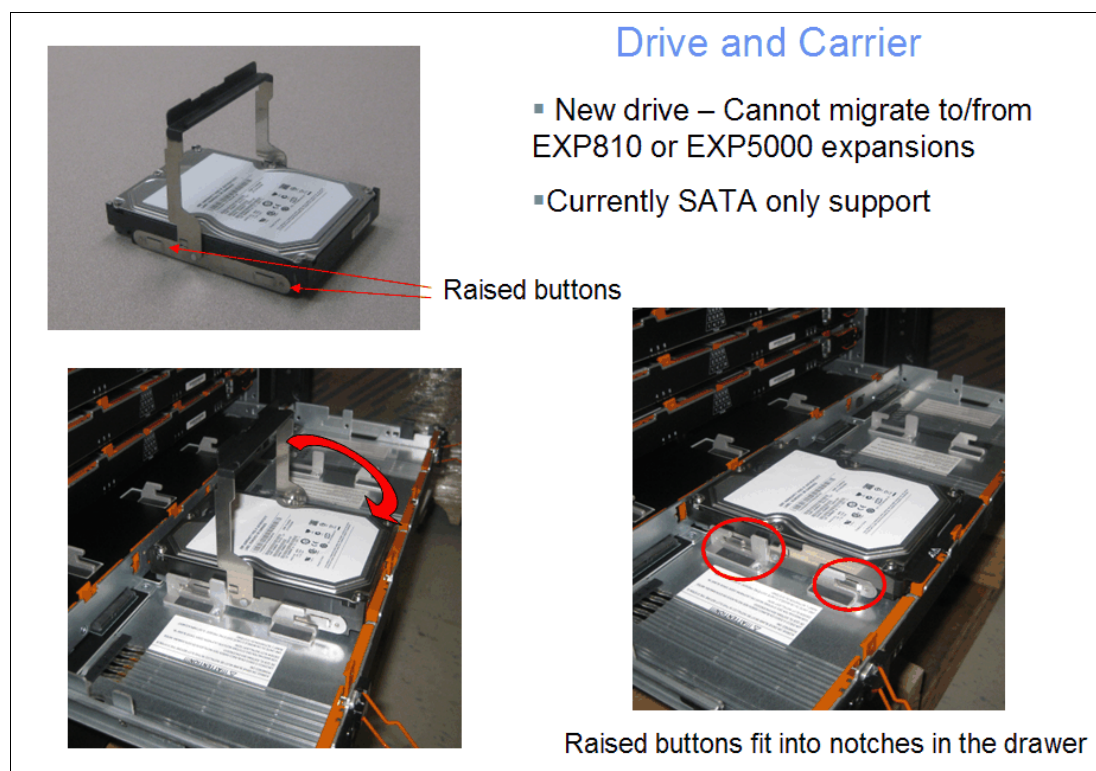


Figure 2-67 EXP5060 drive and carrier assembly

Each drive has two service LED located on the carrier assembly as shown in Figure 2-68 and explained in Table 2-13 on page 93.

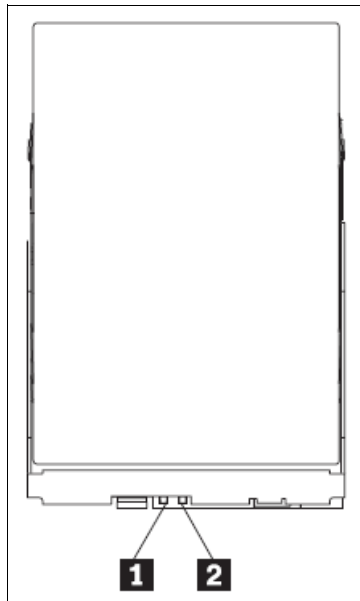


Figure 2-68 EXP5060 DDM LEDs

Table 2-13 EXP5060 DDM service LEDs

Number	LED	Normal Status	Problem Status
1	Service Action Allowed (SAA)	Off	On (Blue) - The disk drive can be removed
2	Service Action Required (SAR) (Fault)	Off	On (Amber) - A fault exists within the disk drive

Drive state of each drive can be determined by combining the LEDs shown on Figure 2-68 and explained in Table 2-13(SAA and SAR), and drive activity LED shown on Figure 2-66 and explained in Table 2-12 on page 91 (Drive activity). These states are explained in Table 2-14.

Table 2-14 EXP5060 Drive States

Drive State	Drive Activity LED (Green)	Drive SAR LED (Amber)	Drive SAA LED (Blue)
Power is not applied	Off	Off	Off
Normal operation: The power is turned on but there is no drive I/O activity	On	Off	Off
Normal operation: Drive I/O activity is occurring	Blinking	Off	Off
Service Action Required: A fault condition exists and the drive is offline	On	On	On
Power is applied but drives are spun-down because they are offline, are part of an "Exported - Ready to import" array, or are incompatible or not certified.	Off	Off	On

EXP5060 Environmental Service Modules

The Environmental Service Modules (ESMs) that are used in the EXP5060 are uniquely designed compared to other DS5000 expansions, because they add both hardware and firmware changes to support the trunking capability. Each of these modules has a second level of built-in fiber switching and a device control manager (DCM) that manages the device I/O operations. These features play a critical part in the handling, managing, and throughput capabilities of these expansions.

Figure 2-69 shows the layout of the ESM LEDs which are described in Table 2-15 on page 94.

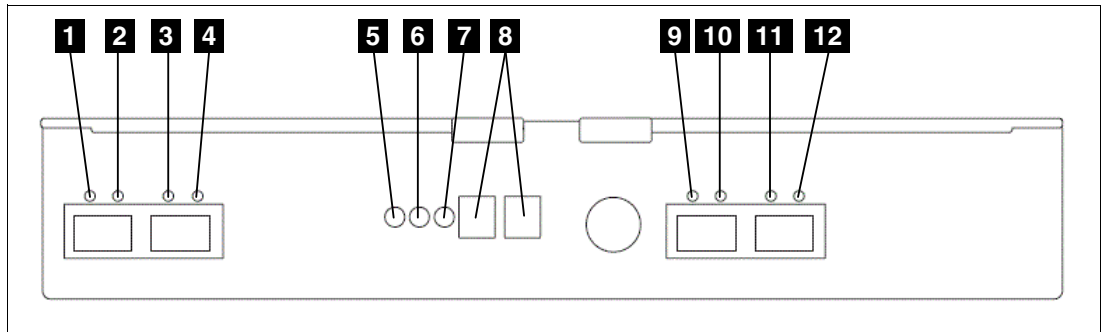


Figure 2-69 EXP5060 ESM LED layout

Table 2-15 EXP5060 ESM LEDs

Number	LED	Normal Status	Problem Status
1	ESM Link Fault (Port 1A Bypass)	Off This LED is also off when there is no SFP installed in the SFP socket.	On (Amber) - A link error has occurred Blinking (Amber) - One of the following conditions has occurred: <ul style="list-style-type: none"> ▶ The enclosure is currently running at a fibre channel rate of 4 Gb/s, but the installed SFP is only rated for 2 Gb/s. Install a 4 Gb/s rated SFP. ▶ There is a hardware problem with the SFP or the link that prevents the port from being successfully inserted into the fibre channel loop. This could be caused by a failed SFP or failed ESMs. ▶ There is a trunking connection problem with the associated SFP port. See the seven-segment display code to determine the nature of the problem.

Number	LED	Normal Status	Problem Status
2, 3	Loop Up/Rate Select	On (Green) Both LEDs light to indicate that the fibre channel loop to ports 1A and 1B is up. These LEDs are not associated with a specific SFP port and their status indicates the overall fibre channel loop status.	Off - A link error has occurred
4	ESM Link Fault (Port 1B Bypass)	Off This LED is also off when there is no SFP installed in the SFP socket.	On (Amber) - A link error has occurred Blinking (Amber) - One of the following conditions has occurred: <ul style="list-style-type: none"> ► The enclosure is currently running at a fibre channel rate of 4 Gb/s, but the installed SFP is only rated for 2 Gb/s. Install a 4 Gb/s rated SFP. ► There is a hardware problem with the SFP or the link that prevents the port from being successfully inserted into the fibre channel loop. This could be caused by a failed SFP or failed ESMs. ► There is a trunking connection problem with the associated SFP port. See the seven-segment display code to determine the nature of the problem.
5	ESM Service Action Allowed	Off	On (Blue) - The ESM can be removed
6	ESM Service Action Required (Fault)	Off	On (Amber) - A fault exists within the ESM
7	ESM Power	On (Green)	Off - No power to the ESM
8	Seven-segment numeric display	See for more information	

Number	LED	Normal Status	Problem Status
9	ESM Link Fault (Port 2A Bypass)	Off This LED is also off when there is no SFP installed in the SFP socket.	On (Amber) - A link error has occurred Blinking (Amber) - One of the following conditions has occurred: <ul style="list-style-type: none"> ► The enclosure is currently running at a fibre channel rate of 4 Gb/s, but the installed SFP is only rated for 2 Gb/s. Install a 4 Gb/s rated SFP. ► There is a hardware problem with the SFP or the link that prevents the port from being successfully inserted into the fibre channel loop. This could be caused by a failed SFP or failed ESMs. ► There is a trunking connection problem with the associated SFP port. See the seven-segment display code to determine the nature of the problem.
10, 11	Loop Up/Rate Select	On (Green) Both LEDs light to indicate that the fibre channel loop to ports 2A and 2B is up. These LEDs are not associated with a specific SFP port and their status indicates the overall fibre channel loop status.	Off - A link error has occurred

Number	LED	Normal Status	Problem Status
12	ESM Link Fault (Port 2B Bypass)	Off This LED is also off when there is no SFP installed in the SFP socket.	On (Amber) - A link error has occurred Blinking (Amber) - One of the following conditions has occurred: <ul style="list-style-type: none"> ▶ The enclosure is currently running at a fibre channel rate of 4 Gb/s, but the installed SFP is only rated for 2 Gb/s. Install a 4 Gb/s rated SFP. ▶ There is a hardware problem with the SFP or the link that prevents the port from being successfully inserted into the fibre channel loop. This could be caused by a failed SFP or failed ESMs. ▶ There is a trunking connection problem with the associated SFP port. See the seven-segment display code to determine the nature of the problem.

EXP5060 power supply

Each EXP5060 has two fully redundant power supplies that provide power to the internal components. If one power supply is turned off or malfunctions, the other power supply maintains electrical power to the storage.

Note: To preserve the optimal airflow, do not remove a failed power supply FRU from the EXP5060 chassis until you are ready to replace it with a new FRU.

Figure 2-70 shows the layout of the LEDs on the EXP5060 power supply and their status is described in Table 2-16 on page 98.

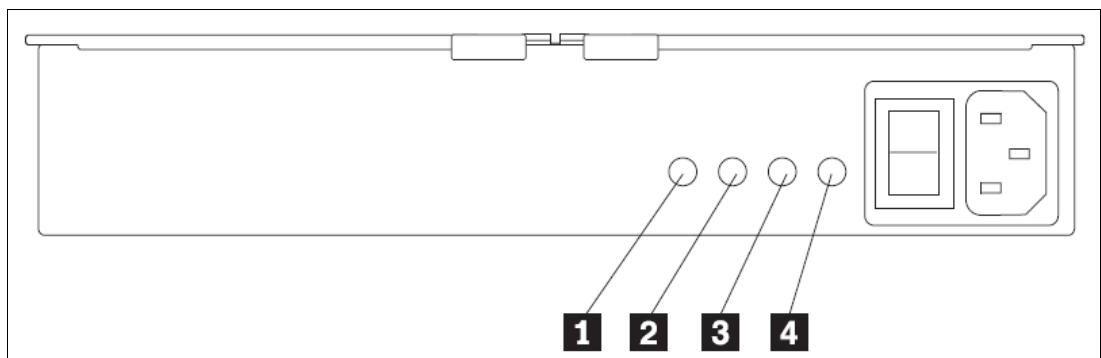


Figure 2-70 EXP5060 power supply LEDs

Table 2-16 EXP5060 power supply LEDs description

Number	LED	Normal Status	Problem Status
1	DC Power	On (Green)	Off - No DC power from power supply. The power supply is faulty.
2	Service Action Allowed	Off	On (Blue) - The power supply can be removed
3	Service Action Required (Fault)	Off	On (Amber) - A fault exists within the power supply
4	AC Power	On (Green)	Off - No AC power to power supply

EXP5060 fan assembly

The storage expansion enclosure has two removable fan assemblies. Each fan assembly contains two fans. The fan assemblies pull air through the enclosure from front to back across the drives. The fans provide redundant cooling, which means that if one of the fans fails, the remaining fan assembly continues to provide sufficient cooling to operate the storage expansion enclosure. The fan will operate at maximum speed under the following conditions:

- ▶ During the first few minutes after power is applied to the EXP5060 enclosure
- ▶ When one of the disk drawers is pulled out or not in the closed/latched position
- ▶ When one of the fan assemblies has failed or is removed from the EXP5060 chassis

Note: To preserve the optimal airflow, do not remove a failed fan assembly FRU from the EXP5060 chassis until you are ready to replace it with a new FRU.

Note: Although both fan assemblies (left and right) are identical, they are seated in the EXP5060 enclosure in opposite orientations. If the fan assembly cannot be fully inserted in the fan assembly bay, rotate it 180 degrees and reinsert it. In addition, there are notches on the top and bottom of the fan assembly bay. Make sure that the slits on the top and bottom of the fan assembly line up with these two notches before the fan assembly is fully inserted in the fanbay.

Figure 2-71 and Table 2-17 on page 99 describe the LEDs found on the EXP5060 fan assembly.

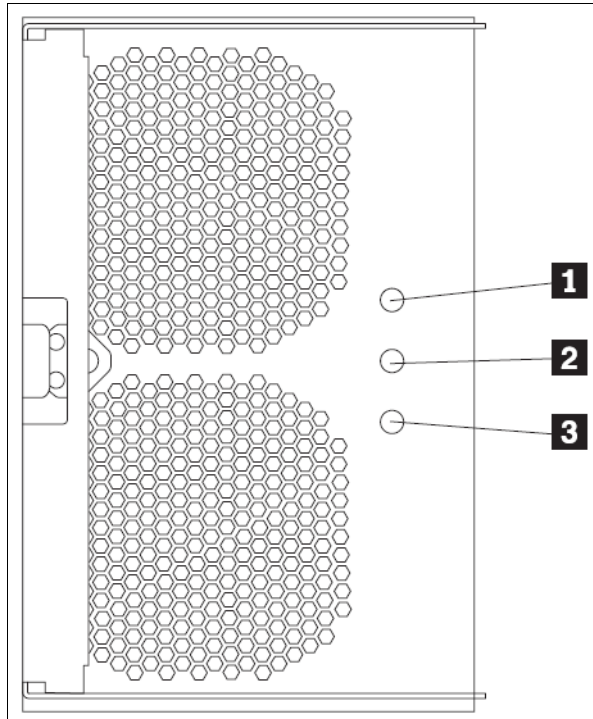


Figure 2-71 EXP5060 fan assembly LEDs

Table 2-17 EXP5060 fan assembly LEDs description

Number	LED	Normal Status	Problem Status
1	Power	On (Green)	Off - No power to fan assembly
2	Service Action Required (Fault)	Off	On (Amber) - A fault exists within the fan assembly
3	Service Action Allowed	Off	On (Blue) - The fan assembly can be removed

EXP5060 component locations

This section will show all EXP5060 storage expansion enclosure component locations as displayed in Storage Manager (SM) software.

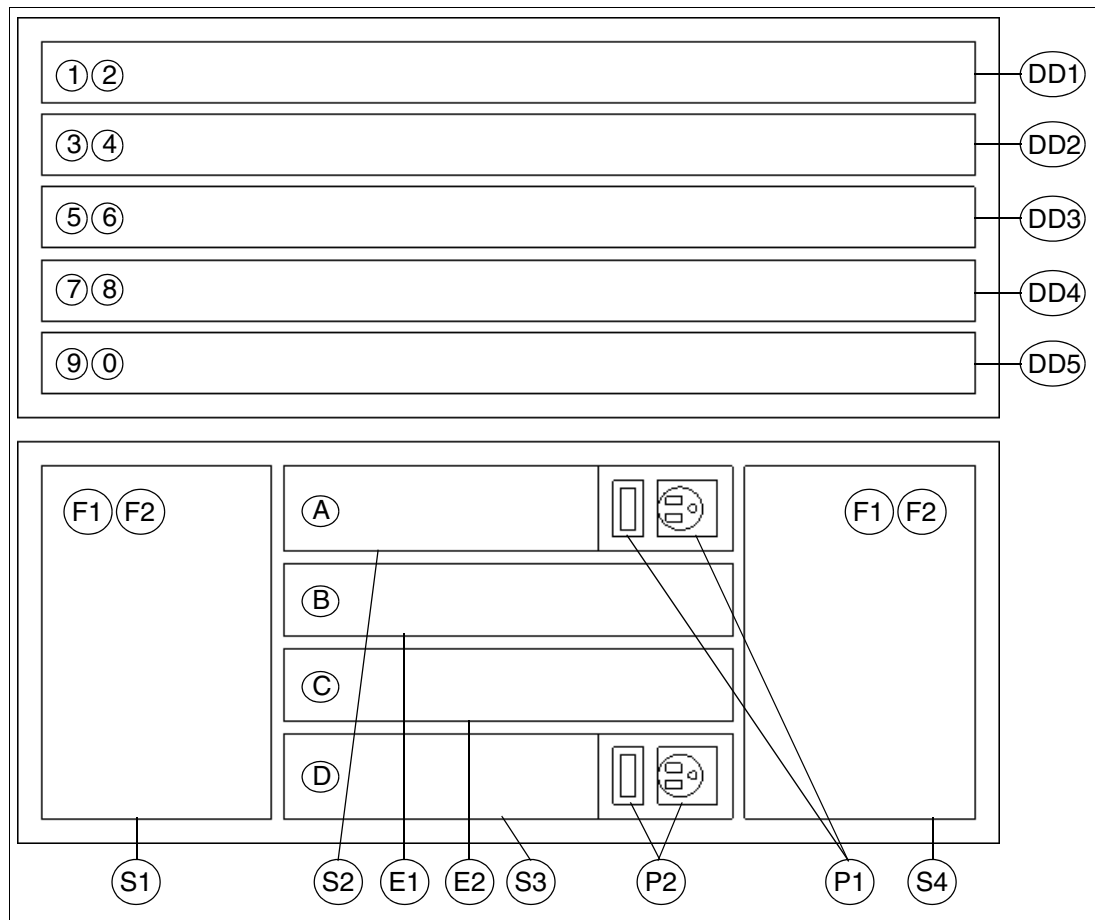


Figure 2-72 EXP5060 component locations

Table 2-18 Storage Manager references to EXP5060 component locations

Reference	Parent	Slot	Name
DD1-DD5	Enclosure	1-5	Drive Drawer 1-5 (contains 12 drives, numbered 1-12)
E1	Enclosure	1	ESM A
E2	Enclosure	2	ESM B
S1	Enclosure	1	Power-fan canister 1 (left)
S2	Enclosure	2	Power-fan canister 2 (top)
S3	Enclosure	3	Power-fan canister 3 (bottom)
S4	Enclosure	4	Power-fan canister 4 (right)
P1	S2	1	Power Supply (top)
P2	S3	1	Power Supply (bottom)
F1	S1	1	Fan
F2	S1	2	Fan
F3	S4	1	Fan

Reference	Parent	Slot	Name
F4	S4	2	Fan
1	DD1	1	Temperature Sensor
2	DD1	2	Temperature Sensor
3	DD2	1	Temperature Sensor
4	DD2	2	Temperature Sensor
5	DD3	1	Temperature Sensor
6	DD3	2	Temperature Sensor
7	DD4	1	Temperature Sensor
8	DD4	2	Temperature Sensor
9	DD5	1	Temperature Sensor
0	DD5	2	Temperature Sensor
A	S2	1	Temperature Sensor
B	E1	1	Temperature Sensor
C	E2	1	Temperature Sensor
D	S3	1	Temperature Sensor

2.6 DS5000 storage subsystem drive-side cabling

In this section, we explore different drive-side cabling configurations for the storage expansion enclosures that are available with the DS5000 family.

2.6.1 EXP5000 storage expansion enclosure cabling rules

The following rules apply while cabling the DS5000 with an EXP5000/EXP810 storage expansion enclosure:

- The maximum number of expansion enclosures (EXP5000 or EXP810) in a drive loop is limited to seven, as the maximum 112 disks limitation is reached with seven enclosures configured with 16 drives each.

Note: Attaching EXP810 to DS5000 is supported but you need to request an RPQ for that configuration.

- Each FC-drive and expansion unit (EXP) in the drive channel must operate at the same Fibre Channel speed (either 2 Gbps or 4 Gbps). SATA drives auto negotiate to the speed of the EXP.
- The DS5000 controller drive port must always be connected to the expansion enclosure port labelled 1B. Because the left and right EXP5000 ESMs (ESMs A and B) or top and are inserted in the ESM bays in different orientations, ensure that you use the port labeled 1B, as shown in Figure 2-73. Port 1A is used to daisy-chain the next expansion units, which we refer to later in this section

- EXP5000 does not support drive-side trunking. Do not make any connections to port 2A and 2B of the EXP5000 ESM ports.

Note: To achieve the best performance, spread all your expansion units among all port channels.

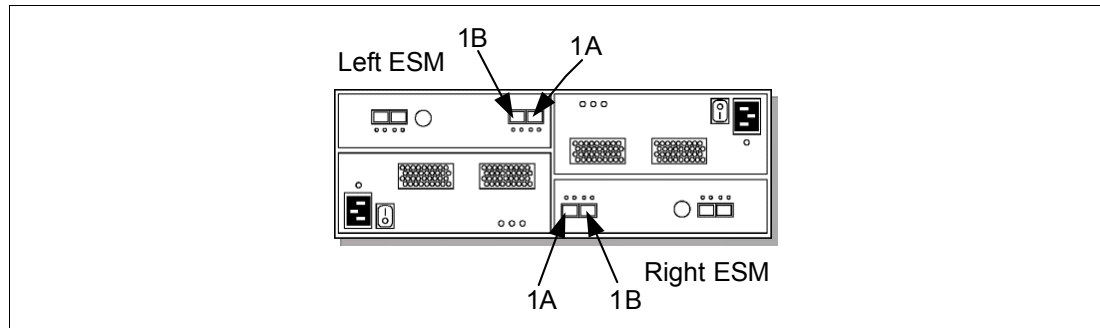


Figure 2-73 Port labels on EXP5000

The DS5000 storage subsystem can attach up to 28 EXP5000s or EXP810s or a intermix of the two for migration purpose. It also fully supports an intermix of the FC and SATA drives inside enclosures to allow users maximum flexibility for customizing storage solutions. It is generally best to spread enclosures evenly among the eight drive channel pairs as you scale up your DS5000 storage subsystem's storage capacity. This allows you to fully utilize the maximum drive-side bandwidth. For attaching the first four enclosures, use all the drive channels, with one port per channel, as shown in Figure 2-74.

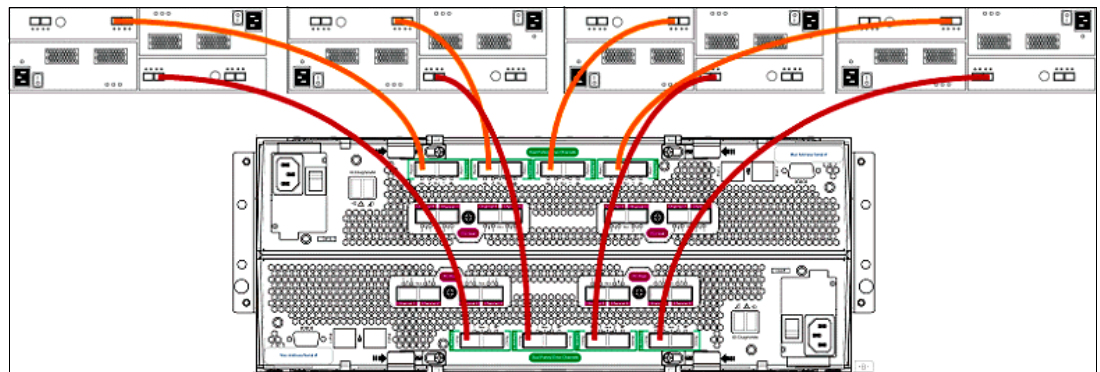


Figure 2-74 DS5000 with four expansion units

When attaching the next four enclosures, use the next ports in each channel, as shown in Figure 2-75. For an eight enclosure configuration, each enclosure is attached to a dedicated drive port pair.

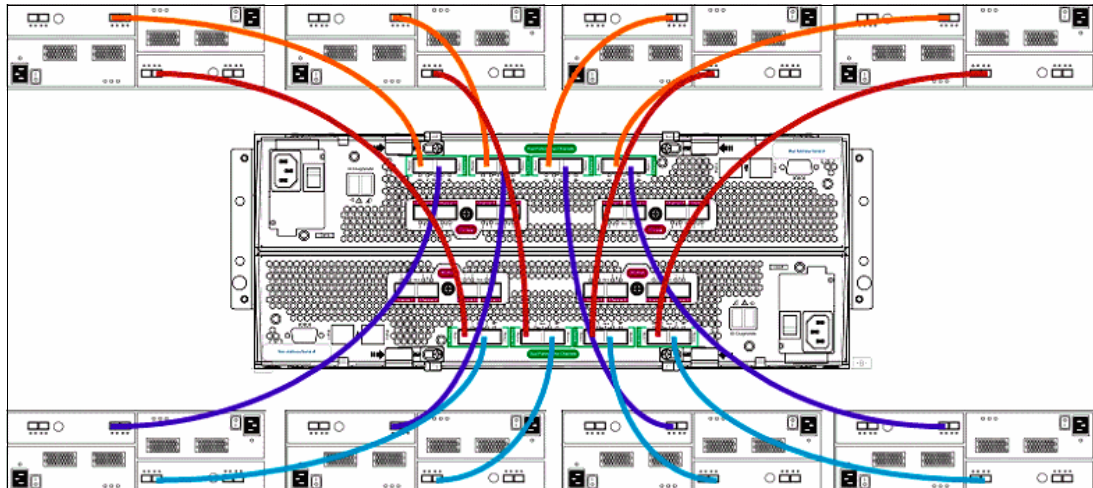


Figure 2-75 DS5000 with eight expansion units

When attaching the nine or more enclosures, attach them to existing drive loops by daisy-chaining them. A 256 drive configuration should have two expansion enclosures on each drive-side channel pair and uses 16 EXPs in summary, as shown in Figure 2-76.

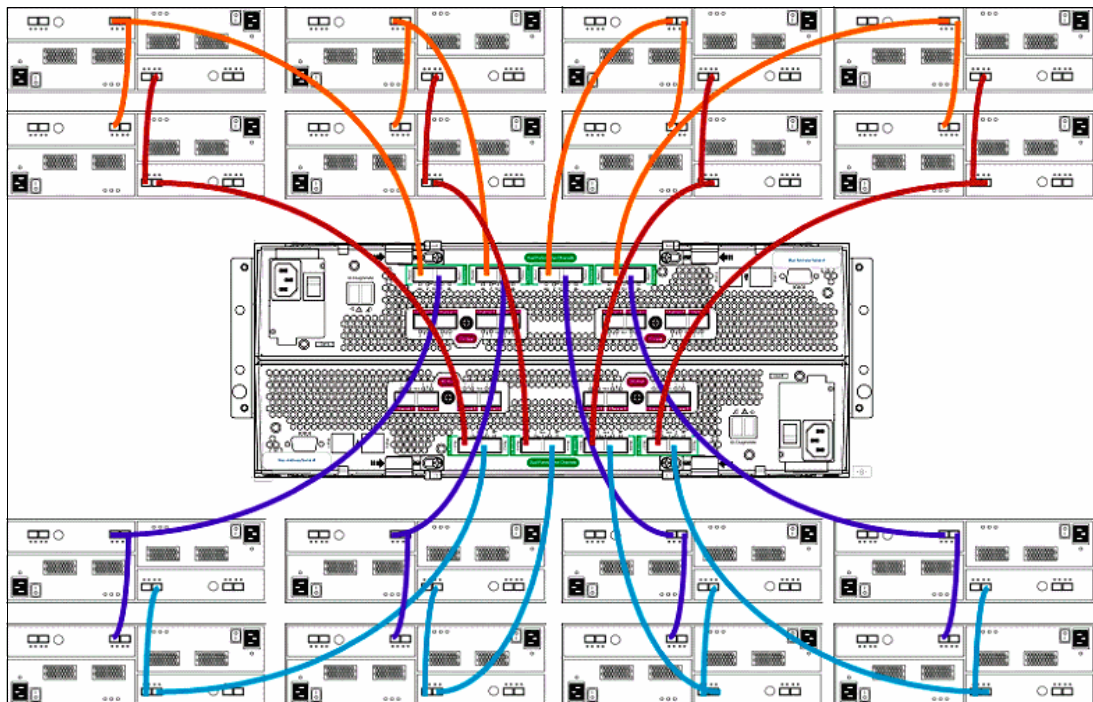


Figure 2-76 DS5000 with 16 expansion units

The DS5000 supports the 448 drive configuration with EXP5000. It requires you to attach seven expansion units (EXP5000) to one redundant drive port channel pair. As a result, you will have four EXPs connected to one drive port pair and three EXPs to the other drive port pair of the same channel, as shown in Figure 2-77.

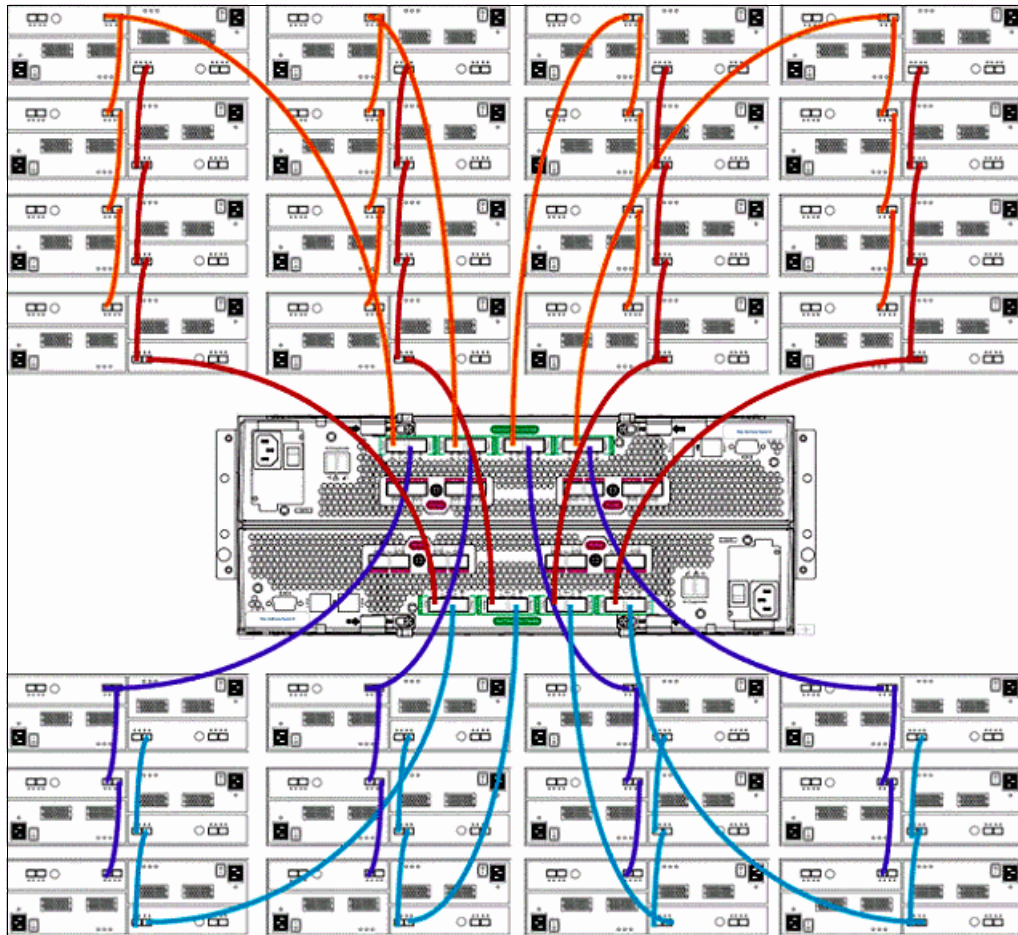


Figure 2-77 DS5000 with 28 expansion units

Note: Make sure that when you mix different speed EXPs that both disk ports in a drive channel operate at the same speed. If you attach a disk enclosure that operates at 2 Gbps, both ports in the controller's disk channel and all drives will work at 2 Gbps.

Remember to connect a 2 Gbps and 4 Gbps enclosure to different channels, as shown in Figure 2-78.

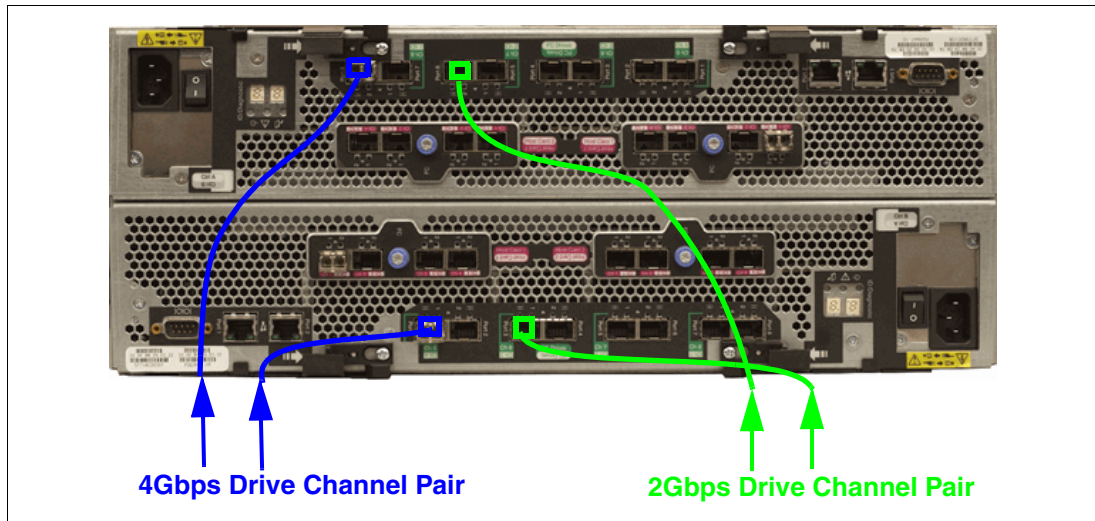


Figure 2-78 Example of a mixed drive-side environment (2 or 4 Gbps)

Additional materials regarding cabling can be found in the *IBM System Storage DS4000/DS5000 Hard Drive and Storage Expansion Enclosure Installation and Migration Guide*, GC53-1139.

2.6.2 EXP5060 storage expansion enclosure cabling rules

The following rules apply while cabling the DS5000 with an EXP5060 storage expansion enclosure:

- ▶ The maximum number of expansion enclosures EXP5060 in a drive loop is limited to two.
- ▶ The maximum number of expansion enclosures EX5060 in a configuration is eight.

Note: Maximum configuration requires purchase of an Attached up to eight EXP5060 feature pack.

- ▶ The DS5000 controller drive port must always be connected to the expansion enclosure port labelled 1B in a non-trunking configuration and 2B in a trunking configuration. Port labels are shown in Figure 2-79.
- ▶ Ports 1A and 2A on EXP5060 are used for a daisy chain configuration which will be explained later in this section.
- ▶ Intermixing enclosures with trunked and non-trunked cabling in the same storage subsystem is supported.
- ▶ Do not cable the EXP5060 storage expansion enclosures in a daisy chain scheme unless all drive channel ports are used to support the additional EXP5060s.
- ▶ Connect the EXP5060 and EXP5000/EXP810 storage expansion enclosures in separate drive channels in each controller to enable drive-side trunking with the EXP5060 storage expansion enclosure.

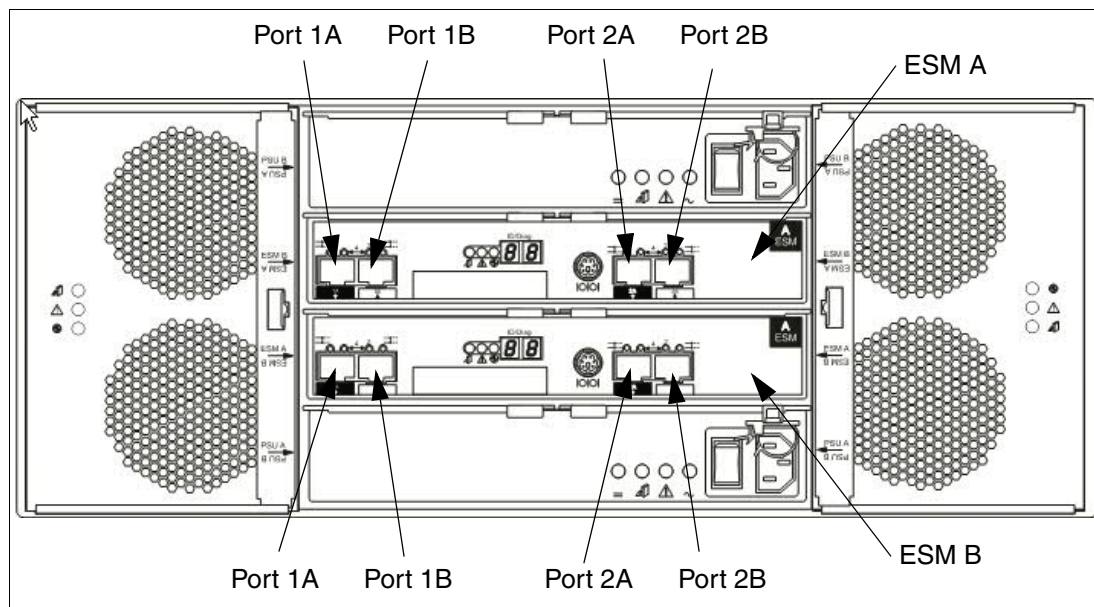


Figure 2-79 Port labels on EXP5060

DS5000 can attach up to eight EXP5060 enclosures for a maximum configuration of 480 SATA drives. EXP5060 can be cabled in two major styles: non-trunked and trunked. In a non-trunked configuration, you can combine the EXP5060 with EXP5000 expansions to create an environment for shared workloads with Fibre Channel drives and large SATA capacity needs. Or, you can trunk the EXP5060 across two loop pairs for dedicated high throughput environments to support large streaming applications. In the trunked configurations, the EXP5060 can reach maximum throughput numbers driving all the back-end channels to their maximum limits

EXP5000 and EXP5060 mixed environment

When mixed with the EXP5000 expansion, place each expansion type on its own loop pair of cables. However, when necessary, you can cable the EXP5060 to cascade directly behind an EXP5000. In this configuration, the single loop pair connects to both of the expansions (as shown in Figure 2-80), which is an example of the cascaded configuration.

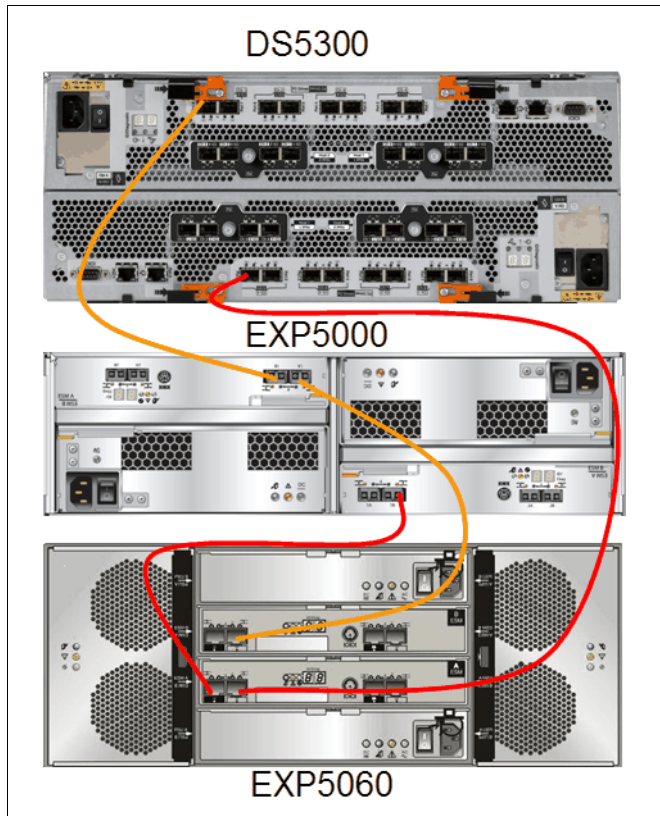


Figure 2-80 EXP5000 and EXP5060 cascaded on the same loop pair

Although it is a supported configuration, we do not recommend that you cascade multiple EXP5000s with the EXP5060. Having a high number of disks on the same loop pair risks higher channel contention from the members. In this configuration, you cannot use trunking to enhance the throughput capabilities.

2.6.3 Non-trunked EXP5060 only

You can also install the EXP5060 in the standard configuration with one EXP5060 per loop pair installed on each of the DS5100 or DS5300 loop pairs. In this configuration, the system can reach its maximum configuration of eight EXP5060s. This configuration cannot include any EXP5000s. To support this maximum configuration, you must add a special feature key to the DS5100 or DS5300 storage subsystems.

Important: For the maximum configuration special feature key to work on the DS5100, you must order the performance enhancement feature key first.

When configuring the EXP5060 in this non-trunked environment, follow the recommended cabling, array, and LUN layout practices that are used with the EXP5000s. Use the *IBM Midrange System Storage Implementation and Best Practices Guide*, SG24-6363, to determine the preferred way to lay out the arrays and LUNs for the best throughput and balanced workload handling. Figure 2-81 shows an EXP5060 that is connected in a non-trunked configuration.

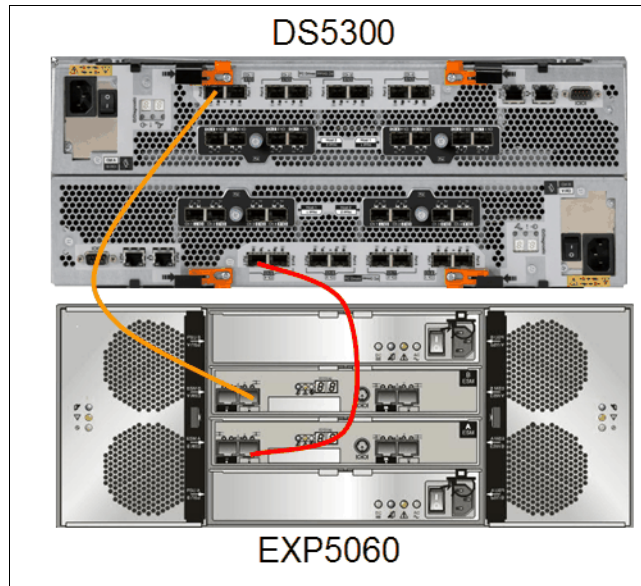


Figure 2-81 EXP5060 cabled non-trunked to the DS5300

You can copy this single unit per port configuration easily for each of the eight expansions on the port pairs for a full configuration. Figure 2-82 shows a simplified drawing of the connections for this full configuration.

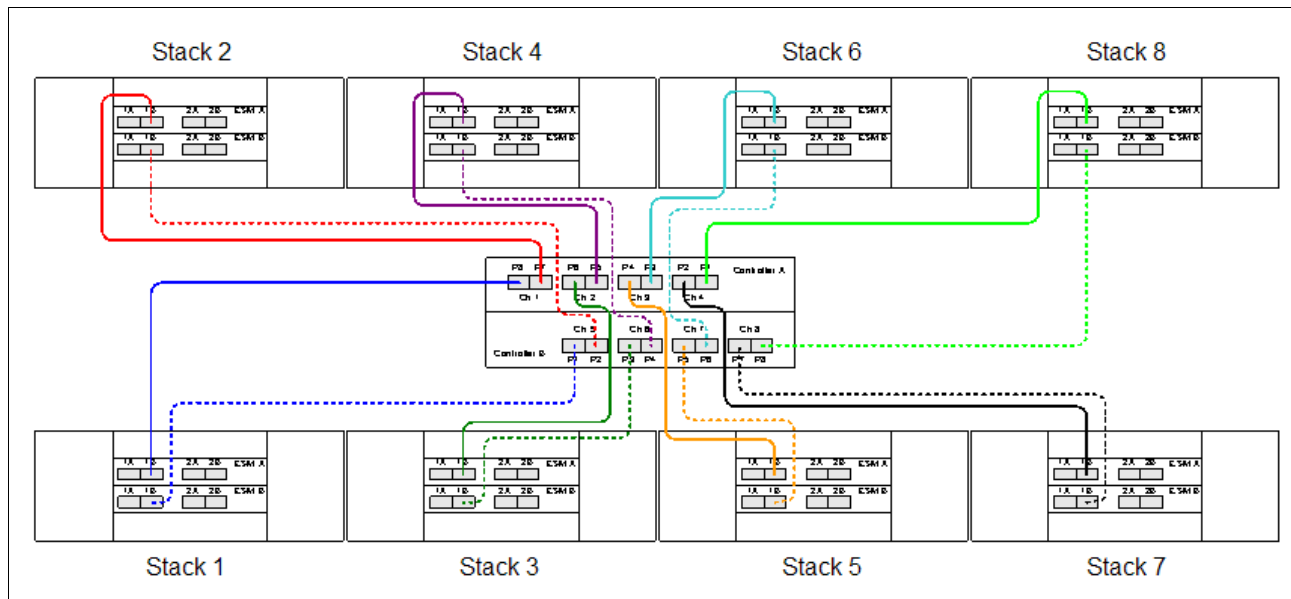


Figure 2-82 Cabling for non-trunked configuration of eight EXP5060s

In certain mixed EXP5000 and EXP5060 environments, it is sometimes necessary to cascade EXP5060s on the same loop pair. Although this configuration is supported, it is not a best practice. If you need large storage capacity that has minimal use, and if disk performance and EXP5000 I/O performance are critical, cascading the EXP5060s by using the non-trunked cabling scheme might meet the need for this environment. However, as shown in Figure 2-83, the disks in the EXP5060s in each drive channel loop pair are limited to an average of half the channel bandwidth for each expansion of 60 disks.

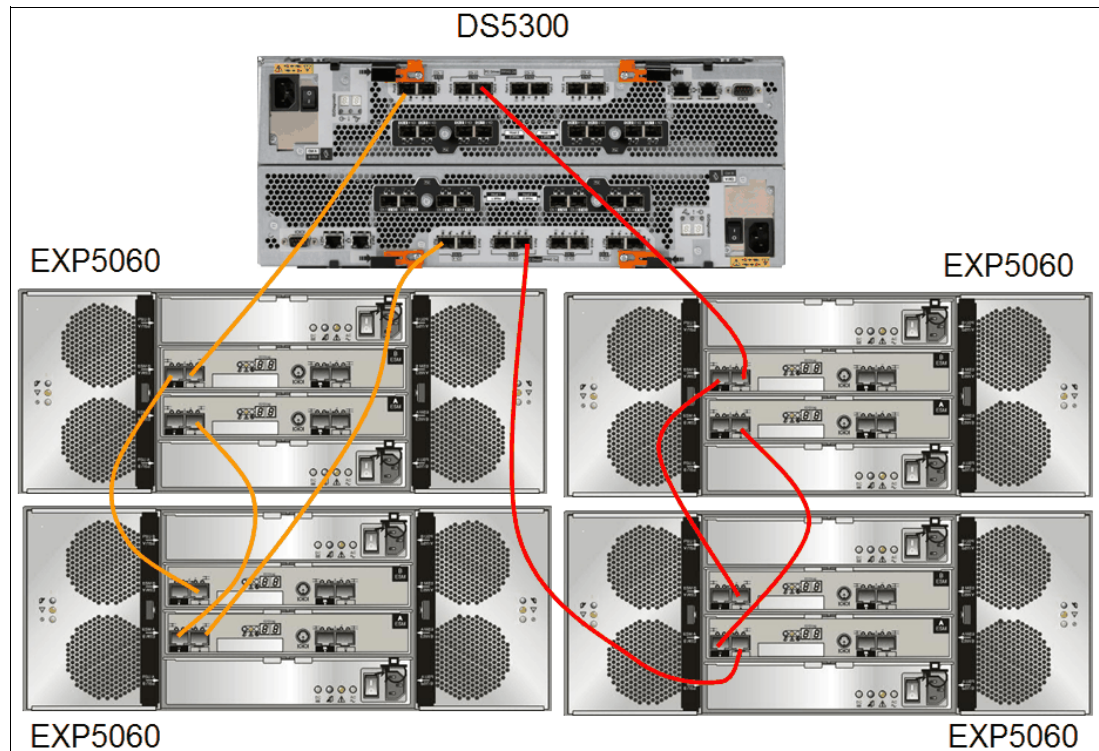


Figure 2-83 EXP5060 non-trunked and cascaded configuration

Normally, in the non-trunked environment, we recommend that you attach a single EXP5060 on a channel loop pair, as shown in Figure 2-81. If possible, it is better to cascade the EXP5000 expansion so that the EXP5060s can be spread across more channel pairs or built into a trunked configuration,

Trunking the EXP5060

With the new design of the EXP5060 expansion, we now can trunk the expansion across four loops to get the full throughput of a pair of channels using only one EXP5060 worth of disks (60 drives). This design makes it possible to achieve over 6 GBps for the DS5300 subsystem. So, when your requirement is for high throughput with fewer EXP5060s and a lower drive count, the trunked design is a great solution. In the trunked configuration, you can use a total of four EXP5060s to drive the full bandwidth of all of the eight back-end channels. Figure 2-84 shows two EXP5060s in a trunked configuration.

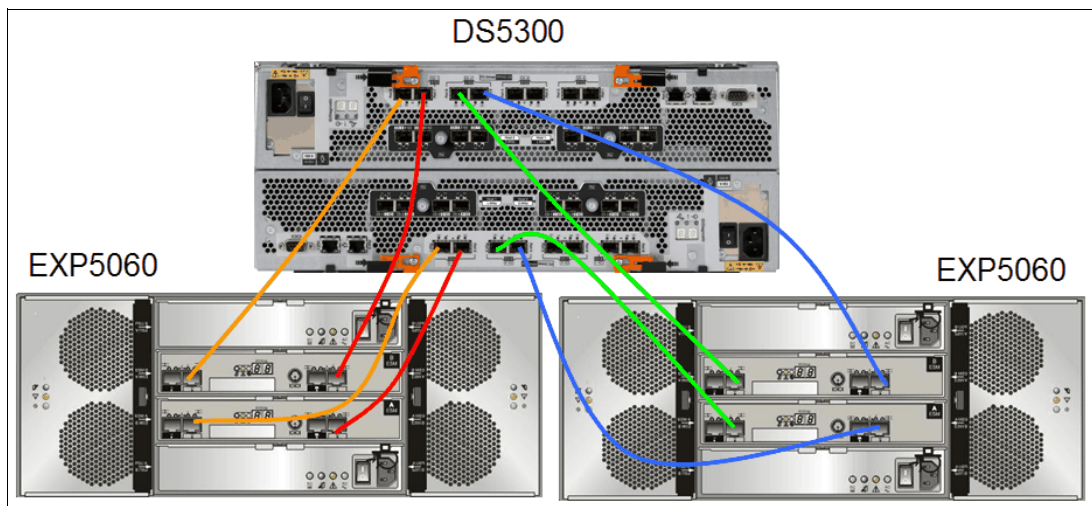


Figure 2-84 EXP5060 trunked configuration

Figure 2-85 shows a drawing of four EXP5060s in a trunked configuration that reaches the full 6 GBps throughput of the DS5300 subsystem.

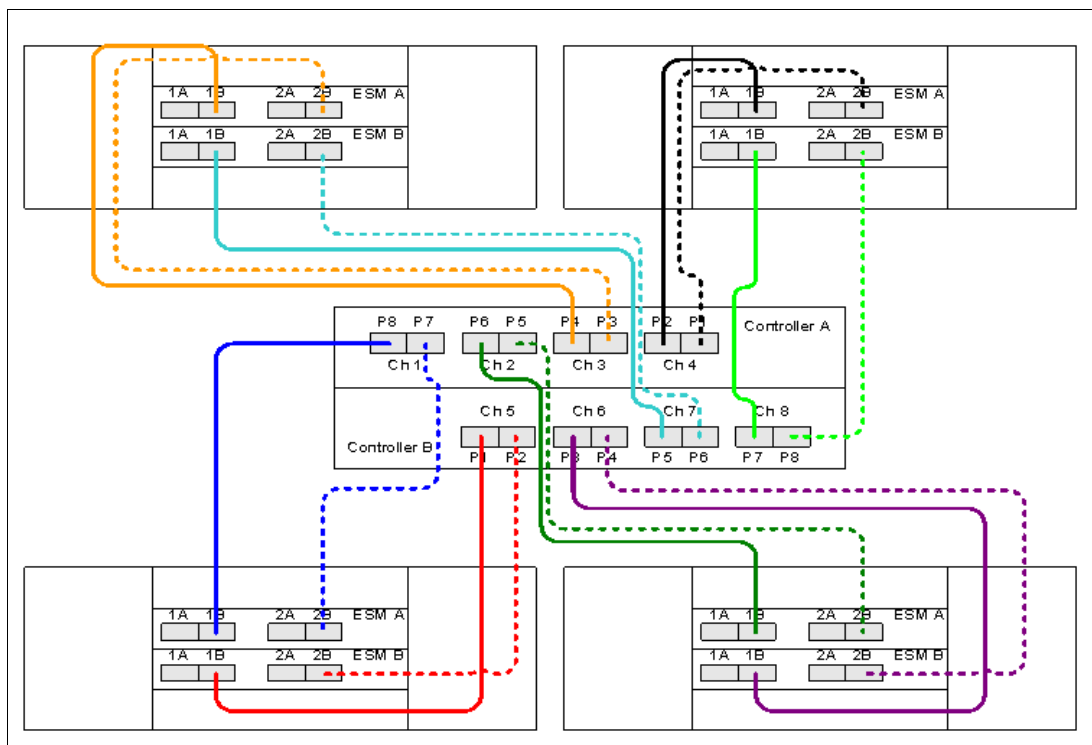


Figure 2-85 Four EXP5060s in trunked configuration for maximum throughput

You also can design a cascaded, trunked configuration with up to the full eight EXP5060s attached. In this configuration, there is no real throughput enhancement over the full non-trunked configuration. The cascaded configuration of the two EXP5060s per trunked channel pair results in the same number of disks being addressed per channel pair as in the non-trunked environment. Therefore, the same number of active disks is possible.

Figure 2-86 shows the four EXP5060s in a cascaded and trunked configuration.

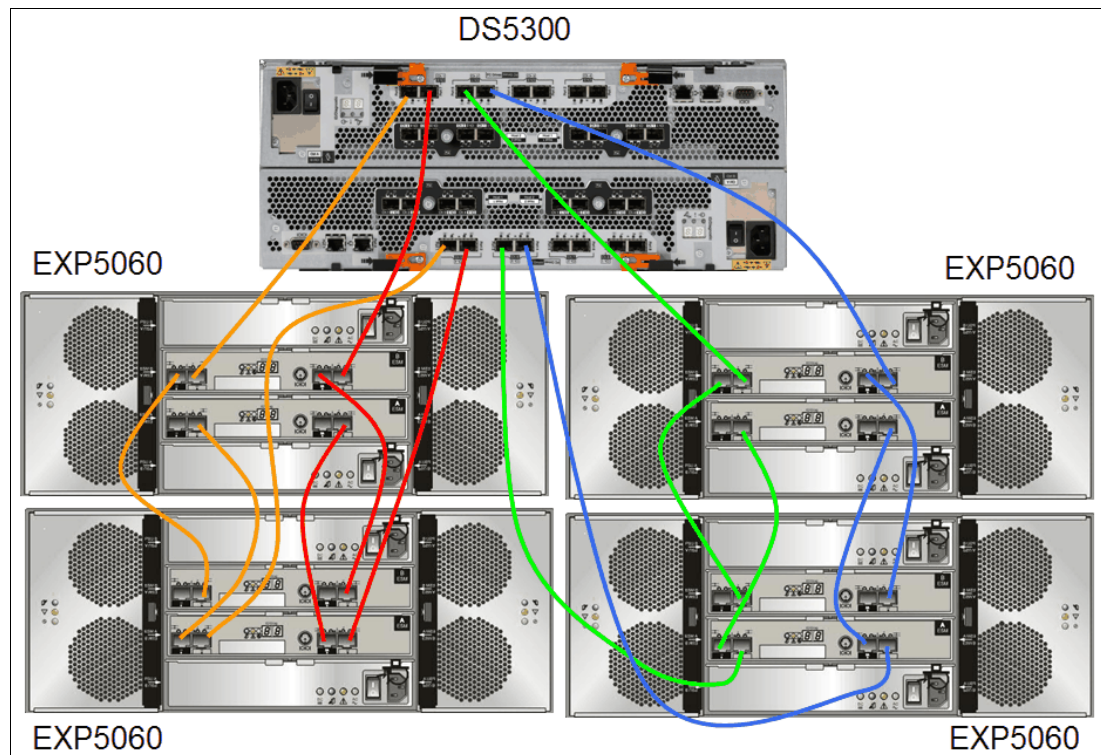


Figure 2-86 EXP5060s in a trunked and cascaded configuration

The major advantage of the cascaded, trunked configuration is the number of paths available for path redundancy. The additional disks can help with I/O per second (IOPS) limits. However, this environment is not designed for I/O-based applications, and the trunking of the channels does not help in this area.

With the EXP5060, it is critical for throughput performance that you observe the cabling recommendations for best practices. It is also critical to build the arrays and LUNs so that the resources are properly spread and evenly used.

2.6.4 DS5020 storage subsystem drive-side cabling

The drive-side cabling for the DS5020 depends on how many expansion units you must attach:

- If you attach only one enclosure, make sure that you have one connection to each of the controllers, thus using one of the two ports on each controller (controller A port 2 and controller B port 1), as shown in Figure 2-87.

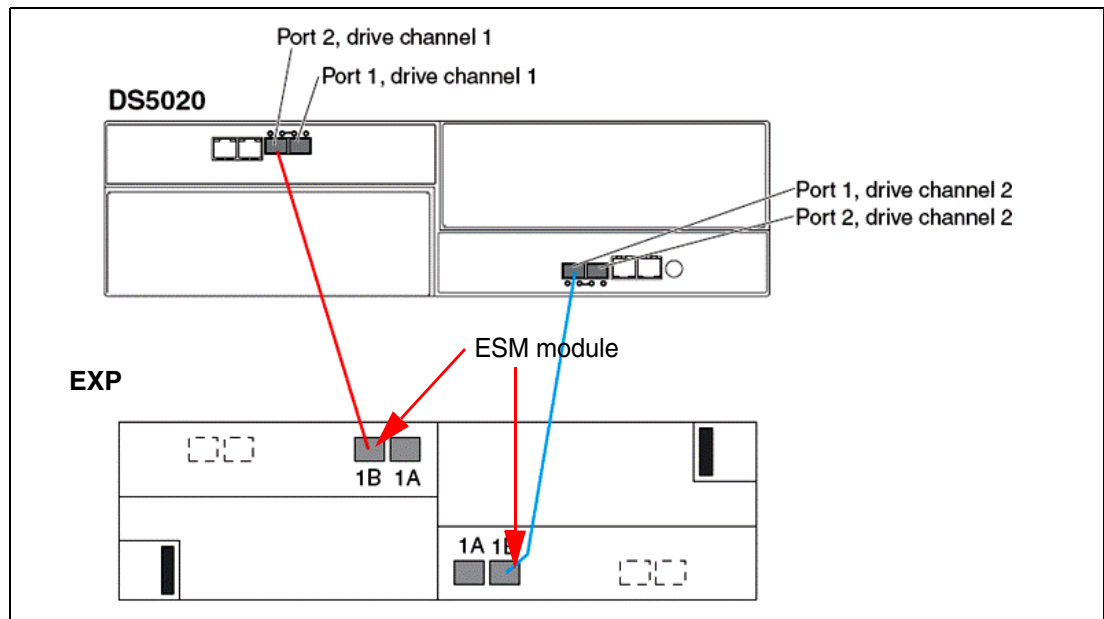


Figure 2-87 DS5020 drive cabling with one EXP

- If you attach a second expansion unit, connect it by using the second port on the controller (controller A port 1 and controller B port 2), as shown in Figure 2-88.

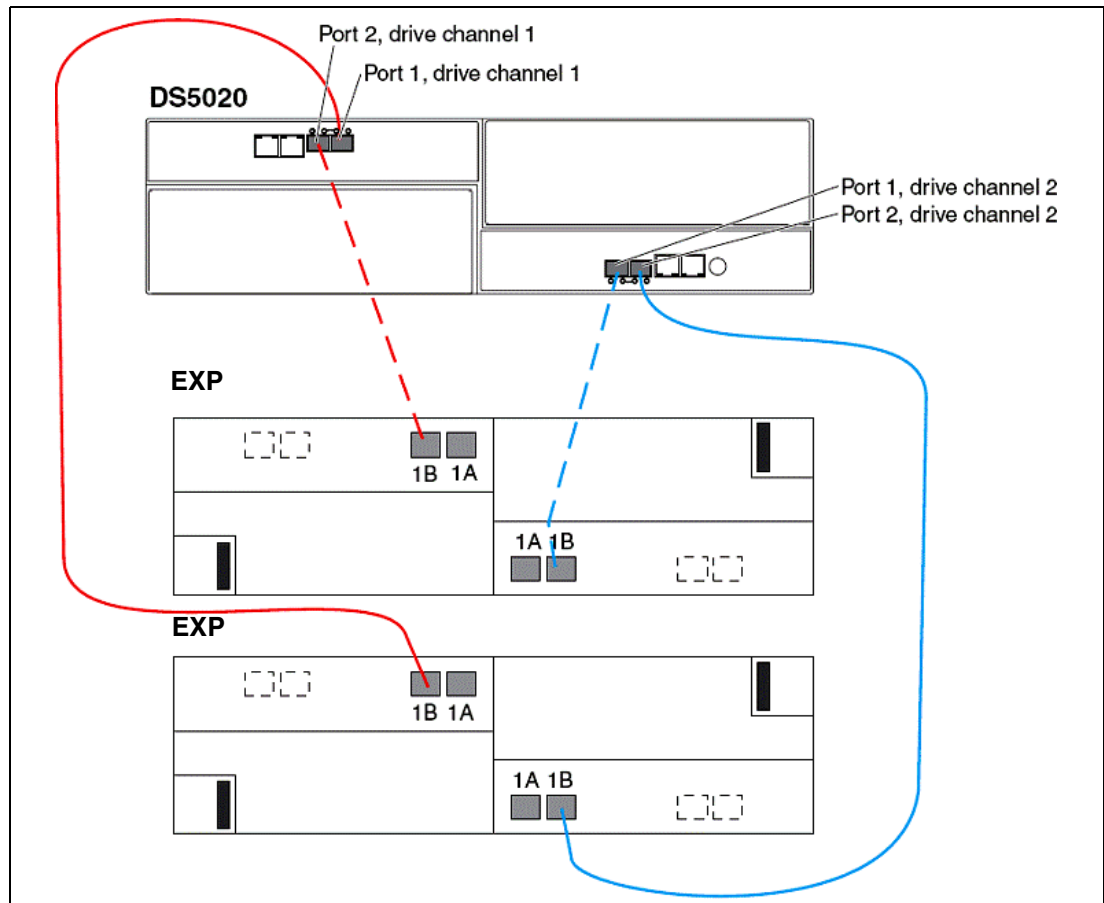


Figure 2-88 DS5020 drive cabling with two EXPs

- Beyond two enclosures (up to a maximum of six), make sure that you equally distribute the enclosures among the redundant drive channel pairs (Figure 2-89 and Figure 2-90).

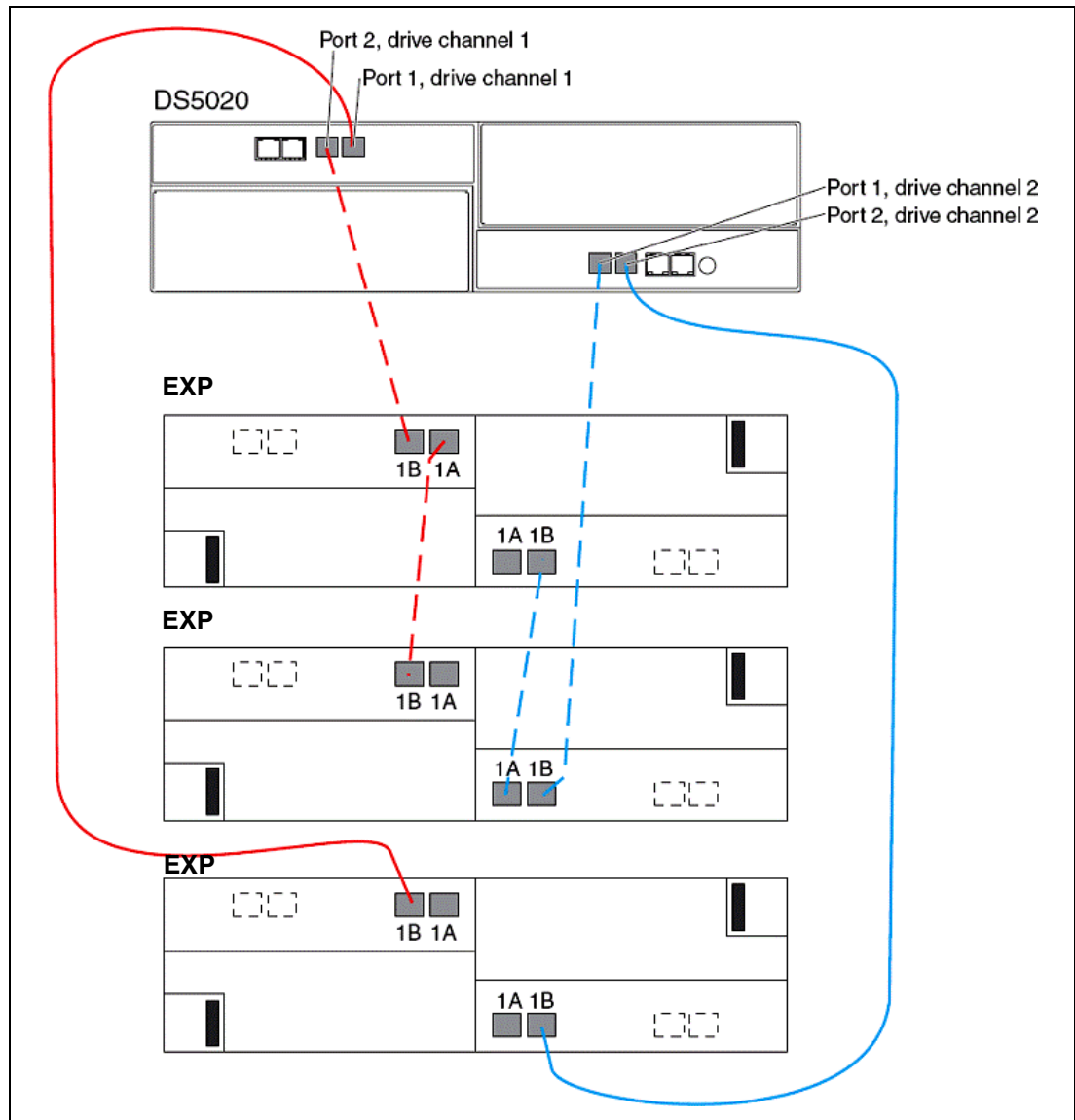


Figure 2-89 DS5020 drive cabling with three EXPs

When six enclosures are required, the same method is employed again, maintaining drive channel redundancy and using both controllers, as shown in Figure 2-90.

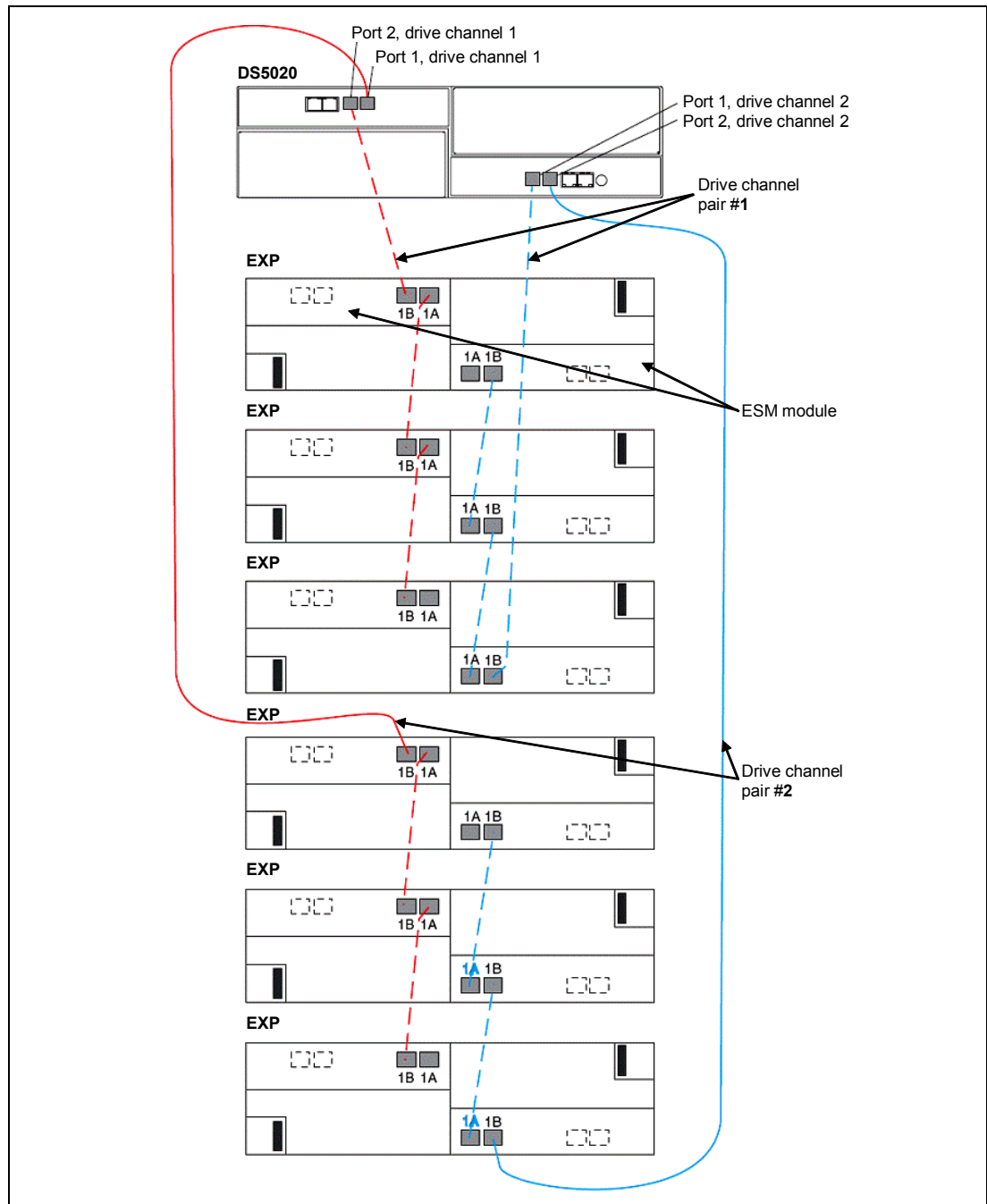


Figure 2-90 DS5020 drive-side cabling with six EXPs

Drive-side cabling example

As shown in Figure 2-90, the DS5020 is cabled using all two-drive channel pairs, assuming that there are six expansion enclosures (EXP) evenly spread out across the drive channel pairs (three enclosures each).

Each enclosure service module (ESM) only has one pair of ports, labelled 1A and 1B, that can be used to connect FC cables. The other pair of ports is reserved for future use. Proceed as follows:

1. Start with the first expansion enclosure, which we attach to drive channel pair #1. Cable controller A, drive port 2 to the port (1B) on the left ESM of the first EXP.
2. Cable the port (1A) of the left ESM on the first EXP to the port (1B) on the left ESM of the second EXP.
3. Cable the port (1A) on the left ESM of the second EXP to the port (1B) on the left ESM of the third EXP.
4. Cable the port (1B) on the right ESM of the first EXP to the port (1A) on the right ESM of the second EXP.
5. Cable the port (1B) on the right ESM of the second EXP to the port (1A) on the right ESM of the third EXP.
6. Cable controller B, drive port 1 to the port (1B) on the right ESM of the third EXP located on the first drive channel pair. This is the last step of the first drive channel pair.

Repeat steps 1–6 (using the next drive-side channel pair ports) for the second drive channel pairs (three EXPs each).



DS5000 storage subsystem configuration

Configuring a DS5000 storage subsystem can be simple, or in cases very complex, especially when encompassing different operating systems, applications, storage partitioning, and other premium features to meet the overall goal of the solution. This chapter will provide you with step by step procedures to lead you to the specific design that you need to implement for your solution's environment.

3.1 IBM System Storage DS Storage Manager software

The IBM System Storage DS Storage Manager software (also referred to as Storage Manager or SM) is used to configure all aspects of the DS storage subsystem. This includes creating the arrays and logical drives, as well as assigning logical drives into storage partitions for their use. You can also vary the settings for the DS storage subsystem wide parameters through the SM. Other features performed through the SM are convert from one RAID level to another, expand the size of arrays and logical drives. Storage Manager also allows the user to perform troubleshooting and management tasks, such as checking the status of the storage subsystem components, replace and rebuild failed disk drives, updating the firmware of controllers, and similar tasks.

Advanced functions, such as FlashCopy, VolumeCopy, and Enhanced Remote Mirroring, are also configured using IBM DS Storage Manager.

The IBM System Storage DS Storage Manager software is packaged as two separate groups of software, *host based* and *controller based* as shown in Figure 3-1.

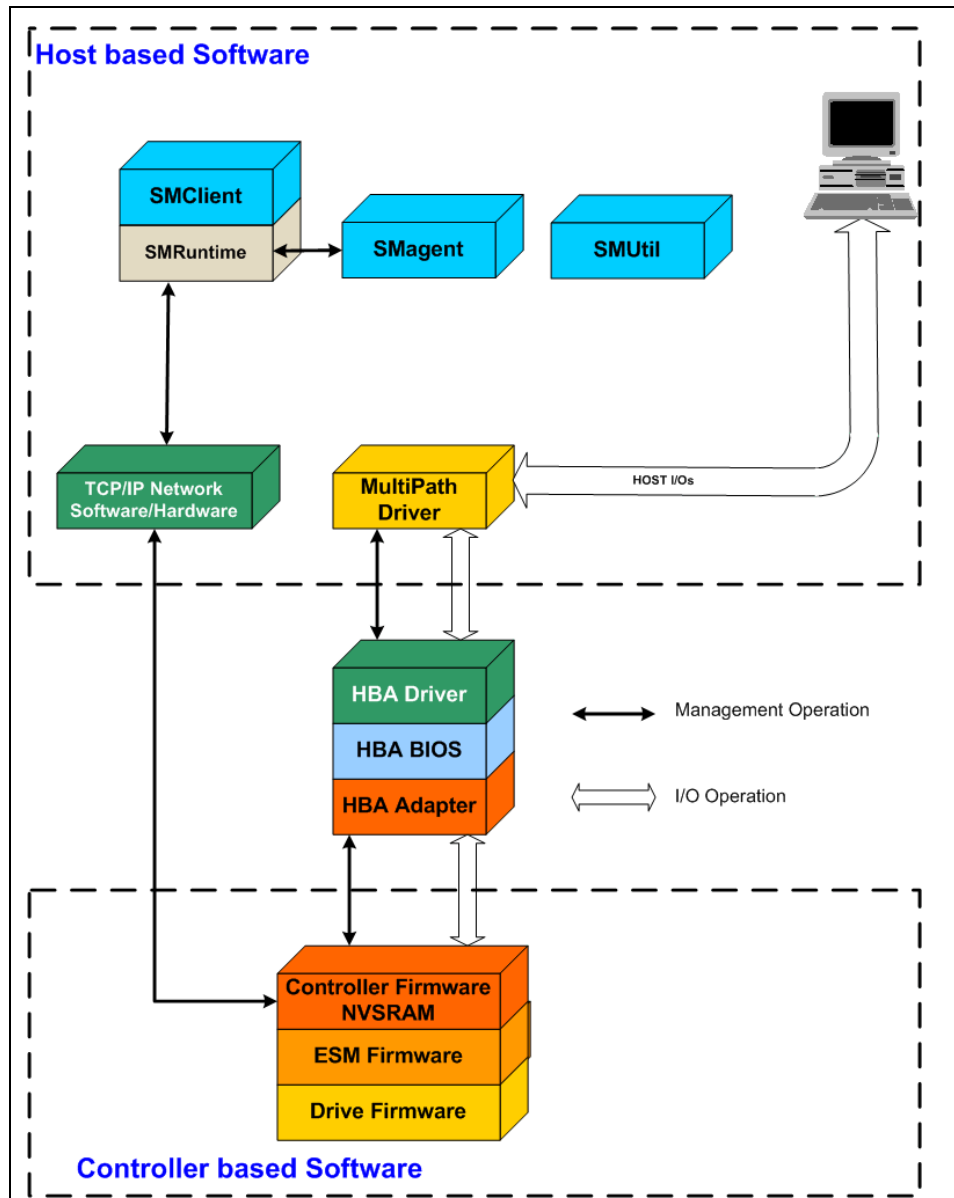


Figure 3-1 Storage Manager software components

The *host-based software* consists of all the software components that will be installed on a host system for using the storage subsystem, and performing management station task to configure and control the storage. The *controller-based software* includes everything required for the components of the storage subsystem enable them to perform their functions and to be managed through a remote LAN/SAN attached host server or PC.

Note: Not all software components are available for all platforms.

Host-based software

The host-based software includes the following software components:

- Storage Manager Client (SMclient):

The SMclient component provides a graphical user interface (GUI) for managing storage subsystems through the Ethernet network or from the host server. It has two main components:

- Enterprise Management: The client can manage multiple storage subsystems in a storage domain, enabling the user to add, remove, and monitor each storage subsystem.
- Subsystem Management: The client can manage and monitor individual storage subsystems.

The SMclient provides an interface for storage management, based on information supplied by the storage subsystem controllers. When the SMclient is installed on a management station, commands are sent to the storage subsystem controllers. The controller firmware contains the necessary logic to carry out the storage management requests. The controller is responsible for validating and executing the commands and providing the status and configuration information that is sent back to the SMclient.

The SMclient is bundled with an Event Monitor that can run in the background and send alert notifications when critical events occur. The Event Monitor service handles notification functions (e-mail and SNMP traps) and can monitor storage subsystems whenever the Enterprise Management window is not open.

The command-line interface (SMcli) is also packaged with the SMclient and provides command-line access to perform all management functions.

See 3.1.2, “Storage Manager client” on page 124 for additional details.

► Storage Manager Runtime (SMruntime):

The SMruntime is a Java runtime environment that is required for the SMclient to function. It is not available on every platform as a separate package, but in those cases, it has been bundled into the SMclient package.

► Storage Manager Agent (SMagent):

The SMagent package is an optional component that allows in-band management of the DS5000 storage subsystem. This agent allows management of the storage subsystem using the same path as the I/O requests coming from the system. The host agent software receives requests from a management station that is connected to a host server through a network connection and passes the requests to the storage subsystem controllers through the Fibre Channel I/O path.

The host agent, along with the network connection on the host server, provides an in-band host agent type network management connection to the storage subsystem instead of the out-of-band direct network management connection through the individual Ethernet connections on each controller. The management station can communicate with a storage subsystem through any host server that has host agent management software installed. The host agent receives requests from the management station through the network connection to the host server and sends them to the controllers in the storage subsystem through the Fibre Channel or iSCSI paths.

► Storage Manager Utilities (SMutil):

SMutil can be used to register and map new logical drives to the operating system and to verify mapping. It can be installed on all UNIX-based host operating systems, including AIX, HP-UX, Solaris, and Linux host servers that are attached to a storage subsystem through Fibre Channel.

The Storage Manager Utilities package contains a number of command-line tools. See 3.1.4, “Storage Manager utilities” on page 128 for more details.

Controller-based software

The controller-based software consists of:

- ▶ DS5000 storage subsystem controller firmware and NVSRAM

The controller firmware and NVSRAM are always installed as a pair and provide the “brains” of the DS5000 storage subsystem. All commands from the SMclient and SMcli come through this code to cause actions to be performed on the storage devices. The controller firmware can be thought of as the operating system and application code for the storage subsystem, and the NVSRAM can be thought of as the configuration of the application.

- ▶ Environmental Service Module (SMesm software)

The ESM canister is a component in a storage expansion enclosure that monitors the environmental condition of the components in that enclosure. The ESM software is required for automatic ESM firmware synchronization. The ESM firmware controls the interface between the controller and the drives.

- ▶ DS5000 storage subsystem drive firmware

The drive firmware is the software that tells the Fibre Channel (FC) drives how to behave Both internally and on the FC loop.

3.1.1 Storage subsystem management methods

The storage management software provides two methods for managing storage subsystems:

- ▶ Host agent (in-band) management method
- ▶ Direct (out-of-band) management method

Depending on specific storage subsystem configurations and host systems, either or both methods can be employed. The management method selected will determine which software components need to be installed.

Host agent (in-band) management method

When the host agent (in-band) management method is used, the storage subsystems are managed through the Fibre Channel or iSCSI I/O path from the host server. This requires installation of the Storage Manager agent (SMagent) package. The management information can either be processed on the host server or passed to the management station through the network connection, as shown in Figure 3-2.

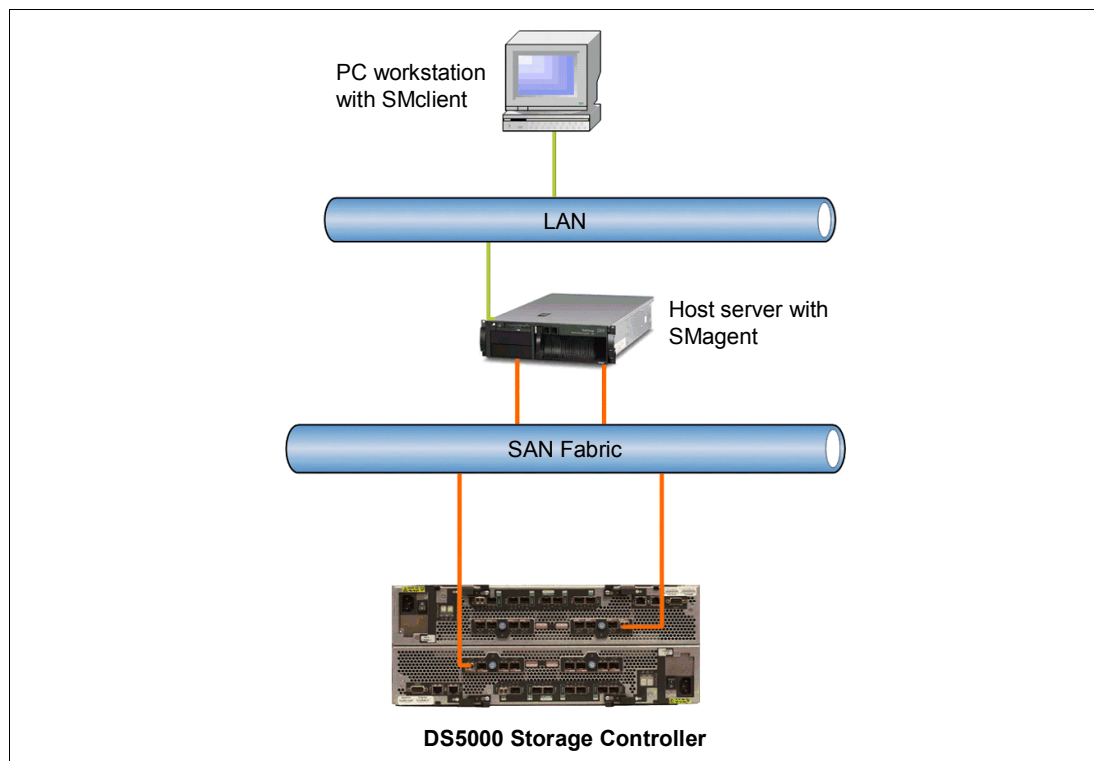


Figure 3-2 In-band management

Managing storage subsystems through the host agent has the following advantages:

- ▶ Ethernet cables do not need to be run to the controllers' management ports.
- ▶ A host name or IP address must only be specified for the host instead of for the individual controllers in a storage subsystem. Storage subsystems that are attached to the host can be automatically discovered.

Managing storage subsystems through the host agent has the following disadvantages:

- ▶ The host agent requires a special logical drive, called the *access logical drive*, to communicate with the controllers in the storage subsystem. Therefore, the host server is limited to one less logical drive than the maximum number that is allowed by the operating system and the host adapter that is being used. Not all operating systems support the *access logical drive*. In-band management is not supported on these systems.
- ▶ If the connection through the Fibre Channel or iSCSI path is lost between the host and the server, the server cannot be managed or monitored.

Important: If a host already has the maximum number of logical drives configured, either use the direct management method or give up a logical drive for use as the access logical drive.

Direct (out-of-band) management method

When the direct (out-of-band) management method is used, storage subsystems are managed directly over the network through a TCP/IP Ethernet connection to each controller. To manage the storage subsystem through the Ethernet connections, the IP address and host name for each controller must be defined or the DS5000 storage subsystem must be set to use DHCP/BOOTP settings. The controllers must be attached to a Local Area Network (LAN) through Ethernet, as shown in Figure 3-3.

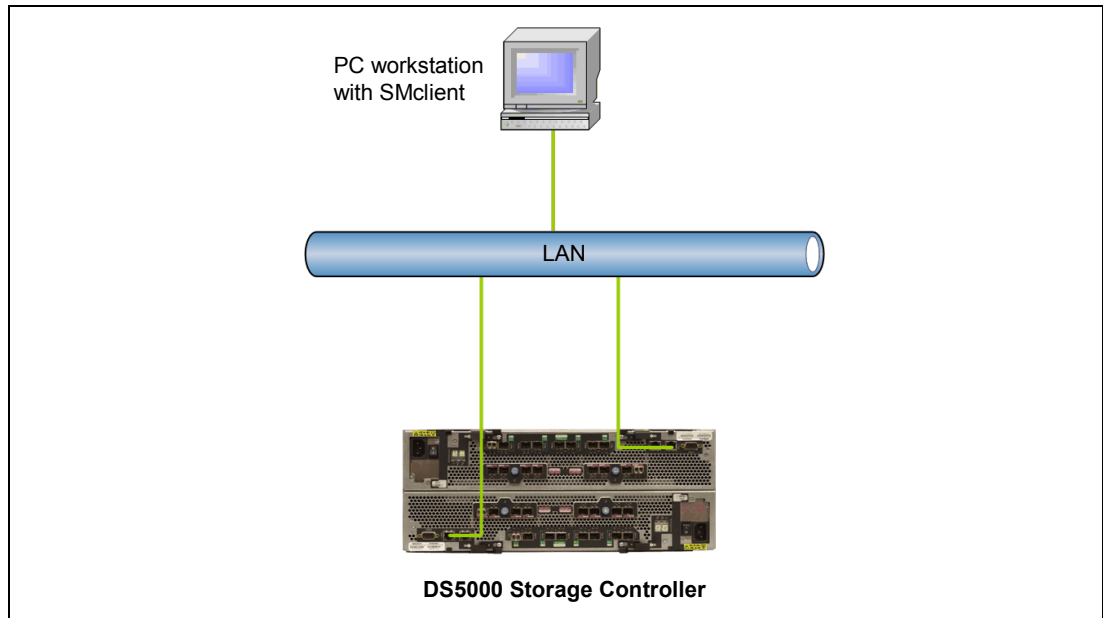


Figure 3-3 Out-of-band management

Managing storage subsystems using the direct (out-of-band) management method has the following advantages:

- ▶ The Ethernet connections to the controllers enable a management station running SMclient to manage storage subsystems that are connected to a host running any of the operating systems that are supported by the current level of Storage Manager.
- ▶ An access logical drive is not needed to communicate with the controllers. The maximum number of logical drives that are supported by the host operating system can be configured and used.
- ▶ The storage subsystem can be managed when there are problems with the Fibre Channel links.
- ▶ Security is enhanced when management LANs/VLANs and more advanced solutions, such as VPN, can be used to manage the system remotely.
- ▶ More DS5000 storage subsystems in the network can be managed through one Storage Manager interface.

Managing storage subsystems using the direct (out-of-band) management method has the following disadvantages:

- ▶ Two Ethernet cables are required to connect the storage subsystem controllers to a network.
- ▶ When adding devices, the IP address or host name for each controller must be provided.
- ▶ DHCP/BOOTP server and network preparation tasks are required. This can be avoided by assigning static IP addresses to the controller, or by using the default IP address.

To assign static IP addresses, see 3.3.3, “Configuring IP addresses of the controllers”.

Tip: To manage storage subsystems through a firewall, configure the firewall to open port 2463 for TCP and UDP data.

3.1.2 Storage Manager client

This section continues our overview of the Storage Manager client, reviewing the different screens and information available.

We know already that the Storage Manager client can be used for either in-band or out-of-band management of the storage subsystem. In-band management uses the Fibre Channel network to communicate with the IBM System Storage DS5000 storage subsystem, and out-of-band management uses the TCP/IP network. On host platforms that support both methods, it is possible to use them on the same machine if you have a TCP/IP connection and also a Fibre Channel connection to the DS5000 storage subsystem.

When you install SMclient and SMagent on a stand-alone host to manage the storage subsystem *inband* through the Fibre Channel I/O path (rather than through the Ethernet network), you should still install the TCP/IP software on the host, and assign an IP address to it. With the TCP/IP configured other workstations on the network with the SMclient installed can be configured to manage the DS5000 storage subsystem by connecting through the SMagent, thereby protecting secure environments from other network traffic.

Next, we review the different host systems where you can install the Storage Manager client and the different windows presented.

Supported host systems

The Storage Manager client is a Java-based GUI utility that is available for various operating systems. For up-to-date information about support for specific DS5000 models and operating systems, check the DS5000 storage subsystem support Web site at the following address:

<http://www.ibm.com/servers/storage/support/disk>

Select downloads and Storage Manager to see current list of packages available.

The Storage Manager client contains two main windows that through which you can monitor and gain control over the storage subsystems:

- ▶ The Enterprise Management window
- ▶ The Subsystem Management window

The Enterprise Management window

The Enterprise Management window is the first window that opens when the storage management software is started. The Enterprise Management window has two different tabs:

- ▶ Devices
- ▶ Setup

Enterprise Management Setup tab

The Setup tab of the Enterprise Management window contains different functions that you can use to perform the initial setup tasks for your storage subsystem, as shown in Figure 3-4.



Figure 3-4 Enterprise Management Setup tab

From here you can add your storage subsystem to the management software, start your configuration, and perform other various tasks, such as providing proper names to each subsystem, configuring alert notification destinations, and updating firmware or selecting a particular storage subsystem (or subsystem) to be managed.

Enterprise Management Devices tab

The Devices view of the Enterprise Management window presents the different storage subsystems that the client can access either directly or through the host agents. If a certain storage subsystem can be accessed in both ways, and possibly through several host agents, it will be listed several times in the Enterprise Management window.

The name, status, and management type (through Ethernet or through host agent) are shown for each listed storage subsystem, as shown in Figure 3-5. In our illustration, we assume out-of-band management from a machine that only has a TCP/IP connection to the DS5000 storage subsystem.

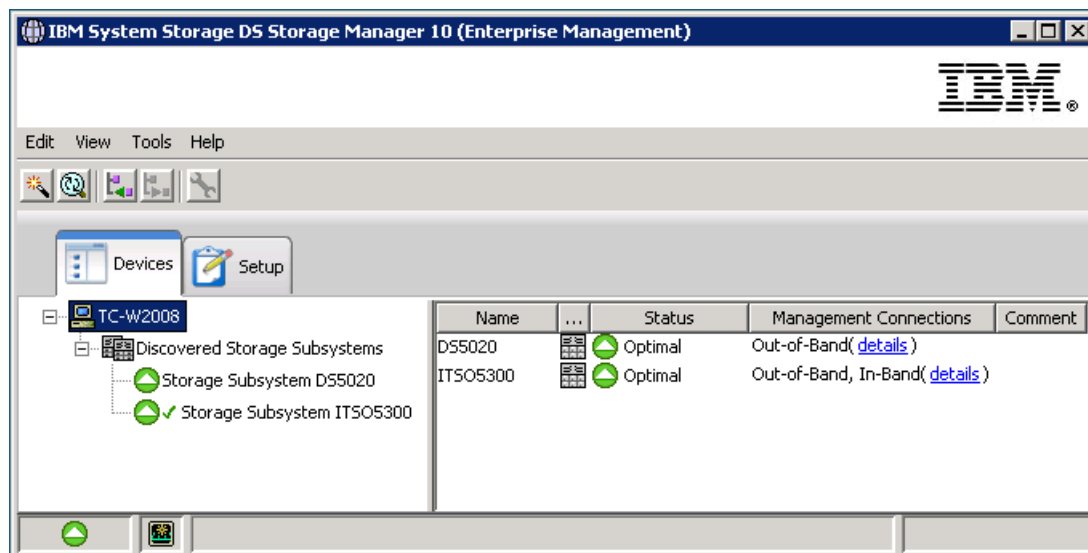


Figure 3-5 Enterprise Management Device view

Note: Although a single storage subsystem can be listed several times in the left pane when it is accessed by various host agents or directly attached, it only appears once in the right pane.

The Subsystem Management window

Once a system to be managed is selected in the Enterprise Management window, clicking it opens the Subsystem Management window for that particular system. In Figure 3-6, there is a sample window showing the summary view of the Subsystem Management window. Note the multiple tabs that are available, each presenting a different view of the subsystem. This multiple tabs view is available with firmware version 10.50 and later. If you are managing a storage subsystem with an earlier firmware version, you will see only two tabs in this view.

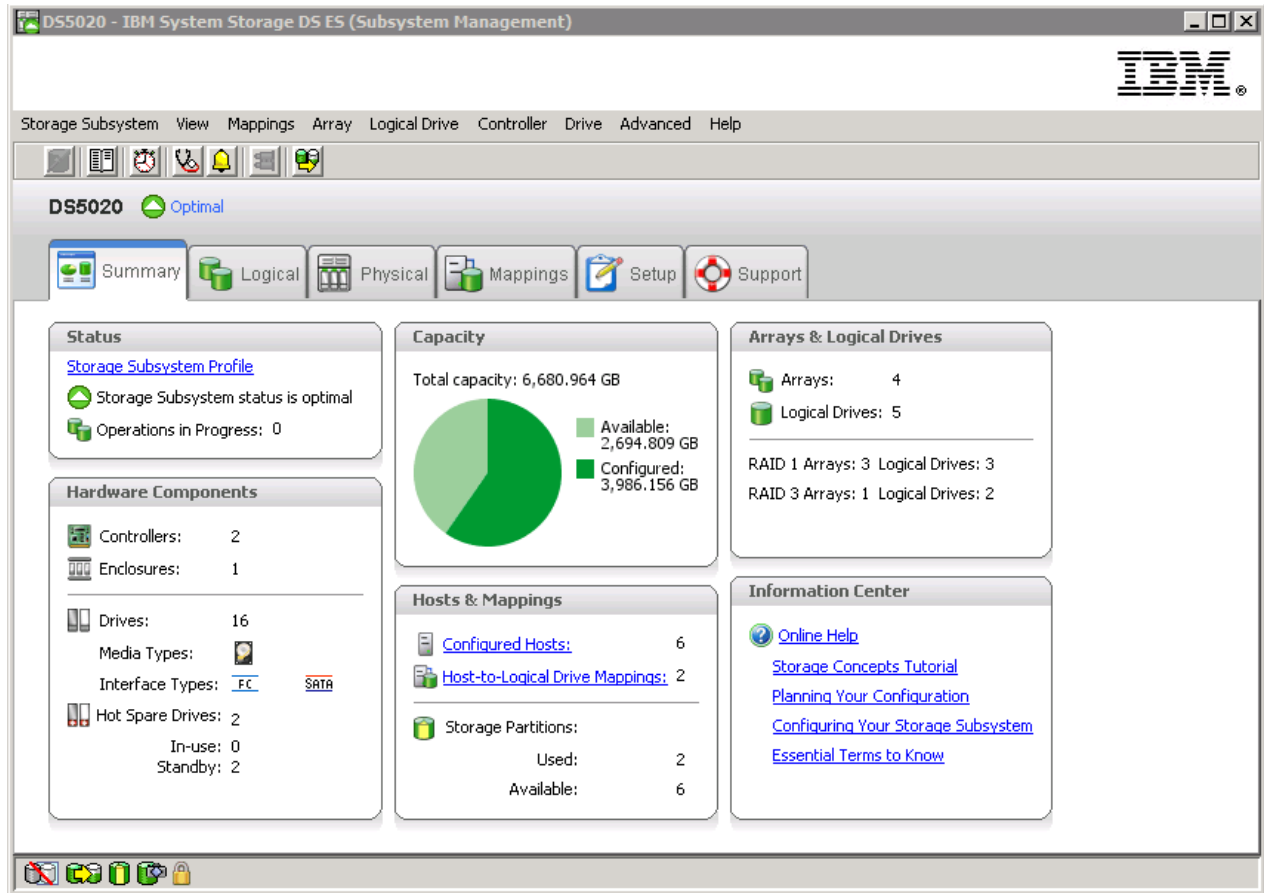


Figure 3-6 Subsystem Management Summary view

We cover the different options available in the Subsystem Management windows later in 3.2.1, “Installing DS Storage Manager software on Windows 2008”.

3.1.3 Event Monitor service

The Event Monitor service handles notification functions (e-mail and SNMP traps) and monitors storage subsystems whenever the Enterprise Management window is not open.

The Event Monitor is a separate program bundled with the Storage Manager client software (the Event Monitor cannot be installed without the client.) The Event Monitor can only be installed on a management station or host server connected to the storage subsystems. For continuous monitoring, the Event Monitor must be installed on a host server that runs 24 hours a day. Once installed, the Event Monitor runs in the background and checks for possible critical problems. If it detects a problem, it notifies a remote system through e-mail, Simple Network Management Protocol (SNMP), or both.

In order to use SNMP notification, you need an SNMP machine listening for the notifications sent by the Event Monitor.

For additional information about how to set up the Event Monitor, see 3.5.7, “Monitoring and alerting” on page 202.

3.1.4 Storage Manager utilities

Storage Manager comes with command-line utilities that are installed separately from the other components. These vary by operating system type, but generally include the following utilities:

- ▶ **hot_add:** This utility is used to scan for new disks available to the operating system after they are defined and mapped in Storage Manager. This is especially useful for operating systems that normally have to be re-booted.
- ▶ **SMdevices:** This utility lists all logical drives available to the host, including target ID and logical drive name (as defined in the Storage Manager). This is useful if there are several logical drives of the same size defined for a given host, because it is able to identify which logical drive is which before mounting and formatting them under the operating system.
- ▶ **SMrepassist:** This utility is a host-based utility for Windows platforms that performs certain functions needed to make the subsystem hardware FlashCopy work smoothly. It is run against a specific drive or mount point and causes the buffers to be flushed to disk.
- ▶ **mppUtil:** This utility is used in conjunction with the Linux driver to configure and troubleshoot the driver. This utility can display information about the RDAC driver itself, assist in debugging errors, and can manually initiate one of the RDAC driver's scan tasks. This utility is installed with the RDAC driver itself.

For information about how to install Storage Manager utilities, see 3.2, "Installing IBM System Storage DS Storage Manager".

3.2 Installing IBM System Storage DS Storage Manager

The IBM System Storage DS Storage Manager consists of a set of client and host server software packages that enable you to manage and connect to the DS5000 storage subsystem.

The IBM System Storage DS5000 storage subsystem comes with a CD that provides the following packages for the various supported operating systems:

- ▶ **Client Software package**
 - **SMruntime software:** Provides the Java runtime environment required to run the SMclient.
 - **SMclient software:** Java-based graphical user interface.
 - **SMesm software:** Provides functions for the Environmental Service Module, ESM, and firmware delivery package.
- ▶ **Host Software package**
 - **SMagent software:** Provides management capabilities through the host I/O path.
 - **SMutil software:** An utility to register and map new logical drives to the operating system.

Note: Before installing your DS5000 storage subsystem hardware and software, be sure to meet all the requirements for your DS5000 model: HBAs, firmware version, SAN, and OS level, as specified at the IBM Support Web site.

Go to the Web page for the System Storage Interoperation Center to get the latest DS5000 storage subsystem compatibility information at the following address:

<http://www.ibm.com/systems/support/storage/config/ssic/index.jsp>

3.2.1 Installing DS Storage Manager software on Windows 2008

This section covers a guided installation of the DS Storage Manager v10.77 software in a Windows Server 2008 R2 host environment. Refer to host configuration section in *IBM System Storage DS5000 Series Implementation and Best Practices Guide*, SG24-8024 for installation procedures in Linux and AIX.

Note: You can also use this information as a base reference for installing in environments using Windows Server 2003 and DS4000.

The host software for Windows includes the following components:

- ▶ SMclient
- ▶ Multipath driver (MPIO Device Specific Module - DSM)
- ▶ SMagent
- ▶ SMutil

Note: On DS Storage Manager v10.77, MPIO Device Specific Module has a separate installation package but is still provided on the IBM DS Storage manager installation source

Follow these steps to install the software:

1. Log on with administrator rights for installing the new software, including new drivers.
2. Locate and run the installation executable file, either in the appropriate CD-ROM directory, or the file that you have downloaded from the IBM support Web site. After it has been executed, select your language of choice. After presenting the introduction and copyright statement windows, you are asked to accept the terms of the license agreement, which is required to proceed with the installation.
3. Select the installation target directory of your choice. The default installation path is:
 32Bit OS -> C:\Program Files\IBM_DS\
 64Bit OS -> C:\Program Files (x86)\IBM_DS\
4. Select the installation type, as shown in Figure 3-7.



Figure 3-7 InstallAnywhere: Select Installation Type

- a. Select the installation type to define the components that will be installed. In most cases, you can select either the Management Station or Host installation type. For example, if you select Management Station, then the multipath driver and Agent components will not be installed, because they are not required on the management computer.
- b. Decide what type of installation you want. Two additional choices are offered: Typical (Full Installation) and Custom. As the name indicates, Typical (Full Installation) installs all components and Custom installation lets you choose the components, as you can see in Figure 3-8.

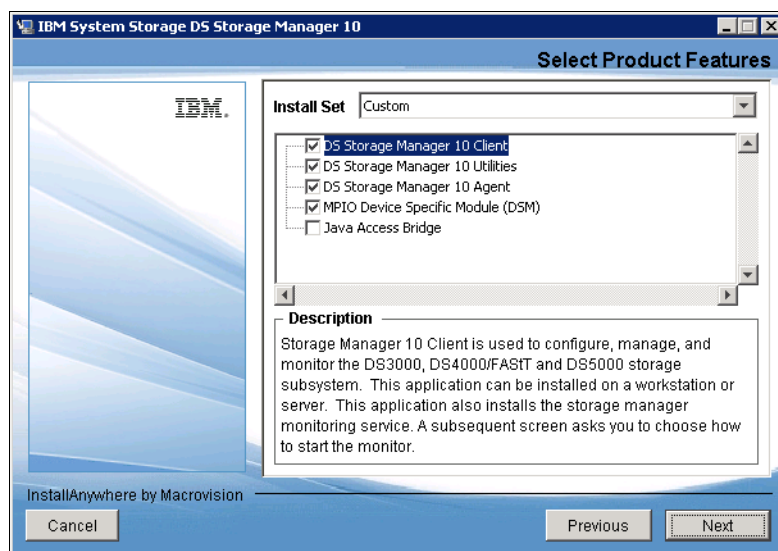


Figure 3-8 InstallAnywhere: Select Storage Manager components

Note: Remember that the SM Failover drivers (MPIO/DSM) are only supported for connection to DS5000 Storage Servers with controller firmware V6.19 and later.

In addition to the usual Storage Manager components, you can choose to install Java Access Bridge. This selection enables support for the window reader (such as JAWS from Freedom Scientific, Inc.) for blind or visually impaired users.

5. Decide whether you want to automatically start the Storage Manager Event Monitor, as shown in Figure 3-9, which depends on your particular management setup. In case there are several management machines, the Event Monitor must only run on one. If you want to use the Event Monitor with SNMP, you have to install the Microsoft SNMP service first, because the Event Monitor uses its functionality.

Note: The Event Monitor must be enabled for both the automatic ESM synchronization and the automatic support bundle collection on critical events.

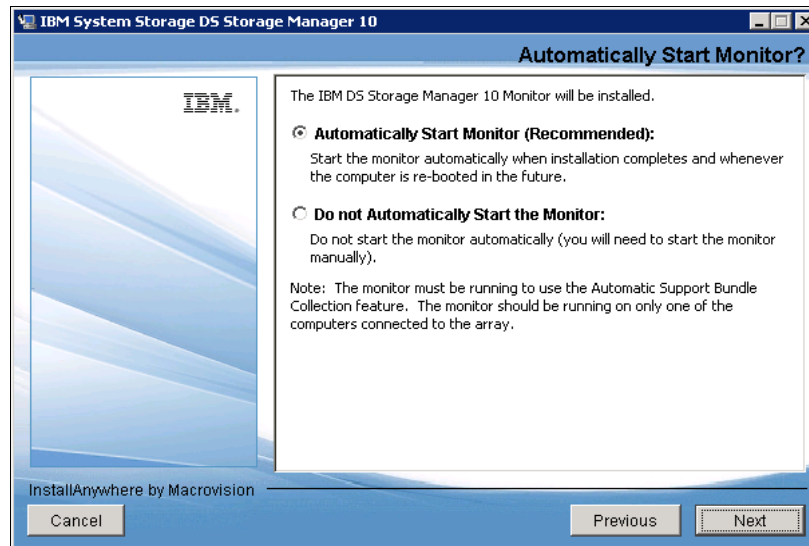


Figure 3-9 InstallAnywhere: Automatically Start Monitor

6. Verify that you have selected the correct installation options by examining the Pre-Installation Summary window, which is presented next. Then click the **Install** button. The actual installation process starts as shown in Figure 3-10.



Figure 3-10 installAnywhere: Pre-Installation Summary window

Verifying the SM installation

This section provides instructions on how to verify that you have installed the SM correctly in your Windows Server 2008.

Look under your programs folder for a new program entry in your named IBM DS Storage Manager 10 Client. This name is the name of the program created after a successful installation, which also generates a log file with the details of the installation process and options selected, and places it into the installation directory. The file name is:

IBM_System_Storage_DS_Storage_Manager_10_InstallLog.log

In case of problems during the installation, have a look at this file for a possible hint about what might be wrong.

Verifying the SMagent installation

This section provides instructions on how to verify that you have installed the SMagent correctly on Windows operating systems. Follow these steps:

1. Select **Start** → **Administrative Tools** → **Services**. The Services window opens.
2. Scroll through the list of services until you find IBM DS Storage Manager 10 Agent as shown in Figure 3-11.

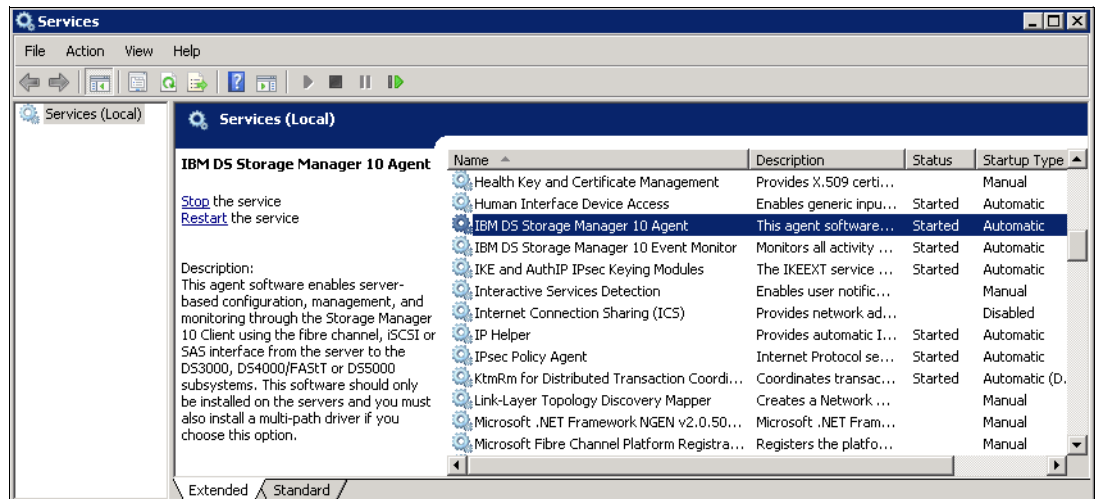


Figure 3-11 Verifying the SMagent installation

3. Determine whether the IBM DS Storage Manager 10 Agent and the Event Monitor services have been started. These services were created by the installation, which normally starts both of them by default. However, if a service has not been started, right-click it and select **Start**. Make sure the Startup Type is set to **Automatic**.

If you are installing the host server and do not plan to use the host-agent software to manage one or more storage systems, you can set the Startup Type to **Manual**.

Verifying the SMutil installation

To verify that you have installed the SMutil correctly on Windows operating systems, follow these steps:

1. Go to the `installation_directory\Util` directory, typically:

```
32Bit OS -> C:\Program Files\IBM_DS\Util
64Bit OS -> C:\Program Files (x86)\IBM_DS\Util
```

2. Verify that the directory contains the following files:

- hot_add.exe
- SMdevices.bat
- SMrepassist.exe

Note: On 64-Bits OS the installation path should be `C:\Program Files <x86>\IBM_DS\Util`

3.2.2 HBA and Multipath device drivers

For a successful implementation, and also to keep your system running at a supported level, be sure to check your host bus adapter firmware and driver levels, as well as the DS Storage System driver level, and compare them against the System Storage Interoperation Center, SCIC. For details, see the IBM System Storage Interoperation Center (SSIC) Web site:

<http://www-03.ibm.com/systems/support/storage/config/ssic>

You can download the necessary files for the DS Storage Systems, including the host bus adapter drivers, from the IBM System Storage support Web site:

<http://www.ibm.com/servers/storage/support/disk>

Verifying your Host Attachment card

Host adapter cards are tested at specified levels for interoperability with the DS Storage Systems, so very often the SSIC Web site output shows specific firmware levels as supported. It might also show specific preferred HBA settings.

To display or update your adapter firmware levels, and specific settings, so that they match the supported SSIC Web site output, you can use the management tool corresponding to your HBA manufacturer. In Figure 3-12, the QLogic SANsurfer Manager is used as an example for showing a QLogic iSCSI adapter additional information, such as firmware, BIOS, and driver versions.

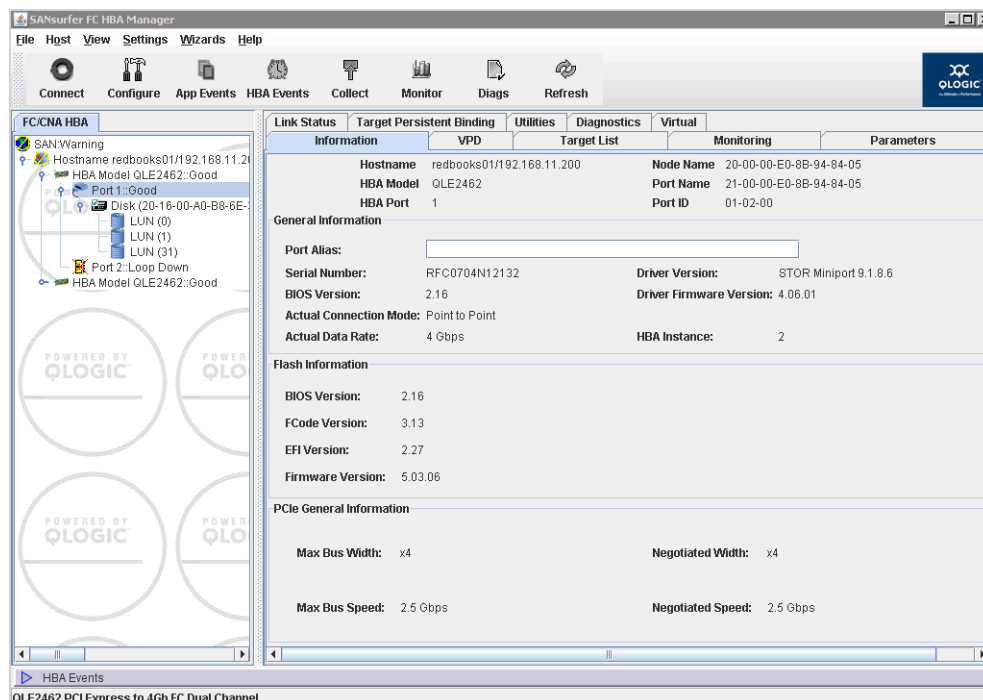


Figure 3-12 Using QLogic SANsurfer to display HBA firmware

Notice that the HBA model is specified. You need that specific model to search the supported levels of firmware and drivers to use it to attach your DS Storage System.

Emulex has another graphic utility for the same purpose, named HBAAnyware, and Brocade too. For more information about the usage of these tools, including how to update the firmware or BIOS levels, refer to 5.1.8, “Updating host bus adapter (HBA) firmware” on page 311.

Verifying your Host Attachment cards driver level

To check or update your host bus adapter driver level in Windows, use the Device Manager to display the status of your host bus adapter cards for both Fibre Channel or iSCSI depending on your system configuration as shown in Figure 3-13.

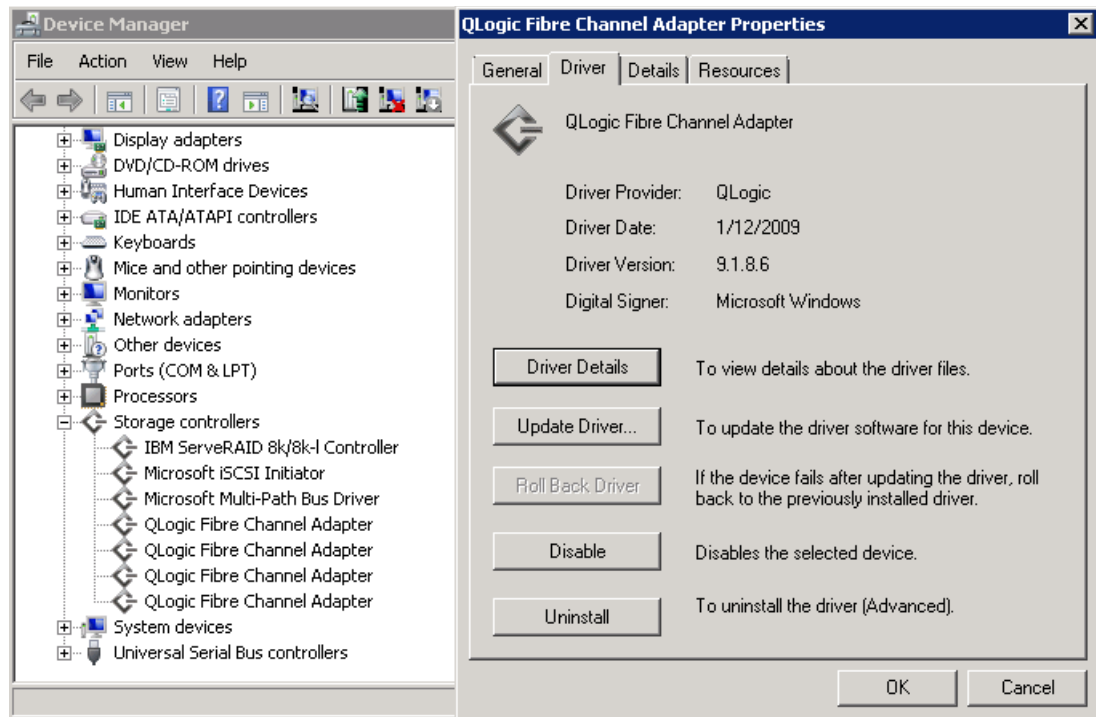


Figure 3-13 Displaying HBA drivers

From here you can display the installed driver level of your adapter card, and even update it by selecting the option **Update Driver**. This procedure is easy, however, it is important to make sure which kind of adapter you have, and its specific model, because both driver and firmware might be specific for the adapter types. The Windows Device Manager does not provide this information, so it is a better alternative to use your adapter specific management tool to determine the exact adapter type, as seen in Figure 3-12.

SM Failover driver (MPIO/DSM)

The following drivers are supported for the DS storage Systems in Windows:

- ▶ **Microsoft MPIO:**
Included with Windows operating systems.
- ▶ **MPIO Device Specific Module (DSM):**
Provided with the DS Storage Manager installation package.

Installing MPIO Device Specific Module (DSM)

On DS Storage Manager v10.77, MPIO Device Specific Module has a separate installation package and it's provided on the IBM DS Storage manager installation source under the windows folder (eg:

"\ibm_sw_ds3-5k_10.77.xx.16_windows_intl386\WS03WS08_10p77_IA32\Windows\").

On prior versions, MPIO DSM support was provided on the same DS Storage Manager installation package and available on "Custom" installation.

1. For installing MPIO DSM, Log on with administrator rights for installing MPIO Device Specific Module support. Locate and run the installation executable file, click on **Next** on the Welcome windows and then accept the License Agreement, as shown in Figure 3-14 and Figure 3-15.

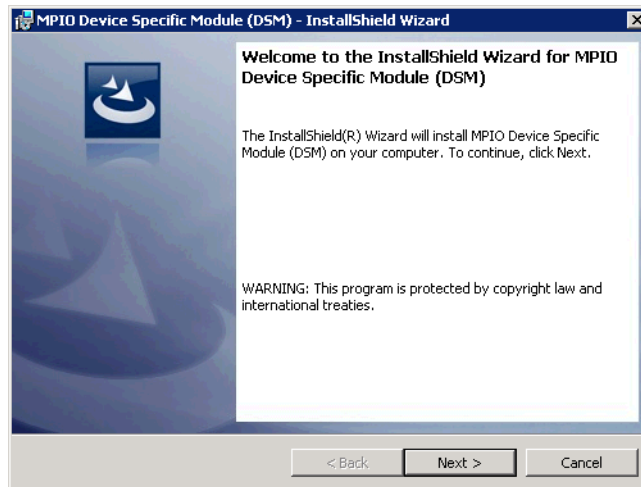


Figure 3-14 MPIO Device Specific Driver - Welcome screen

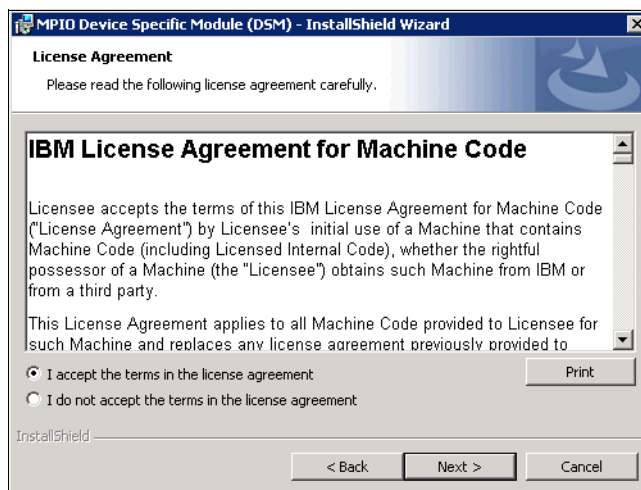


Figure 3-15 MPIO Device Specific Driver - License Agreement

2. Click on **Install** to start with the installation process, as shown in the Figure 3-16.

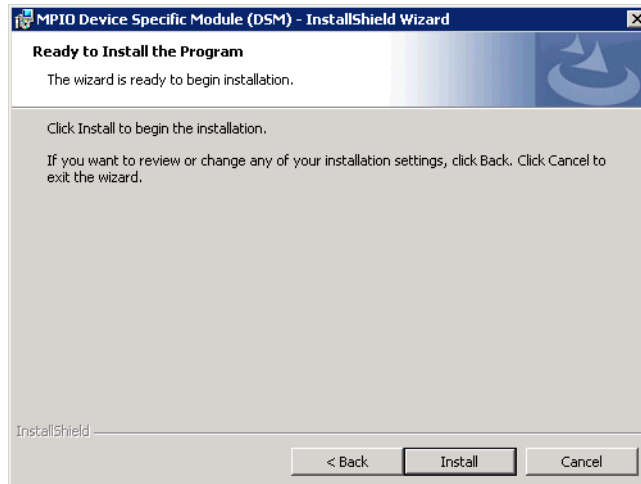


Figure 3-16 MPIO Device Specific Driver - Install begin.

3. During the installation process a new windows will be opened showing the installation process from the console as shown in Figure 3-17.

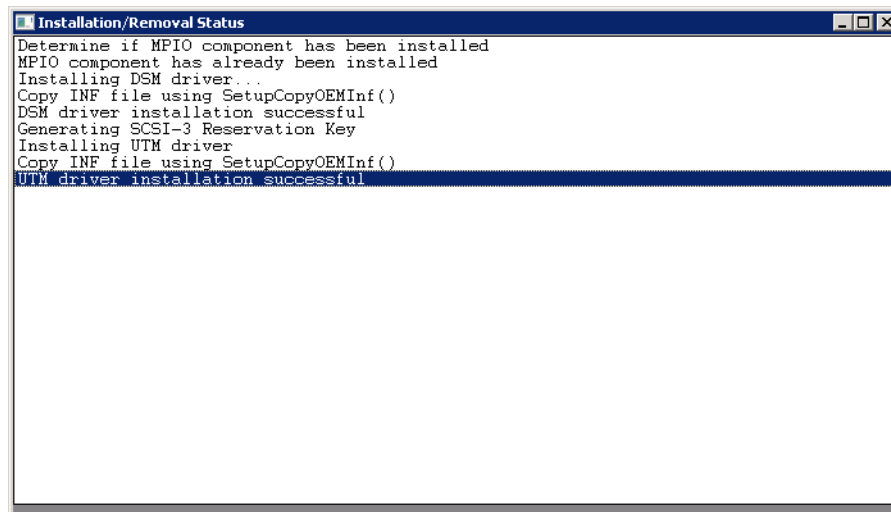


Figure 3-17 - MPIO Device Specific Driver - Installation process status console

4. Finally click on **Finish** to complete the installation process. A reboot is required to apply the new driver changes. See Figure 3-18 for an example of the completion of the wizard.

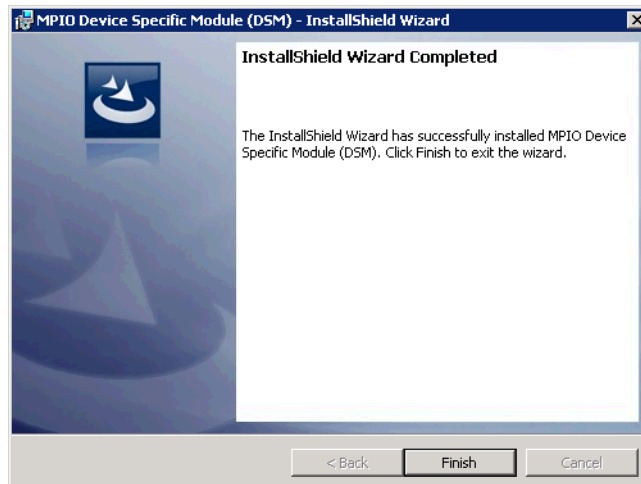


Figure 3-18 MPIO Device Specific Driver - Installation completed

You can verify the installation of the MPIO DSM software by viewing the driver with the Manager as shown in Figure 3-19.

5. Open the Device Manager in Computer Management. There should be a Multi-Path Support entry under the SCSI and RAID Controller folder, as shown in Figure 3-19.

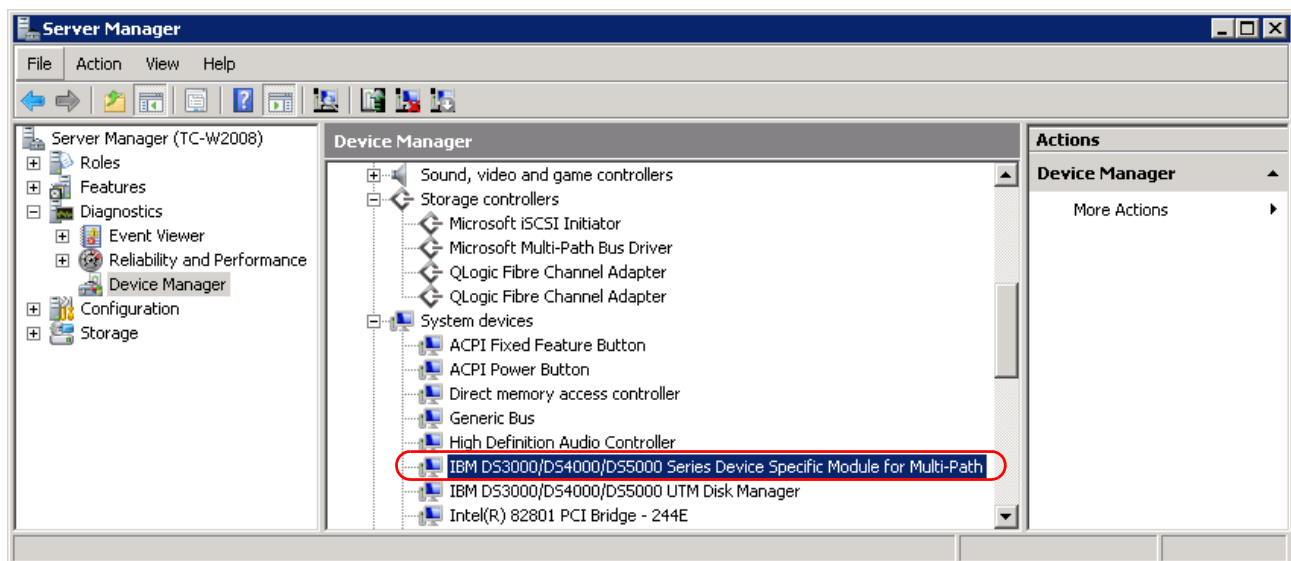


Figure 3-19 SM Failover (MPIO/DSM) Multi-Path Support

3.3 Preparing the DS5000 storage subsystem

This section explains how to configure the DS5000 storage subsystem. This includes:

- ▶ Physical installation
- ▶ Powering on the storage subsystem
- ▶ Configuring IP addresses on the DS5000 storage subsystem
- ▶ Initializing the Storage Manager client
- ▶ Updating the controller microcode
- ▶ Updating the drive and ESM microcode

3.3.1 Physical installation

You should have already completed the physical installation of your DS5000 storage subsystem hardware. See the installation, user's, and maintenance guides for your specific IBM System Storage DS5000 for specific instructions. You can also refer to *IBM System Storage DS5000 Series Implementation and Best Practices Guide*, SG24-8024 for more information about the hardware installation procedures.

Take note of the order in which you install the expansion enclosures. Once the Storage Manager software is installed, it is important that the representation in the software interface matches the current disposition of the expansions in the rack.

Follow the recommendations on cabling the expansion enclosures to the storage subsystem controllers, to allow an optimization of the drive channel paths, and consider any plans for future expansions.

3.3.2 Powering on the storage subsystem

Before powering on your storage subsystem, make sure you have your hardware installed correctly. The EXP5000 and EXP810 expansion enclosures will automatically assign their ID at first power on.

When turning power on or off, a certain order must be followed on the DS5000 storage subsystem.

The drives attached to the storage subsystem must be available when the storage subsystem is powered up. In other words, when expansion enclosures are attached to a storage subsystem, the expansions must be powered up first.

Important: Always power up the expansion enclosures first. The controllers in the storage subsystem might not recognize the correct configuration if the drives are powered up after the storage subsystem.

Note: In the case of a power failure in a lights out operation there is a built-in delay to allow for the drives to come up first when the entire storage subsystem is powered on at one instance of time.

The Fibre Channel and Ethernet hubs and switches, if installed, must be powered on before the host to ensure proper initialization. When connecting your DS5000 storage subsystem ports to a SAN switch, or directly to a host, match whenever possible the maximum speed of the ports, that is, avoid connecting an 8 Gb SFP to a 2 Gb switch or host bus adapter, for example.

The normal power up procedure includes the following steps:

1. Turn on the SAN or Ethernet switches (if attached).
2. Turn on the expansion enclosures.
3. After the last enclosure is powered on, wait for all the disks to be ready (steady green LED for each disk).
4. Turn on the DS5000 storage subsystem.
5. Turn on the host application server.

The power-down procedure includes the following steps:

1. Turn off the host application server.
2. Turn off the DS5000 storage subsystem.
3. Turn off the expansion enclosures.
4. Turn off hubs/switches (if attached).

Important: It is generally a best practice to ensure that your system is in an optimal state before you shut it down. Never turn the power off if any fault light is lit. Be sure to resolve any error conditions before you shut down the system. Powering down will clear important data that may have been needed to resolve the fault that was encountered.

3.3.3 Configuring IP addresses of the controllers

The DS5000 storage subsystem has two Ethernet ports per controller. Use one Ethernet port for daily management of your DS5000 storage subsystem. The second port is reserved for use by service personnel or for subsystem monitoring hardware that might be available in the future.

By default, the DS5000 storage subsystem will try the BOOTP/DHCP service to request an IP address. If no BOOTP/DHCP service is found in the network, the controllers revert to fixed IP addresses.

By default, the fixed addresses for first ports are:

- ▶ Controller A: 192.168.128.101
- ▶ Controller B: 192.168.128.102

The default IP addresses of the additional Ethernet ports are:

- ▶ Controller A: 192.168.129.101
- ▶ Controller B: 192.168.129.102

See the specific Ethernet port locations with their default IP addresses in Figure 3-20.

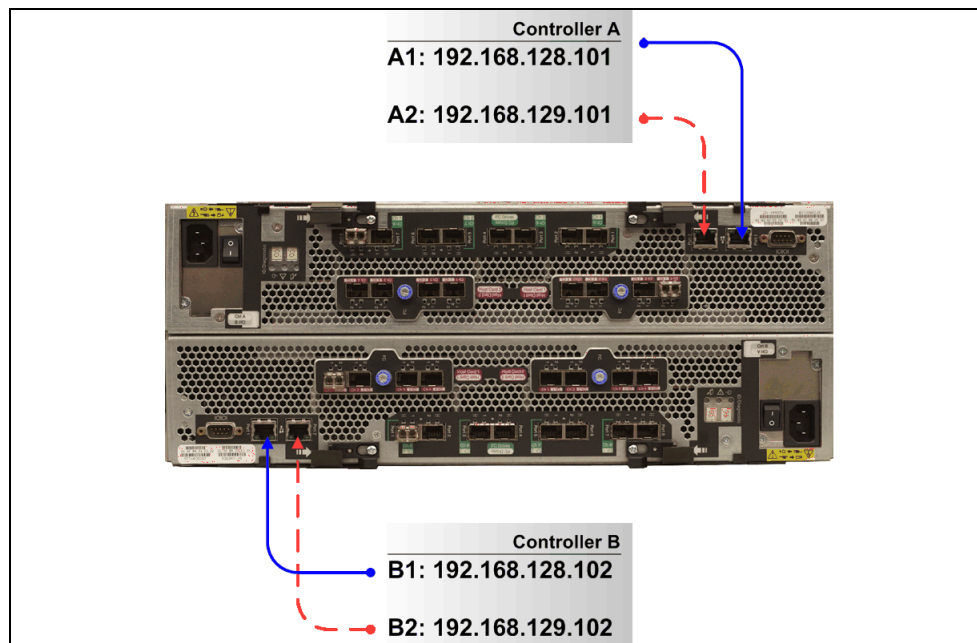


Figure 3-20 DS5000 storage subsystem default IP addresses

Given the importance of the storage subsystems in any environment, we recommend that an IP address be assigned to them rather than relying on a BOOTP/DHCP dynamic address. There are two ways to change the IP addresses of the controllers by changing them with the Storage Manager utility:

- ▶ Using out-of-band management (recommended)
- ▶ Using in-band management

Because of the host, HBA, and driver specifics required to step up and configure the host with their specific HBA's and drivers to use the in-band method, we will describe the out-of-band method in this section using the ethernet management capability. For details on setting up the IP address through the in-band method see the *IBM System Storage DS Storage Manager Version 10 Installation and Host Support Guide*, available at:

<http://www.ibm.com/support/entry/portal/docdisplay?ln docid=MIGR-5075652&brandind=5000028>

Changing the IP addresses with the Storage Manager utility

In order to change the default IP addresses, first we must connect to the DS5000 storage subsystem.

Perform the following steps:

1. Connect the Ethernet ports to an isolated Ethernet switch.
2. Set the IP address in your management machine to match the network address of the default IPs on the DS5000 storage subsystem.
3. Connect the management machine to the same Ethernet switch.
4. Use the Storage Manager client GUI interface to change the IP addresses on both controllers:

- a. Start the Storage Manager client interface.

If this is the first time you are using the Storage Manager software, after it is launched, the program presents a window to start automatic discovery of the attached devices.

- b. Select **OK** to initiate an automatic discovery.

If the DS5000 storage subsystem does not appear after this action, check the network connectivity to both default IP addresses of the storage subsystem using the **ping** command. Consider that each time a network cable is plugged into an Ethernet port of a controller, it detects the linkup and initiates a request for a dynamic address. If one is not found, it assigns the default IP address. If you try to connect to the storage during that time, you receive an error, so we recommend waiting at least 5 minutes after plugging in the cable to attempt either the automatic discovery or to manually add the controller IP addresses.

Tip: Before starting the automatic discovery or adding the DS5000 storage subsystem manually, wait for the controller to finish its boot process and then another 5 minutes after connecting the network cable to allow for the DHCP process to complete.

Alternatively, you can add your storage manually from the Enterprise Management selecting the **Setup** tab, selecting **Add Storage Subsystem**, and then completing the fields with the default IP addresses, as shown in Figure 3-21.

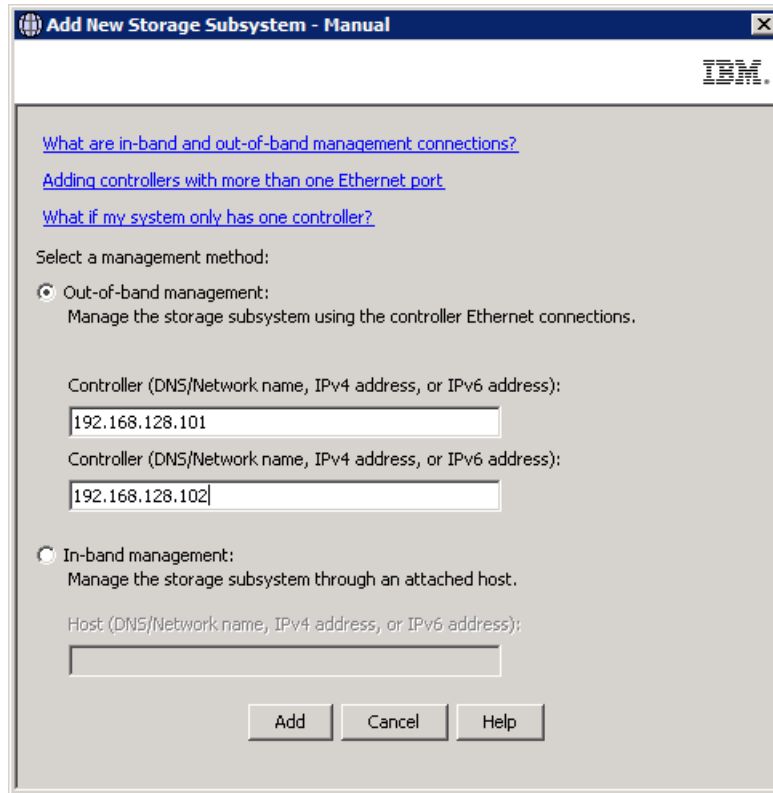


Figure 3-21 Manually adding a storage subsystem

- c. A confirmation message appears and prompts you for additional storage subsystems. Click **No** to finish adding storage subsystems.
- d. After successfully adding a storage subsystem, the Devices tab shows the new system as shown in Figure 3-22. Note that you can check the IP address of the managed system by selecting **Details** under Management Connections.

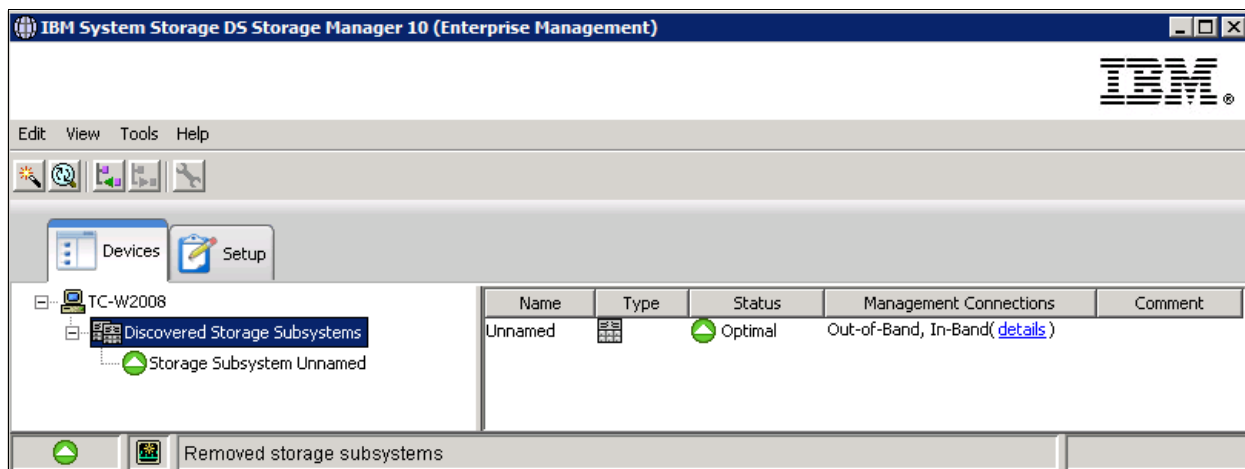


Figure 3-22 Managing a storage subsystem

Select the **Setup** tab to view the Initial Setup window. Right-click the storage subsystem or double-click it to open the Subsystem Management window. You are prompted to set a password for your storage subsystem, as shown in Figure 3-23.

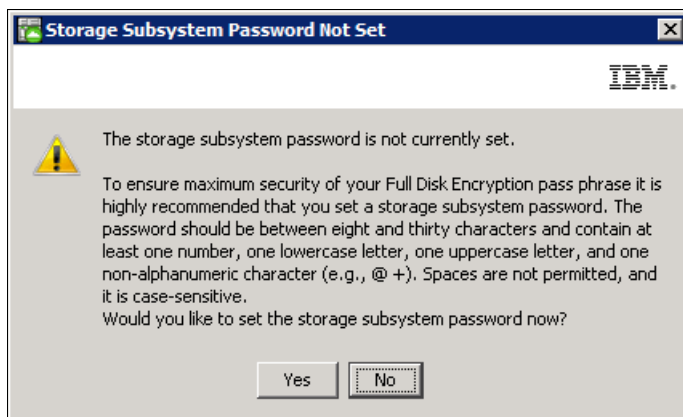


Figure 3-23 Password protection

Note: Make sure to take advantage of the security features of the Storage Manager by setting a password for each of your DS5000 storage subsystems.

- e. The storage subsystem synchronizes with the management station clock when they become out of synchronization. Click **OK** to accept synchronization if prompted to do so.
- f. Now we are connected to the DS5000 storage subsystem, but with the default IP addresses. We need to change the address to your specific ones. In the Subsystem Management window, select the **Setup** tab, and then scroll down to select **Configure Ethernet Management Ports**, as shown in Figure 3-24.

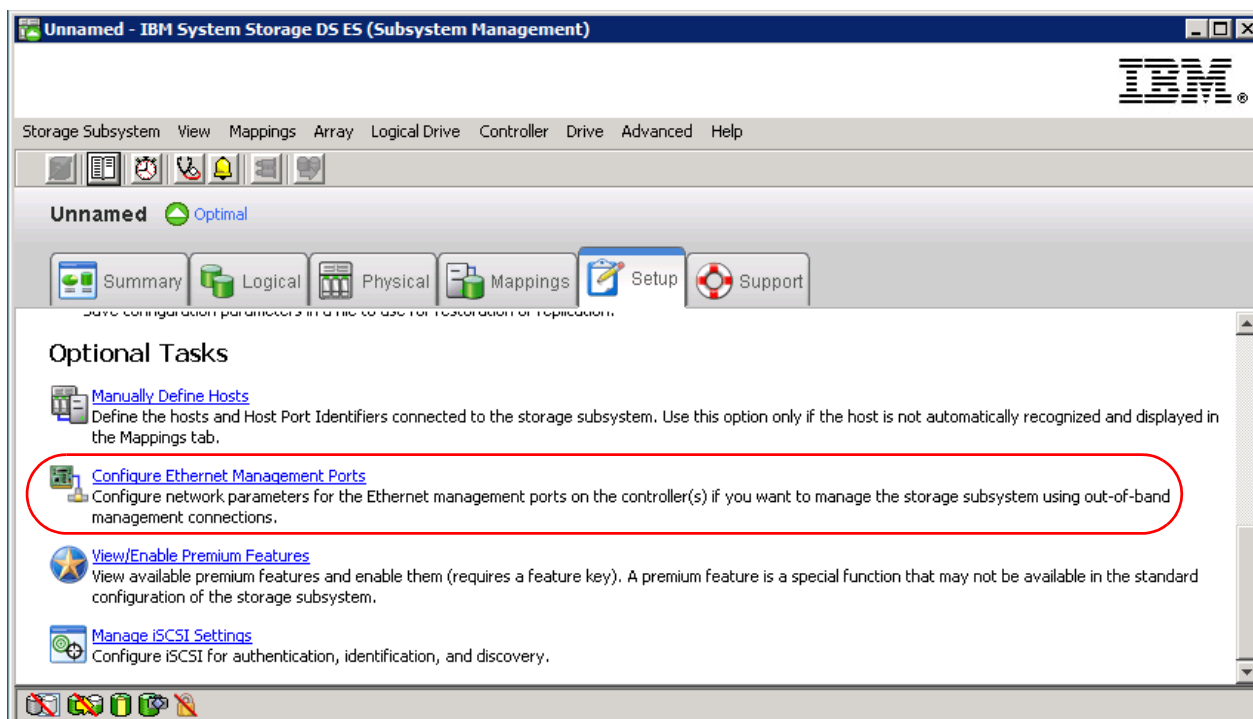


Figure 3-24 Changing the network configuration in the Subsystem Management window

- g. Select either IPv4 or/and IPv6 addressing from the Change Network Configuration screen as shown in Figure 3-25 and Figure 3-26 below.
- h. For IPv4 input the network information on the IPv4 selection panel under the IPv4 tab and click **OK**, as shown in Figure 3-25. You can configure both controllers from this window by selecting the Ethernet port. Make sure to click **OK** after configuring both of them.
- i. This option enables you to specify the controller's IP address, including the gateway address and the network subnet mask. If you want to change the gateway address, click the Change Controller Gateway button. This button is enabled only when the Specify configuration option is selected.
- j. The DS5000 has two Ethernet ports per controller. Cable and select a port from each controller for your management port. If you are planning to have the system connected to only one network, select port 1, leaving port 2 for service. If you are connecting port 2 then you must connect it to a different subnet than that used with port 1. See Figure 3-20 to confirm port locations for where to connect the LAN cables.

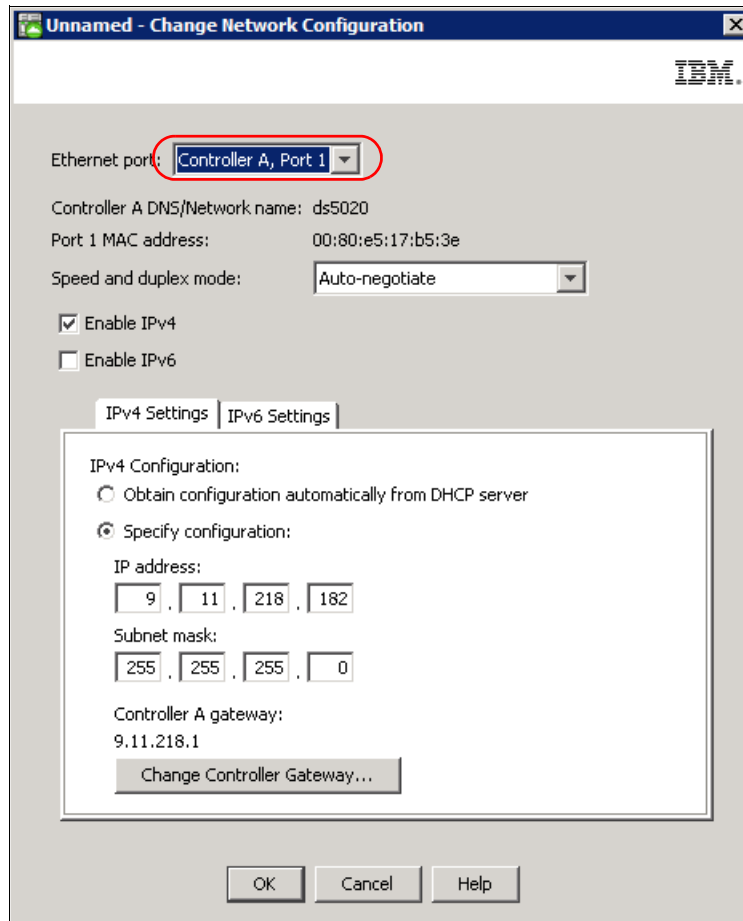


Figure 3-25 DS5000 Controller Network Configuration change IPv4 only

- k. After changing the IP addresses, close the Storage Subsystem window, and remove the selected subsystem from the Enterprise Management window. Then re-add the subsystem, repeating Step b on page 140, but this time, with your newly assigned IP addresses.

Note: To manage storage subsystems through a firewall using out-of-band management, configure the firewall to open port 2463 to TCP data.

- I. If you are selecting both IPv4 and/or IPv6 then you will want to select both the IPv4 and the IPv6 check buttons to enable both as shown in Figure 3-26.

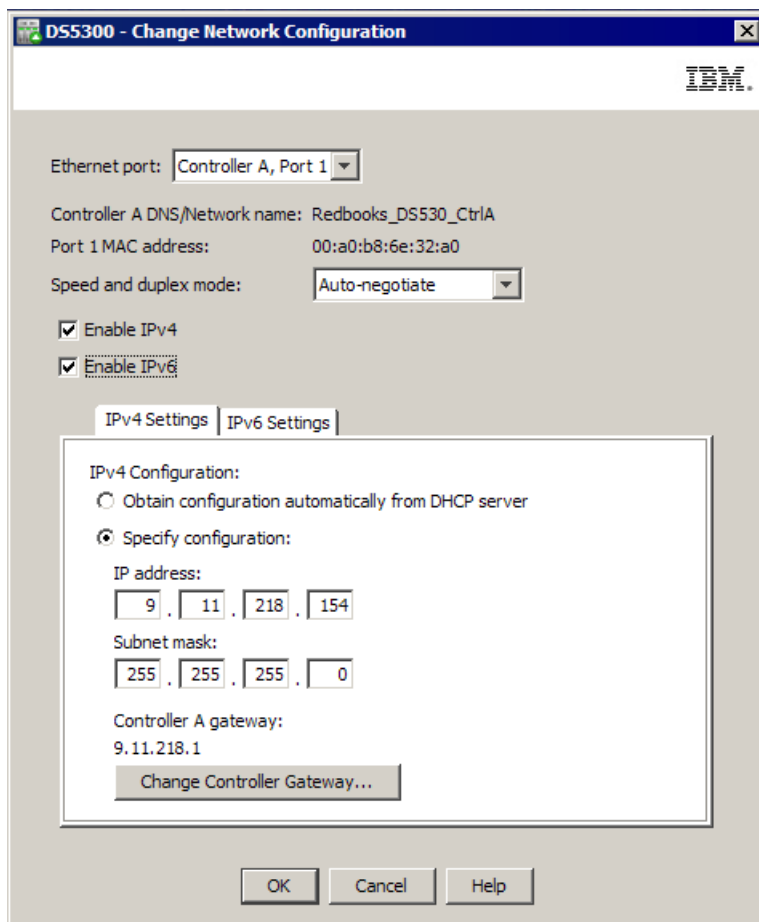


Figure 3-26 DS5000 Controller Network Configuration with IPv4 and IPv6 enabled

- m. With the IPv6 option enabled, IPv6 is now supported and the IPv6 Settings tab shows the IPv6 configuration settings as shown in Figure 3-27. If this option is not selected, all of the configuration settings on the IPv6 Settings tab are disabled.

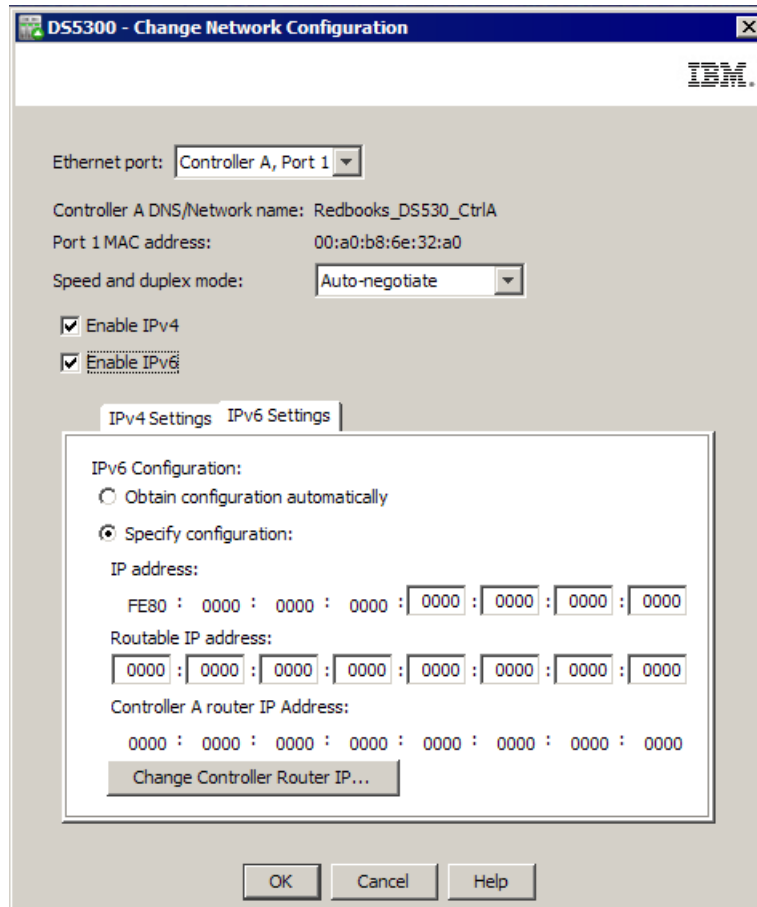


Figure 3-27 IPv6 parameter setting tab

- n. Enter the desired settings you your specific environment and network by selecting the desired choices defined below:
 - i. Obtain configuration automatically

This configuration is obtained using Stateless Address Auto-configuration. If this option is selected, the values appear in the disabled text boxes for IP address, Routable IP address, and Controller router IP address. This option is disabled if the Enable IPv6 check box is not selected.
 - ii. Specify configuration

This option enables you to specify the IP address, the Routable IP address, and the Controller router IP address. This option is disabled if the Enable IPv6 check box is not selected.
 - iii. IP address

This option enables you to specify the last half of an IP address manually. The first half is always FE80:0000:0000:0000. The last four text boxes accept between one and four hexadecimal characters.
 - iv. Routable IP address

This option enables you to manually specify the routable IP address. Each text box accepts between one and four hexadecimal characters.
 - v. Change Controller Router IP

This button opens a dialog that enables you to change the default router IP address that is used when the selected controller's configuration is specified manually. Each text box accepts between one and four hexadecimal characters. This button is only enabled when the Specify configuration option is selected.

- o. When you have completed all your entry selections click “OK” to save the changes; and yes to confirm.
- p. As stated in Step k on page 143, changing the IP addresses, requires closing the Storage Subsystem window, and removing the subsystem from the Enterprise Management window. Then adding the subsystem back, repeating step b on page 140, but this time, with your newly assigned IP addresses.

Note: To manage storage subsystems through a firewall using out-of-band management, configure the firewall to open port 2463 to TCP data.

3.3.4 Using and configuring the DS Storage Manager client

We already know by now that the Storage Manager client GUI uses two main windows:

- ▶ Enterprise Management window
- ▶ Subsystem Management window

In the following sections, we review the different initial setup tasks that you should perform before configuring the storage subsystems for arrays and data storage.

When you start the Storage Manager client, the Enterprise Management window opens, either showing the Device Management section or Setup section, as shown in Figure 3-28.

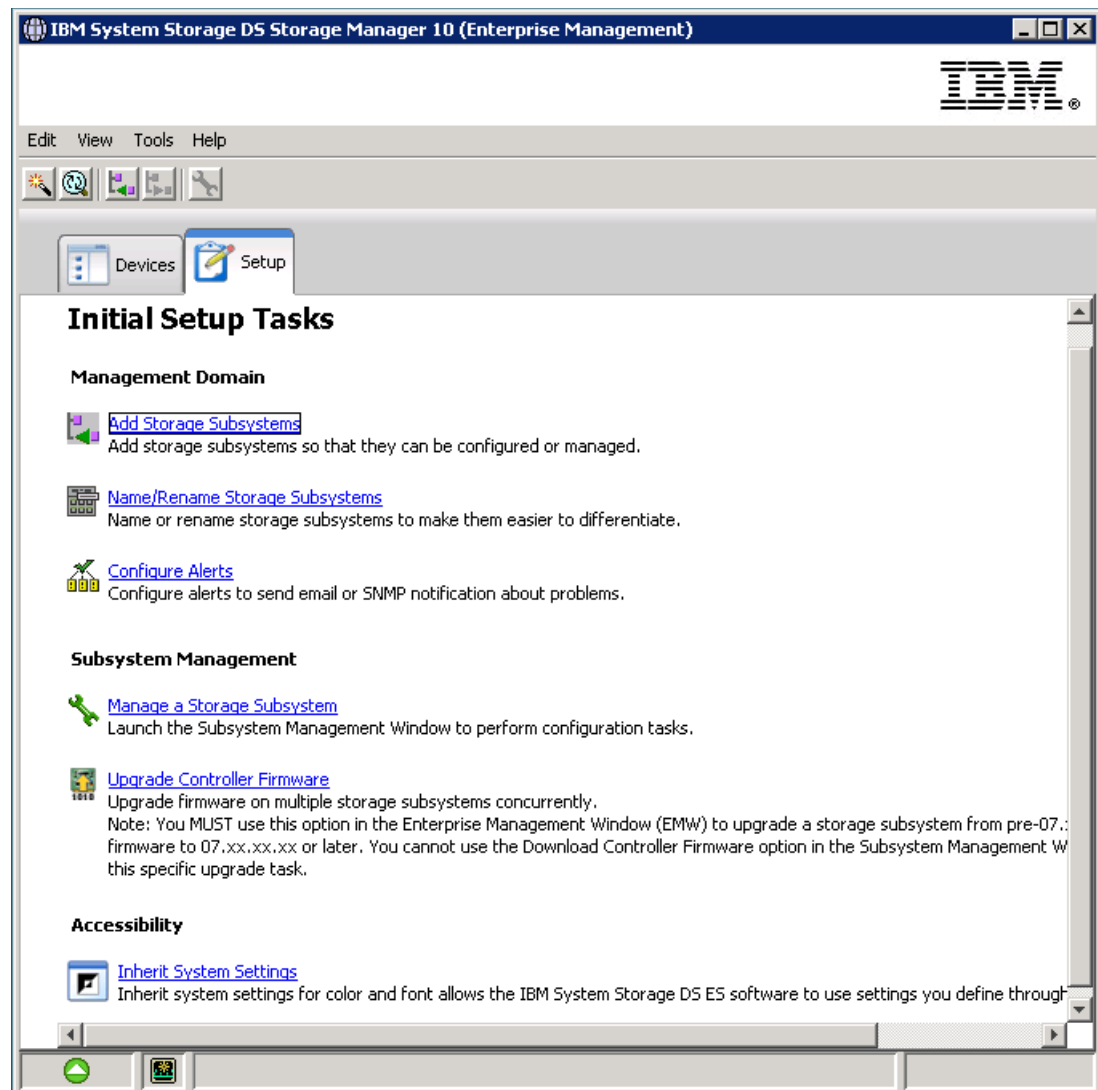


Figure 3-28 Enterprise Management Initial Setup Tasks window

Adding storage subsystems

Before you can manage a DS5000 storage subsystem, you have to add it to the Enterprise Management window. The first time the DS Storage Manager is used, it will prompt you to add a storage subsystem, either automatically or manually. Using the Enterprise Management setup view, you can also invoke the Add Storage Subsystem option at a later time as well as any of the other initial setup tasks shown. You can select either the automatic or the manual addition method, as shown in Figure 3-29.

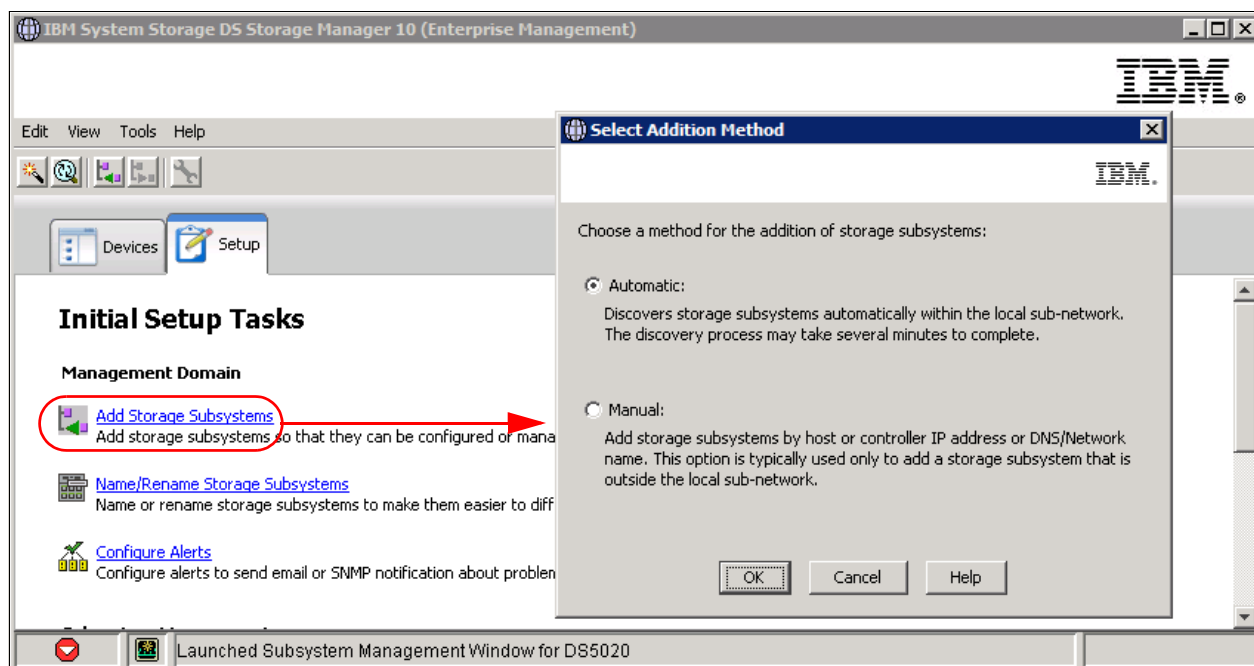


Figure 3-29 Add Storage Subsystems setup task

The automatic discovery process sends out broadcasts through Fibre Channel (if SMagent is installed and started) and the IP network. If it finds directly attached storage subsystems or hosts running the Storage Manager agent (with an attached storage subsystem), and it adds these storage subsystems into the Enterprise Management window.

The manual addition method requires that you provide the IP addresses (or host names) of both controllers for out-of-band management. If one of the controllers is not connected or is not reachable, then some of the management functions cannot be performed (except in cases where you manage a single-controller storage subsystem).

If the DS5000 storage subsystem is managed through the FC path (in-band management), and you want to manage it using a workstation with SMclient installed instead of using the in-band management, you have to specify the IP address of the host attached to the storage subsystem. The Enterprise Management window with different DS5000 storage subsystems is shown in Figure 3-30.

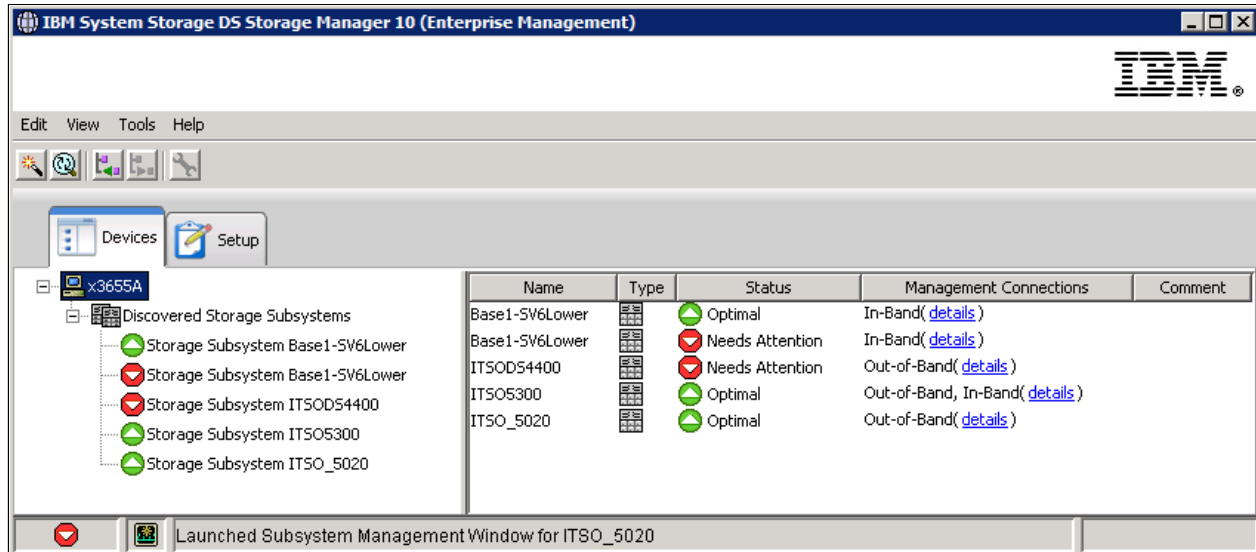


Figure 3-30 Enterprise Management window

You can see all detected DS5000 storage subsystems and how they are managed, either direct (out-of-band) or host-agent attached (in-band), or through both connections. There is also a status column. Usually, the status is Optimal with a green icon next to it, but if there are any problems, the status changes to Needs Attention and a red icon is displayed.

Naming or renaming a storage subsystem

If you installed multiple DS5000 systems, or plan to install more than one, it is important to give each a unique and meaningful name so that you can differentiate it easily from others in the Enterprise Management window.

To accomplish this task, perform these steps:

1. To rename the DS5000 storage subsystem, from the Devices view of the Enterprise Management window, right-click the subsystem to rename and select **Storage Subsystem** → **Rename**.

The other option is to select the **Name/Rename Storage Subsystem** option in the Setup view of the Enterprise Management window, as shown in Figure 3-31.

Name/Rename Storage Subsystems

To name a storage subsystem or change an existing name, select a storage subsystem from the list and enter a new name and optional comment. Use the locate button to help physically identify a storage subsystem.

Storage arrays

Select storage subsystem:

Name	Status	Management Connections	Comment
Unnamed	Optimal	Out-of-Band, In-Band	

Locate

Name and comment

Storage Subsystem name (max. 30 characters):
DS5020

Additional comment (max. 60 characters):
DS5020 located in Rack3 of Main Datacenter

Tip: Comments can be helpful in locating an array, and are displayed in the Enterprise Management Window.

OK Cancel Apply Help

Figure 3-31 Initial Setup Tasks: Name or rename a storage subsystem

2. Type in the name you want to assign to your storage subsystem (there is a 30-character limit). All leading and trailing spaces are deleted from the name. Use a unique, meaningful naming scheme that is easy to understand and remember. You can also assign a comment to facilitate its identification.
3. Click **OK** to finish the name assignment.

Setting the controller clocks

Because the DS5000 storage subsystem stores its own event log, you need to synchronize the controller clocks with all the host systems accessing it. This improves problem determination procedures. If you have not already set the clocks on the storage subsystems, set them now. Be sure that your local system is using the correct time, and then select **Storage Subsystem** → **Set Controller Clock** (Figure 3-32).

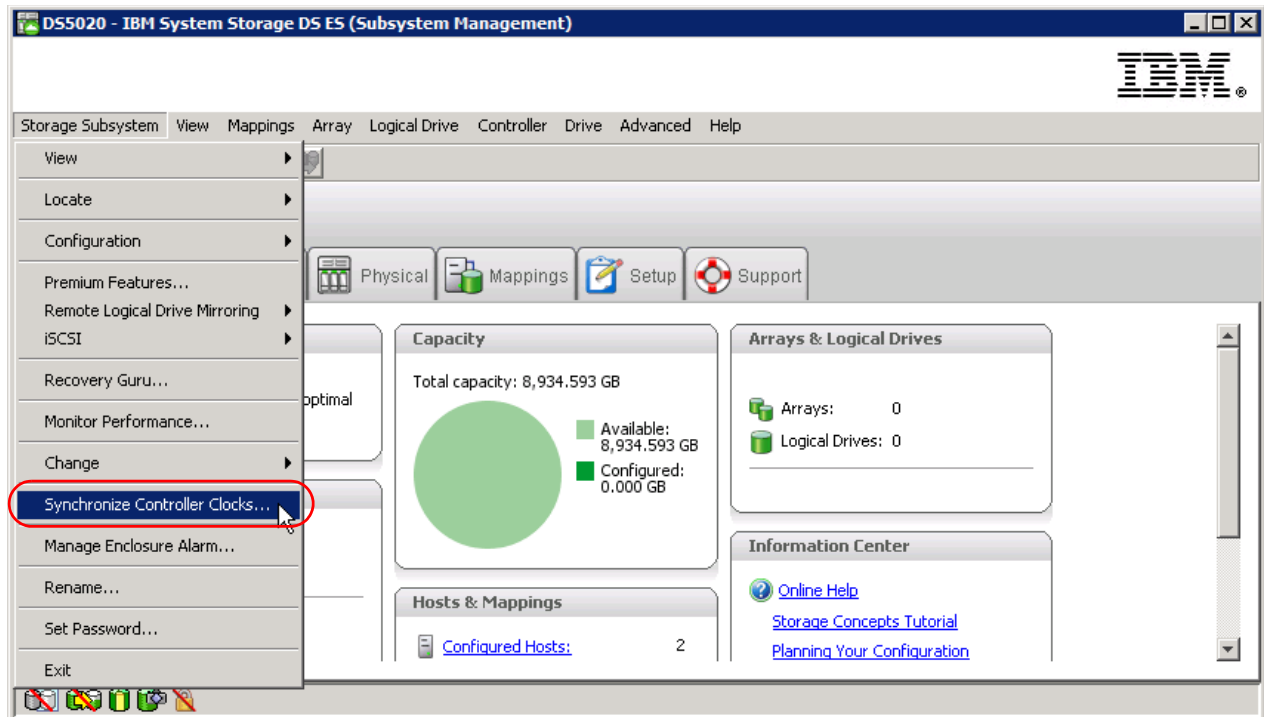


Figure 3-32 Setting the controller clock

Setting a security password

For security reasons, especially if the DS5000 storage subsystem is directly attached to the network, you should set a password. This password is required for all actions on the DS5000 storage subsystem that change or update the configuration in any way.

To set a password, highlight the storage subsystem, right-click it, and select **Storage Subsystem** → **Set Password** (see Figure 3-33). This password is then stored on the DS5000 storage subsystem. It is used if you connect through another SMclient, no matter whether you are using in-band or out-of-band management.



Figure 3-33 Setting the password

Note: Setting a password provides additional protection for a DS5000 storage subsystem in a public LAN. However, you gain higher protection by connecting the DS5000 storage subsystem to a private network reserved for administration.

Be aware that after the password is set, no modification commands will be allowed without the password.

Configuring alerts

This option allows you to set up the alert structure. If there are any problems with any of the storage subsystems, an e-mail or an SNMP notification can be sent. The Initial Setup Tasks view of the Enterprise Management window allows you to configure alerts for all storage subsystems, for a group of them, or for a single one.

We provide a detailed description of the Configure Alerts option in 3.5.7, “Monitoring and alerting” on page 202.

Setting Enclosure Order

Verify that the enclosures in the right half of the window reflect your actual physical layout. This ensures that you do not perform maintenance activities in the wrong enclosure. If the enclosures are listed in an incorrect order, select **Storage Subsystem** → **Change** → **Enclosure Order**, as shown in Figure 3-34.

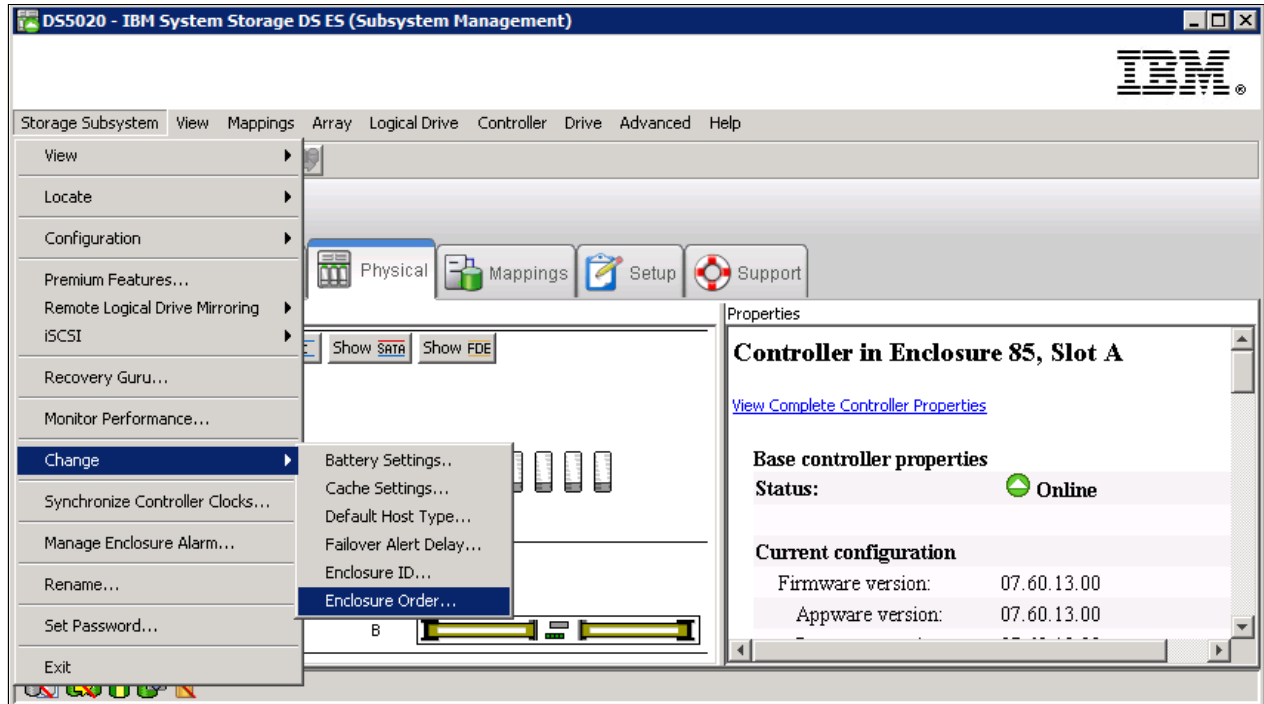


Figure 3-34 Change the enclosure order

Now you can sort the enclosures according to your site setup, as shown in Figure 3-35.

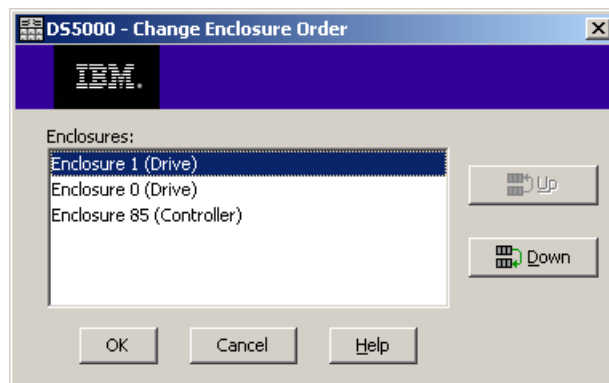


Figure 3-35 Changing the enclosure order

Manage Enclosure Alarm

Enclosure alarms can be managed from the Storage Manager subsystem window. This is done by selecting **Storage Subsystem** → **Manage Enclosure Alarms**.

Manage Enclosure Alarms is used to respond to an alarm on the DS5000 storage subsystem. If a critical failure of the storage subsystem or an enclosure attached to it occurs, then an audible alarm will sound if it is enabled.

The audible alarm is just one of three ways in which Storage Manager will inform you of a fault. The other two are that the Alarm button becomes animated and the Recovery Guru button in the toolbar appears.

By default, the alarm is disabled, but this can be changed by the Storage Manager client. This can be done on all enclosures or individual enclosures and controllers (Figure 3-36). The two options are to always sound an alarm or never sound an alarm.

The lower part of the window shows the alarms that are already sounding, which can be silenced by clicking the **Silence Alarm(s)** button.

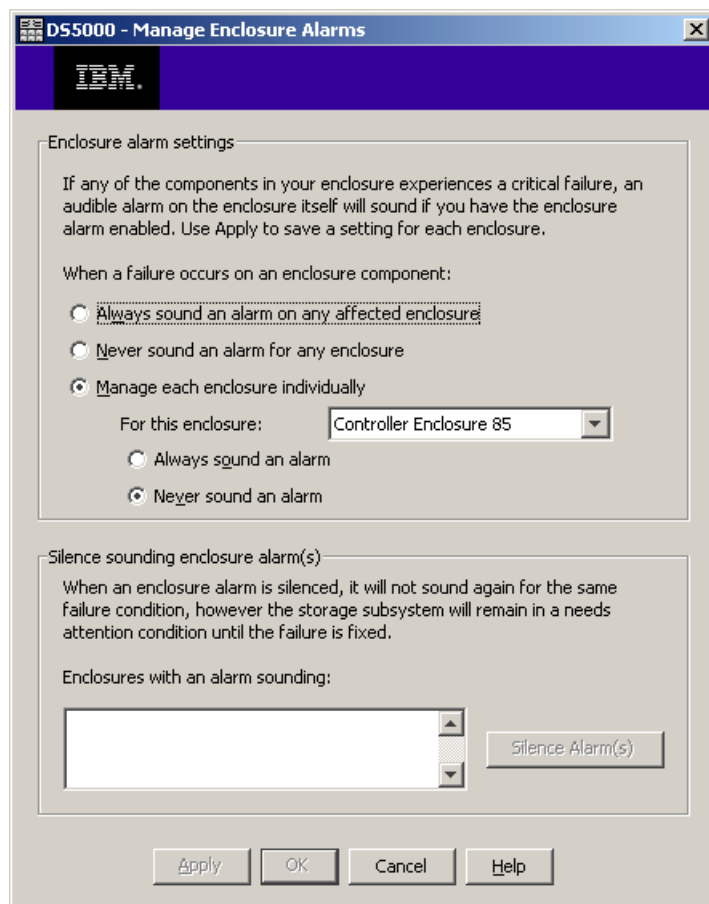


Figure 3-36 Manage Enclosure Alarms

3.3.5 Updating the controller microcode

Before you use your DS5000 storage subsystem to process production data, update the firmware (or microcode) of your DS5000 storage subsystem to prevent any unnecessary, known failures, and make use of the latest improvements. New firmware might be required when installing a new version of the Storage Manager software. Check the IBM support Web site for all available updates at the following address:

<http://www.ibm.com/servers/storage/support/disk>

Because firmware updates are a customer responsibility, it is a recommended practice to periodically review this Web site for newer versions in order to keep your DS storage subsystem updated with the latest fixes and enhancements.

To facilitate this task, you can subscribe to a service at the IBM My Support Web site that will send you automatic notifications about new firmware. You will receive an e-mail when new firmware levels have been updated and are available for download and installation. To register for My Support, visit the following address:

<http://www.ibm.com/support/mysupport/us/en>

From the Web site, select your specific DS5000 model and click **Download**. The available firmware packages and versions for your product will be shown.

The DS5000 storage subsystem components that can be updated are:

- ▶ Controller firmware
- ▶ Non-Volatile Static Random Access Memory (NVSRAM)
- ▶ Environmental services monitor, ESM, and canister
- ▶ Disk drives

For complete instructions, see the *readme* file included with the specific component and version you want apply, which is available at the IBM support Web site. You can find a detailed procedure in 5.1.5, “Updating controller firmware” on page 292.

Always check the IBM System Storage Interoperation Center (SSIC) Web site for the latest supported combinations of firmware in your specific environment before upgrading at the following address:

<http://www.ibm.com/systems/support/storage/config/ssic/index.jsp>

Note: Use the IBM System Interoperation Center Web site to check the latest compatibility information before making any changes in your storage subsystem environment

3.4 Step-by-step configuration

This section describes the major steps in the configuration of a DS5000 storage subsystem:

1. Configuration planning
2. Enabling the premium features
3. Creating arrays and logical drives
 - a. Using the Automatic Configuration Wizard
 - b. Using the manual procedure
4. Configuring storage partitioning
5. Configuring logical drives from Windows
6. Monitoring and alert options
7. Protecting the configuration

3.4.1 Configuration planning

Before starting to configure your DS5000 storage subsystem, you should draw up a plan of how the storage subsystem will be designed and layed out for use. This will allow you implement your storage requirements in the best way, minimizing any problems with a future desired reconfiguration. Keep all the necessary information regarding the different configuration options in your plan in order to configure your storage. See the planning tasks section of *IBM System Storage DS5000 Series Implementation and Best Practices Guide*, SG24-8024 for more information about planning your storage layout.

3.4.2 Enabling the premium features

In order to activate your purchased premium features, perform these steps:

1. Obtain the Feature Enable Identifier for your Storage Subsystem.
2. Use the Web to generate the activation file.
3. Install the activation file using the DS Storage Manager.

Obtain the Feature Enable Identifier for your storage subsystem

From the Subsystem Management window of your DS5000 storage subsystem, select **Storage Subsystem** → **Premium Features**. This opens a window that shows the current activation status of the premium features in your subsystem, as shown in Figure 3-37.

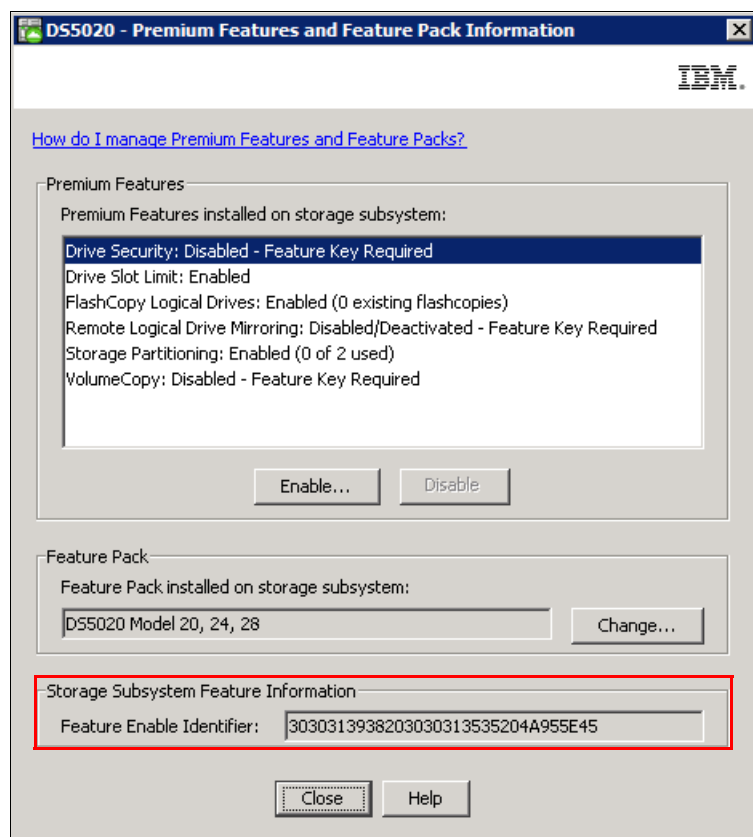


Figure 3-37 Premium Features and Feature Pack Information

Record the Feature Enable Identifier and continue with the next section to generate your activation file. Later we use the same options and window to activate the purchased premium features.

Use the Web to generate the activation file

With the Feature Enable Identifier and the registration card provided with the machine for the purchased premium features, go to the following Web site to generate the activation file:

<https://www-912.ibm.com/PremiumFeatures/>

In the Web site, select **Activate a Premium Feature**, read the requirements, and then click **Continue**. Complete the fields presented in the window shown in Figure 3-38 by entering the feature activation code received in the card shipped with the DS5000 storage subsystem, the

feature enable identifier obtained in “Obtain the Feature Enable Identifier for your storage subsystem” on page 156, and your specific machine type, model number, and serial number.

IBM System Storage: Storage subsystem premium feature activation and registration: gather ...

File Edit View Favorites Tools Help

Address <https://www-912.ibm.com/PremiumFeatures/jsp/keyInput.jsp> Go

IBM Systems support

- BladeCenter
- Power
- System i
- System p
- System x
- System z
- System Storage
 - Support search
 - Register
 - Feedback
- Systems networking
- System Blue Gene
- IntelliStation Pro
- IBM Monitors
- Systems Management software
- Hardware options and upgrades

Related links

- Storage Interoperability with Systems
- Warranty information
- Case studies
- IBM Business Partners
- IBM Systems agenda
- IBM eServer
- Redbooks
- Small & Medium Business

IBM Systems > Support >

IBM DS3000, DS4000, DS5000 and BladeCenter Boot Disk System activation and registration

Activate a Premium Feature

The fields indicated with an asterisk (*) are required to complete this transaction; other fields are optional. If you do not want to provide us with the required information, please use the "Back" button on your browser to return to the previous page, or close the window or browser session that is displaying this page.

*Activation type ☒ Premium Feature

Enter your feature activation code. The feature activation code (XX-XXXX-XXXXX) is located at the top of the expansion module license activation card that you purchased.

*Feature activation code

Enter your 32-digit DS3000, DS4000, DS5000, FASTT or BladeCenter Boot Disk System subsystem feature enable identifier from your storage manager software. This information can be found in your Storage Subsystem Profile or by selecting from your subsystem management window *Storage Subsystem > Premium Features > List* or *Tools > View/Enable Premium Features*.

*Feature enable identifier

Enter your DS3000, DS4000, DS5000 or BladeCenter Boot Disk System controller unit machine type, model number and serial number. This information is printed on a label, which is located on the back of your DS4000 controller unit (for DS4100, DS4300, DS4400, DS4500 and FASTT), or on the left front mounting bracket (for DS3000, DS4200, DS4700, DS4800, DS5100, DS5300 and BladeCenter Boot Disk System). To access the mounting bracket, you will need to remove the front bezel.

*Machine type

*Model number

*Unit serial number (sn)

Figure 3-38 Premium features registration

Note: At the time of writing, the serial number for the storage subsystem is only located on the rear of the DS5000 controller on an IBM serial number sticker.

Scroll down, complete the remaining fields by entering your e-mail address, and submit the information by clicking **Continue**. The activation key file is then e-mailed to you. Save the received file in your folder, and continue with next step.

Install the activation file using the DS Storage Manager

From the Subsystem Management window of your DS5000 storage subsystem, select **Storage Subsystem → Premium Features**. This opens a window that shows the current activation status of the premium features in your subsystem. For our example we will use the *VolumeCopy* premium feature as shown in Figure 3-39.

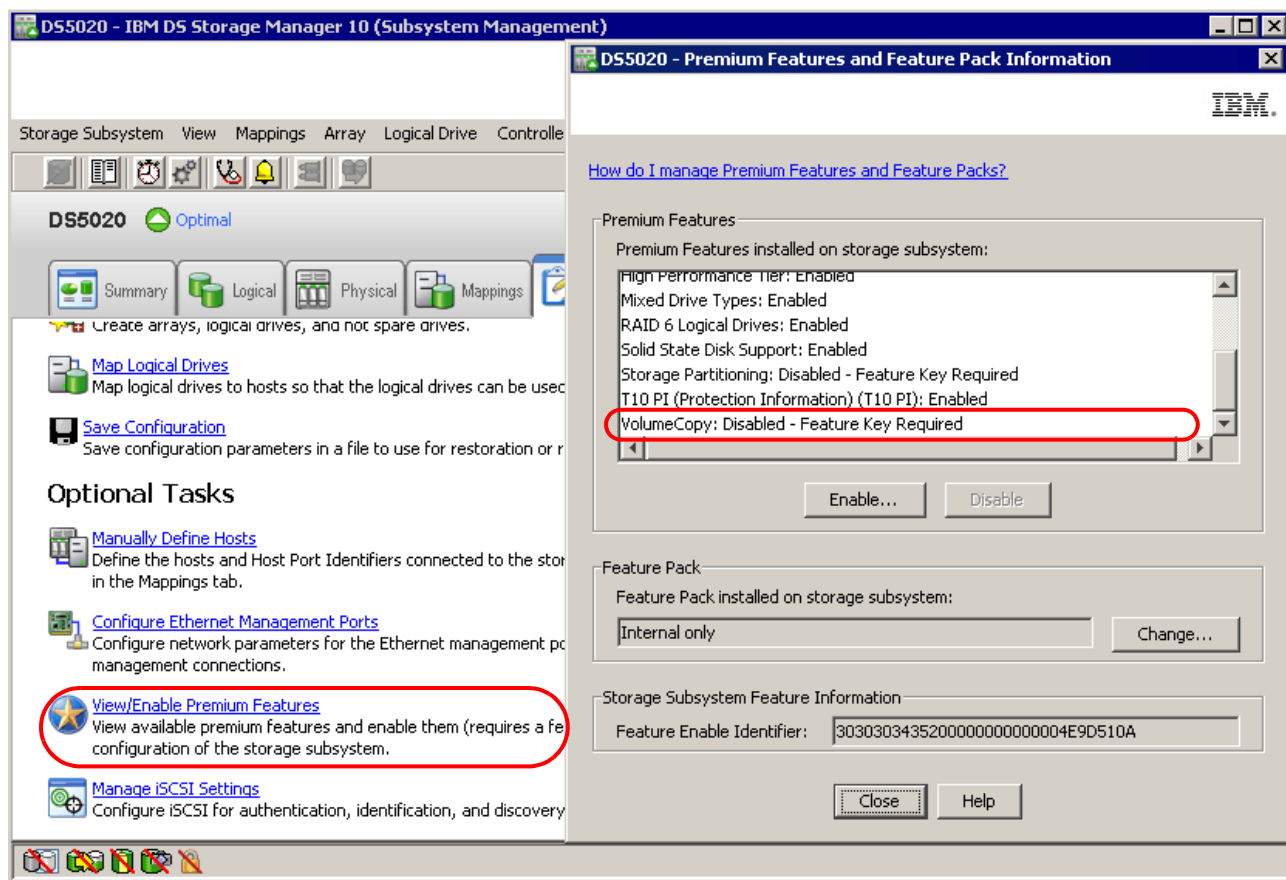


Figure 3-39 Example of premium feature in disabled state

Click **Enable** and select the key file that you received by e-mail as shown in Figure 3-40.

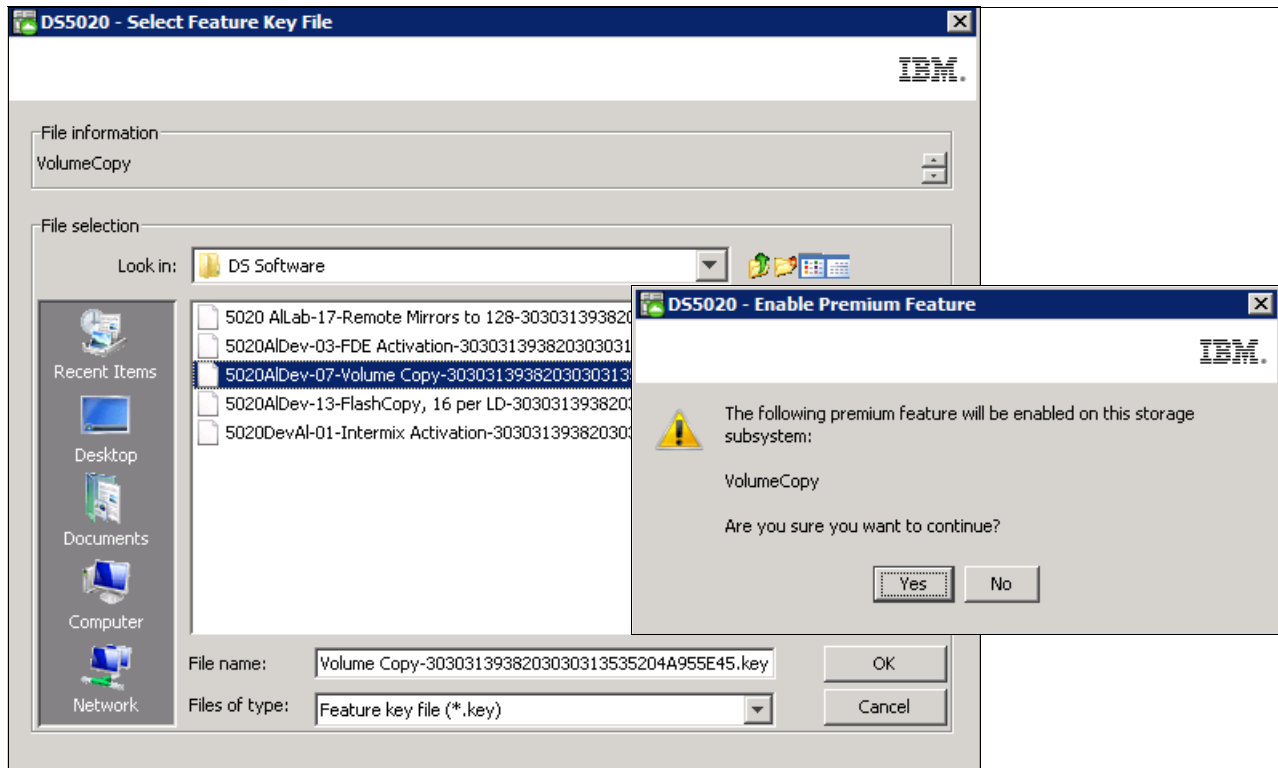


Figure 3-40 Selecting key file for premium features activation

Confirm the Enable Premium Feature action by clicking the **Yes** button. Then select **Storage Subsystem** → **Premium Features**, or select the **Setup** view of the Subsystem Management window and then **View/enable Premium Features**. The premium feature activated shows as **Enabled**, as shown in Figure 3-41.

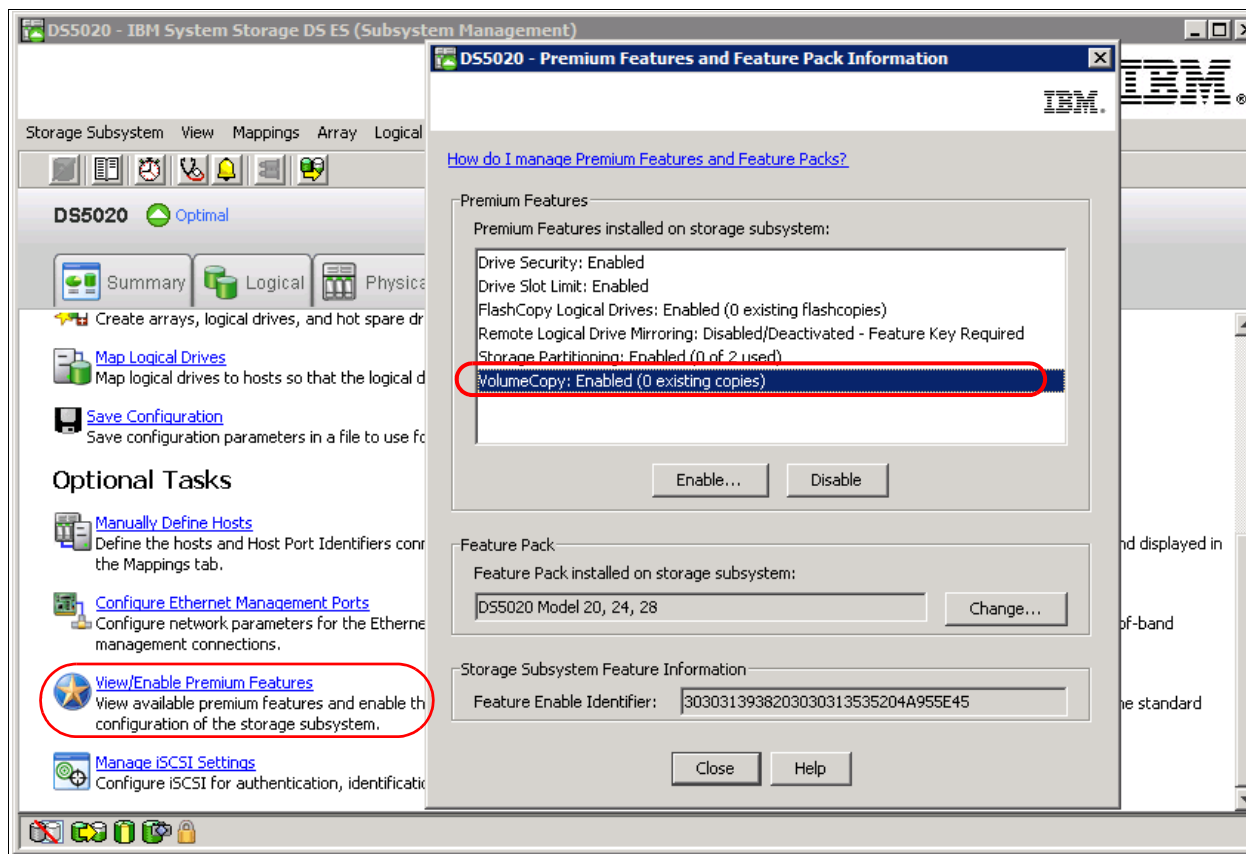


Figure 3-41 Premium feature activated

Repeat the previous steps for any purchased premium features that have not yet been activated.

3.5 Methods of configuring

With the IBM DS Storage Manager there are two methods by which you can configure the storage in the DS5000 storage subsystem;

- ▶ Automatic - using the configuration wizard building a single configuration model for all arrays and LUNs.
- ▶ Manual - using the step by step process to chose the configuration and settings as selected during the planning phase for each of the arrays and LUNs.

3.5.1 Automatic configuration

In this section, we cover the necessary steps to configure unconfigured storage subsystem capacity into logical drives using the Automatic Configuration wizard integrated into the DS Storage Manager software.

The Automatic Configuration wizard can be used to create multiple arrays with logical drives, and hot spare drives using the same attributes for all arrays, such as RAID level, number of drives per array, number of logical drives, and I/O type. The wizard configures all the non-configured disk drives in the system with minimal interaction.

Important: Default settings for the Automatic Configuration are to build 3+P RAID 5 arrays. This configuration may not provide optimal performance for your environment, and uses a good amount of space for parity. Therefore, it is recommended that you consider changing this to a larger number of drive members as discussed in the planning tasks section of *IBM System Storage DS5000 Series Implementation and Best Practices Guide*, SG24-8024.

If you need to define space that has not been used in already defined arrays, or wish to configure capacity with specific parameters you have selected in planning, you may find the manual configuration method more useful. It is described in 3.5.2, “Manual configuration” on page 166, and allows you to select each of the parameters for the creation of both arrays and logical drives. This method is best when you need to mix various array types and sizes, and differing LUN size and settings on your configuration.

To access the Automatic Configuration wizard, perform these steps:

1. From the Enterprise Management window, select the DS5000 storage subsystem you want to configure. Double-click it or right-click it and select **Manage Storage Subsystem**.
2. From the Subsystem Management interface, select **Storage Subsystem** → **Configuration** → **Automatic**, or from the Setup view of the Subsystem Management interface, select **Configure Storage Subsystem** → **Automatic Configuration** → **OK**.

Here is an example showing the different steps:

1. Select **Configure Storage Subsystem** → **Automatic Configuration** → **OK**, as shown in Figure 3-42.

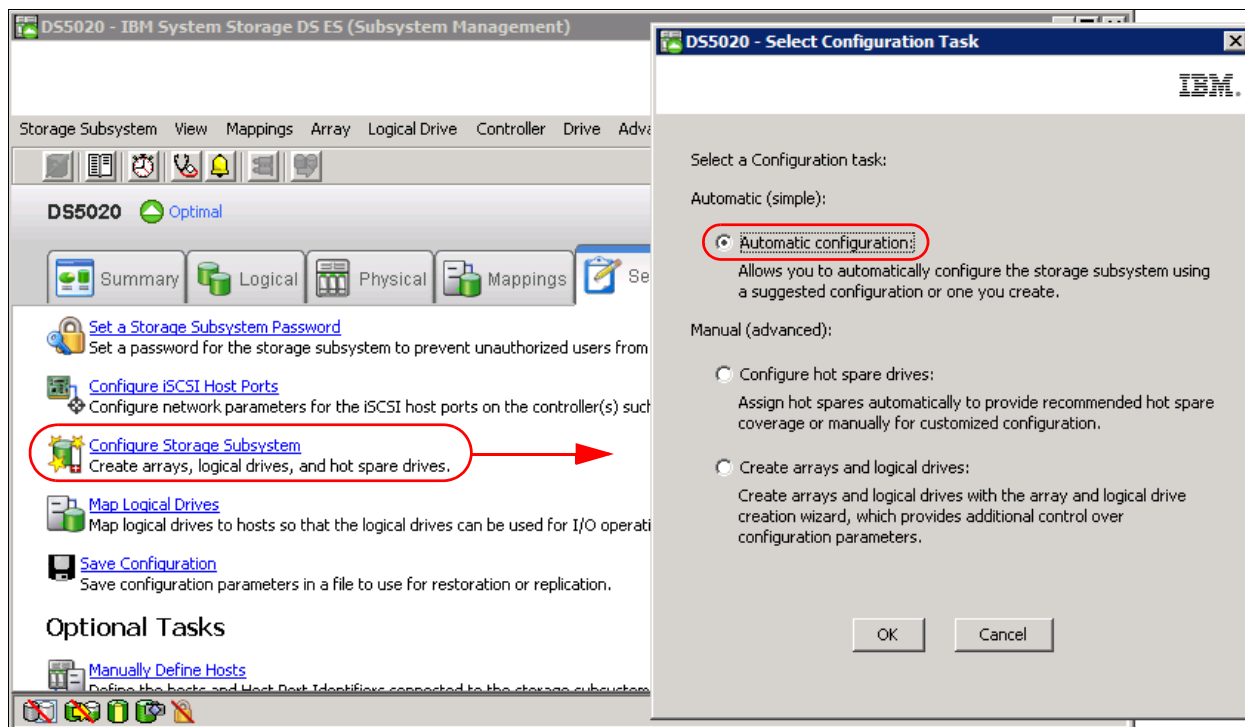


Figure 3-42 Automatic configuration

2. Read the introduction window. It reminds you to quit the wizard and start a manual configuration process if your requirements need different RAID levels, volume sizes, and so on. If this is not the case, click **Next** to continue.

3. In the window that follows, choose between **Choose a suggested configuration**, selecting the RAID level desired, or **Create your own configuration**, as shown in Figure 3-43.

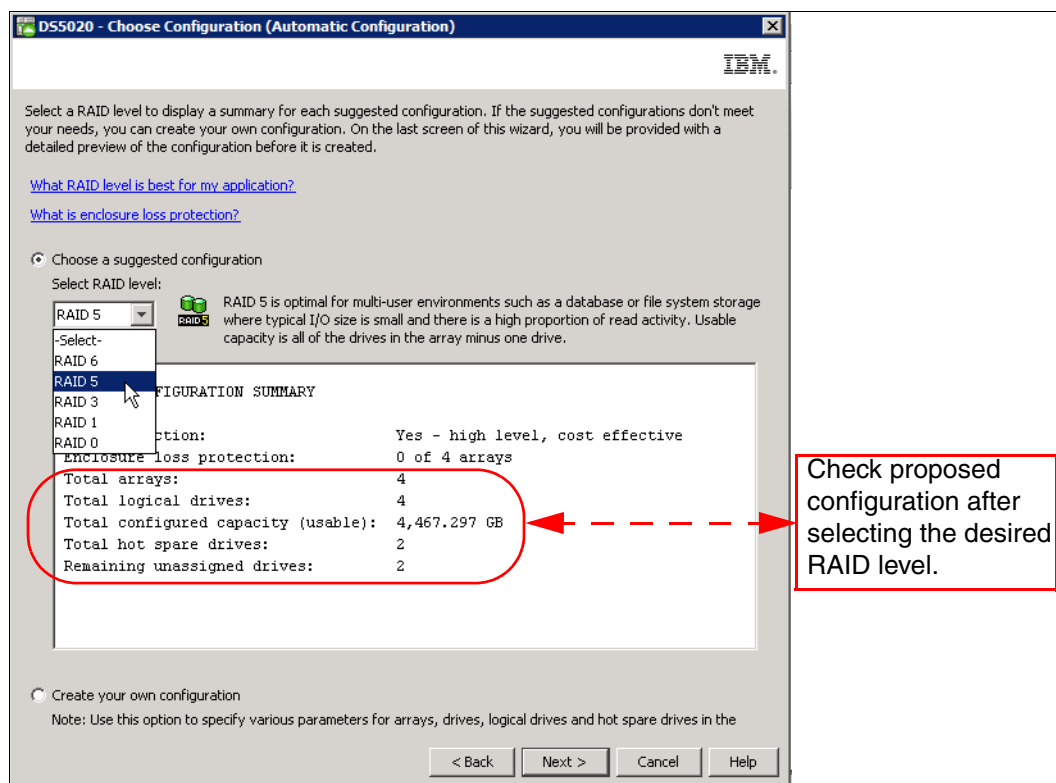


Figure 3-43 Choosing the RAID level

- Suggested configuration: This is the default option, where you only have to select the RAID level to be applied to all unconfigured disks. Once you select the RAID level, a summary is presented based on the resources available in your configuration. Check this summary configuration. You can also click **Next** to see a preview of the resulting configuration, based on the RAID level selected and the quantity of free drives in the system.

Review the information carefully, and if it is correct, click **Finish** to proceed.

- Create your own configuration: This allows you to customize the configuration by selecting the additional parameters shown in Figure 3-44.

DS5020 - Create Your Own (Automatic Configuration)

HDD/FIBRE | HDD/SATA

Use the following worksheet to define the appropriate number of arrays, drives, and logical drives you want to create.

[Tips and examples on allocating capacity](#)

[What RAID level is best for my application?](#)

[What is the I/O characteristic type?](#)

Array parameters

Drives available for configuration: 8

Select RAID level:

RAID 5 RAID 5 is optimal for multi-user environments such as a database or file system storage where typical I/O size is small and there is a high proportion of read activity. Usable capacity is all of the drives in the array minus one drive.

Number of arrays: 1

Drives per array: 7

Hot spare drives: 1

Allocated Drives

Total allocated drives (8 maximum): 8

Remaining unassigned drives: 0

Number of logical drives

Number of equal-sized capacity logical drives (per array): 6

I/O characteristic type: File system (typical)

Dynamic cache read prefetch: Enabled

Segment size: 128 KB

Change I/O Type...

Show Summary

< Back Next > Cancel Help

Figure 3-44 Customized automatic configuration

The options for both Fibre Channel or SATA drives are:

- RAID level: 0, 1, 3, 5, or 6 (or RAID 10 by selecting multiple drives in RAID 1)
- Number of logical drive groups or arrays
- Number of drives per array
- Number of hot spares
- Number of logical drives per array
- I/O type characteristics

The window that appears lets you modify each of the parameters, as though you were using a worksheet, and gives you the option to have a red warning appear if your selections exceed the available resources. If you have both FC and SATA drives, you have to complete two separate worksheet windows to set your desired configuration.

You can select the online help for an explanation of each of the parameters. For additional information, refer to the planning tasks section of *IBM System Storage DS5000 Series Implementation and Best Practices Guide*, SG24-8024.

Click **Change I/O type** if you want to set up your logical drives for other types of access (this is different than the preset defaults for regular file systems, as shown in Figure 3-45).

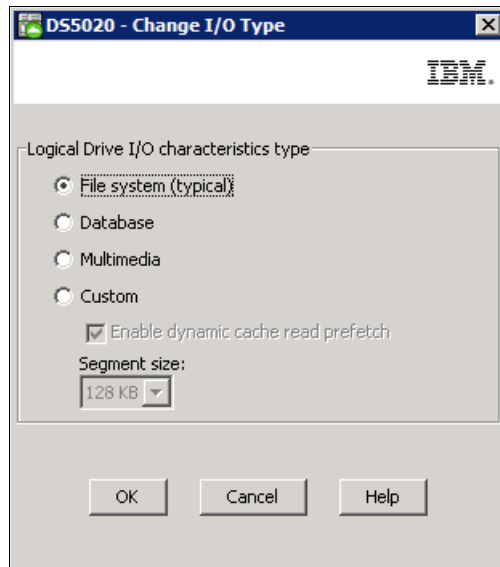


Figure 3-45 Changing I/O characteristics

For additional information about these values, refer to the planning tasks section of *IBM System Storage DS5000 Series Implementation and Best Practices Guide*, SG24-8024.

Once you have specified all of your desired values, click **OK** to open the window shown in Figure 3-46.

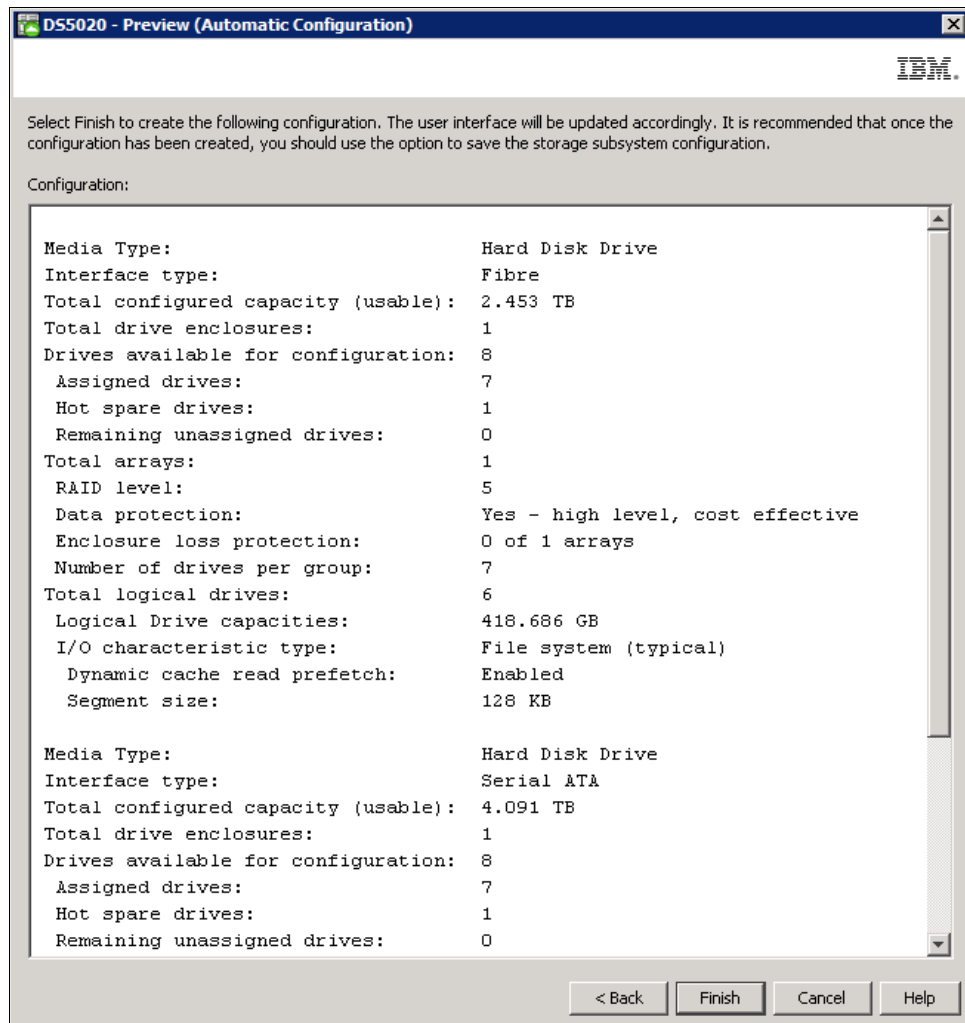


Figure 3-46 Preview automatic configuration

- Review the configuration that will be created based on your input, and click **Finish** to proceed. You see a confirmation message informing you that, depending on the number of drives and volumes, it might take some time for all the changes to appear in the Management window. Do not submit another request until this configuration is complete. You can check the event log to see whether the operation was successful.

5. After completion, the Storage Manager shows the arrays, logical drives, and hot spares created automatically based on your input, as shown in Figure 3-47.

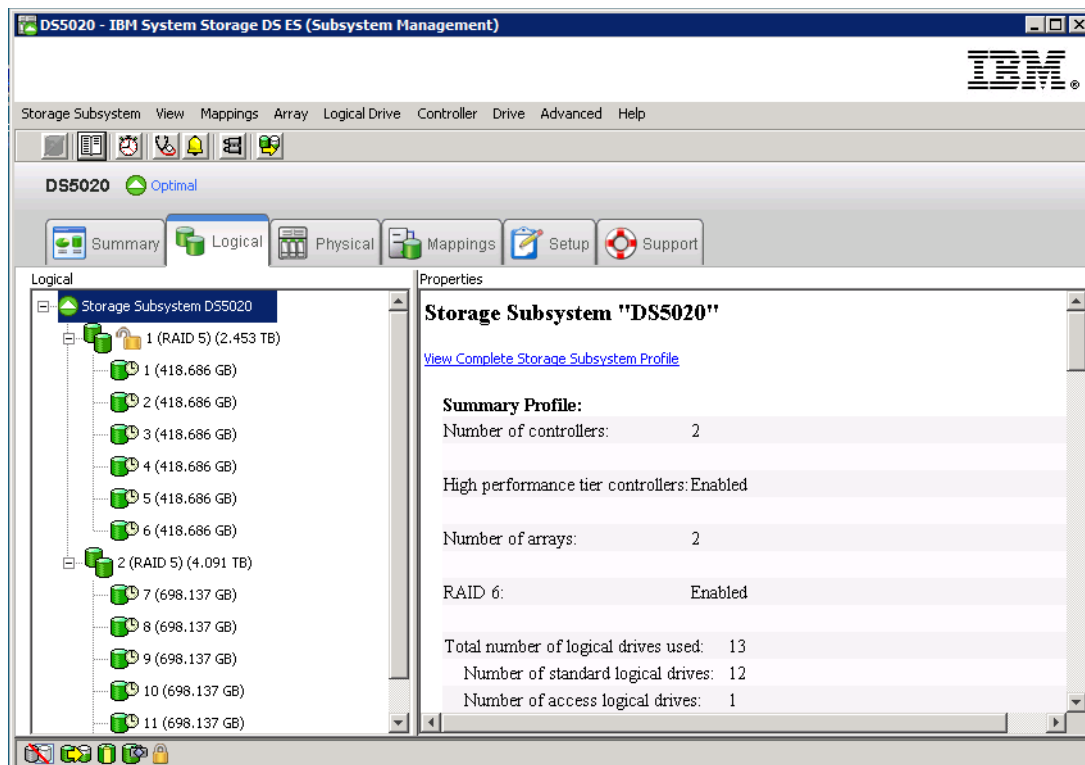


Figure 3-47 Automatic configuration results

3.5.2 Manual configuration

In this section, we cover the necessary steps to configure available storage subsystem capacity into logical drives using the Storage Manager interface. We already covered the automatic procedure, where the options are limited. Now we cover the additional parameters that you can select to better configure the storage for your environment.

We split the tasks into two sections, starting with the creation of global hot spares. We recommend performing this task first to ensure that you have enough spare drives before creating the logical drives.

3.5.3 Defining hot spare drives

The concept of a hot spare drive is explained in the planning tasks section of *IBM System Storage DS5000 Series Implementation and Best Practices Guide*, SG24-8024. Here we cover the available methods of defining hot spare drives with Storage Manager V10.77. Because we planned for hot spares in our configuration, we will start with assigning hot spare drives and then continue to the arrays.

To start configuring hot spares, from the Setup view of the your Subsystem management window, select **Configure Storage Subsystem**, as shown in Figure 3-48.

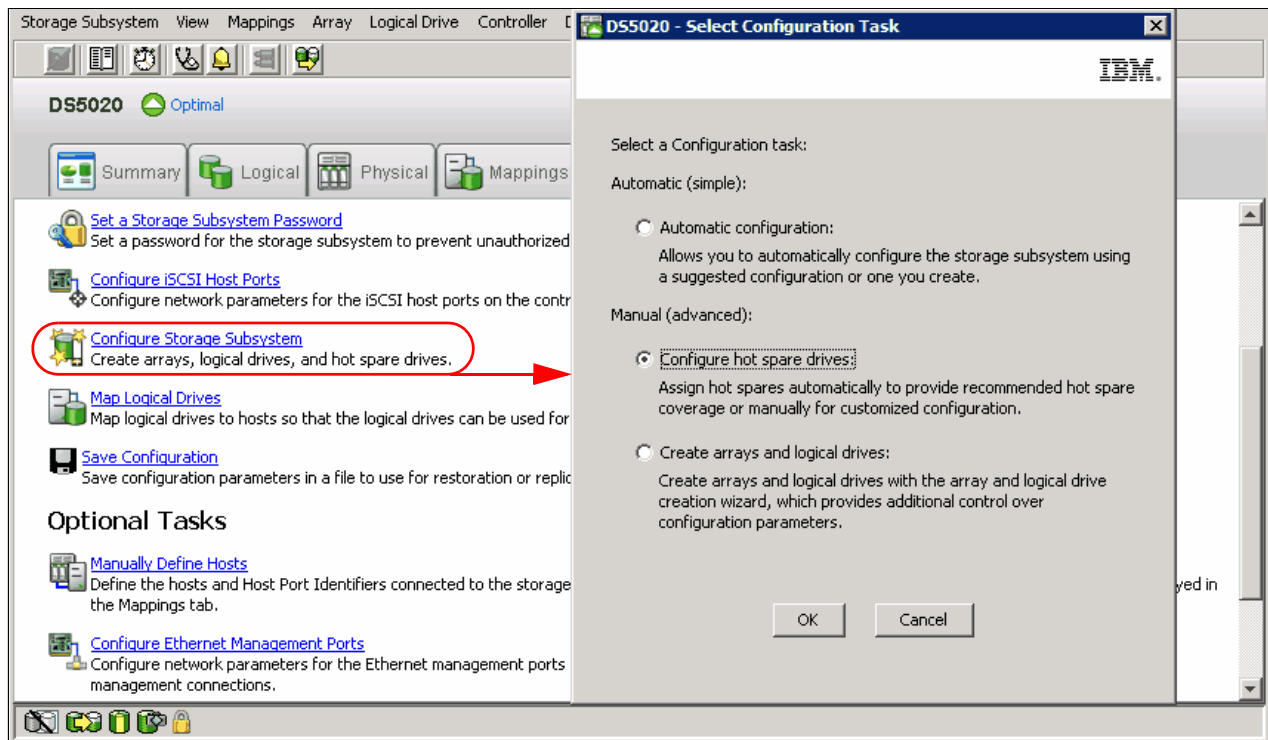


Figure 3-48 Configuring hot spares

Select **Configure hot spare drives**. The window shown in Figure 3-49 opens.

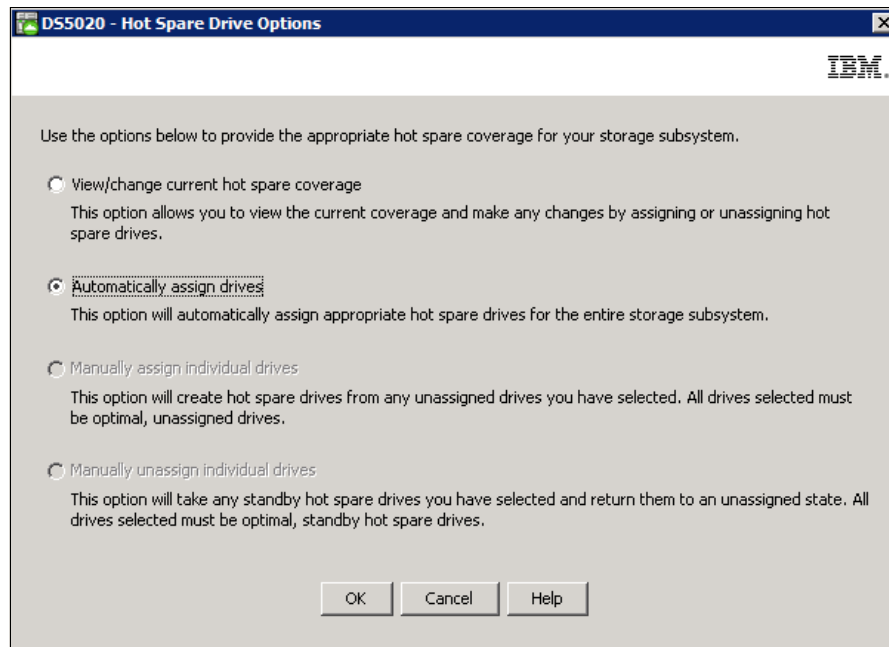


Figure 3-49 Hot Spare Drive Options

You have two methods to define hot spare drives:

- ▶ Automatic assignment
- ▶ Manual assignment

Tip: Select drives of equal or greater size than the total capacity of the largest disk in the storage subsystem.

Especially in large configurations with arrays containing many drives, it might be necessary to define multiple hot spares, because the reconstruction of a failed drive to a hot spare can take a long time.

Consider having spares for each type of disk drives, that is, FC, FC-SSD, SAS, SAS-SSD, SATA, and security enabled FDE.

For an array that has FDE drives that are not secured, the hot-spare drive can be either an unsecured FDE drive or a non-FDE drive.

For an array that has secured FDE drives, the hot-spare drive should be an unsecured FDE drive of the same or greater capacity. While the unsecured FDE hot-spare drive is used as a spare for a failed drive in a secured RAID array, it is security enabled. After the failed drive in the secured RAID array is replaced, and the rebuild is complete, the use of the secured FDE hot-spare drive is finished, and it the FDE hot-spare is cleaned and again set back to the unsecured FDE state for reuse as a hot spare for both unsecure and secure arrays.

Automatic assignment

For automatic hot spare assignment, follow these steps:

1. To automatically create the hot spare coverage using the drives that are available, select **Automatically assign drives**, as shown in Figure 3-49 and click **OK**. The recommended quantity of spares drives needed for your configuration are created automatically.
2. Select the **Physical** tab to view the results of the automatic hot spare creation. You see the drives assigned in Figure 3-50.

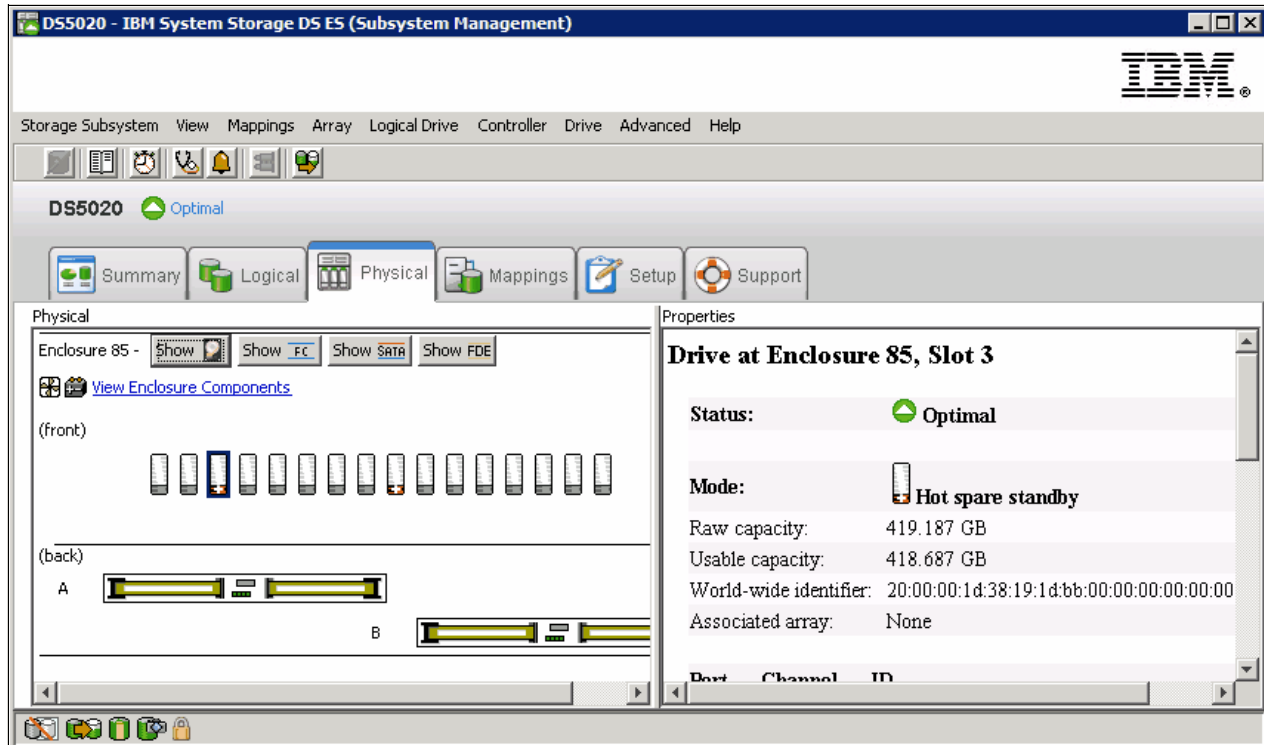


Figure 3-50 Automatic hot spare creation

This automatic hot spare creation function created one hot spare drive for every 30 disk drives of the same type (FDE/FC/SATA).

Manual assignment

To perform manual hot spare assignment, follow these steps:

1. To manually define a hot spare drive, select, from the Setup view, **Configure Storage Subsystem** → **Configure hot spare drives** → **View/change current hot spare coverage**.

You can also select, from the Physical view, the specific non-assigned drive you want to set up as a hot spare, right-click it, and select **Hot Spare Coverage**, or, from the top menu, select **Drive** → **Hot Spare Coverage**, as shown in Figure 3-51.

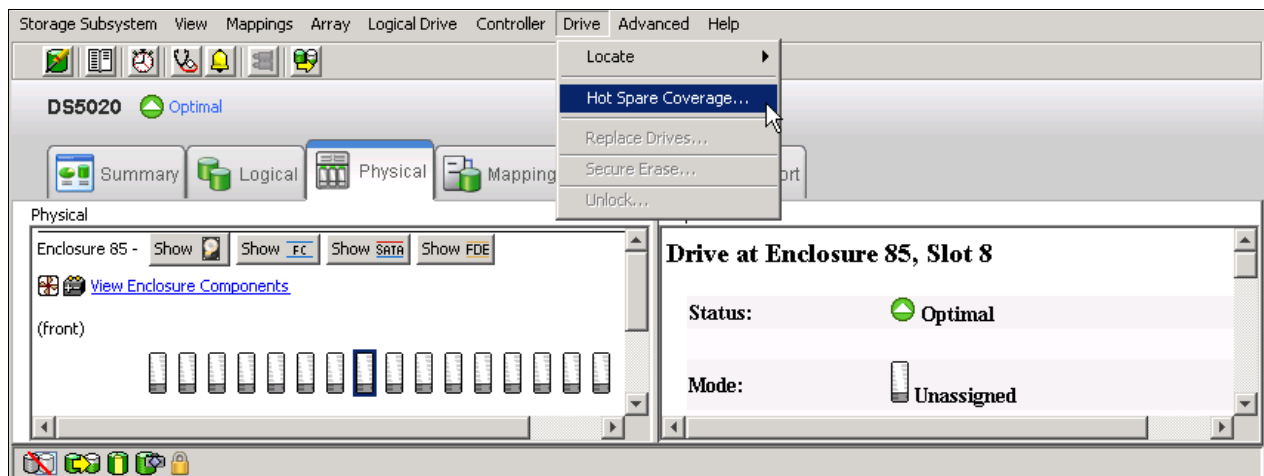


Figure 3-51 Hot Spare Coverage

2. This opens the Hot Spare Drive Options window, as shown in Figure 3-49, but this time with the option **Manually assign individual drives** selected by default. Click **OK** and the unassigned drive is defined as a hot spare.

If any array on the DS5000 storage subsystem contains larger drives than the drive you have chosen, a warning message appears notifying you that not all arrays are protected by the hot spare drive.

Remember to create hot spares for each type of disk drive. Use the push buttons in the Physical view to show each type of drives, as shown in Figure 3-52.

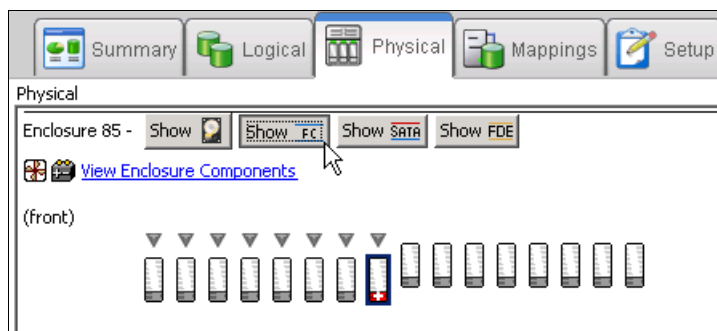


Figure 3-52 FC drives protected with hot spare

3. Because in this example we have more than one type, we repeat the previous steps to create a second hot spare drive for the SATA disk drives, which are still unprotected. The operation finishes and the window shown in Figure 3-53, in the physical view, opens. Click the **Show SATA** button.

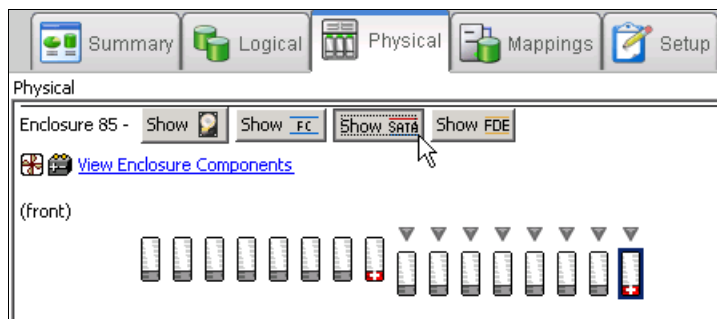


Figure 3-53 SATA drives protected with hot spare

4. To unassign a hot spare drive and have it available again as a free drive, highlight it, select **Drive → Hot Spare Coverage**, and then select **Manually unassign individual drives**.

View/change hot spare coverage

After you have configured your spare drives, you can review or modify your settings using this option. Perform the following actions:

1. To start the option from the Storage Manager Client, select **Drive → Hot Spare Coverage**.

- The Hot Spare Drive Options window opens, as shown earlier in Figure 3-49. Select **View/Change current hot spare coverage** and click **OK**. This opens the window shown in Figure 3-54.

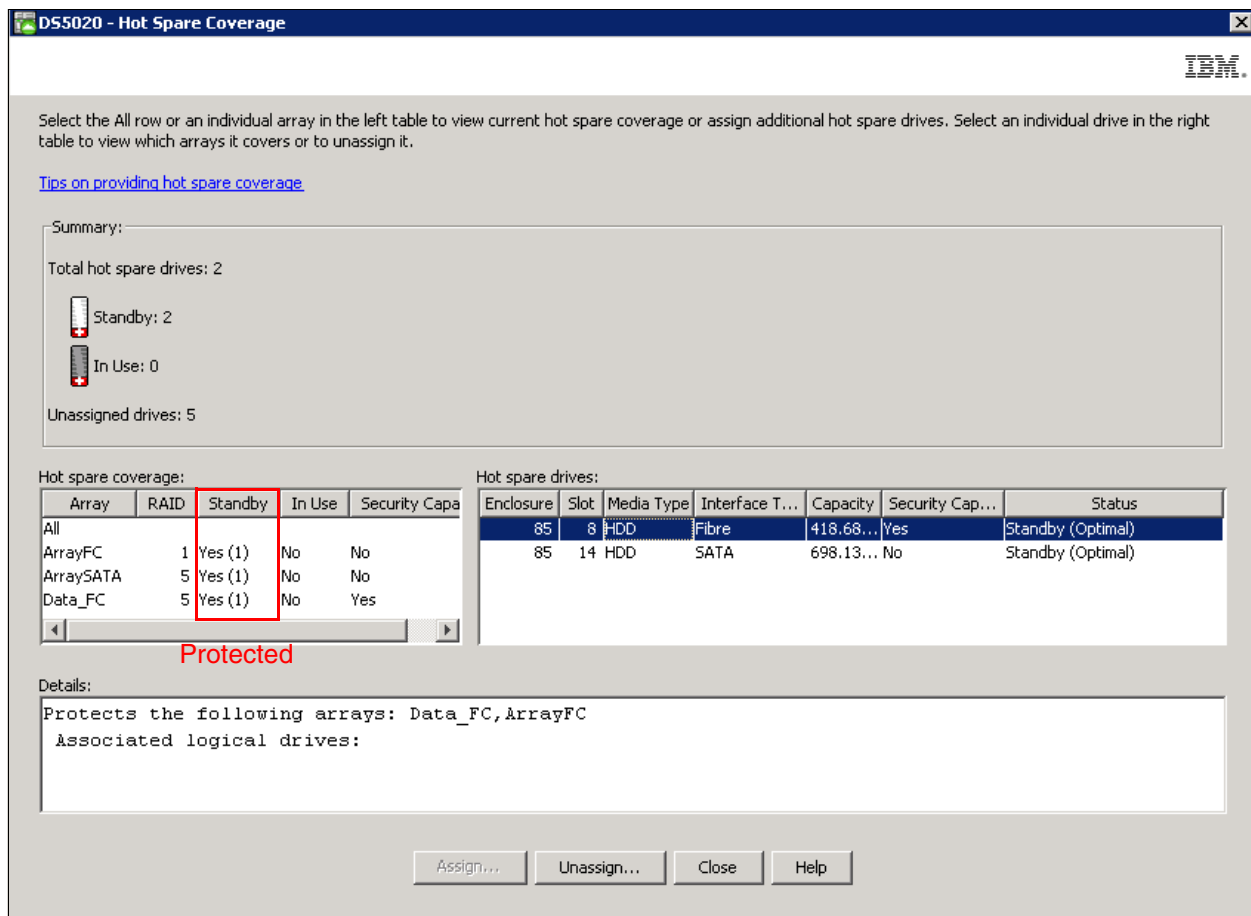


Figure 3-54 View/Change hot spare coverage

Make sure to use this window to check that all your arrays are protected. If they are not protected, implement complete hot spare protection for all the arrays, as shown in Figure 3-55.

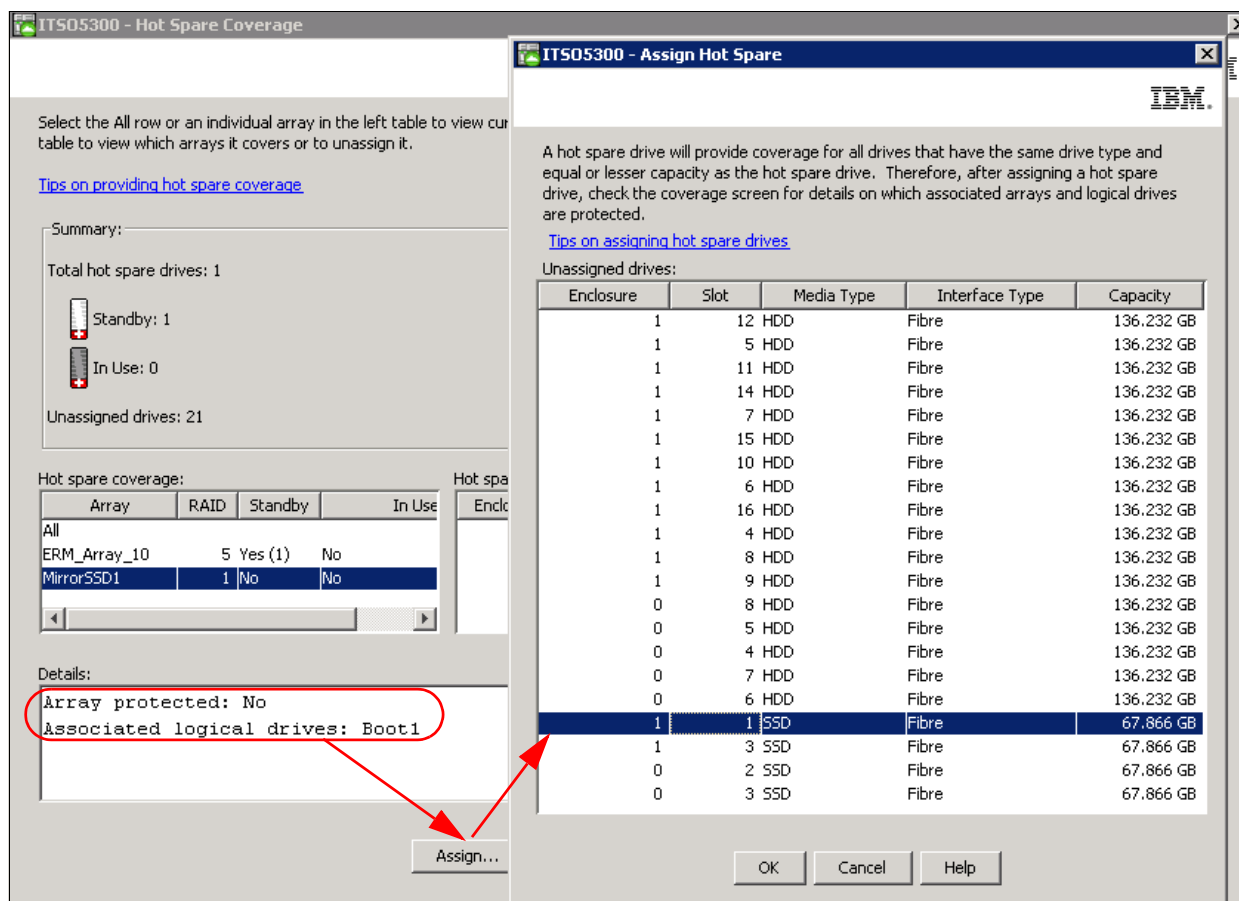


Figure 3-55 Assigning hot spare protection for an array

Notice in this example that there is only one spare drive assigned, but because there are arrays defined with different types of disk, Array MirrorSSD1 is not protected by a hot spare drive. You can run into this situation if the arrays are created before assigning hot spare drives, or by adding drives of a different type after the storage is defined. We can assign an additional hot spare drive using this interface to solve this issue

3. To resolve this exposure, click the **Assign** option button. The Assign Hot Spare window opens, as shown in Figure 3-55.
4. It is clear that there are different disks in the storage subsystem, both hard disk drives (HDDs) and Solid State Drives (SSDs). Select a disk of the same type as the ones in the unprotected array (SSD in this case), and click **OK** to assign it. Remember to select a drive type of equal or greater capacity than the disks to protect.
5. Finally, review the results window, checking that all arrays are protected, and click **Close**.

3.5.4 Creating arrays and logical drives

At this stage of the process, the storage subsystem is installed, upgraded to the newest microcode level, and at least one hot spare drive is defined for each drive type. Arrays and logical drives can now be configured.

You can define logical drives from unconfigured capacity or from free capacity already available in previously defined arrays on the storage subsystem:

- ▶ When you create a logical drive from unconfigured capacity, you create an array by first choosing the RAID type, and so on, and then the needed logical drives.
- ▶ If an array is not created, you can still create a logical drive, but the Storage Manager will direct you to create the array first.
- ▶ If there is free capacity on a previously defined array, you can create additional logical drives using that free capacity.

The example that follows assumes that there is unconfigured capacity on the DS5000 storage subsystem. Note that the unconfigured capacity for Fibre Channel and SATA disks are grouped separately. This procedure illustrates the most common steps to follow in setting up a logical drive from unconfigured drives:

1. In the Subsystem Management window (Figure 3-56), right-click the unconfigured capacity for the selected drive type. Because we have selected unconfigured capacity, we first create an array option. Choosing **Create Logical Drive** causes a window to open that requests that you create the array first. Select **Create Array**.

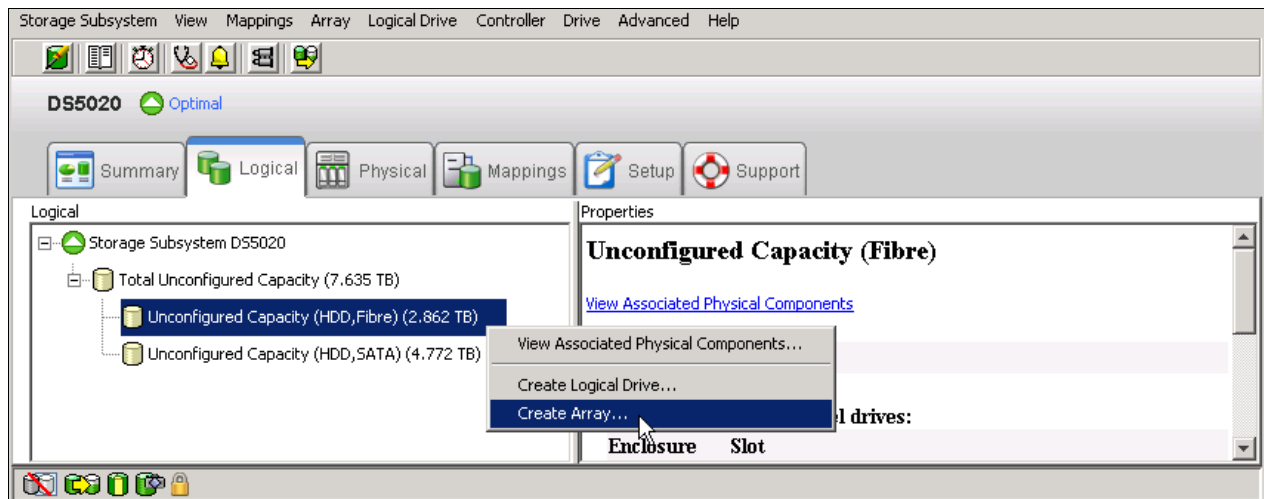


Figure 3-56 Create logical drive from unconfigured capacity

This action starts the wizard for creating the array first and then the logical drives. The first window of the wizard is an introduction to the process. It displays the available unconfigured capacity for the type of disks selected. Read the introduction and then click **Next** in order to proceed.

2. In the Create Array window, type a meaningful array name that describes your set of disks, and then select either Automatic mode or Manual mode. Automatic mode is the default option, as shown in Figure 3-57. By selecting the Automatic option, the Storage Manager software selects a combination of available drives to optimize performance and availability, and attempts to select physical drives from different enclosures in order to provide enclosure protection whenever possible. Click **Next**.

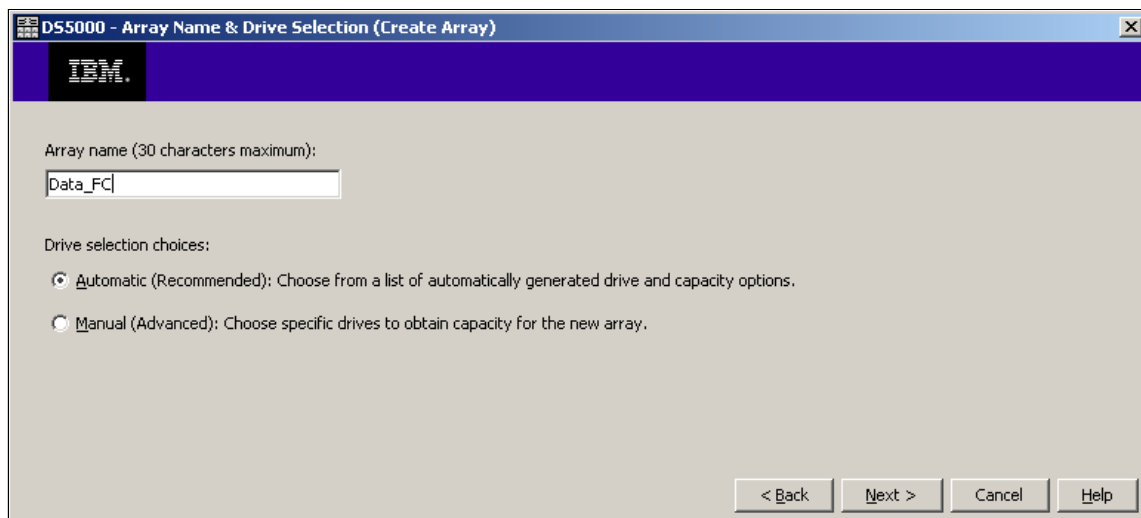


Figure 3-57 Create array and assign a name and mode

The automatic creation of the array selects the drives in the following order:

- Same capacity-same speed enclosure redundancy
- Same capacity-mixed speed enclosure redundancy
- Same capacity-mixed speed no enclosure redundancy
- Mixed capacity-same or mixed speed-no enclosure redundancy

In manual mode, you have to select all the drives individually. Make sure that you select them to maximize performance and availability.

3. Click **Next** in order to select the RAID level.
 - Select the desired RAID level. The window now displays the different capacity options depending on the unconfigured drives available in your configuration. If you have different disk sizes, you have more than one option for the same number of disks. Refer to the planning tasks section of *IBM System Storage DS5000 Series Implementation and Best Practices Guide*, SG24-8024 to determine the best RAID level for your specific environment and application.
 - Select the total capacity required and click **Finish**.

In our example (Figure 3-58), we created a RAID 0 array with three drives.

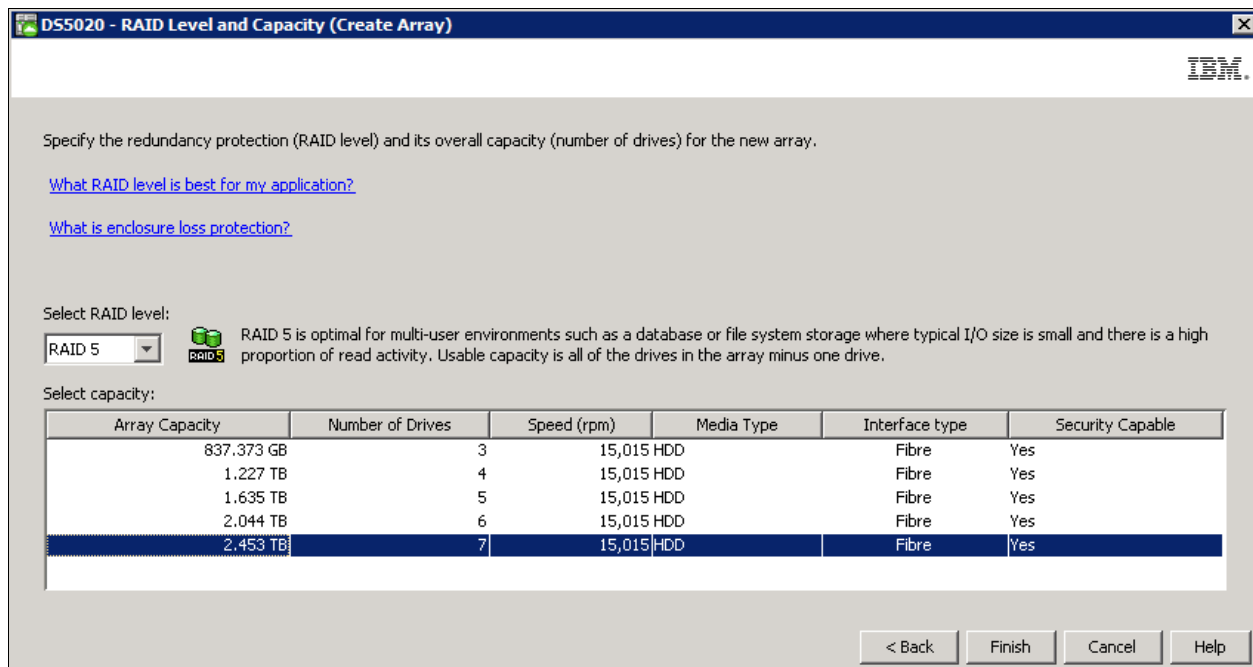
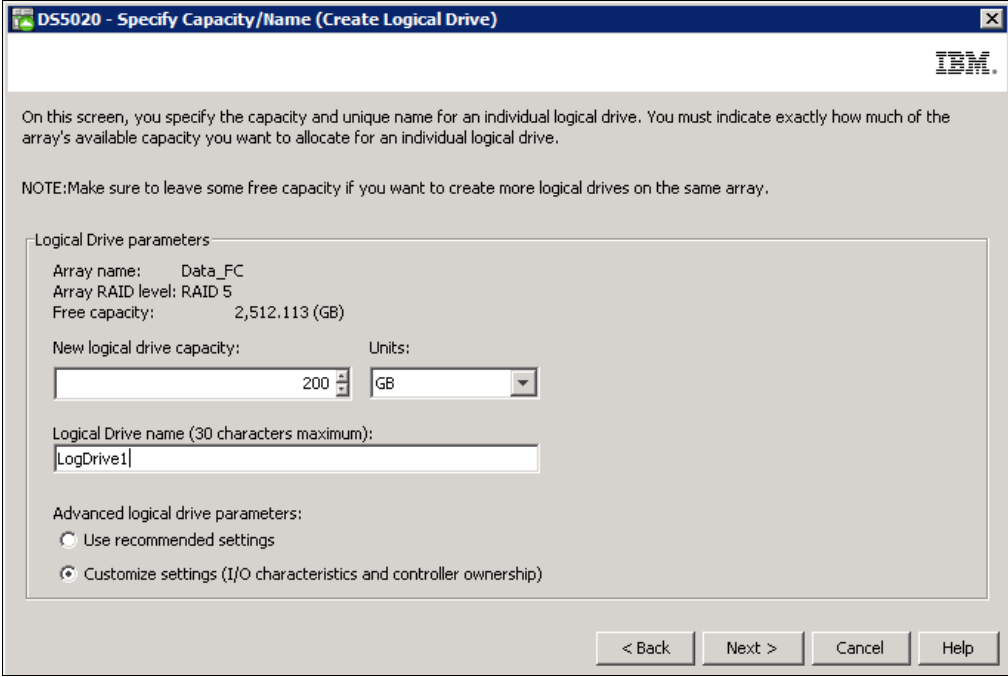


Figure 3-58 RAID level and capacity

4. The Array Success dialog box appears and confirms that the array is now created. Click **Yes** to continue with the creation of a logical drive.
5. In the Create Logical Drive wizard window, click **Next** to start configuring the logical drive.
6. In the Specify Capacity/Name dialog window:
 - a. If you want to define more than one logical drive in the array, enter the desired size capacity below the limit of the array capacity.
 - b. Assign a name to the logical drive.
 - c. If you want to change advanced logical drive settings, such as the segment size or cache settings, select the **Customize settings** option and click **Next**.

Note: The recommended settings values for creating volumes (Figure 3-59) are dynamic cache read prefetch enabled for all RAID types, and the segment size 128 KB for all but RAID 3, which is set to 256 KB.



DS5020 - Specify Capacity/Name (Create Logical Drive)

On this screen, you specify the capacity and unique name for an individual logical drive. You must indicate exactly how much of the array's available capacity you want to allocate for an individual logical drive.

NOTE: Make sure to leave some free capacity if you want to create more logical drives on the same array.

Logical Drive parameters

Array name: Data_FC
 Array RAID level: RAID 5
 Free capacity: 2,512.113 (GB)

New logical drive capacity: Units:

Logical Drive name (30 characters maximum):

Advanced logical drive parameters:

☐ Use recommended settings
☒ Customize settings (I/O characteristics and controller ownership)

< Back Next > Cancel Help

Figure 3-59 Specifying logical drive capacity

7. The Customize Advanced Logical Drive Parameters window opens (Figure 3-60). You can set your new logical drive using any of the predefined I/O types listed, or manually set the cache read ahead multiplier, segment size, and controller ownership.
 - a. For logical drive I/O characteristics, you can specify file system, database, or multimedia defaults. The Custom option allows you to disable or enable the dynamic cache read prefetch and the segment size. Table 3-1 shows the defaults predefined for each I/O type.

Table 3-1 Logical drive defaults I/O characteristics

I/O type	File system	Database	Multimedia
Segment size	128 K	128 K	256 K
Modification priority	High	High	High
Read cache	Enable	Enable	Enable
Write cache	Enable	Enable	Enable
Write cache without batteries	Disable	Disable	Disable
Write cache with mirroring	Enable	Enable	Enable
Flush write cache after	10 seconds	10 seconds	10 seconds
Dynamic cache prefetch	Enable	Enabled	Enable
Enable background media scan	Enable	Enable	Enable
Media scan with redundancy check	Disable	Disable	Disable

I/O type	File system	Database	Multimedia
Pre-read redundancy check	Disabled	Disabled	Disabled

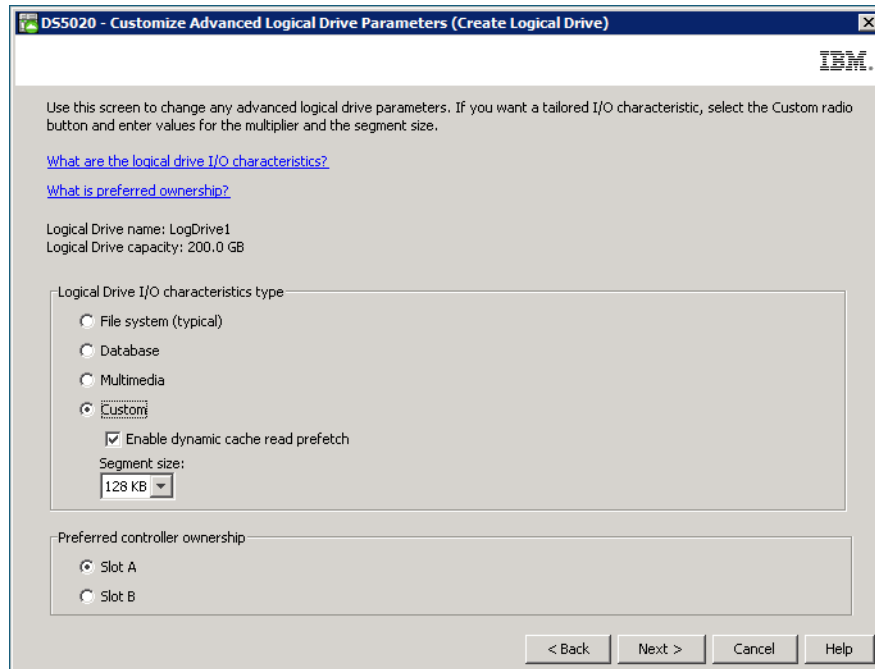


Figure 3-60 Customize logical drive parameters

- b. The segment size is chosen according to the usage pattern. For custom settings, you can directly define the segment size.
- c. Dynamic cache read prefetch is important for multimedia applications that use sequential I/O, by allowing the controller, while it is reading and copying host-requested data blocks from disk, to copy additional data blocks into the cache.
- d. The preferred controller handles the logical drive normally if both controllers and I/O paths are online. You can distribute your logical drives between both controllers to provide better load balancing between them. The default is to alternate the logical drives on the two controllers.

It is better to spread the logical drives by the load that they cause on the controller. If you do not know the expected access pattern for each logical drive, you can evaluate it by using the performance monitor option integrated with the Storage Manager client. Based on data gathered from the Performance Monitor, move some logical drives to the other preferred controller to balance the load if required (see 3.5.7, “Monitoring and alerting” on page 202, and 3.6.6, “Controller ownership” on page 226 for more information).

8. The Specify Logical Drive-to-LUN Mapping window opens (Figure 3-61). This window allows you to choose between mapping your created logical drive to the default group or to “Map later using the Mappings View.” If you choose the Default mapping, then the physical volume is mapped to the default host group and is available to any host zoned to the DS5000 storage subsystem, so it is not the recommended choice if your DS5000 storage subsystem supports more than a single partition.

Important: Manually mapping logical drives to hosts prevents unwanted mapping and is always the recommended choice.

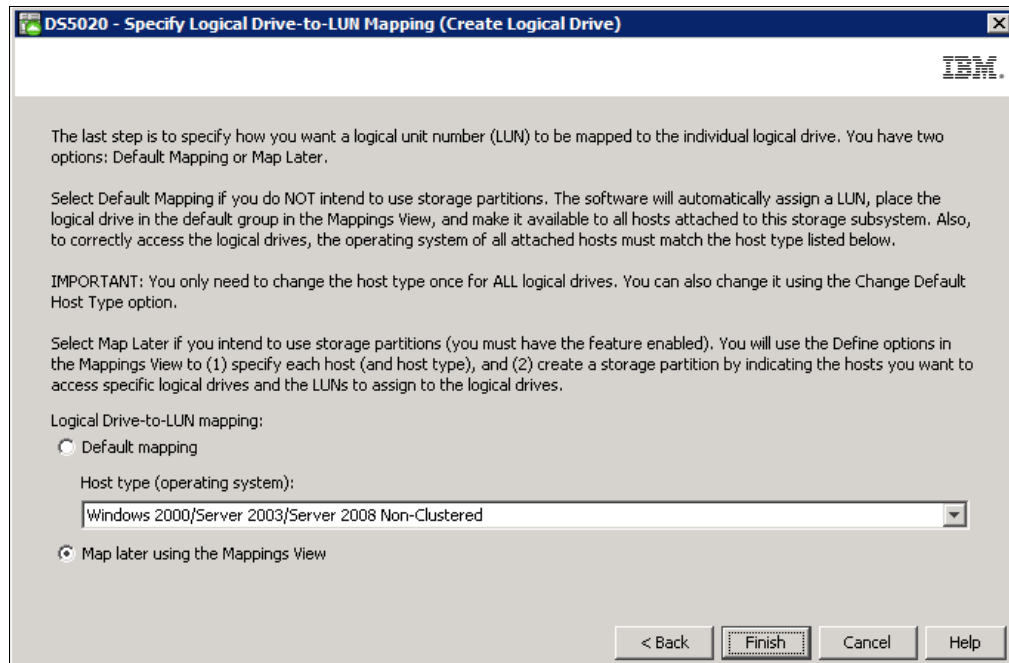


Figure 3-61 Logical drive mapping

9. Click **Finish** and the Creation Successful window opens. You are prompted about whether you want to create another logical drive. Click **No** if you have finished creating logical drives or want to finish at a later time.
10. The Completed window opens. The Mapping section presents the logical volume to a desired host. Click **OK** to finish.
11. Repeat the same process for creating other arrays and logical drives.

If you left unconfigured capacity inside the array, you can later define another logical drive in this array. Simply highlight this capacity, right-click, and choose **Create Logical Drive**. Follow the steps that we previously outlined in this section, except for the selection of drives and RAID level (because the array is already defined).

Displaying arrays and logical drives

After creating the arrays and logical drives, the Logical view of the Subsystem Management window shows the status of the current configuration for arrays and logical drives, as shown in Figure 3-62.

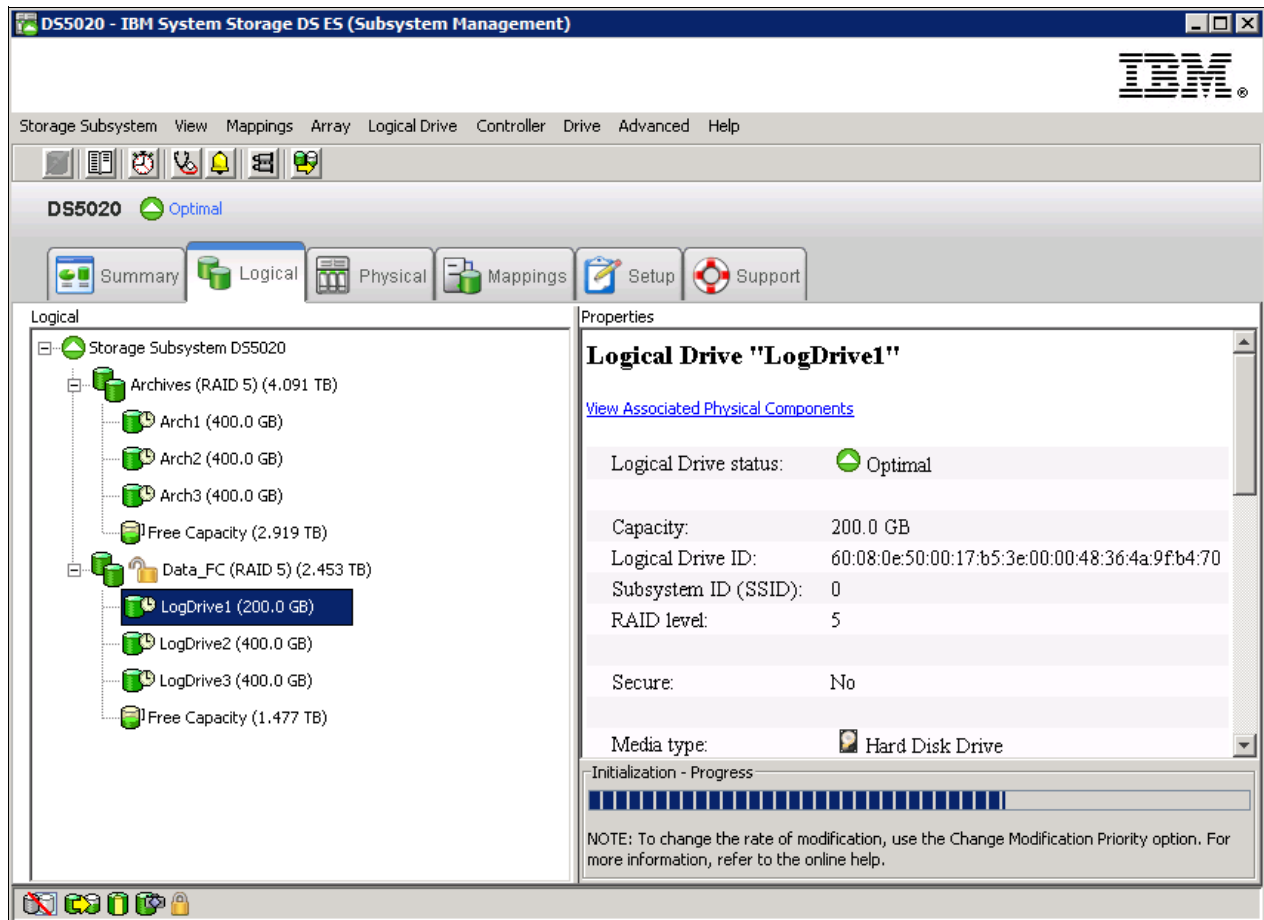


Figure 3-62 Logical Drive initialization progress

Notice that after creating a logical drive that the disk space is initialized, and shows a clock icon to the right of its name. The right frame shows the properties for the selected logical drive or array, with details about the initialization's progress in the lower part of the window. Be aware that even during the initialization process, the logical drive is immediately available for access if mapped.

To attach the arrays or logical drives to the physical disks, right-click one of them and select **View associated physical components**. The window that opens shows a blue dot under each physical disk where the array or logical drive selected belongs, as shown in Figure 3-63.

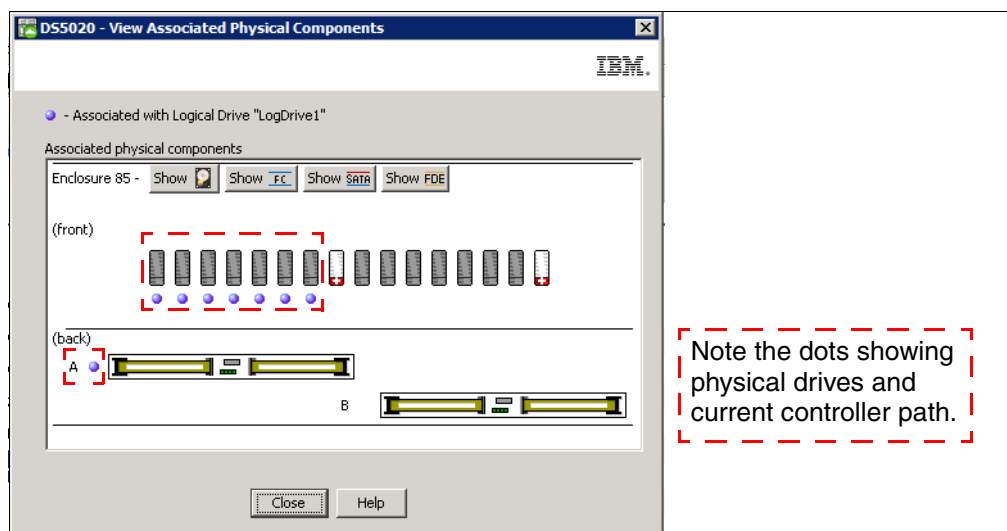


Figure 3-63 Logical/Physical relationship

The current path of the logical drive is represented by the blue dot at the right side of the controller. In this case, the logical drive named LogDrive1 is using controller A.

You can also use the Physical view of the Subsystem window and click one disk at a time to display that disk's related array, as shown in Figure 3-64.

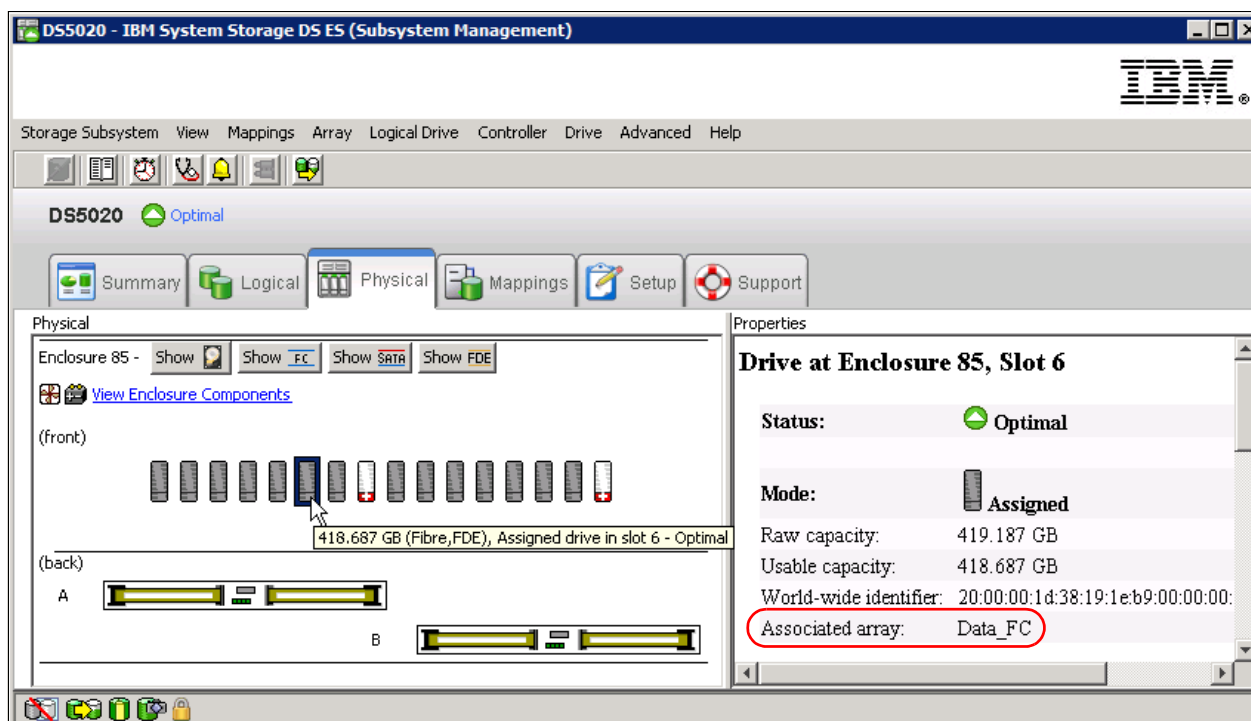


Figure 3-64 Physical/Logical relationship

3.5.5 Configuring storage partitioning

We explain the concept of storage partitioning in 3.5.5, “Configuring storage partitioning” on page 181. Here we show an example of configuring partitions for a FC host. If you need a specific procedure for iSCSI attachment, see *IBM System Storage DS5000 Series Implementation and Best Practices Guide*, SG24-8024.

Because heterogeneous hosts can be attached to the DS5000 storage subsystem, you need to configure storage partitioning for two reasons:

- ▶ Each host operating system requires slightly different settings on the DS5000 storage subsystem. You need to tell the storage subsystem the host type to which it is attached.
- ▶ There is interference between the hosts if every host has access to every logical drive. By using storage partitioning and LUN masking, you ensure that each host or host group only has access to its assigned logical drives. You can have up to 256 LUNs assigned to a single storage partition. You might have a maximum of 2048 LUNs configured per DS5000 storage subsystem.

The overall process of defining the storage partitions is as follows:

1. Define host groups.
2. Define hosts.
3. Define host ports for each host.
4. Define storage partitions by assigning logical drives to the hosts or host groups.

The Subsystem Management has an specific view called *Mappings*. From this view, you can display the current status, create your hosts and hosts groups, and map the logical drives to them.

Selecting the **Mappings** view, if you have not defined any storage partitions, opens the Mapping Start-Up Help window (shown in Figure 3-65). The information in the window advises you to only create host groups if your plan includes sharing logical volumes across different hosts, normally a cluster.

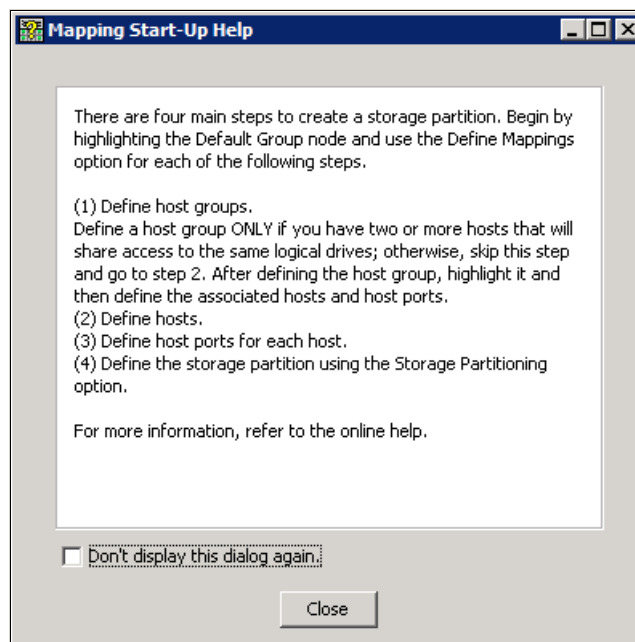


Figure 3-65 Mappings Start-Up Help

The Setup view has the option Map Logical Drives, which you can use for mapping your logical drives to the Default group, or to previously defined hosts or groups.

Figure 3-66 shows an example of the Mappings view. The right side of the window lists all mappings that are owned by the object you select on the left side. If you highlight the storage subsystem, you see a list of all defined mappings. If you highlight a specific host group or host, its mappings are listed.

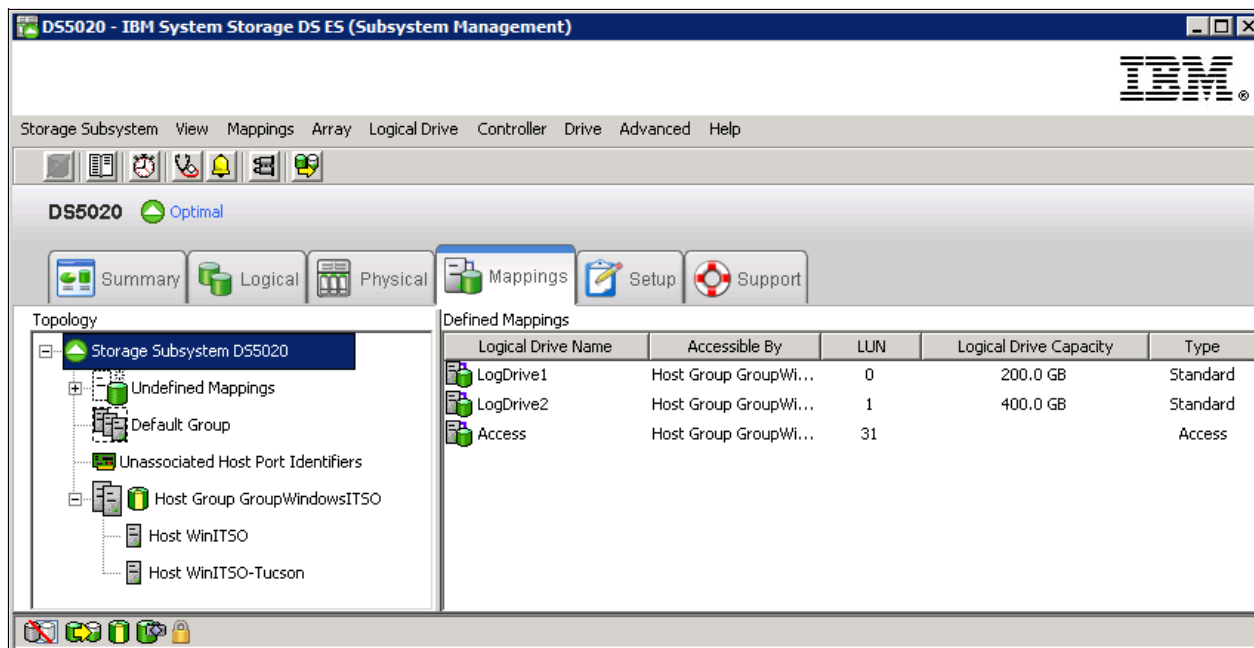


Figure 3-66 Mappings view in Subsystem Management window

In our example, we show how to configure the following storage partitioning scenario:

- ▶ We have a host with Windows Server 2008. We want that host to have access to the logical drives LogDrive1 and LogDrive2 of the storage subsystem.
- ▶ This host contains two FC HBAs.
- ▶ At some time, the host becomes a part of the Windows 2008 cluster, so we have to put it into a host group. The host group name will be WinGroupITSO.
- ▶ We map the two logical drives (LogDrive1 and LogDrive2) to that host group.
- ▶ We show how to modify the mapping to integrate it later into a cluster.

Note: Before configuring the partitions, if you have your storage connected to a FC switch, make sure to first define the zones appropriately.

Next, perform a hardware rescan on each host that is to be mapped to the DS5000 storage subsystem to reconfigure the FC devices and allow the WWN to be presented in the Storage Manager.

It is a best practice to configure only one host HBA per zone, together with one DS5000 storage subsystem controller.

Defining hosts

Perform the following steps:

1. Right-click your storage subsystem and select **Define** → **Host**, as shown in Figure 3-67. Even with no host group created, it is easier to create the hosts first and then the host groups.

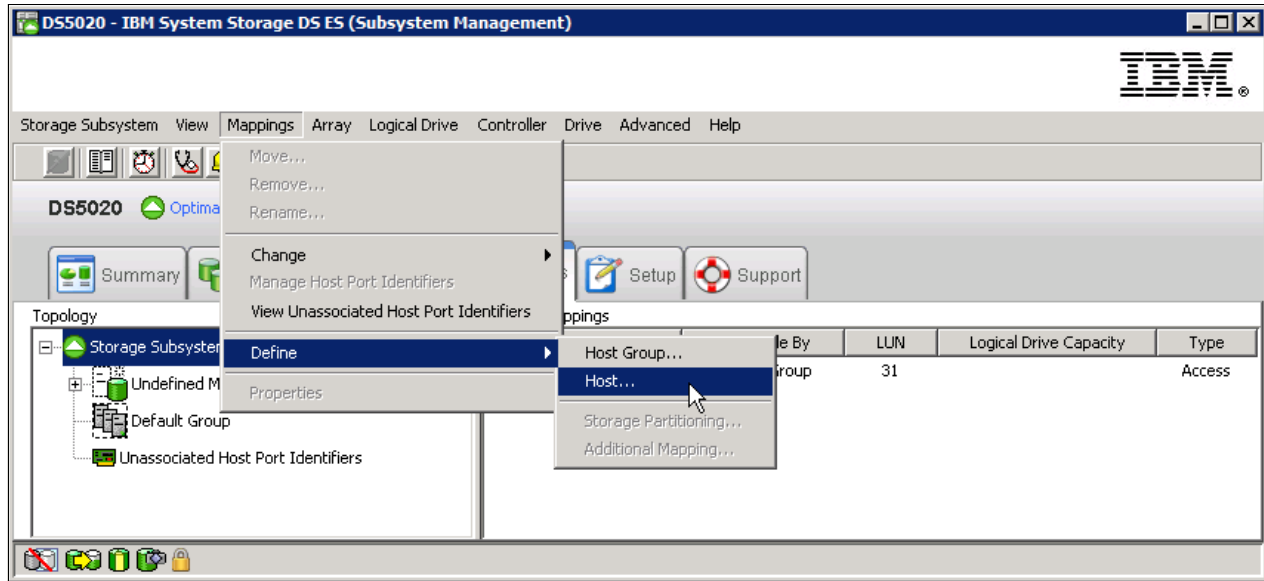


Figure 3-67 Selecting Define Host

This launches the wizard for defining a new host. You have to provide the following information during the process:

- Name of the new host.
- Protocol attachment method:
 - FC
 - iSCSI
- Host port identifiers with their Alias or Labels.
- Host type (the operating system that runs on the host).
- Whether the host is going to participate in a cluster.
- Host Group name if the host is defined as clustered.

- The first window of the wizard is an introduction (Figure 3-68). You are asked to assign a name to the host being defined, and whether you plan to use storage partitioning.

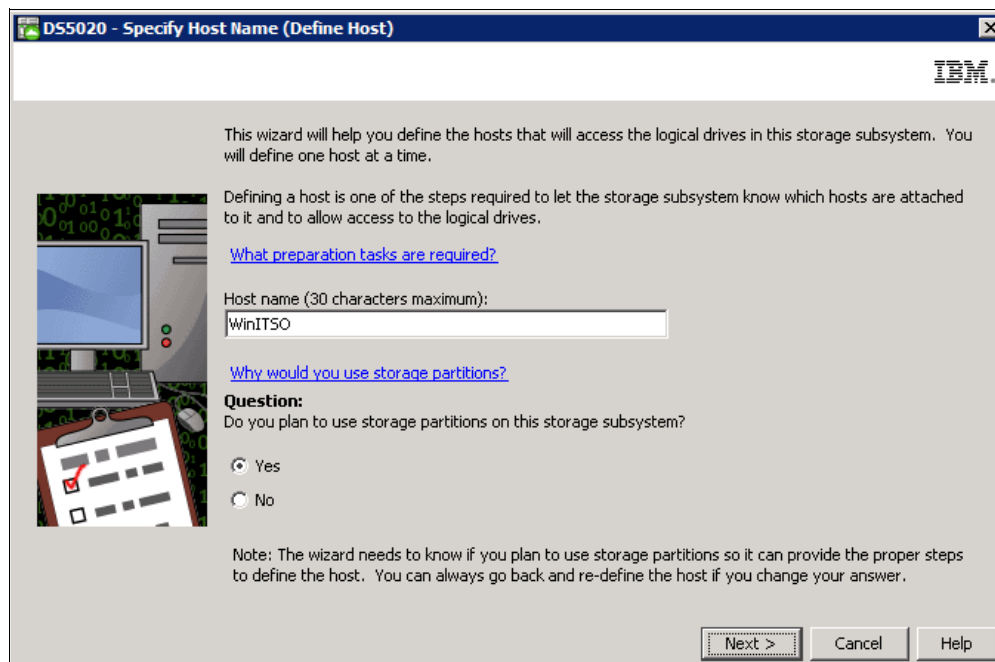


Figure 3-68 Define Host wizard

- If you only plan to attach a single host server, then you do not need storage partitioning. But if you plan group different host environments together, or if clusters sharing logical drives is recommended, click **Yes** to create different hosts groups at a later time.
- In the next window, you need the attachment protocol to specify the host interface type, FC or iSCSI, and the HBA host port information (host port identifier and alias). Remember that the HBA host port identifier is the world-wide port name of the particular HBA. To make sure that you know what your server's HBA WWPN is, use the SANsurfer management tool (which is discussed in 5.12.3, "Qlogic HBAs and SANsurfer (Windows/Linux)" on page 426) as shown in Figure 3-69.

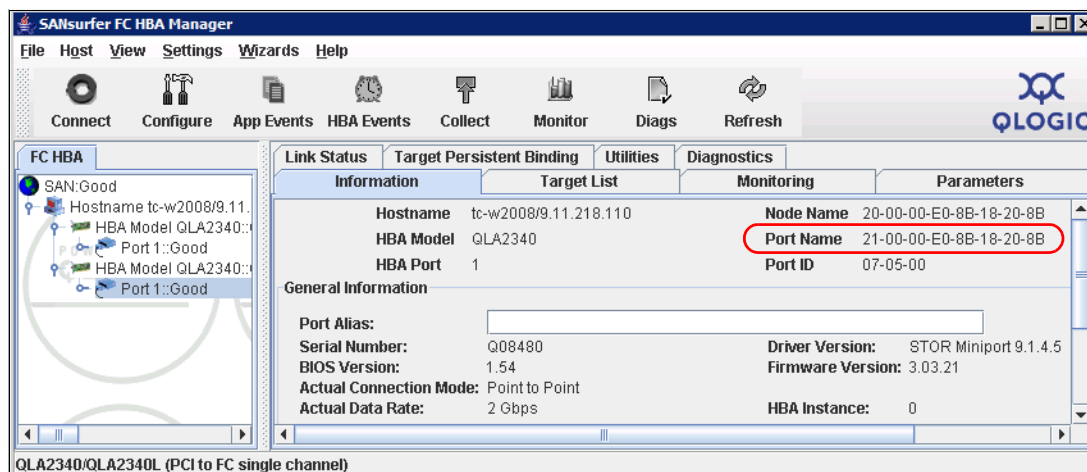


Figure 3-69 Displaying WWPN with SANsurfer

Note: The *IBM QLogic SANsurfer User's Guide* and the QLogic SANsurfer program are located on the IBM DS Storage Manager CD.

5. Enter the data from Step 4 on page 184 into the window shown in Figure 3-70.

The host communicates with the storage subsystem through its host bus adapters (HBAs) or its iSCSI initiators where each physical port has a unique host port identifier. In this step, select or create an identifier, give it an alias or user label, then add it to the list to be associated with host WinITSO.

[How do I match a host port identifier to a host?](#)

Choose a host interface type:
 FC

Choose a method for adding a host port identifier to a host:

☒ Add by selecting a known unassociated host port identifier

Known unassociated host port identifier:
 21:00:00:e0:8b:89:2c:c0 Refresh

☐ Add by creating a new host port identifier

New host port identifier (16 characters required):

Alias (30 characters maximum):

Add ? Remove ?

Host port identifiers to be associated with the host:

Host Port Identifier	Alias / User Label
21:00:00:e0:8b:18:20:8b	HBA-1
21:00:00:e0:8b:89:2c:c0	HBA-2

< Back Next > Cancel Help

Figure 3-70 Define Host: Specifying the host name and HBA

- Select your interface type (FC in our example) and an active port already detected by the DS subsystem, or type its world-wide port name directly into the field.
 - Type an alias for the specified host port identifier and click **Add**.
 - Repeat the same process until you define all the HBAs. Remember that if you define only one HBA, the host can lose access if there is a problem. Click **Next** after defining all the HBAs.
6. The next window requires you to specify the host type. This is basically the operating system running on the host. It is vital that you select the appropriate host type because the RDAC and ADT settings rely on this setting. In addition, this is the part of the configuration where you configure the heterogeneous host support. Each operating system expects slightly different settings and handles SCSI commands differently. If you make a wrong choice, your operating system might not boot anymore or path failover cannot be used.

We show an example of this window in Figure 3-71. In our particular case, we selected **Windows 2000/Server 2003/Server 2008 Non-Clustered**.

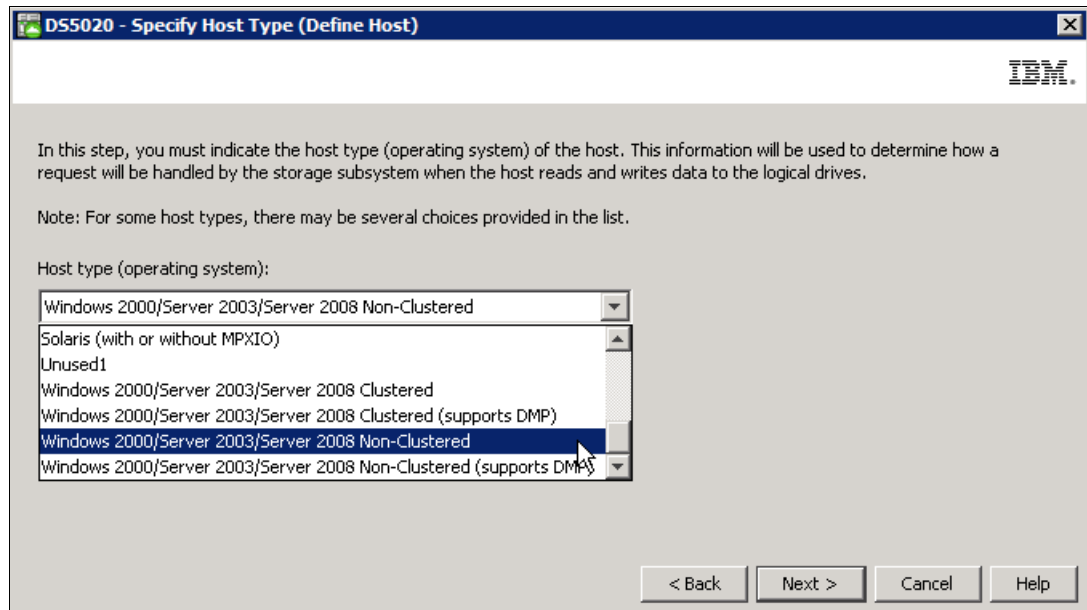


Figure 3-71 Define Host: Specifying the host type

7. In the next step, you are asked whether the host is a part of a cluster. Click **Yes** or **No**, depending your configuration, and **Next** to continue.

8. If the answer is **Yes**, as in our example, then you need to specify a host group. The host group can be either a new or an existing one, as shown in Figure 3-72.

DS5020 - Specify Host Group (Define Host)

[What is a host group?](#)

Because you specified on the previous screen that the host you are defining will share access to logical drives with one or more other hosts, you must indicate the name of the host group that this host will be associated with.

You can either (1) manually enter a new host group name or (2) select an existing host group. If you select an existing one, you will be shown the hosts currently associated with it.

☒ Enter name (30 characters maximum)

GroupWindowsITSO

☐ Select existing host group

-Select from list-

Associated hosts in host group:

Name	Host Type
------	-----------

< Back Next > Cancel Help

Figure 3-72 Define Host: Specifying a host group

9. Finally, you have the chance to preview the new host definition (Figure 3-73). If all the selections are correct, click **Finish** to define the new host.

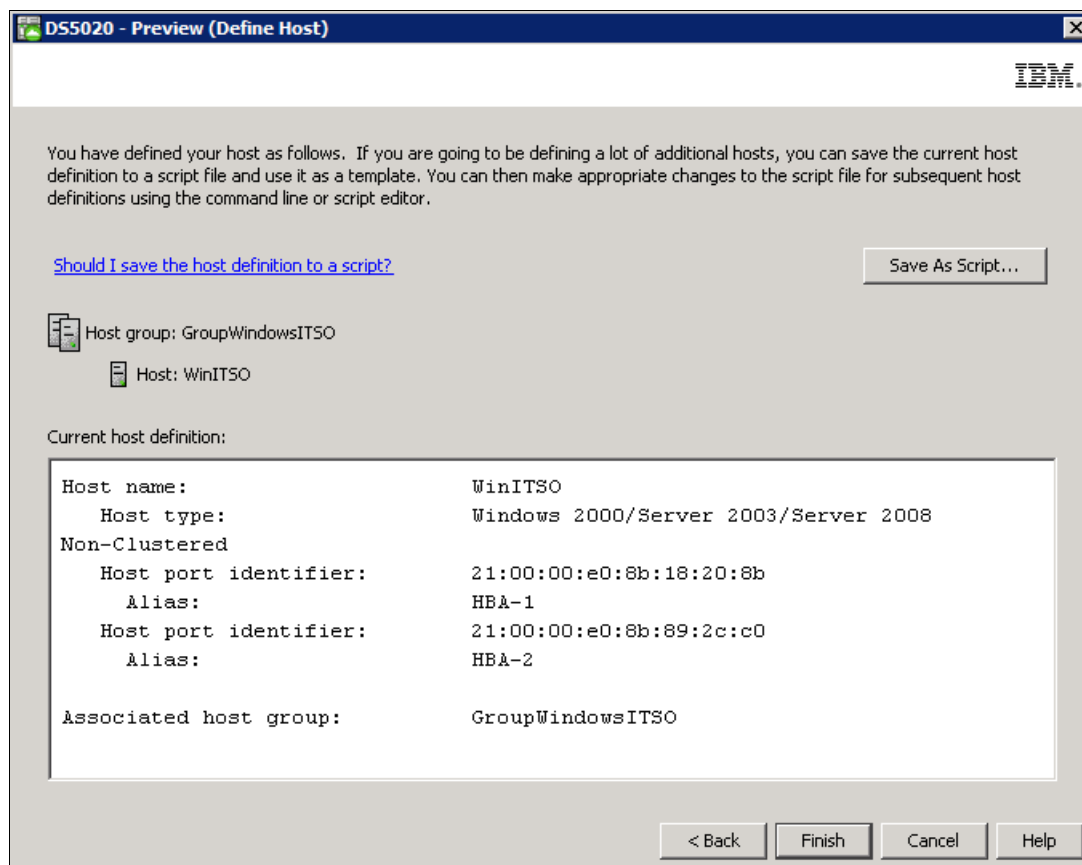


Figure 3-73 Define Host: Preview

10. Repeat the same steps to create more hosts and host groups. Once finished, the new host (and the host group, if it was also defined) is placed in the default group. It will stay there until you actually create a storage partition by assigning the logical drives to that host (or group). Figure 3-74 shows an example.

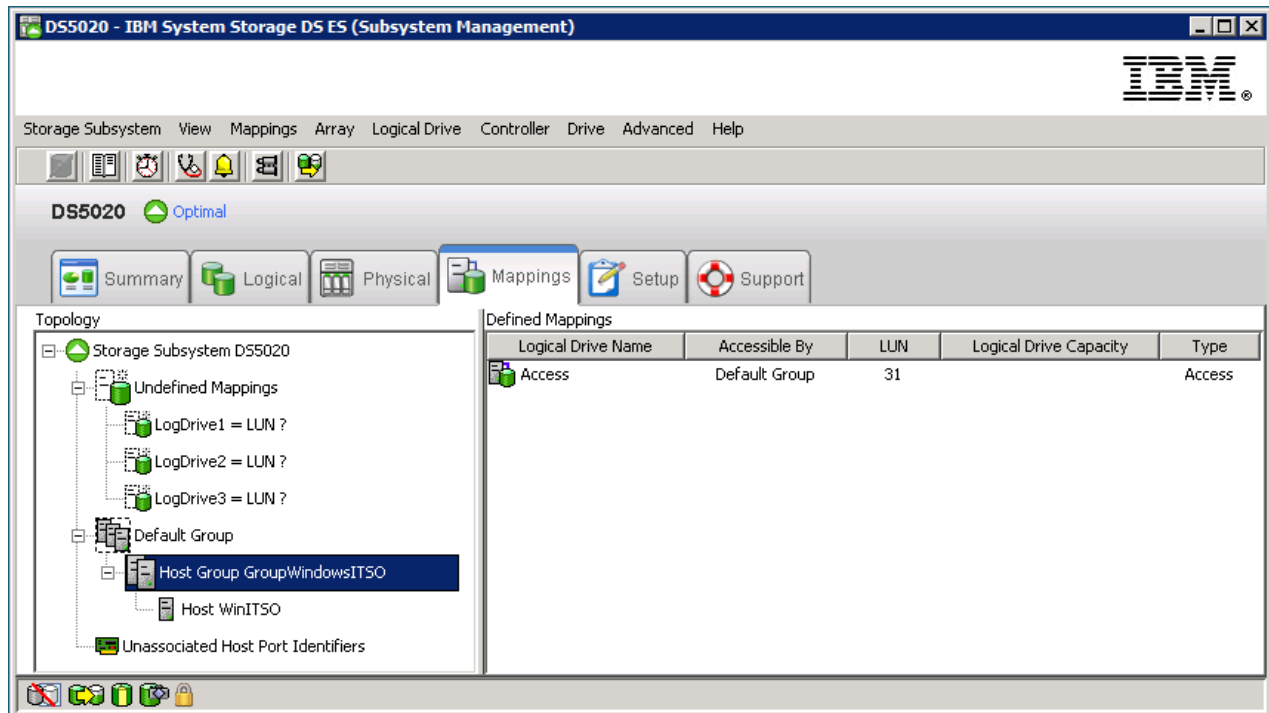


Figure 3-74 New host and host group placed in the default group

Defining storage partitioning

Next, we define storage partitioning:

1. We start by creating a storage partition by assigning the logical drives to the hosts or host groups. The Storage Partitioning wizard leads you through the process, and you initiate it by right-clicking **Default Group** and selecting **Define** → **Storage Partitioning**. We show an example in Figure 3-75.

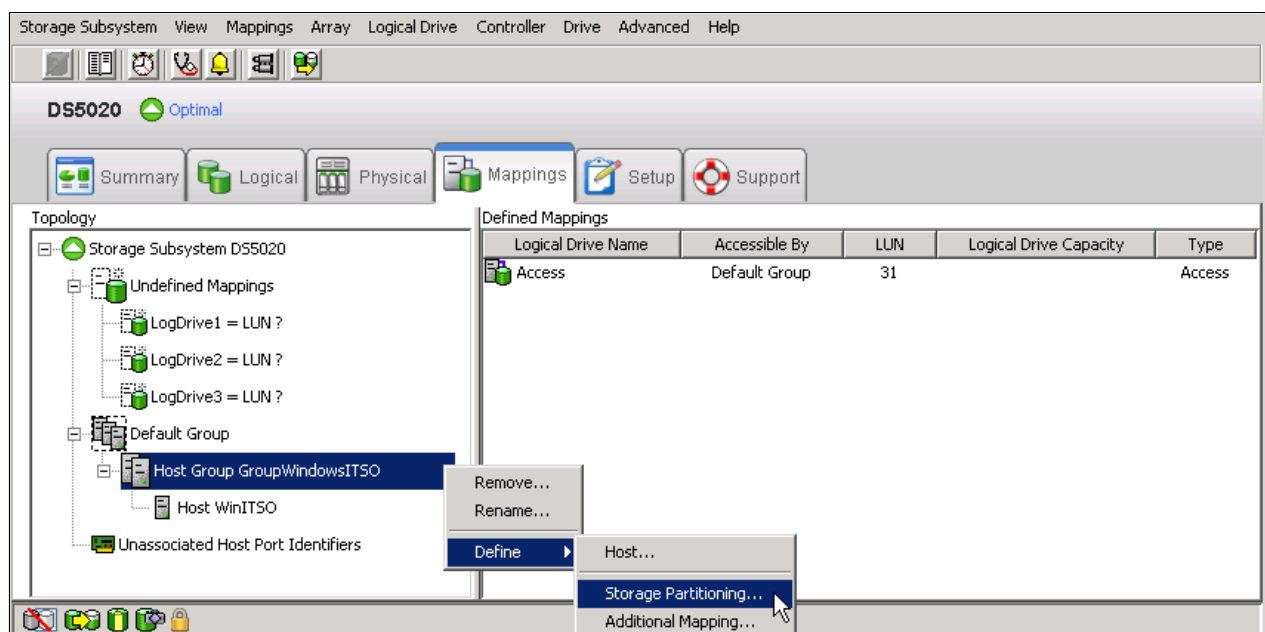


Figure 3-75 Define storage partitioning

2. After the introductory window, the wizard asks you to select either a host or a group of hosts. If you are creating a storage partition for clustered host servers, you need to specify the appropriate group; otherwise, you can select an individual host.
3. The next window allows you to select the logical drives that are going to be mapped to the host or the group. You also have to specify a LUN for each logical drive. In our example, shown in Figure 3-76, we selected LogDrive1 and LogDrive2. We assigned the LUNs 0 and 1, respectively, to these two logical drives.

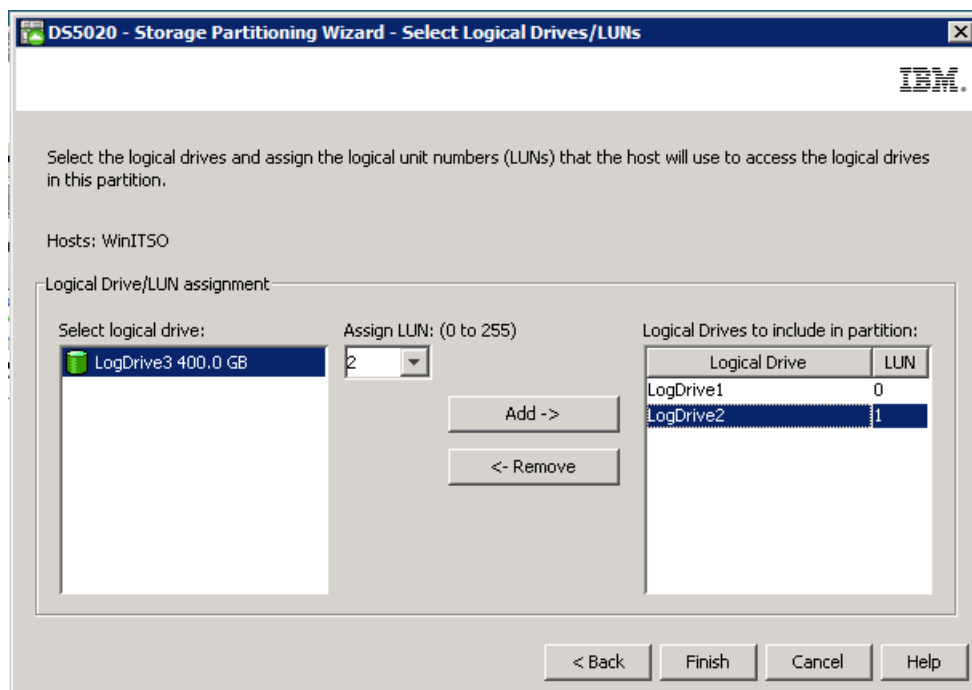


Figure 3-76 Storage Partitioning wizard: Selecting logical drives/LUNs

4. Click **Finish** when you are done with selecting the logical drives and assigning the LUNs.
5. Display your newly defined host groups, host, and mappings by selecting the **Mappings** view in the Subsystem management windows, as shown in Figure 3-77.

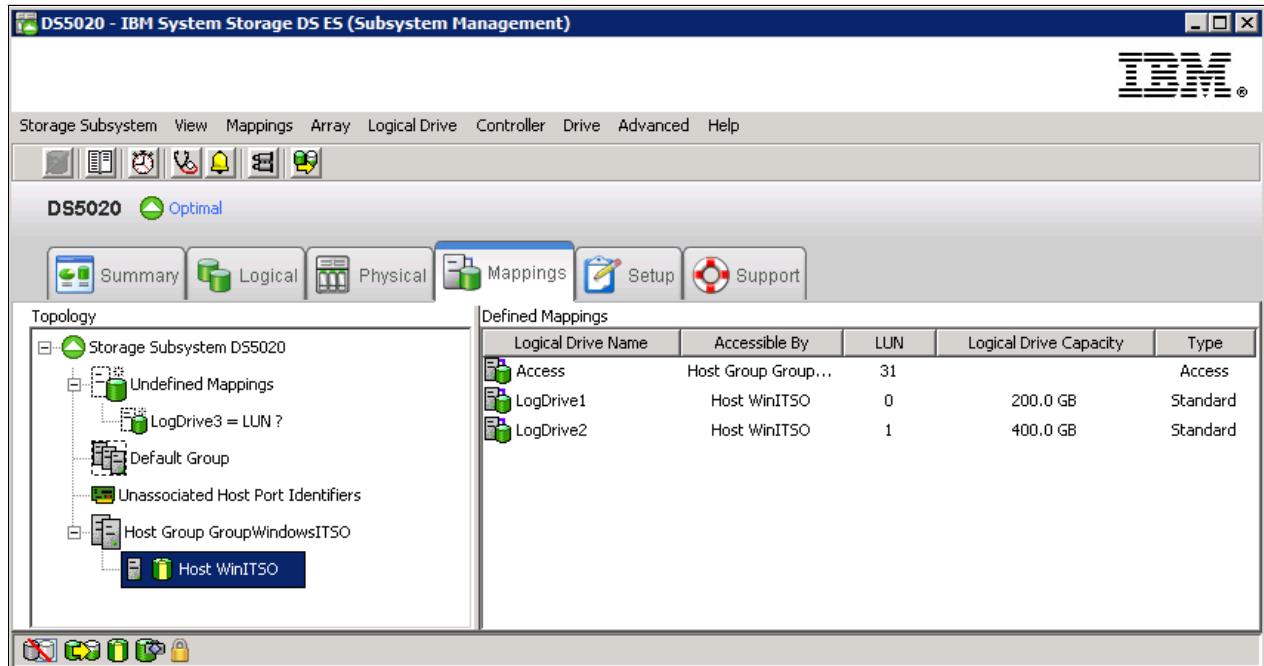


Figure 3-77 Displaying created mappings

Notice that even if the host WinITSO is defined under a host group, the logical drives are mapped exclusively to the host WinITSO. If later you decide to incorporate another host, and make it work together with the first host as a cluster, perform the following steps:

1. Add the second host by performing the steps shown in “Defining hosts” on page 183. Specify the host type and select **Will participate in a cluster**, and incorporate it into the existing host group where your other host is already defined.
2. Change the previous host type from Windows 2008 Nonclustered to Clustered.
3. Reassign the mappings of logical drives. Now we want to map them to the host group, not to an specific host, so all the hosts belonging to the group can reach all the logical volumes.

After performing these steps, the Mappings view appears as shown in Figure 3-78, showing the correct configuration for a cluster environment.

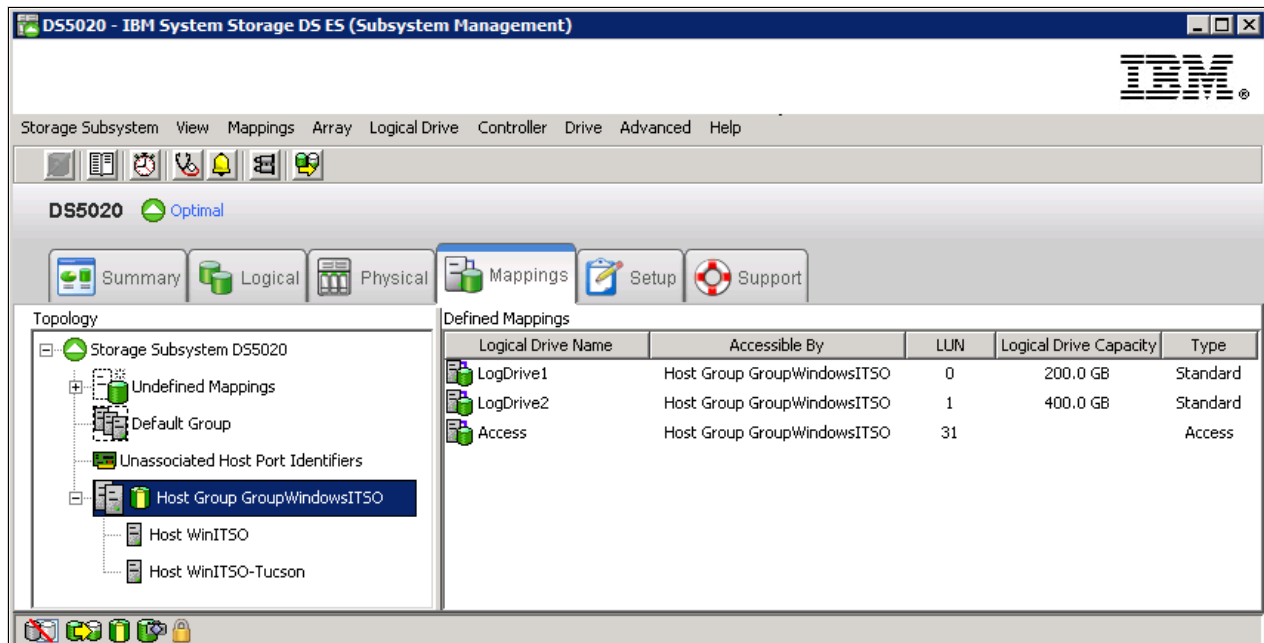


Figure 3-78 Host group mappings for clustering

You can continue creating other partitions or host groups, you should know that even though you can create multiple partitions, you can only map logical drives to partitions up to the maximum number allowed by your specific system and premium feature configuration. Check your storage subsystem for the allowed number of partitions by selecting, in the Subsystem Management view, **Storage Subsystem** → **Premium Features**, and review the information presented, as shown in Figure 3-79.

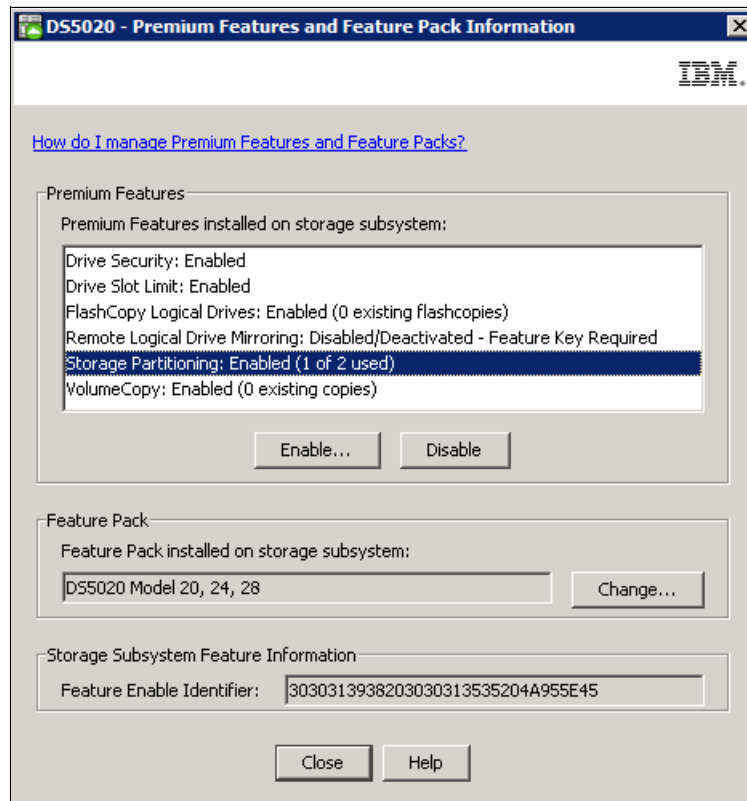


Figure 3-79 Partitions allowed

Define Host Group option

Because the host groups can be created with the Define Host wizard, there is usually no need to define the groups from outside the wizard. But you still have the option to do so by performing the following steps:

1. Right-click **Default Group** and select **Define** → **Host Group**, as shown in Figure 3-80.

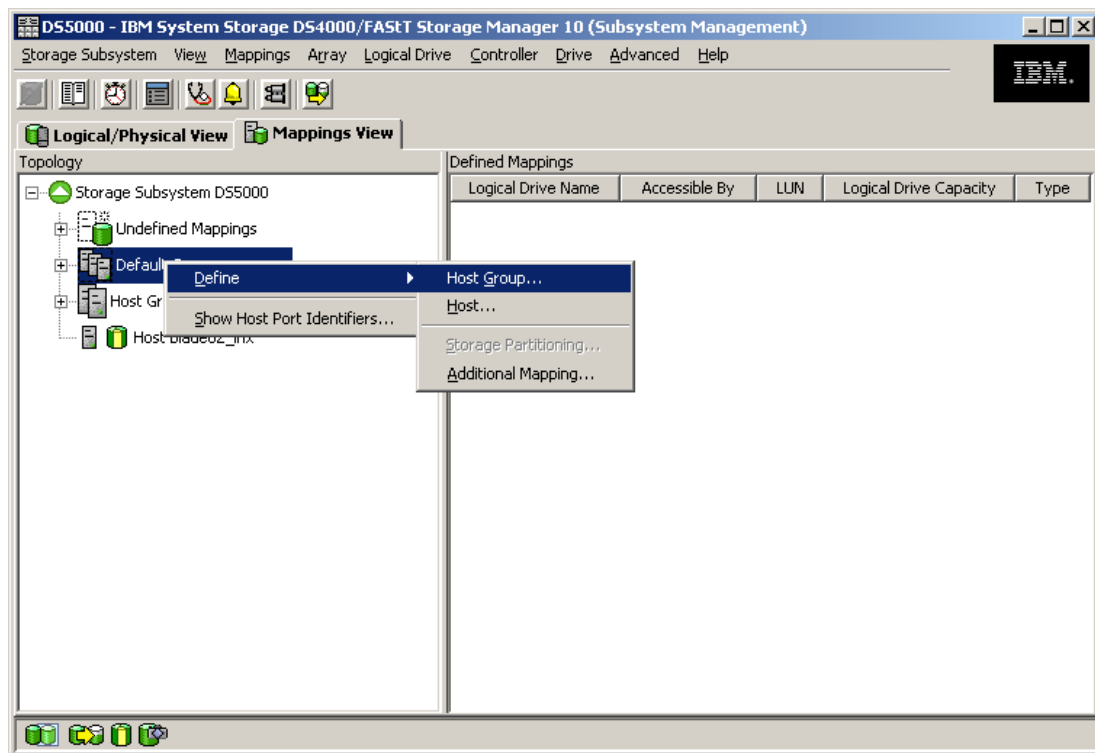


Figure 3-80 Define Host Group

2. The Define Host Group window (shown in Figure 3-81) opens. Enter the name of the host group you want to add. Select every host you want to add to the group and click **Add**. When you are done, you can exit the dialog by clicking **OK**.

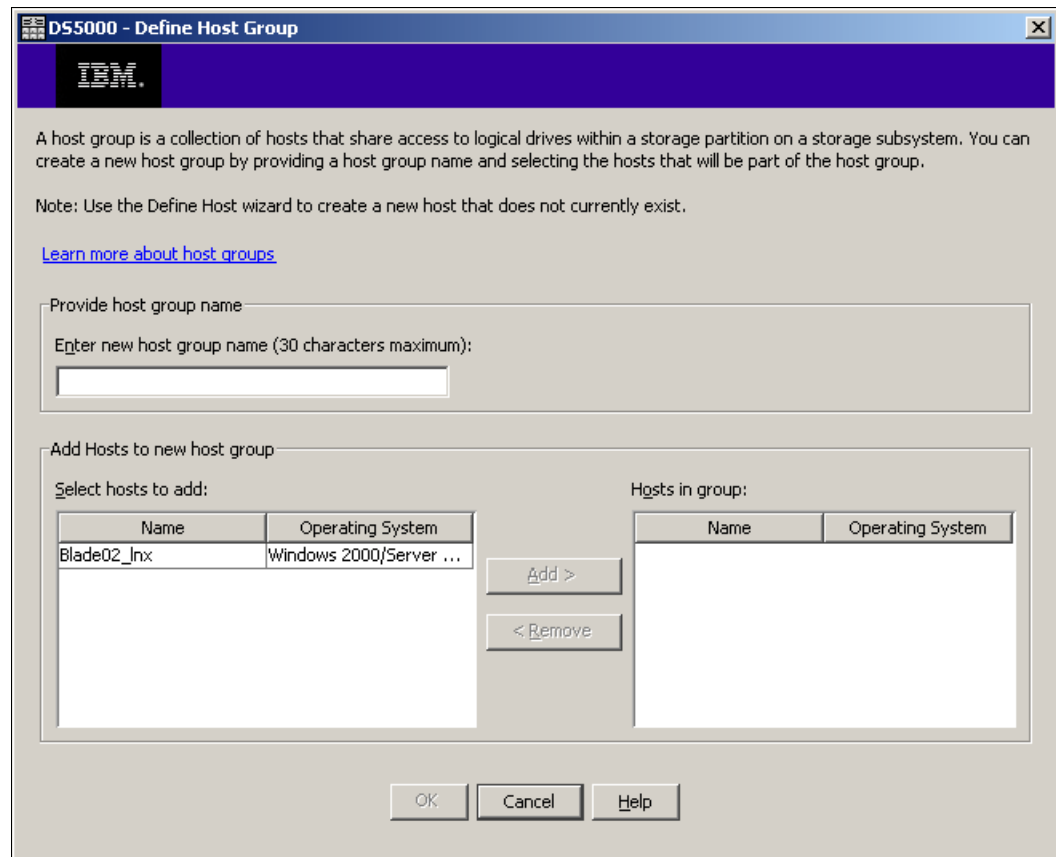


Figure 3-81 Define Host Group name

3. If you accidentally assign a host to the wrong host group, you can move the host to another group. Simply right-click the host and select **Move**. A window opens and prompts you to specify the host group name.
4. Because storage partitioning of the DS5000 storage subsystem is based on the world wide names of the host ports, the definitions for the host groups and the hosts only represent a view of the physical and logical setup of your fabric. When this structure is available, it is much easier to identify which host ports are allowed to see the same logical drives and which are in different storage partitions.

Manage Host Port Identifiers

For environments with multiple hosts and attachment types, you can use this option to have a single source of information about the different available host ports.

From the Subsystem Management window, select **Mappings** → **Manage Host Port Identifiers**. This option opens a window similar to Figure 3-82.

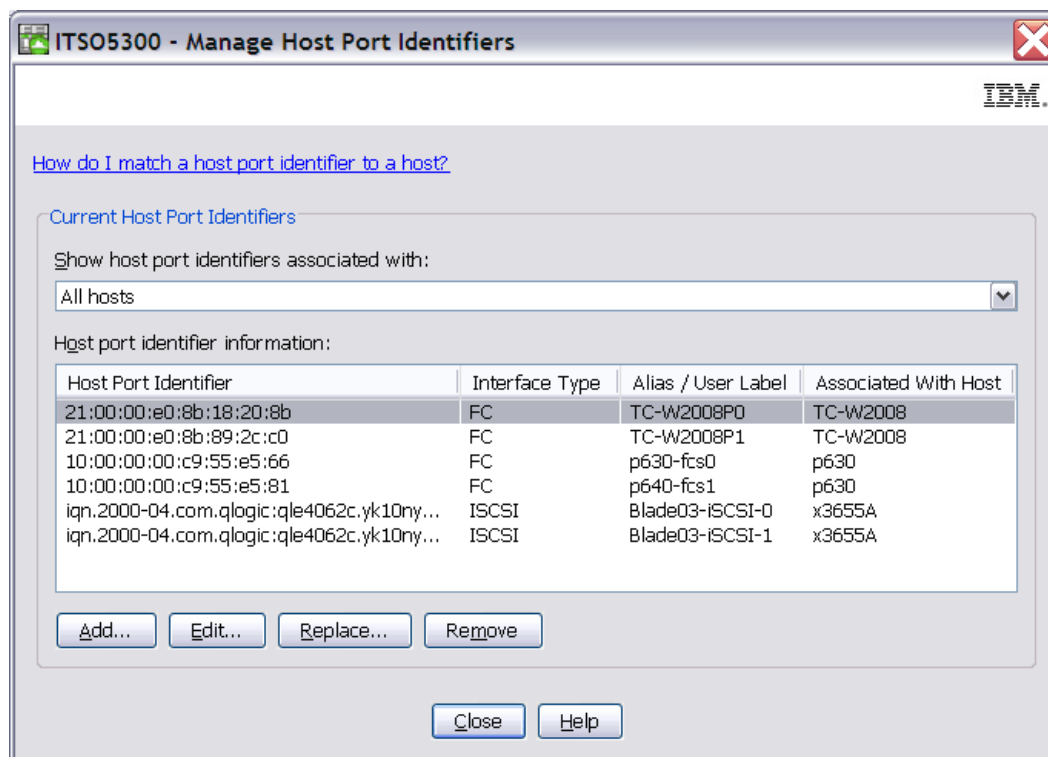


Figure 3-82 Manage Host Port Identifiers

Select this option if you need to review your port configuration assignment, add, remove, and change port settings, and whenever you need to replace a host interface card after a hardware replacement to continue presenting the logical volumes to the new host port identifier, WWPN, or iSCSI Initiator.

Define Additional Mapping option

Suppose that a particular host (or a host group) is already a part of a certain storage partition. This means the logical drives are already mapped to that host or group. If you need to map additional logical drives to the same host or group, use the Define Additional Mapping option:

1. Right-click the host or group to which you want to map a new logical drive. Select **Define** → **Additional Mapping**, as shown in Figure 3-83.

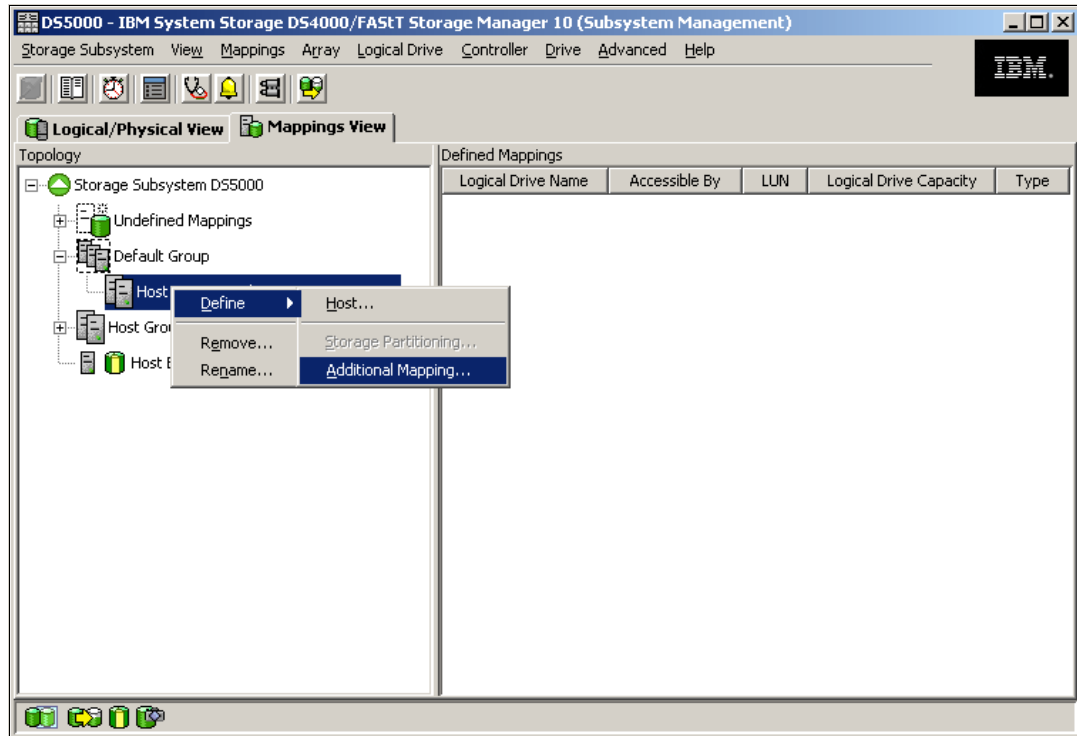


Figure 3-83 Define Additional Mapping

2. In the Define Additional Mapping window, select the logical drive you want to map to this host group or host and assign the correct LUN number, as shown in Figure 3-84.

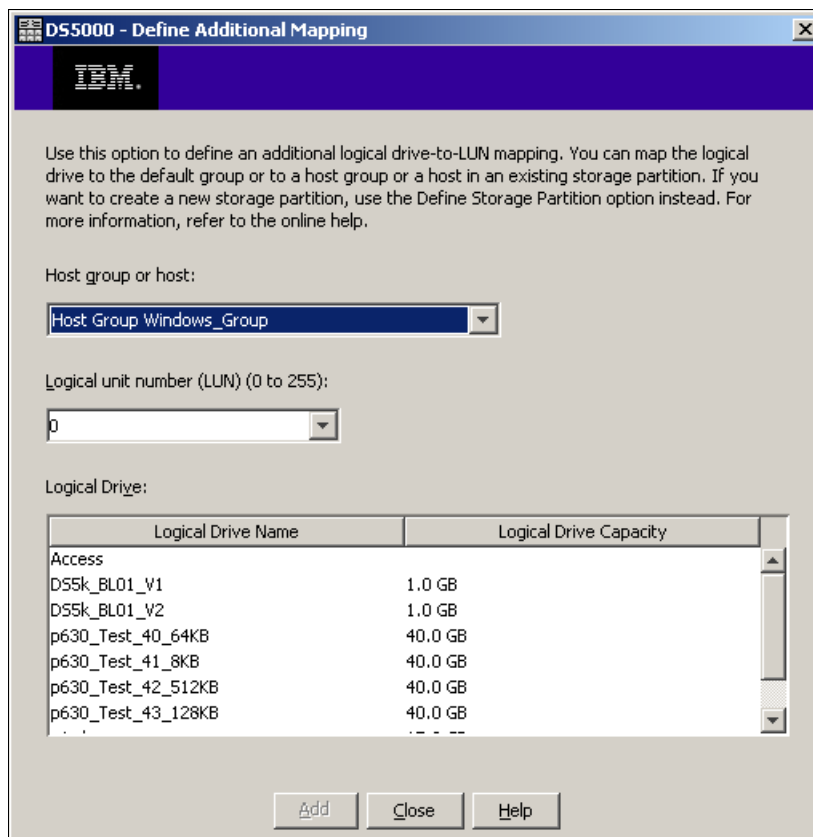


Figure 3-84 Define Additional Mapping

Note: If you change an existing mapping of a logical drive, the change is effective immediately. Therefore, make sure that this logical drive is not in use or even assigned by any of the machines attached to the storage subsystem.

3. To make the logical drives available to the host systems without rebooting, the Storage Manager Utilities package provides the **hot_add** command-line tool (for some operating systems). You simply run **hot_add**, all host bus adapters are rescanned for new devices, and the devices are assigned within the operating system.
 - You might have to take appropriate steps to enable the use of the storage inside the operating system, such as formatting the disks with a file system and mounting them.
 - If you attached a Linux system to the DS5000 storage subsystem, you need to remove the mapping of the access logical drive. Highlight the host or host group containing the Linux system in the Mappings View. In the right part of the window, you see the list of all logical drives mapped to this host or host group. To remove the mapping of the access logical drive, right-click it and choose **Remove Mapping**. The mapping of the access logical drive is removed immediately.

3.5.6 Configuring mapped drives from Windows

To check the new mapped logical drives from the Windows Server 2008 used in this example, start with the SANsurfer management tool. Refresh it so that the HBAs search for all the new mapped drives. After that action completes, you see the information shown in Figure 3-85.

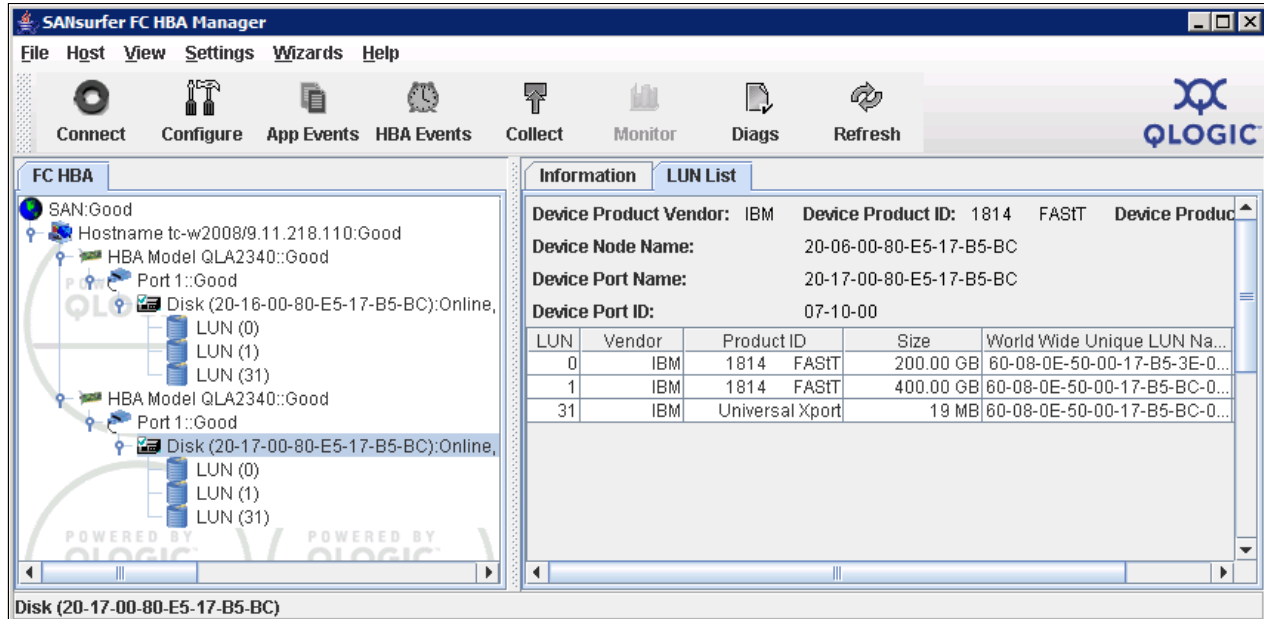


Figure 3-85 Displaying mapped logical drives

The verified HBAs show all the mapped LUNs, so you can use the Windows Disk Administrator utility to scan for new storage, create and format partitions, and begin using the new disk space.

First, use the Windows Device Manager to scan for new hardware changes. Once refreshed, you see the newly mapped logical drives from your DS5000 storage subsystem under the Disk drives folder of the server.

Each logical drive is presented as IBM xxxx Multipath Disk Device under the Disk drives folder, where xxxx is the product ID of the DS Storage subsystem, as shown in Figure 3-86.

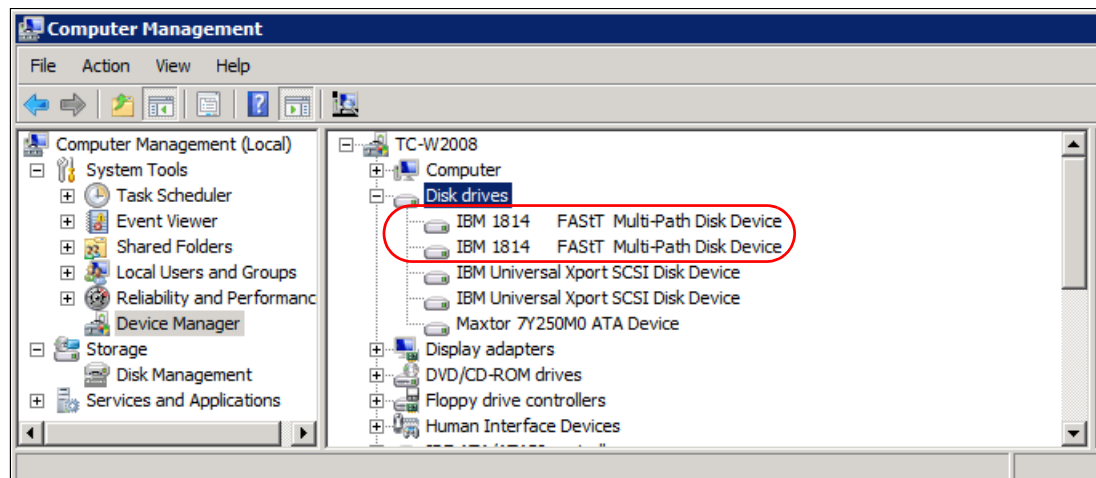


Figure 3-86 Verifying new disks in Device Manager

With MPIO, each device listed here represents a logical drive. In order to display the different paths of each one, select it and then choose **Properties**. Select the **MPIO** tab to display the different paths to the DS5000 storage subsystem. From the same Properties window, you can set the different Load Balance policies for the MPIO driver. Depending on the current physical path state, and the policy selected, the paths are both Active (round robin, weighted paths), or one Active and the other in Standby (failover, Least queue depth), as shown in Figure 3-87.

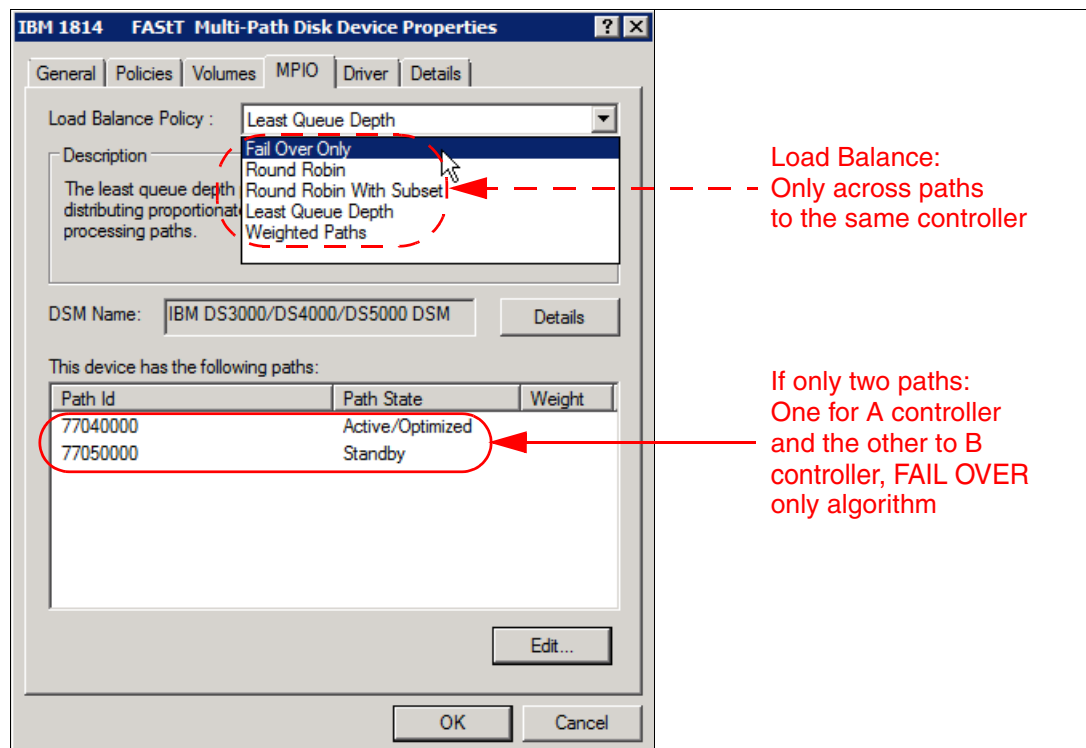


Figure 3-87 MPIO load balancing policy

Important: The Load Balance algorithms only work between multiple paths to the same controller. If you only have one path, you can only have failover capability.

For a correct data assignment to your defined logical volumes, you need to determine which of the disks drives in the Windows Device Manager or Disk Manager relates to the previously defined logical volumes of your DS5000 storage subsystem.

Select the disk drive, right-click it, and select **Properties**. Use the LUN number to isolate each logical drive, as shown in Figure 3-88.

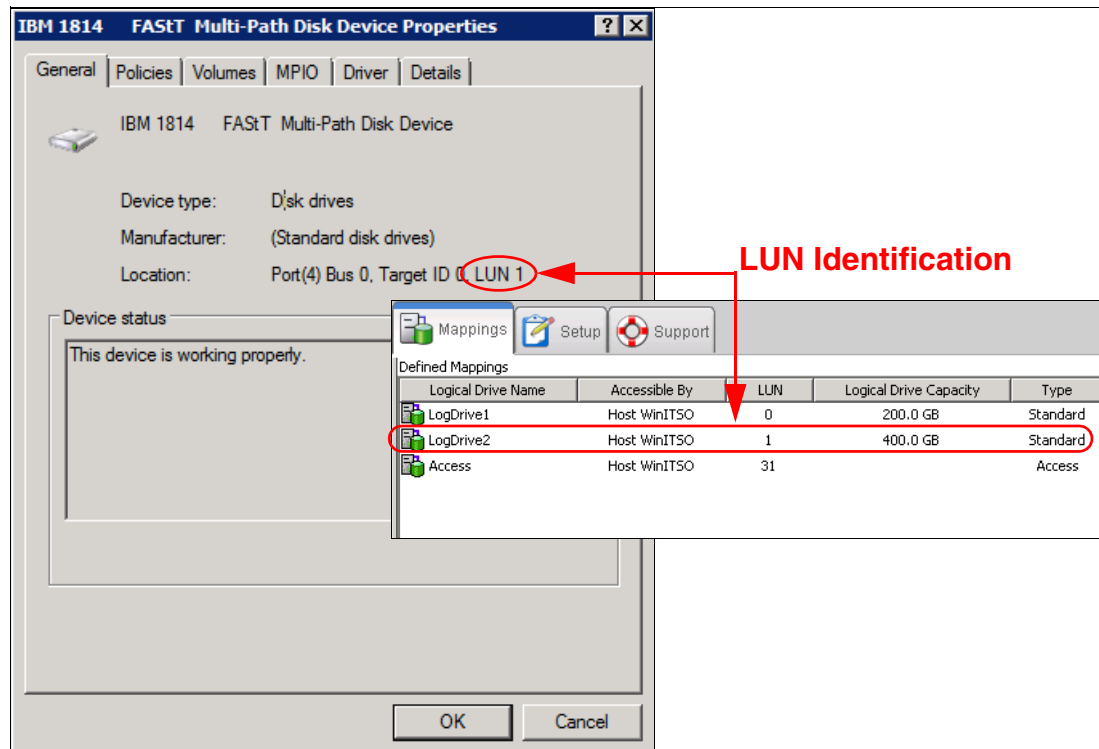


Figure 3-88 Matching LUNs between a Windows host and SM

Finally, use the Windows Disk Management to start using your new mapped DS5000 storage subsystem disks, as shown in Figure 3-89. You can get the information shown in Figure 3-88 by clicking each of the drives and selecting **Properties** as highlighted in Figure 3-89.

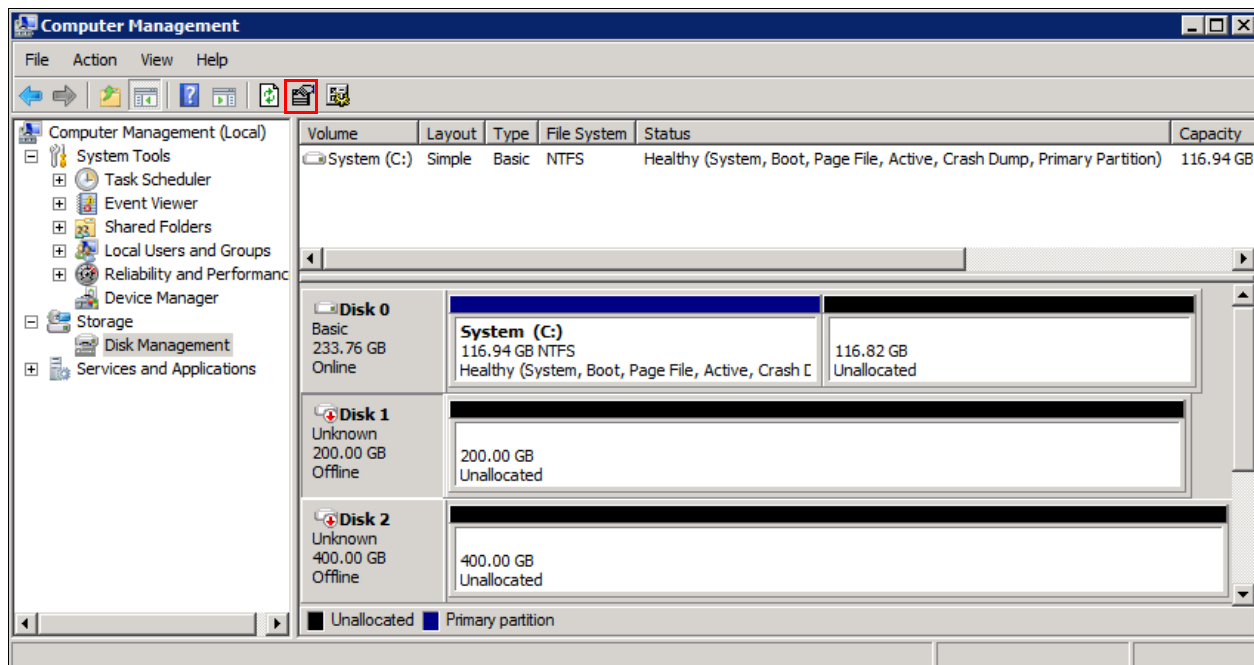


Figure 3-89 Windows Disk Management

The disks drives are shown as Offline. To start using one, right-click it, select **Online**, and then **Initialize**. After that, click the **Unallocated** space to partition the disk and assign a drive letter.

When disks are found through the Windows scanning process the IBM DS Storage Manager provides a utility in *SMUtils* to display the logical drives mapped. You can access this utility by opening your Storage Manager installation directory and run the *SMdevices* utility from a command prompt. Once you run the utility, you will see the output shown in Example 3-1.

Example 3-1 SMdevices output

```
C:\Program Files\IBM_DS\util>SMdevices
DS Storage Manager Utilities Version 10.01.35.01
Built Fri Jun 19 06:12:18 CDT 2009
IBM System Storage DS Storage Manager(Enterprise Management)
(C) Copyright International Business Machines Corporation, 2003-2009 Licensed Ma
terial - Program Property of IBM.
All rights reserved.
US Government Users Restricted Rights - Use, Duplication, or disclosure restrict
ed by GSA ADP Schedule Contract with IBM Corp.
IBM Support URL=http://www.ibm.com/servers/storage/support/disk/

\\.\PHYSICALDRIVE1 [Storage Subsystem DS5020, Logical Drive LogDrive1, LUN 0,
Logical Drive ID <60080e500017b53e000048364a9fb470>, Preferred Path (Controller-
A): In Use]
\\.\PHYSICALDRIVE2 [Storage Subsystem DS5020, Logical Drive LogDrive2, LUN 1,
Logical Drive ID <60080e500017b5bc000044e34a9fb474>, Preferred Path (Controller-
B): In Use]
\\.\SYMsmUTMLun0 [Storage Subsystem DS5020, Logical Drive Access, LUN 31, Logi
cal Drive ID <60080e500017b5bc000043834a955f8a>]
\\.\SYMsmUTMLun1 [Storage Subsystem DS5020, Logical Drive Access, LUN 31, Logi
cal Drive ID <60080e500017b5bc000043834a955f8a>]
```

Note that so far we updated the storage subsystem to the latest level, configured logical drives, set up storage partitioning, and configured you host system. The next step is to define the alerting methods to be used in case of failures.

For more information about drive mapping in other operating systems, see *IBM System Storage DS5000 Series Implementation and Best Practices Guide*, SG24-8024.

3.5.7 Monitoring and alerting

The Event Monitor program is included in the Storage Manager Client package. It enables the host running this monitor to send out alerts (through e-mail (SMTP) or traps (SNMP)) about any of the DS5000 storage subsystems in your environment.

Earlier versions of Storage Manager include the Event Monitor, where the Enterprise Management window had to remain open to monitor the storage subsystems and receive alerts. Now you will receive an alert either from the SMclient, if it is opened, or from the Event Monitor program.

For continuous monitoring, install the Event Monitor on a host computer that runs 24 hours a day. If you choose not to install the Event Monitor, you should still configure alerts on the host computer where the client software is installed, but it will only work when the SMclient is

opened. The installed server should be capable of out-of-band and in-band management. This ensures proper alerting, even if one server is down, or a connection type has failed.

Important: The DS5000 storage subsystem does not send the e-mail or SNMP trap itself. The management station running the event monitor service sends the e-mail or SNMP trap on behalf of the DS5000 storage subsystem. If the management station is down, or if the event monitor process is not running, no notifications will be sent.

The Enterprise Storage Management Task Assistant lets you configure alerts with the following options:

- ▶ All storage subsystems in the management domain
- ▶ An individual storage subsystems
- ▶ All storage subsystems managed through an specific host

The steps are:

1. Make sure the SMclient package has been installed in the workstation you configure to send alerts.
2. Decide which storage subsystems you want to monitor. You can set up alert-notification destination addresses where you will be notified. Use the Enterprise Task or the following options to configure the alerts.

3. If you right-click your local system in the Enterprise Management window (at the top of the tree) and choose **Configure Alerts**, this applies to all storage subsystems listed in the Enterprise Management window. If you want to monitor only one subsystem, then click that particular one and select **Edit** → **Configure Alerts**. You can also select the **Setup** tab of the Enterprise Management window, and then select the **Configure Alerts** option. You will be prompted about whether you want to configure alerts for all storage subsystems or any one in particular, as shown in Figure 3-90.

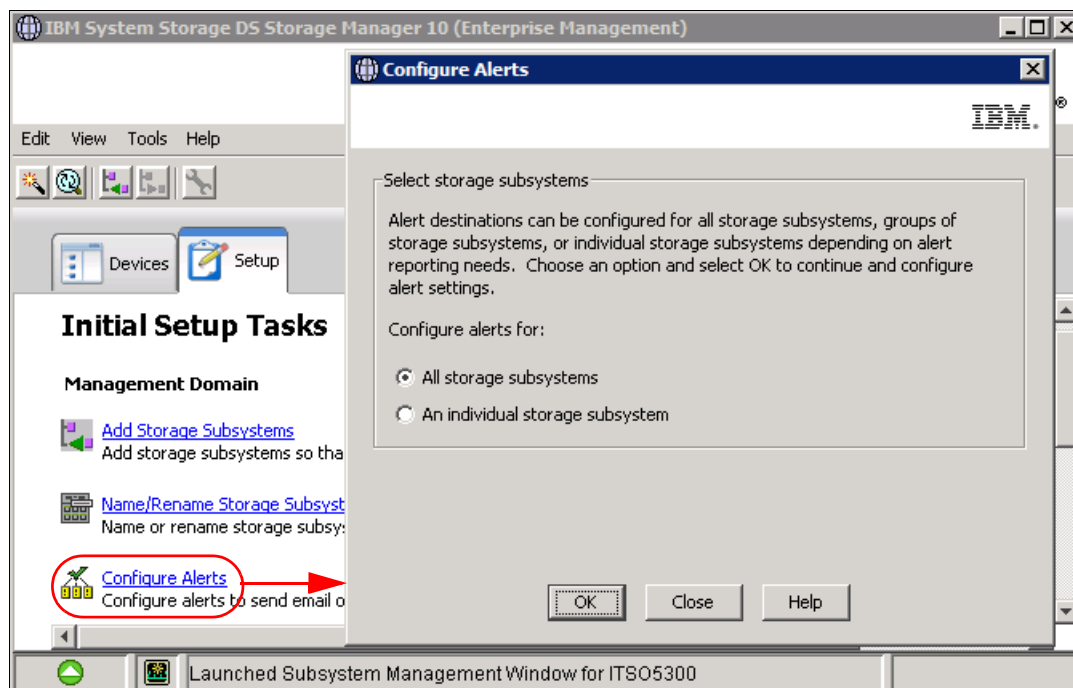


Figure 3-90 Selecting the Configure Alerts option

4. If you want to send e-mail alerts, you have to define an SMTP server first. Enter the Mail SMTP Server name or IP address of your mail server and the e-mail that will show as the origin of the message, as shown in Figure 3-91. You can also complete the contact information, if desired.

The image shows a 'Configure Alerts' dialog box with an IBM logo in the top right corner. The title bar says 'Configure Alerts'. Below the title bar, it states 'Alerts are generated for critical events only.' There are three tabs: 'Mail Server', 'Email', and 'SNMP'. The 'Mail Server' tab is selected. Inside this tab, there are two text input fields. The first is labeled 'Mail server (SMTP server name, IPv4 address, or IPv6 address):' and contains the text '9.18.81.50'. The second is labeled 'Email sender address:' and contains the text 'DSalerts@ar.ibm.com'. Below these fields is a checked checkbox labeled 'Include contact information with alerts:'. Underneath the checkbox is a large text area containing the following text: 'Name: ITSO', 'Title: Alerts from DS Storage subsystems', 'Company: IBM', 'Phone:', 'Cell phone:', 'Pager:', 'Email:', 'Fax:', and 'Additional info:'. At the bottom of the dialog box are three buttons: 'OK', 'Cancel', and 'Help'.

Figure 3-91 Configure Alerts: Defining the SMTP server

5. Select the **Email** tab. This tab allows you to configure the e-mail addresses to which the alerts are sent. Enter the e-mail address and press **Add** to append it to the list of notifications.

6. The default notification sends only the event when it occurs.

Note that you can also modify the Information to Send field to forward profile data or support data, either when an event occurs or at regular intervals. Make use of this feature whenever possible, as shown in Figure 3-92.

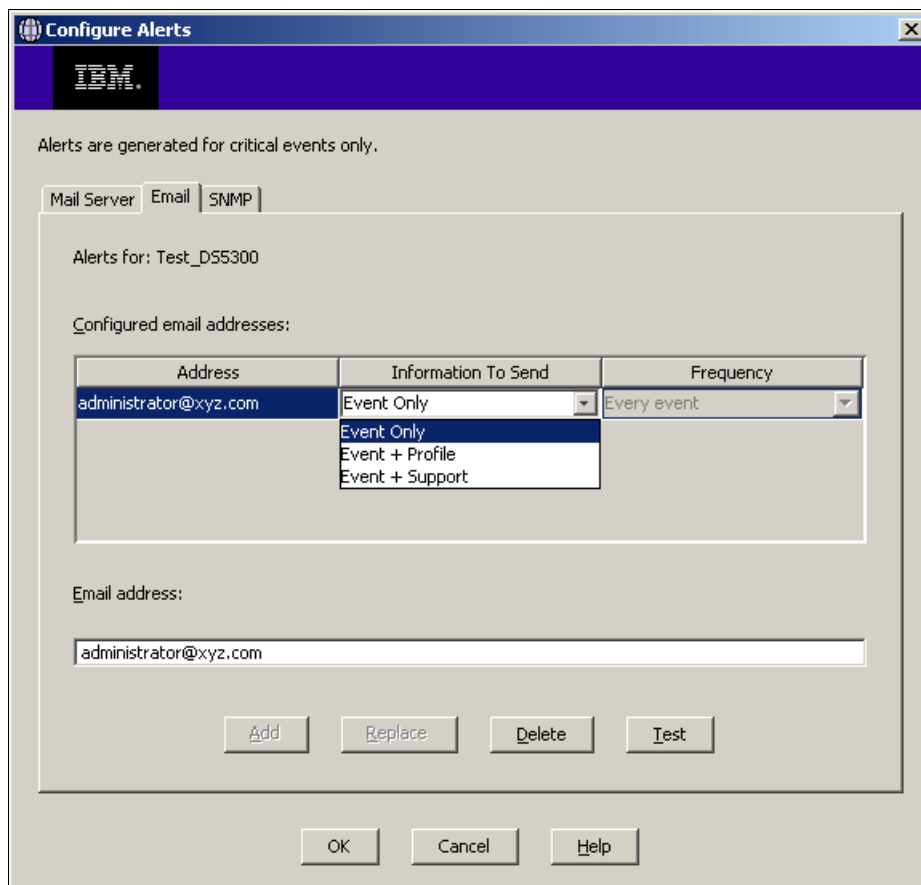


Figure 3-92 E-mail notification setup

Be aware that sending the support data at regular frequencies might impact the capacity of the destination e-mail address box.

Note: Besides the e-mail notification with error capture attached, there is another option to collect diagnostic data when an error is detected, that is, by enabling automatic collection of support data. See , “Gathering support information” on page 211 for more information.

7. When you have finished adding e-mail addresses to notify, test your specified SMTP and e-mail addresses by clicking the **Test** button.
8. If you have a Network Management Station (NMS) in your network collecting traps, select the **SNMP** tab to define the settings for SNMP alerts. Type the IP address of your SNMP console and the community name. As with the e-mail addresses, you can define several trap destinations.

The NMS can decode the received traps using the MIB file included in the Storage Manager software CD, which should be compiled into the NMS console to allow proper display of the traps. To set up alert notification to an NMS using SNMP traps, perform the following steps:

- Insert the IBM DS Storage Manager CD into the CD-ROM drive on an NMS. You need to set up the designated management station only once.
- Copy the SMxx.x.MIB file from the SMxxMIB directory to the NMS.
- Follow the steps required by your NMS to compile the management information base (MIB) file. (For details, contact your network administrator or see the documentation specific to your particular storage management product.)

After configuring the storage subsystem for alerts, check the results in the Enterprise Management window, as shown in Figure 3-93.

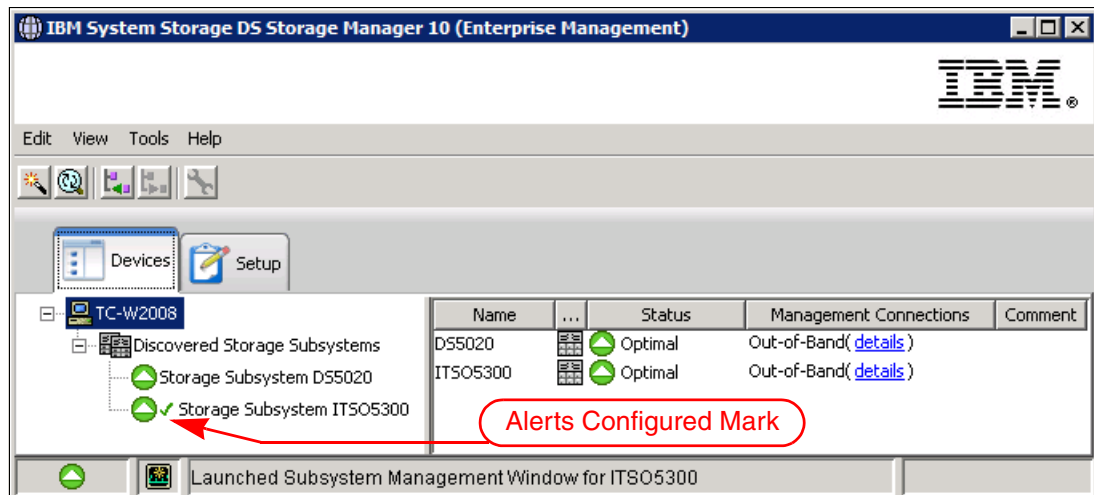


Figure 3-93 Alerts configured for one specific DS5000 storage subsystem

Check for the mark besides each representation of the storage subsystem configured for alerts.

- ▶ Only the storage subsystems with a Alerts Configured mark will be monitored.
- ▶ Event Monitor will send only one alert per event, even if the events are monitored through different hosts or out-of-band. However, if you configure the Event Monitor in more than one management station, you will receive duplicate messages.

See Chapter 6, “IBM Remote Support Manager for Storage” on page 455 if you want IBM to receive these notifications.

3.5.8 Saving the configuration

Once your DS5000 storage subsystem is configured and running, you should save this configuration. This allows you to replicate the configuration already performed in another DS5000 with identical physical resources, or in the same system in case you need it. It can also be used to recover part of the configuration in case of problems.

These are the different type of information to save:

- ▶ Save Configuration option
- ▶ Storage Profile option
- ▶ Support Data

We show how to save each of the options available in the following sections. If you need assistance to recover part of the configuration, contact your IBM Support representative.

Save Configuration

The Save Configuration option includes information for the arrays and logical drive configuration, the name of the subsystem, its cache settings, and other parameters, including the storage partitioning configuration.

The saved file can be used to restore the configuration data to the same DS5000 storage subsystem, or also to other DS5000 storage subsystems in case you want to set up multiple storage subsystems with the same configuration. To allow that action, the destination subsystem must have the same hardware layout, number of enclosures and drives, and drive capacities.

All information is stored in a file that contains a script for the script editor. To save the configuration of the subsystem, open the Subsystem Management window, highlight the subsystem, and select **Storage Subsystem** → **Configuration** → **Save** as shown in Figure 3-94.

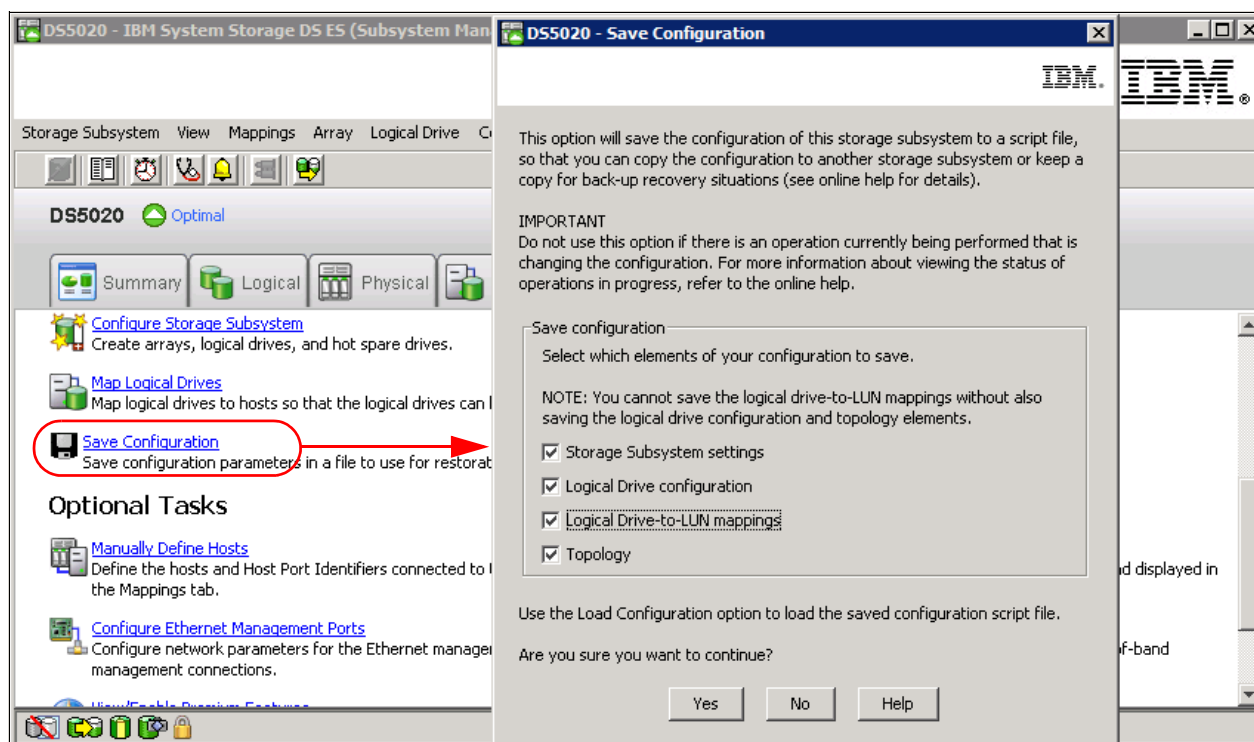


Figure 3-94 Saving the DS5000 storage subsystem configuration

We can choose to save specific elements of the configuration.

Select the desired configuration elements, click **Yes**, and select a file name and destination folder in which to save the file. Make sure not to use a directory located on a DS5000 storage subsystem disk, or you might not be able to access it when needed.

The script created can be used to replicate the configuration of the DS5000 storage subsystem. You can apply the configuration to the destination subsystem for all the saved elements, or any particular element.

Remember that this save option does not include the data resident on the logical volumes, only configuration data. Make sure to make periodic backups of your data to avoid exposures.

Storage subsystem profile

Configuring a DS5000 storage subsystem is a complex task and it is therefore essential to document the configuration. The profile data contains information that could help recover part or all of the configuration of the DS5000 storage subsystem, and can also be saved in a file known as the *subsystem profile*. This profile stores information about the controllers, attached drives, and enclosures, and their microcode levels, arrays, logical drives, and storage partitioning.

Tip: You should save a new profile every time you change the configuration of the DS5000 storage subsystem, even for minor changes. The profile is stored in a location where it is available even after a complete configuration loss, for example, after a site loss.

1. To obtain the profile, open the Subsystem Management window and select **Storage Subsystem** → **View** → **Profile**, as shown in Figure 3-95.

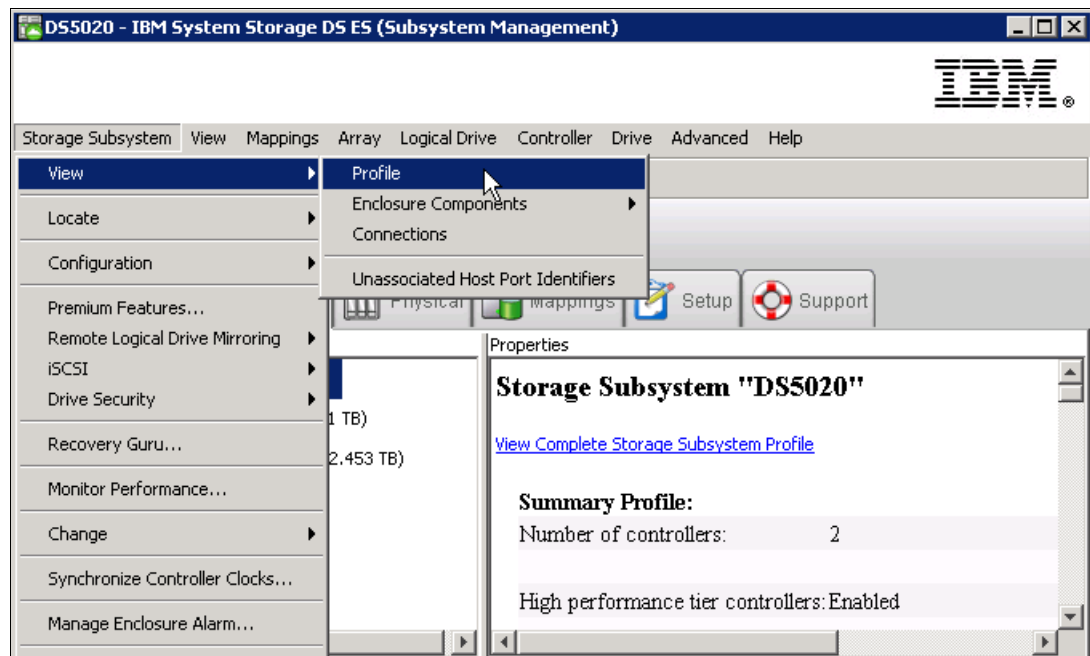


Figure 3-95 Viewing the storage subsystem profile

2. The information is gathered from various components when you request the profile. The profile can be saved locally and included in the documentation to maintain a change history for the storage subsystem.

We recommend that you save a new version of the profile and store it securely whenever a configuration change takes place. Even in the case of a complete configuration loss, you can restore the arrays and logical drives configuration as well as the mappings for the storage partitioning using the profile information.

A sample profile window is shown in Figure 3-96.

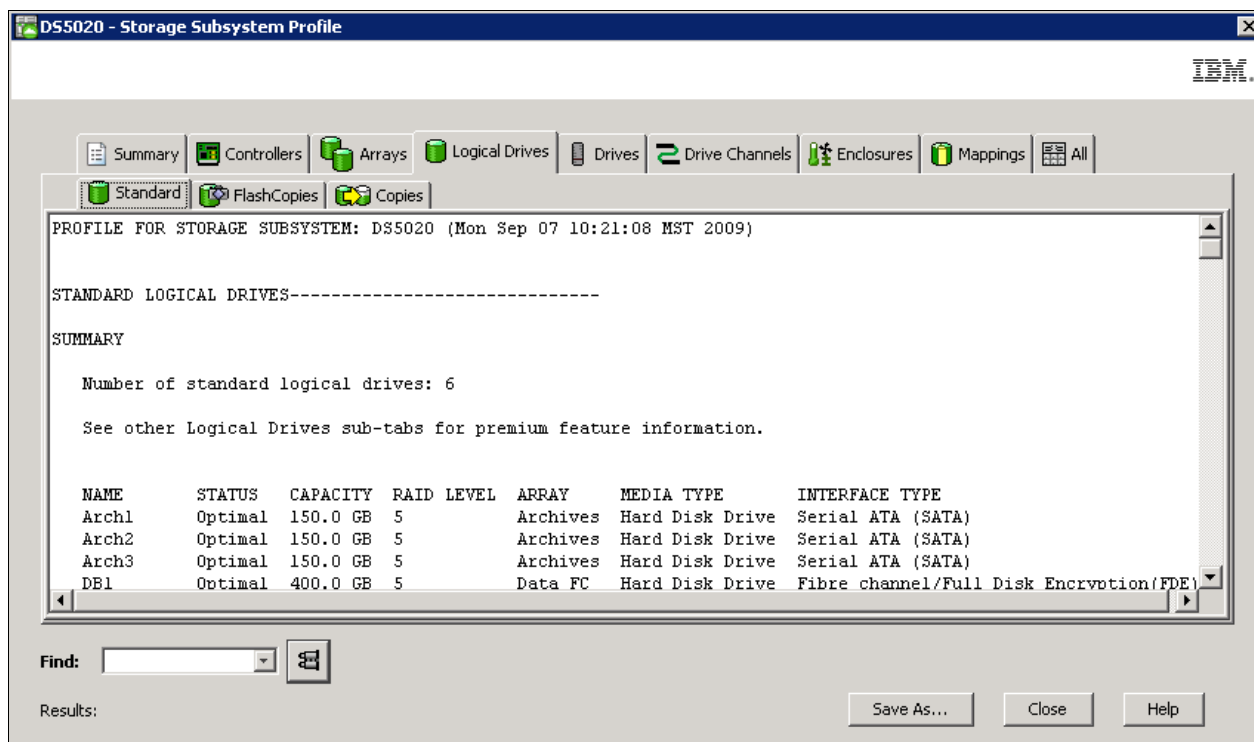


Figure 3-96 Storage Subsystem Profile

3. Select the **Save As** option to keep a copy of the current profile configuration. In the next window, select **All Sections** and specify a directory and file name where you will save a copy, as shown in Figure 3-97.

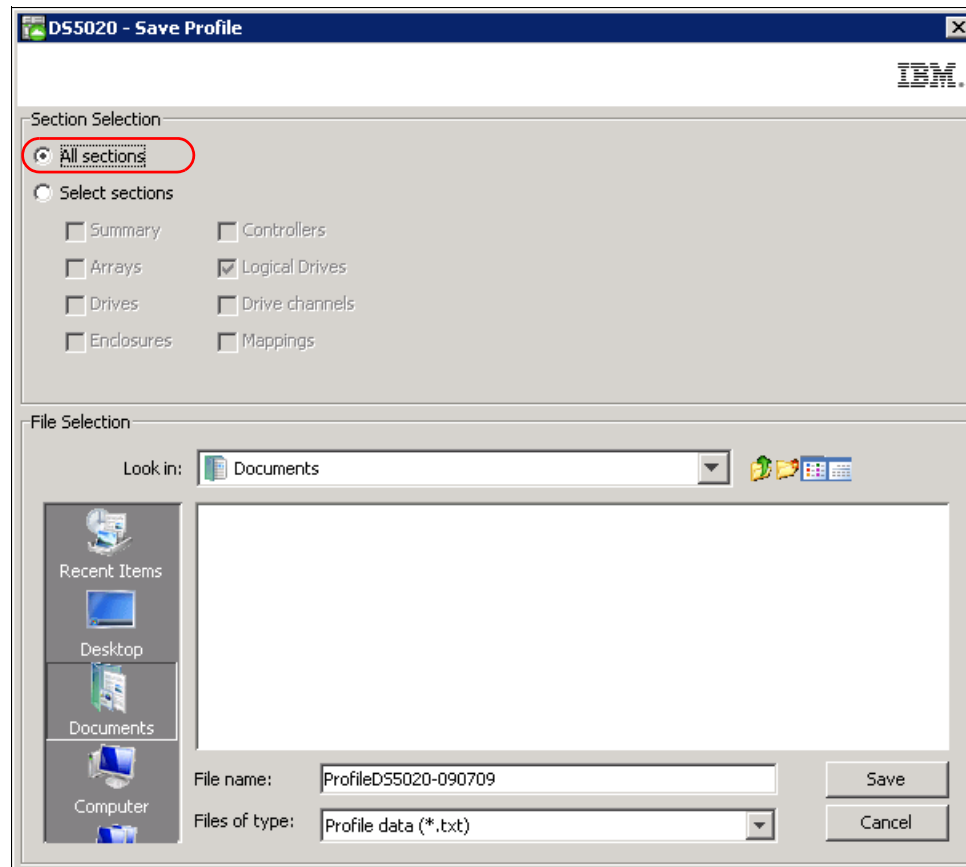


Figure 3-97 Save Profile: All sections

Gathering support information

Support Data is an option of the Storage Manager that lets you collect all the internal information of the DS5000 storage subsystem for review by the support organization. This includes the storage Subsystems Profile, majorEventLog, driveDiagnosticData, NVSRAM data, readLinkStatus, performanceStatistics, and many others.

This information can be collected manually at any time, but if there is a critical problem, it is collected automatically and saved to the folder `\client\data\monitor\` under the installation path of the Storage Manager. In case of problems, your IBM support representative might need this data to identify the source of the problem and make the necessary corrections.

Make sure to check that the automatic collection of support data is not disabled, select **Advanced** → **Troubleshooting** → **Support Data** → **Support Data** → **Automatic Settings**, as shown in Figure 3-98.

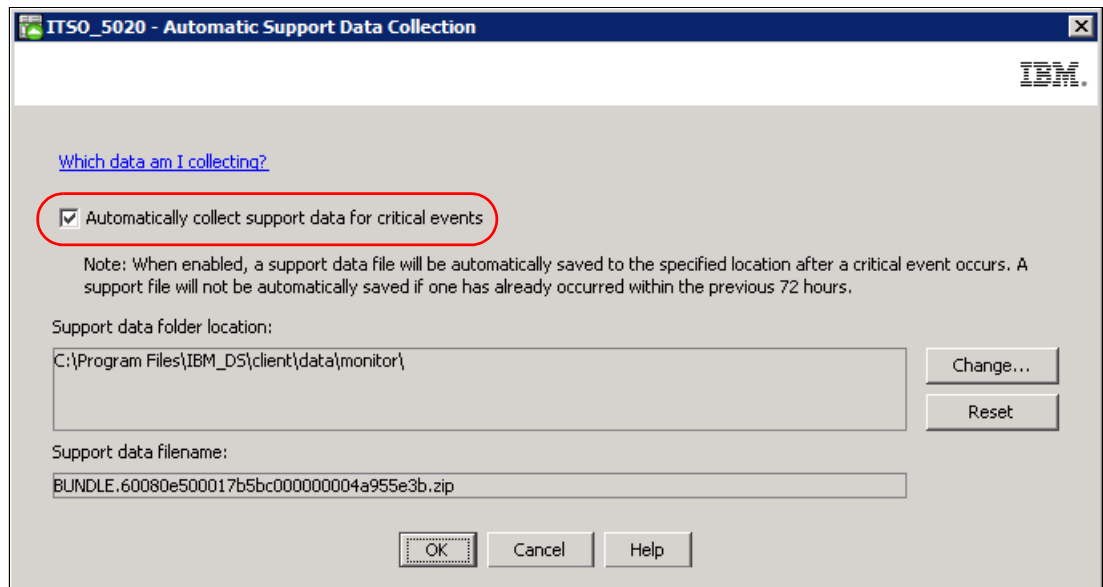


Figure 3-98 Automatic Support Data Collection

Collect data before and after any major changes by selecting **Gather support information** from the Support view of the Subsystem Management window, as shown in Figure 3-99.

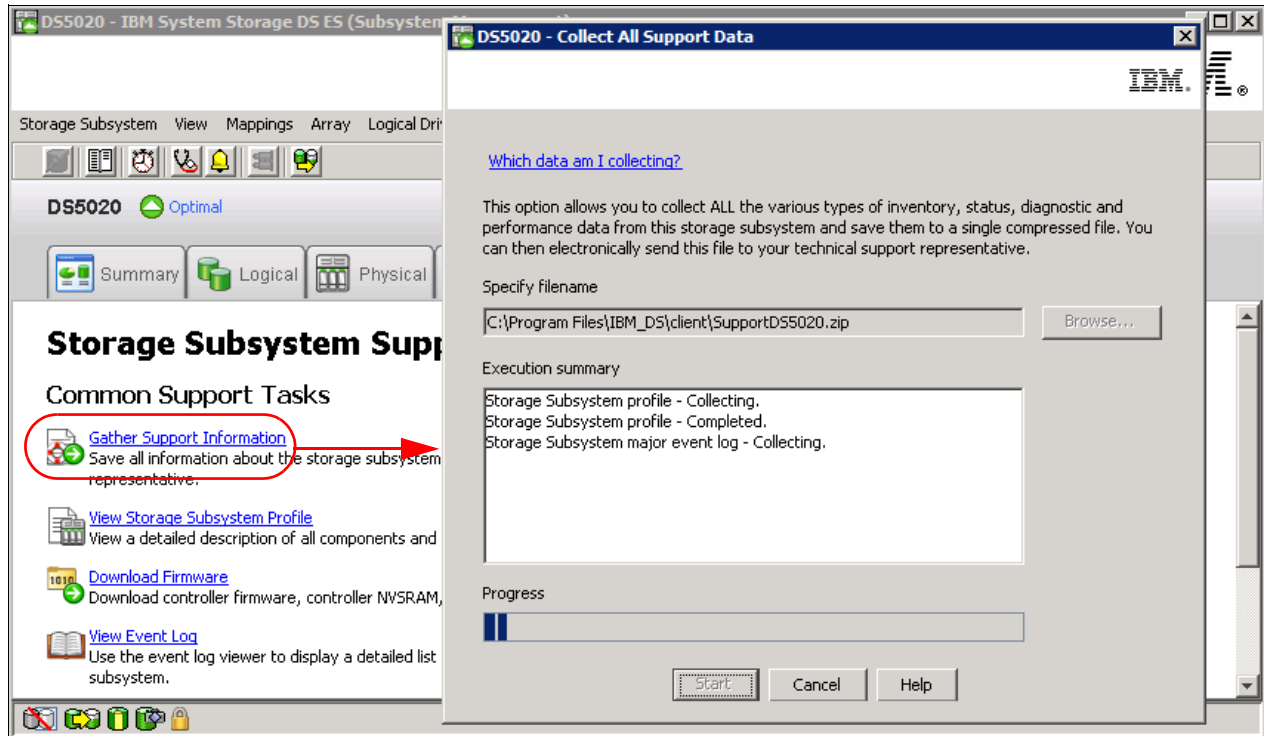


Figure 3-99 Gather support information

Important: The profile and support data files provides configuration information that can be used in case of a failure to recover the configuration. Remember to save a copy after making changes in the configuration, and keep it outside of the DS5000 storage subsystem disks.

3.6 Advanced functions

This section introduces some of the advanced features of the Storage Manager.

3.6.1 Expanding arrays

The ability to increase the available free capacity in an array (*Dynamic Capacity Expansion (DCE)*) without needing to restart the host system is a very important feature. In today's IT environment, the need for storage space grows constantly. Many customers exhaust their existing space sooner or later and have to expand their storage capacity. It is essential that this process be nondisruptive and not cause any downtime.

With Storage Manager, it is possible to add new disk drives to the storage subsystem and start the expansion procedure while the system remains fully operational. Once the procedure starts, it cannot be stopped. This procedure might have a performance impact, because the expansion process competes with normal disk access. We recommend that, where possible, that this type of activity be performed when I/O activity is at a minimum. The new free capacity can be used to create additional logical drives. Existing logical drives in the array do not increase in size as a result of this operation.

Note: Storage Manager supports RAID 0 and 1 arrays with more than 30 drives. In certain DS5000 storage subsystem configurations, this can improve performance, provided that the system is optimally tuned. It also improves the data capacities of these arrays. RAID 1 or 10 requires an even number of disk drives.

Attention: It is still not possible to use more than 30 drives in RAID 3, 5, and 6 arrays. Once the maximum number of drives is reached, you obviously cannot add new drives anymore.

To add new drives to an array, highlight the array, right-click, and select **Add free Capacity (Drives)**. In the Add Drives window (Figure 3-100), choose one or two drives to be added to the array, depending on whether RAID 1 or 10 is being used by the array. The controller firmware imposes a maximum of two drives to be added *at one time*, although this operation can be repeated to add more than two drives to an array.

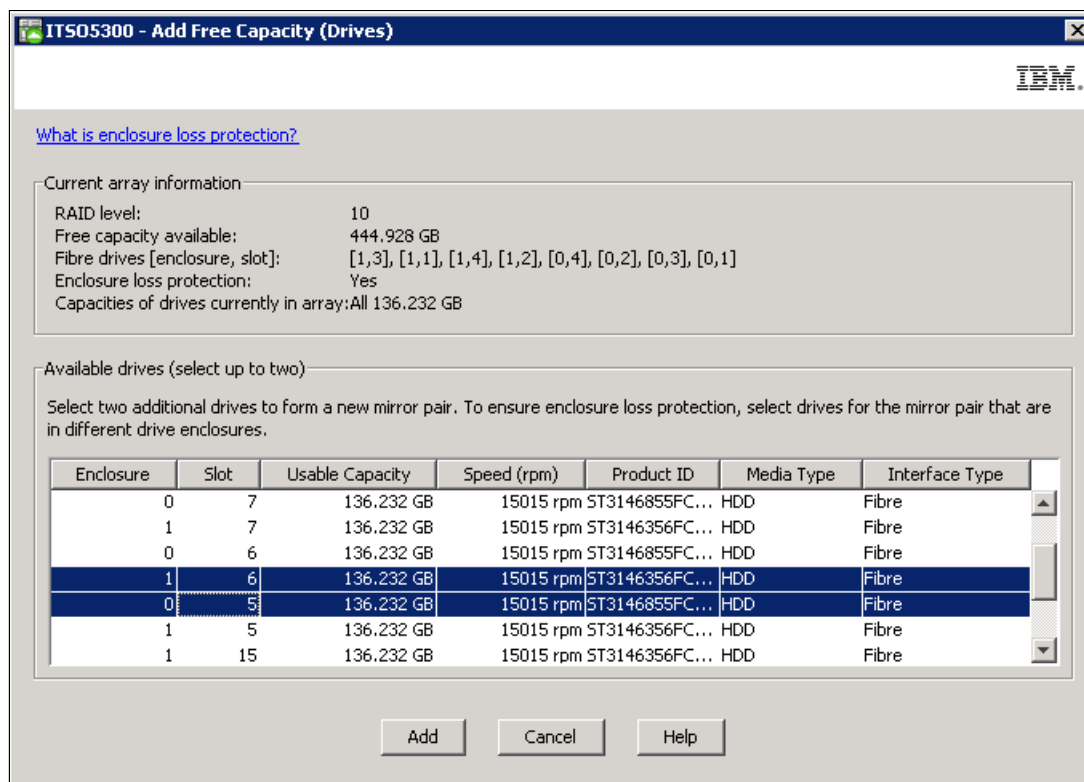


Figure 3-100 Adding new drives to an array

For RAID levels 3, 5, and 6, select one drive, and for RAID levels 1 and 10, two drives must be selected, with the following considerations:

- ▶ Only the type of disks are listed as candidates to add (FC/SATA).
- ▶ Select drives that have a capacity equal to the current drive capacities in the array.

Note: Drives larger than the other drives participating in the array can be added, but we do not recommend it, because their usable capacity will be reduced so that they match the current drives capacities in the array.

Once the procedure is started, it cannot be stopped, as the subsystem needs to redistribute the data contained in the array to all drives, including the new ones. There is a performance impact during this operation, but the logical drives of the array remain available to the host systems.

3.6.2 Changing the RAID array level

Changing the RAID level of an array is performed in a nondisruptive manner. The system remains fully operational while the process takes place. A few possible reasons why customers might want to do this operation are:

- ▶ The storage requirements changed over time and existing RAID levels are no longer optimal for a particular environment.
- ▶ The performance tuning process indicates that a different RAID level is more appropriate than the existing one.

It is possible to change any RAID level to any other one. There are some restrictions that apply to the new arrays:

- ▶ RAID 1 or 10 requires an even number of disk drives.
- ▶ RAID 3 and 5 require at least three drives.
- ▶ RAID 6 requires at least five drives.
- ▶ There is a limit of 30 drives per array for RAID 3, 5, and 6 arrays.

There are limitations if there is not enough free space in the array. For example, a RAID 5 array of four disk drives with no free space cannot be migrated directly to RAID 1. If this migration is attempted, an error message will be displayed stating that there is not enough free space. There must be enough free capacity to change the RAID level. Also, if the array has an odd number of drives and a migration to RAID 1 is required, a disk must be added to the array prior to performing the procedure.

When changing from RAID 1 to RAID 5, free space in the array can be gained, which can be used to define new logical drives or expand existing ones.

When the procedure starts, it reorganizes the data segments in the array according to the new RAID level, and a large amount of I/O happens, so there is an impact on performance while the migration lasts. The performance impact can be controlled to a certain extent by changing the value of the modification priority. This parameter is set on a logical drive basis, which is where it should be changed for all logical drives in the array.

Changing the modification priority to a low value during the migration process minimizes performance degradation. When the migration finishes, the value can be increased to reduce the time for a rebuild in case of a drive failure. This minimizes the critical time of non-redundant operation caused by the disk drive fault.

Attention: Once the migration starts, it cannot be stopped.

Note: Even though RAID migration is a nondisruptive process, we recommend carrying out this migration when I/O activity is at a minimum.

Even though the DS5000 storage subsystem always tries to optimize the layout of the disk arrays, some settings might require a change to optimize the disk usage or the performance.

To change an array's RAID level, from the Storage Manager window, select the array, right-click it, select **Change** → **RAID Level**, and then the desired RAID level, as shown in Figure 3-101.

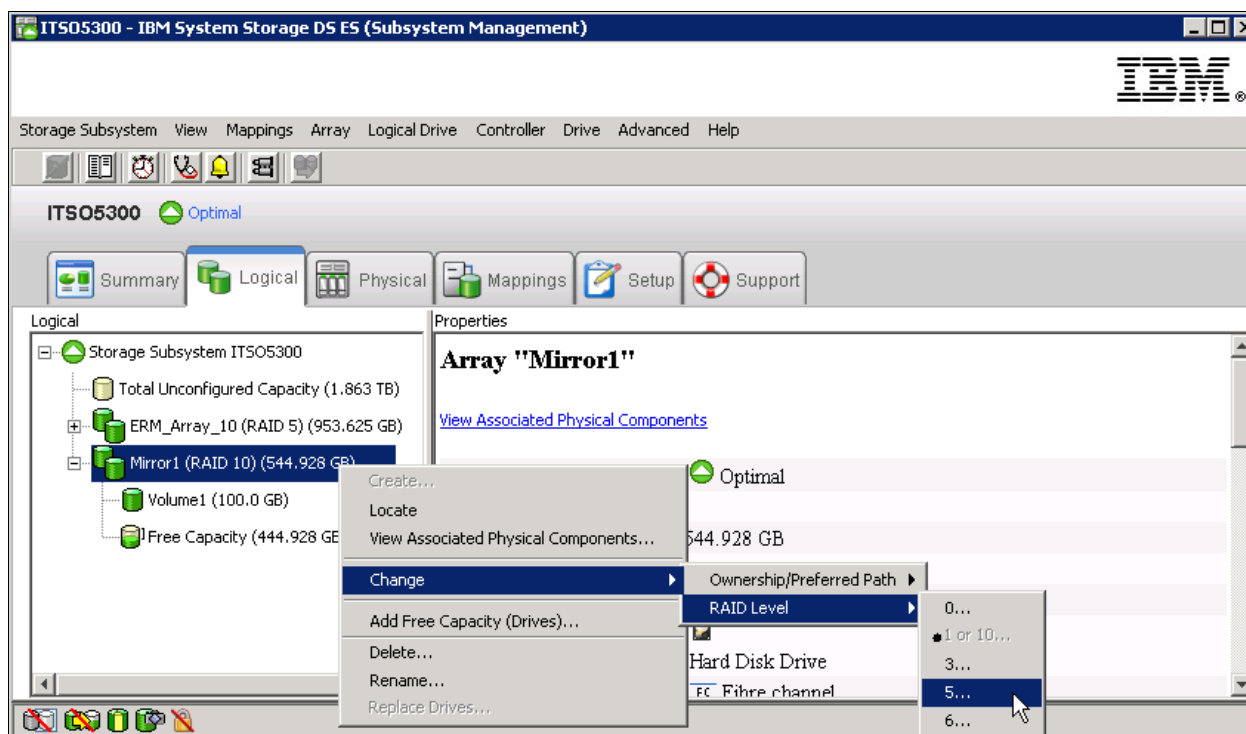


Figure 3-101 Changing RAID level

A confirmation message appears and informs you that the operation cannot be stopped until it is complete. The data remains accessible during this operation, which might take a long time. To check the progress status, select the logical drives in the array being modified, right-click it, and then select **Properties** to display a progress bar for the operation.

3.6.3 Unconfiguring a storage subsystem and arrays

Storage Manager allows the storage subsystem or previously created arrays to be cleared if required.

Clearing the storage subsystem completely removes the complete configuration of the storage subsystem and data, bringing it back to the state when it was initially installed. Information defining all arrays, logical drives, and hot spares are deleted. This feature can be used to create a new configuration on a storage subsystem that already has a configuration defined that is now redundant.

Clearing an array configuration clears logical drives and group configuration in *all* arrays and leaves the remaining subsystem configuration intact.

Warning: In both cases (clearing the storage subsystem or array configuration), data loss occurs. Ensure that a backup of the storage subsystem data as well as the storage subsystem configuration profile is made before attempting these operations.

3.6.4 Performing advanced functions on logical drives (LUNs)

This section details the advanced functions that can be performed on logical drives.

Pre-read redundancy check

RAID arrays are created to provide tolerance against disk failure and errors. To allow recovery from failures, the RAID array stores additional data called redundancy data. This redundancy data can potentially become inconsistent from time to time. Redundancy data is “consistent” if every portion of the redundancy group can be reliably and consistently reconstructed in the event of a failure to the array, and “inconsistent” if it cannot be read or the consistency cannot be verified.

With Storage Manager, a pre-read redundancy check feature is available. The pre-read redundancy feature allows the consistency of redundancy data of a RAID array to be optionally checked prior to returning data for host read requests. The consistency check cannot determine whether the data itself is correct. It does, however, determine that a redundancy consistency error has occurred within the extent of the read command. Once an inconsistency is discovered, an error is reported in the storage subsystem, and no read data is returned, depending on the data inconsistency error.

This feature can be activated on a logical drive basis, which is created as a RAID array that supports redundancy information. The feature allows data verification in environments where data consistency is a key requirement. This feature cannot be enabled for logical drives that do not have any redundancy data.

When a read request is issued to the storage subsystem, the controller verifies that the redundancy group is consistent for the extent of the data specified in the read request. If the controller found that the redundancy group data is in a consistent state, the read request is returned to the host successfully. If the redundancy group data is found to be in an inconsistent state, the read request is returned to the host with a check condition status. The consistency check is only performed for data not already in cache.

In order to verify the consistency of the redundancy group, the entire redundancy group must be read from disk into cache. Should no inconsistency be found, all user data that comprises the redundancy group is left in cache in order to potentially satisfy subsequent cache hits. The data left in cache might include data that is outside the extent of the original read request. Such data does not require a consistency check, because the data is already in cache.

Note: Should a drive associated with an array become degraded, the pre-check feature is disabled.

During the process of verifying the consistency of the redundancy group, a media error or unreadable sector might be encountered within the extent of the redundancy group. When such an error occurs, the RAID controller attempts to perform a reconstruction of the data, using the redundancy information of the data. If this operation is successful, the consistency check indicates that the redundancy group is consistent and the read data is returned to the host.

During the process of verifying the consistency of the redundancy group, an unrecoverable read error might be encountered. When such an error occurs, the consistency check fails. However, the original read request continues to be processed. If the entire extent of the request is still readable, the read data is returned to the host. If some portion of the original read request is unavailable, the read command fails.

In most situations, recovery from an inconsistent redundancy group involves restoring the volume from a backup source.

Note: In a FlashCopy or Enhanced Remote Mirror copy pair relationship, the pre-read redundancy feature is only supported on the source logical drives.

When activating the pre-read redundancy check feature, the media scan feature no longer automatically corrects discovered redundancy group inconsistencies.

Attention: Take care when enabling this feature, as it could have an impact on I/O performance.

To enable this feature, perform these steps:

1. Select the logical drive where the pre-read redundancy check is to be enabled.
2. Select **Logical Drive** → **Change** → **Pre-Read redundancy check**, as shown in Figure 3-102.

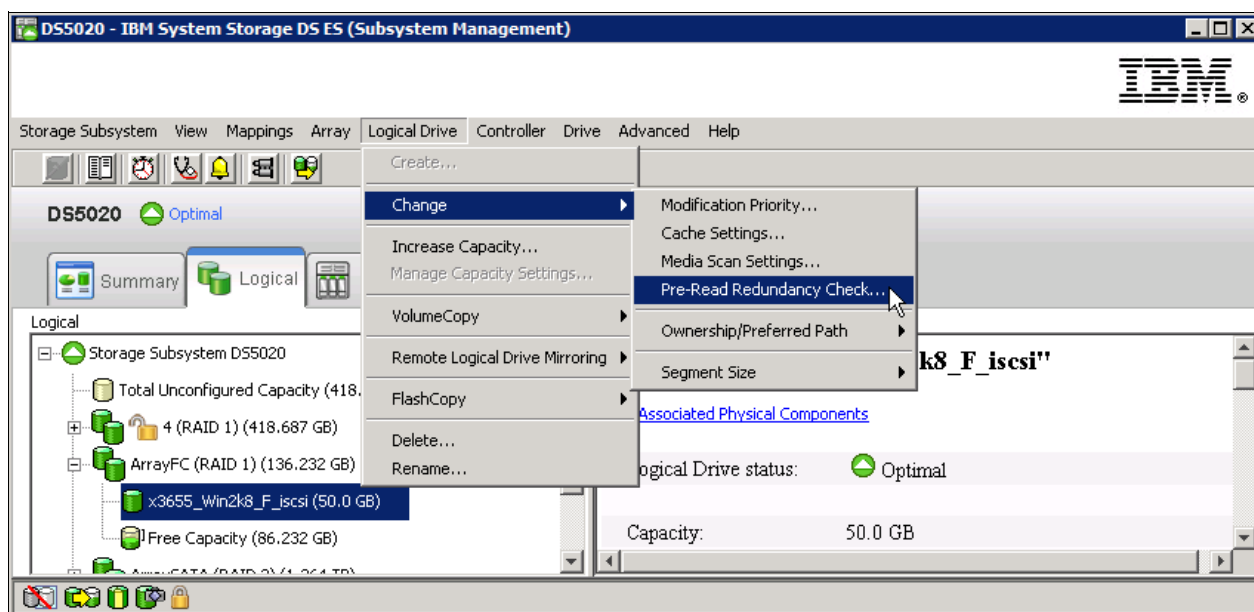


Figure 3-102 Pre-read redundancy check

3. Make sure that the correct logical volume is selected, and click the lower box to enable the value, as shown in Figure 3-103.

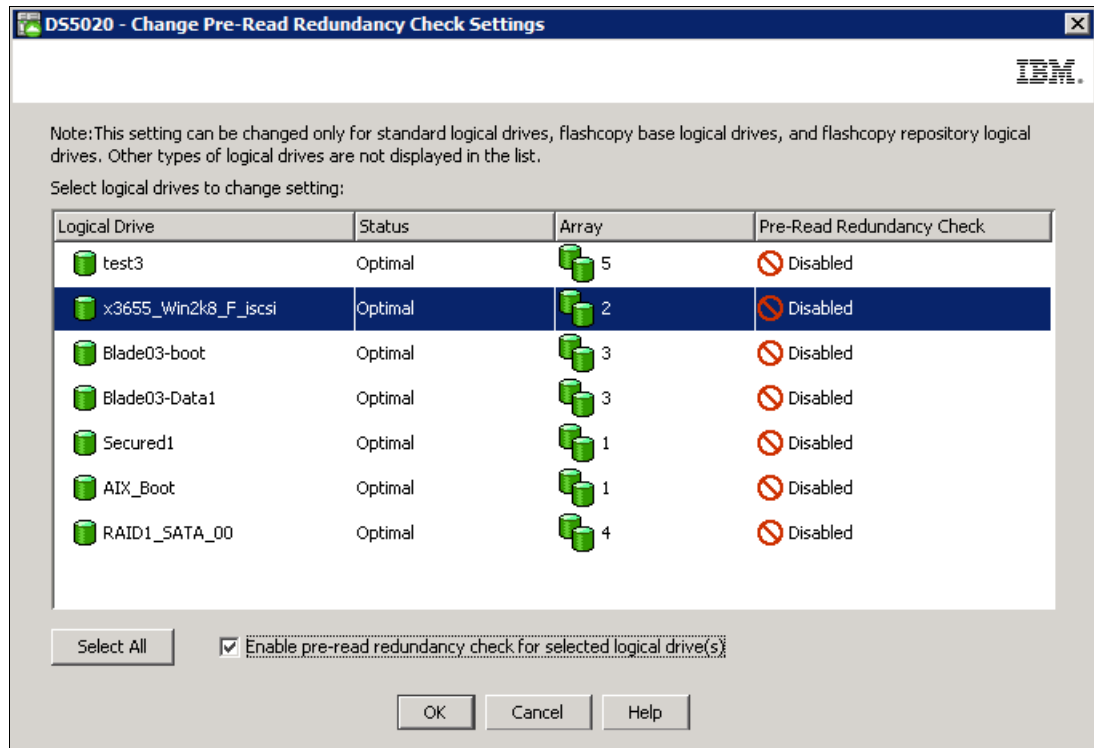


Figure 3-103 Enabling pre-read redundancy check

Expanding logical drives

It is also possible to increase the size of logical drives. This action is called *Dynamic Volume Expansion* (DVE). The capacity of standard logical drives and FlashCopy repository logical drives might be increased using one or both of the following capacities:

- ▶ Free capacity available on the array of the standard or FlashCopy repository logical drive
- ▶ Unconfigured capacity (in the form of unused drives) on the array of the standard or FlashCopy repository logical drive

Increasing the capacity of a FlashCopy repository logical drive does not increase the capacity of the associated FlashCopy logical drive. The FlashCopy logical drive's capacity is always based on the capacity of the base logical drive at the time the FlashCopy is created.

Note: Storage Manager provides support for logical drives greater than 2 TB. This improves the capacity requirement for applications that requires large capacity logical drives.

Note: Increasing the capacity of a standard logical drive is only supported on certain operating systems. If the logical drive capacity is increased on a host operating system that is not supported, the expanded capacity will be unusable and the original logical drive capacity will not be able to be restored.

The operating systems that support a dynamic increase of capacity in a mapped logical drive are:

- ▶ AIX
- ▶ Linux
- ▶ NetWare
- ▶ Windows Dynamic Disks
- ▶ Windows Basic Disks

Tip: If a logical drive-to-LUN mapping has not yet been defined, it is possible to increase the capacity for a standard logical drive on any host operating system, that is, before host system data is placed on the drive.

The storage capacity of a standard logical drive cannot be increased if:

- ▶ One or more hot spare drives are in use in the array that it resides on.
- ▶ The logical drive has *Non-Optimal* status.
- ▶ Any logical drive in the array is in any state of modification.
- ▶ The controller that owns this logical drive is in the process of adding capacity to another logical drive (each controller can add capacity to only one logical drive at a time).
- ▶ No free capacity exists in the array and no unconfigured capacity (in the form of drives) is available to be added to the array.

To increase the logical drive capacity, on the SM Logical/Physical view, highlight the logical drive to be expanded, right-click it, and select **Increase Capacity**. In the Increase Logical Drive Capacity window (Figure 3-104), enter the amount of space by which the logical drive will be enlarged.

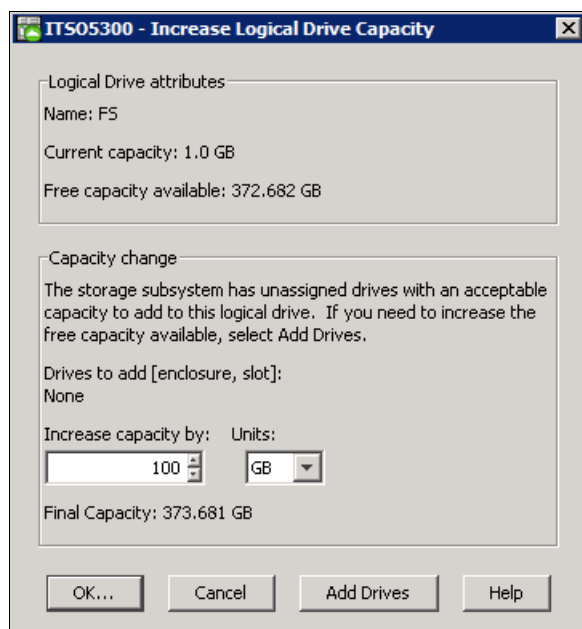


Figure 3-104 Dynamic logical drive expansion

In the top part of the window shown in Figure 3-104, the current size of the logical drive and the available free capacity in the array is displayed. If no free configured space is available, but there are unassigned drives, these can be added from this same window by clicking **Add Drives** before proceeding to enlarge the logical drive. This will perform the same process described in 3.6.1, “Expanding arrays” on page 213.

Note: If the RAID level of the array is 3, 5, or 6, and the drive enclosure has enclosure loss protection, the Add Drives option displays only drives that ensure enclosure loss protection. If the RAID level is 1 or 10, a minimum of two drives must be added.

Click **OK** after selecting the capacity to add. A warning message appears indicating that this operation cannot be stopped after it is started and that it might take a long time to complete. However, the data on the selected logical drive and all other logical drives on this array (if new drives have been added) remains accessible during this time. As with all operations requiring a redistribution of the data on the physical disks, the procedure might affect the performance. From the host operating system, the administrator will then have to perform a procedure in order to utilize the newly allocated space. As an example we will show this procedure for a Windows host below.

Extending a basic disk on a Windows platform

In the following example, we have a Windows 2008 system with a basic disk partition of 1 GB. The partition has data on it, the partition is disk 6, and its drive letter is J. We have used DS5000 Dynamic Volume Expansion (DVE) to expand the logical drive by adding 100 GB. This leaves the operating system with a disk of 101 GB, with a partition of 1 GB and free space of 100 GB, as shown in Figure 3-105.

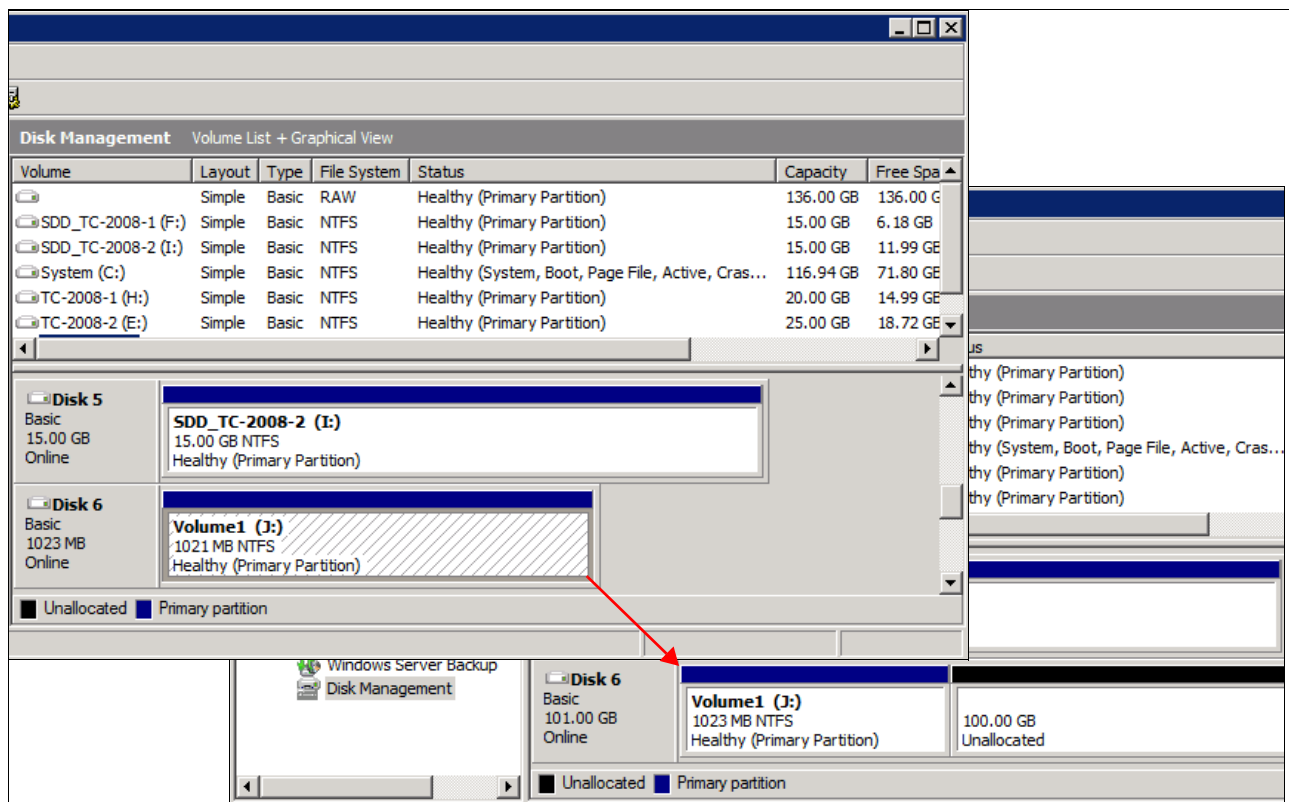


Figure 3-105 The Windows 2008 basic disk with free space

We use the Windows 2008 command-line utility diskpart.exe to extend the original 1021 MB partition to the full size of the disk, as shown in Example 3-2.

Example 3-2 The diskpart utility extends the basic disk in a command window

CMicrosoft DiskPart version 6.0.6002
 Copyright (C) 1999-2007 Microsoft Corporation.
 On computer: TC-W2008

DISKPART> list volume

Volume ###	Ltr	Label	Fs	Type	Size	Status	Info
-----	---	-----	----	-----	-----	-----	-----
Volume 0	D			DVD-ROM	0 B	No Media	
Volume 1	G			DVD-ROM	0 B	No Media	
Volume 2	C	System	NTFS	Partition	117 GB	Healthy	System
Volume 3	H	TC-2008-1	NTFS	Partition	20 GB	Healthy	
Volume 4	E	TC-2008-2	NTFS	Partition	25 GB	Healthy	
Volume 5			RAW	Partition	136 GB	Healthy	
Volume 6	F	SDD_TC-2008	NTFS	Partition	15 GB	Healthy	
Volume 7	I	SDD_TC-2008	NTFS	Partition	15 GB	Healthy	
Volume 8	J	Volume1	NTFS	Partition	1021 MB	Healthy	

DISKPART>

DISKPART> select volume 8

Volume 8 is the selected volume.

DISKPART> extend

DiskPart successfully extended the volume.

DISKPART> list volume

Volume ###	Ltr	Label	Fs	Type	Size	Status	Info
-----	---	-----	----	-----	-----	-----	-----
Volume 0	D			DVD-ROM	0 B	No Media	
Volume 1	G			DVD-ROM	0 B	No Media	
Volume 2	C	System	NTFS	Partition	117 GB	Healthy	System
Volume 3	H	TC-2008-1	NTFS	Partition	20 GB	Healthy	
Volume 4	E	TC-2008-2	NTFS	Partition	25 GB	Healthy	
Volume 5			RAW	Partition	136 GB	Healthy	
Volume 6	F	SDD_TC-2008	NTFS	Partition	15 GB	Healthy	
Volume 7	I	SDD_TC-2008	NTFS	Partition	15 GB	Healthy	
* Volume 8	J	Volume1	NTFS	Partition	101 GB	Healthy	

DISKPART>exit

After diskpart.exe has extended the disk, the partition is now 101 GB. All the data is still intact and usable, as shown in Figure 3-106.

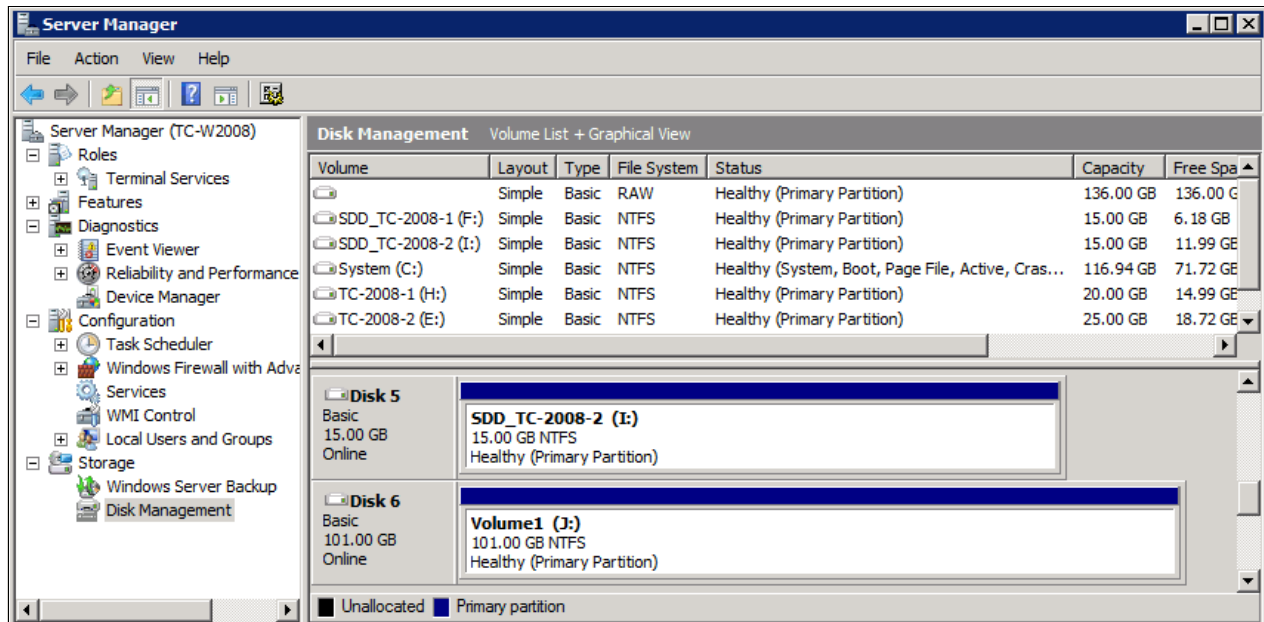


Figure 3-106 Disk Management after diskpart has extended the partition

Notes:

- ▶ The **extend** operation is dynamic.
- ▶ The **extend** command only works on NTFS formatted volumes.
- ▶ Officially, you do not need to stop I/O operations to the disk before you extend. However, keeping I/O operations at a minimum is a best practice.

With dynamic disks, the Disk Management GUI utility can be used to expand logical drives.

3.6.5 Modification priority

The modification priority defines how much processing time is allocated for operations modifying the logical drive relative to the system performance. Operations that cause a logical drive modification are:

- ▶ Initializing a logical drive
- ▶ Reconstructing after a disk failure
- ▶ Copying back from a hot spare drive
- ▶ Changing the segment size of a logical drive
- ▶ Expanding a dynamic logical drive
- ▶ Adding free capacity to an array
- ▶ Defragmenting an array
- ▶ Changing the RAID level of an array

If the logical drive contains critical data, you might prefer a high modification priority to keep the time of a critical state (for example, after losing a disk) as short as possible, even if this affects the system performance during the modification process.

The following modification priority rates are available:

- ▶ Lowest
- ▶ Low
- ▶ Medium
- ▶ High
- ▶ Highest

Note: The lowest priority rate favors system performance, but the modification operation takes longer. The highest priority rate favors the modification operation, but system performance might be compromised.

The progress bar at the bottom of the Logical Drive Properties window displays the progress of a modification operation.

When a storage subsystem logical drive is a primary logical drive and a full synchronization is necessary, the controller owner performs the full synchronization in the background while processing local I/O writes to the primary logical drive and associated remote writes to the secondary logical drive. The full synchronization diverts controller processing resources from I/O activity, where it can impact performance on the host application. The synchronization priority defines how much processing time is allocated for synchronization activities relative to system performance.

The guidelines in Table 3-2 can help determine how long a synchronization can take and how much various synchronization priorities can affect system performance.

Table 3-2 Impact of modification priority on relative time for full synchronization

Modification priority	Relative time
Highest	Fastest possible time
High	Two times longer than fastest possible time
Medium	Three and a half times longer than fastest possible time
Low	Six times longer than fastest possible time
Lowest	Eight times longer than fastest possible time

To change the modification priority, perform the following steps:

1. Select a logical drive, right-click it, and select **Change** → **Modification Priority**, as shown in Figure 3-107.

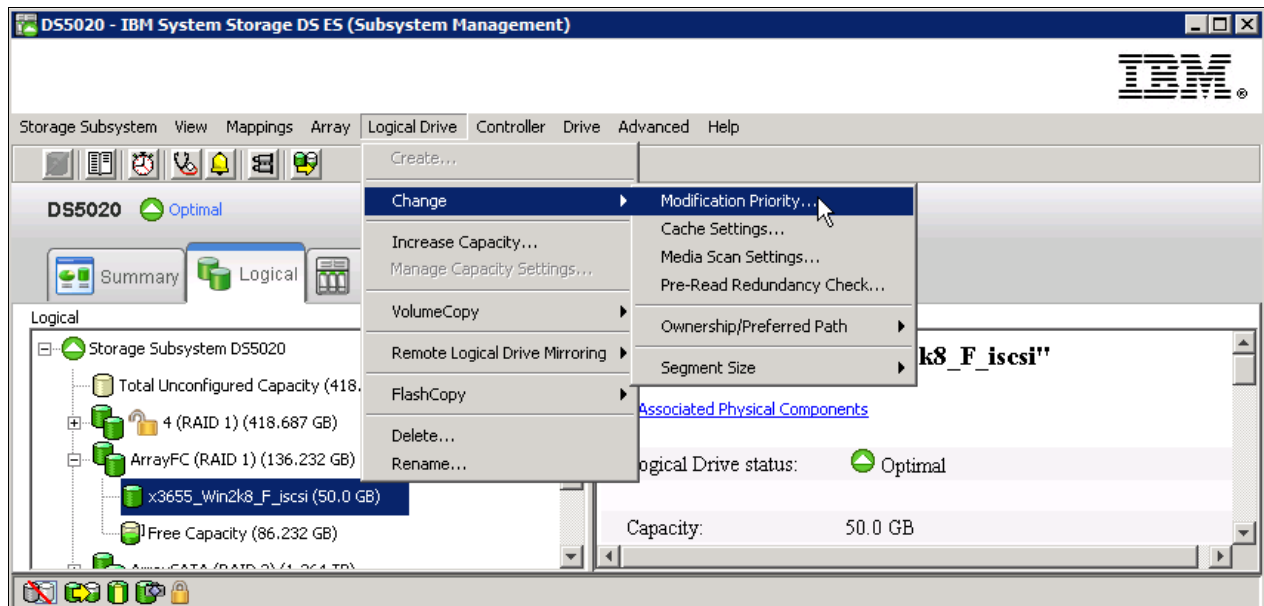


Figure 3-107 Changing the modification priority

2. Make sure that the correct logical drive is selected, and set the new Modification Priority value, as shown in Figure 3-108.

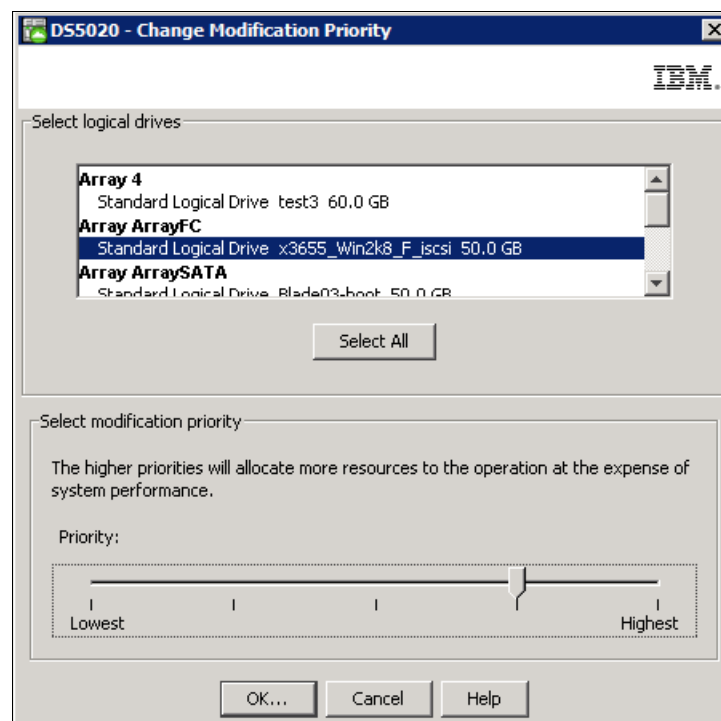


Figure 3-108 Modification priority for a logical drive

If a logical drive modification is in progress, a status bar appears at the bottom of the window, as shown in Figure 3-109.

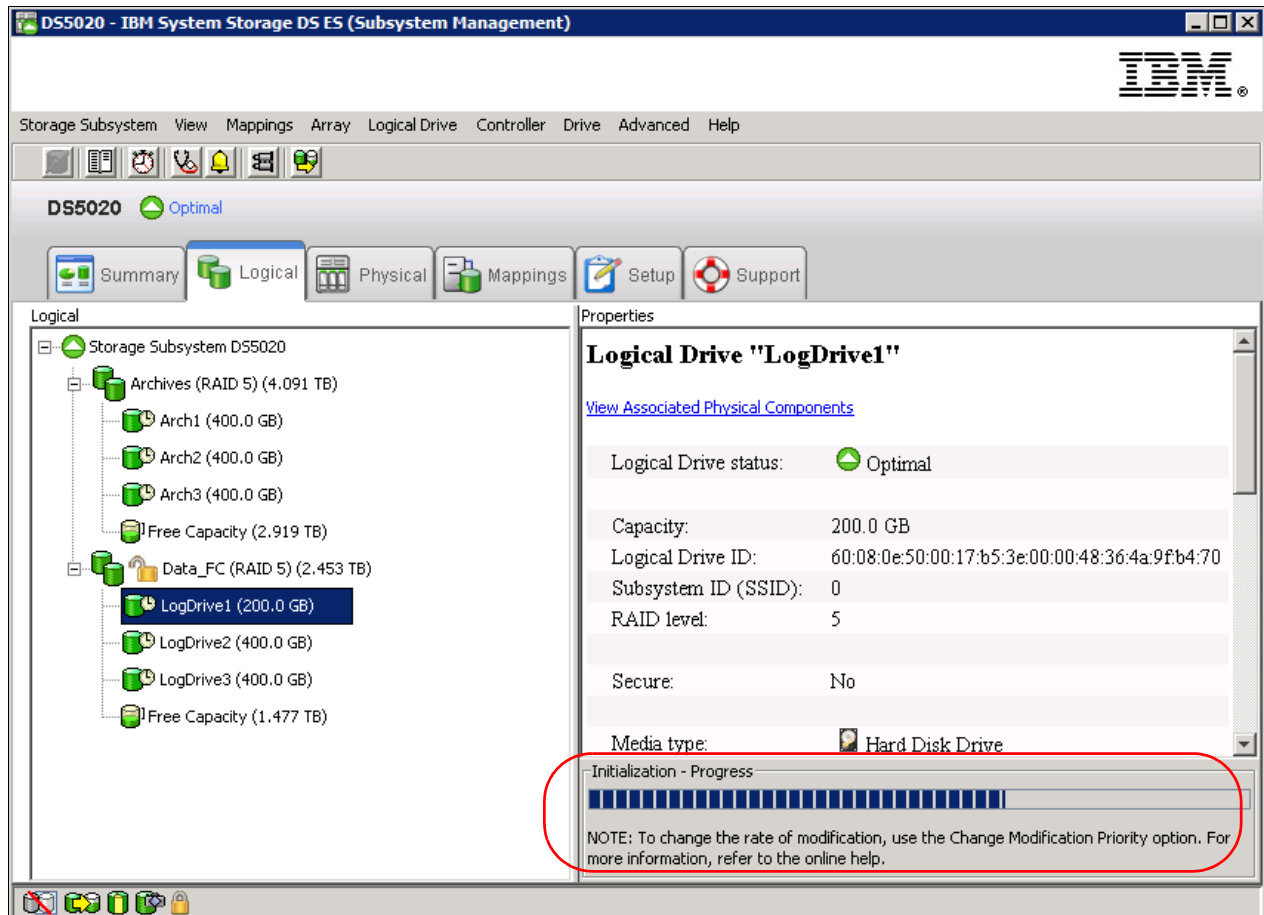


Figure 3-109 Modification progress

3.6.6 Controller ownership

Each logical drive has a preferred controller of ownership. This controller normally handles all I/O requests for this particular logical drive. In other words, each logical drive is owned by one and only one controller. The alternate controller only takes over and handles the I/O requests in case of a failure along the I/O path, for example, a defective host bus adapter or switch. When defining logical drives, the system normally alternates ownership between the two controllers as they are defined.

Situations can occur when all heavily stressed logical drives can reside on only one controller and the other one handles only a small amount of all I/O requests. To balance the workload between the controllers, the preferred ownership of a logical drive can be changed to the other controller.

Important: Be sure that the operating system using the logical drive uses a multipath I/O driver; otherwise, it loses access to the logical drive.

Balancing traffic is unfortunately not always a trivial task. For example, if an application requires large disk space to be located and accessed in one chunk, it becomes harder to balance traffic by spreading the smaller volumes among controllers.

In addition, typically, the load across controllers and logical drives are constantly changing. The logical drives and data can be accessed at any given time depending on which applications and users are active during that time period, which is why monitoring the system is important.

The Performance Monitor provides data that is useful for monitoring the I/O activity of a specific controller and a specific logical drive, which can help identify possible high-traffic I/O areas. Identify actual I/O patterns in the individual logical drives and compare them with the expectations for an application. If a particular controller has considerably more I/O activity, consider moving logical drives to the other controller in the storage subsystem.

A disparity in the total I/Os (workload) of controllers might be noticed. For example, the workload of one controller is heavy or is increasing over time, and that of the other controller is lighter or more stable. In this case, consider changing the controller ownership of one or more logical drives to the controller with the lighter workload.

Tip: Here are some guidelines for logical drives assignment and storage partitioning:

- ▶ Assign defined logical drives evenly across all controllers to balance controller utilization.
- ▶ Use the manual method of creating logical drives. This allows for greater flexibility of configuration settings, such as enclosure loss protection and utilizing both drive loops.
- ▶ If some logical drives are highly utilized, where possible, separate them by putting them on their own or another array. This will reduce disk contention for that array.

If the preferred controller is undergoing a firmware download, ownership of the logical drives is automatically shifted to the other controller, and that controller becomes the current owner of the logical drives. If the preferred controller has to be replaced, the controller should be disabled first. This will intentionally cause a failover of LUNs to the other controller and allow the removal and replacement of the preferred controller. This is considered a routine ownership change and is reported with an informational entry in the event log.

There can also be a forced failover from the preferred controller to the other controller because of I/O path errors. This is reported with a critical entry in the event log, and will be reported by the Enterprise Management software to e-mail and SNMP alert destinations.

Consideration: A secondary logical drive in a Remote Mirror does not have a preferred owner. Instead, the ownership of the secondary logical drive is determined by the controller owner of the associated primary logical drive. For example, if controller A owns the primary logical drive in the primary storage subsystem, then controller A owns the associated secondary logical drive in the secondary storage subsystem. Changing the controller ownership of the primary logical drive causes a corresponding controller ownership change of the secondary logical drive.

To change the preferred ownership from one controller to the other, highlight the logical drive, right-click, and select **Change → Ownership/Preferred Path**. Then select the controller to which the logical drive is to be moved. Depending on the current workload, the operation can take a while to finish.

3.6.7 Cache parameters

The Storage Manager utility enables various cache settings to be configured:

- ▶ Specify the DS5000 system wide settings:
 - Start and stop cache flushing levels (this setting will affect all arrays and logical drives created on the system)
 - Cache Block size
- ▶ Specify settings per logical drive:
 - Read caching
 - Cache read-ahead multiplier
 - Write caching or write-through mode (write caching disabled)
 - Enable or disable write cache mirroring

Figure 3-110 shows the typical values when using the Create Logical Drive Wizard. With the Storage Manager, cache settings can be specified for each logical drive independently, giving greater flexibility.

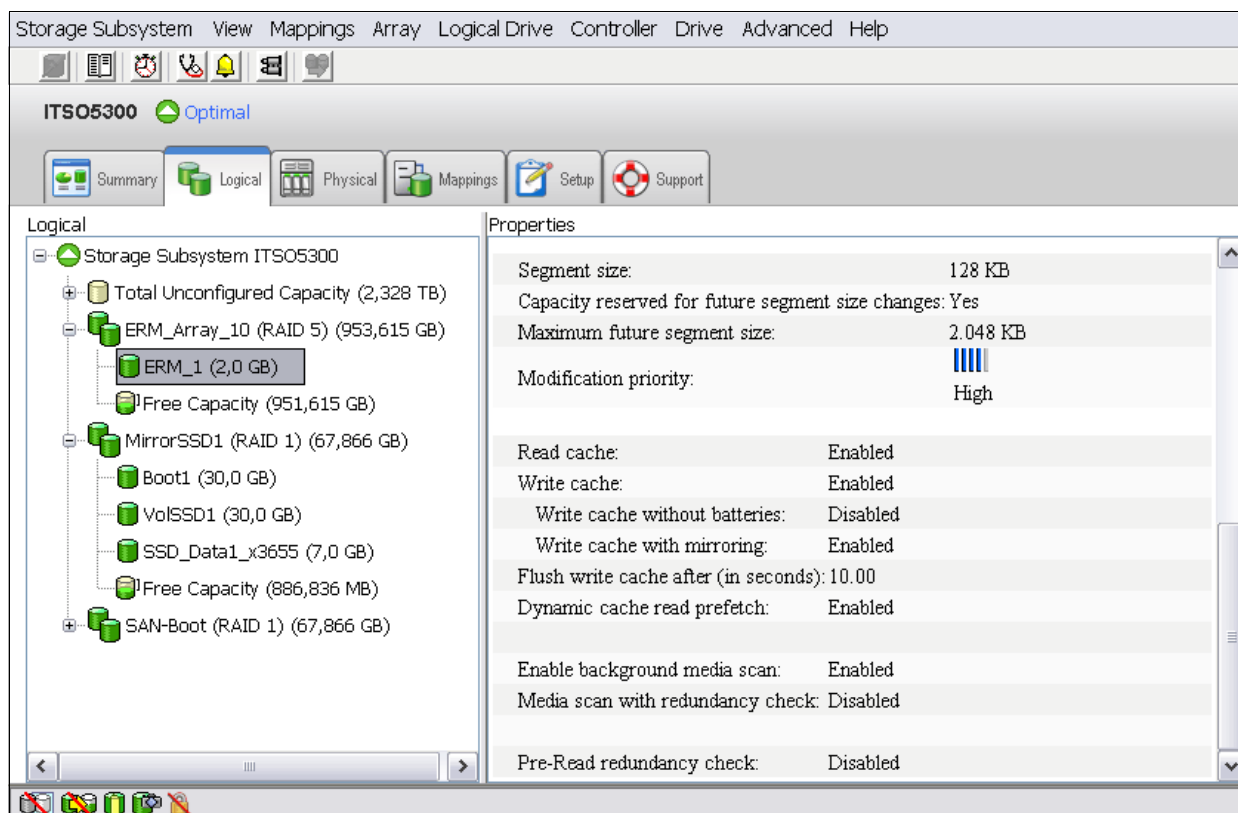


Figure 3-110 Default values used by the Create Logical Drive Wizard

Note: We recommend that the values are manually set during creation to suit the expected performance needs of the logical drive. These settings can be changed after logical drive creation for tuning purposes.

3.6.8 Logical drive

To locate this setting, highlight the logical drive in the Storage Manager menu and select **Logical Drive** → **Change** → **Cache Settings....** The window shown in Figure 3-111 will appear.

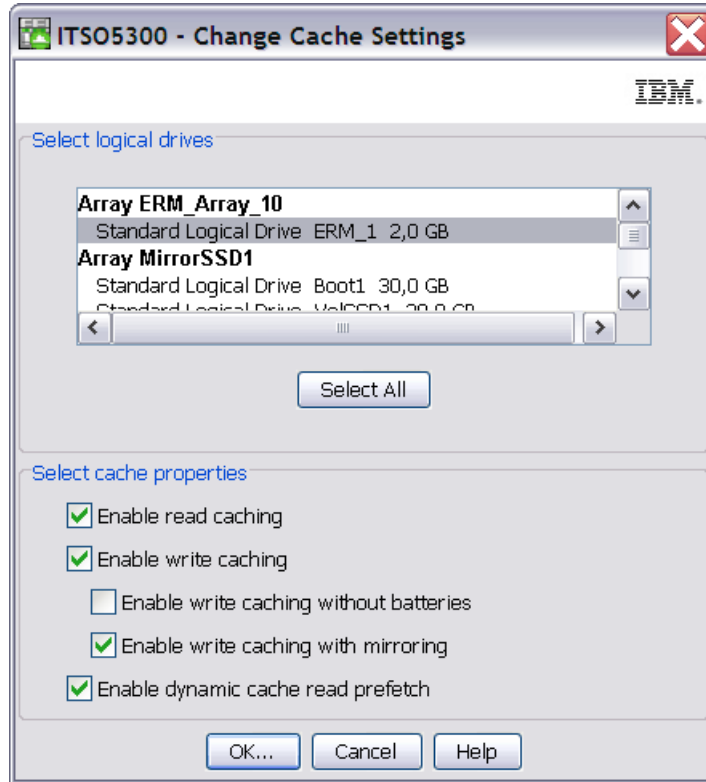


Figure 3-111 Logical drive changes to cache settings

These settings have a large impact on the performance of the DS5000 storage subsystem and on the availability of data. Be aware that performance and availability often conflict with each other. If maximum performance is required, in most cases availability might have to be compromised and vice versa.

The default settings are read and write cache for all logical drives, with cache mirroring to the alternate controller for all write data. The write cache is only used if the battery for the controller is fully charged. Read ahead is not normally used on the logical drives.

Read caching

Read caching allows read operations from the host to be stored in controller cache memory. If a host requests data that is not in the cache, the controller reads the needed data blocks from the disk and places them in the cache. Until the cache is flushed, any other requests for this data are fulfilled with the cache data instead of initiating another read operation to the disk.

Write caching

The write caching parameter enables the storage subsystem to cache write data instead of writing it directly to the disks. This can improve performance significantly, especially for environments with random writes, such as databases. For sequential writes, the performance gain varies with the size of the data written. If the logical drive is only used for read access, it

might improve overall performance to disable the write cache for this logical drive, and no cache memory is reserved for the logical drive.

Write cache mirroring

The DS5000 storage subsystem write cache mirroring provides the integrity of cached data if a RAID controller fails. This is excellent from a high availability perspective, but it decreases performance. The data is mirrored between controllers across dedicated PCI Express buses. We recommend that the controller write cache mirroring be left enabled for data integrity reasons in case of a controller failure.

By default, a write cache is always mirrored to the other controller to ensure proper contents, even if the logical drive moves to the other controller. Otherwise, the data of the logical drive can be corrupted if the logical drive is shifted to the other controller and the cache still contains unwritten data. If you turn off this parameter, you risk data loss in the case of a controller failover, which might also be caused by a path failure in your fabric.

The cache of the DS5000 storage subsystem is protected by a battery against power loss. If the batteries are not fully charged, for example, just after powering on, the controllers automatically disable the write cache. If you enable the parameter, the write cache is used, even if no battery backup is available, resulting in a higher risk of data loss.

Write caching or write-through

Write-through means that writing operations do not use cache at all. The data is always going to be written directly to the disk drives. Disabling write caching frees up cache for reading (because the cache is shared for read and write operations).

Write caching can increase the performance of write operations. The data is not written straight to the disk drives; it is only written to the cache. From an application perspective, this is much faster than waiting for the disk write operation to complete. Therefore, a significant gain in application writing performance can be expected. It is the responsibility of the cache controller to eventually flush the unwritten cache entries to the disk drives.

Write cache mode appears to be faster than write-through mode, because it increases the performance of both reads and writes. But this is not always true, because it depends on the disk access pattern and workload.

A lightly loaded disk subsystem usually works faster in write-cache mode, but when the workload is high, the write cache can become inefficient. As soon as the data is written to the cache, it has to be flushed to the disks in order to make room for new data arriving into cache. The controller performs faster if the data goes directly to the disks. In this case, writing data to the cache is an unnecessary step that decreases throughput.

Dynamic cache read prefetch

Cache read-ahead, or “prefetch,” allows the controller, while it is reading and copying host-requested data blocks from disk into the cache, to copy additional data blocks into the cache. This increases the chance that a future request for data will be fulfilled from the cache. Cache read-ahead is important for multimedia applications that use sequential I/O.

This feature uses an automatic pre-fetching multiplier to maximize its cache hit efficiency and system performance. This will turn on monitoring of the I/O to the logical drive and enable the new algorithm to dynamically choose how much to read ahead. This simplifies the process for the administrator, as there is no need to manually set a specific value for the read ahead multiplier. The system will tune itself depending on the I/O characteristics. When sequential access is detected, the controller will automatically start using read ahead buffering. When random or non-sequential I/O is used, then it will stop using the read ahead buffer. To disable

this feature, simply uncheck the **Dynamic Cache Read Prefetch** check box for the relevant logical drive.

3.6.9 Storage subsystem Cache settings

The storage subsystem parameters are settings that impact all of the array and LUN usage of the user cache space on the DS5000. These settings should be configured and set to best support the most critical applications to your entire solution. These two settings affect the way the cache controller handles unwritten cache entries. They are only effective when the write-back cache policy is configured.

Cache flush Settings

Writing the unwritten cache entries to the disk drives is called *flushing*. The start and stop flushing level values can be configured, as shown in Figure 3-112. They are expressed as percentages of the entire cache capacity. When the number of unwritten cache entries reaches the start flushing value, the controller begins to flush the cache (write the entries to the disk drives). The flushing stops when the number of unwritten entries drops below the stop flush value. The controller always flushes the oldest cache entries first. Unwritten cache entries older than 20 seconds are flushed automatically.

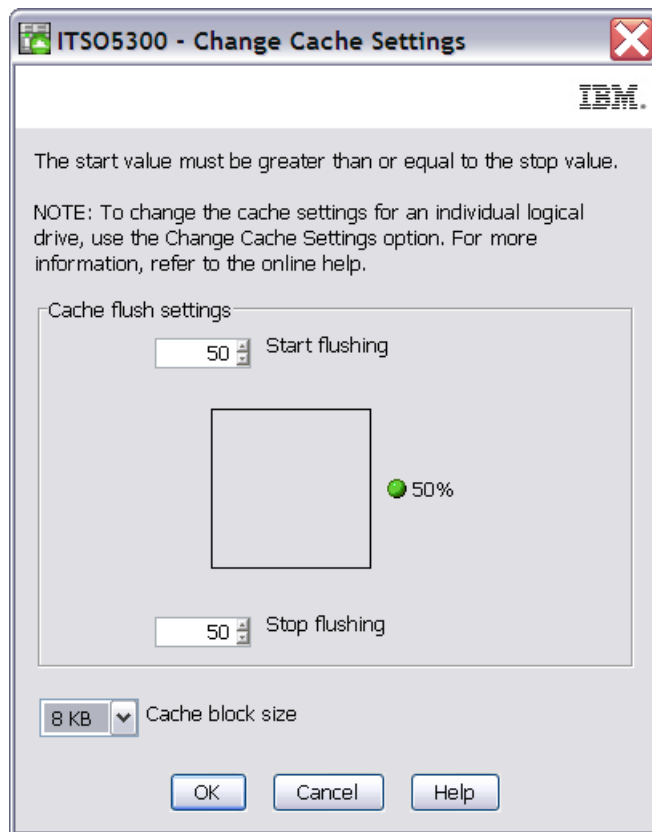


Figure 3-112 Storage subsystem cache settings

The default is the start flushing level and the stop flushing level is set to 80%. This means that the cache controller does not allow more than 80% of the entire cache size for write-back cache, but it also tries to keep as much of it as possible for this purpose. If such settings are used, a high number of unwritten entries in the cache is expected. This is good for writing performance, but be aware that it offers less data protection.

Performance tests have shown that it is a good idea to use similar values for start and stop flushing levels. If the stop level value is significantly lower than the start value, this causes a high amount of disk traffic when flushing the cache. If the values are similar, then the controller only flushes the amount needed to stay within limits.

Note: In our experience, a start flushing level of 50% and a stop flushing level of 50% is best for customer environments.

To locate this setting, highlight the logical drive in the Storage Manager menu and select **Storage Subsystem** → **Change** → **Cache Settings**....

Cache block size

This is the size of the cache memory allocation unit and can be either 4 K, 8 K, 16 K, or 32 K. This provides more flexibility in managing and customizing your cache setup on the DS5000 storage subsystem, based on specific requirements. By selecting the proper value for a particular situation, improvements can be seen in caching efficiency and performance. For example, if applications mostly access the data in small blocks up to 8 K, but a 16 K for cache block size is used, then each cache entry block is only partially populated. Blocks will always occupy 16 K in cache to store 8 K (or less) of data. This means only up to 50% of cache capacity is effectively used to store the data. This inefficiency lowers the performance. For random workloads and small data transfer sizes, 4 K is better.

Alternatively, if the workload is sequential and a large segment size is used, as is the case with multimedia applications, it is better to use the larger cache block sizes of 16 or 32 K. A larger block size means a lower number of cache blocks and reduces cache delays. In addition, a larger cache block size requires fewer cache data transfers to handle the same amount of data.

3.6.10 Media scan

Media scan is a background process enabled by default that checks logical drives over hard disk drives for defects by reading the raw data from the disk and writing it back. This detects possible problems caused by bad sectors of the physical disks before they could eventually disrupt normal data reads or writes. This process is sometimes known as *data scrubbing*.

Important: Media scan is an option available for logical drive space configured on hard disk drives, not over Solid State Drives. Unused hard disks or hot spares are not scanned.

The media scan runs on all logical drives in the storage subsystem that meet the following conditions:

1. The logical drive is in an optimal status.
2. The logical drive is not defined over Solid State Drives.
3. There are no modification operations in progress.
4. The Media Scan parameter is enabled.

The media scan continuously runs in the background, using spare cycles to complete its work. The default media scan is for a scan every 30 days, that is, the maximum time the media scan has to complete the task. During the scan process, the DS5000 storage subsystem calculates how much longer the scan process will take to complete, and adjusts the priority of the scan to ensure that the scan completes within the time setting allocated. Once the media scan has completed, it starts over again and resets its time for completion to the current setting. This media scan setting can be reduced. However, if the setting is too low,

priority is given to the media scan over host activity to ensure that the scan completes in the allocated time. This scan can impact performance, but will improve data integrity in the long term.

The media scan is enabled for the entire storage subsystem. The system-wide enabling specifies the duration over which the media scan runs, which by default is 30 days. By default, the media scan process runs without checking redundancy data. You can optionally specify whether to do a redundancy check or to stop media scan.

A media scan can be considered a surface scan of the hard drives, and a redundancy check scans the blocks of a RAID 3, 5, or 6 logical drive and compares it against the redundancy data. In the case of a RAID 1 logical drive, the redundancy scan compares blocks between copies on mirrored drives.

Note: A media scan is only capable of resolving media errors and data or parity mismatches. A media scan does not attempt to resolve any other sort of error occurring during I/O operations.

We have seen no effect on I/O when we use a 30-day setting unless the processor is utilized in excess of 95%. The length of time that it takes to scan the logical drives depends on the capacity of all the logical drives on the system and the utilization of the controller.

Important: The media scan must be enabled for the entire storage subsystem and enabled on each logical drive within the storage subsystem to protect the logical drive from failure due to media errors. This is the default and recommended configuration.

Table 3-3 shows the errors and describes several of the actions that the DS5000 storage subsystem takes as a result of a media scan and redundancy check operations.

Table 3-3 Media scan errors

Reported error	Description	Result
Unrecovered media error	The data cannot be read on its first attempt, or on any subsequent retries.	With redundancy check: Data is reconstructed and scanned again. Without redundancy check: No error correction.
Recovered media error	The drive cannot read the requested data on its first attempt, but succeeded on a subsequent attempt.	Data is written to drive and verified.
Redundancy mismatches	Redundancy errors are found.	The first 10 redundancy mismatches found on a logical drive are reported. Operating system data checking operations should be executed.
Unfixable error	The data cannot be read, and parity or redundancy information cannot be used to regenerate it.	An error is reported.

To locate this setting, highlight the logical drive in the Storage Manager menu and select **Storage Subsystem** → **Change** → **Media Scan Settings**. The window shown in Figure 3-113 opens.

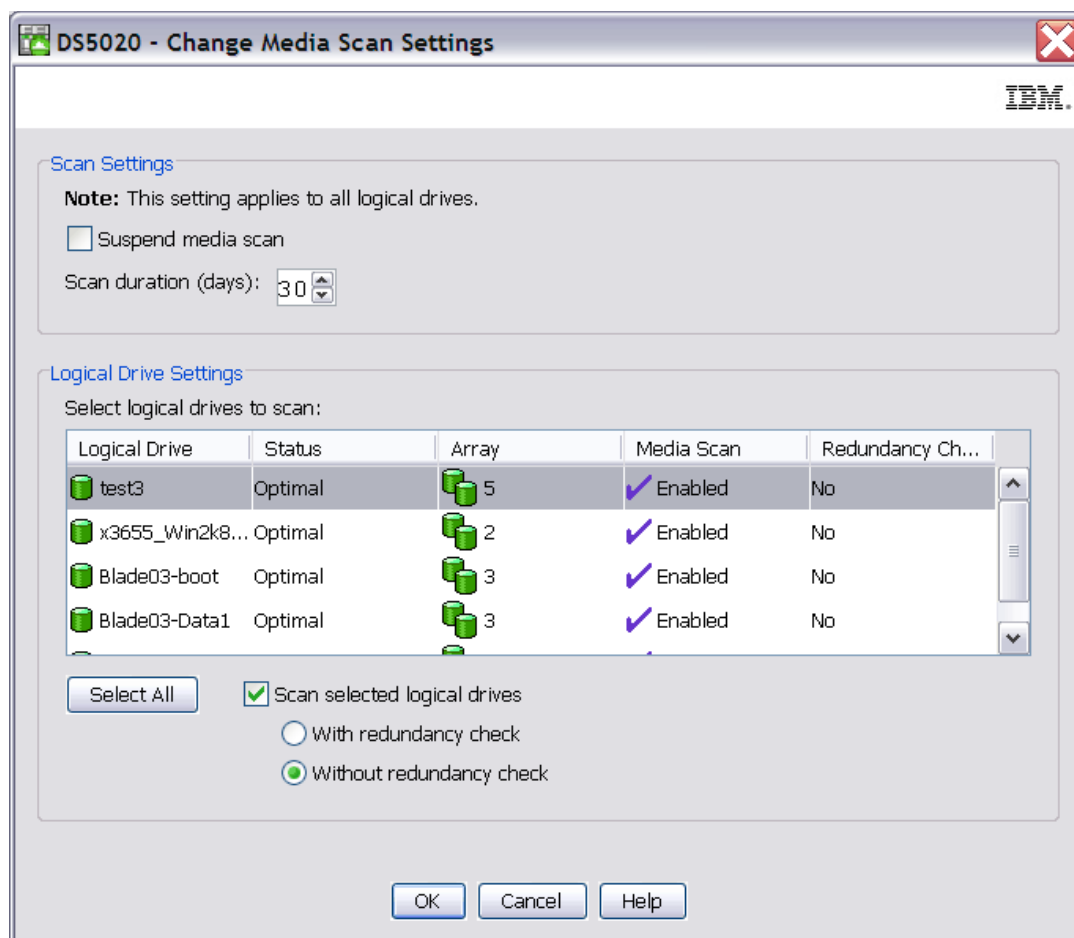


Figure 3-113 Media scan settings for storage subsystem

3.6.11 Failover alert delay

Storage Manager provides alert notification on ADT-induced logical drive ownership changes. The logical drive transfer alert notification is issued for any instance of a logical drive owned by a non-preferred controller, whether ADT is enabled or not, and is in addition to any informational or critical event already logged within the ADT or RDAC context.

A failover alert delay can be specified that lets you delay the logging of a critical event if the multipath driver transfers logical drives to the non-preferred controller. If the multipath driver transfers the logical drives back to the preferred controller within the specified delay period, no critical event is logged. If the transfer exceeds this delay period, then a logical drive-not-on-preferred-path alert is issued as a critical event. This option also can be used to minimize multiple alerts when many logical drives fail over because of a system error, such as a failed host adapter.

Attention: Whenever a logical drive not-on-preferred-path condition occurs, only the alert notification is delayed. A needs attention condition is raised immediately.

To make the best use of this feature, set the failover alert delay period such that the host driver failback monitor runs at least once during the alert delay period. Note that a logical drive ownership change might persist through the alert delay period, but correct itself before you can inspect the situation. In such a case, a logical drive-not-on-preferred-path alert is issued as a critical event, but the array will no longer be in a needs-attention state.

Important:

- ▶ The failover alert delay option operates at the storage subsystem level, so one setting applies to all logical drives.
- ▶ The failover alert delay option is reported in minutes in the storage subsystem profile as a storage subsystem property.
- ▶ The default failover alert delay interval is five minutes. The delay period can be set within a range of 0 to 60 minutes. Setting the alert delay to a value of zero results in instant notification of a logical drive not on the preferred path. A value of zero does not mean alert notification is disabled.
- ▶ The failover alert delay is activated after controller start-of-day completes to determine if all logical drives were restored during the start-of-day operation. Thus, the earliest that the not-on-preferred path alert will be generated is after boot up and the configured failover alert delay time.

To change this setting, from the Subsystem Management window, select **Storage Subsystem** → **Change** → **Failover Alert Delay**. The window shown in Figure 3-114 opens.



Figure 3-114 Storage subsystem failover alert delay

3.7 Removing logical drives and arrays

After building your storage solution there are times that may arise where you may want to delete a logical drive or array to reconfigure the space for new needs that have arose. This section will show the steps needed to walk through this process. We will use as an example logical drive and array a secure array so we can also discuss the additional steps needed to perform these functions when using full disk encryption (FDE) drives with secure data feature enabled.

3.7.1 Deleting logical drives

You can delete logical drives from the DS500 Storage subsystem to allow for reconfiguring your space in a different configuration. To delete a logical drive you need to follow these steps:

1. Select the logical drive, right click and select **Delete** as shown in Figure 3-115.

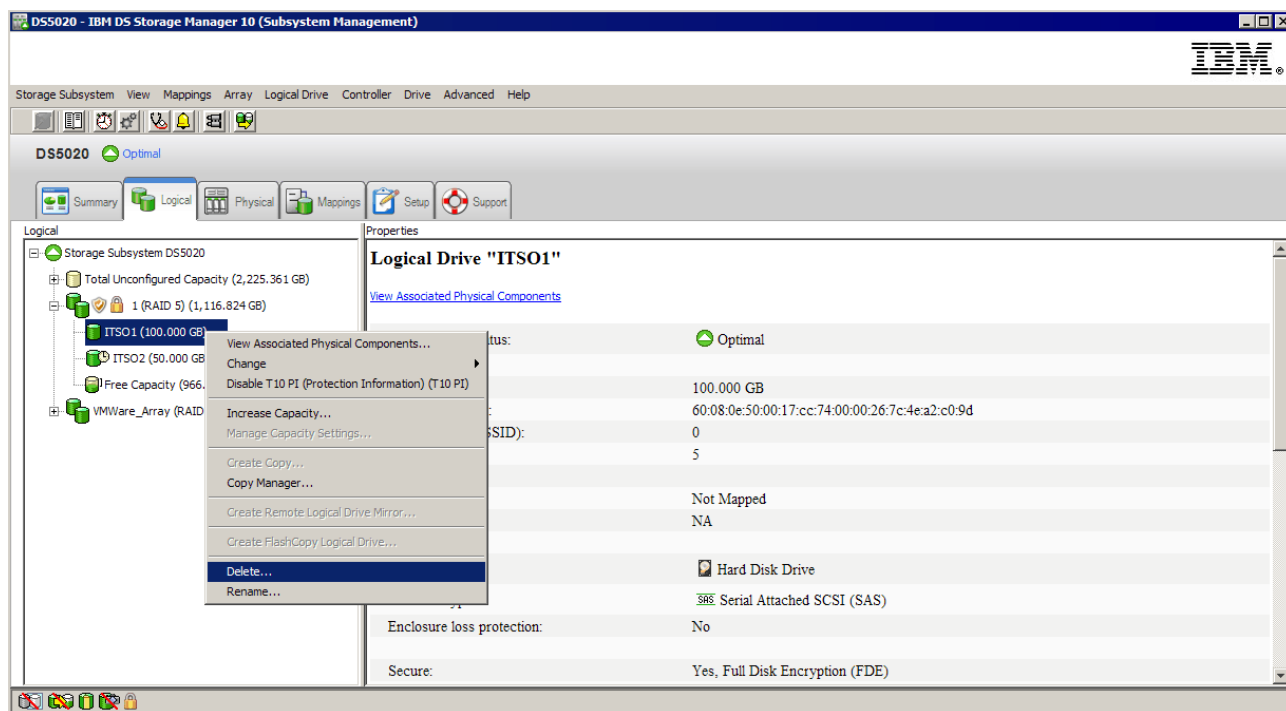


Figure 3-115 Selecting a logical drive to delete

2. This will open the Delete LUN selection screen as shown in Figure 3-116. Select the logical drive or drives you wish to delete.

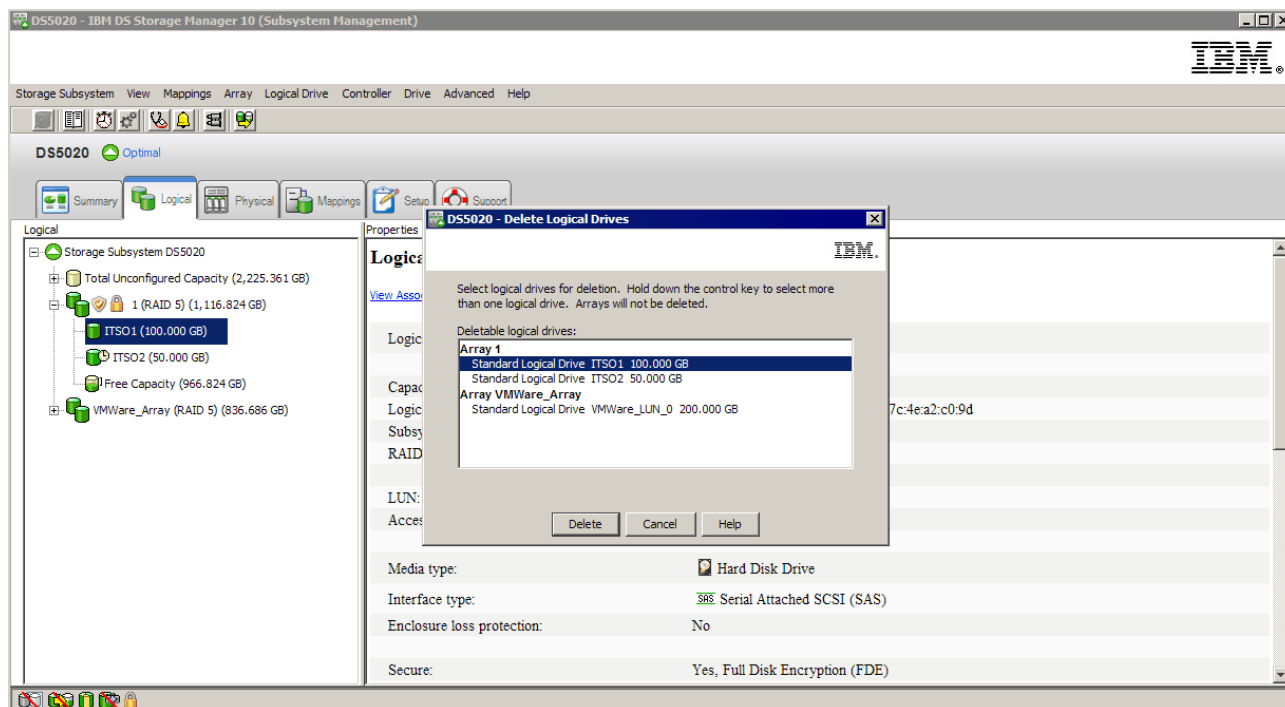


Figure 3-116 Selecting all logical drives to be deleted

- Now confirm your action to delete the logical drives selected by typing “yes” into the box as shown in Figure 3-117.

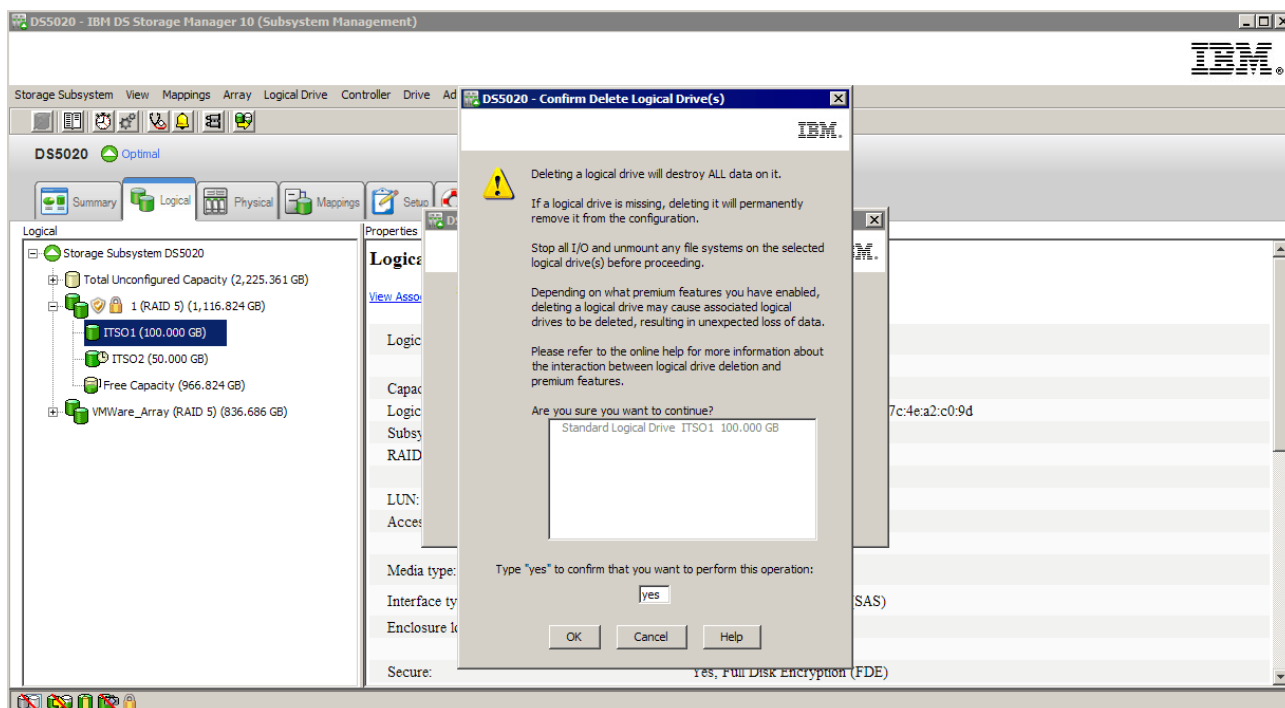


Figure 3-117 Confirm the selection to be deleted

- When deletion is complete window is displayed as shown in Figure 3-118; select “OK”.

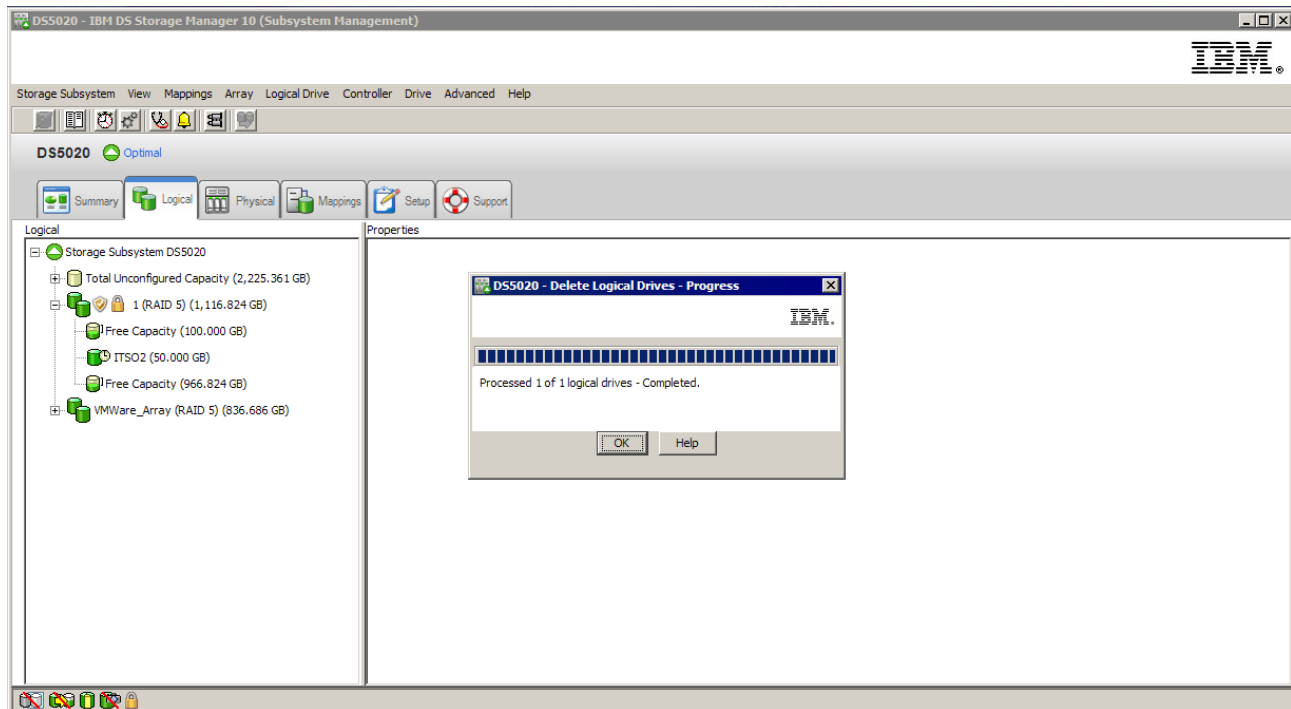


Figure 3-118 Task completed screen

When you delete a logical drive, the capacity of the logical drive becomes an additional free capacity and remains as a separate piece as also shown in Figure 3-119.

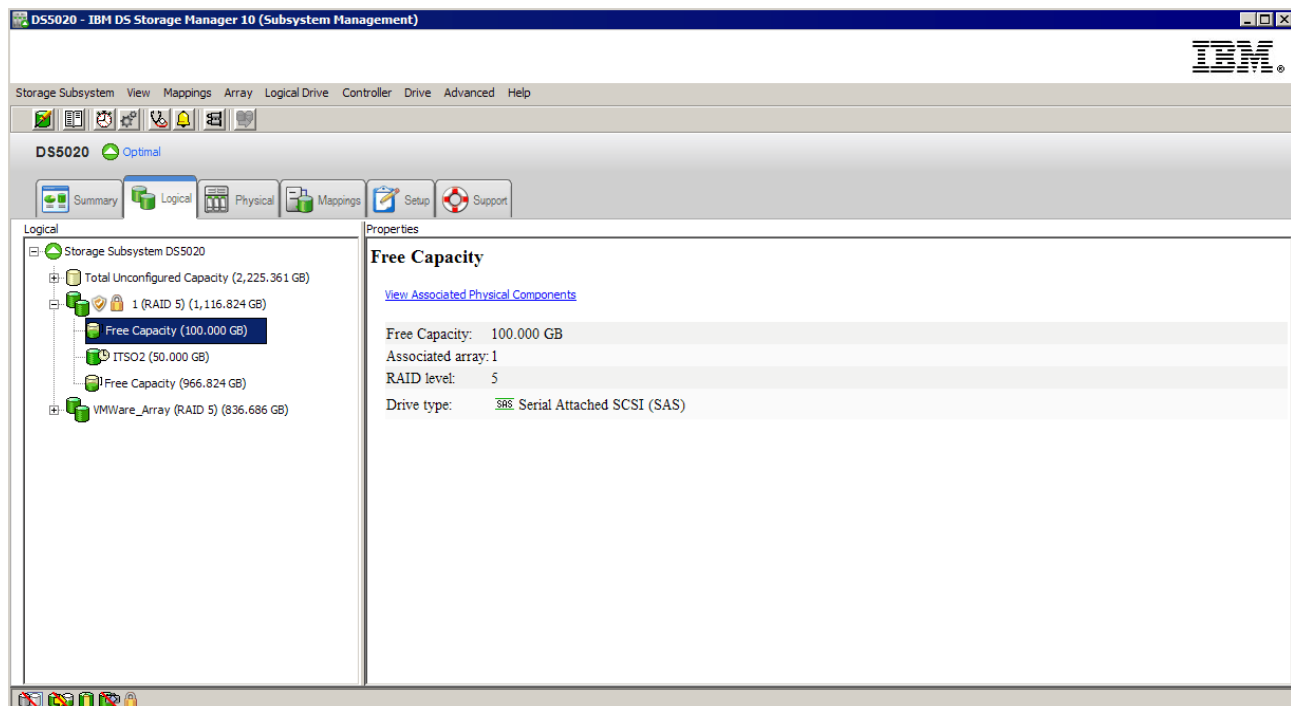


Figure 3-119 Additional free space results from deleting the logical drive

This free space can be used to create a new logical drive of equal or smaller size than this free space. By defragmenting the array all free space parts can be combined into one

creating a single free space of the totals and eliminating these smaller free capacity islands. See 3.7.2, “Defragmenting an array” on page 239 for more information on this procedure.

3.7.2 Defragmenting an array

A logical drive can be deleted anytime to free the space in the array. The free space might be fragmented within the array in different free space nodes.

New logical drives cannot spread across several free space nodes, so the logical drive size is limited to the greatest free space node available, even if there is more free space in the logical drive. The array needs to be defragmented first to consolidate all free space nodes to one free space node for the array. Then, all new logical drives can use the whole available free space.

To accomplish this task, open the Subsystem Management window, highlight the array to defragment, and select **Advanced** → **Recovery** → **Defragment Array** to start the procedure, as shown in Figure 3-120.

The defragmentation can run concurrently with normal I/O, but it impacts performance because the data of the logical drives must be moved within the array. Depending on the array configuration, this process continues to run for a long period of time. Once the procedure is started, it cannot be stopped again. During this time, no configuration changes can be performed on the array.

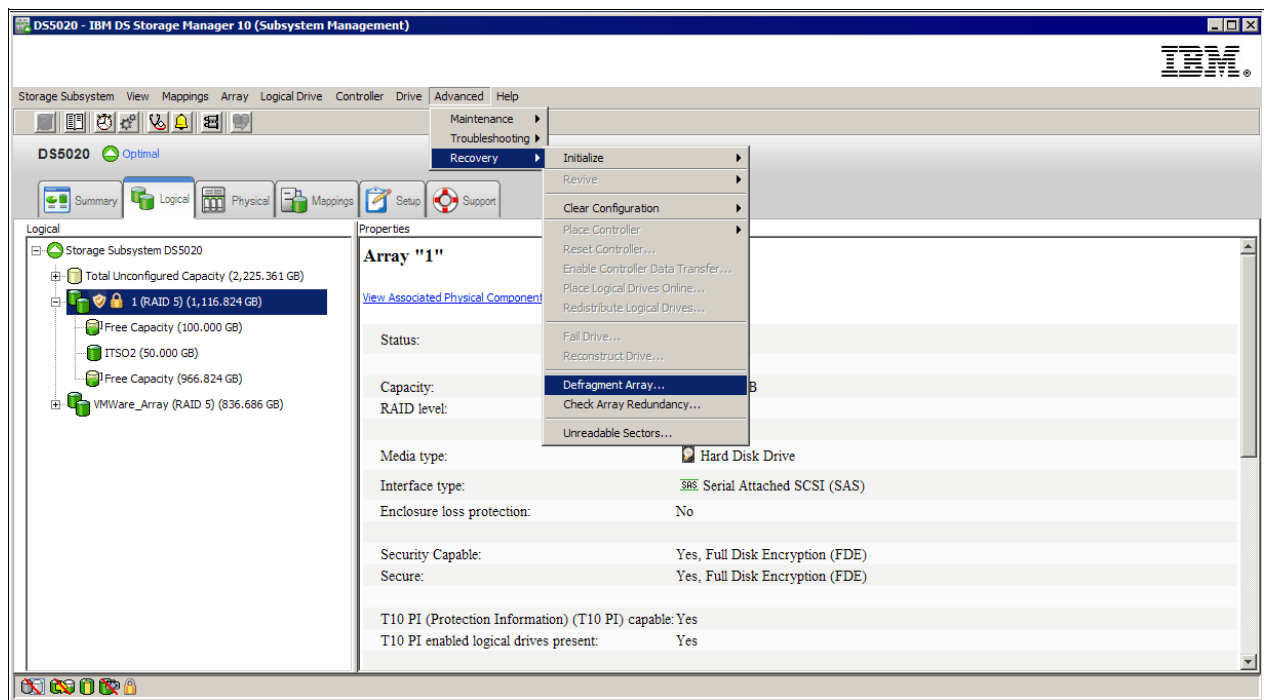


Figure 3-120 Defragment an array

The defragmentation done on the DS5000 storage subsystem only applies to the free capacity nodes on the array as shown in Figure 3-121. It is not connected to a defragmentation of the file system used by the host operating systems in any way.

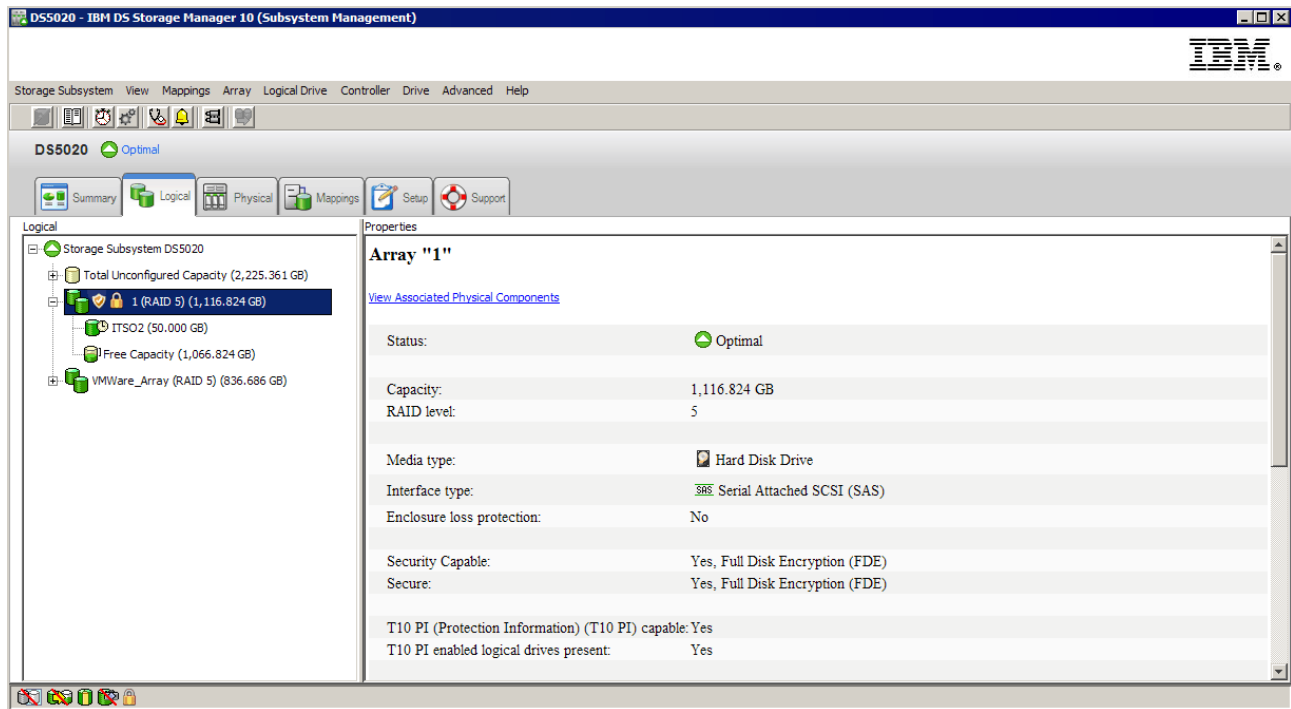


Figure 3-121 Defragmentation results in a single free capacity

3.7.3 Deleting an array

In this section we discuss the steps necessary to delete an array configuration from the DS5000 storage subsystem. In our example we will use a secure array that is built on FDE drives so all the steps needed are covered. With a non-secure array there are fewer steps needed and we will point these out as we go.

1. Select the array you want to delete from the configuration and right click and select *Delete* from the dropdown menu as shown in Figure 3-122.

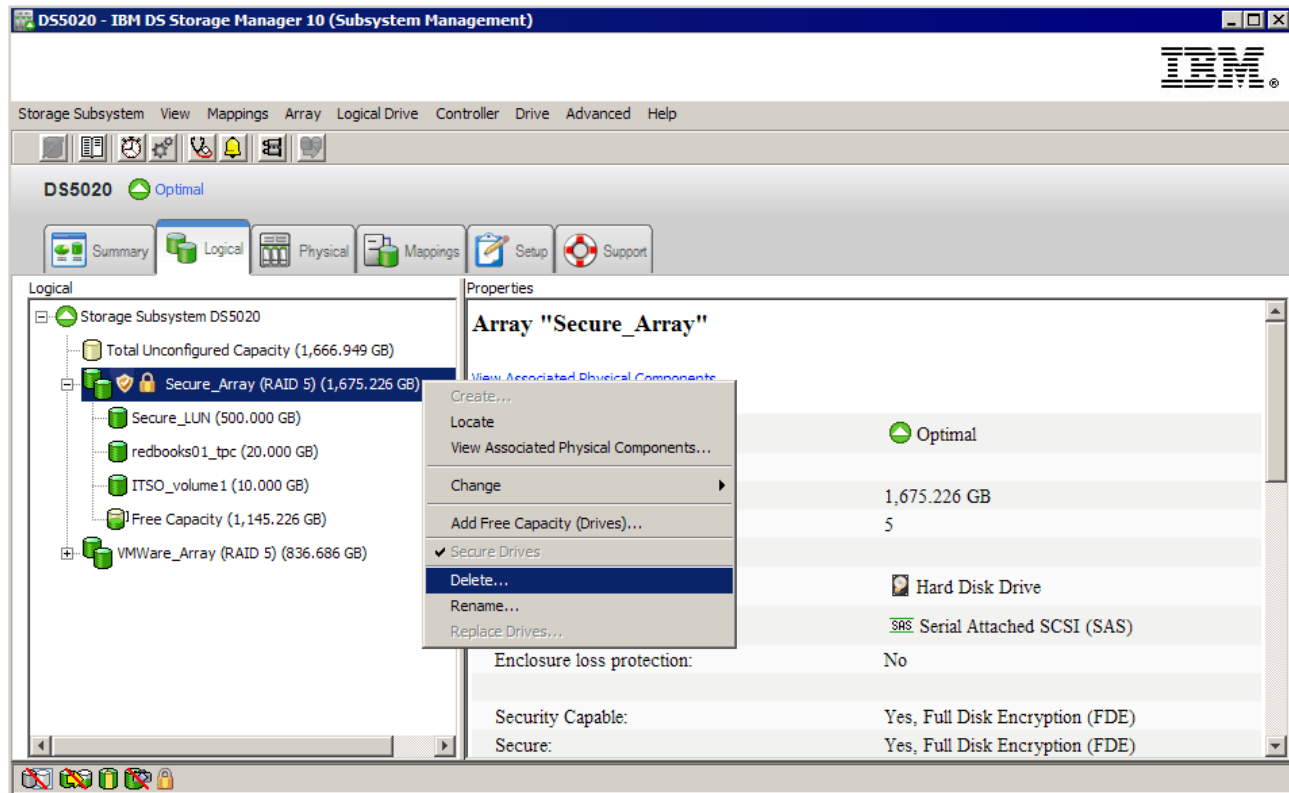


Figure 3-122 Select the array to delete

2. This will bring up the *Delete Array* window shown in Figure 3-123. Confirm that the array (and logical drives) you wish to remove is selected and click *Delete*.

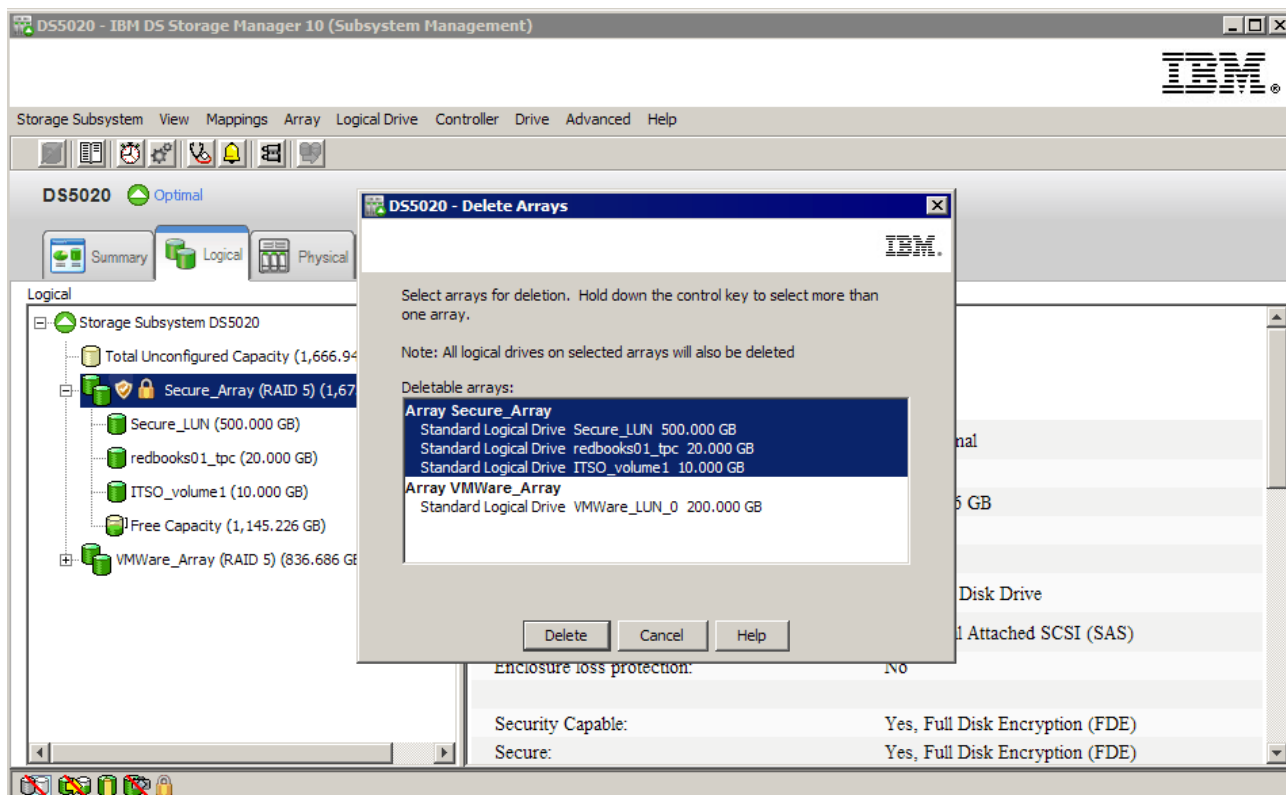


Figure 3-123 Delete Arrays Window to select arrays to be deleted

- Now we will need to confirm that we truly want to delete the selected array and its logical drives. In Figure 3-124 you will need to type “yes” and select **OK** to continue.

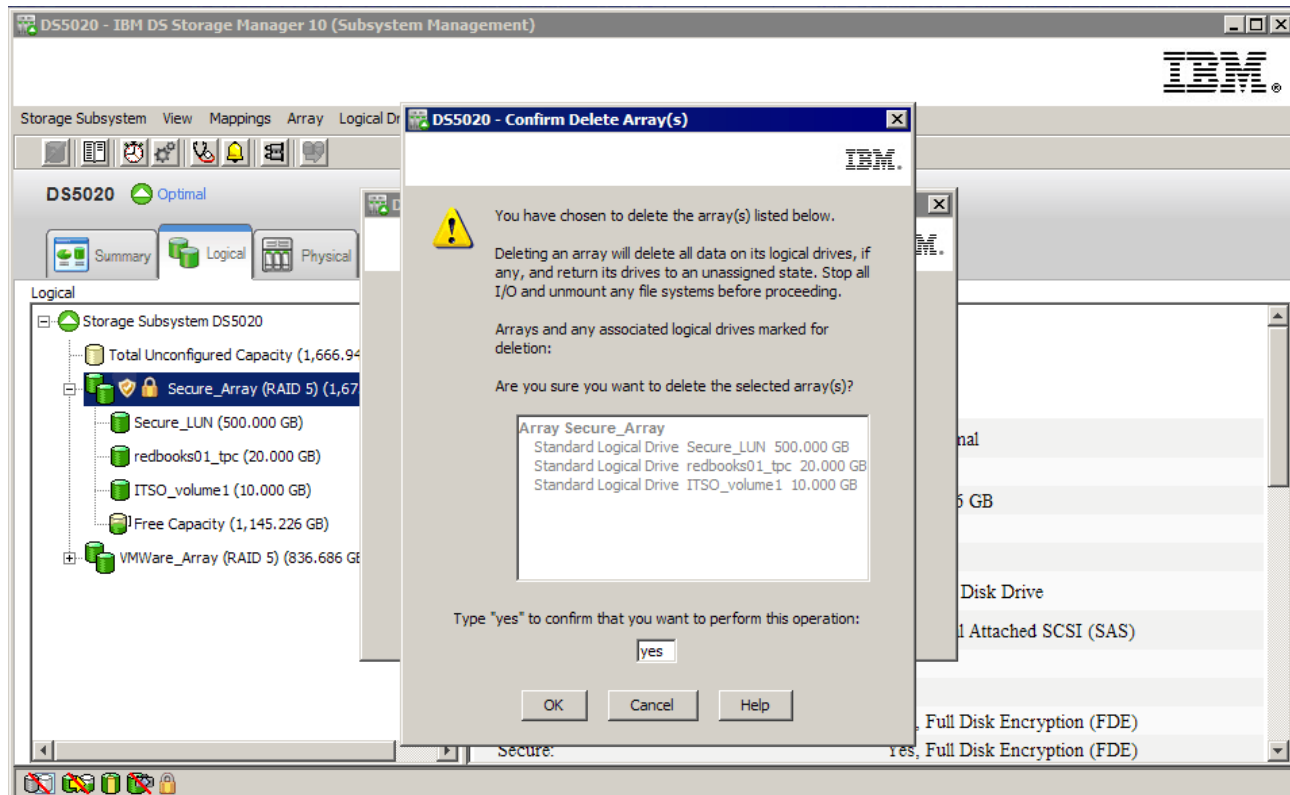


Figure 3-124 Delete confirmation screen

4. If you did not enter the password for management mode when you opened the Subsystem Window, you will be required to do so now. Enter the password and click **OK** to continue as shown in Figure 3-125.

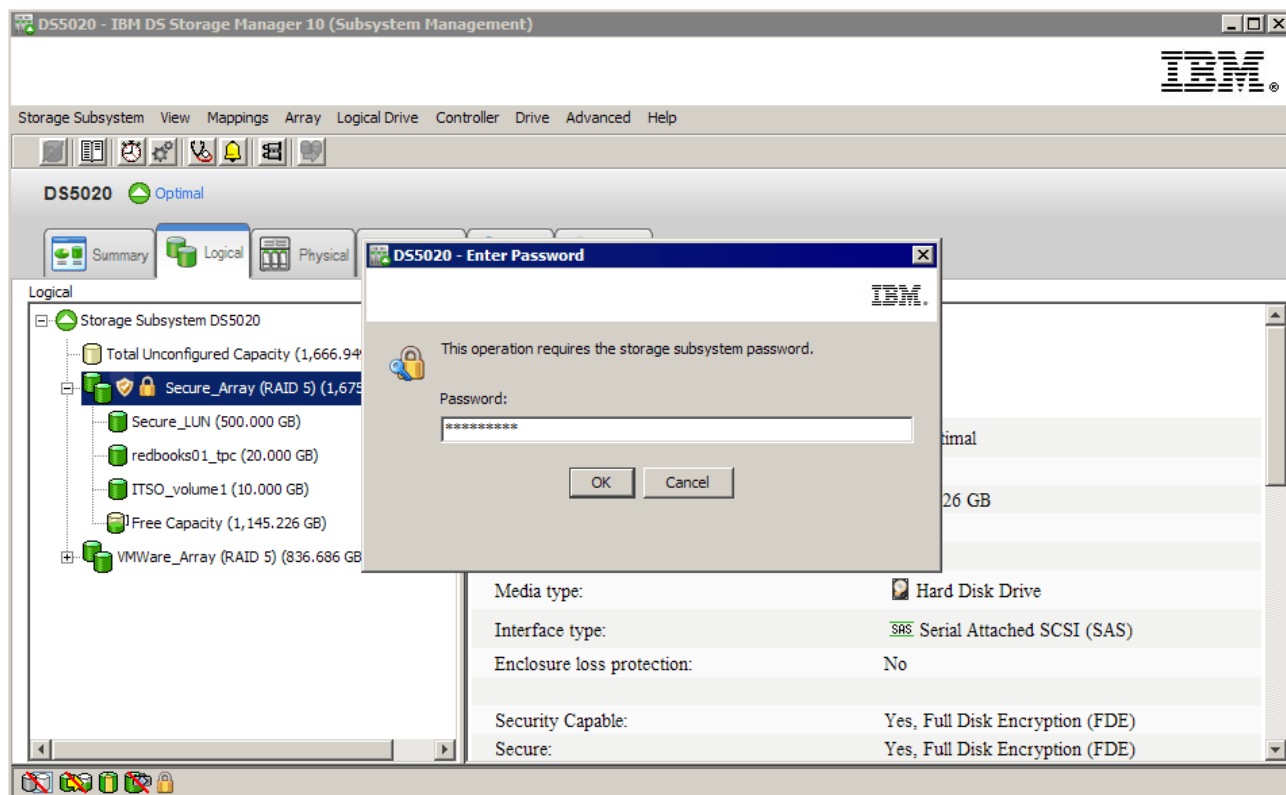


Figure 3-125 Selected array and its members are shown

5. As shown in Figure 3-126 when the delete progress bar is complete; select **OK**.

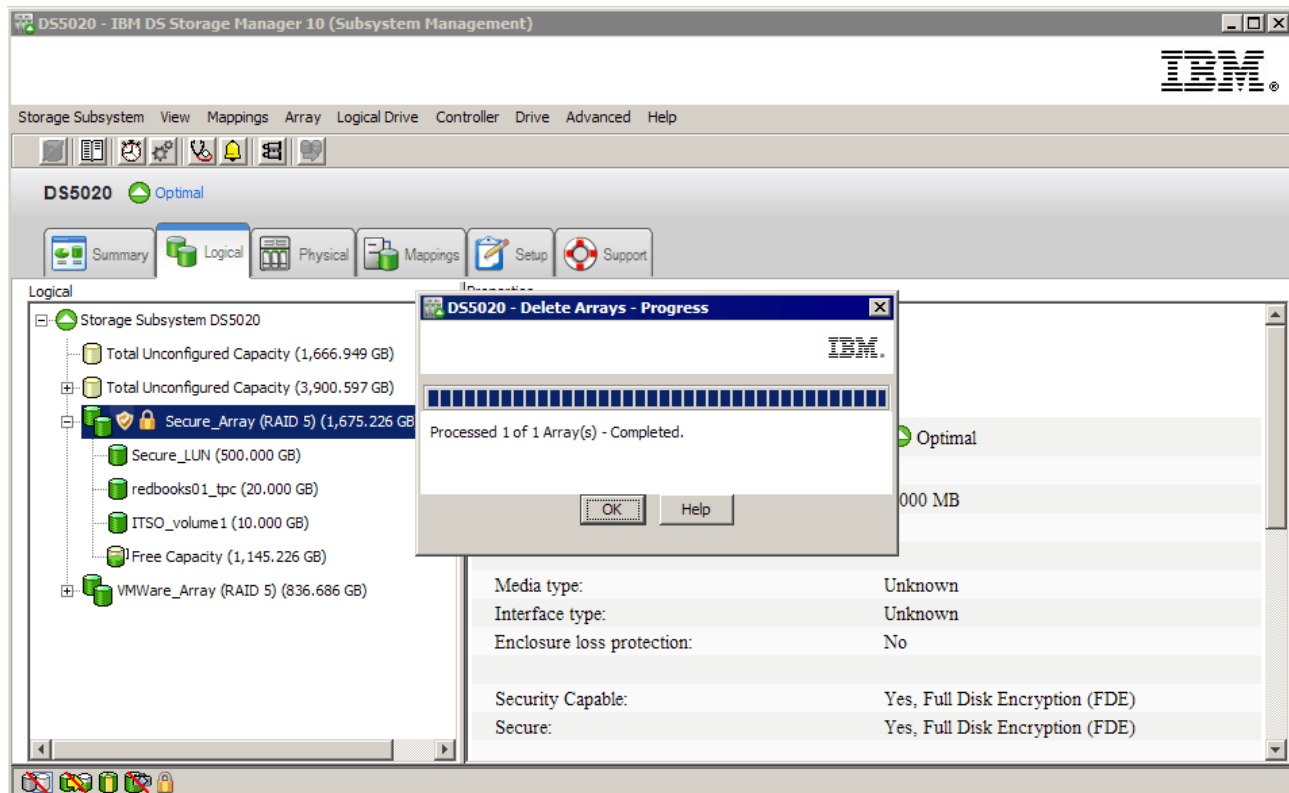


Figure 3-126 Delete Arrays - Completed

3.7.4 Secure erase

Secure erase provides a higher level of data erasure than traditional methods. When you initiate secure erase with the IBM DS Storage Manager on your DS5000 secured disks which were members of a secure array group, a command is sent to the FDE drive to perform a “cryptographic erase”. This erases the existing data encryption key and then generates a new encryption key inside the drive, making it impossible to decrypt the data on the drive. Drive security becomes disabled and must be re-enabled if it is required again.

The secure erase process is shown in Figure 3-127.

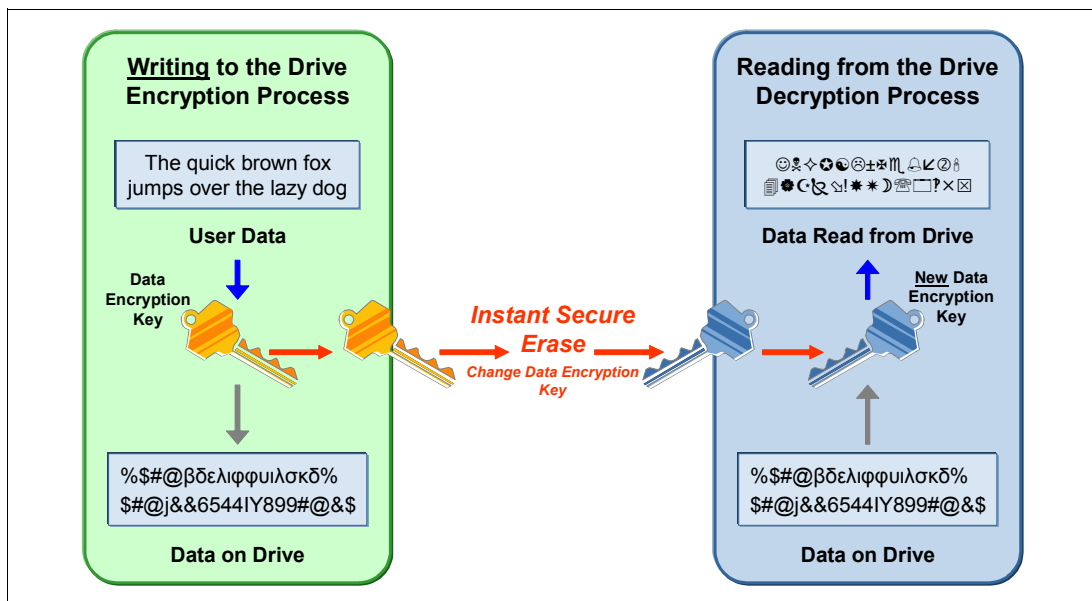


Figure 3-127 Secure erase process

Warning: All data on the disk will be permanently and irrevocably erased when the secure erase operation is completed for a security-enabled FDE drive. Do not perform this action unless you are sure that you want to erase the data.

To perform a secure erase procedure on FDE secure drives follow these steps:

1. Select and right-click the drive to select **Secure Erase** as shown in Figure 3-128.

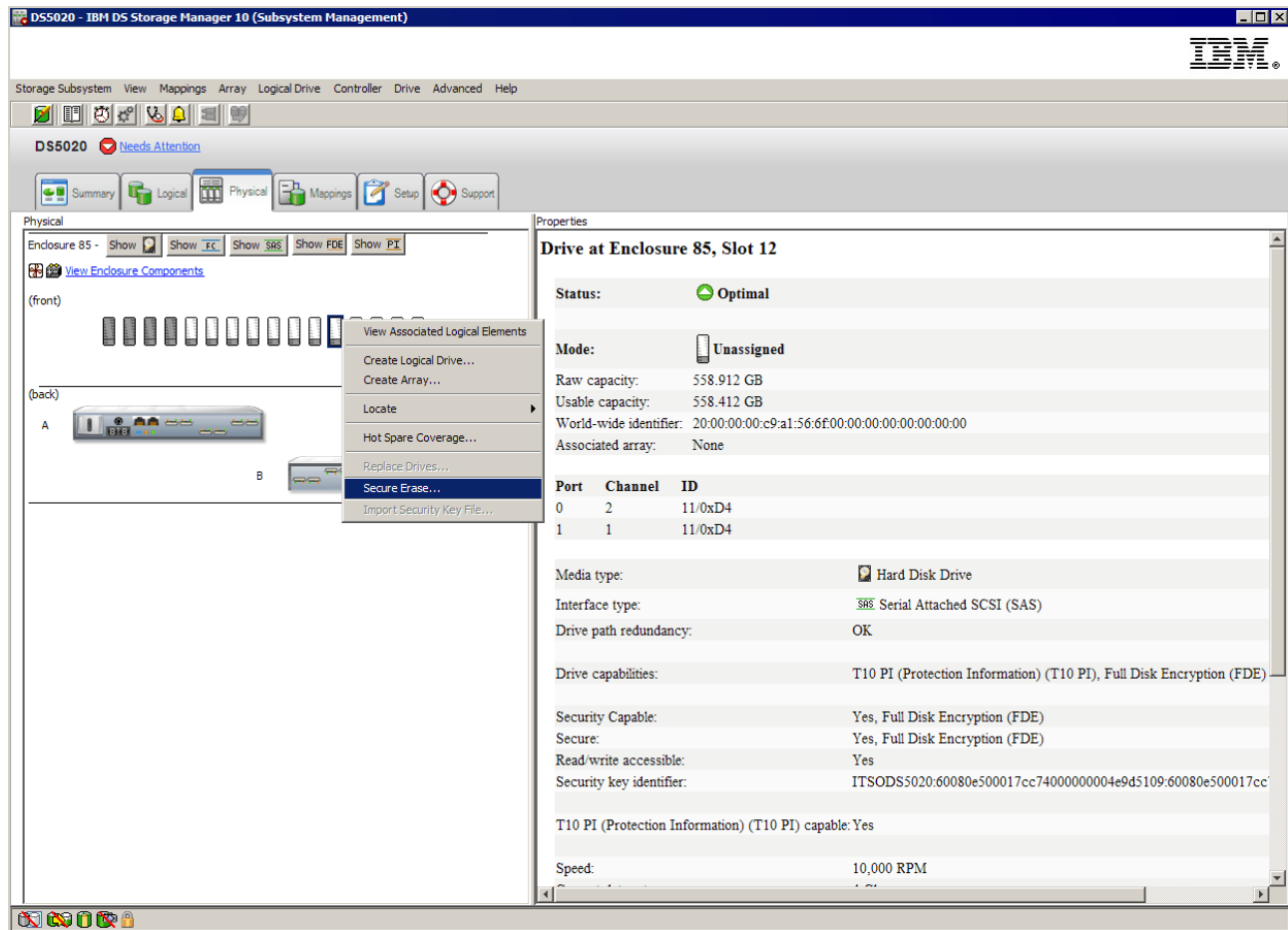


Figure 3-128 Selected FDE drive to be secure erased

2. Confirm the selection of the drive to be secure erased by entering “yes” and **OK** as shown in Figure 3-129.

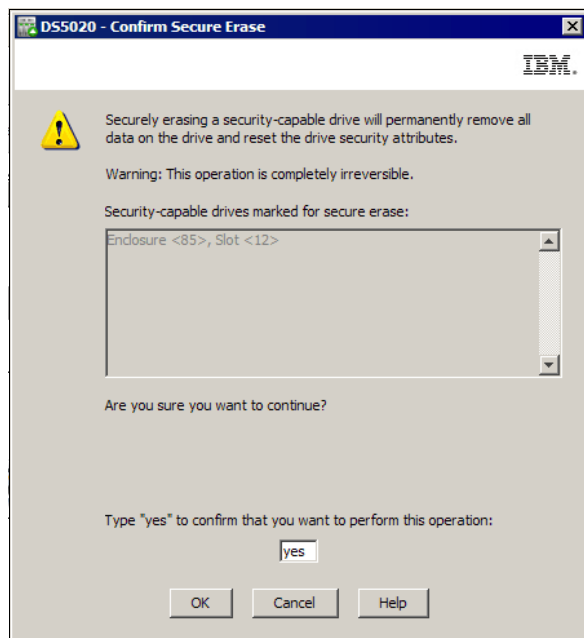


Figure 3-129 Confirm Secure Erase screen

3. After the secure erase operation is complete as shown in Figure 3-130, click "OK".

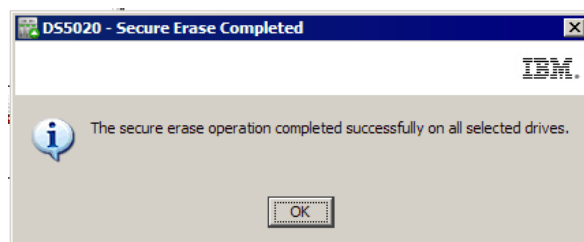


Figure 3-130 Secure erase completed.

Checking the drive property settings after the completion shows that the drive is no longer in the secure state (Figure 3-131). Drive can now be used to build an array that is either secure or unsecure, or as a hot spare for both secure and unsecured arrays.

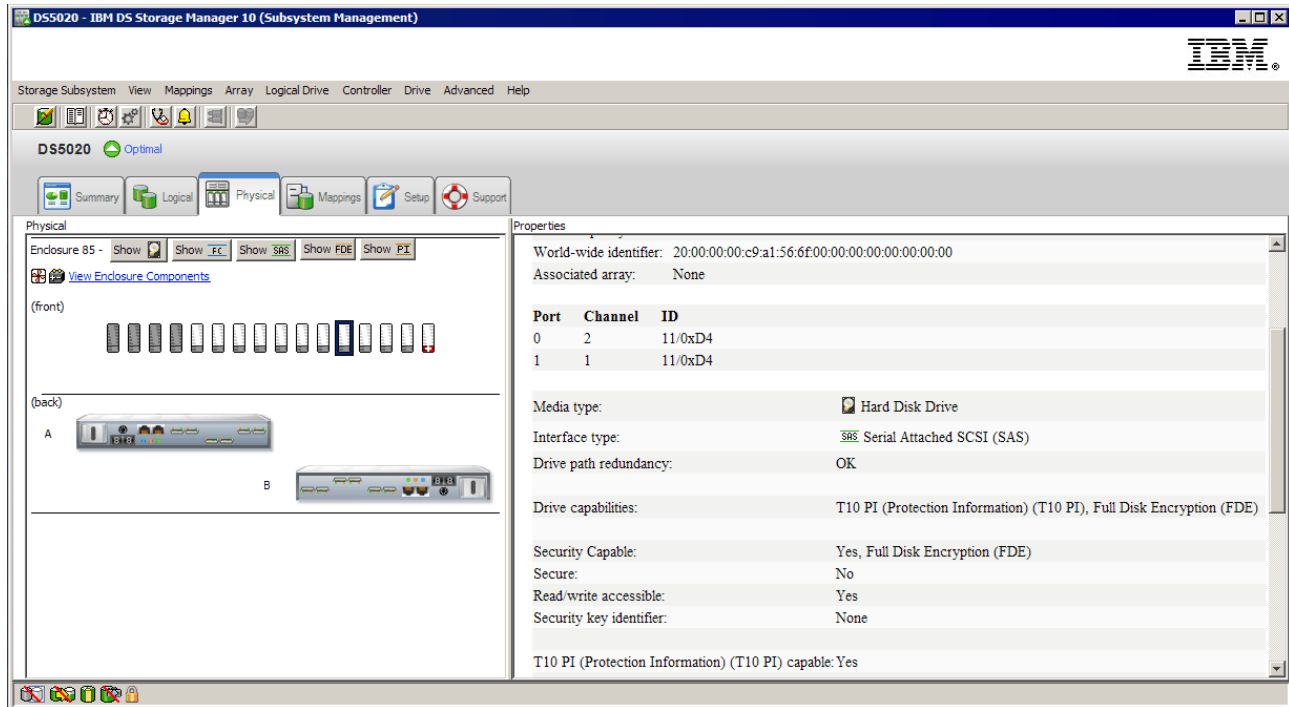


Figure 3-131 Secure erase sets drive to “Secure - No state

3.8 Storage Manager Advanced Monitoring features

Included with the Storage Manager are advanced maintenance features that allow for further maintenance steps to be used gathering much needed support information. These features are also covered in detail in the Chapter 5, “Advanced maintenance, troubleshooting, and diagnostics” on page 285.

3.8.1 Persistent reservations

Persistent reservations are a SCSI-3 feature for restricting access to storage media, based on the concept of reservations that the host can establish and manipulate. Earlier versions of SCSI provide a simple reservation capability through the RESERVE and RELEASE commands. SCSI-3 persistent reservations provide a significant superset of the earlier capability. Improvements that come with persistent reservations include:

- ▶ A well-defined model for reserving across multiple host and target ports
- ▶ Levels of access control, for example, shared reads, exclusive writes, exclusive reads, and writes
- ▶ Ability to query the storage subsystem about registered ports and reservations
- ▶ Provisions for persistence of reservations through power loss at the storage subsystem

A logical drive reservation is a feature of the cluster software (the actual reservation of the logical drive is handled by the host application) that allows one or more host ports to reserve a logical drive, thus preventing other host ports from accessing the same logical drive.

Unlike other types of reservations, a persistent reservation reserves across multiple host ports, provides various levels of access control, offers the ability to query the storage

subsystem about registered ports and reservations, and, optionally, provides for persistence of reservations in the event of a storage subsystem power loss.

The benefits of the persistent reservations feature is that it allows the DS5000 storage subsystem to integrate with cluster solutions that use shared logical drives for increased availability, scalability, and performance.

The Persistent Reservation options provided with the DS Storage Manager enables you to view and clear logical volumes reservations and associated reservations.

To locate this setting, highlight the logical drive in the Storage Manager menu and select **Advanced** → **Maintenance** → **Persistent Reservations**. The window shown in Figure 3-132 opens.

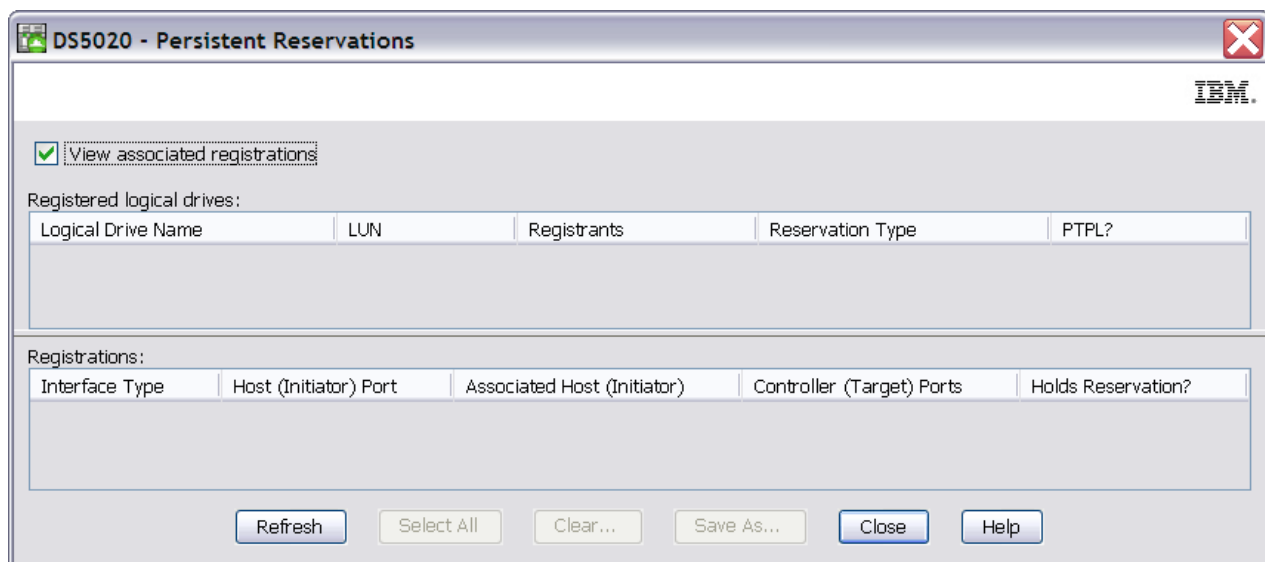


Figure 3-132 View of persistent reservations

3.8.2 Automatic firmware synchronization

The Automatic Code Synchronization (ACS) feature ensures that both controllers within a storage subsystem are executing the same version of the controller firmware. The primary purpose of this feature is to reconcile the possible difference in controller firmware version present on a replacement controller. ACS is also used to address inconsistent versions of firmware that can occur without controller replacement if a firmware upgrade is interrupted.

The replacement of both controllers is not a recommended operation, because ACS is intended to use the firmware image on the remaining native controller to resolve the inconsistency. ACS does address the replacement of both controllers. In this case, ACS synchronizes to the newer of the two firmware.

A failure to successfully transfer the incumbent image from the native to the foreign controller results in the native controller holding the alternate controller in reset.

The ACS feature behavior is based on three key persistent data representations:

- ▶ The serial number of each controller.
- ▶ The serial numbers of the last known native controllers. The identities of the last known controllers are contained within the metadata on the native drive set.

- The firmware version number of the incumbent firmware. This is the firmware associated with the metadata on the native drive set. The version of the incumbent firmware is stored within the drive metadata.

The controller firmware uses this information to determine what ACS action is required. If the serial number of a controller does not match the serial number for the slot in which it resides, this controller is considered to be *foreign* for the purposes of ACS, and a firmware synchronization occurs.



Full Disk Encryption with Full Disk Encryption drives

Full Disk Encryption (FDE) is an optional premium feature that prevents unauthorized access to the data on a DS5000 drive that is physically removed from the storage array. It is supported by the DS5000 firmware Version 7.60 and higher and Storage Manager 10.60 and higher. FDE is a premium feature of the storage management software and must be enabled either by you or your storage vendor.

The FDE premium feature requires security capable drives. A security capable drive encrypts data during writes and decrypts data during reads. Each security capable drive has a unique drive encryption key. Secure drives provide access to data only through a controller that has the correct security key. When you create a secure array from security capable drives, the drives in that array become security-enabled. When a security capable drive has been security-enabled, the drive requires the correct security key from a controller to read or write the data. All of the drives and controllers in a storage array share the same security key. The shared security key provides read and write access to the drives, while the drive encryption key on each drive is used to encrypt the data.

4.1 The need for encryption

Data security breaches are becoming increasingly common, and the threat of unauthorized access to sensitive data and intellectual property is growing. Data security is now a common component of the corporate landscape, mostly driven by regulatory compliance, and security efforts can often be fragmented.

At some point, all drives are out of an organization's control and vulnerable to a security breach. For example, with "re-purposing", decommissioning, or disposal of individual drives, common methods of security are often insufficient when:

- ▶ Deleted files can be reinstated.
- ▶ Drive disposal methods are subject to human error.
- ▶ Password protected data can still be accessed by a skilled individual.
- ▶ Disk reformatting erases data on drives but information can still be recovered.¹

In each case, a risk is introduced where legible data might be recovered from disk. This can be made significantly more difficult if Full Disk Encryption on a DS5000 storage subsystem is employed.

Important: Full Disk Encryption is an additional level of data protection, but it does not replace the access controls and security processes; rather, it complements them.

4.1.1 Encryption method used

The FDE drives have encryption hardware that performs symmetric encryption and decryption of data at full drive speed with no impact on performance. The disk encryption hardware is used in conjunction with IBM DS5000 Disk Encryption Manager on the DS5000 storage subsystem. Each FDE drive has a unique drive encryption key. IBM DS5000 Encryption Manager uses asymmetric encryption to encrypt and decrypt the drive encryption key.

Without IBM DS5000 Disk Encryption Manager security key, the user (authorized or unauthorized) can no longer decrypt the data on the drive.

Important: Should the security key and all copies be lost, then the encrypted data on the drive cannot be decrypted and is therefore considered lost.

Figure 4-1 shows the relationship of the IBM DS5000 Disk Encryption Manager and an individual FDE drive with encryption enabled.

¹ Some utilities used to "erase" data from disks and arrays are not fully successful when such data can still be recovered using forensic techniques

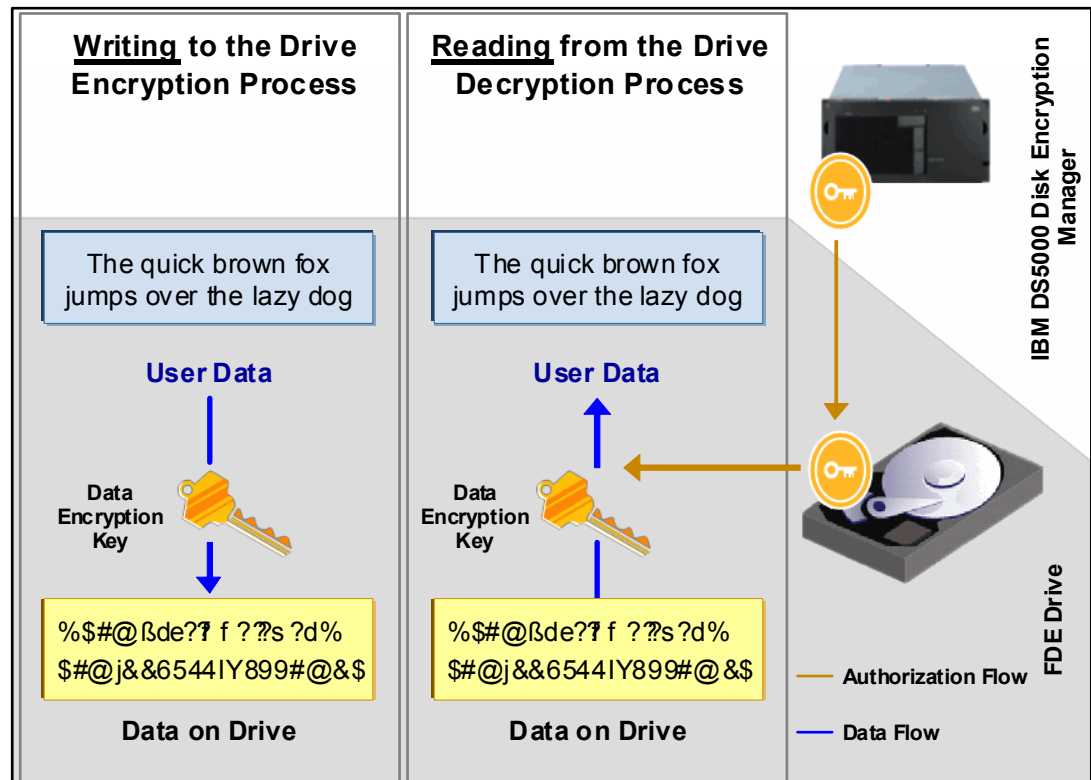


Figure 4-1 Full Disk Encryption using IBM Disk Encryption Manager and FDE drives

With this relationship, the correct keys, and authentication, the FDE drive will encrypt data written and decrypt data read from it. But if the drive is removed and data on the drive is attempted to be read, as shown in Figure 4-2, the user will not have the appropriate authorizations, as data cannot be read from or written to the drive without authenticating with the IBM DS5000 Disk Encryption Manager, which will unlock the drive.

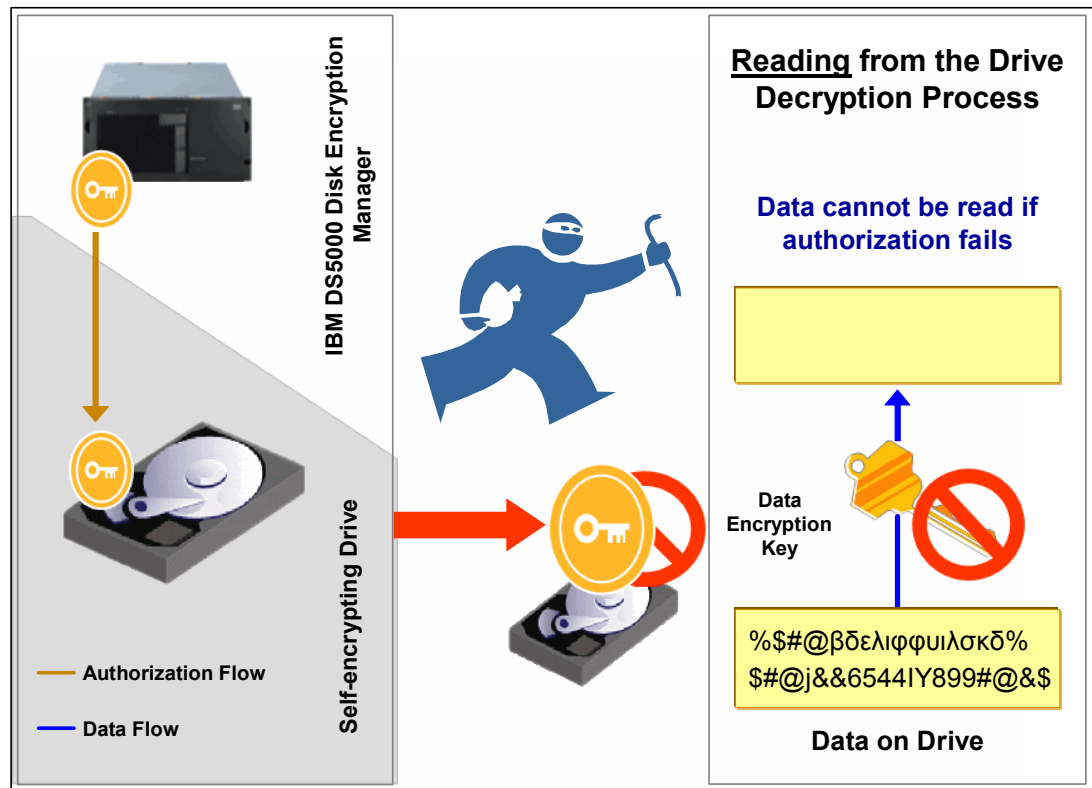


Figure 4-2 Unauthorized access to the drive results in the data remaining encrypted

4.2 Disk Security components

There are a number of new components to this new feature that are detailed in this section. All of these features are managed by the Storage Manager (V10.6.x and higher).

4.2.1 DS5000 Disk Encryption Manager

The Disk Encryption Manager on the DS5000 system maintains and controls the key linkage and communications with FDE drives. It is included with the firmware and Storage Manager. It:

- ▶ Provides all the management tools necessary to quickly and simply enable and secure FDE drives.
- ▶ Establishes and manages a single authorization scheme for all the FDE drives in a DS5000 storage subsystem.
 - Places FDE drives in a secured state.
 - Defines secure arrays.
 - Supports the decommissioning or re-purposing of drives with Instant Secure Erase.

With this function you can record both the security key ID, pass phrase, and the secure file location in a safe place.

- ▶ Using the FDE drive, it generates and encrypts a security key:
 - Creates a unique security key ID that is paired with the security key.
 - Adds a randomly generated number.

- The security key ID is saved. This folder location will be needed whenever a security operation requires the key ID (for example, when a drive powers up).
- Creates a backup of the security key and the security key identifier.
- A secure backup is provided in which the security key and the security key identifier are encrypted utilizing a user-selected pass phrase.

4.2.2 Full Data Encryption (FDE) drives

FDE drives are required to enable Full Disk Encryption feature. These are the currently available FDE disk drives:

- ▶ FC disk with encryption:
 - 300 GB/15K 4 Gbps FC encryption-capable E-DDM
 - 450 GB/15K 4 Gbps FC encryption-capable E-DDM
 - 600 GB/15k 4 Gbps FC encryption-capable E-DDM
- ▶ SAS drives (with FC-SAS interposer) with encryption
 - 300 GB/10k FC-SAS encryption-capable E-DDM
 - 600 GB/10k FC-SAS encryption-capable E-DDM
 - 900 GB/10k FC-SAS encryption-capable E-DDM

4.2.3 Premium feature license

The DS5000 requires that the Full Disk Encryption premium feature be installed and enabled for Full Disk Encryption to function. See 3.4.2, “Enabling the premium features” on page 156 for details about this topic.

4.2.4 Security key management

Security key management can be handled locally, using Storage Manager, or externally, using Tivoli Key Lifecycle Management (TKLM). Adding external management capabilities to DS5000 Storage Subsystem enables better integration with existing solutions and centralized key management. The DS5000 requires that the External Key Management premium feature be installed and enabled to be able to use TKLM for key management. Figure 4-3 on page 258 shows how keys are managed locally (top) or externally (bottom).

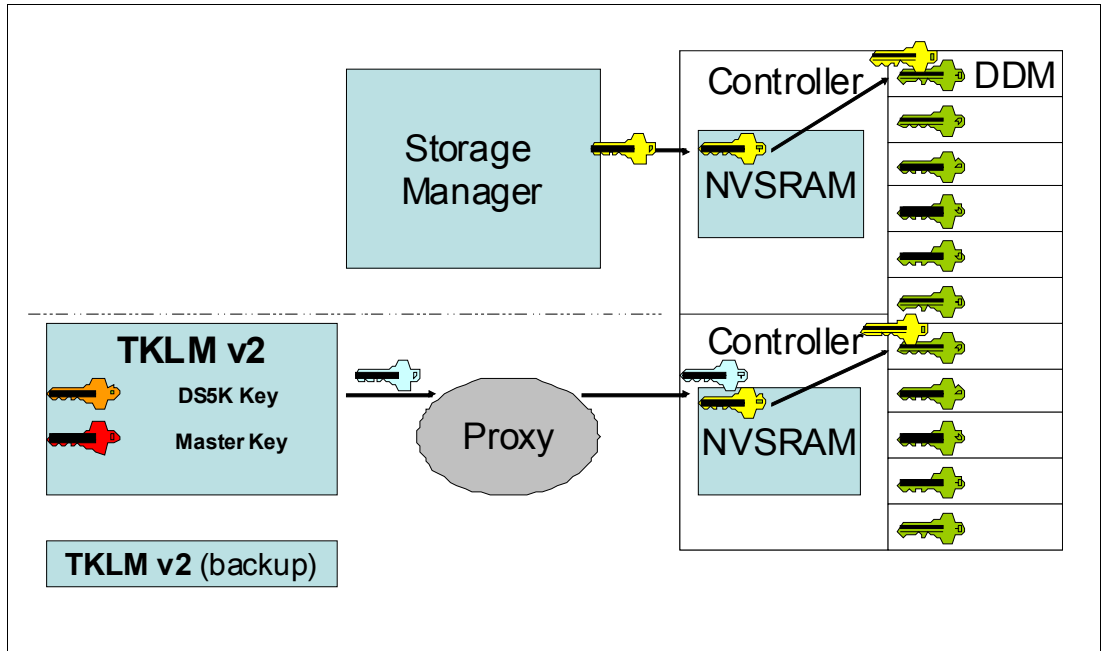


Figure 4-3 Key management overview

Local security key management

With local security key management, the security key is created and contained in the storage subsystem controller. Local security key management does not require additional software. To move secured drives from one storage subsystem to another, you must use the saved security key file from the original storage subsystem to unlock the drives.

External security key management

Instead of using a security key created by the storage subsystem controller, external security key management uses a central key location on your network to manage keys for different storage subsystems. External security key management is facilitated by external key license manager software, such as IBM Tivoli Key Lifecycle Manager (TKLM). If you do not already have this software, you must purchase it, install it, and configure the proxy server.

With external security key management, the controllers obtain the security key from the external security key management source. This key is then obfuscated in the controller volatile memory for future use, as long as the storage subsystem power is turned on. This key is erased from volatile memory when the storage subsystem power is turned off. Because the key is not stored permanently in the storage subsystem, the storage subsystem must have a non-FDE drive in the configuration to boot successfully; it then requests the security key from the external key management server to unlock the FDE drives.

This method provides a common and consistent key management interface; the external key license manager software also manages security keys for other storage hardware, such as secured tape drives. You do not have to access a saved security key file to move secured drives from one storage subsystem to a second storage subsystem. Rather, the external key license manager software supplies the security key that unlocks the drives automatically, if the second storage subsystem is connected to the key license manager when the drives are inserted.

To enable external security key management, complete the following tasks:

1. Upgrade the controller firmware to version 7.70.xx.xx or later. Follow the FDE premium feature web-activation instructions to enable both the FDE and External Key Management premium features.
2. Install and configure the external key license manager software. See the documentation that came with the software for more information.
3. Install and configure the DS TKLM Proxy Code Server.
4. Configure the external key management software to receive an external key request.
5. Use Storage Manager to command the storage subsystem controller to request the security key from the external key license manager, instead of generating a local security key.
6. Configure the external key license manager software to accept an external key request.

Important: There are some requirements when using external key management:

1. Tivoli Key Lifecycle Manager is the only external security key management software that is supported on IBM DS storage subsystems.
2. External security key management requires controller firmware version 7.70.xx.xx or later.
3. Make sure that at least one non-FDE drive is installed in the storage subsystem when you use external security key management. Otherwise, if the storage subsystem power is turned off and then on again, the storage subsystem might require that you supply the security key from the saved file manually to unlock the secured FDE drives and complete the boot process.

When using TKLM, a DS TKLM Proxy Code Server is needed to facilitate communication between DS5000 Storage Subsystem and TKLM server. It can be installed on the following operating systems:

- ▶ AIX 5.x, 6.x
- ▶ Red Hat Enterprise Linux 4.x, 5.5
- ▶ SUSE Linux Enterprise 10.3, 11
- ▶ Windows 2008 R2
- ▶ Windows 2008 SP2
- ▶ Windows 2008 Standard Edition, Enterprise Edition

Note: DS TKLM Proxy Code Server has the following limitations:

1. A maximum of four storage subsystem controllers can be monitored by one proxy server.
2. A maximum of four TKLM servers can be connected to one proxy server.

Details about installation and implementation of DS TKLM Proxy Code Server can be found in *Installation and Host Support Guide - IBM Storage Manager v10* which can be downloaded from: <http://www-947.ibm.com/support/entry/portal/docdisplay?ln docid=MIGR-5075652>

4.2.5 Keys

There are two types of keys that are used with Full Disk Encryption and FDE drives:

- ▶ The *encryption key* is generated by the drive and never leaves the drive, so it always stays secure. It is stored in encrypted form and performs symmetric encryption and decryption of data at full disk speed with no impact on disk performance. Each FDE drive uses its own unique encryption key that is generated when the disk is manufactured and regenerated when required by the storage administrator using the DS5000 Disk Encryption Manager.
- ▶ The *lock key* or *security key* is a 32 byte random number that authenticates the drive with the DS5000 Disk Encryption Manager using asymmetric encryption for authentication. When the FDE drive is secure “enabled”, it has to authenticate with the Disk Encryption Manager or it will not return any data and remains locked. After the drive has been authenticated, access to the drive operates like any other disk drive. After the security key is created by the controllers, or is obtained from the external key management software, an encrypted version of the security key is obfuscated in the storage subsystem and cannot be viewed directly. The authentication only occurs typically after the FDE has powered up, where it will be in a “locked” state.

If the lock key is not initially established between the DS5000 Disk Encryption Manager and the disk, then the disk is considered unlocked with access unlimited, as per a non-FDE drive.

The security key file contains the encrypted security key and the security key identifier. You must provide the pass phrase during the save security key operation. The pass phrase is not stored anywhere in the storage subsystem or in the security key file. The controller uses the pass phrase to encrypt the security key before it exports the security key to the security key file. The security key identifier is stored in the security key file so that you can identify the storage subsystem to which the security key file is associated. Make sure that you protect the security key file and its associated pass phrase, because these two pieces of information can be used to unlock secured FDE drives.

To decrypt the security key in the security key file, you must provide the same pass phrase that was entered when the security key file was generated. The drive then determines whether its security key and the security key that was provided by the storage subsystem are the same. If they are the same, data can be read from and written to the security-enabled FDE drives.

If you use local security key management, the security key file provides protection against a corrupted security key or the failure of both controllers in the storage subsystem. The security key file is also needed to unlock security-enabled FDE drives when they are moved from one storage subsystem to another. In these cases, the security-enabled FDE drives remain locked until the drives are unlocked by the security key that is stored in the security key file. To decrypt the security key in the security key file, you must provide the same pass phrase that was entered when the security key file was generated. The drive then determines whether its security key and the security key that was provided by the storage subsystem are the same. If they are the same, data can be read from and written to the security-enabled FDE drives.

If you use external security key management, the security key file provides protection in the following situations:

1. If communication is lost to either the proxy server or the external key license servers when the controller unlocks the secured FDE drives.
2. If the secured FDE drives are moved to or from a storage subsystem that is not managed by the same external key license manager.
3. If drives must be unlocked after the power cycle of a storage subsystem configuration that has only secured FDE drives and no unsecured FDE or non-FDE drives in the configuration.

After the storage subsystem controller creates the security key, the RAID arrays can be changed from a state of Security Capable to a state of Security Enabled. The Security Enabled state requires the RAID array FDE drives to be unlocked after power to the drive is turned on using the security key to access the data that is stored on the drives. Whenever power is applied to the drives in a RAID array, the drives are all placed in Security Locked state. They are unlocked only during drive initialization with the storage subsystem security key. The Security Unlocked state makes the drives accessible for the read and write activities. After they are unlocked, the drives remain unlocked until the power is removed from the drives, the drives are removed and reinserted in the drive bays, or the storage subsystem power is cycled.

After a drive is secured, the drive becomes locked if power is turned off or if it is removed. The encryption key within that drive will not encrypt or decrypt data, making the drive unreadable until it is unlocked by the controllers.

4.2.6 Security key identifier

For additional protection, the security key that is used to unlock FDE drives is not visible to the user. The security key identifier is used to refer to a security key instead. You can see the security key identifier during operations that involve the drive security key backup file, such as creating or changing the security key. The security key identifier is stored in a special area of the drive; it can always be read from the drive and can be written to the drive only if security has been enabled and the drive is unlocked.

The security key identifier field in the FDE Drive Properties window, shown in Figure 4-4, includes a random number that is generated by the controller and appended to the identifier you specified when you create or change the security key. One security key is created for all FDE drives on the storage subsystem.

Note that the Security Capable and Secure fields in the Drive Properties window show whether the drive is secure capable and whether it is in Secure (Yes) or Unsecured (No) state. The example shows that the drive is both capable (FDE) and enabled.





Drive at Enclosure 85, Slot 12		
Status:	 Optimal	
Mode:	 Assigned	
Raw capacity:	558,912 GB	
Usable capacity:	558,412 GB	
World-wide identifier:	20:00:00:00:c9:a1:56:6f:00:00:00:00:00:00:00	
Associated array:	Secure_Array	
Port	Channel	ID
0	2	11/0xD4
1	1	11/0xD4
Media type:	 Hard Disk Drive	
Interface type:	 Serial Attached SCSI (SAS)	
Drive path redundancy:	OK	
Drive capabilities:	T10 PI (Protection Information) (T10 PI), Full Disk Encryption (FDE)	
Security Capable:	Yes, Full Disk Encryption (FDE)	
Secure:	Yes, Full Disk Encryption (FDE)	
Read/write accessible:	Yes	
Security key identifier:	DS5020:60080e500017cc74000000004eb75752:60080e500017cc74000029064eb78d89	

Figure 4-4 FDE drive properties showing security ID and status

4.2.7 Passwords

For Full Disk Encryption to be enabled, the DS5000 has to have the administration pass phrase or password set. The password must be “strong” and not easy to guess. A check is made on the password and if the system does not consider it to be strong enough when you log in or are prompted for the password, the message shown in Figure 4-7 on page 265 will appear. It will include suggestions about how the password can be made stronger.

The security key and the security key identifier are encrypted using a different password or pass phrase when the key is created or changed (see 4.3.2, “Secure key creation” on page 264 and 4.4.1, “Changing the security key” on page 268). The array then returns a file that is called a *blob*, or key backup. If the array needs that key later, you give the blob and pass phrase to the GUI, which sends it down to the array where the original key is decrypted.

The user-specified alphanumeric character string is not stored anywhere on the DS5000 or in the security key backup file.

4.3 Setting up and enabling a secure disk

This section shows a step-by-step process to create a key and file on the IBM Disk Encryption Storage Manager of the DS5000. It will then show how to enable a previously configured array that has FDE drives.

4.3.1 FDE and premium feature check

There are a number of checks to make prior to key creation. First, you must check that the premium feature key has been applied to the system. To do this task, from the Storage Manager window, select **Storage Subsystem** → **Premium Features**.

Figure 4-5 shows that the Full Disk Encryption premium feature key has been obtained and successfully installed. This premium feature key is installed the same as any other premium feature key (see 3.4.2, “Enabling the premium features” on page 156 for details about how to install premium feature keys).

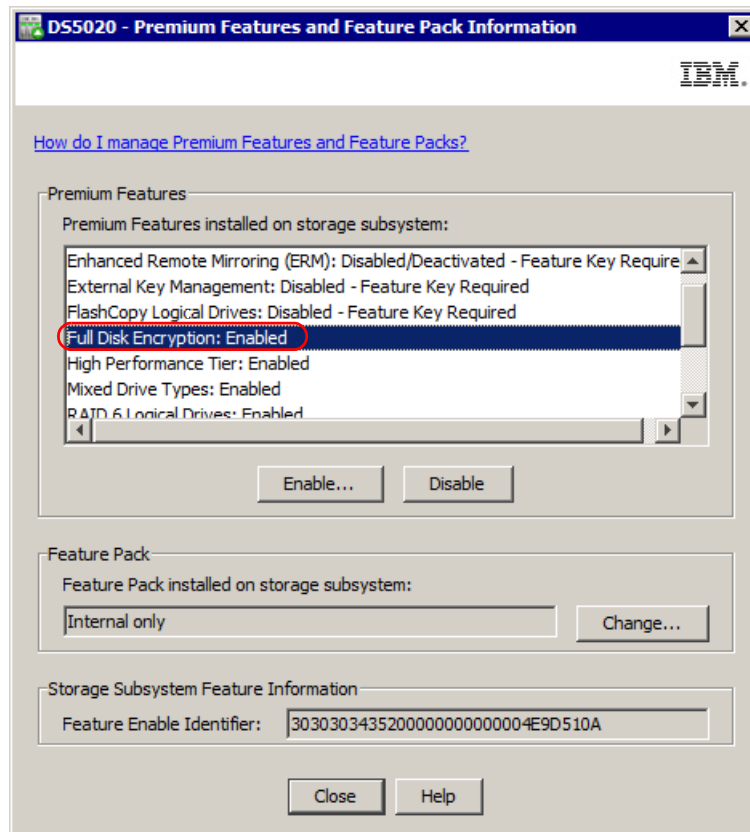


Figure 4-5 The correct premium feature has been obtained and installed

The next check is to ensure that the physical disks are FDE drives and are secure capable. In Figure 4-6, you can see that an array has been created where disk security is not enabled, as indicated by the unlocked padlock. If you click the array and then right-click and select **View Associated Physical Components**, you can view the disks. If you click the **Show FDE** button, it will display all the FDE drives and confirm that all the drives in the array are all secure capable.

The array is already being used and has several logical drives configured and consists of all FDE drives; therefore, it can be enabled.

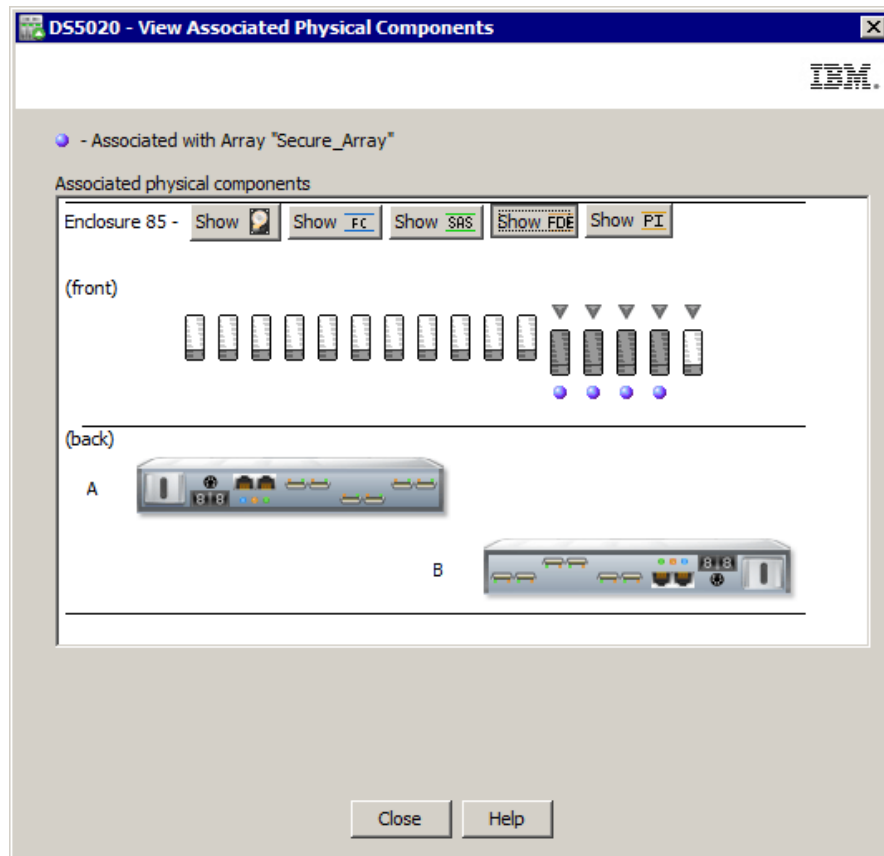


Figure 4-6 Array created with FDE drives with Disk Security disabled

4.3.2 Secure key creation

To create the secure key, select, in the top left corner of the IBM System Storage DS ES window, **Storage Subsystem** → **Drive Security** → **Create Security Key**.

You must have your DS5000 subsystem password set to proceed, and you might see the message shown in Figure 4-7 if the existing password be considered too weak.

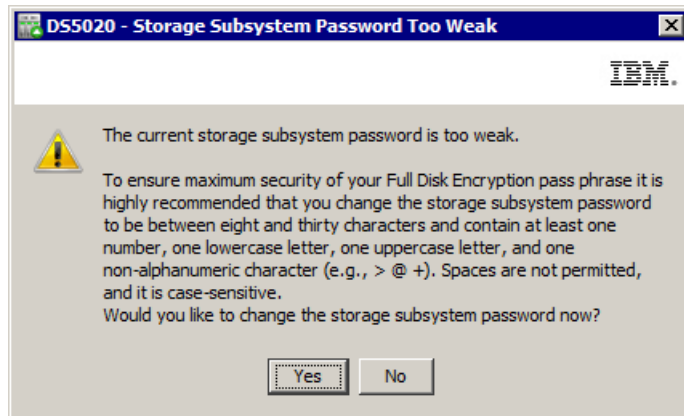


Figure 4-7 Warning regarding the weak subsystem password

The window shown in Figure 4-8 opens, where you need to complete the fields.

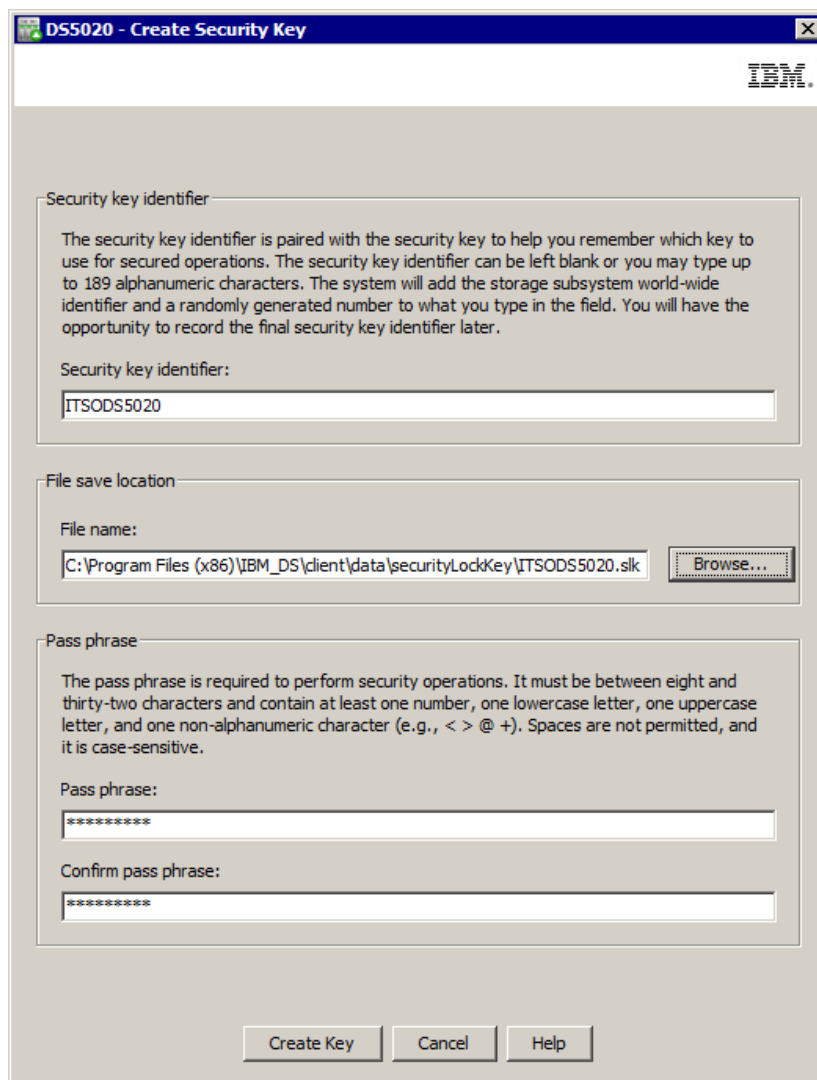


Figure 4-8 Requirements displayed for the security key creation

The key location default is in the user's local PC directory. We strongly advise that the key be copied and kept in a safe location.

Tip: The best practice is to store the security key file with your key management policies along with the pass phrase. It is important to record and remember where this file is stored because the security key file is required along with pass phrase when a drive is moved from one storage subsystem to another or when both controllers in a storage subsystem are replaced at the same time.

When the process is complete, the key is created and located as specified; also, as shown in Figure 4-9, the security identifier is displayed. There are three items that must be kept secure in order to manage any changes to the FDE drives when they are encryption enabled.

- ▶ Security key file created from the process
- ▶ Security key identifier created from the process
- ▶ Password used



Figure 4-9 Security key creation process complete

The key authorizations now generated are synchronized between both controllers in the DS5000 storage subsystem. With these authorizations in place, arrays on the FDE drives in the storage subsystem can be secured.

4.3.3 Enable Disk Security on array

Now that the keys have been created, Disk Security can now be enabled on the array. Right-click the array and select **Secure Drives**, as shown in Figure 4-10.

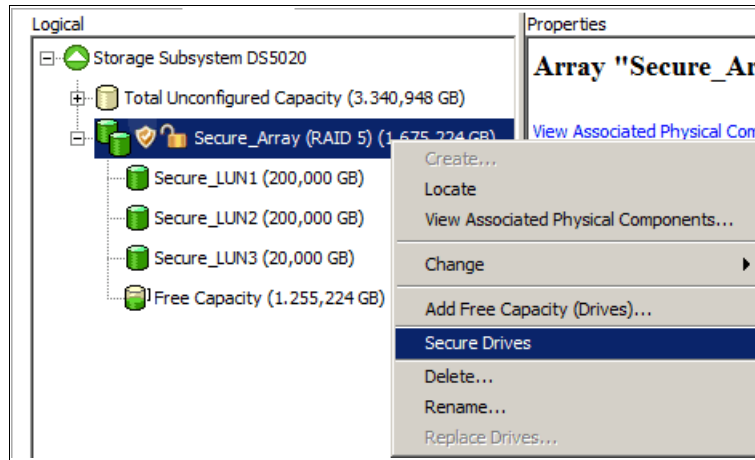


Figure 4-10 Secure all drives in the array

You will then be prompted to confirm the Secure Drives on the array, as shown in Figure 4-11.

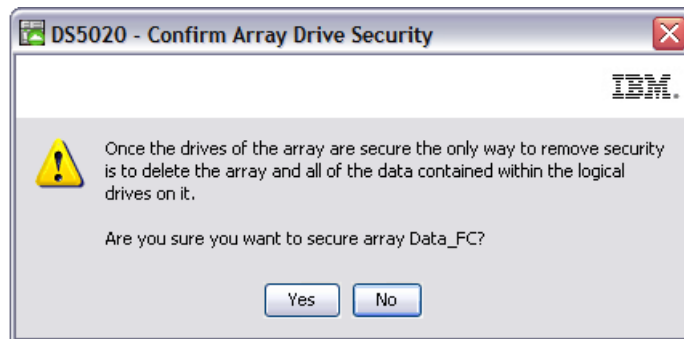


Figure 4-11 Confirm Array Drive Security

The array is now secured, as indicated by the padlock in a locked position, as shown in Figure 4-12.

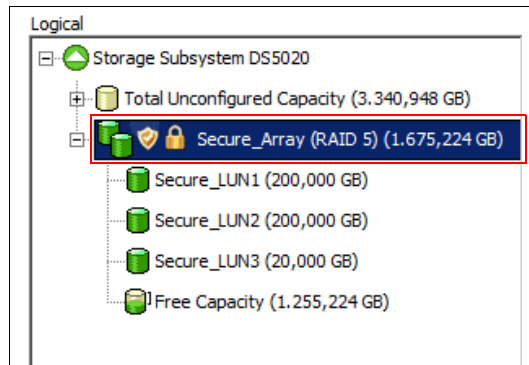


Figure 4-12 Array is now secured with Disk Security enabled

4.4 Additional secure disk functions

In the following sections, we discuss the following functions:

- ▶ Changing the security key
- ▶ Saving the security key file
- ▶ Secure disk erase
- ▶ FDE drive status
- ▶ Hot spare drives

4.4.1 Changing the security key

The security key can be changed if the details of the existing key be corrupted or the pass phrase forgotten, provided that there are no outstanding Secure Disk communications between the FDE drives and Disk Encryption Manager (for example, if a disk is in a “locked” state). Because the disk encryption key never leaves the disk, you might want to periodically change the encryption key, the way a user might periodically change the administrative password to an operating system. This depends on the organization’s security guidelines.

The process to change the security key is very similar to that of creating it initially. To change the key, select, in the top left hand corner of the Storage Manager menu, **Storage Subsystem** → **Drive Security** → **Change Security Key**.

You are prompted by a panel asking you to confirm the security key change. Type **yes** as shown in Figure 4-13 on page 269 and click on **OK**.

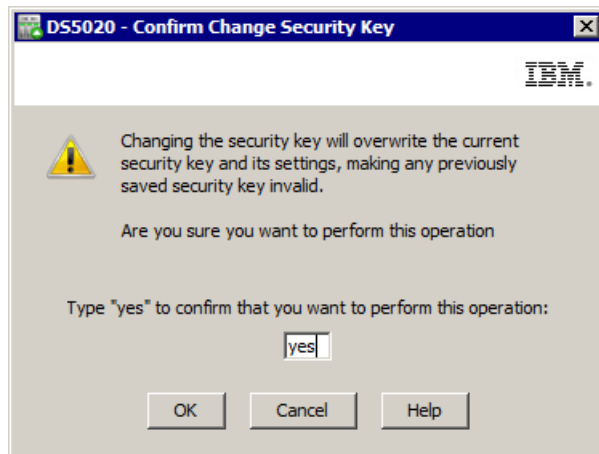


Figure 4-13 Security key change prompt

The window shown in Figure 4-14 opens and you are prompted to add a security identifier (optional), a location to store the key file in, and a pass phrase.

DS5020 - Change Security Key

IBM

Security key identifier

The security key identifier is paired with the security key to help you remember which key to use for secured operations. The security key identifier can be left blank or you may type up to 189 alphanumeric characters. The system will add the storage subsystem world-wide identifier and a randomly generated number to what you type in the field. You will have the opportunity to record the final security key identifier later.

Security key identifier:

ITSODS5020another

File save location

File name:

ram Files (x86)\IBM_DS\client\data\securityLockKey\ITSODS5020another.slk

Browse...

Pass phrase

The pass phrase is required to perform security operations. It must be between eight and thirty-two characters and contain at least one number, one lowercase letter, one uppercase letter, and one non-alphanumeric character (e.g., < > @ +). Spaces are not permitted, and it is case-sensitive.

Pass phrase:

Confirm pass phrase:

Change Key Cancel Help

Figure 4-14 Change Security Key options

The new security key is generated by the controller firmware and is hidden in the storage subsystem. The new security key replaces the previous key that was used to unlock the security-enabled FDE drives in the storage subsystem. The controller negotiates with all of the security-enabled FDE drives for the new key.

The original security key is also stored in the storage subsystem for protection in case something prevents the controllers from completing the negotiation of the new security key with the security-enabled FDE drives (for example, loss of storage subsystem power during the key change process). If this happens, you must change the security key so that only one version of the security key is used to unlock all drives in a storage subsystem. The original key is stored in the storage subsystem only. It cannot be changed directly or exported to a security key backup file.

When the security key has been successfully changed, a confirmation window opens, as shown in Figure 4-15, where the new key file location and security key identifier are shown.



Figure 4-15 Change Security Key Complete confirmation window

4.4.2 Save security key file

This action will save a backup of the security key file and will require the original pass phrase in order to copy it. It can therefore also be used to verify that the pass phrase stored is correct. To save the security key file, select, from the top left hand corner of the Storage Manager menu, **Storage Subsystem** → **Drive Security** → **Save Security Key File**.

You will be prompted for the location to store the file and the pass phrase used to create or change the existing security key file, as shown in Figure 4-16. The DS5000 Disk Encryption Manager uses the pass phrase to encrypt the security key before it exports the security key to the security key backup file.

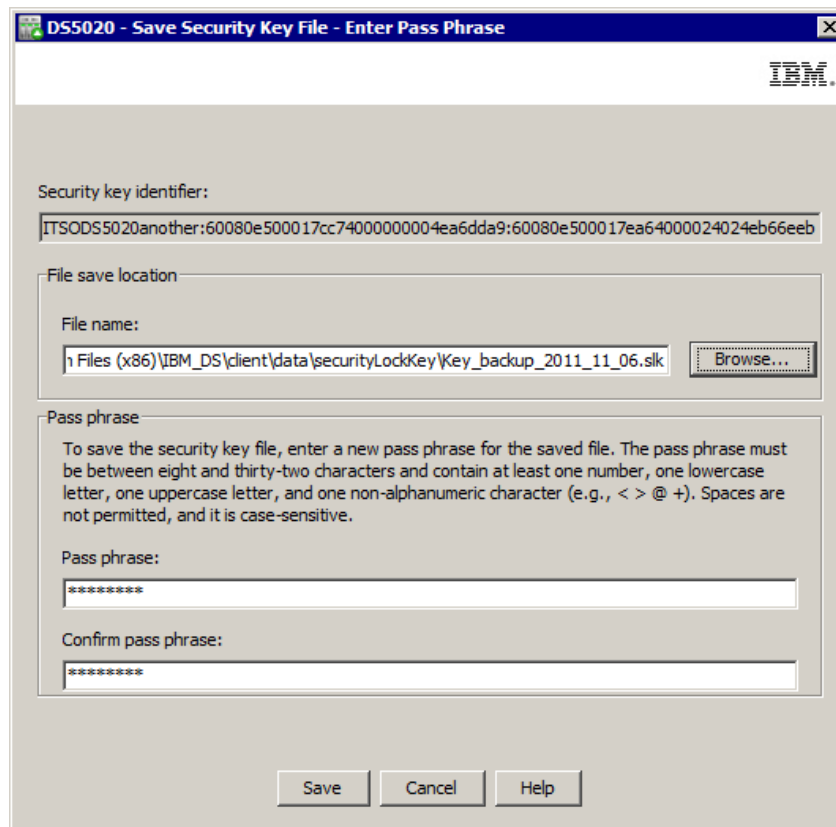


Figure 4-16 Save Security Key File window

4.4.3 Secure erase

Secure erase provides a higher level of data erasure than other traditional methods. When you initiate secure erase with the DS5000 Disk Encryption Manager, a command is sent to the FDE drive to perform a “cryptographic erase”. This erases the existing data encryption key and then generates a new encryption key inside the drive, making it impossible to decrypt the data. Drive security becomes disabled and must be re-enabled if it is required again.

The secure erase process is shown in Figure 4-17.

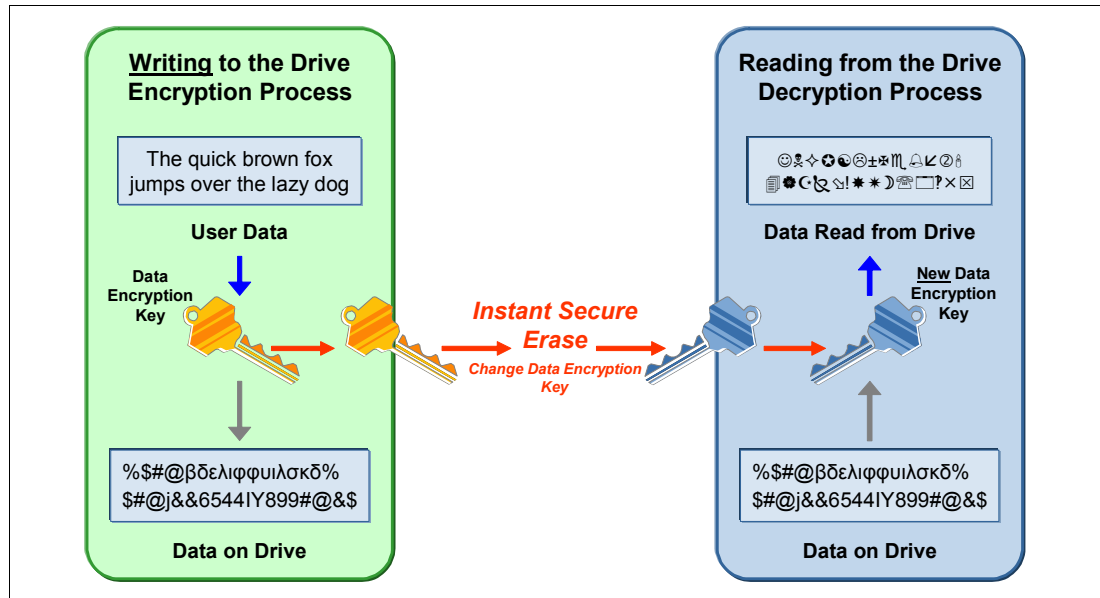


Figure 4-17 Secure erase process

Warning: All data on the disk will be permanently and irrevocably erased when the secure erase operation is completed for a security-enabled FDE drive. Do not perform this action unless you are sure that you want to erase the data, as there is no recovery.

Secure erase can only be performed on drives that are not allocated to an array. The process is also referred to as re-provisioning, where:

- ▶ The FDE drive becomes fully reusable.
- ▶ The drive can be reused in secure or non-secure applications.
- ▶ Previous data and keys are not accessible.
- ▶ It executes in less than a second.
- ▶ It returns the drive to the original factory state.

4.4.4 FDE drive status

The FDE drives have a status indicating whether the disk can be accessed. The statuses are:

- ▶ Locked
 - The drive is security capable.
 - The drive has security enabled.
 - The lock key has not been supplied to the drive.
 - Data cannot be read or written from drive.
- ▶ Unlocked
 - The drive is security capable.
 - The drive has security enabled.
 - The lock key has been supplied to the drive.
 - Data can be read or written from drive.

The locked state will rarely be seen, that is, only when the array containing the disks have been moved to another DS5000 or controllers have been replaced. The drive becomes locked whenever the disk is powered down. The drive will remain unlocked during firmware upgrades or while other components are being replaced. When the drive is powered on, the status will be locked. If it detects a security key identifier, then it will remain locked until it has successfully authenticated with the DS5000 Disk Encryption Manager or external key management software.

4.4.5 Hot spare drive

If a disk drive fails in the DS5000 storage subsystem, the controller uses redundant data to reconstruct the data on the failed drive on a global hot-spare drive. The global hot-spare drive is automatically substituted for the failed drive without intervention. When the failed drive is eventually replaced, the data from the hot-spare drive is copied back to the replacement drive.

Hot-spare drives must meet the array hot-spare requirements. The following drive types are required for hot-spare drives when secure-capable arrays are configured. If a drive does fail, the Storage Manager automatically determines which hot-spare drive to substitute according to the type of the failed drive:

- ▶ For an array that has secured FDE drives, the hot-spare drive must be an unsecured FDE drive of the same or greater capacity. After the unsecured FDE hot-spare drive is used as a spare for a failed drive in the secured RAID array, it is security enabled.
- ▶ For an array that has FDE drives that are not secured, the hot-spare drive can be either an unsecured FDE drive or a non-FDE drive.
- ▶ An unconfigured secured FDE drive cannot be used as a global hot-spare drive. If a global hot spare is a secured FDE drive, it can be used as a spare drive only in secured arrays.

4.5 Migrating secure disk arrays

This section will detail how to migrate an array with Full Disk Encryption enabled to another DS5000. The process consists of exporting the array on the source DS5000 and importing the array on the target DS5000 after the disk have been physically moved. User data remains intact on the drives because configuration metadata (DACStore) is stored on every drive in the DS5000. The export process is the same as an ordinary array, but there are some extra steps to be carried out for the locked drives of the secure array when importing.

4.5.1 Planning checklist

This list is displayed in a window of the migration wizard (Figure 4-19 on page 276). It is important to follow this list when planning an export and import of an array.

On the source DS5000:

- ▶ Save the DS5000 configuration by selecting **Storage Subsystem** → **Configuration** → **Save**.
- ▶ Back up all data at the host level on logical drives of the array.
- ▶ Ensure that all I/O has been stopped to the array, and unmap any logical drives that are mapped on the array, ensuring that each host no longer requires the disk presented to it by the array to be migrated.
- ▶ Locate the array drives on the DS5000, noting the enclosure ID and location slot of each drive member.

- ▶ Save the security key file, as discussed in 4.4.2, “Save security key file” on page 271.
- ▶ Obtain blank canisters or new drives to be inserted in the DS5000 when the drives are removed.

On the target DS5000:

- ▶ Verify that there are available drive slots to host the disk drives.
- ▶ Check that the drives that are being moved are supported. The Full Disk Encryption premium feature should be already enabled, as shown in Figure 4-5 on page 263.
- ▶ Verify that the firmware is the same on the target DS5000 as the source DS5000, and is up to date.
- ▶ Unlock drives before importing the array.

4.5.2 Export the array

From the Storage Manager window, in the Logical tab, select the array that you want to export and then select **Advanced** → **Maintenance** → **Export Array**.

The Export Array wizard will guide you through the export.

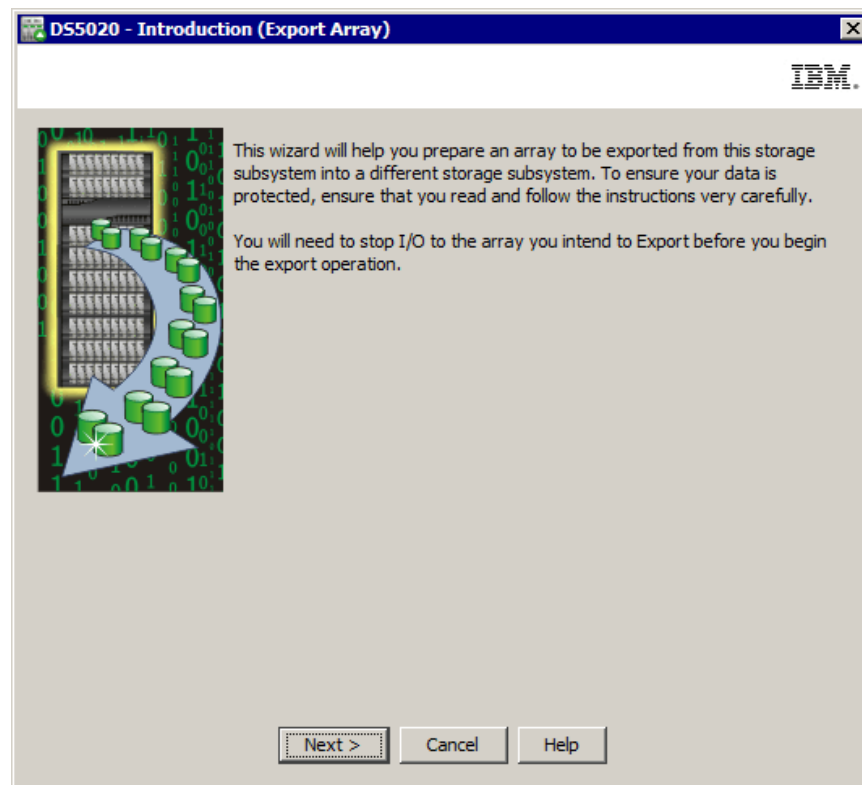


Figure 4-18 Export Array wizard

The window with the preparation checklist opens, as shown in Figure 4-19 on page 276. Check that no planning steps have been missed.

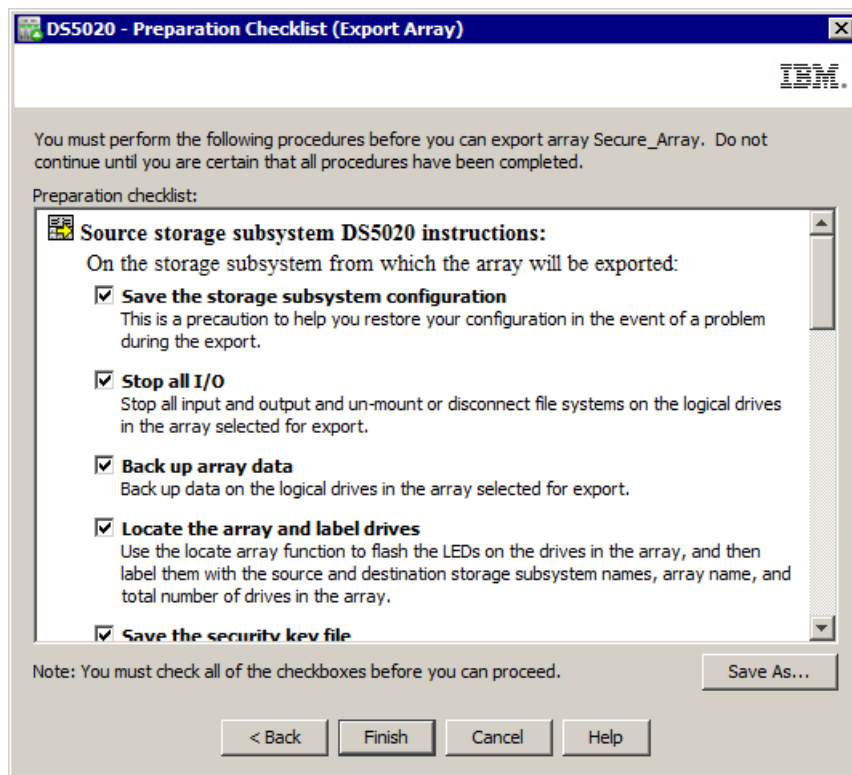


Figure 4-19 Preparation checklist

You need to confirm the export procedure by typing **yes** as shown in Figure 4-20. Click **OK** when you are finished.

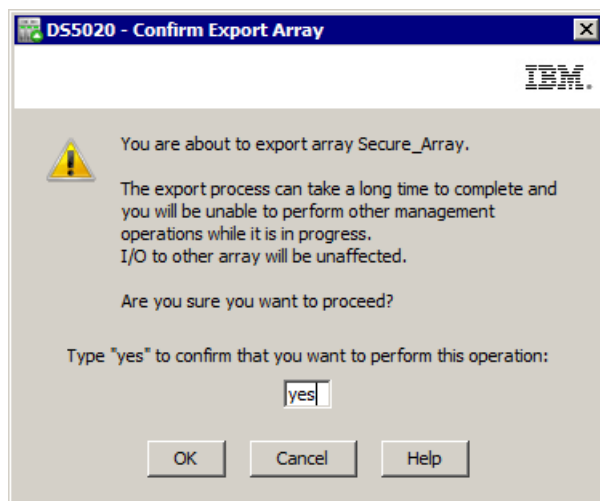


Figure 4-20 Export completed

After export is completed and a window shown in Figure 4-21 on page 277 details the drives that need to be removed from the source DS5000 and inserted in the target DS5000.

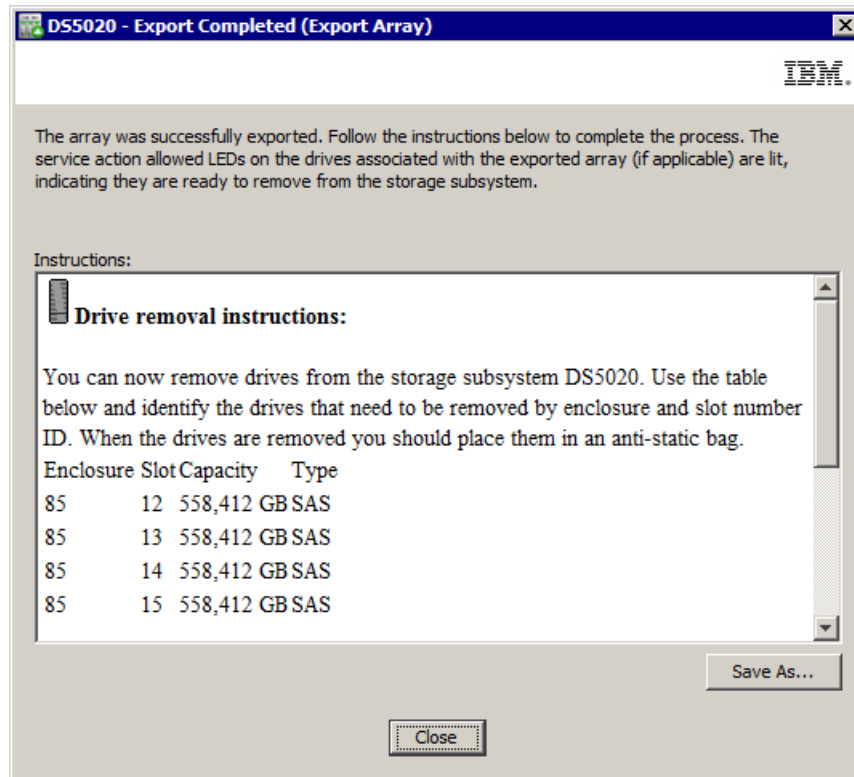


Figure 4-21 Export completed

The Storage Manager will now indicate that the array has been exported and the physical disks are offline. The windows shown in Figure 4-22 and Figure 4-23 confirm this information.

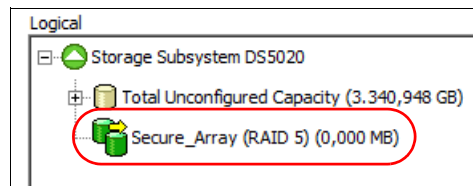


Figure 4-22 Array now exported

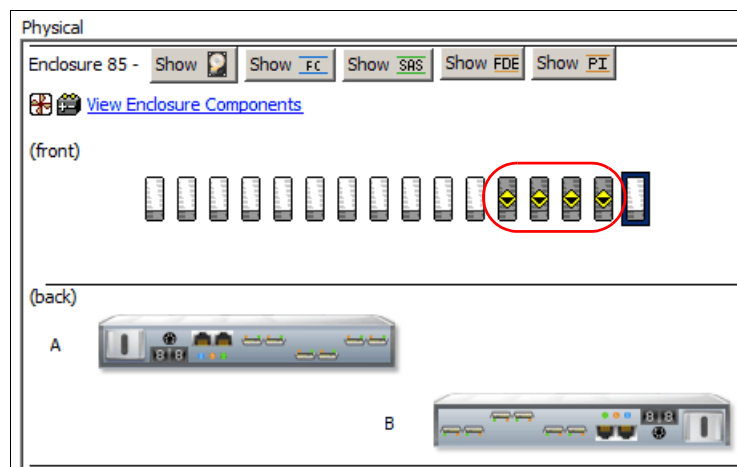


Figure 4-23 Array disks now offline

4.6 Import secure drive array

Once all the disks have been physically moved and are seated correctly in the target DS5000 enclosure, the drives can be unlocked and then the array can be imported. It is necessary to ensure that all the drives are seen by the DS5000 and that there is not a problem with them, as any problems will affect the array after it has been imported.

All drives will be in a locked state, as shown by the event viewer and the individual drive properties, as shown in Figure 4-24 on page 278.


Drive at Enclosure 85, Slot 9		
Status:  Incompatible		
Cause: Full Disk Encryption (FDE) security locked.		
Mode: Incompatible		
Raw capacity: 279,396 GB		
Usable capacity: 279,396 GB		
World-wide identifier: 20:00:00:1d:38:4b:d6:d4:00:00:00:00:00:00:00		
Associated array: None		
Port	Channel	ID
0	1	8/0xD9
1	2	8/0xD9

Figure 4-24 Drive properties show drive being locked

The DS5000 storage subsystem will also indicate that it needs attention due to the locked state of the drives. You can see the details about this situation in the Recovery Guru, as shown in Figure 4-25.

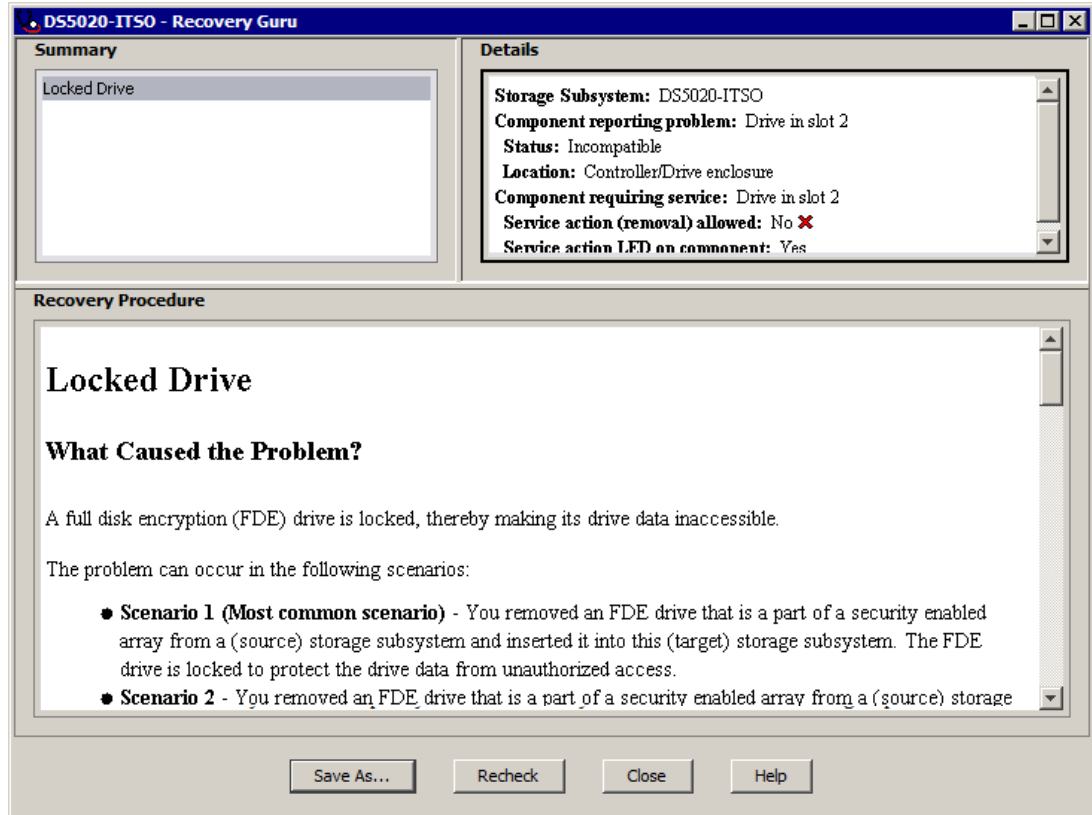


Figure 4-25 Drive locked message in the Recovery Guru

4.6.1 Unlock drives

Prior to importing the array, all drives must be unlocked. Unlock will be done by importing the security key from the source machine. This procedure is performed on one drive, but will then be applied to all drives.

From the Physical tab in the Storage Manager window, select one of the FDE drives that has just been installed (it will be marked as offline). Right-click the drive and select **Import Security Key File...**, as shown in Figure 4-26.

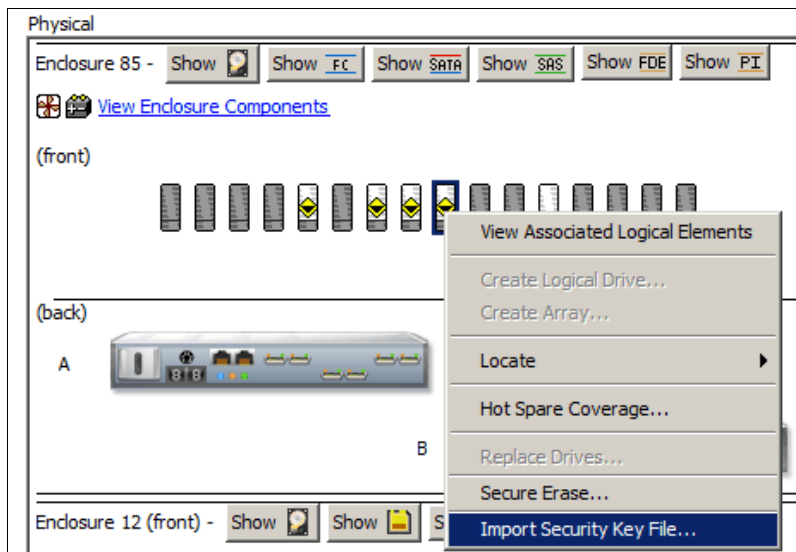


Figure 4-26 Select the Unlock option on the FDE drive

The DS5000 storage subsystem will recognize the FDE drives that are locked and will prompt for the key file and pass phrase, as shown in Figure 4-27.

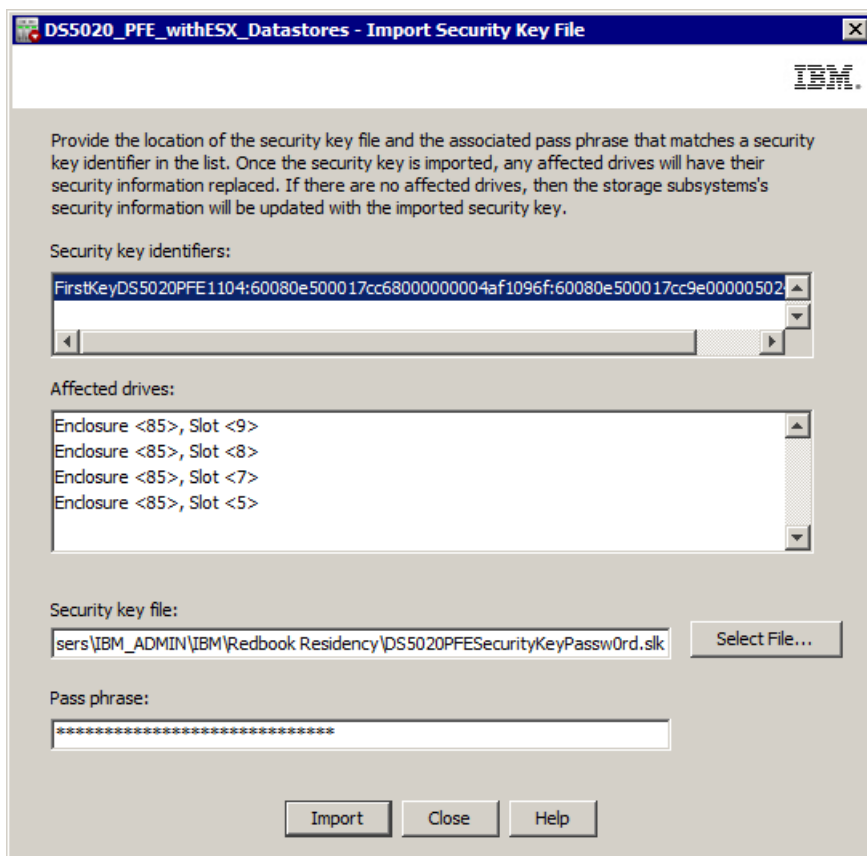


Figure 4-27 FDE drives locked with the key file and pass phrase to unlock

When the correct key file is selected and the pass phrase is entered, all the drives will be successfully unlocked, as shown in Figure 4-28.

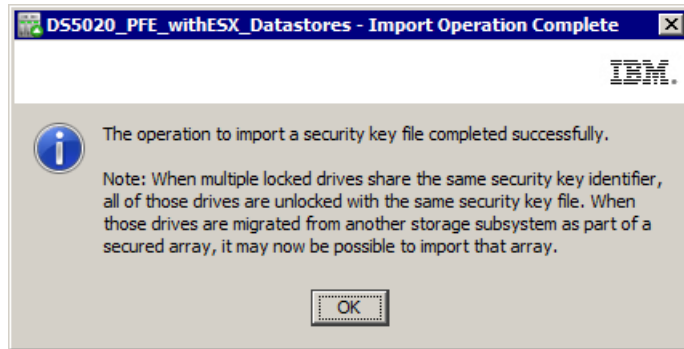


Figure 4-28 FDE drive unlock completed successfully

4.6.2 Import array

The array will be displayed in the Logical tab of the Storage Manager window, and is ready to import, as shown in Figure 4-29.

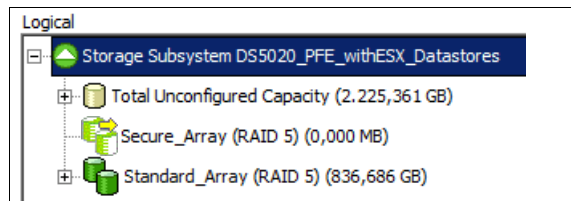


Figure 4-29 Array ready to be imported

Use the Import Array option to import an array that you have previously exported. From the Storage Manager window in the Logical view, select the array and then select **Advanced** → **Maintenance** → **Import Array**. On the introduction screen, shown on Figure 4-30 on page 282, click **Next**.

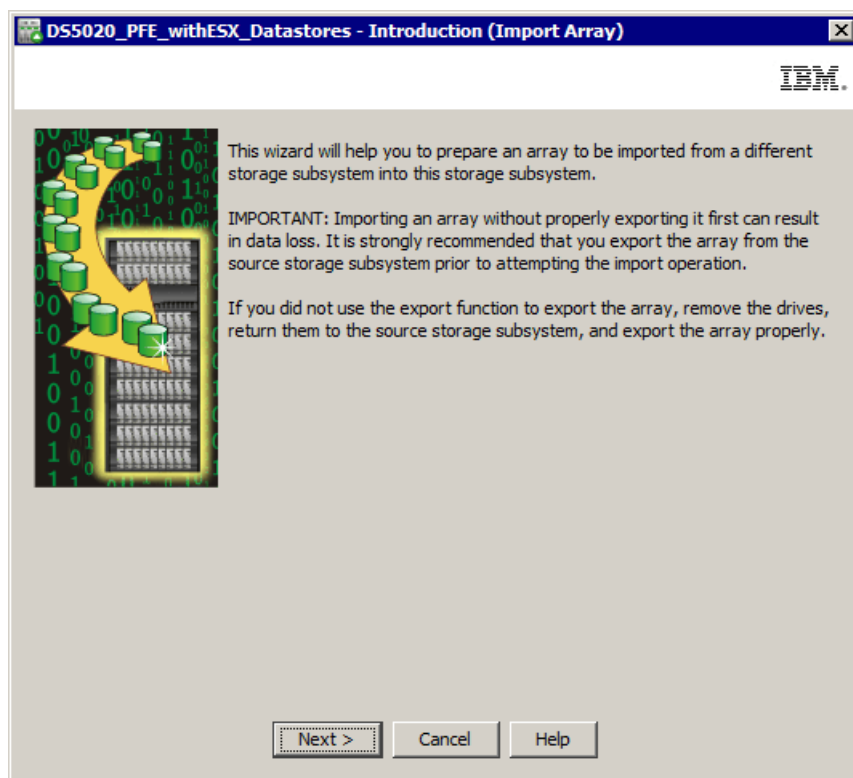


Figure 4-30 Import Array introduction screen

The import array, shown in Figure 4-31, gives details about the disks that will be imported. You need to check that all the disks that are displayed are correct and that none of them are missing.

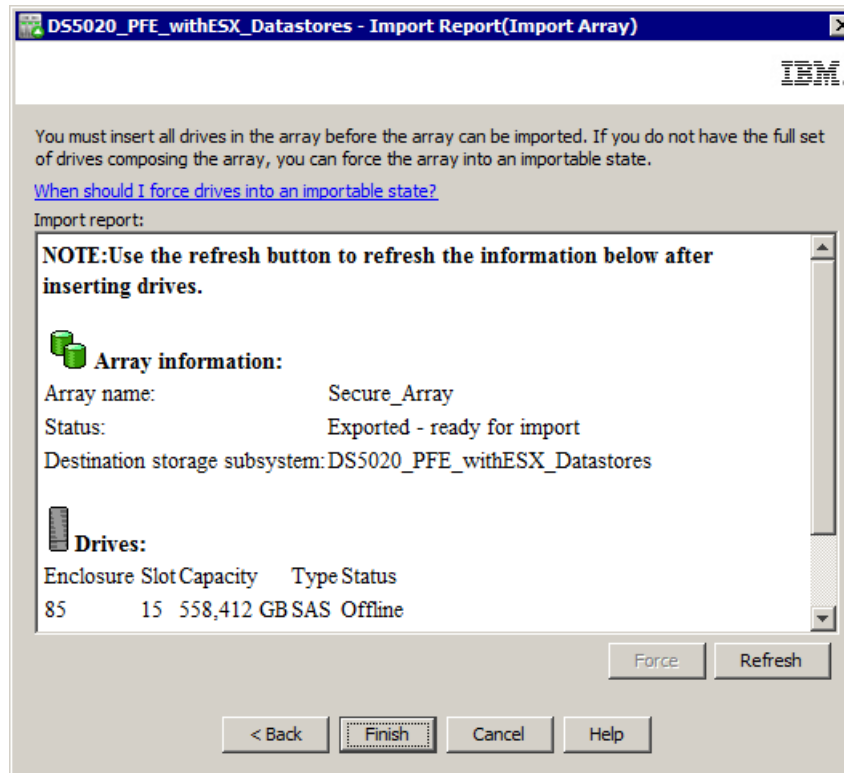


Figure 4-31 Import report indicating all that drives to be imported

Answer **yes** to the prompt to import drives shown in Figure 4-32. Then click on **OK**.

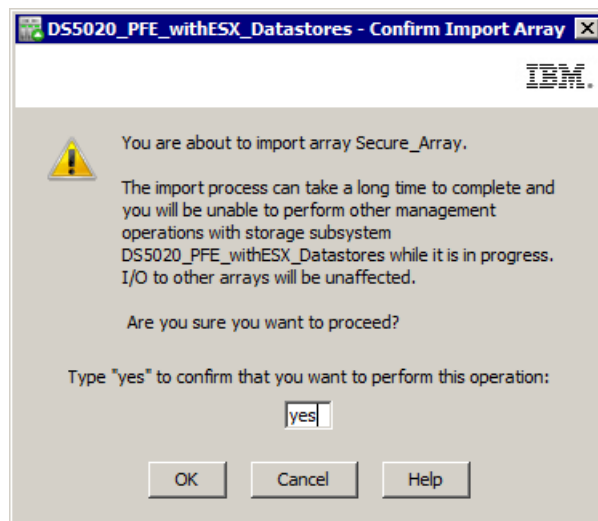


Figure 4-32 Confirm Import Array

Figure 4-33 confirms the importation of the drives.

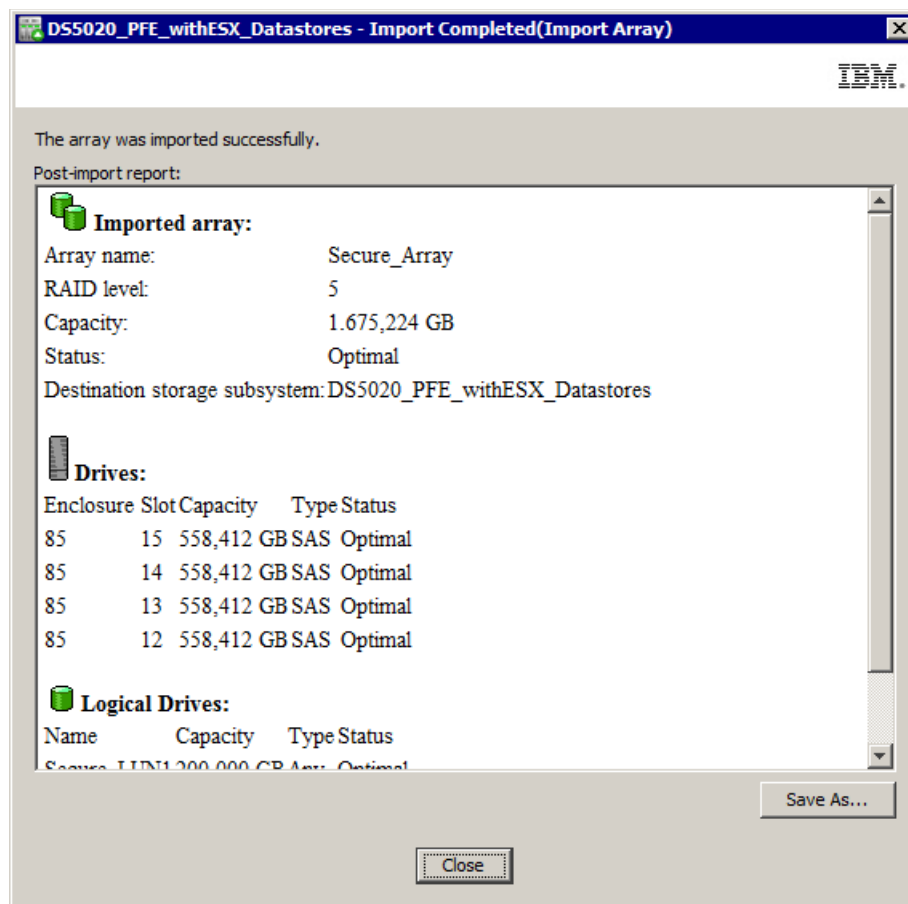



Figure 4-33 Import completed

The logical drives in the newly imported array are now ready to be mapped to hosts, where data can be accessed for read and write operations.

We recommend that you change the key after a secure array is imported to a DS5000 storage subsystem when it already has secure arrays. This will ensure that all secure enabled FDE drives will use a common key for authentication with the DS5000 storage subsystem when they are powered on.

5



Advanced maintenance, troubleshooting, and diagnostics

In this chapter, we explain the advanced Storage Manager functions. We explain, based on examples, how to use the Recovery Guru, the Major Event Log (MEL), Read Link Status, and other diagnostic and recovery tools.

For some operating systems that can be used with the DS5000, we cover tools to manage your DS5000 logical disks, with commands' usage and examples.

We address advanced maintenance topics for the IBM System Storage DS5000 storage subsystem, such as:

- ▶ Upgrade firmware for the different DS5000 components.
- ▶ Upgrade HBA firmware.
- ▶ Other management and maintenance tasks, such as handling the premium features.
- ▶ How to back up your configuration.
- ▶ How to perform drive migration from between different DS storage subsystems using the new facilities for import-export volumes.

5.1 Upgrades and maintenance

This section covers how to manage your DS5000 storage subsystem firmware, describing the steps that are required to upgrade the DS5000 storage subsystem code (this includes the Storage Manager client and firmware of all components) to the latest supported level.

5.1.1 Displaying installed firmware versions

You need to know the firmware level currently installed in your DS5000 storage subsystem. This information is needed when you report a problem to your support representative, if you plan an update after receiving notification of the availability of a new level, or when you want to use a new feature only available with a particular level.

Use the profile data to find the different components' firmware versions in your DS5000 storage subsystem. You can view this data by performing the following steps:

1. Select **Storage Subsystem**, → **View** → **Profile** from the Subsystem Management window, or **Storage Subsystem** → **View Profile** if using older levels of the Storage Manager client.
1. Click the **Controller** tab to display a window, as shown in Figure 5-1. This shows the controller firmware (CFW) and NVSRAM version installed.

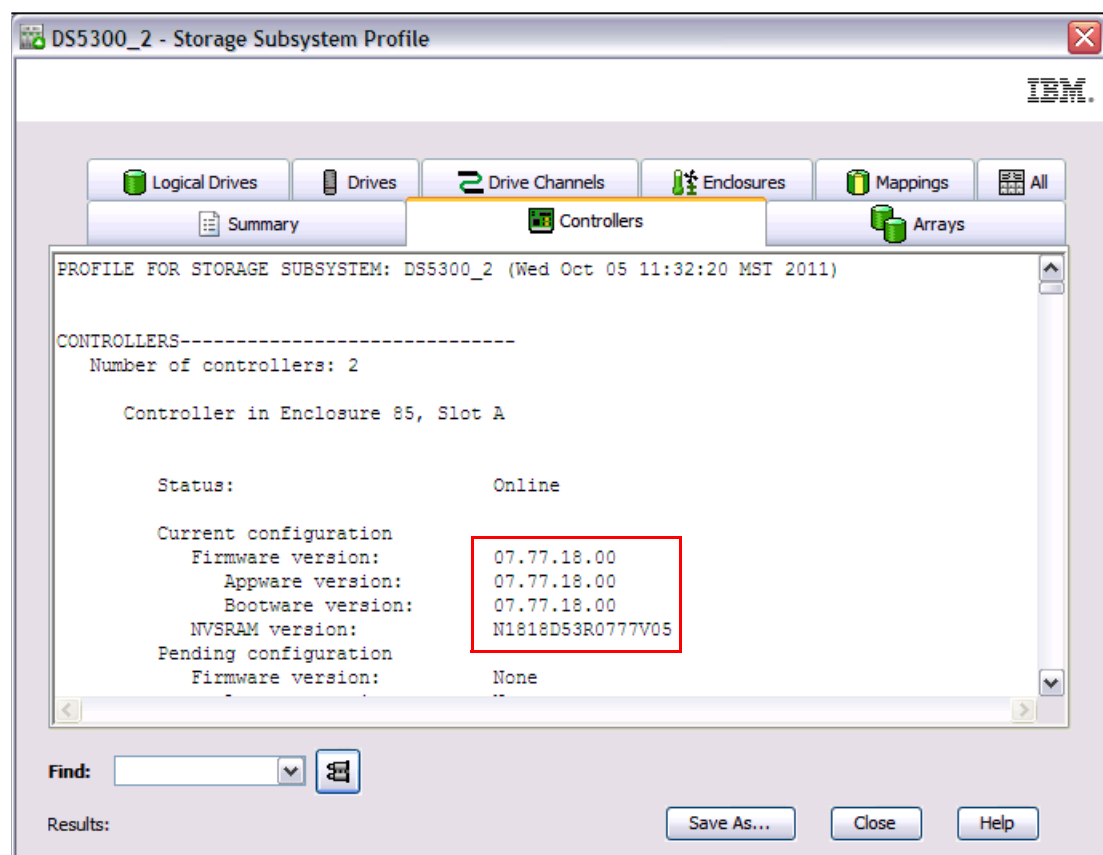


Figure 5-1 Controller and NVSRAM version in Storage Subsystem Profile

- Click the **Enclosures** tab to see the ESM current firmware level. As shown in Figure 5-2, you have to use the scroll bar to show all of the ESM firmware (two per enclosure), as shown in Figure 2-2 by the pointers.

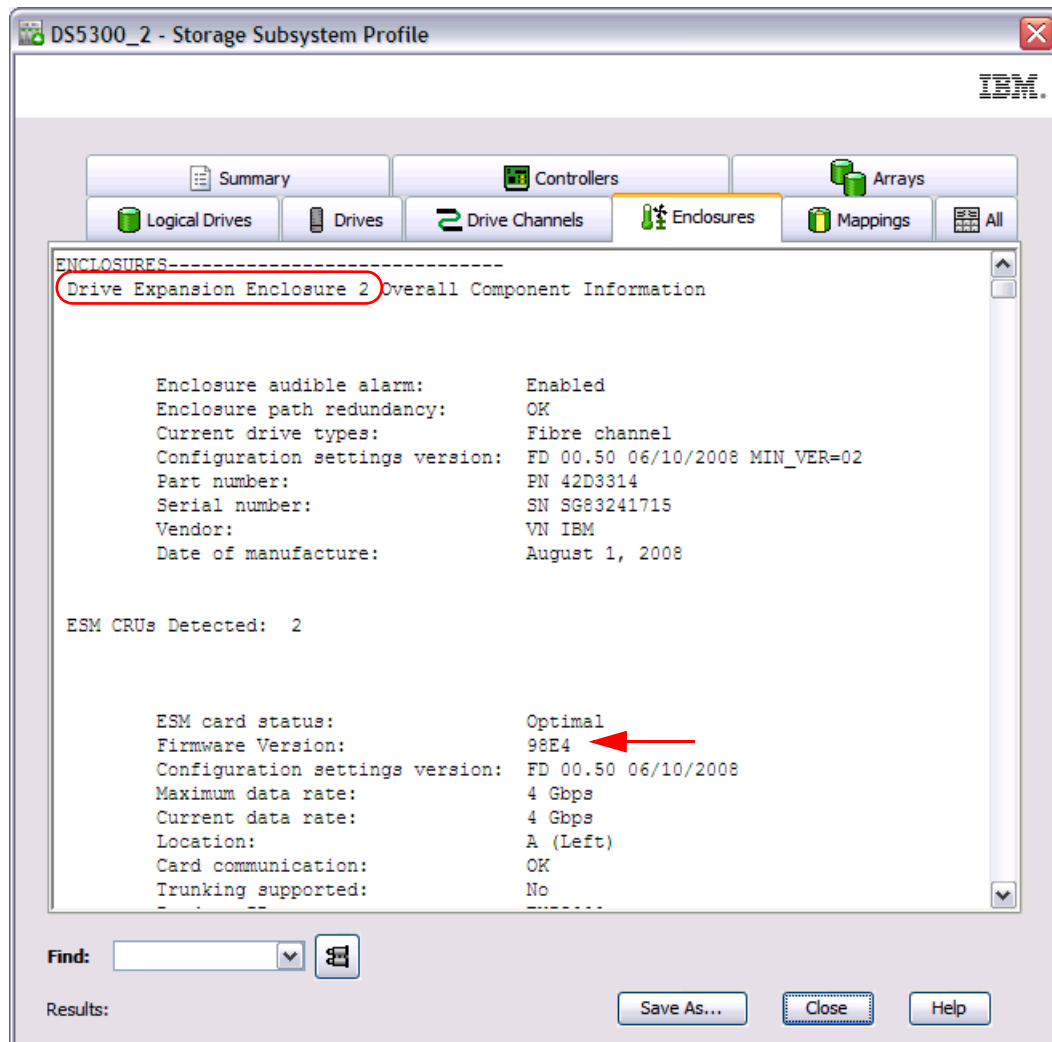


Figure 5-2 ESM firmware in Storage Subsystem profile

- Click the **Drives** tab to see the drives information. Scroll to the right side of the window until the column Firmware Version is visible. Be aware that you might have different drive types in your enclosures, so you can find multiple versions. See Figure 5-3.

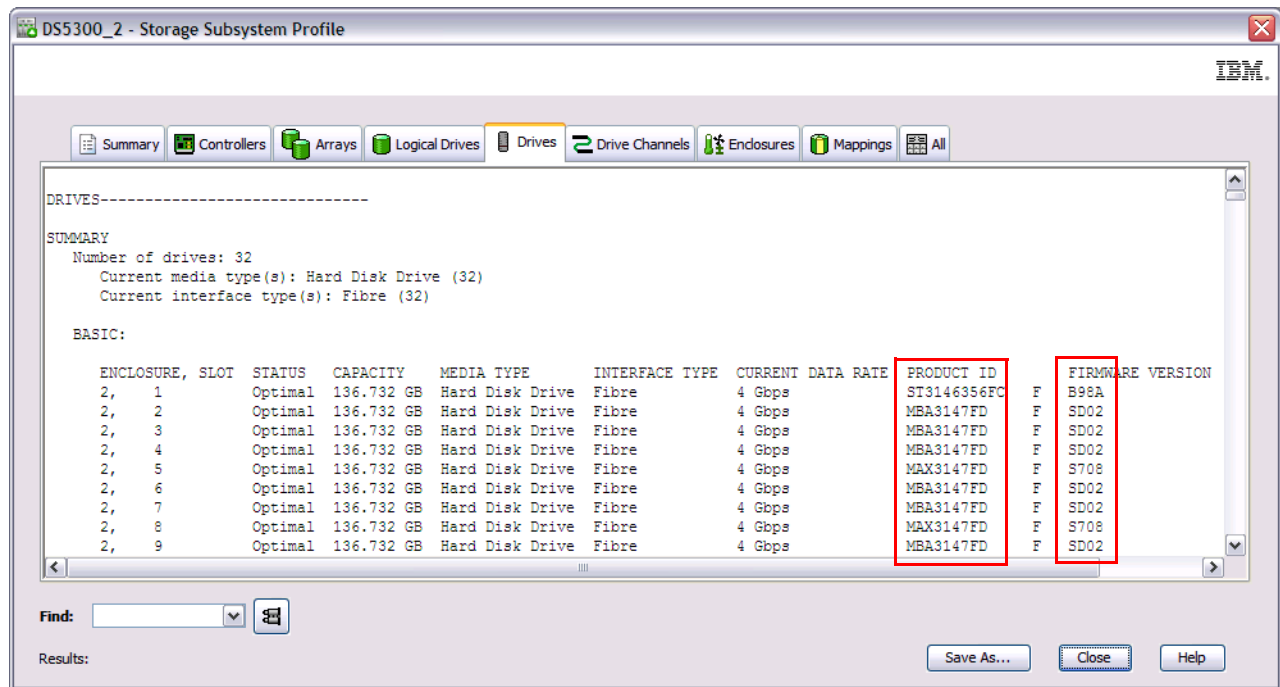


Figure 5-3 Drive firmware in Storage Subsystem profile

5.1.2 Obtaining updates

To download the latest firmware and drivers, and for updates, hints, and tips about known problems, fixes, technical notes, and product flashes (alerts), consult the IBM Support Web site at the following address:

<http://www.ibm.com/support/entry/portal/>

Select your specific DS5000 storage subsystem from **Manage my product list** pop-window and click **Finish** as shown in Figure 5-4 on page 289.

Manage my product list

☒ Browse for a product
☐ Search for a product

☐ DS4300 and DS4300 Express Midrange Disk System
☐ DS4400 Midrange Disk System
☐ DS4500 Midrange Disk System
☐ DS4700 Express
☐ DS4800 Midrange Disk System
☐ DS5020
☐ DS5100
☒ DS5300 | Select OS
☐ IBM Storwize V7000 (2076)
☐ IBM Storwize V7000 Unified
☐ IBM System Storage DCS9550
☐ IBM System Storage DCS9900
 ▶ Fibre Array Storage Technology
 ▶ Entry-level disk systems

>>

My products list

Delete all inactive
Delete all products

Active	Product name
<input type="checkbox"/>	DS5300

Checked products are active and determine the content displayed on the IBM Support Portal pages.

Sign in to access advanced support features.

Finish
Close

Figure 5-4 Manage my product list

On **Support home** page click the **Download** tab and then **View DS5x00 downloads** under **Downloads and fixes** frame to get the latest versions of Storage Manager, firmware, HBA tools, tips, and publications available. There might be more than a one version of firmware available for download. Always review the readme file to make sure that it is the correct version for your product and configuration. If the readme contains specific enhancements or fixes specifically for your system, then consider updating your DS5000 storage subsystem.

Info: You will be required to sign in with an IBM Identity in order to access the code.

If you do not already have one, click the **Register** link on the Sign in page to obtain one. IBM Support is instituting this new procedure so that those who download the code can be contacted if that becomes necessary.

Support Notifications subscription service

There is a Support Notifications subscription service that can be accessed at the IBM System Storage product support Web site. This service is designed to keep you informed of new or updated IBM System Storage support site information, without the need to periodically check the IBM Support Web site for updates. Subscribe Support Notification service for your product at the following address:

https://www.ibm.com/systems/support/myview/subscription/css.wss/subscriptions?methodName=createNewSubscription&brandind=5000028&css_key=s028

System Storage Interoperation Center (SSIC)

If you are planning to add a new host to your storage, add expansions, change HBAs in your hosts, perform other hardware configuration changes, or upgrade Operating System on your host, check for the latest supported combinations at the following Web site:

<http://www.ibm.com/systems/support/storage/ssic/interoperability.wss>

This replaces the older compatibility matrix PFD files.

5.1.3 Planning for upgrades

Upgrading the firmware and management software for the DS5000 storage subsystem is a relatively simple procedure, but some preparation and caution are needed to ensure a smooth upgrade.

Important: Always check the readme files of the firmware you are going to install for prerequisites before proceed with the update.

Attention: All subsystems currently using 7.36.08 and 7.36.12 firmware **MUST** run a file system check tool (DbFix) before and after the firmware upgrade to 7.60.xx.xx or higher.

Check the Dependencies section on firmware readme for further details. The components that typically need to be updated are:

- ▶ Storage Manager software
- ▶ Controller firmware
- ▶ NVSRAM firmware
- ▶ ESM firmware
- ▶ Disk drives firmware

Note: Always make a backup of data before you start an upgrade.

Upgrading large storage configurations can be time consuming. Time estimates for upgrading all the associated firmware and software are listed in Table 5-1.

Table 5-1 Upgrade times

Element being upgraded	Approximate time of upgrade
Storage Manager and associated drivers and utilities	35 minutes
ESM firmware	5 minutes per ESM
DS5000 storage subsystem firmware and NVSRAM	5 to 35 minutes
Hard drives	2 minutes per drive (but it is possible to do a parallel firmware upgrade, even for multiple drive types)

These times were observed in the lab. They are approximate and might vary from system to system. When activating controller firmware or NVSRAM, the maximum times are 15 minutes per controller.

It is mandatory to update all components to the matching levels (refer to the firmware readme file you are upgrading to). You must *not* run a mismatched set.

Linux environments

It is required to have the correct kernel version in order to install the RDAC driver. RDAC is still the preferred failover driver for Linux systems. Following are the supported versions.

Table 5-2 linux OS and RDAC versions list

Operating System	kernel version	RDAC version
SLES 11.1	2.6.32.12-0.7	09.03.0C05.0504
SLES 10-SP4	2.6.16.60-0.85.1	09.03.0C05.0504
SLES 10-SP3	2.6.16.60-0.54.5	09.03.0C05.0504
RHEL6	2.6.32-71	09.03.0C05.0504
RHEL5-u6	2.6.18-238	09.03.0C05.0504
RHEL5-u5	2.6.18-194	09.03.0C05.0504
RHEL4-u8	2.6.9-89.EL	09.03.0B05.0439

Note: Starting from version 07.70.38 Linux Device Mapper Multipath (DMM) driver is also supported.

5.1.4 Updating the DS5000 storage subsystem host software

In this section we discuss how to update the DS5000 storage subsystem host software on a Windows and Linux host server.

Important: Storage Manager host software has to be updated to version 10.77 in order to manage a DS5000 storage subsystem with controller firmware version 7.77. You must update the Storage Manager software before performing the firmware upgrade.

Older storage subsystems running at controller firmware version 5.x are no longer supported by Storage Manager Version 10.77.

Code update for the Windows environment

The IBM System Storage DS Storage Manager could be upgraded by the Installation wizard InstallAnywhere. Launching the installation program all the components previously installed on the management console will be automatically upgraded. For details about the installation procedures, see 3.2, “Installing IBM System Storage DS Storage Manager” on page 128.

Code update for the Linux environment

You can update the host-based DS5000 storage subsystem software for Linux either with InstallAnywhere or manually. See the readme of the host software for a detailed procedure.

The steps below explain the manual update procedure for all hosts running with RDAC:

1. Uninstall the earlier version of Storage Manager components.
2. Install SMruntime.
3. Install SMclient.
4. Disable and enable the Event Monitor.
5. Install the IBM FC HBA non-failover version device driver for Linux.
6. Install Linux RDAC.
7. Install SMagent (optional).
8. Install SMutil.
9. Make sure that the correct host type is specified.

5.1.5 Updating controller firmware

You have the option to download the firmware and NVSRAM immediately but activate it later, when it might be more convenient, or at the same time.

The firmware is transferred to one of the controllers, which then copies the file to the other. The image is verified through a CRC check on both controllers. If the checksum is okay, the uploaded firmware is marked as ready and available for activation. If one of the two controllers fails to validate the CRC, the image is marked as invalid on both controllers and is not available for activation. An error is returned to the management station as well.

Important: Always check the readme files of the firmware you are going to install for prerequisites and dependencies before proceed with the update.

Upgrading firmware and NVSRAM

The microcode of the DS5000 storage subsystem controllers consists of two packages:

- ▶ Controller firmware
- ▶ NVSRAM

The NVSRAM is a part of code which contains the storage subsystem settings. You can image it similar to the settings in the BIOS of a Host Bus Adapter (HBA). The firmware and the NVSRAM are closely tied to each other and are *not* independent. Be sure to install the correct combination of the two packages.

Important: Before upgrading the storage subsystem firmware and NVSRAM, make sure that the system is in an optimal state. Fix any problems before you proceed with the upgrade.

The upgrade procedure needs two independent connections to the DS5000 storage subsystem, one for each controller. It is not possible to perform a microcode update with only one controller connected. Therefore, both controllers must be accessible either through Fibre Channel or Ethernet. Both controllers must also be in the Optimal state.

Important: Make sure to install the firmware for each of the DS5000 storage subsystem components (ESM, drives, controller, and NVSRAM) in the sequence described in the attached readme file.

Update the controller firmware and then the NVSRAM, or both at the same time.

Any power or network/SAN interruption during the update process might lead to configuration corruption or extended downtime. Therefore, do not power off the DS5000 storage subsystem or the management station during the update. If you are using in-band management and have Fibre Channel hubs or managed hubs, then make sure that no SAN-connected devices are powered up during the update. Otherwise, this can cause a loop initialization process and interrupt the process.

In general, the controller, NVSRAM, and ESM firmware upgrades can be done online during non-peak time if your DS5000 storage subsystem has redundant controllers, if a multipath driver is installed on all the hosts, and if a correct san zoning is implemented.

The activation procedure can be done immediately after the transfer, or later during a period of low I/O access. During the activation, the first controller moves all logical drives to the second one, then it reboots and activates new firmware. After that, once reboot is completed,

it takes ownership of all logical drives, and the second controller reboots in order to activate the new firmware. When both controllers are up again, the logical drives are redistributed to the preferred paths.

If you choose to do not activate the new firmware just transferred, remember that a normal reboot of a controller or a power cycle of the DS5000 storage subsystem does not activate the new firmware. To activate the pending firmware you have to select **Advanced** → **Maintenance** → **Activate Controller Firmware**.

To perform the firmware and NVSRAM update, perform these steps:

1. Open the Subsystem Management window for the DS5000 storage subsystem that you want to upgrade. To download the firmware, select **Advanced** → **Maintenance** → **Download** → **Controller Firmware**, as shown in Figure 5-5.

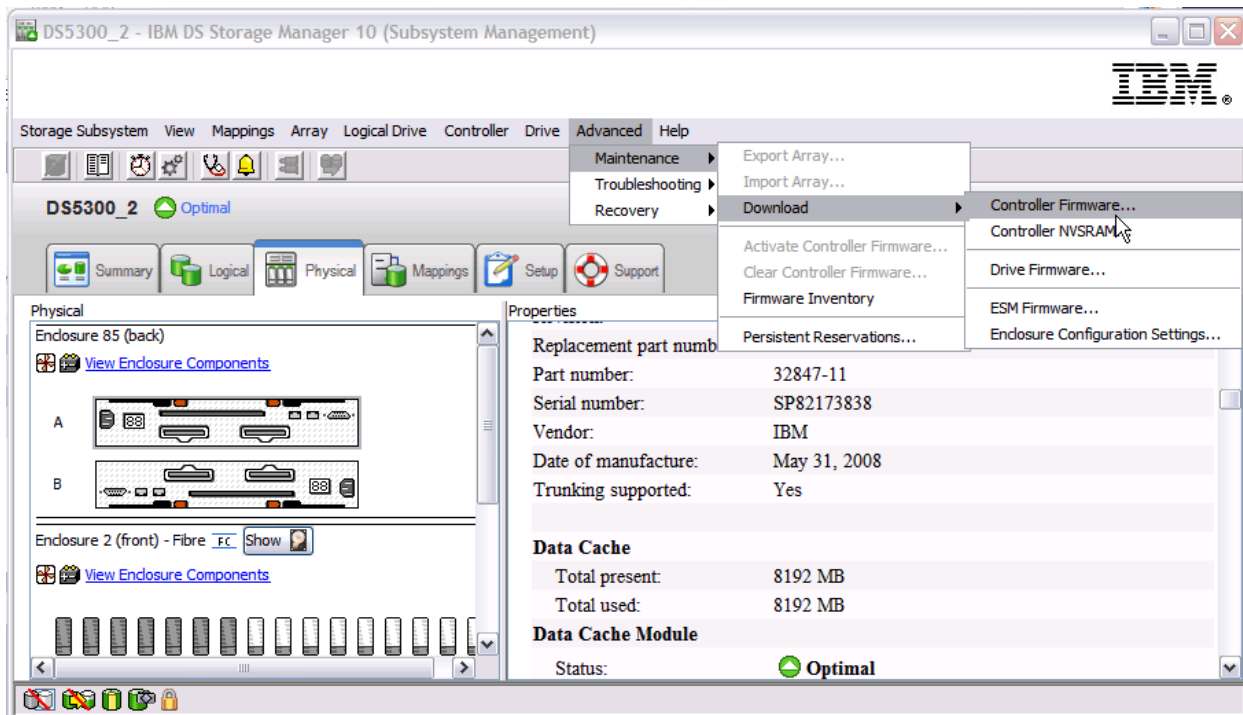


Figure 5-5 Subsystem Management window: Controller Firmware upgrade

2. Click **OK** on pop-up window to run firmware precheck as shows on Figure 5-6.

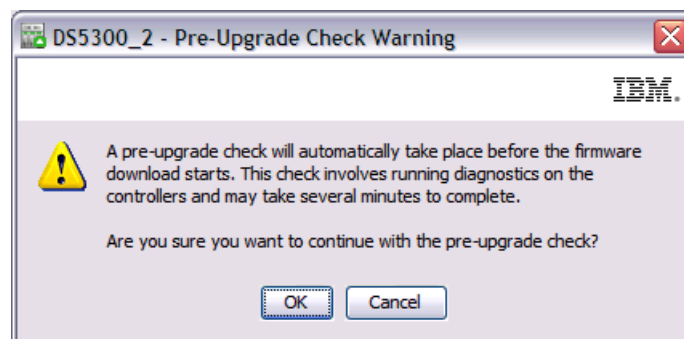


Figure 5-6 confirm system precheck

3. Once precheck is completed, the Download Firmware window opens, showing the current firmware and NVSRAM versions. Select the firmware and NVSRAM files you want to upgrade to, as shown in Figure 5-7. Check the box to download the NVSRAM file as well.

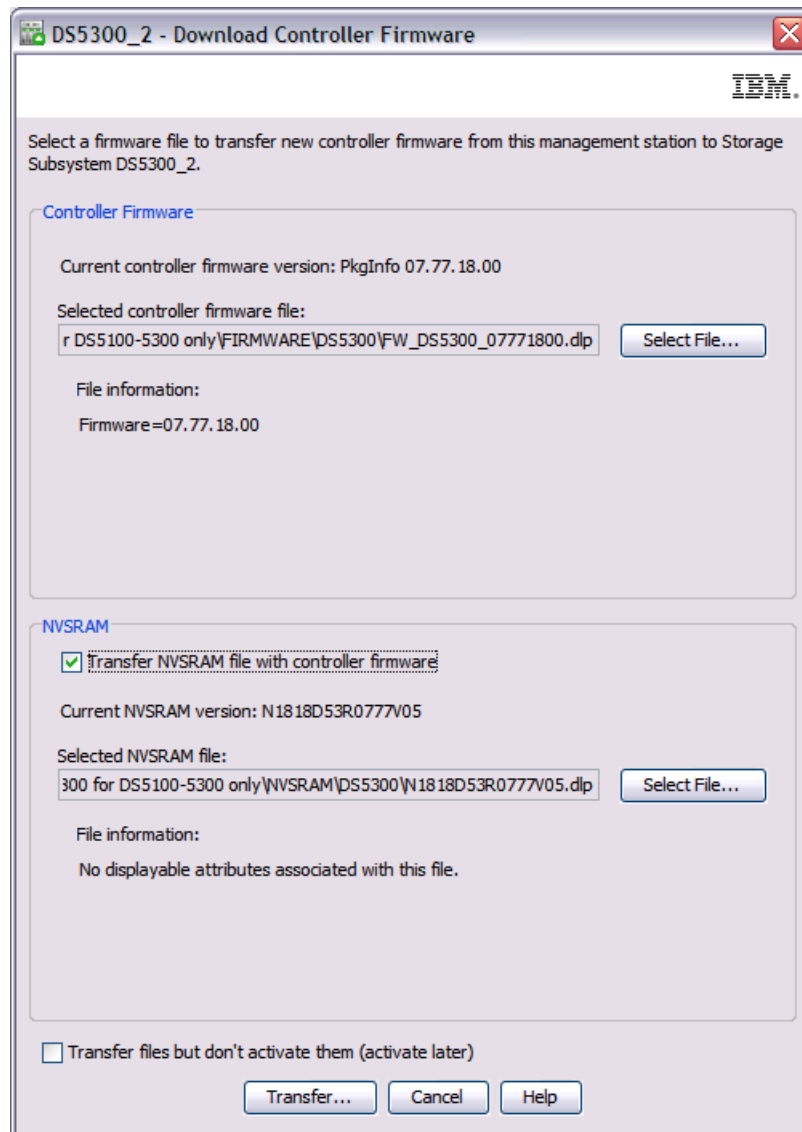


Figure 5-7 Download Firmware window

Note: If you choose to transfer and activate immediately, do not select **Transfer files but don't activate them (activate later)**. Otherwise, select the check box to select **Transfer files but don't activate them (activate later)**. To activate the firmware at a later time, click **Advanced** → **Maintenance** → **Activate Controller Firmware** in the Subsystem Management window.

4. Then click **Transfer...** to continue. You will see the window shown in Figure 5-8 on page 295.

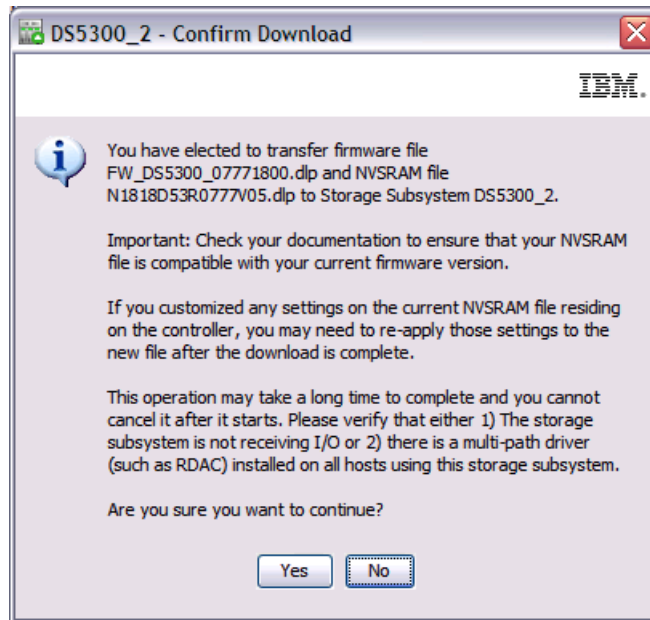


Figure 5-8 Firmware Download confirmation window

5. Click **Yes** to confirm the firmware and NVSRAM download (Take care that the process cannot be cancelled after it begins). The firmware/NVSRAM transfer begins and you can see the progress as shown in Figure 5-9.

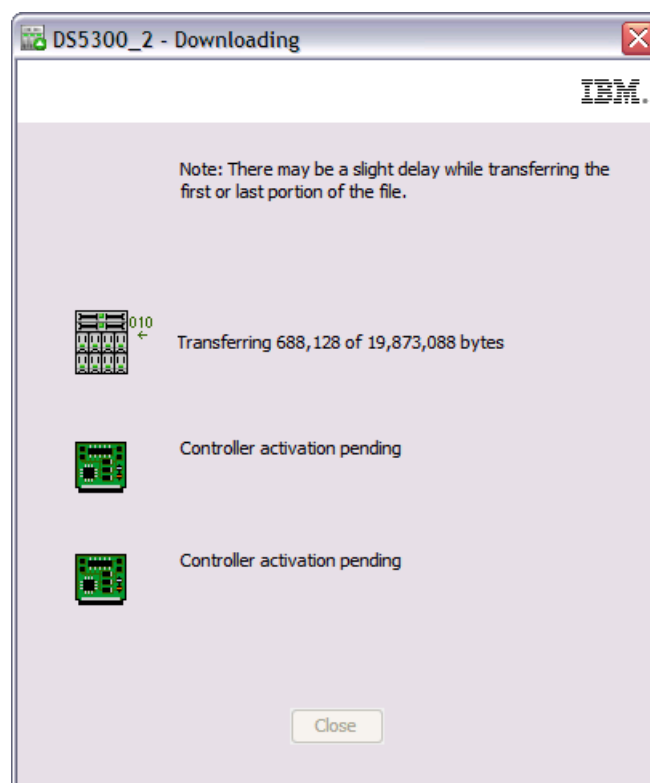


Figure 5-9 Firmware transfer progress

When transfer is completed, if you selected to activate the firmware immediately, the activation automatically starts on one controller at a time as shown in Figure 5-10.

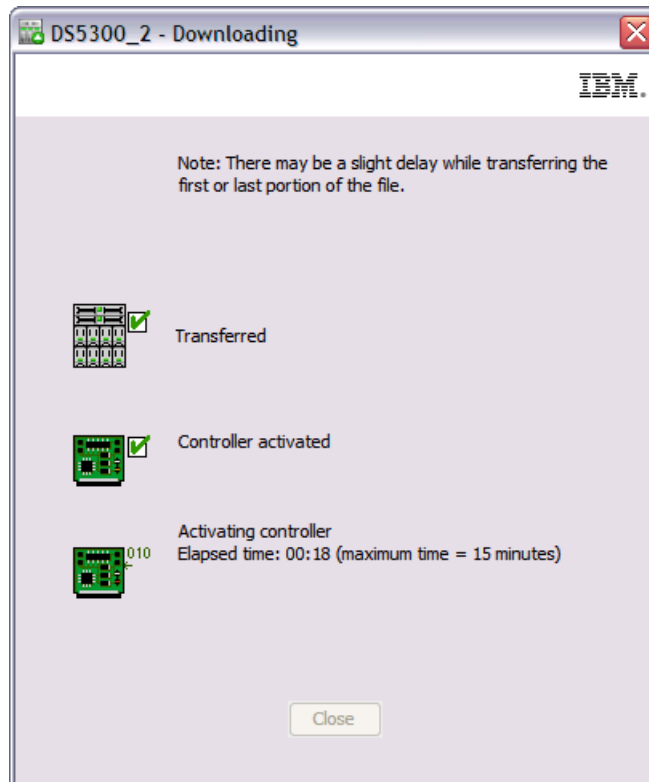


Figure 5-10 Activation code progress status

Once firmware download is successfully completed, click on close as shown in Figure 5-11.

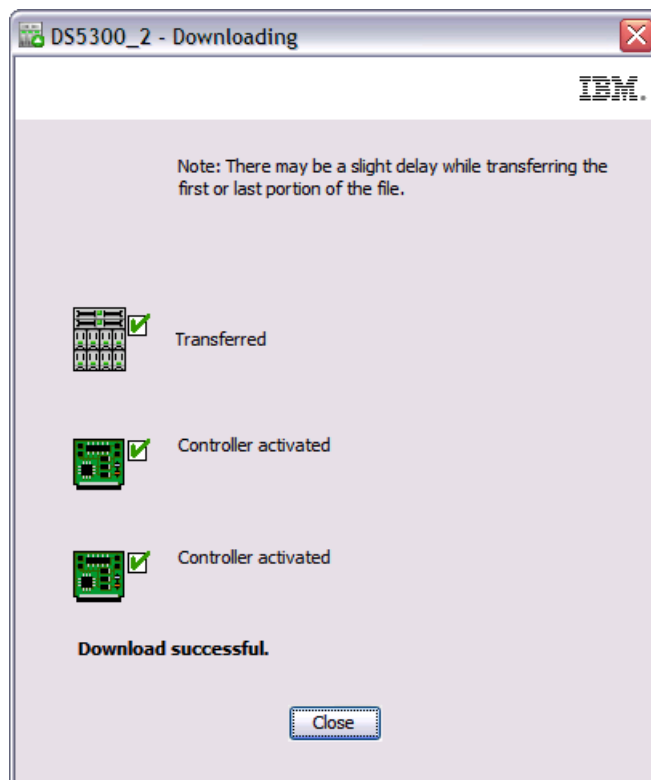


Figure 5-11 Activation firmware completed

6. Once completed clicking on **Close** you are back in the Subsystem Management window.
7. If you choose a staged firmware upgrade, the new firmware is now ready for activation but not yet active. To activate it, select **Advanced** → **Maintenance** → **Activate Controller Firmware**, as shown in Figure 5-12.

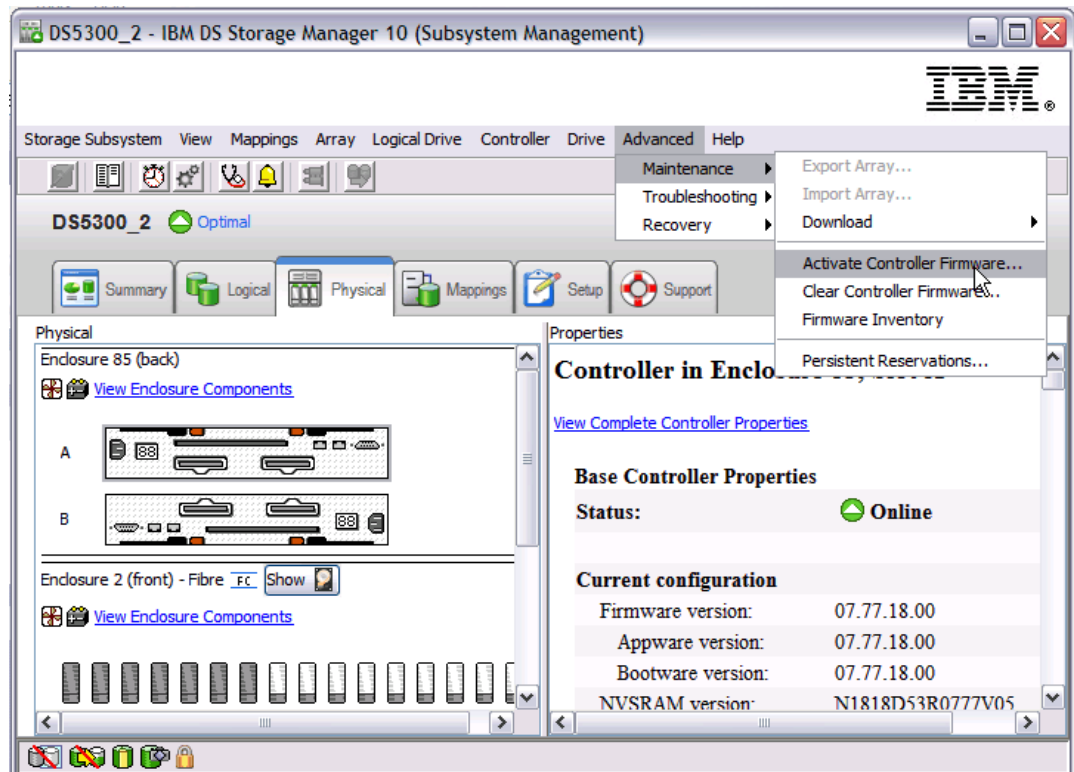


Figure 5-12 Activate staged firmware manually

8. The Activate Firmware window opens and asks you for confirmation to continue, as shown in Figure 5-13. Click **Yes**.

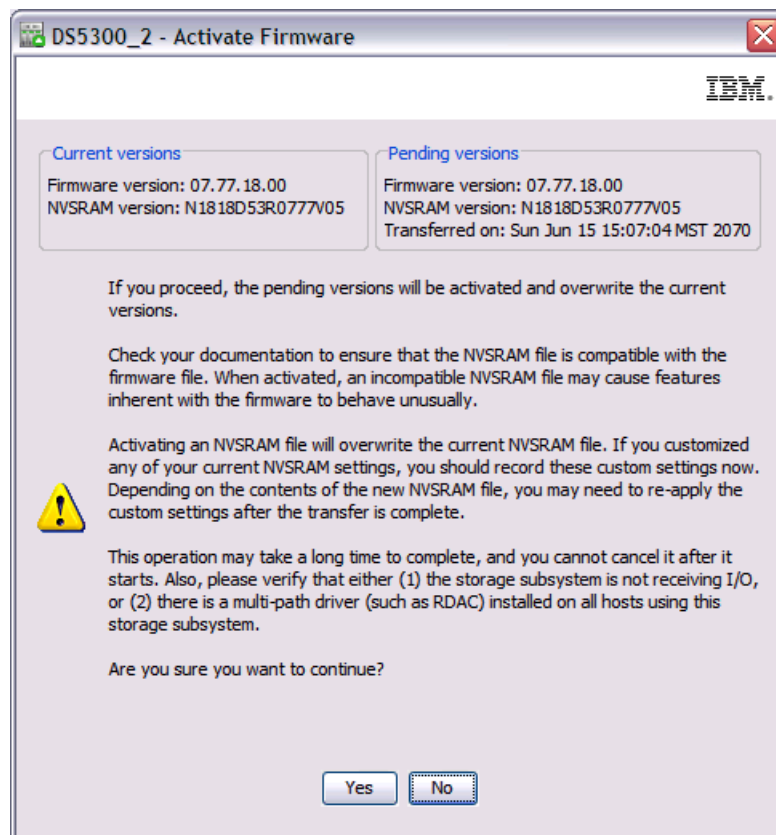


Figure 5-13 Activation firmware confirmation

After you click **Yes**, the activation process starts. The activation applies the transferred code to the controllers one at a time, rebooting first one, then the other. If you have all your hosts with path redundancy, you should not see more of a problem than with the disks going through one controller to the other while they are rebooted. We recommend scheduling this activation during a period of low I/O access.

You can monitor the progress in the Activation window, as shown in Figure 5-14 and Figure 5-15.

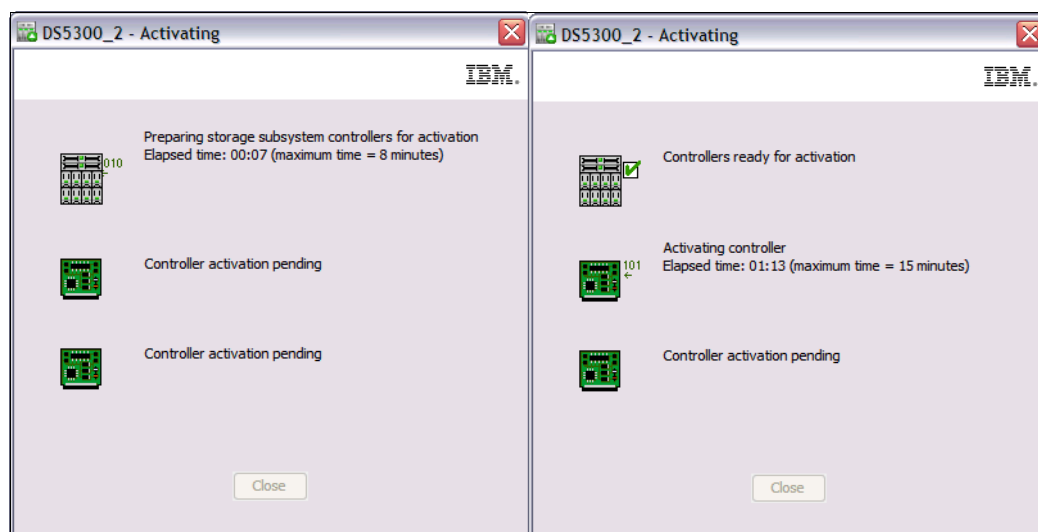


Figure 5-14 Activating firmware progress

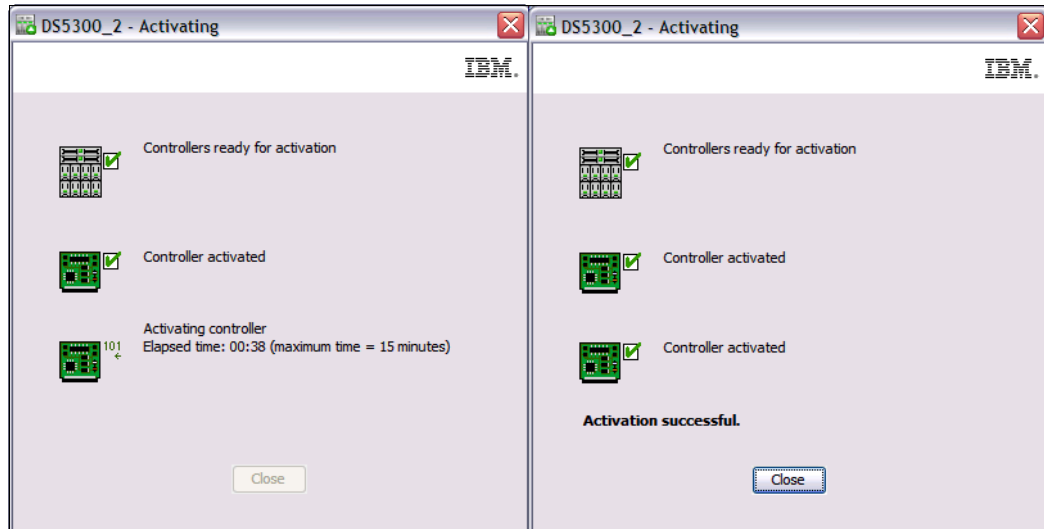


Figure 5-15 Activating firmware progress

When the new firmware is activated on both controllers, you see the “Activation successful” message. Click **Close** to return to the Subsystem Management window.

5.1.6 Updating the ESM board firmware

Before performing a firmware upgrade, read the specific firmware version readme file for details about the installation. Pay attention to any dependencies between controller and ESM, or drives, because there might be a specific sequence in which each of the components are updated. ESM updates are necessary to allow new drive types in the expansion enclosure.

If an ESM is replaced in an EXP5000, EXP520, or EXP810, there is a firmware synchronization feature that ensures that a new ESM is automatically synchronized with the firmware in the existing ESM. This resolves any ESM firmware mismatch conditions automatically. You still have the option to update the ESM firmware manually to a new level, or, if there is a failure that prevents the code from synchronizing, identify which ESM is the original and which is the replacement one to synchronize.

For EXP5000, EXP520, and EXP810, there is an option to set the enclosure settings using the Storage Manager by selecting **Maintenance** → **Download** → **ESM Configuration Settings**. This option should be used when ESM reports different versions of configuration settings, and the software could not resolve the mismatch problem by automatically synchronizing the configuration settings between the two ESMs automatically.

Important: Before upgrading the ESM firmware, make sure that the system is in an Optimal state. If not, run the Recovery Guru to diagnose and correct the problem before you proceed with the upgrade.

If you have new expansion enclosures firmware to update, perform the following steps to transfer a firmware file to the ESM boards:

1. From the Subsystem Management window, select **Advanced** → **Maintenance** → **Download** → **ESM Firmware**, as shown in Figure 5-16.

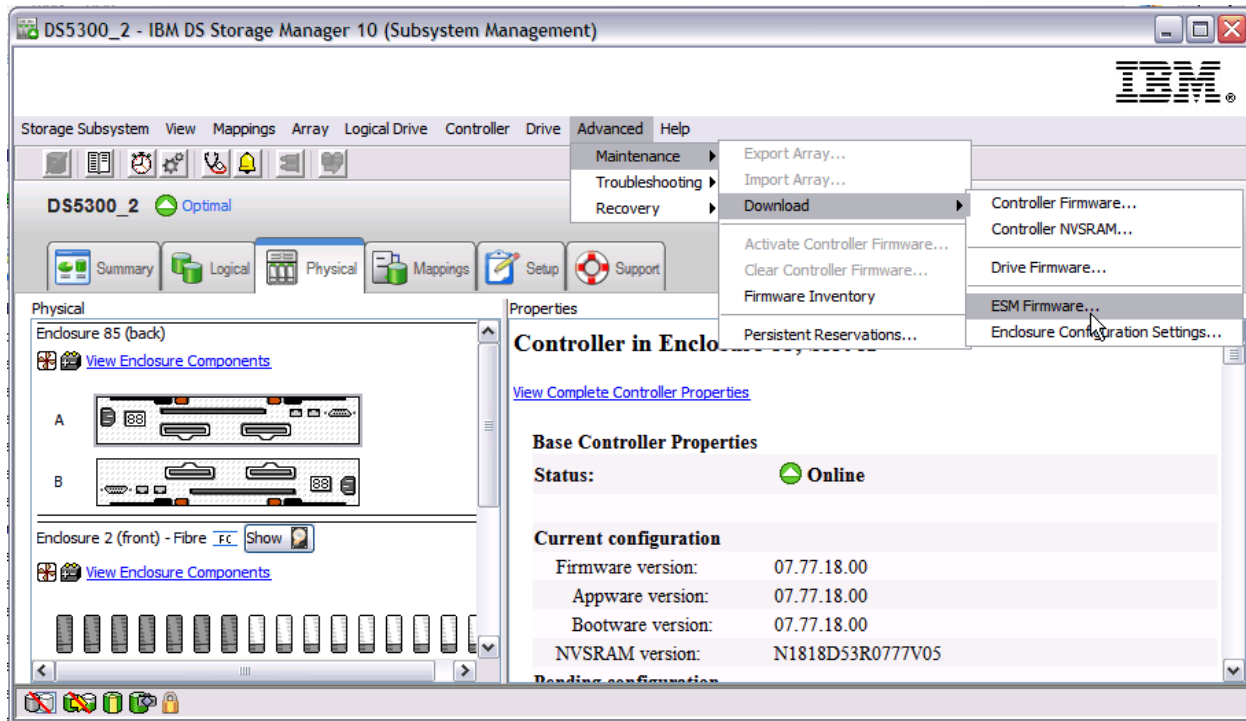


Figure 5-16 Download ESM firmware

2. The Download Environmental (ESM) Card Firmware main window opens, as shown in Figure 5-17.
 - The Select Enclosures Table lists all the enclosures found attached to the storage array that contain ESM cards.
 - The Select File allows you to specify the ESM firmware file to use as the source of the upgrade.

Note: If an ESM card does not show up in the list (because of a loss of redundancy or some other problem), run the Recovery Guru to diagnose and correct the problem before continuing with the download to avoid losing both paths to the disks.

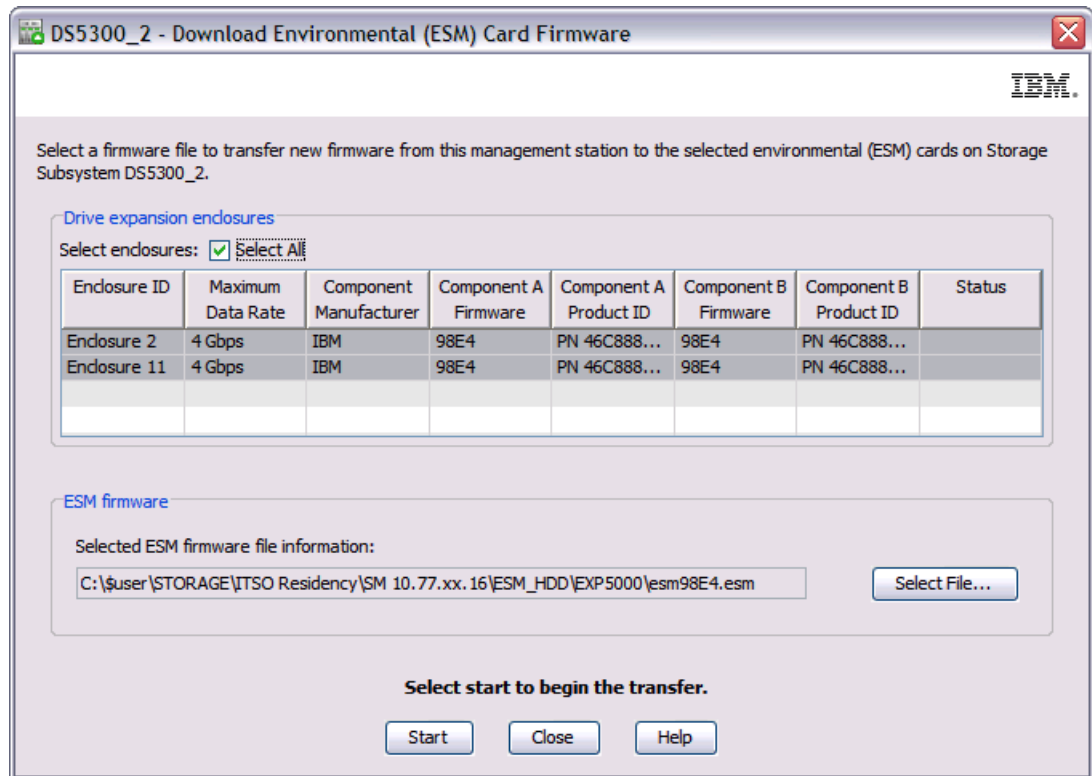


Figure 5-17 Download ESM firmware window

3. In the Select enclosures area, highlight each enclosure to which you want to download firmware or check the **Select All** button to highlight all drive enclosures in the storage subsystem (each drive enclosure selected should have the same product ID).
4. Enter the firmware file to download in the Select file area by either entering the location and name of the file in the Select file text box, or by selecting **Select File...** and getting the firmware file from a local or network drive. (The browse button is unavailable until an enclosure has been selected.)
5. Click on **Start**. Confirm your selections and then confirm download by typing **yes** and click **OK** to continue with the firmware download as shown in Figure 5-18 on page 301 or **Cancel** to quit.

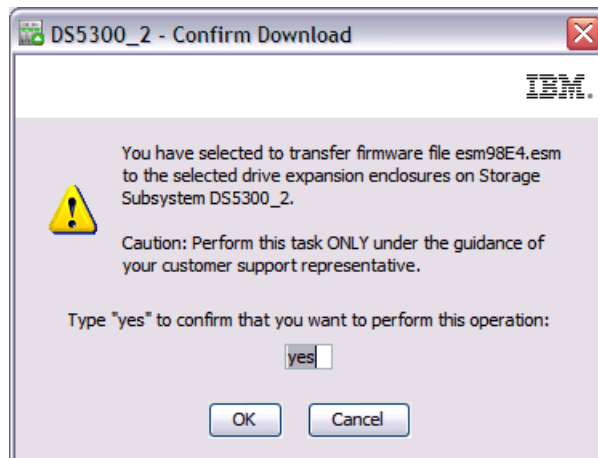


Figure 5-18 confirm ESM firmware download

6. The Status field in the Select enclosures table changes from Pending to Transferring for the ESM card firmware operation in progress.

Monitor the progress and completion status of the download to the enclosures. The progress and status of each drive enclosure participating in the download is displayed in the status field of the Select enclosures table as shown in Figure 5-19.

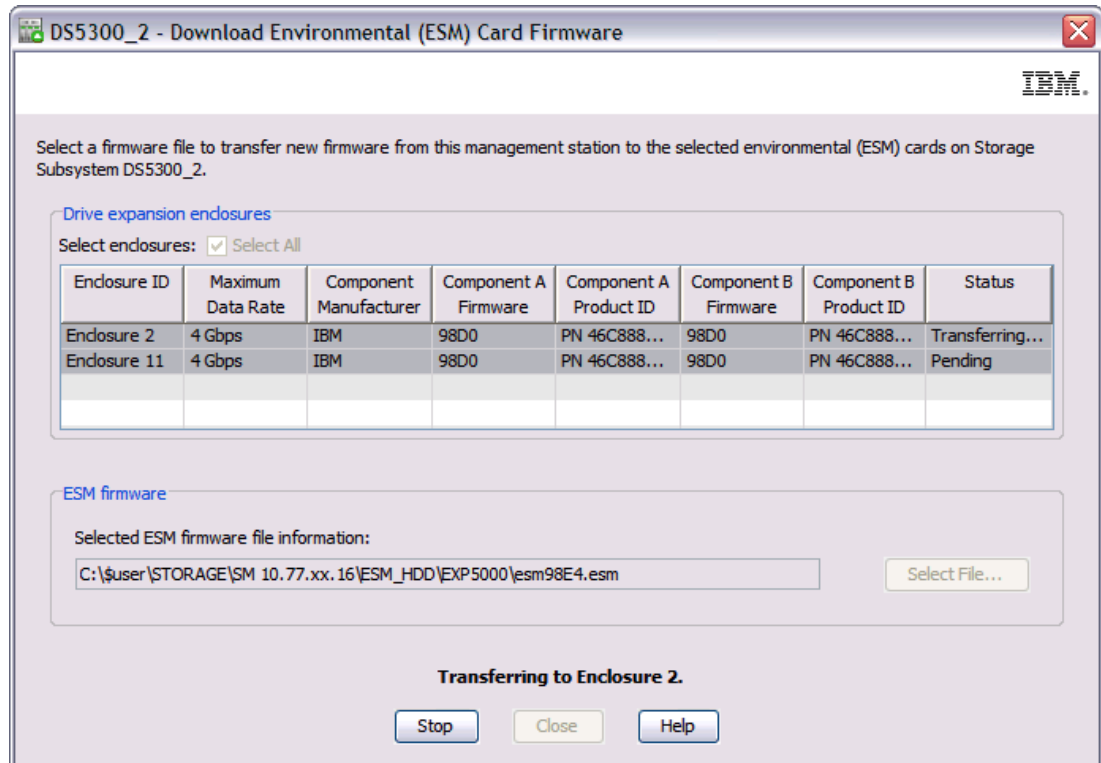


Figure 5-19 ESM firmware upgrade progress

When the transfer is complete, you see the window shown in Figure 5-20 on page 303.

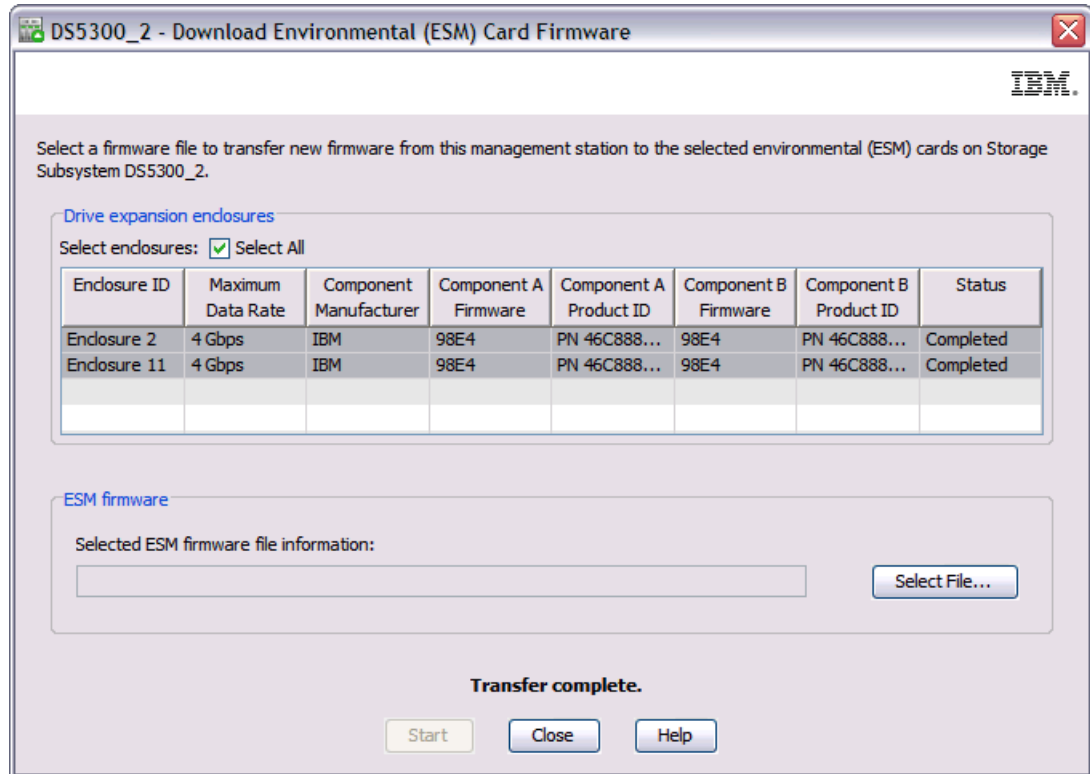


Figure 5-20 ESM firmware update completed

Click on **Close** to return to the Subsystem Management window.

5.1.7 Updating the hard disk drives firmware

Updating the hard disk drives firmware is sometimes required after upgrading the ESM firmware or the controller firmware/NVSRAM. Always refer to the readme file associated with the hard drive and ESM firmware upgrade package for precise instructions and dependencies.

Parallel drive firmware download

Storage Manager allows you to download hard disk drive firmware to several drives in parallel. This way, large configurations with multiple expansion enclosures are not affected by the download time that updating a large amount of drives might generate.

You can update up to four different drive types simultaneously. It does not matter whether there are different types or different firmware versions.

Note: All I/O has to be stopped while downloading the firmware to the drives.

In the DS5000 storage subsystems with the FC/SATA intermix premium feature enabled, do not download the drive firmware to both SATA-technology hard drives and Fibre Channel technology hard drives at the same time. Complete the drive firmware download to all of the drives of a drive technology (either SATA or FC) before downloading the drive firmware to the drives of the other drive technology (either FC or SATA).

You can find the firmware files and full instructions at the following address:

<http://www.ibm.com/support/entry/portal/>

Choose your DS5000 product on IBM Support Portal Quick start to go directly to support content and tool.

Perform these steps to update the firmware of the disk drives:

1. To start the hard disk drives firmware update process, select **Advanced** → **Maintenance** → **Download** → **Download Drive Firmware...**, as shown in Figure 5-21.

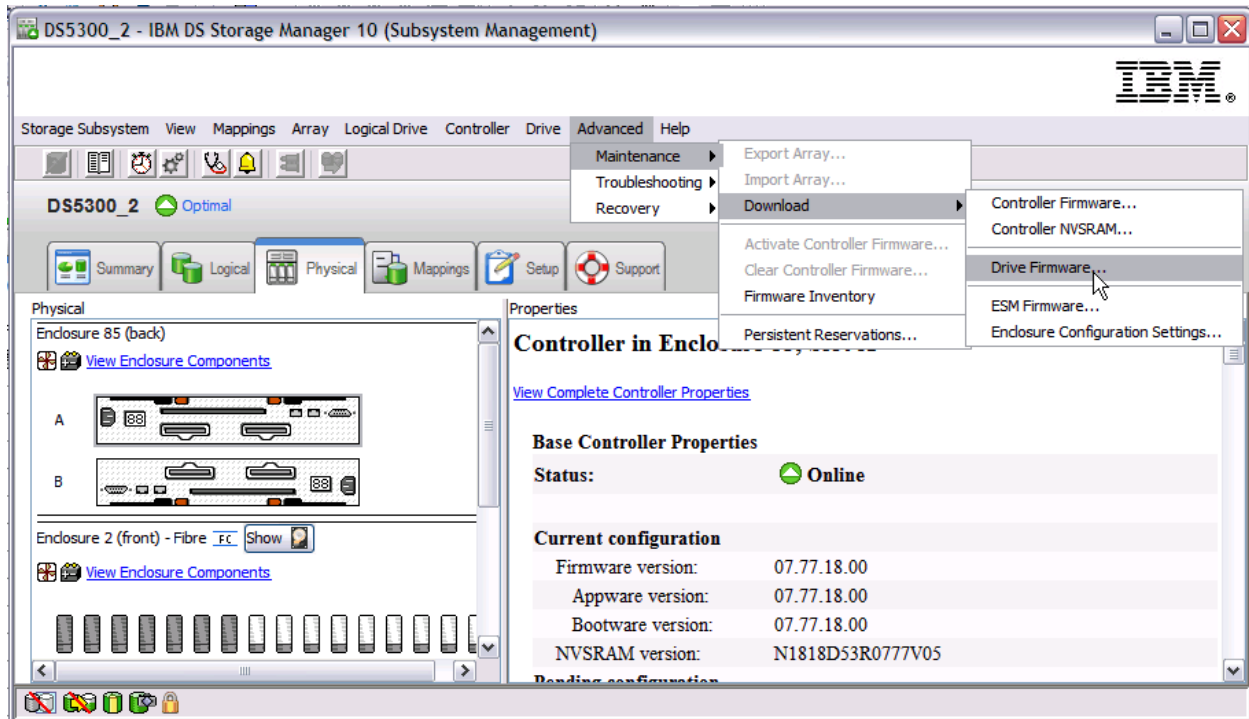


Figure 5-21 Drive firmware update

2. Start the wizard and a window opens, as shown in Figure 5-21 on page 304. Click **Next >**.
3. The window shown in Figure 5-22 opens, which shows all the types of drives you have with the current firmware level. Click **Add** to choose the firmware package.

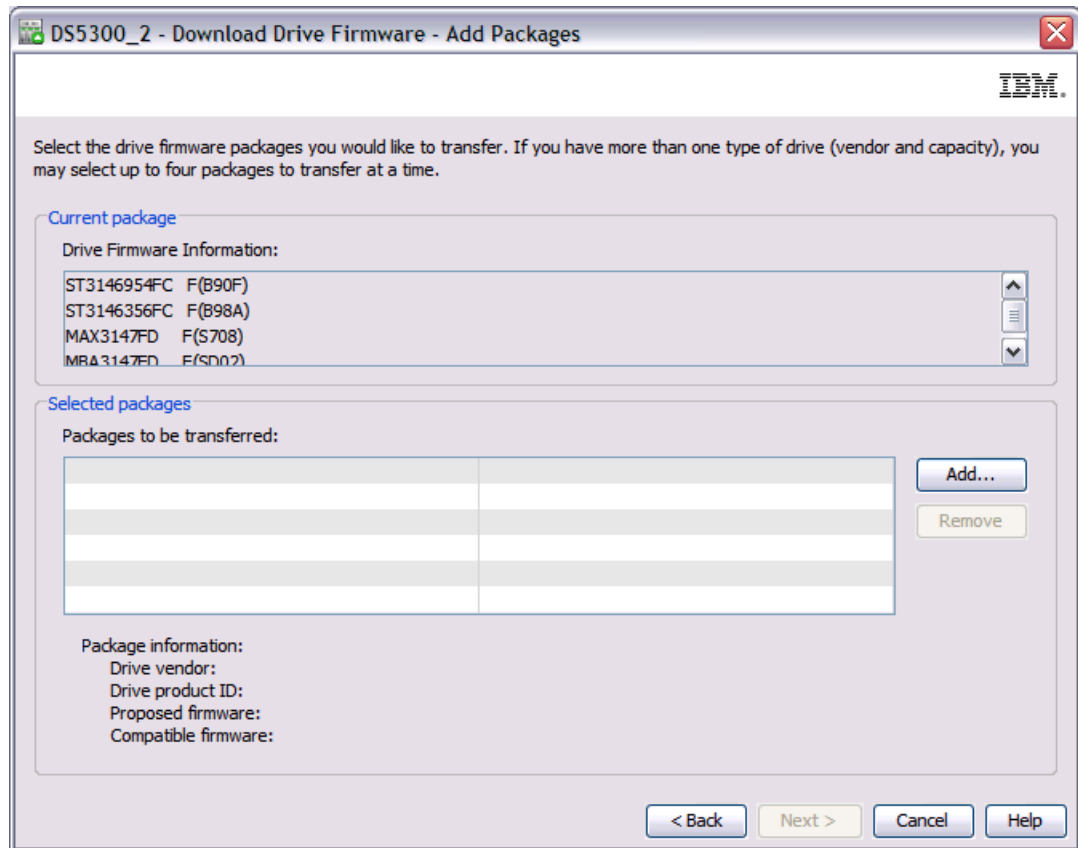


Figure 5-22 Selecting drive to be upgraded

- The window shown in Figure 5-23 opens. Here you can browse and choose drive firmware packages that you have previously downloaded. This window shows, in the File Information pane, all packages available and if a selected firmware package is compatible with disk drives present in the DS5000. Figure 5-23 shows compatible firmware.

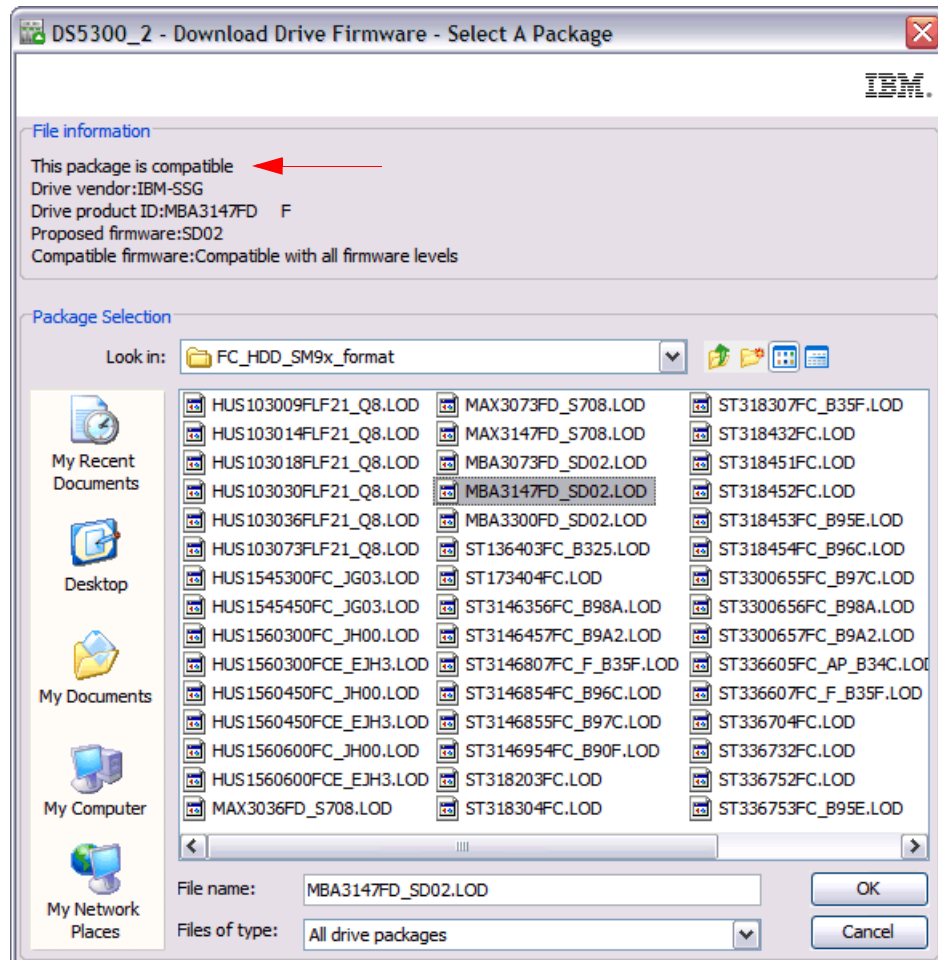


Figure 5-23 Drive firmware: Compatible package

Figure 5-24 on page 307 shows incompatible firmware.

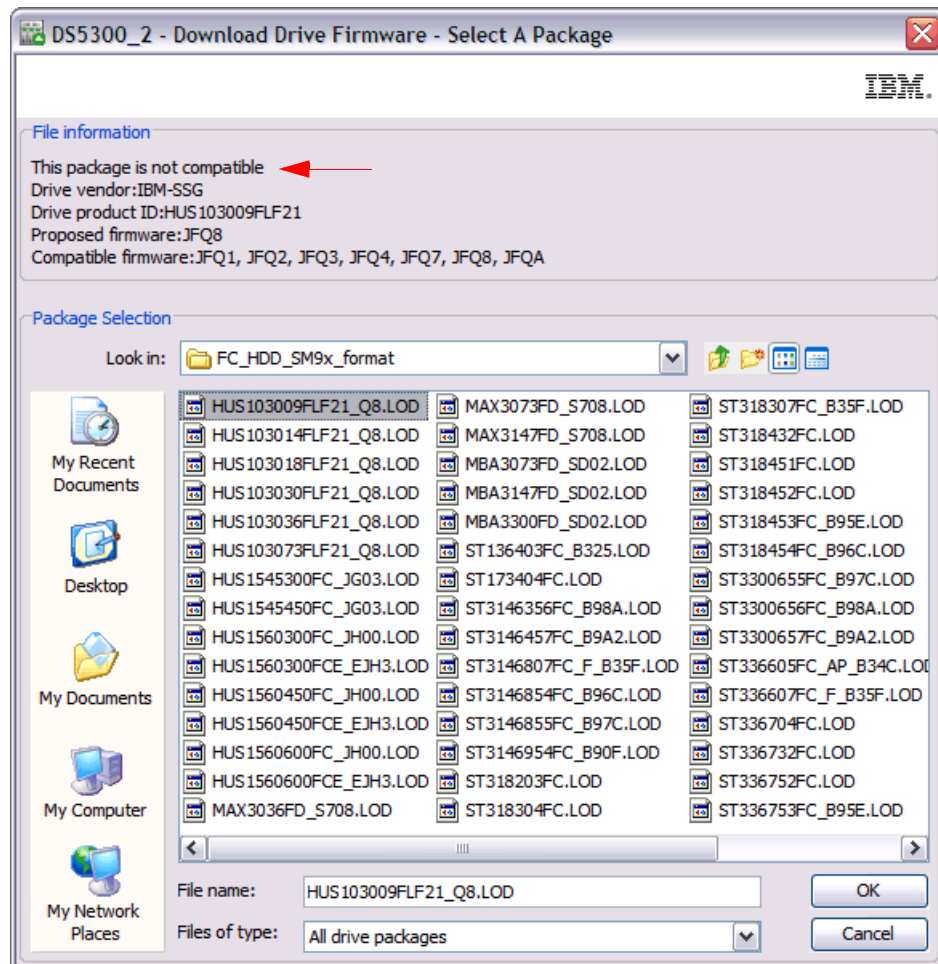


Figure 5-24 Drive firmware: Incompatible package

5. You can select more drive firmware if you have different drives in enclosure as shown in Figure 5-25.

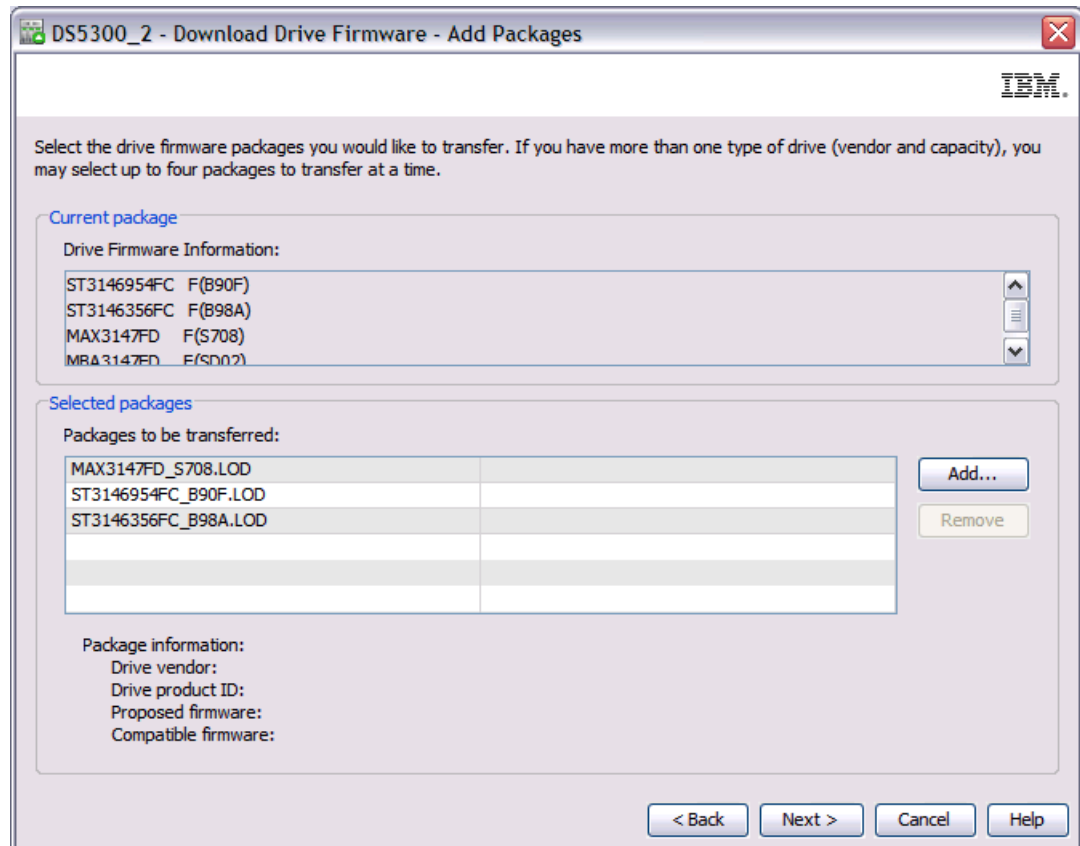


Figure 5-25 Adding drive firmware packages

6. If you click **Next >**, a new window opens showing all the drives with the current and proposed firmware. We had one type of drive that did not require an upgrade, because the firmware was on the same level, as shown in Figure 5-26. Select the drives you want to upgrade by checking **Select all** box and click **Finish...** Confirm your selections by typing **yes** and click **OK** on warning pop-up window in order to continue with the firmware download or **Cancel** to quit.

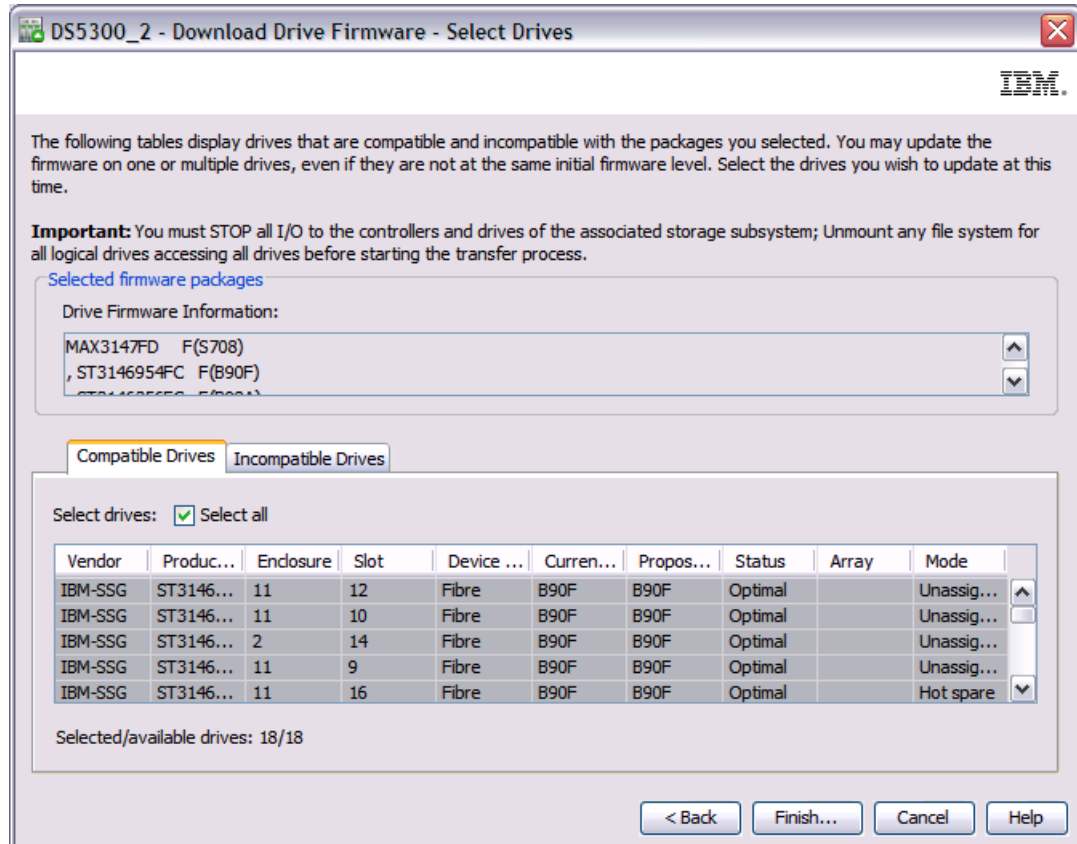


Figure 5-26 Selecting drives to upgrade

7. Once the drive firmware download procedure starts, you can monitor the progress, as shown in Figure 5-27. This gives you information about the current status of the download. After the process is finished, you can also see whether all drives were successfully updated.

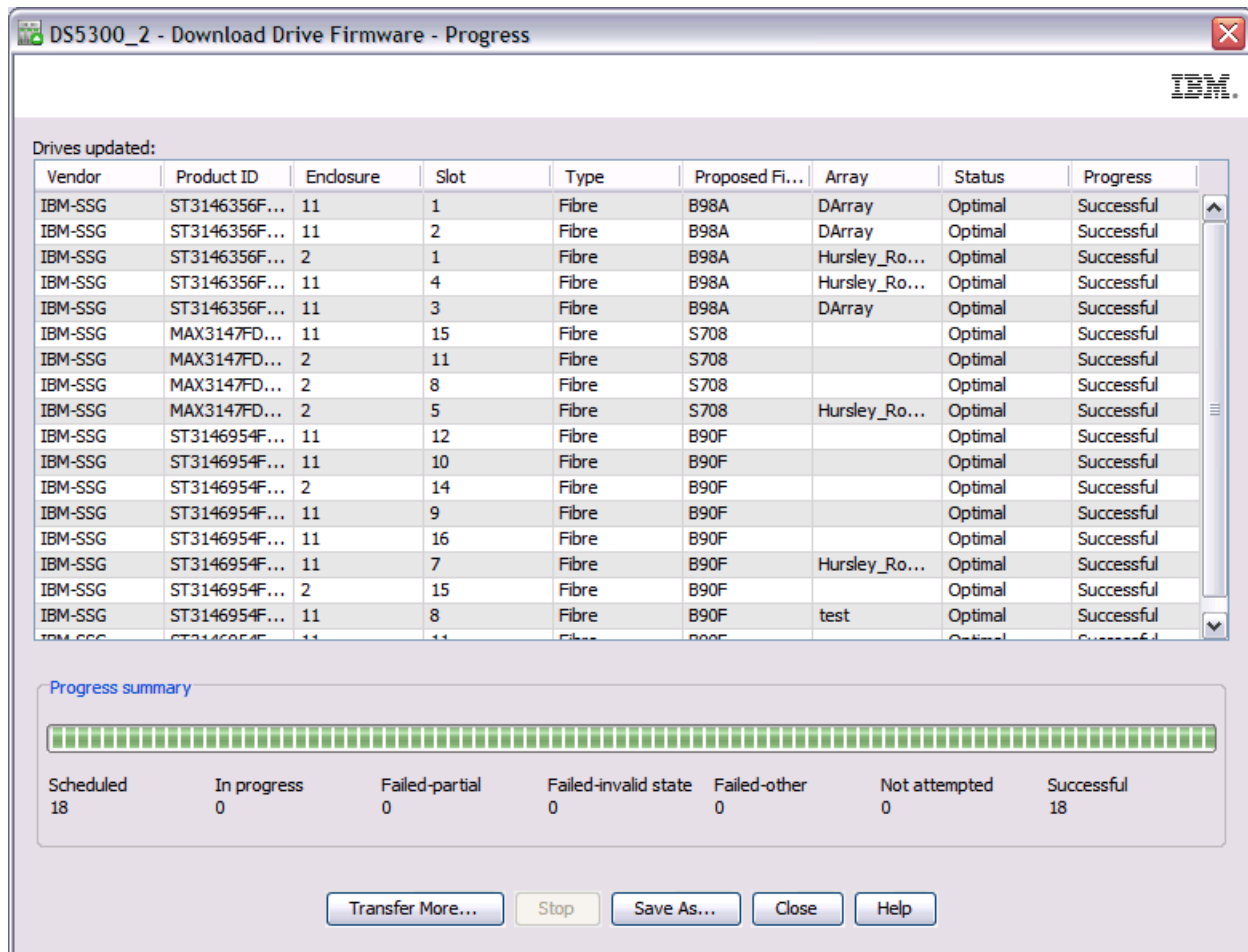


Figure 5-27 Drive firmware update: Download progress window

8. Click on **Close** when firmware download is complete to return to the Subsystem Management window.

5.1.8 Updating host bus adapter (HBA) firmware

This section describes the procedure to update the HBA firmware in Windows, Linux (graphical based), and AIX environments. However, different HBA vendors offer different tools to manage the HBAs.

We describe the following procedures in this section:

- ▶ “Update Brocade HBA firmware using Brocade Host Connectivity Manager (HCM)” on page 311.
For more details about Brocade HCM, see 5.12.1, “Brocade HBA and Brocade Host Configuration Manager (HCM)” on page 419.
- ▶ “Update Emulex HBA firmware using Emulex HBAnyware” on page 312.
For more details about Emulex HBAnyware, see 5.12.2, “Emulex HBA tools” on page 425.
- ▶ “Update the HBA firmware using QLogic SANsurfer” on page 313.
For more details about QLogic SANsurfer, see 5.12.3, “Qlogic HBAs and SANsurfer (Windows/Linux)” on page 426.
- ▶ “Updating HBAs in AIX environments” on page 315.

Download the HBA firmware

You can find the latest HBA firmware version supported by DS5000 at the IBM DS5000 System Storage Support site at the following address:

<http://www.ibm.com/support/entry/portal/>

Select **System Storage**, then select **Disk systems** from the drop-down menu, and choose your IBM DS5000 storage subsystem model. Select the **Download** tab to access the supported firmware for your host bus adapter. You will find the appropriate files for your HBA depending on the vendor (either Brocade, Emulex, or Qlogic) in this table.

Note: When updating HBAs, make sure to install matching versions of BIOS and drivers for your adapters. Also make sure to install at least the minimum versions recommended on the IBM Storage support Web site. Check *always* on IBM Storage web site before download the firmware from the vendor Web site itself, as this could be not IBM tested code.

Update Brocade HBA firmware using Brocade Host Connectivity Manager (HCM)

Brocade calls its HBA firmware *boot code* or *EFI*. There are different ways to update the boot code of the HBA. These are:

- ▶ Using a bootable live CD.
- ▶ Using the HCM GUI (which is explained here).
- ▶ Using the BCU command line tools.

The Brocade HCM offers an easy way to update the HBA's firmware.

You can obtain the latest version at IBM page on Brocade web site at the following address:

<http://www.brocade.com/services-support/drivers-downloads/adapters/IBM.page>

Note: Refer *always* to firmware readme file on IBM Support Portal for installation and configuration details.

To update the firmware, perform the following steps:

1. Start HCM and log in to the agent. The HCM window opens, as shown in Figure 5-28.

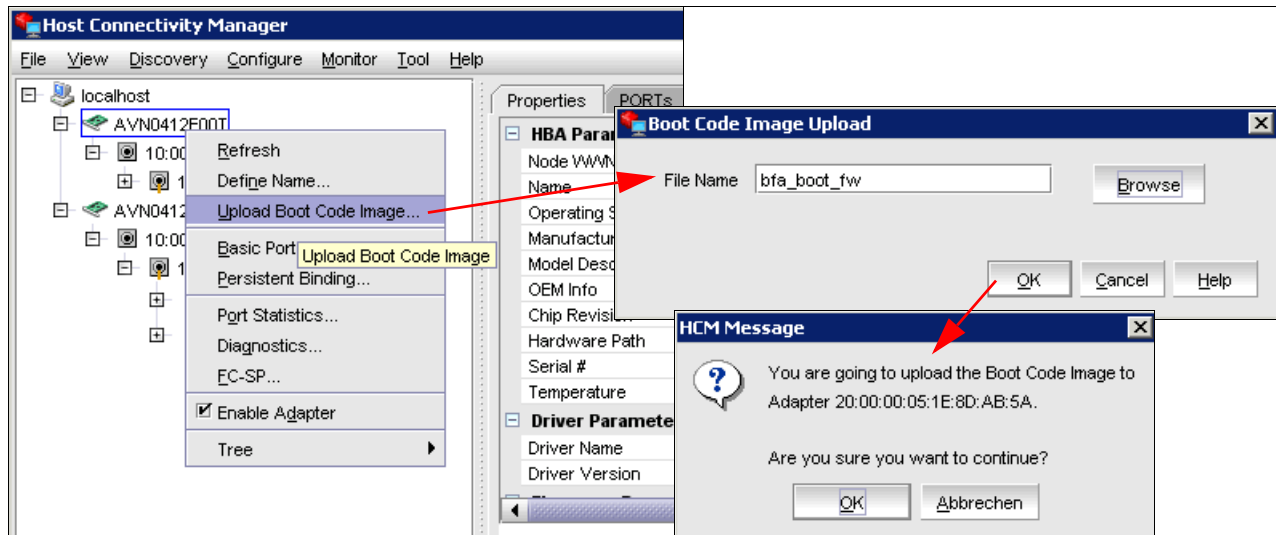


Figure 5-28 HCM update firmware

2. Right-click the HBA entry in the left pane and select **Upload Boot Code Image...** from the menu.
3. In the resulting Boot Code Image Upload window, click **Browse** to select the boot code image on the computer and then click **OK**.
4. Confirm your choice by clicking **OK** in the next window.
5. After a few seconds, a confirmation window appears.
6. Reboot the server in order to activate the new HBA BIOS.

Update Emulex HBA firmware using Emulex HBAnyware

You can update firmware or boot code with either HBAnyware or lputilnt.

- ▶ HBAnyware allows you to update firmware or boot code on remote and local HBAs.
- ▶ lputilnt allows you to update firmware or boot code on local HBAs only.

Prerequisites

You must meet the following prerequisites:

- ▶ The SCSIport Miniport driver is properly installed.
- ▶ The HBAnyware utility is properly installed.
- ▶ The firmware or boot code file has been downloaded from the Emulex Web site and extracted to a directory on your local drive.

You can find the latest version at the IBM dedicated page on Emulex Download web site at the following address:

<http://www.emulex.com/downloads/ibm/fw-and-bootcode.html>

Note: Refer *always* to firmware readme file on IBM Support Portal for installation and configuration details.

Procedure

To update firmware or boot code using HBAAnyware, perform the following steps:

1. Start the HBAAnyware utility.
2. In the discovery-tree (left pane), click the HBA entry you want to update. In the menu bar, click **Batch** and select **Download Firmware** (see Figure 5-29).
3. A Select Firmware File window appears (Figure 5-29). Select the firmware you want to update and click **Open**.

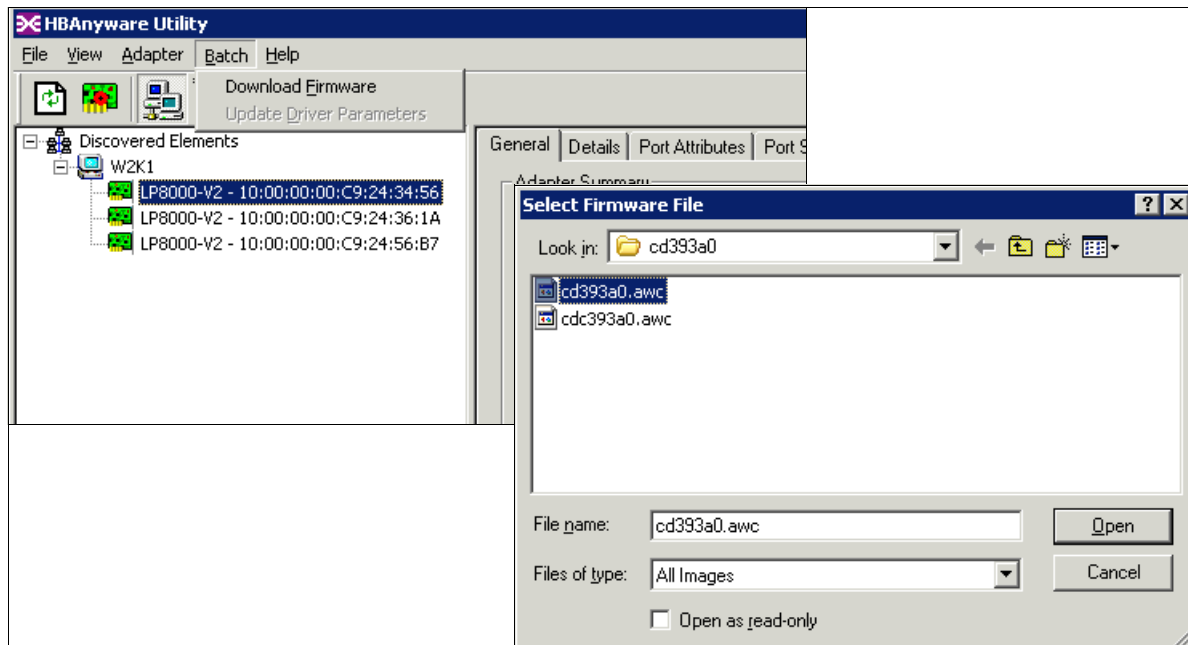


Figure 5-29 HBAAnyware: Download firmware

4. The Firmware Download dialog box appears. Click **Yes**. Next, the adapter reset notice appears. Click **Yes**.
5. After a few seconds, the Firmware Upgrade Successful message appears. Click **OK**. The firmware update is done.
6. The server need to be rebooted in order to activate the new HBA firmware.

Update the HBA firmware using QLogic SANsurfer

The Qlogic SANsurfer is available for Windows and Linux hosts.

You can find the latest version at the IBM page on QLogic Download web site at the following address:

http://driverdownloads.qlogic.com/QLogicDriverDownloads_UI/Product_detail_new.aspx?oemid=304&companyid=6

Note: Refer *a/ways* to firmware readme file on IBM Support Portal for installation and configuration details.

To update the HBA firmware using QLogic SANsurfer, perform these steps:

1. In order to update the BIOS version of the HBA, click the **Utilities** tab, and you will be presented with a window shown in Figure 5-30 on page 314.

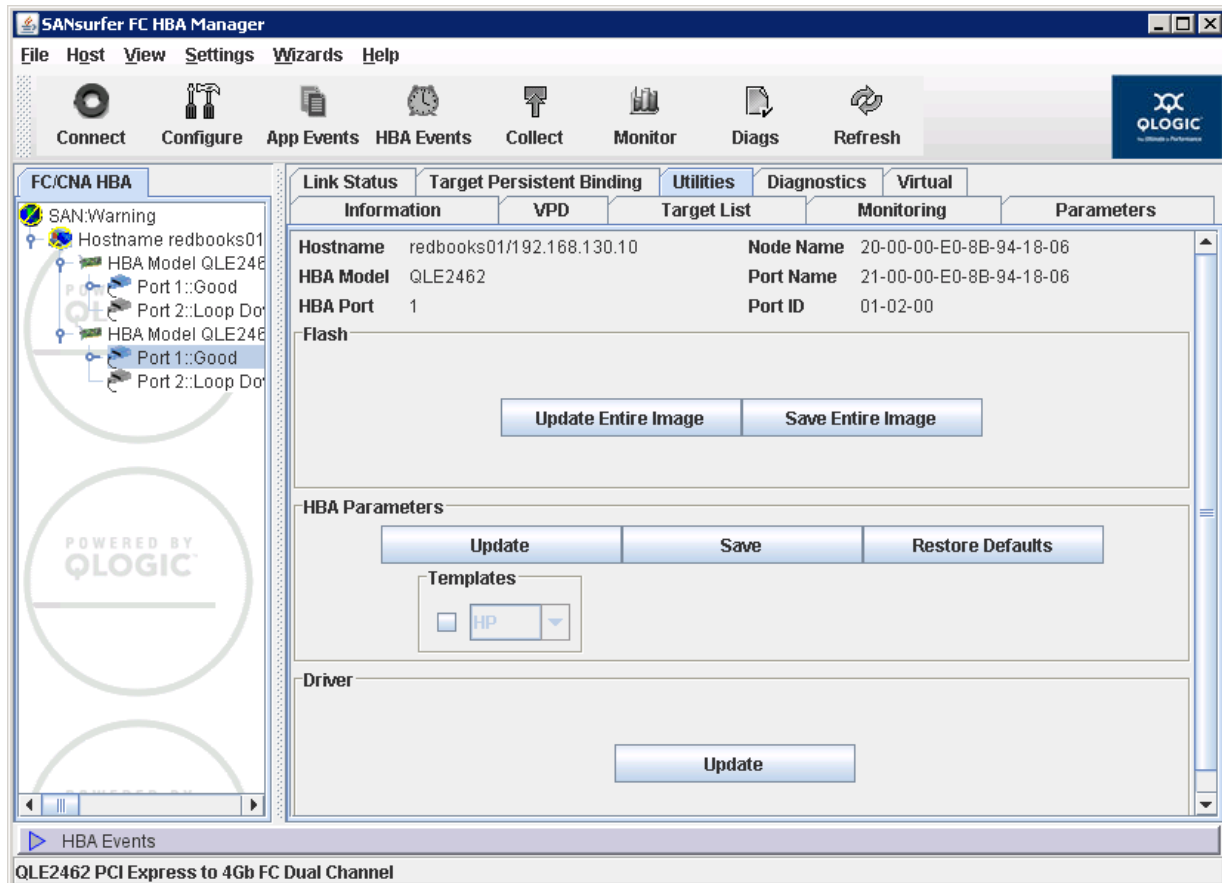


Figure 5-30 QLogic sansurfer utility

2. Click **Update Entire Image**, which corresponds to the BIOS version.
3. Select the corresponding file for your adapter as shown in Figure 5-31.

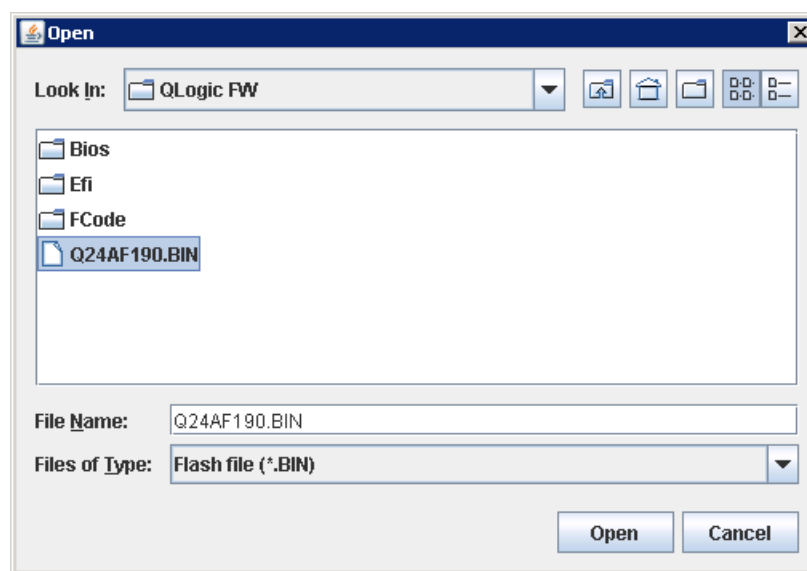


Figure 5-31 QLogic SANsurfer HBA BIOS update file

Once you have selected the file, you will be prompted for the password. The default password for all adapters is *config*. Click on **OK** once the upload is finished as shown in Figure 5-32.

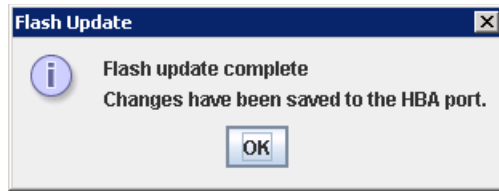


Figure 5-32 QLogic SANsurfer HBA BIOS update completed

You can upload BIOS for multiple adapters subsequently.

Updating HBAs in AIX environments

To update HBAs in AIX, perform these steps:

1. For IBM System p microcode, see the IBM Fix Central Web site at the following address:
<http://www.ibm.com/support/fixcentral/>
2. Go through all selection choosing the right one for your system and then click on **Continue**.
3. Select **Device firmware** radio button and click on **Continue**
4. **Select by device type** and then **Adapter**.
5. Search for your server-specific FC adapter type. Once found, the description provides detailed instructions about how to check the current version, install the update, and check the results.

Select the RPM file and click **Continue** at the bottom of the page to download the rpm file.

6. Follow the instructions to download the file and transfer it to `/etc/microcode`.
7. Unpack the transferred file in `/etc/microcode` by running the following command:

```
#cd /etc/microcode
#rpm -ihv --ignoreos pci.df1000f9-3-93a0.aix.noarch.rpm
```

Replace `pci.df1000f9-3-93a0.aix.noarch.rpm` with the name of the package downloaded for your particular HBA.

8. Flash the adapter microcode by running the following command:

```
#diag -d fcsX -T download
```

Where *X* is the number returned by the `lsdev -C | grep fcs` command. Self-explanatory menus take you through the microcode installation. Repeat this process for all the HBAs that need to be updated.

9. Verify the adapter microcode level by running the following command:

```
#lsmcode -d fcsX
```

Compare the obtained level with the readme file of the downloaded code.

5.2 Handling premium features

Depending on your specific IBM Midrange System Storage storage subsystem model, you might want to use a specific function or capability of your storage subsystem. Some of these capabilities, although included in the firmware, are not enabled by default. These are called

premium features, and you have to activate them by entering an activation key. You must buy a license for the premium feature to get a key and instructions about how to activate it.

You can activate an individual premium feature by providing its corresponding key, or activate a pack or bundle of multiple features.

Here we cover how to order, list, and install any of the premium features available for your IBM DS5000 Storage Subsystem.

The available premium features are:

- ▶ Full Disk Encryption
- ▶ Storage partitioning
- ▶ FlashCopy
- ▶ Enhanced Remote Mirroring (ERM)
- ▶ VolumeCopy
- ▶ External Key Management
- ▶ High Performance Tier (for DS5100 only)
- ▶ Drive Slot Limit

5.2.1 Listing premium features/feature enabler

From the Storage Manager client GUI, you can check what premium features are already activated in your DS storage subsystem.

Starting with Storage Manager V10 and its related firmware, this information, with additional details, is generated as a text file. The file is available within the zip package generated by selecting the option to collect all support data in Storage Manager Client.

To list the premium features, perform the following steps:

1. Select **Storage Subsystem** → **Premium Features** from the Subsystem Management window. The Premium Features window opens and shows a list of enabled premium features (see Figure 5-33).

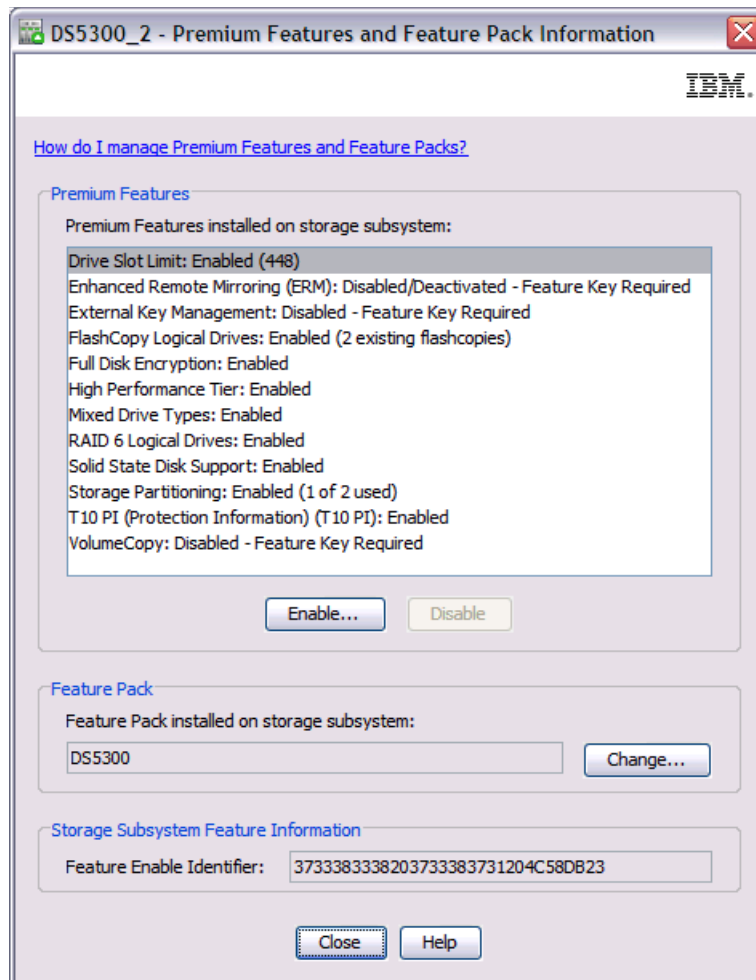


Figure 5-33 List of premium features

If you receive a Premium Features - Out of Compliance error message during a management session, use the Recovery Guru to resolve the problem.

2. Collect all support data by selecting **Advanced** → **Troubleshooting** → **Support Data** → **Collect...** Provide a file name and directory where you want to store the zip file generated.

Once the file is generated, open the zip file, and then look at the file named `featureBundle.txt` to see the status, limits, and in-usage capacities for the premium features, as illustrated in Example 5-1.

Example 5-1 Collect support data featureBundle.txt file

FEATURE BUNDLE FOR STORAGE SUBSYSTEM: DS5300_2 (Thu Oct 06 13:49:20 MST 2011)

Total logical drives allowed: 2048

Total logical drives allowed per partition: 256

Management application client: 1

Drives supported: B,1; J,1; S,1; E,1; BM ,2

Drive expansion enclosures supported: IBM,EXP5000,HUSKER;
IBM,EXP810,HUSKER; IBM,EXP5060,WEMBLEY-HUSKER

High Performance Tier: No data is available about supported values of this feature

Storage Partitioning

Enabled by default: Yes
Default limit: 2
Enable/Upgrade via key: Yes
Limit with feature key: 512

FlashCopy Logical Drives

Enabled by default: Yes
Enable/Upgrade via key: Yes
Total flashcopies allowed: 2

VolumeCopy

Enabled by default: No
Enable/Upgrade via key: Yes
Total copies allowed: 2047

Enhanced Remote Mirroring (ERM)

Enabled by default: No
Enable/Upgrade via key: Yes
Total mirrors allowed: 0

Mixed Drive Types

Enabled by default: Yes
Enable/Upgrade via key: No

3. Gather the following data along with the Feature Enable Identifier:

- Machine type
- Model
- Serial number

Note: The machine type, model, and serial information is printed on a label on the back of your DS storage subsystem controller unit.

5.2.2 Enabling a premium feature

Obtaining a feature key depends upon the DS storage subsystem packaging procedures and time of order:

- ▶ If you bought any premium features together with the DS storage subsystem, you will receive the feature keys with the DS storage subsystem hardware, but you still have to activate them separately.
- ▶ If you are purchasing a new premium feature, you can get the key from your local storage sales support (IBM or Business Partner).

In any case, a premium feature is a chargeable option for every DS storage subsystem, and you have to request the premium feature from your sales contact person for a specific machine type, model, and serial number.

Once you have purchased a premium feature, you receive an envelope containing a license activation card for that particular feature, with detailed instructions about how to proceed to activate it.

Important: All the premium features are activated immediately and do not require a reboot of the controllers.

The following procedure will help you activate the new feature, or reactivate it if for any reason it is out of compliance:

1. On the card you received, locate the feature activation code, and make sure that the instructions received are for your machine type and model. The feature activation code (XX-XXXX-XXXX) is located at the top of the license activation card.
2. From the Subsystem Management window, select **Storage Subsystem** → **Premium Features**.
3. Write down the 32-digit number next to the feature enable identifier, or copy and paste the complete number to a text file to avoid typing errors.

You can also find the feature enable identifier in the profile data, either by selecting **Storage Subsystem** → **View** → **Profile** or by opening the `storageArrayProfile.txt` file contained in the zip file that was generated when you collected all the support data.

4. Go to the following Web site to personalize the received key to your specific system and generate the activation key file:

<http://www-912.ibm.com/PremiumFeatures/>

5. Select the option to activate a premium feature.
6. Complete the form in the Web page with the following information:
 - Feature activation code
 - Feature enable identifier
 - Machine type
 - Model number
 - Unit serial number

The Web page generates a an activation key file that you have to download to your management station. It also sends the file to the specified e-mail address if you filled out the Email address field.

Please note that if your feature activation code is for a **Full Disk Encryption** feature, you must enter a valid email address so that we may send your security certificate.

7. Once you have received the key file, go to Storage Manager and select **Storage Subsystem** → **Premium Features** in the Subsystem Management window to open the premium feature info, as shown in Figure 5-34.

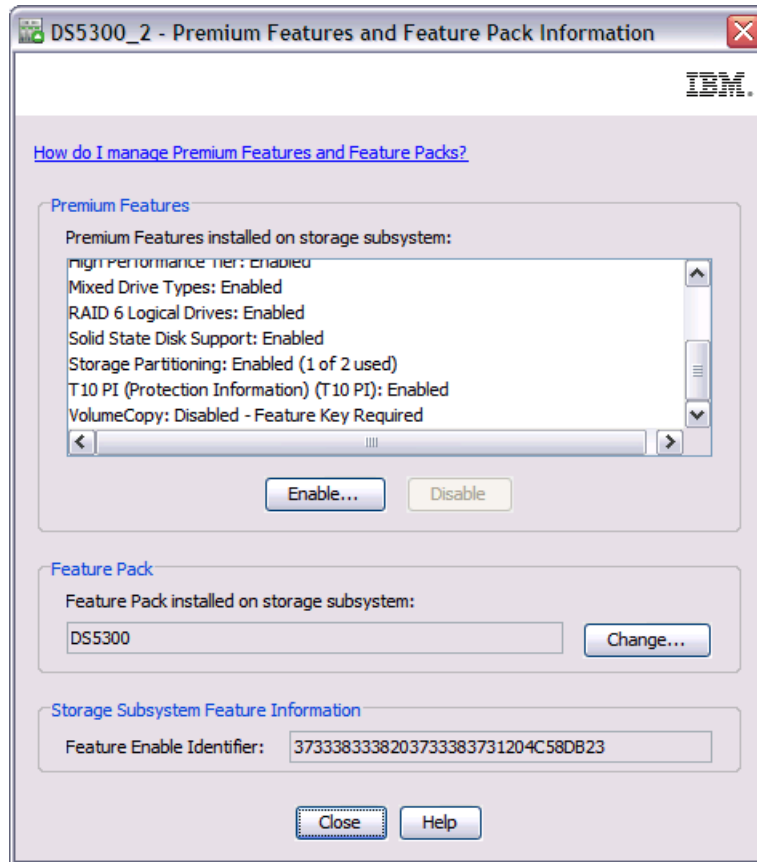


Figure 5-34 Enabling a premium feature

8. Click **Enable** and select the premium feature key file to enable and click **OK**, as shown in Figure 5-35 on page 321.

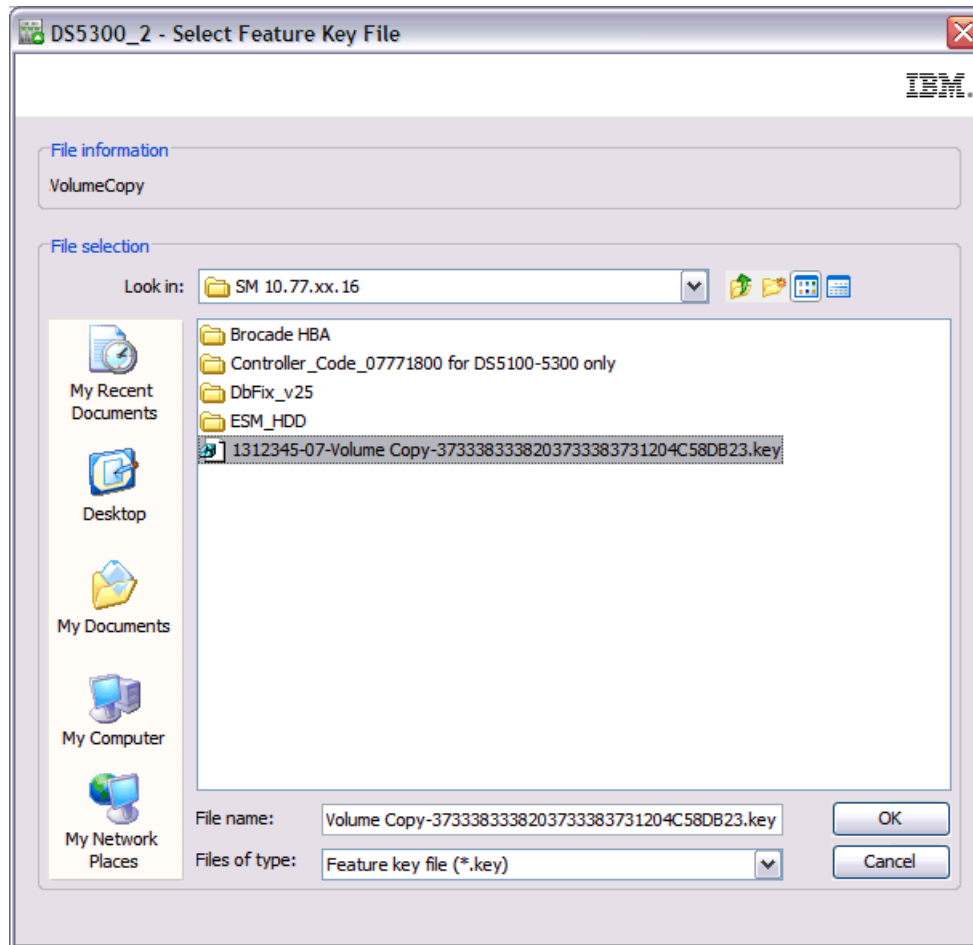


Figure 5-35 Select feature key file

9. Confirm feature enabling by clicking OK on popup window as show in Figure 5-36.

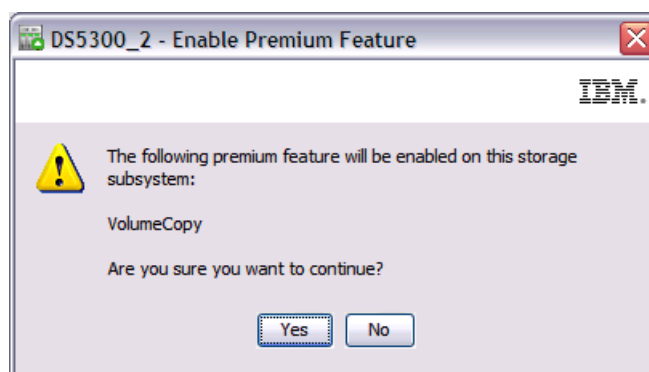


Figure 5-36 confirm feature enabling

10. New feature has been enabled as shown in Figure 5-37 on page 322

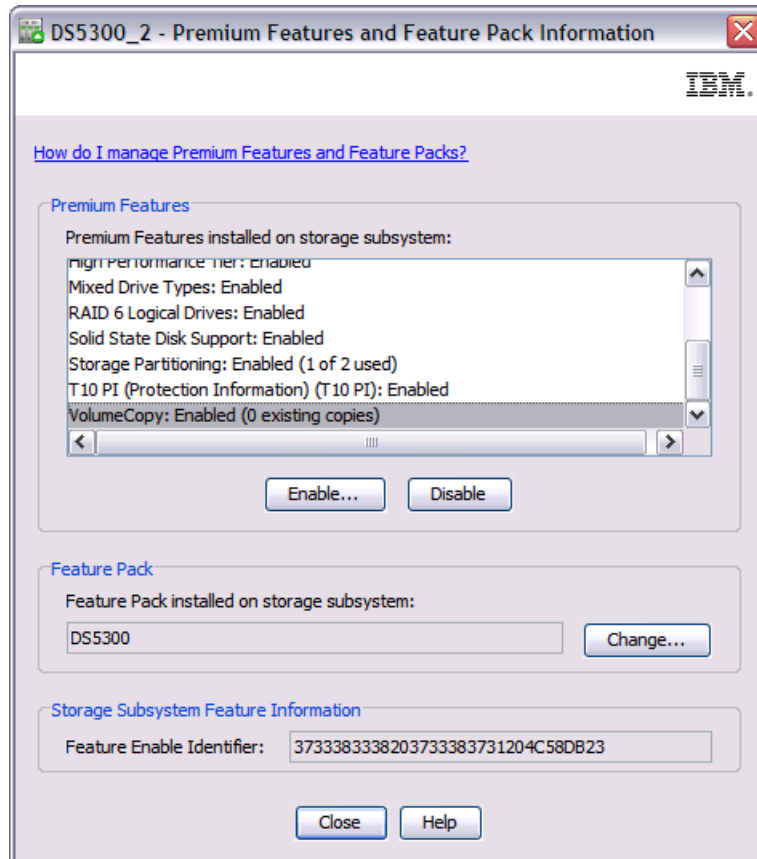


Figure 5-37 Feature enabled

The DS storage subsystem validates the supplied code to make sure that it is suitable for the specific serial number and is compatible with the machine type and model. It also checks that it is not already installed.

If everything is okay, the feature is applied and is immediately available for use.

If the feature enable identifier does not match the DS storage subsystem, or it is already installed, you receive a notification and the key will not be installed.

5.2.3 Disabling a premium feature

To disable a premium feature do following:

1. Select **Storage Subsystem** → **Premium Features** in the Subsystem Management window. Choose the feature you want to disable from the list as shown in Figure 5-38 and click on **Disable**.

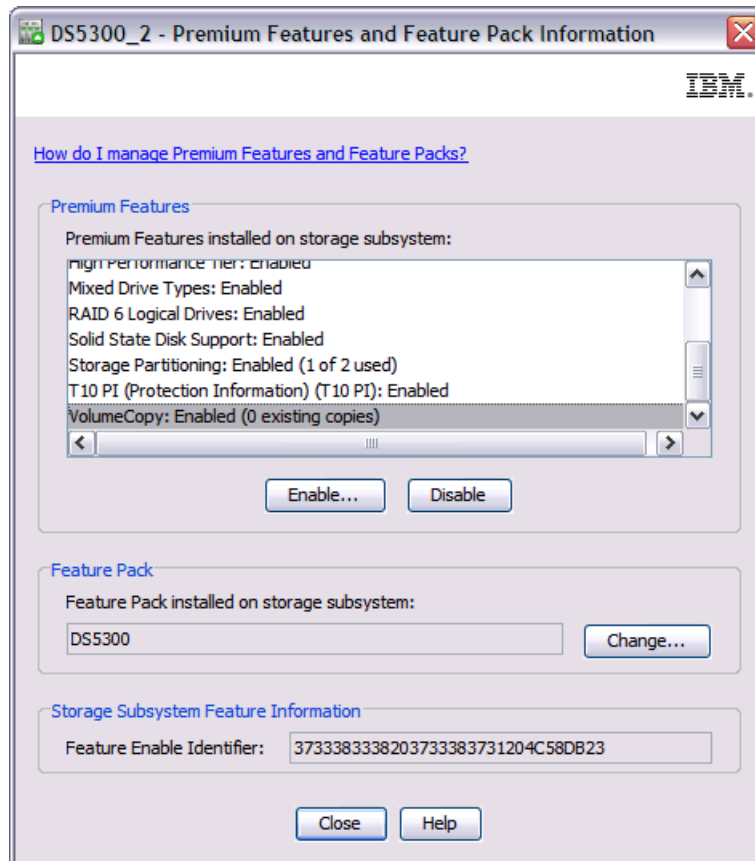


Figure 5-38 Disabling premium feature

2. Click **Yes** to confirm feature disabling as shown in Figure 5-39.

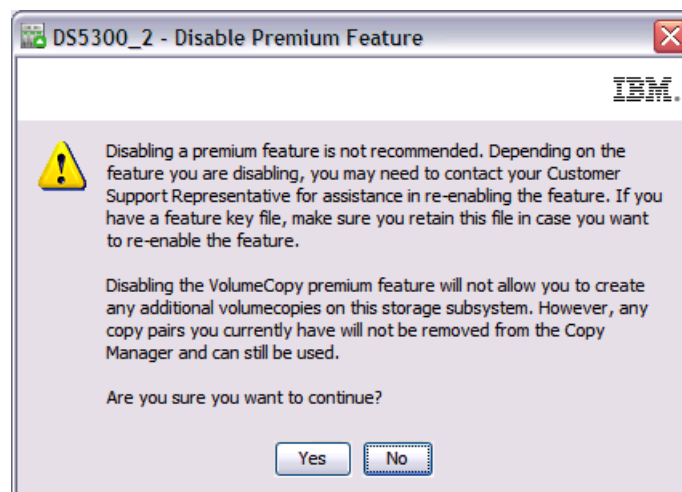


Figure 5-39 Disable premium feature - Confirm

The feature is now disabled as shown in Figure 5-40.

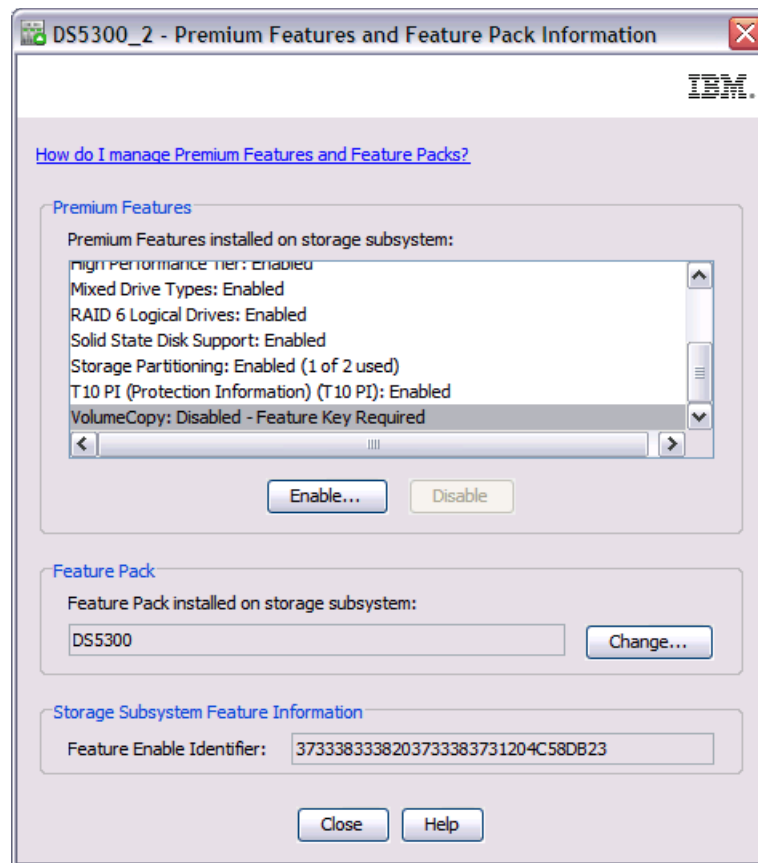


Figure 5-40 Feature disabled

Keep in mind that the change happens immediately. If you use storage partitioning and disable the premium feature, then you cannot create new partitions. However, any existing partitions remain operational.

5.3 Saving and loading the configuration

Once your DS storage subsystem is configured and running, save this configuration in order to be able to restore it in case of problems.

The saved configuration includes the array and logical drive configuration, the name of the subsystem, its cache settings, and other parameters, including the storage partitioning configuration.

The saved file can be used to restore the configuration data to the same DS storage subsystem, or also to other DS storage subsystems in case you want to set up multiple storage subsystems with the same configuration. To allow that action, the destination subsystem must have the same hardware layout, number of enclosures and drives, and drive capacities.

All information is stored in a file that contains a script for the script editor. To save the configuration of the subsystem, open the Subsystem Management window and select **Storage Subsystem** → **Configuration** → **Save** as shown in Figure 5-41.

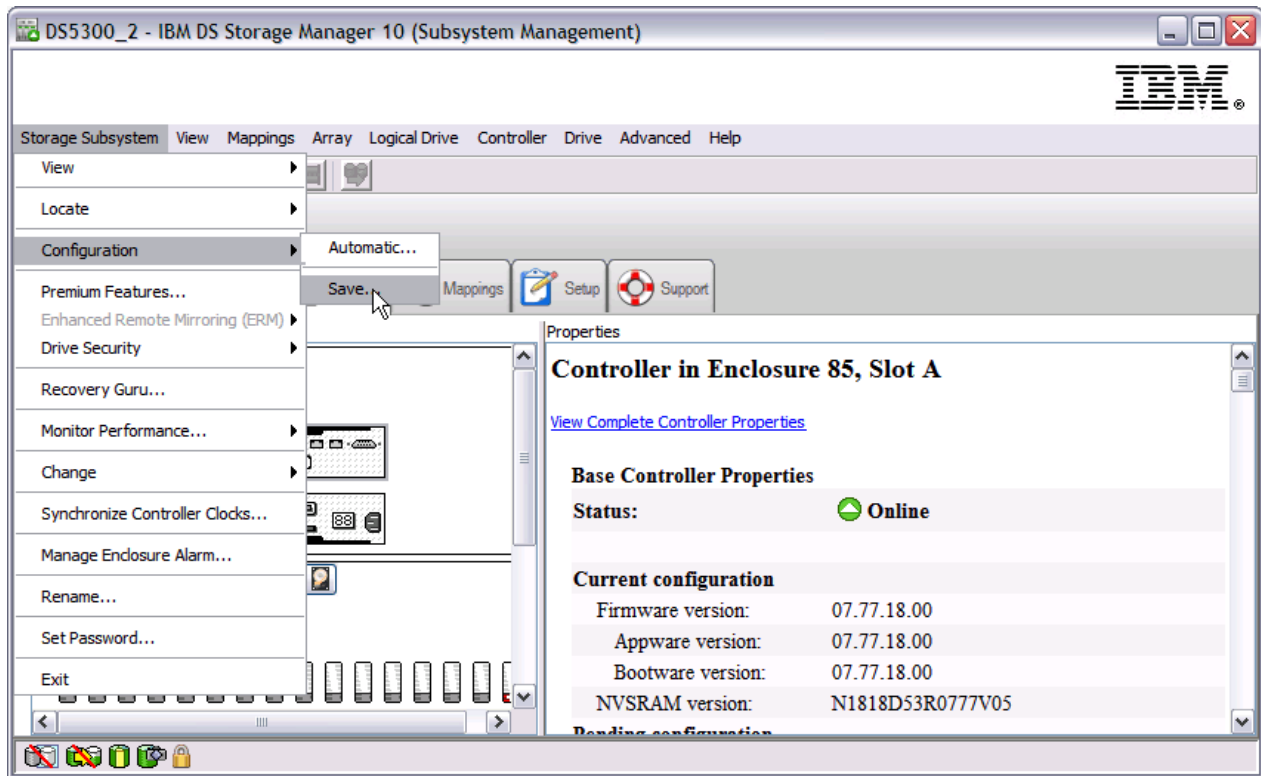


Figure 5-41 Saving the DS5000 storage subsystem configuration

We can choose to save specific elements of the configuration as shown in Figure 5-42.

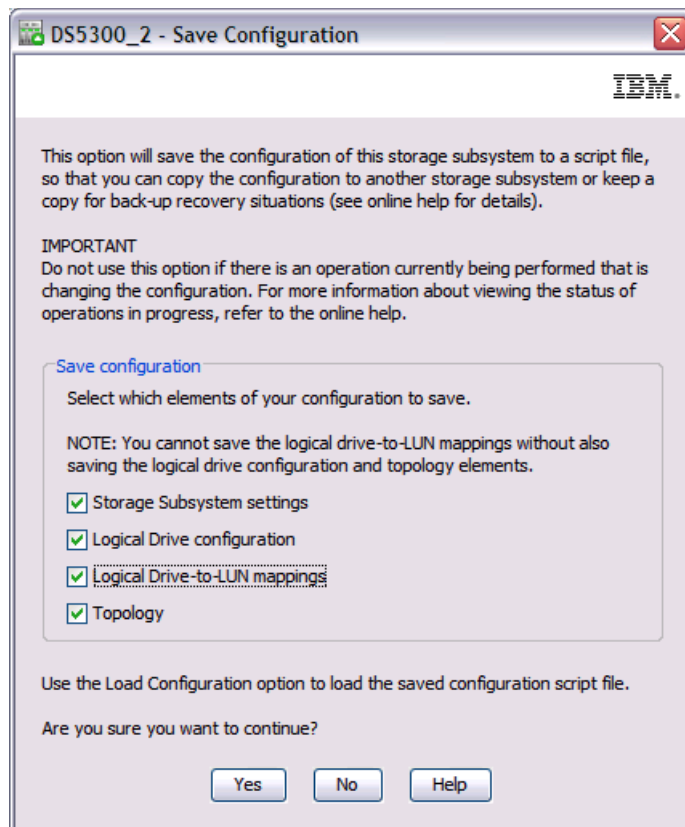


Figure 5-42 Saving configuration elements

Select the desired configuration elements, click **Yes**, and select a file name and destination folder in which to save the file. Make sure not to use a directory located on a DS storage subsystem disk, or you might not be able to access it when needed.

The script created can be used to replicate the configuration of the DS storage subsystem. You can apply the configuration to the destination subsystem for all the saved elements, or any particular element. The script consists of the following information:

- ▶ Storage subsystem settings
 - User label
 - Media scan rate
 - Cache block size
 - Cache flush start
 - Cache flush stop
 - Default host type
 - Failover alert delay
- ▶ Logical drive configuration
 - RAID level
 - User label
 - Owning controller
 - Segment size
 - Capacity
 - Cache flush modifier
 - Read-ahead multiplier
 - Modification priority

- Caching without batteries enabled/disabled
- Cache mirroring enabled/disabled
- Read caching enabled/disabled
- Write caching enabled/disabled
- Media scan enabled/disabled
- Redundancy check enabled/disabled
- ▶ Logical drive-to-LUN mappings
- ▶ Topology
 - Host groups
 - Hosts and parent host groups
 - Host ports, associated host type, and parent hosts

Attention: This procedure replaces any configuration on the storage subsystem. All data stored on the DS storage subsystem is lost because all logical drives are initialized. It is a good idea to save the configuration every time a change on the storage subsystem is made and collect all support data as well.

Do not attempt to load a saved configuration on the DS storage subsystem unless you fully understand the consequences.

To load the storage subsystem configuration, perform the following steps:

1. Open the Enterprise Management window and select the subsystem.
2. Select **Tools** → **Load Storage Subsystem Configuration...** from the tool bar menu.
3. Point to the file containing the configuration and load it.
4. The Script Editor and a warning message appear. To load the configuration onto the DS storage subsystem, choose **Execute**. You can also edit the script before executing.

The procedure can take a long time, depending on the number of arrays and logical drives defined. When the procedure finishes, the storage subsystem contains the same configuration as the source.

While the configuration file allows an immediate recreation of all the parameters configured, it does not provide a friendly reading file to list all of the configuration. To read the current configuration, we use the View Profile option described in 5.3.1, “Storage subsystem profile” on page 327.

5.3.1 Storage subsystem profile

The storage subsystem profile is one of the most important items needed for IBM Support to help you solve whatever problem you have with your DS storage subsystem. It is a simple text file that includes data about the various firmware levels, array and volume configuration, storage partitioning, and the status of all the hardware components of the DS storage subsystem.

It can also be accessed through the Storage Manager interface in a readable format, as opposed to the saved configuration option (script), which is mostly used for backup and restore purposes.

Note: Always collect All Support Data after you change the configuration of the DS storage subsystem. For example, if you create or delete logical drives, change the mapping, or add new disks or enclosures to the DS storage subsystem, collect All Support Data, as IBM Support might need it to help you in case of any problems.

To save the profile only, select **Storage Subsystem** → **View** → **Profile** in the Subsystem Management window. There are seven different sections (Controllers, Arrays, Logical drives, Drives, Drive Channels, Enclosures, and Mappings). The section All simply shows all seven sections on one page. Click **Save as** to continue saving the profile.

Note: instead of save the profile only, we strongly recommend to click **Advanced** → **Troubleshooting** → **Support data** → **Collect...** to collect all the various types of inventory, status, diagnostic and recovery data from this storage subsystem and save them in a single compressed file.

For more details, including graphics, see “Storage subsystem profile” topic in Chapter 4. IBM System Storage DS planning and configuration.

Reading the profile

Reading and interpreting the profile is a task usually done by IBM Support. There are some common information and failure situations that can be used, analyzed, and fixed easily by an administrator.

Controller and NVSRAM information

In Example 5-2, you can see the firmware and NVSRAM versions of controller A.

Example 5-2 Controller firmware and NVSRAM

Controller in Enclosure 85, Slot A

Status:	Online
Current configuration	
Firmware version:	07.77.18.00
Appware version:	07.77.18.00
Bootware version:	07.77.18.00
NVSRAM version:	N1818D53R0777V05
Pending configuration	
Firmware version:	None
Appware version:	None
Bootware version:	None
NVSRAM version:	None
Transferred on:	None

HDD information

The Drives tab in the profile data provides the information shown in Example 5-3.

Example 5-3 Drive information

DRIVES-----

SUMMARY

Number of drives: 32
 Current media type(s): Hard Disk Drive (32)
 Current interface type(s): Fibre (32)

BASIC:

	ENCLOSURE,	SLOT	STATUS	CAPACITY	MEDIA TYPE	INTERFACE TYPE	
CURRENT DATA RATE	PRODUCT ID	FIRMWARE VERSION	CAPABILITIES				
	2,	1	Optimal	136.732 GB	Hard Disk Drive	Fibre	4
Gbps			ST3146356FC	F B98A			
	2,	2	Optimal	136.732 GB	Hard Disk Drive	Fibre	4
Gbps			MBA3147FD	F SD02			
	2,	3	Optimal	136.732 GB	Hard Disk Drive	Fibre	4
Gbps			MBA3147FD	F SD02			
	2,	4	Optimal	136.732 GB	Hard Disk Drive	Fibre	4
Gbps			MBA3147FD	F SD02			
	2,	5	Optimal	136.732 GB	Hard Disk Drive	Fibre	4
Gbps			MAX3147FD	F S708			
	2,	6	Optimal	136.732 GB	Hard Disk Drive	Fibre	4
Gbps			MBA3147FD	F SD02			
	2,	7	Optimal	136.732 GB	Hard Disk Drive	Fibre	4
Gbps			MBA3147FD	F SD02			
	2,	8	Optimal	136.732 GB	Hard Disk Drive	Fibre	4
Gbps			MAX3147FD	F S708			
	2,	9	Optimal	136.732 GB	Hard Disk Drive	Fibre	4
Gbps			MBA3147FD	F SD02			
	2,	10	Optimal	136.732 GB	Hard Disk Drive	Fibre	4
Gbps			MBA3147FD	F SD02			
.....							

Mappings information

Example 5-4 shows what is in the profile Mappings tab, which is similar to what is found in the mapping section of the Storage Manager client.

Example 5-4 Mappings information

MAPPINGS (Storage Partitioning - Enabled (1 of 2 used))-----

Logical Drive Name	LUN	Controller	Accessible by	Drive status
Access Logical Drive	31	A,B	Default Group	Optimal
Access Logical Drive	31	A,B	Host ssd-tbird-02	Optimal
HurleyLUN1	11	A	Host ssd-tbird-02	Optimal
Hurley_LUN03	2	B	Host ssd-tbird-02	Optimal
Hurley_LUN08	7	A	Host ssd-tbird-02	Optimal
Hurley_LUN01	0	B	Host ssd-tbird-02	Optimal
Hurley_LUN02	1	A	Host ssd-tbird-02	Optimal

Reading profile in a failed disk scenario

Using the profile data, select the **Arrays** tab to see the information shown in Example 5-5.

Example 5-5 Failed drive protected by hot spare

 ARRAYS-----

Name:	test
Status:	Degraded
Capacity:	272.464 GB
RAID level:	5
Media type:	Hard Disk Drive
Interface type:	Fibre Channel
Enclosure loss protection:	No
Security Capable:	No
Secure:	No
Current owner:	Controller in slot B

Associated logical drives and free capacity

Logical Drive	Capacity
1	1.000 GB
2	1.000 GB
3	1.000 GB
Free Capacity:	269.464 GB

Associated drives - present (in piece order)

Enclosure	Slot
2	6
11	8
2	7
11	15 [hot spare drive is sparing for drive at 11, 8]

You can see that the array named test is a RAID 5 built from the disks in slots 2-6, 11-8 and 2-7. However, the drive in 11-8 seems to be failed and is using a hot spare, as location 11-15 is sparing for the drive in 11-8.

The status of the array is degraded, so the reconstruction is likely still in progress for the hot spare drive, but we have to check the logical drives (1, 2 and 3, in this case) that are part of this array, as shown in Example 5-6.

Example 5-6 Profile data: Logical drives

STANDARD LOGICAL DRIVES-----

SUMMARY

Number of standard logical drives: 15

See other Logical Drives sub-tabs for premium feature information.

NAME	STATUS	CAPACITY	RAID LEVEL	ARRAY	MEDIA TYPE	INTERFACE TYPE
1	Optimal	1.000 GB	5	test	Hard Disk Drive	Fibre Channel
2	Degraded	1.000 GB	5	test	Hard Disk Drive	Fibre Channel
3	Degraded	1.000 GB	5	test	Hard Disk Drive	Fibre Channel

1 has already finished the reconstruction to the hot spare, as the status is Optimal, but the 2 and 3 logical drives are still reconstructing, because it still shows a Degraded status. We can cross check the information about the drives by using the Drives tab of the profile data (Example 5-7).

Example 5-7 Profile data: Drives

DRIVES-----

SUMMARY

Number of drives: 32

Current media type(s): Hard Disk Drive (32)

Current interface type(s): Fibre (32)

ENCLOSURE, SLOT	STATUS	CAPACITY	MEDIA TYPE	INTERFACE TYPE	CURRENT
DATA RATE PRODUCT ID	FIRMWARE VERSION	CAPABILITIES			
2, 6	Optimal	136.732 GB	Hard Disk Drive	Fibre	4
Gbps MBA3147FD	F SD02				
2, 7	Optimal	136.732 GB	Hard Disk Drive	Fibre	4
Gbps MBA3147FD	F SD02				
2, 8	Optimal	136.732 GB	Hard Disk Drive	Fibre	4
Gbps MAX3147FD	F S708				
2, 9	Optimal	136.732 GB	Hard Disk Drive	Fibre	4
Gbps MBA3147FD	F SD02				
11, 8	Failed	136.732 GB	Hard Disk Drive	Fibre	4
Gbps ST3146954FC	F B90F				
11, 9	Optimal	136.732 GB	Hard Disk Drive	Fibre	4
Gbps ST3146954FC	F B90F				
11, 14	Optimal	136.732 GB	Hard Disk Drive	Fibre	4
Gbps MBA3147FD	F SD02				
11, 15	Optimal	136.732 GB	Hard Disk Drive	Fibre	

Here we see that the drive in 11,8 has the status Failed and needs to be replaced.

5.4 Migrating arrays between DS storage subsystems

The DS Storage Manager incorporates export and import options to safely move arrays between different DS storage subSystems without losing data.

This capability is very helpful when you have to upgrade or replace a DS storage subsystem with a new model or faster disks, but want to preserve the expansions and their data.

The export/import options check that all the conditions to support the disk migration are met before placing the disks offline and allowing removal of the disks.

Now, instead of using the option to place an array offline, as was the case with previous versions of Storage Manager, just select the **Export Array** option on the source machine. Select the **Import Array** option on the destination machine to accept the exported disks with their data.

Important: We recommend upgrading both the source and the destination DS storage subsystems to the latest applicable firmware available before attempting any disk migration. Before you attempt to complete the drive migration procedure, review the information provided in the *IBM System Storage DS4000/DS5000 Hard Disk Drive and Storage Enclosure Installation and Migration Guide GA32-0962*.

5.4.1 Intermixing EXP810 and EXP5000 storage expansion enclosures

If you want to protect your current investment in IBM Midrange System Storage DS storage subsystems, you can migrate existing EXP810 expansion enclosures attached to an installed DS4700 or DS4800 to attach them to a DS5100 or DS5300. An RPQ approval from IBM is required for support of all migration configurations. With approved migration of EXP810 expansion enclosures to a DS5100 or DS5300, special consideration needs to be done about proper firmware levels and careful coordination needs to be made about differences in warranty and maintenance terms that will affect you. The purchase of new EXP810 expansion enclosures to attach to DS5100 or DS5300 will not be supported. When cabling EXP810 expansion enclosures behind a DS5100 or DS5300 storage subsystem, EXP810 expansion enclosures are cabled in the same manner as EXP5000 expansion enclosures. There are no special requirements to cable a mix of EXP810 and EXP5000 storage expansion enclosures behind a DS5100 or DS5300.

5.4.2 Intermixing EXP520 and EXP810 storage expansion enclosures

You can attach the EXP810 expansion enclosure to the DS5020 storage subsystem only after purchasing the Attach EXP810 to DS5020 Activation license option and activating it in the DS5020 storage subsystem. When cabling an EXP810 expansion enclosure behind a DS5020 storage subsystem, the EXP810 expansion enclosure is cabled in the same manner as an EXP520 expansion enclosure. There are no special requirements to cable a mix of EXP810 and EXP520 storage expansion enclosures behind a DS5020.

5.4.3 Migration prerequisites

To perform a successful export and import of arrays, the following conditions must be observed:

Attention: Failure to meet these conditions before you migrate hard disk drives might result in loss of data availability or loss of data.

- ▶ Run the Recovery Guru and make sure that the source and destination subsystems are in the Optimal state. Make sure to correct any problems before starting the migration. Check:
 - For failed drives
 - For hot spare drives in use (they all should be in Standby status)
 - That the entire array will be migrated (the disks in the array will be removed)
 - Missing logical drives
- ▶ The array being migrated must *not* have:
 - Logical drives with persistent reservations
 - Logical drives re-configuring or reconstructing
 - FlashCopy repository logical drive
 - Volume copy source or target logical drive
 - Mirror primary or secondary logical drive or mirror repository logical drive
- ▶ The array being migrated must have no mappings assigned.
- ▶ Verify the hardware compatibility and requirements.
- ▶ Obtain and activate any required premium features.
- ▶ Make sure that the hard disk drives are compatible.
- ▶ Make sure that the hard disk drive firmware is the latest applicable level.
- ▶ Install the latest applicable levels of firmware in both the source and destination DS storage subsystems.
- ▶ Do not migrate from a DS storage subsystem with a newer firmware level than the destination.
- ▶ Make sure that your source and destination DS storage subsystems have unique array names and logical drives names.

Important: Before you attempt to complete the drive migration procedure, review the information provided in the latest *IBM System Storage DS4000/DS5000 Hard Disk Drive and Storage Enclosure Installation and Migration Guide GA32-0962*.

In addition to these prerequisites, there are additional distinct considerations specifically for the source and for the destination DS storage subsystems.

Source DS storage subsystem prerequisites

On the source storage subsystem, perform the following actions before starting the export operation:

- ▶ Verify that the storage subsystem is in Optimal state and does not in the middle of long running tasks like Dynamic Volume Expansion (DVE) or Array RAID-level modification.

See the Recovery Guru function in the Storage Subsystem Management window for instructions on bringing the storage subsystem into Optimal state.

- ▶ Save and store the storage subsystem profile and configuration script along with the collect all support data bundle. This is a precaution to help you restore your configuration in the event of a problem during the export. Make sure to save both the configuration and profile files outside of the DS storage subsystem.
- ▶ Stop all I/Os and unmount the file systems to flush I/O from the server cache to disk.
- ▶ Back up array data. Back up data on the logical drives in the array selected for export, and verify the backup. Make sure that you save the backup outside of the DS storage subsystem disks.
- ▶ Locate the array and label drives. Use the locate array function to flash the LEDs on the drives in the array, and then label them with the source and destination storage subsystem names, array name, and total number of drives in the array.
- ▶ If you continue using the source enclosure expansion, obtain blank drive canisters or new drives, because after you remove the drives in the array, you must replace them with blank drive canisters or new drives to maintain proper airflow within the enclosure.
- ▶ If the migrated drives are FDE drives and were configured as part of secured array, save the storage subsystem security (lock) key to unlock the drives after installing them in a new storage subsystem.

If the migrated drives from the storage subsystem operate in external license key management mode, make sure that the new storage subsystem also operates in external license key management mode and uses the same external key server.

Destination DS storage subsystem prerequisites

On the destination storage subsystem, be sure of the following items:

- ▶ The storage subsystem have the latest firmware versions.
- ▶ Activate any required premium features.
- ▶ Verify the available drive slots. Be sure that you have enough empty slots for the drives you will be importing.
- ▶ The storage subsystem supports the RAID level that you are importing. You cannot exceed the maximum number of logical drives that the storage subsystem supports.
- ▶ Check that the drives to be imported are supported by the storage subsystem.
 - The storage subsystem must support the type of drives that you are exporting (that is, an intermix of SATA and Fibre Channel drives).
 - You cannot exceed the maximum number of drives supported by the storage subsystem.
 - Make sure that the drives are compatible with the storage expansion enclosure. For example, insert a 4 GB drive into a storage expansion enclosure that supports 4 GB drives.
- ▶ Make sure that the storage subsystem has the latest applicable controller firmware, nonvolatile storage random access memory (NVS RAM), and ESM firmware. Also, make sure that the installed controller firmware in the storage subsystem supports the drives and expansion enclosures.

5.4.4 Exporting an array

The migration is started using the export option in the DS Storage Manager client, and it will perform a preliminary check to validate the migration.

Perform the following steps:

1. In the Subsystem Storage Manager window, select the array to be exported.
2. Select **Advanced** → **Maintenance** → **Export Array...** from the Subsystem Management window, as shown in Figure 5-43.

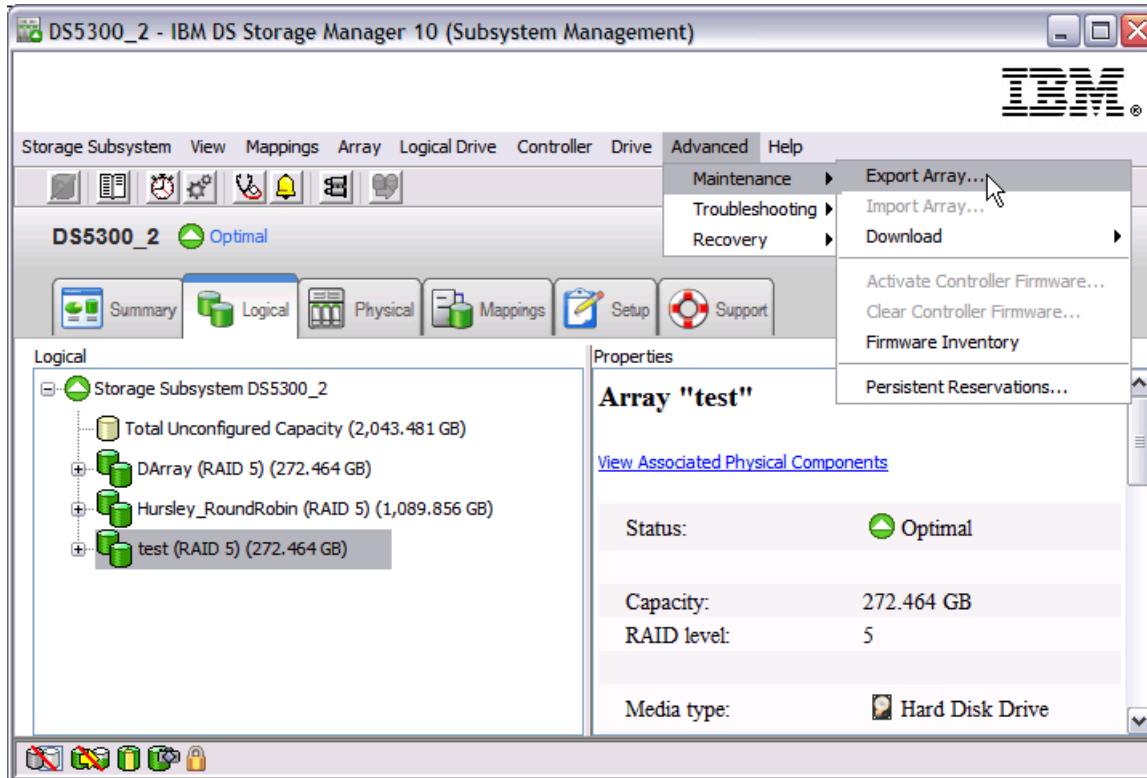


Figure 5-43 Exporting array

3. The Export Array option opens a wizard window. Clicking on **Next** you get a detailed Pre-check list with all the steps to cover on source storage subsystem as shown in Figure 5-44. The steps can be saved to a text file by clicking **Save As...**

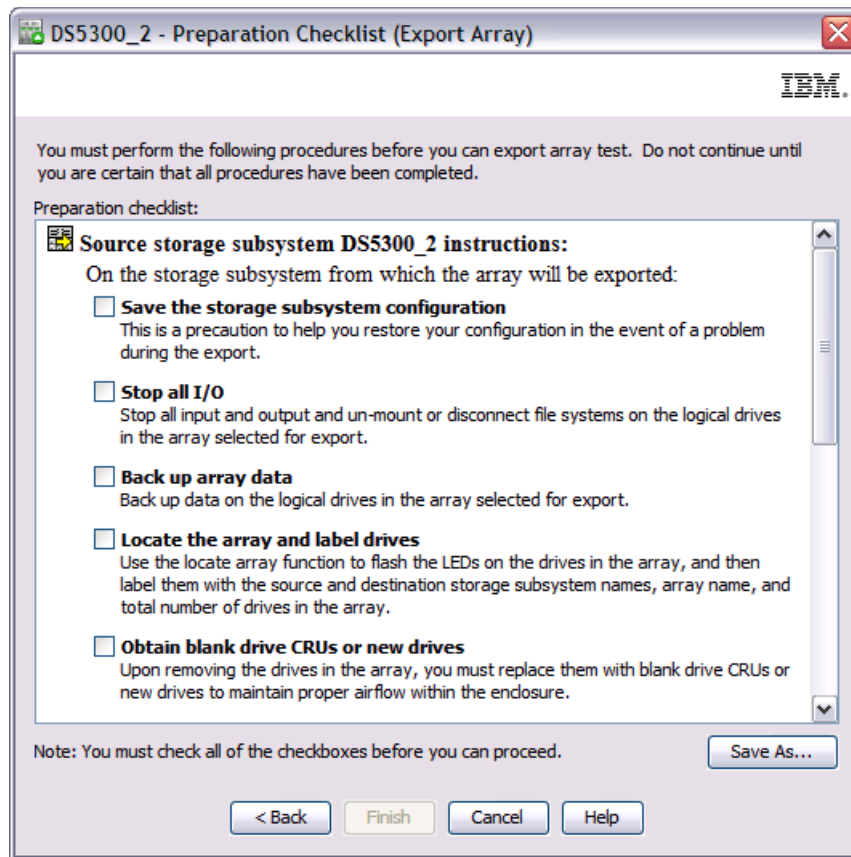


Figure 5-44 exporting array instructions

Figure 5-45 on page 337 shows all the steps to cover on target storage subsystem before continuing the operation.

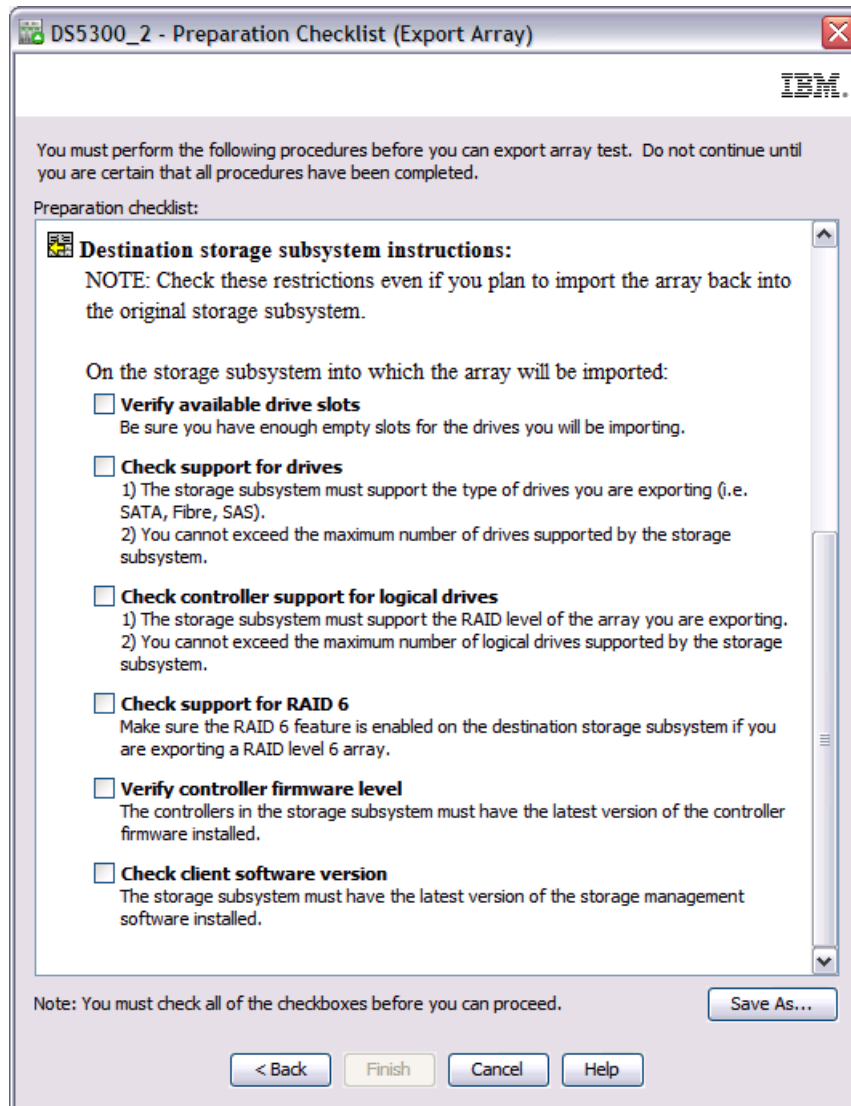


Figure 5-45 Exporting array instructions

Once you have verified all the conditions listed, check the box next to each item and click **Finish** to continue.

Note: Checking the box beside each task does not automatically cause the task to be completed. You must complete each task as you typically would. Checking the box simply helps you track the tasks you have completed and enables the Export button in the Export Array window.

4. Confirm the export operation in the confirmation window by typing yes and clicking on OK as shown on Figure 5-46 on page 338.



Figure 5-46 confirm export operation

When operation is completed, you get the window shown in Figure 5-47 on page 339 with instruction about how to remove the disks and move them to the destination system. These instructions can be saved to a text file by clicking **Save As...** .

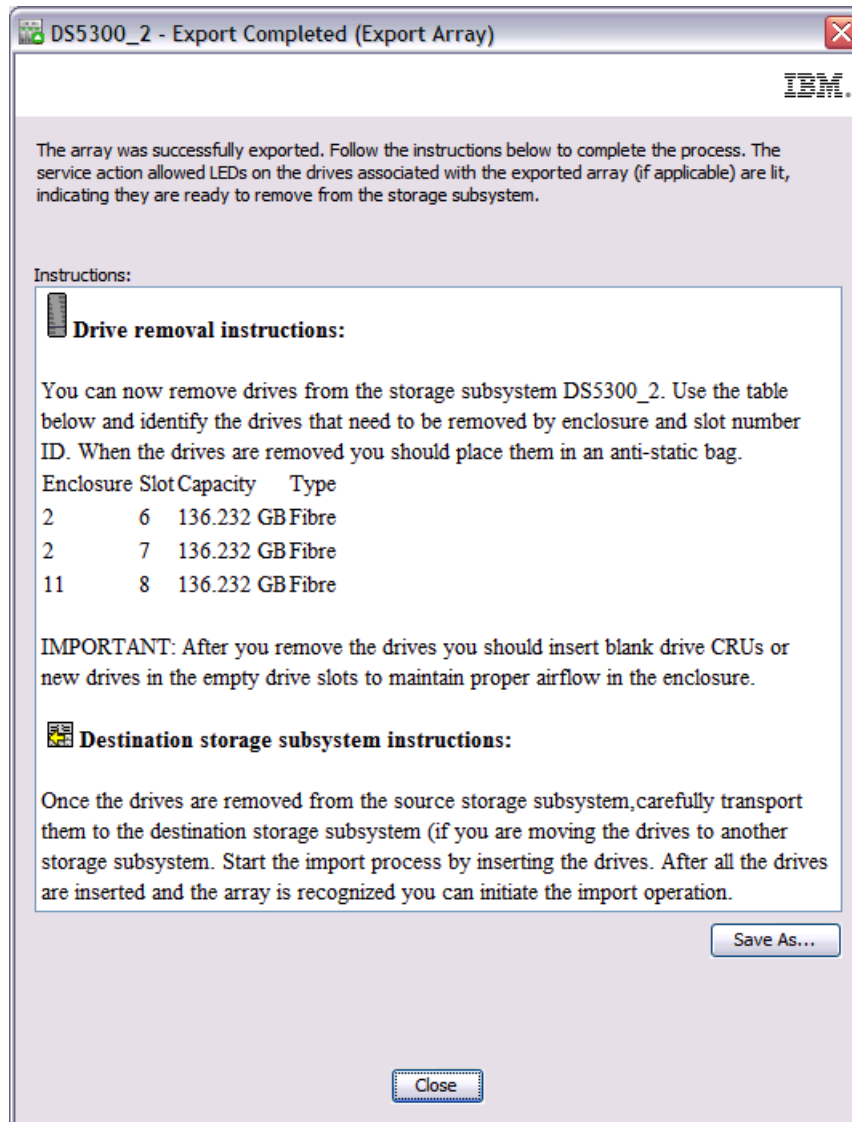


Figure 5-47 Exporting array: Disk removal instructions

- Before you start removing the disks, check the Storage Manager window to make sure that array status is **Exported ready for import** as shown on all Figure 5-48.

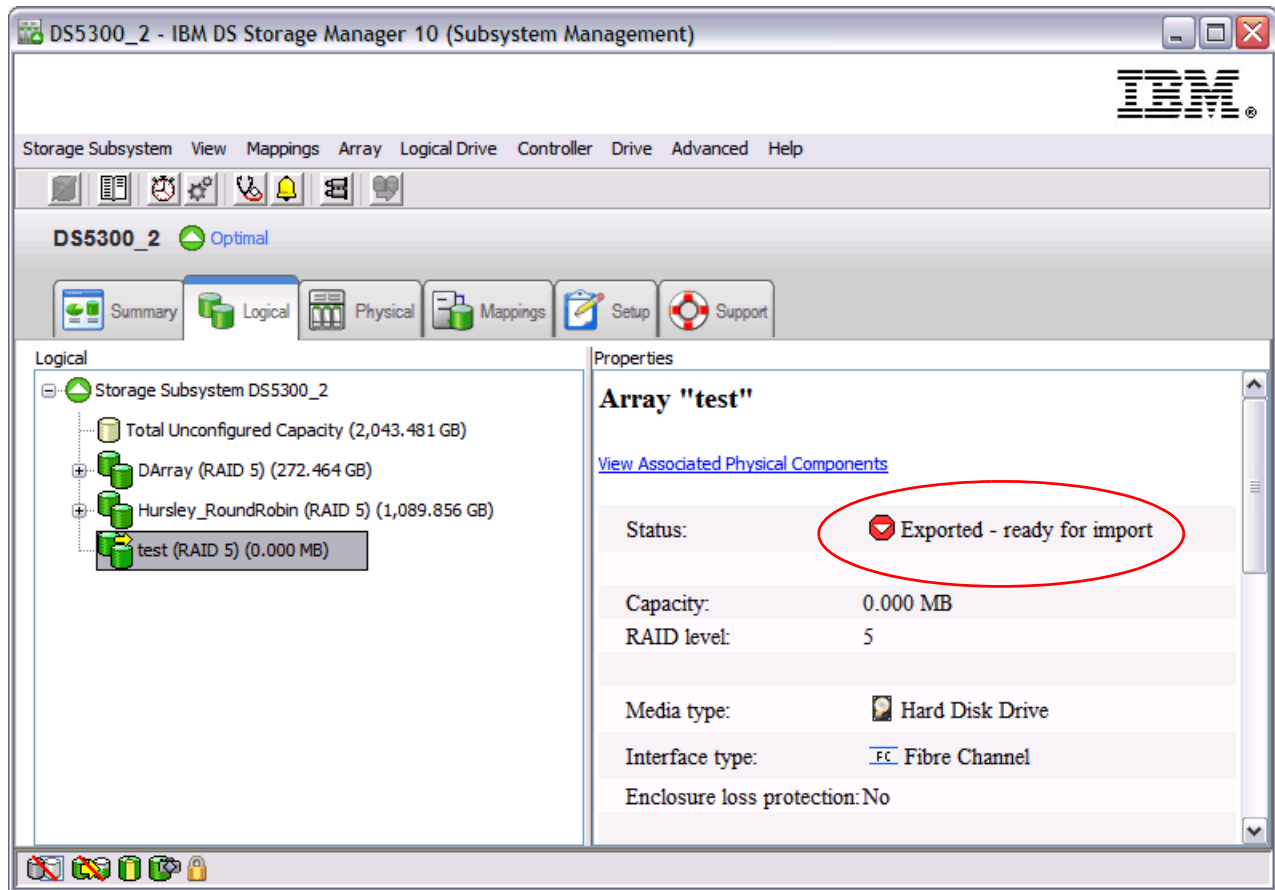


Figure 5-48 Array exported - ready for import

- Check also that the disks of the exported array are in an offline status, as shown in Figure 5-49 on page 341.

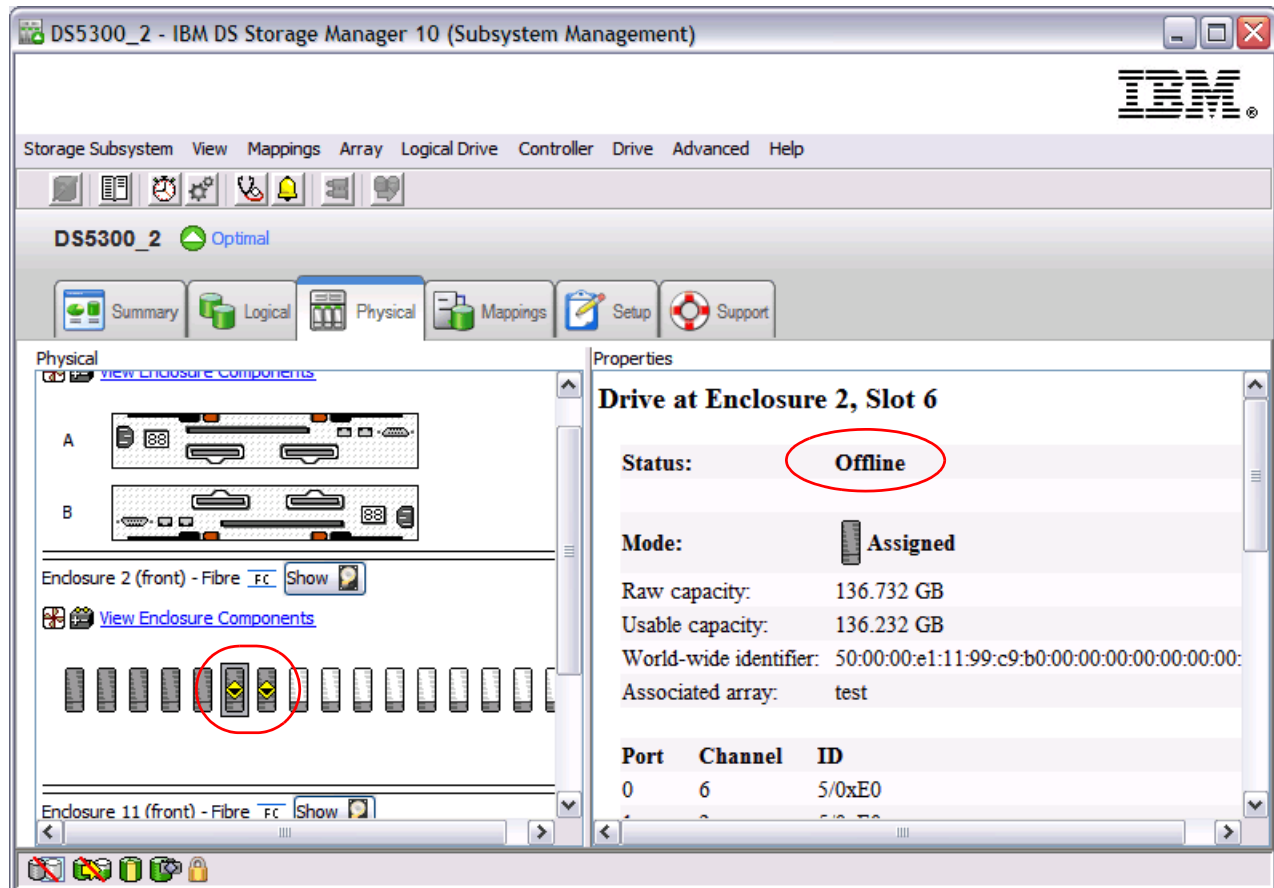


Figure 5-49 Array exported - Disks offline

7. You can now remove the drives (be sure to label them before removal). You have to remove *all* the of the exported array disks, and insert a dummy drive in each slot after removal to allow proper airflow. The dummy is needed only if the enclosure will remain operational.

Note: The export array operation sets all array disks in an offline status as part of the procedure. *Before* removing any disk, make sure that all the array disks are effectively marked offline, and all of them were appropriately labeled.

8. Carefully package each drive and move it to the destination system.

Proceed with the import process described in the 5.4.5, “Importing an array” on page 341.

5.4.5 Importing an array

Once you have removed all the disks being migrated from the source DS storage subsystem, you can start importing the disks into the destination DS storage subsystem.

Note: Migrate one array at a time. When migrating hard drives from multiple DS storage subsystems a single DS storage subsystem, move all of the hard drives from the first DS storage subsystem and import them onto the destination DS storage subsystem before proceeding with other sets.

To start with the process, follow these steps:

1. Use the Import Array option to import an array that you have previously exported. From the Subsystem Management window in the Logical view, select the array, and then select **Advanced** → **Maintenance** → **Import array**, as shown in Figure 5-50.

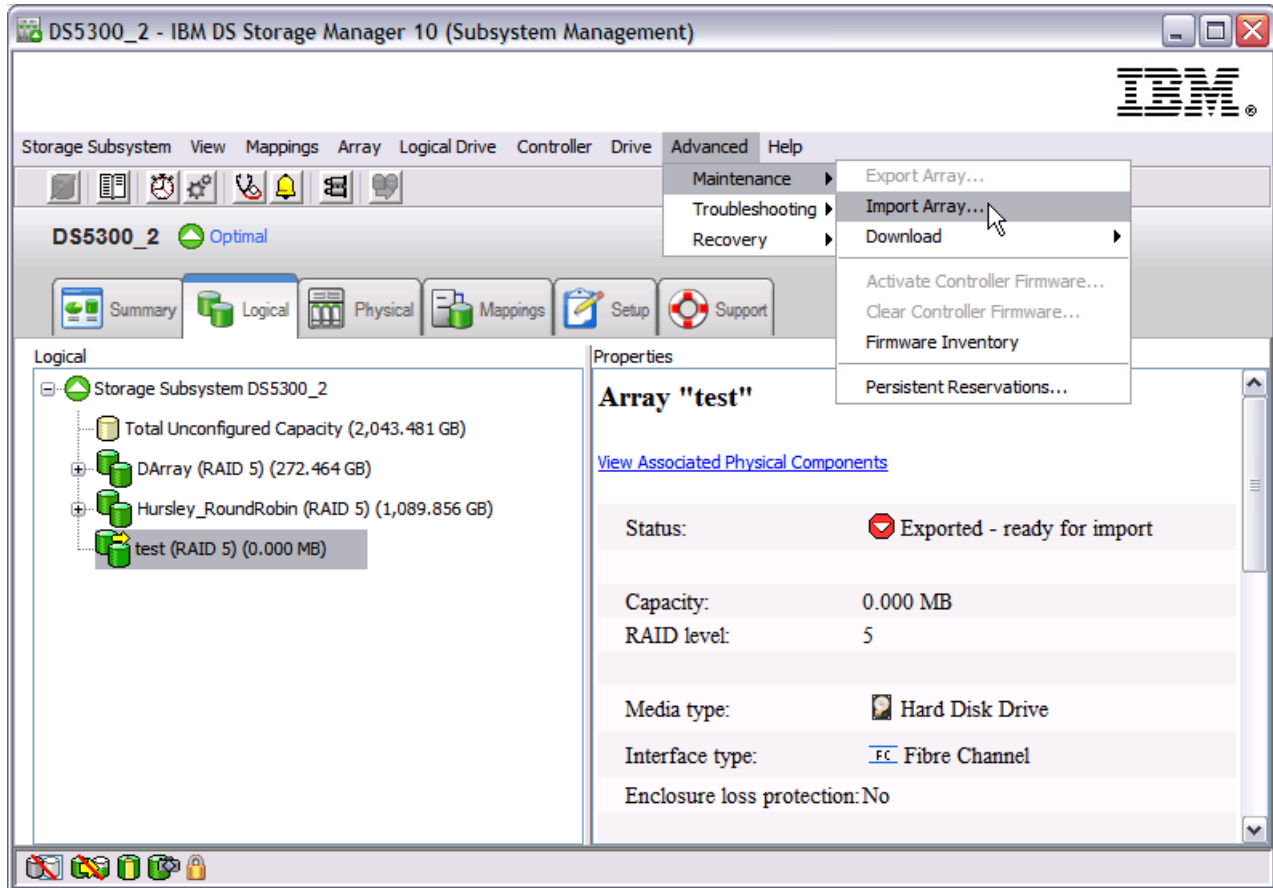


Figure 5-50 importing array

2. The Import Array option opens a wizard window. Clicking on **Next** you get the import array window as shown in Figure 5-51 on page 343.

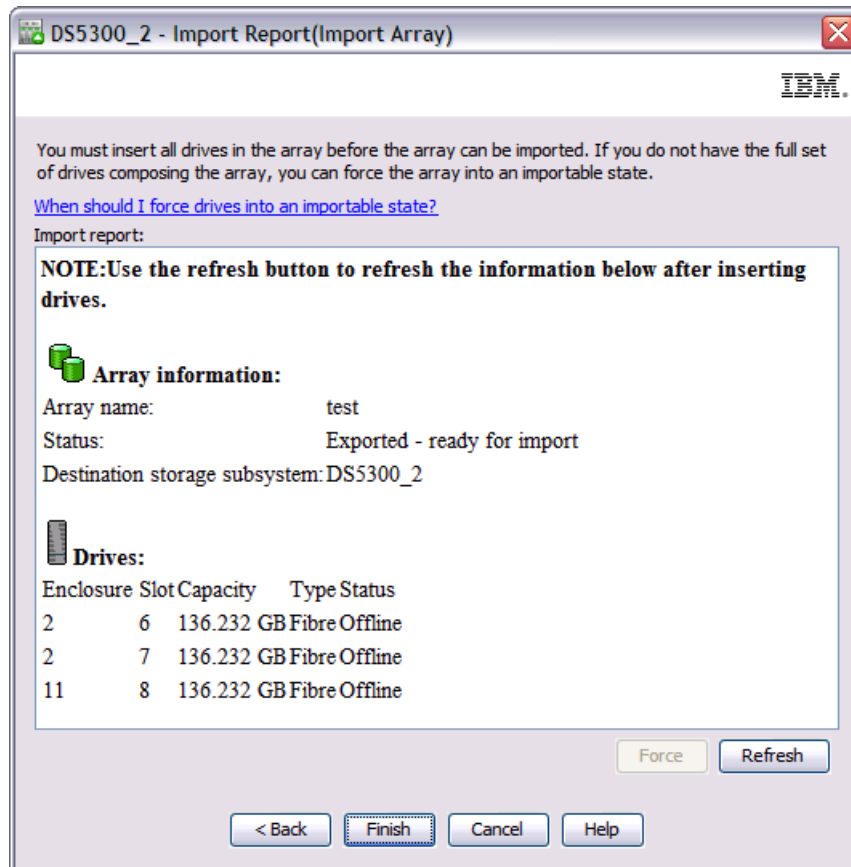


Figure 5-51 import array window

3. Click **Finish** if the configuration to import matches the exported configuration. If not, stop and go back to the original DS storage subsystem.
4. If the controller detects any condition that will interfere with the current configuration, it lets you know. If the condition detected is more critical, *stop here*. It is better to go back to the source DS storage subsystem to solve the issue.
5. A confirmation window displays as shows in Figure 5-52. Enter Yes and click **OK**.

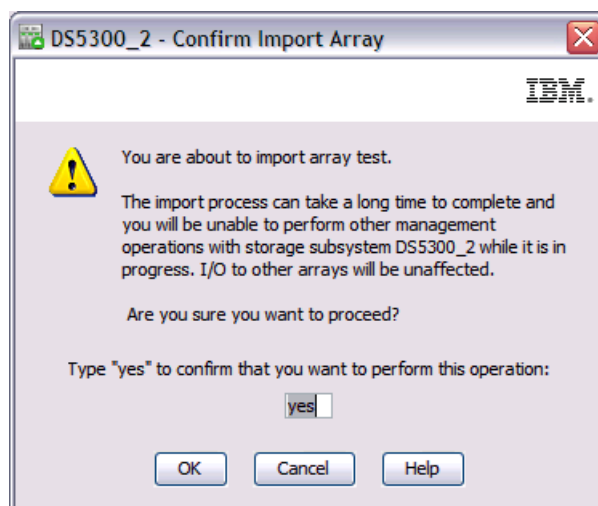


Figure 5-52 import array confirmation

6. The next window displays the result of the import process as shown in Figure 5-53. Make sure that the operation finished successfully, and scroll down the window to see the logical drives imported with the array. Make sure that all of them are available and click **Close** to terminate the dialog.

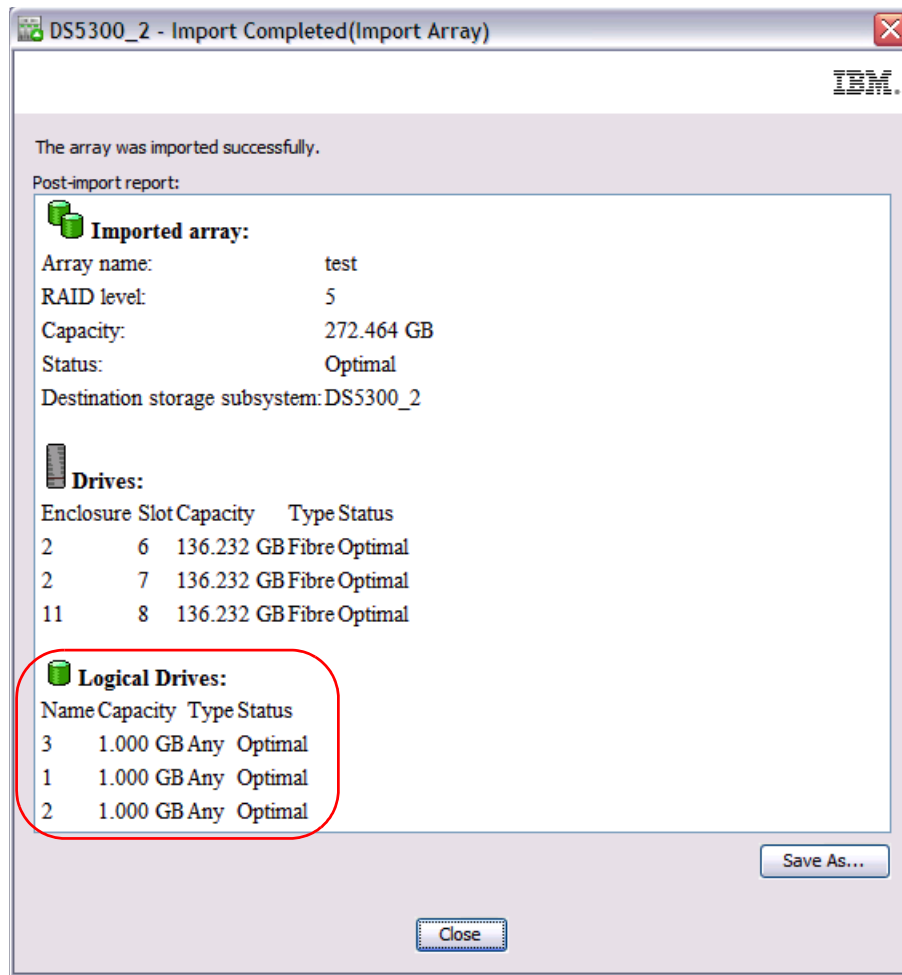


Figure 5-53 Import successfully done

A successful import operation finishes with the Storage Manager recognizing the disks in a Optimal status, as well as the array and the logical drives as they were in the source DS Storage Subsystem. See Figure 5-54 on page 345.

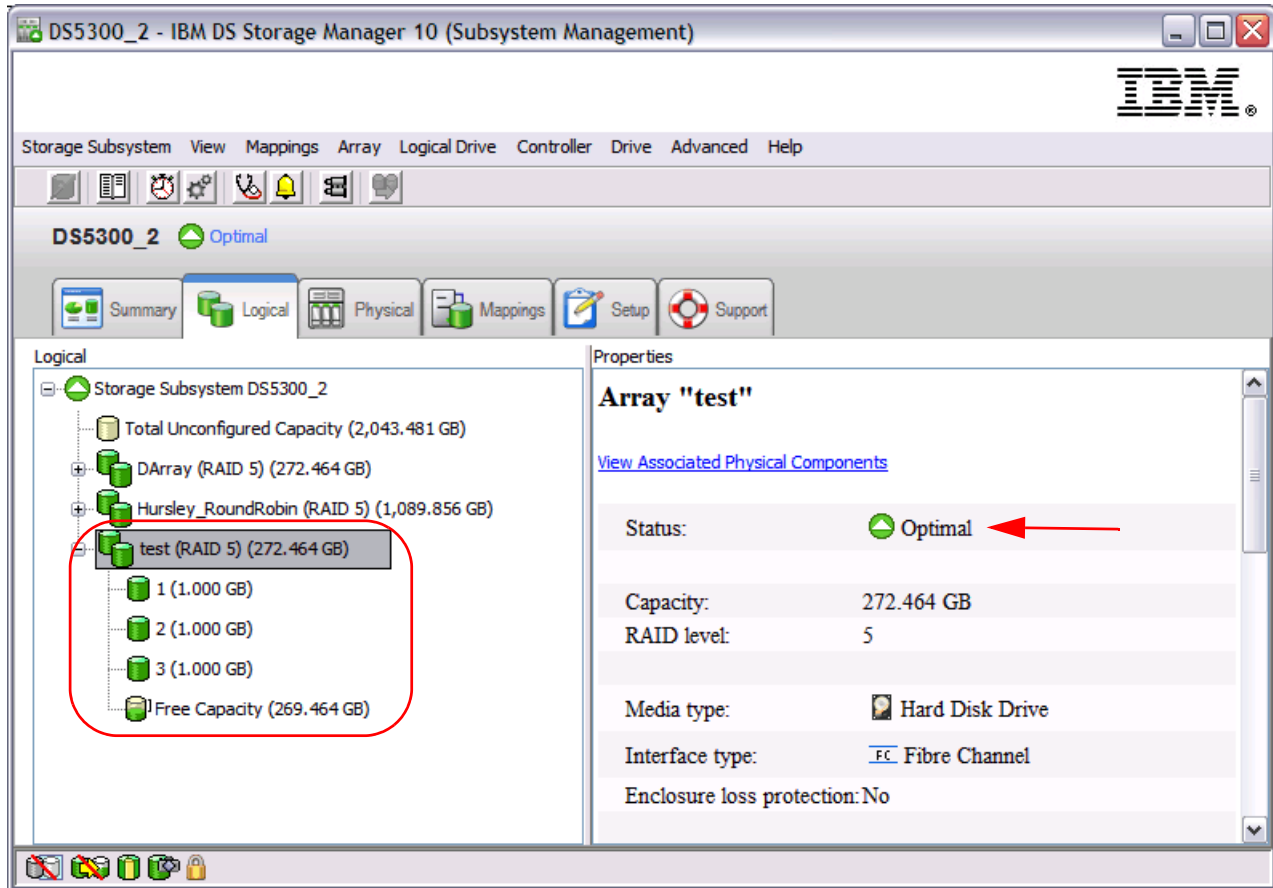


Figure 5-54 Finish import operation

A last step to perform before using the disks is to create the desired mappings. Once done, you will be able to access the migrated data, thus completing a successful migration.

5.5 Upgrading from a DS4700 or DS4800 to a DS5000

Important: Before you attempt the upgrade procedure, review the information provided in the *IBM System Storage DS4000/DS5000 Hard Disk Drive and Storage Enclosure Installation and Migration Guide GA32-0962* for additional instructions.

To upgrade a DS4700 or DS4800 storage subsystem to a DS5000 storage subsystem, complete the following steps:

1. Make sure that the data in the existing configuration is backed up in a secure place before starting the upgrade procedure.
2. Consider the following items before you upgrade a functioning storage subsystem:
 - a. Host attachment and premium feature entitlements:
 - i. To enable premium features in a new or replacement configuration that were enabled in an original configuration, you must purchase the applicable entitlements for the new or replacement storage subsystem, if that premium feature is not standard in the new or replacement storage subsystem. In addition, host attachment kits are only assigned to specific storage subsystems. You must also

purchase the applicable host attachment kits for new or replacement storage subsystems.

- ii. After the upgrade, premium features that were previously enabled in the original storage subsystem along with the enable-by-default premium features in the new storage subsystem are automatically placed in the Out of Compliance state. You must generate new premium feature SAFE keys to re-enable premium features.
- b. Storage firmware migration:
 - i. You can migrate the drives and drive expansion enclosures in a functioning storage subsystem to a new controller enclosure only if the firmware in the controllers of the functioning storage subsystem and the new controller enclosure have the same release version.
 - ii. The controller firmware version in the original controller enclosure must be the same or earlier than the controller firmware version in the new controller. Otherwise, the controller firmware in the new controller enclosure is placed in the Controller Lock down state.
 - iii. To migrate from an original storage subsystem controller with firmware Version 6.xx or earlier to a new storage subsystem controller with firmware Version 7.xx or later, upgrade the original storage subsystem controller firmware to Version 7.xx or later before you perform the migration. Otherwise, the controller firmware in the new controller enclosure is placed in the Controller Lock down state.
- c. Supported upgrades:
 - i. Migrating from a configuration with an integrated drive/RAID controller DS4700 storage subsystem to one with the RAID controller Ds5000 storage subsystem requires an additional storage expansion enclosure for the drives that are installed in the integrated drive/RAID controller DS4700 storage subsystem chassis.
 - ii. Some storage subsystem models require that hard disk drives and drive expansion enclosures operate at a specified Fibre Channel speed. Make sure that the hard disk drive and drive expansion enclosures can operate at that speed before you begin the upgrade.

5.5.1 Planning the upgrade

To plan the upgrade, perform the following steps:

1. Migrating from a DS4700 or DS4800 storage subsystem to a DS5100 or DS5300 storage subsystem is supported. However, you must submit a RPQ with IBM to migrate any EXP810 drive expansion enclosures connected to the existing DS4700 or DS4800 controller. You can submit an RPQ to your IBM marketing representative or authorized reseller.

Note: Only EXP810 drive enclosures can be migrated from a DS4700 or DS4800 configuration into DS5100 or DS5300 configuration.

2. Purchase the premium feature entitlements that are enabled in the original storage subsystem for the new storage subsystem, if that premium feature is not standard in the new storage subsystem.
3. Purchase the host attachment entitlement kits for the new storage subsystem.
4. If you are migrating from a working DS4700 configuration, purchase an additional EXP5000 drive expansion enclosure to install the hard disk drives in the internal bays of the DS4700.

If there are enough empty drive bays in the existing drive expansion enclosures, you can move the drives in the original DS4700 enclosure to the empty drive bays.

5. Lay out the drive expansion enclosure cabling to the new storage subsystem. See the documentation that comes with the new DS5000 storage subsystem for more information. See the *Installation, User's, and Maintenance Guide - IBM System Storage DS5100 and DS5300 GA32-0955* for information about the storage expansion enclosures cabling rules.
6. Purchase any additional hardware that is required to cable the existing drive expansion enclosures to the new storage subsystem using the drive expansion enclosure cabling layout as a guide.
7. Make sure that the original subsystem is in the Optimal state.
8. Perform a full backup of the original storage subsystem and schedule it for down time.
9. Retrieve the proofs of purchase for both the original and new storage subsystems and for any additional premium feature entitlements on the new and original storage subsystems.
10. If there are any switch zoning definitions or applications that rely on the storage subsystem worldwide names, plan to update them to use the new storage subsystem worldwide names after the migration to the new storage subsystem is complete.

5.5.2 Preparing the new storage subsystem

To prepare the new storage subsystem for the upgrade, perform the following steps:

1. Unpack the new DS5000 storage subsystem and install it in a rack. *Do not connect* it to the drive expansion enclosures attached to the original DS4700 or DS4800 storage subsystem.
2. Connect the new storage subsystem to the systems-management network using the default IP addresses of the controllers and record the version of the controller firmware on the new storage subsystem.

The default TCP/IP address of controller A Ethernet port 1 is 192.168.128.101 and the default TCP/IP address of controller A Ethernet port 2 is 192.168.129.101.

The default TCP/IP address of controller B Ethernet port 1 is 192.168.128.102 and the default TCP/IP address of controller B Ethernet port 2 is 192.168.129.102.

Note: Only one Ethernet port connection from each controller is required to establish a direct (out-of-band) management connection to the DS5100 or DS5300. We recommend to use Ethernet port 1 only. Also, to minimize security risks, do not connect the DS5100 or DS5300 in a public LAN or public subnet. Use a local private network for the DS5100 or DS5300 and the management station Ethernet ports.

5.5.3 Preparing the original storage subsystem

To prepare the original storage subsystem for the upgrade, perform the following steps:

1. If any long running tasks are processing in the original storage subsystem, make sure that they have completed. Examples of long running tasks are:
 - Dynamic volume expansion (DVE)
 - Dynamic capacity expansion (DCE)
 - Logical drive segment size modification
 - Array RAID-level modification
 - User-initiated array redundancy checking (on the Storage Subsystem Management window, select **Array** → **Check Redundancy**).

- Remote mirror logical drive synchronization, FlashCopy image or VolumeCopy image logical drive creation.
 - Logical drive reconstruction or copyback.
2. Save and store the storage subsystem profile and configuration script along with the collect all support data bundle. Save it in a safe location and not on the logical drives that are mapped from the original storage subsystem.
 3. Record the version of the controller firmware that is on the storage subsystem.
 4. Stop all programs, services, and processes on the host servers that access the logical drives that are defined in the migrated hard disk drives. Also, make sure that there are no programs, services, or processes running in the background that write data to the logical drives.
 5. Unmount the file systems to flush I/O from the server cache to disks.
 - If you are using a Windows operating system, remove the drive letter or the mount points of the drive-to-LUN map definitions, instead of unmounting the file systems.
 - See your operating-system documentation for information about the file system unmount procedure.
 6. Perform an incremental backup of the data that was changed since the full backup that you made in 5.5.1, “Planning the upgrade” on page 346.
 7. Make sure that the environmental service modules (ESMs) and hard disk drives in the original storage subsystem are updated to the latest firmware level. To download the latest firmware level, go to the following address:

<http://www.ibm.com/support/entry/portal/>

5.5.4 Upgrading the controller firmware

To upgrade the controller firmware, perform the following steps:

1. Use the flow chart shown in Figure 5-55 on page 349 to determine the firmware version required in the new storage subsystem. To download the latest firmware level, go to the following address:
<http://www.ibm.com/support/entry/portal/>
2. The controller firmware is normally listed as either xx.yy.zz.aa or xxyyzzaa, where xx.yy or xxyy is the controller firmware version used for compatibility checking. If the first x=0, it might not be identified. For example, 07.77.18.00 is the same as 7.77.18.00.

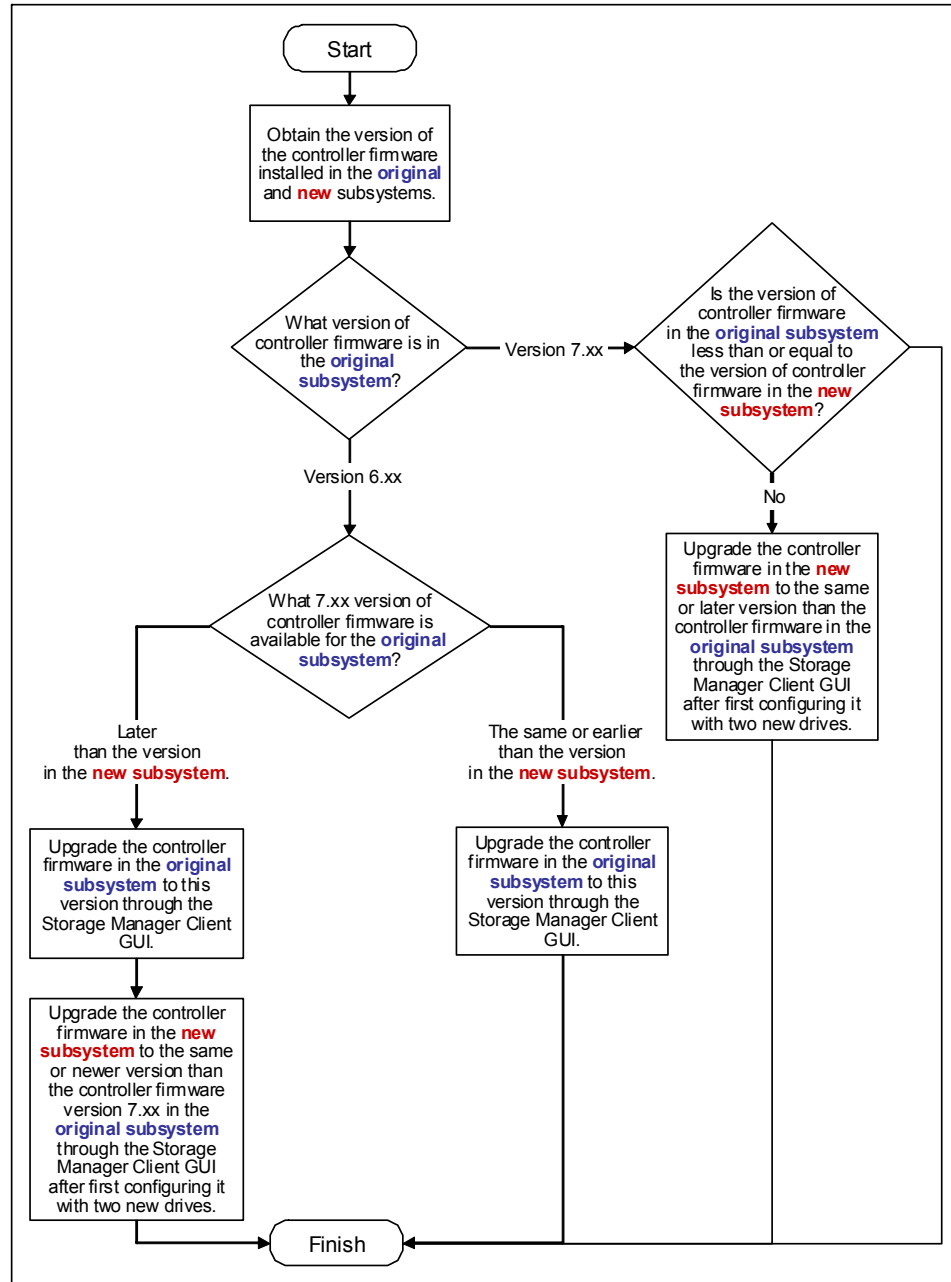


Figure 5-55 Firmware compatibility flow chart for a DS4700 or DS4800 to a DS5000 storage subsystem upgrade

3. Save and store the storage subsystem profile and configuration script along with the collect all support data bundle.
4. Delete any FlashCopy images of the logical drives.
5. Delete any VolumeCopy logical drive pairs.
6. Delete any remote mirror relationships.
7. Delete any host-to-LUN mapping definitions in the original storage subsystem.

If you configured the new storage subsystem with at least two new drives to place the storage subsystem into the Optimal state for updating the controller firmware, power off the new

storage subsystem controller enclosure and remove the two drives (along with the additional expansion enclosure, if attached).

5.5.5 Switching from the original to the new storage subsystem

To switch from the original to the new storage subsystem, perform the following steps:

1. Perform one of the following tasks to export arrays, depending on the availability of hot spare drives and unconfigured drives in the storage subsystem:
 - If hot spare drives or unconfigured hard disk drives are installed in the original storage subsystem, export all of the defined arrays.
 - If no hot spare drives or unconfigured hard disk drives are installed in the original storage subsystem, keep one array on the original storage subsystem and export all the other arrays. One array must be in the Optimal state for the storage subsystem to be up and running.

Note: An error occurs if you try to export the last defined array in a storage subsystem configuration and no hot spare drives or unconfigured drives are installed.

To export an array using the Storage Subsystem Management window, right-click the name of the array and select **Advanced** → **Maintenance** → **Export Array**, and follow the instructions in the window that opens (refer to 5.4.4, “Exporting an array” on page 335). You can also use the Start Array <array name> Export command in the IBM Storage Manager Client script window.

2. Power off the original controller enclosure first, and then power off the drive expansion enclosures. This is the best practice power-off sequence. See the documentation that comes with the storage subsystem for details about the power-off sequence.

Note: The controller enclosure must be powered off before the drive expansion enclosure.

3. Label all the cables connected to the original storage subsystem enclosure.
4. Wait until the LEDs on the storage subsystem chassis are off, and then disconnect all cables from the storage subsystem chassis.
5. Remove the original storage subsystem enclosure from the rack.
6. Install the new storage subsystem enclosure in the rack.
7. If the original storage subsystem is a DS4700 storage subsystem, install an EXP5000 drive expansion enclosure and move the hard disk drives from the original storage subsystem to the drive expansion enclosure.
8. Insert the SFPs into the new storage subsystem drive loop/channel port bays and cable the drive expansion enclosures to the new storage subsystem using the cabling layout you defined in 5.5.1, “Planning the upgrade” on page 346.
9. Insert the SFPs into the new storage subsystem host port bays and cable the host interface ports and the storage subsystem management ports of the new storage subsystem enclosure.
10. Make sure that all of the storage expansion enclosures are set to the same speed for each drive channel/loop.

5.5.6 Preparing the new storage subsystem for use

To prepare the new storage subsystem for use, perform the following steps:

1. If the controller TCP/IP addresses are assigned using DHCP, update the DHCP records with the new controller Ethernet port MAC addresses.

The controllers first check for a DHCP server during the boot process. If the controllers do not detect a DHCP server, they use either the static IP address (if defined) or the default IP addresses.

2. Power on the drive expansion enclosures if they are powered off. Do not power on the new storage subsystem controller enclosure. Check the drive expansion enclosure LEDs to make sure that the drive expansion enclosures are connected properly.
3. Power on the new storage subsystem controller enclosure.

If the TCP/IP addresses of the Ethernet management ports are statically defined for the original storage subsystem controllers, the TCP/IP addresses are used for the same Ethernet management ports in the new controllers.

4. Connect the new storage subsystem to the IBM DS Storage Manager Client either through the out-of-band method using the applicable TCP/IP addresses of the controller Ethernet management ports or through the in-band method through Fibre Channel connections.

Note: The new storage subsystem identifies itself as the machine type that it replaced until you download the applicable NVSRAM firmware for the new storage subsystem.

5. Make sure that the new storage subsystem configuration is in the Optimal state and that all of the drives are identified. Use the Recovery Guru in the DS Storage Manager Client Subsystem Management window to resolve any Needs Attention conditions.
6. Update the controller firmware of the new storage subsystem to the latest available version, if required.
7. Download the applicable NVSRAM firmware for the new storage subsystem.
8. Import all of the arrays that were exported in 5.5.5, "Switching from the original to the new storage subsystem" on page 350 (refer to 5.4.5, "Importing an array" on page 341). Make sure that all of the imported arrays are online and in the Optimal state.
9. If any of the following conditions persist, contact IBM Support for assistance:
 - The empty drive bay icon is displayed for the drive bay into which you inserted the migrating drive.
 - The Failed unconfigured drive icon or the Failed configured drive icon is displayed for the drive bay into which you inserted the migrating drive.
 - The Incompatible drive icon is displayed for the drive bay into which you inserted the migrating drive.
 - Array configuration data on the drives you have added is incomplete.
 - You cannot import the array.
10. Use the Enable Identifier storage subsystem premium feature to generate and apply premium features keys to remove *Out of Compliance* errors on enabled premium features from the original storage subsystem. See 5.2, "Handling premium features" on page 315 or the instructions that come with the Enable Identifier premium feature for information about generating the premium feature keys.

11. Extract the applicable SMCli commands in the configuration script file that you saved in 5.5.4, "Upgrading the controller firmware" on page 348 to recreate the FlashCopy images, VolumeCopy images, remote mirror relationships, and host-to-LUNs map definitions, as required.
12. Make sure that the enclosure IDs in each drive loop/channel contain a unique first-position digit (x1). In addition, if the drive expansion enclosures are re-cabled behind the new storage subsystem controller enclosure, modify the second-position digit (x10) so that they have the same second-position digit for all the drive expansion enclosures in a drive channel/loop.
13. Update the switch zoning definitions and any applications that rely on the storage subsystem worldwide names to use the new storage subsystem worldwide names.

5.6 Connecting a new storage enclosures to your DS5000

If you are adding new expansion enclosures model or new disks type on your DS5000 configuration, check following:

- ▶ Review the minimum requirements of firmware for your DS5000 Storage Subsystem.
- ▶ Check if your DS5000 Storage Subsystem supports the new disk or expansion to add, and if the expansion supports the new disk type.
- ▶ Check if the new hardware is compatible to operate in the current speed of the current drive side Fibre Channel speed. You can connect storage enclosures at either end, or in the middle, of an existing storage enclosure drive loop.

If you have no particular reasons to connect the new expansion at the top or in the middle, it's a Best practice to connect the new expansion to the end of the drive loop. In this way you avoid eventual drive channel errors the may be cause by disconnecting the existing drive loop cabling.

To connect a storage enclosure at the end (bottom) of a drive loop, as shown in Figure 5-56 on page 353, complete the following steps:

1. Insert the small form-factor pluggables (SFPs) into only those ports that you intend to use. Do not leave SFPs inserted into port connectors without connecting them to other ports using cables. An unused SFP, even pulled slightly away from the socket might generate random errors in the drive loop/channel.
2. Extend the drive loops connected to controller A by connecting the ESM port 1A of the left ESM in the last storage enclosure on the existing drive loop/channel A to the ESM port 1B of the left ESM in the new storage enclosure (cable 1).
3. Make sure that there are not any drives fully inserted in the drive bays; then, turn on the power to the added storage enclosure.
4. Wait a few seconds. Check the drive port LEDs to make sure that the link to the new storage enclosure is up and optimal and that there are no link problems in the modified drive loop A. Using the DS Storage Manager Client Subsystem Management window, verify that the storage enclosure is added and displayed in the Logical/Physical view of the window.
5. Extend the drive loops connected to controller B by moving the connection from controller B drive port to the ESM port 1B in the right ESM of the last storage enclosure in the existing drive loop/channel B to the ESM port 1B of the right ESM in the new storage enclosure (cable 2). Controller B drive port is now connected to the ESM port of the new storage enclosure.

6. Wait a few seconds. Check the drive port LEDs to make sure that the link to the new storage enclosure is up and optimal and that there are no link problems in the modified drive loop A. Using the DS Storage Manager Client Subsystem Management window, verify that the storage enclosure is added and displayed in the Logical/Physical view of the window.
7. In drive loop B, cable the ESM port 1A in the right ESM of the new storage enclosure to the ESM port 1B in the right ESM of the last storage enclosure in drive loop B (cable 3).
8. Wait a few seconds. Check the drive port LEDs to make sure that the link to the new storage enclosure is up and optimal and that there are no link problems in the modified drive loop A. Using the DS Storage Manager Client Subsystem Management window, verify that the storage enclosure is added and displayed in the Logical/Physical view of the window. The DS Storage Manager Client Subsystem Management window displays a new storage enclosure with no drives in the configuration.
9. Insert drives into empty drive bays in the new enclosure one at a time. Wait (up to 5 minutes) until the inserted drive fully spins up and is identified in the Storage Subsystem Management window; then, insert the next hard disk drive.
10. Upgrade expansion and drive firmware if needed. *Mix of enclosure firmware versions is not supported.*

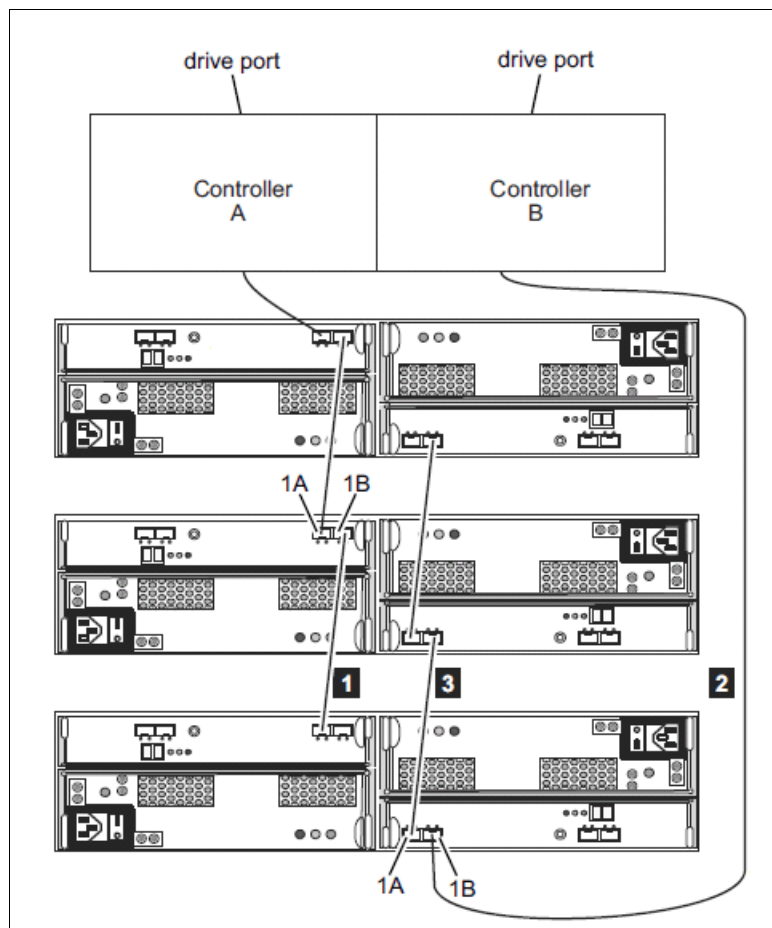


Figure 5-56 Connecting a new drive enclosure to a working DS5000

Note: Refer to the Capacity Upgrades section of *IBM System Storage DS5000 Series Implementation and Best Practices Guide*, SG24-8024 to choose the best way to increase your capacity or the *Installation and Migration Guide for Hard Drive and Storage Expansion Enclosure - GA32-0962 (MIGR-57818)* if you need more details about procedure.

5.7 Securing the DS5000 storage subsystem client using remote management

The Remote Services feature of Microsoft Windows XP allows users of the DS5000 storage subsystem to remotely access the storage subsystem's client, profile, information, and logs through a Virtual Private Network (VPN) connection and Microsoft's Remote Desktop (RDP) function.

Remote access of the client workstation has some big advantages. It allows you to configure the DS5000 storage subsystem without having to be physically present at the client workstation. This will allow you to be more responsive to your storage environment at any time and from any place. However, using a secure connection is very important. If unauthorized users are able to gain access to your internal client workstation, they can launch the Storage Manager client and gain access to any of the DS5000 storage subsystem's configuration information. Also, if you do not have a password set, they can even modify the configuration or potentially compromise data.

Note: The IBM System Storage DS Storage Manager client allows you to set a password to prevent unauthorized users from making configuration changes. However, the password does not prevent an unauthorized user from viewing the Storage Manager client if they can gain access to your client workstation.

Securing your internal Storage Manager Client workstation, while allowing authorized users remote access, can be best achieved by implementing the following:

- ▶ Virtual Private Network (VPN) connection: Permits only authorized users access to your internal network.
- ▶ Remote Desktop Users/Passwords: Permits only authorized users to access your Storage Manager Client workstation.
- ▶ "Dual-homed" Storage Manager Client workstation:
 - One network card for the DS5000 Management LAN
 - One network card for the customer WAN
 - Physically separates the DS5000 management network from the rest of the enterprise network
- ▶ Storage Manager Client Password: Permits only authorized users to make configuration changes to the DS5000 storage subsystem through the Storage Manager Client.

Figure 5-57 shows how to secure your environment for remote access. By introducing multiple layers of security, you will be best protected from unauthorized access to your DS5000 storage subsystem.

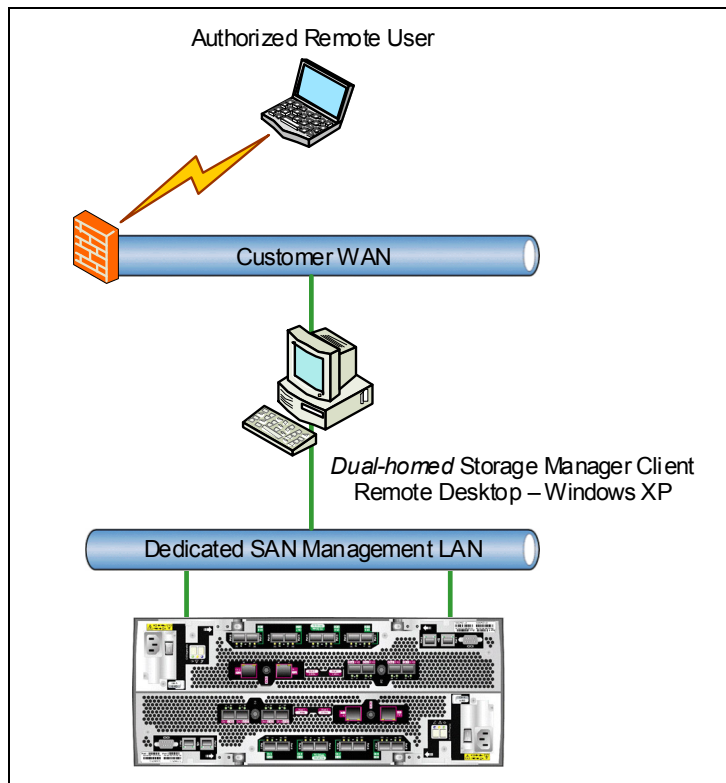


Figure 5-57 Securing remote access to the Storage Manager Client

In addition, Remote Desktop (RDP) is a high-encryption client that can run on any Windows server. It uses RSA Security's RC4 cipher, a stream cipher designed to efficiently encrypt small amounts of data. RC4 is designed for secure communications over networks. Administrators can choose to encrypt data by using a 56- or 128-bit key.

Hardware requirements

In order to use Remote Desktop for the secure remote management of the DS5000 storage subsystem, you must have the following hardware/settings:

- ▶ Windows XP Professional or higher on the client workstation.
- ▶ Client workstation must be “dual-homed”:
 - One network card for the dedicated DS5000 Management LAN (can be VLAN).
 - One network card for the customer WAN.
- ▶ Accounts that will allow authorized users to remote control the desktop.
- ▶ Client configured with Remote Desktop.
- ▶ Client configured for Remote Assistance.
- ▶ The client should have these DS5000 storage subsystem tools installed for management:
 - Storage Manager Client (latest version)
 - Storage Manager Utilities (latest version)
 - Qlogic SANsurfer (latest version)
 - PuTTY Version 0.6 or higher

- ▶ Dedicated DS5000 Management LAN (or VLAN).
- ▶ Customer firewall configuration:
 - Open firewall for well-known TCP Port (3389)
 - Must be able to support dedicated VPN connection
 - Can be disabled (when not needed) for security precautions

The following Web sites offer more information about RDP and Remote Assistance:

- ▶ How to connect to another computer using Remote Desktop Connection:
<http://windows.microsoft.com/en-US/windows-vista/Connect-to-another-computer-using-Remote-Desktop-Connection>
- ▶ Microsoft RDP Frequently Asked Questions (FAQ):
<http://windows.microsoft.com/en-US/windows7/Remote-Desktop-Connection-frequently-asked-questions>

5.8 Preventative maintenance and data collection

It is essential to regularly monitor the status of the DS5000 storage subsystem in order to identify potential problems promptly before they become more critical. The IBM System Storage DS Storage Manager V10.77 client software is ideally suited for this purpose. In this section, we cover some of the basic monitoring functions.

5.8.1 Storage Manager Enterprise Management window

This window is opened when we first launch Storage Manager. It provides a clear indication of the status of all DS5000 storage subsystems managed from this workstation. These units may be accessed either out-of-band (via an Ethernet connection) or in-band (via a Fibre Channel or iSCSI connection).

Figure 5-58 shows a typical Enterprise Management window highlighting which units are in an Optimal state and which require attention. Double-clicking any one of the units will launch the Subsystem Management window.

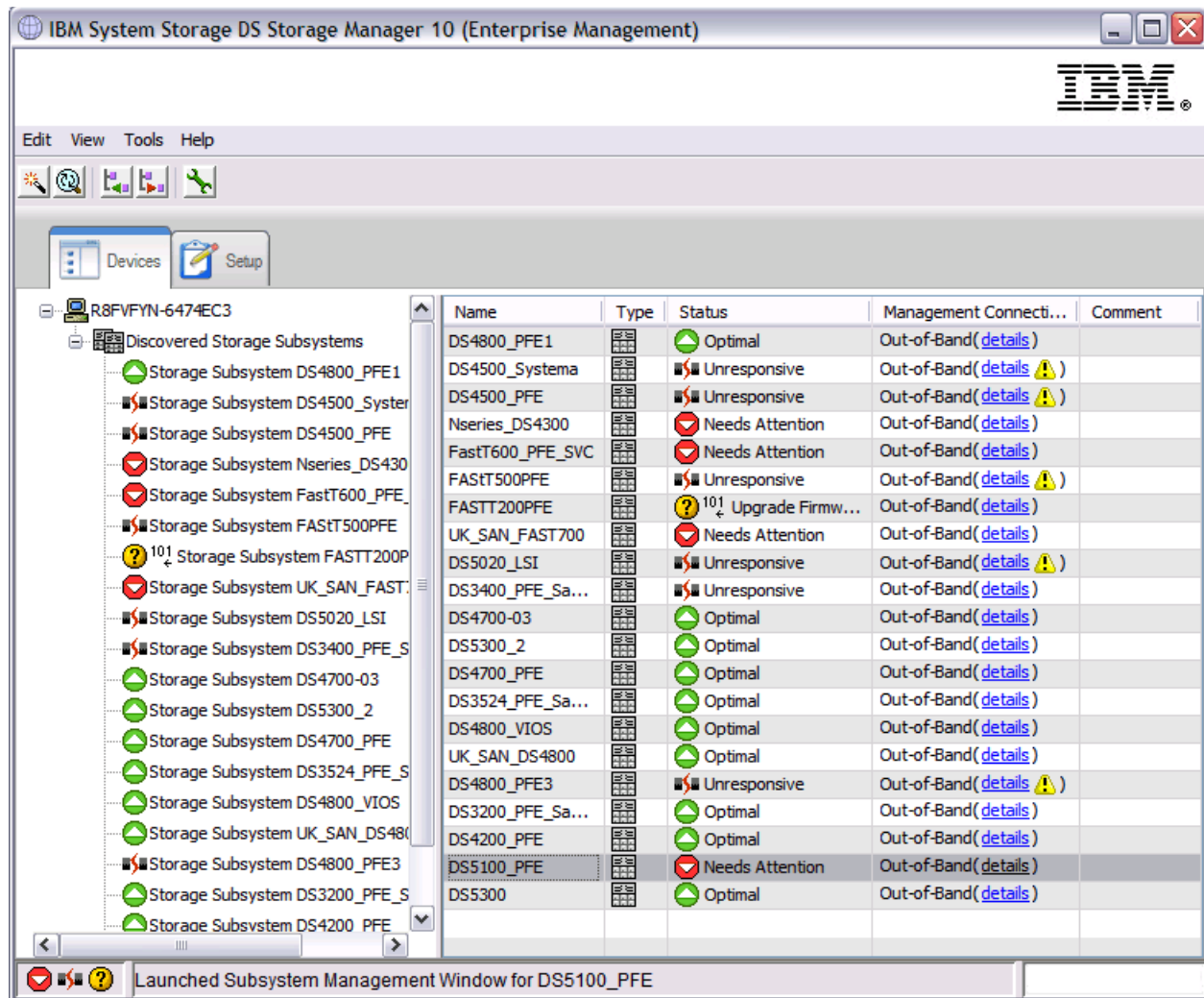


Figure 5-58 Storage Manager Enterprise Management window

Configuring e-mail or SNMP alert notifications in Enterprise Management window

After you add devices to the management domain, you can set up alert notifications to report critical events on the storage subsystems. The following alert-notification options are available:

- ▶ Notification to a designated network management station (NMS) using Simple Network Management Protocol (SNMP) traps.
- ▶ Notification to designated e-mail addresses.

You can only monitor storage subsystems within the management domain. If you do not install the Event Monitor service, the Enterprise Management window must remain open. If you close the window, you will not receive any alert notifications from the managed storage subsystems. See the Enterprise Management window online help for additional information.

Alert notification with SNMP traps

To set up alert notification to a Network Management Station (NMS) using SNMP traps, perform the following steps:

1. Extract the downloaded Storage Manager image file onto an NMS. You need to set up the designated management station only once.
2. Copy the SMxx.x.MIB file from the SMxxMIB directory to the NMS.
3. Follow the steps required by your NMS to compile the management information base (MIB) file. (For details, contact your network administrator or see the documentation specific to your particular storage management product.)
4. Select **Storage subsystem** → **Edit** → **Configure alerts** from the Enterprise Management window and complete the entries in the SNMP tab.

Alert notification with e-mail

To set up alert notification without using SNMP traps, select **Storage subsystem** → **Edit** → **Configure alerts** from the Enterprise Management window.

First, select the **Mail Server** tab to define the SMTP server. Then select the **Email** tab to define the e-mail addresses in the notification list together with an option to include contact information with the alert notification e-mail.

5.8.2 Storage Manager Subsystem Management window

The Storage Manager Subsystem Management interface includes a number of tools that can be used for monitoring, troubleshooting, and diagnostics:

- ▶ Storage Subsystem Profile
- ▶ Recovery Guru
- ▶ Major Event Log
- ▶ Collect all Support Data

Figure 5-59 shows some of the main visual problem indicators in the Subsystem Management window. Anyone using Storage Manager to monitor DS5000 storage subsystem could immediately tell when the unit is in a non-optimal state.

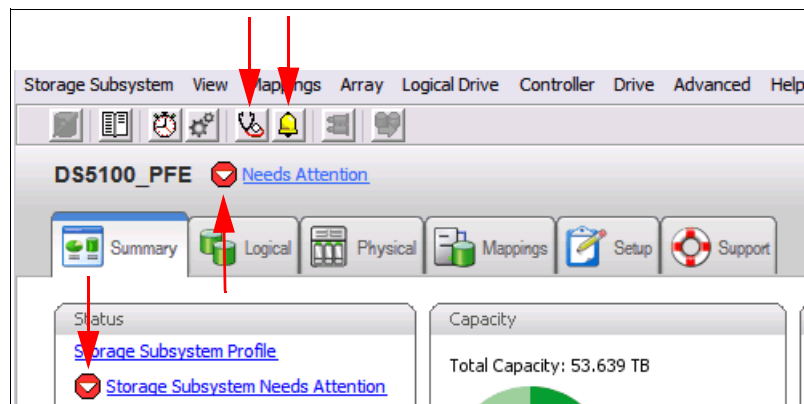


Figure 5-59 Storage Manager Subsystem Management window toolbar buttons

The Recovery Guru and Enclosure Alarm buttons blink when there is an error condition.

5.8.3 Storage subsystem profile

The storage subsystem profile provides a description of all of the components and properties of the storage subsystem. The profile viewer also allows the user to save the storage subsystem profile information to a text file. You might want to use the storage subsystem profile as an aid during recovery or as an overview of the current configuration of the storage subsystem. You might want to save a copy of the storage subsystem profile on the Storage Manager workstation and keep a hard copy with the DS5000 storage subsystem. Create a new copy of the storage subsystem profile if your configuration changes.

To open the storage subsystem profile, perform one of the following actions:

- ▶ Select **Storage Subsystem** → **View** → **Profile**.
- ▶ Select the **Summary** tab, and click **Storage Subsystem Profile** in the Status area.

The profile viewer provides tabs for navigating to a specific section of the profile. The information in the profile includes essential configuration and release code versions that might prove useful in troubleshooting. The storage subsystem profile is included in the Collect all Support Data bundle.

5.8.4 Recovery Guru

The Recovery Guru is a component of the Subsystem Management window (SMW) that diagnoses problems and recommends recovery procedures to fix the problems. When a fault occurs, the user is notified with a flashing Recovery Guru button and the Unit Status changing to “Needs Attention”. By clicking either the “Needs Attention” or **Recovery Guru** button, we are presented with the Recovery Guru window (Figure 5-60) which shows:

- ▶ A summary view listing the faults detected.
- ▶ A detailed view providing an expanded explanation of the fault.
- ▶ A recovery procedure view that suggests some recovery actions.

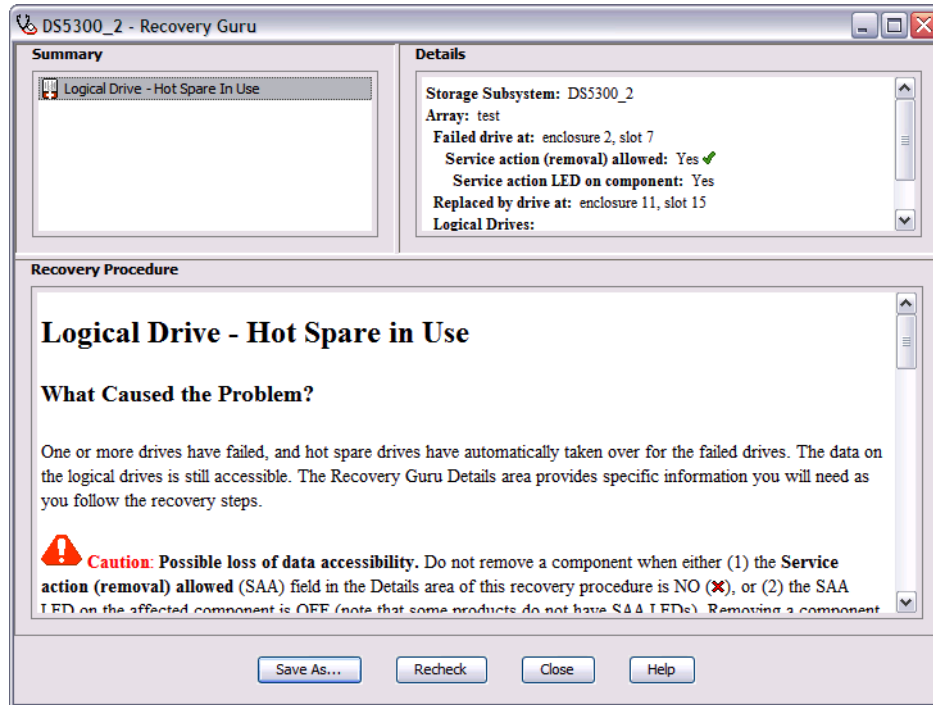


Figure 5-60 Recovery Guru window

In this example, the fault turned out to be a Drive issue. The detailed view shows that the drive 2-7 is failed and removed by hotspare drive 11-15 and that removal is allowed. The recovery procedure view provides a further explanation of the cause and the recommended recovery steps.

It is always advisable to review all the information in Recovery Guru before logging a support call. The Recovery Guru status file is included in the Collect all Support Data bundle.

5.8.5 Major Event Log

The Major Event Log (MEL) is the primary source for troubleshooting a DS5000 storage subsystem. It provides a chronological trace of events logged from both controllers. To access the MEL, select **Advanced** → **Troubleshooting** → **View Event Log**. The MEL is shown in Figure 5-61.

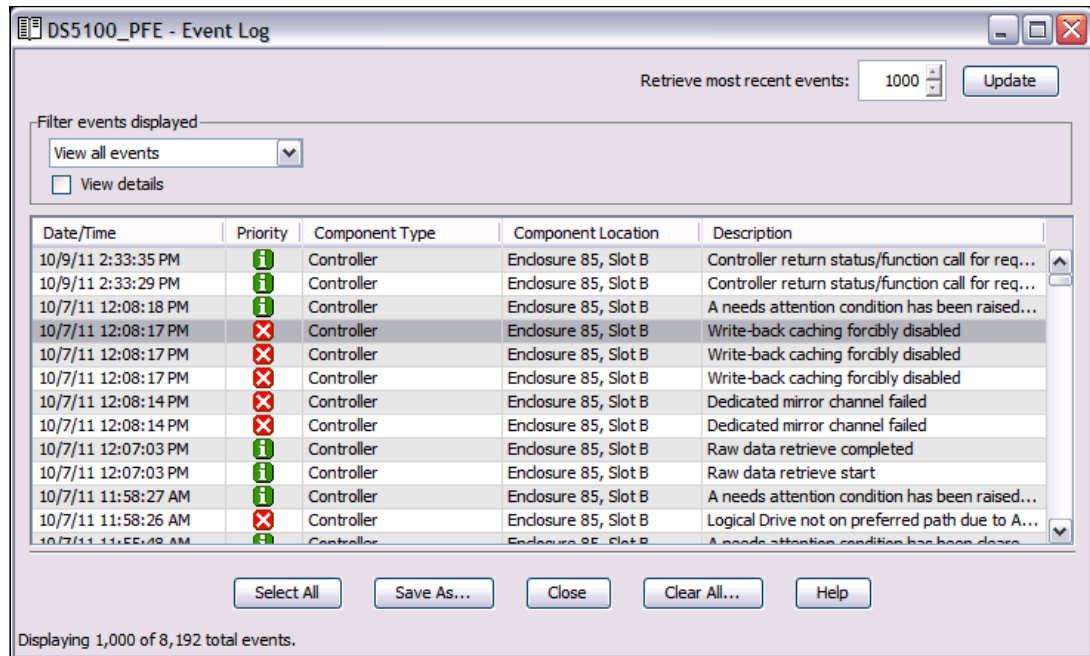


Figure 5-61 Major Event Log viewer

By default, only the 100 most recent critical events are shown, but this can be adjusted. The MEL holds up to 8192 events. It is best practice to capture a Collect all Support Data file as early as possible after an error occurs. Sometimes the error condition might generate a constant stream of events, so a delay could result in the MEL buffer wrapping around making it more difficult to determine the root cause of a fault. Enabling the Automatic Support Data Collection feature will ensure that this is captured whenever a critical event is logged.

There is a Clear All button to delete all the entries in the event log. Once a DS5000 storage subsystem is installed in a live environment, there is no reason to clear the MEL. The log will automatically wrap around when full. There is no benefit to reducing the number of events in MEL. However, clearing the MEL could result in the loss of vital information required in problem determination.

Important: Remember to configure the Event Monitor. An alert will notify you in case of critical events as soon as they occur.

The MEL captures both critical errors and informational messages. Some of the informational messages, such as media scan start / stop events, will not normally be of any assistance during problem determination. The MEL viewer has a check box option for filtering the output:

View only critical events (default option)

For a quick overview of all events that might affect the operational status of your DS5000. This is an effective way of filtering out only the critical events rather than looking through the entire log file.

View all events Detailed information about all events logged by the controller. Sometimes this is useful when determining a time line of configuration changes or looking for marginal errors.

The MEL viewer also has a check box option called View details. When selected, this expands the window into two panes. The bottom pane will display additional data bytes associated with the event highlighted in the top pane. This information is also contained within the Collect all Support Data file, which might be required by the IBM Support representative during problem analysis.

5.8.6 Collect All Support Data option

Use the Collect All Support Data option to gather various types of inventory, status, and performance data that can help troubleshoot any problems with your storage subsystem. All of the files gathered are compressed into a single archive in a zipped-file format. Then, you can forward the archive file to an IBM Support representative for troubleshooting and further analysis. In most cases, this provides sufficient detail to help a hardware defect investigation, although sometimes switch logs, host logs, or cabling diagrams might also be required.

The data gathered in the Collect all Support Data bundle includes:

- ▶ Drive-side cabling connection summary
 - driveCommandAgingTimeout.txt
- ▶ Features list of the storage subsystem
- ▶ Firmware information for the storage subsystem
- ▶ Major Event Log (MEL) information
- ▶ Nonvolatile static random access memory (NVS RAM) data
- ▶ A detailed description of the status of your storage subsystem and its components
- ▶ Performance statistics for the entire storage subsystem
- ▶ Persistent registration and persistent reservation information
- ▶ Read Link Status (RLS) data
- ▶ Current problems and the associated Recovery Guru procedures
- ▶ Recovery profile for the storage subsystem
- ▶ The switch-on-a-chip (SOC) statistics
- ▶ Controller state capture data
- ▶ Storage Subsystem configuration script
- ▶ The storage subsystem profile
- ▶ Trace information useful for debugging
- ▶ Unreadable sectors detected on the storage subsystem

Automatic support data collection

Storage Manager incorporates an option to enable automatic support data collection. When enabled, a support data file is collected and transferred to a specified directory whenever a critical event occurs. This information is not overwritten for at least 72 hours. This allows all information relevant for troubleshooting by your support representative to be preserved.

Tip: We recommend you to enable the Automatic Support Data Collection option in order to have a support data file automatically generated and saved to the specified location when the client monitor process detects a critical event. Make sure that:

- ▶ You specify a directory outside your DS5000 system to collect the information.
- ▶ The Event Monitor process is running on the workstation or host where you indicate to collect the logs.

To enable automatic captures, perform the following steps:

1. Select **Advanced** → **Troubleshooting** → **Support Data** → **Automatic Settings...** as shown in Figure 5-62.

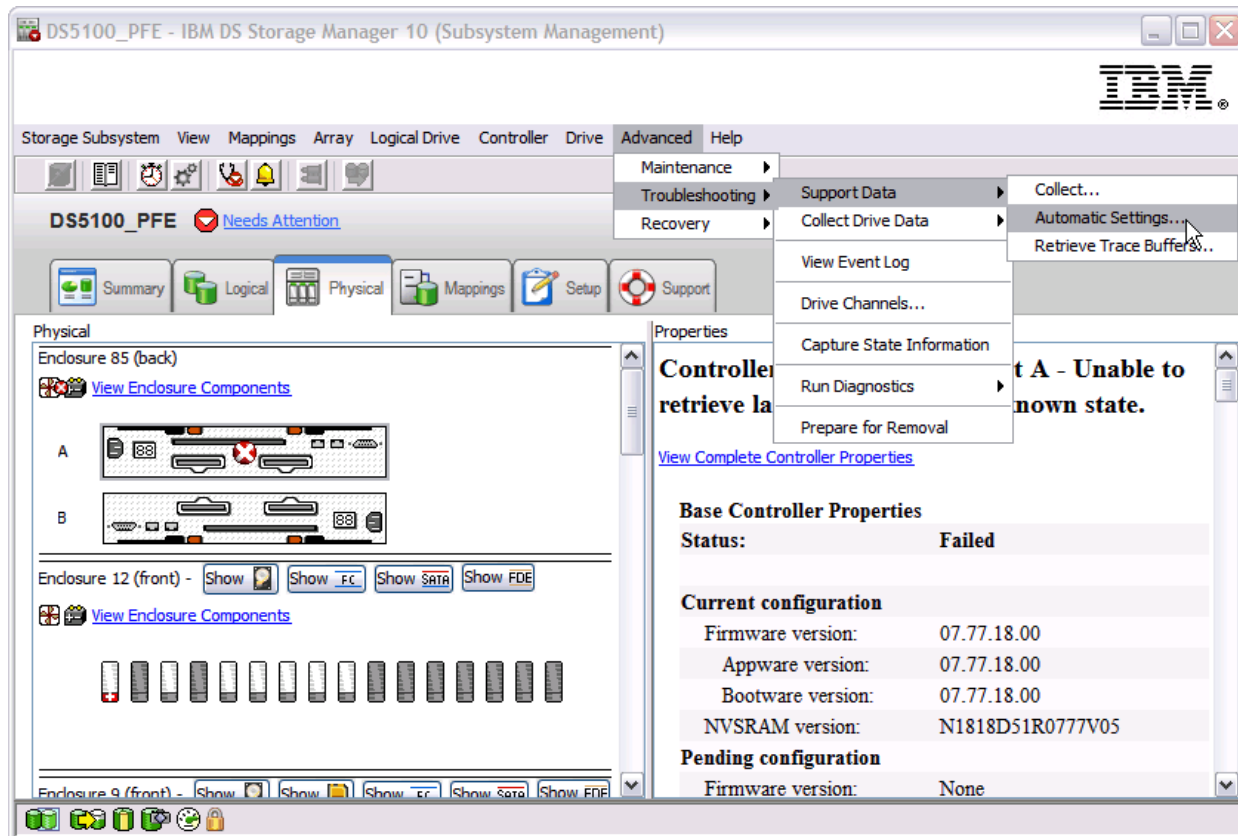


Figure 5-62 Enabling Automatic Data Collection

2. Select the check box to enable the automatic data collection and specify the destination folder, as shown in Figure 5-63.

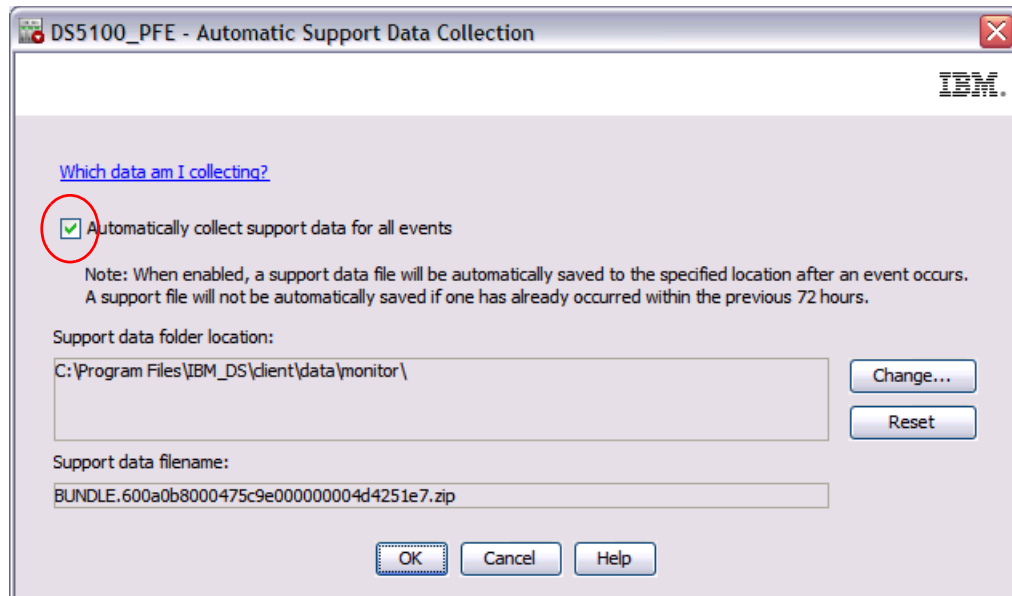


Figure 5-63 Enabling Automatic Data Collection

Running Collect All Support Data from Storage Manager Client

In addition to automatically collecting support data, you can manually generate a new collection at any time from the Storage Manager GUI by performing these steps:

1. Select **Advanced** → **Troubleshooting** → **Support Data** → **Collect...** as shown in Figure 5-64.

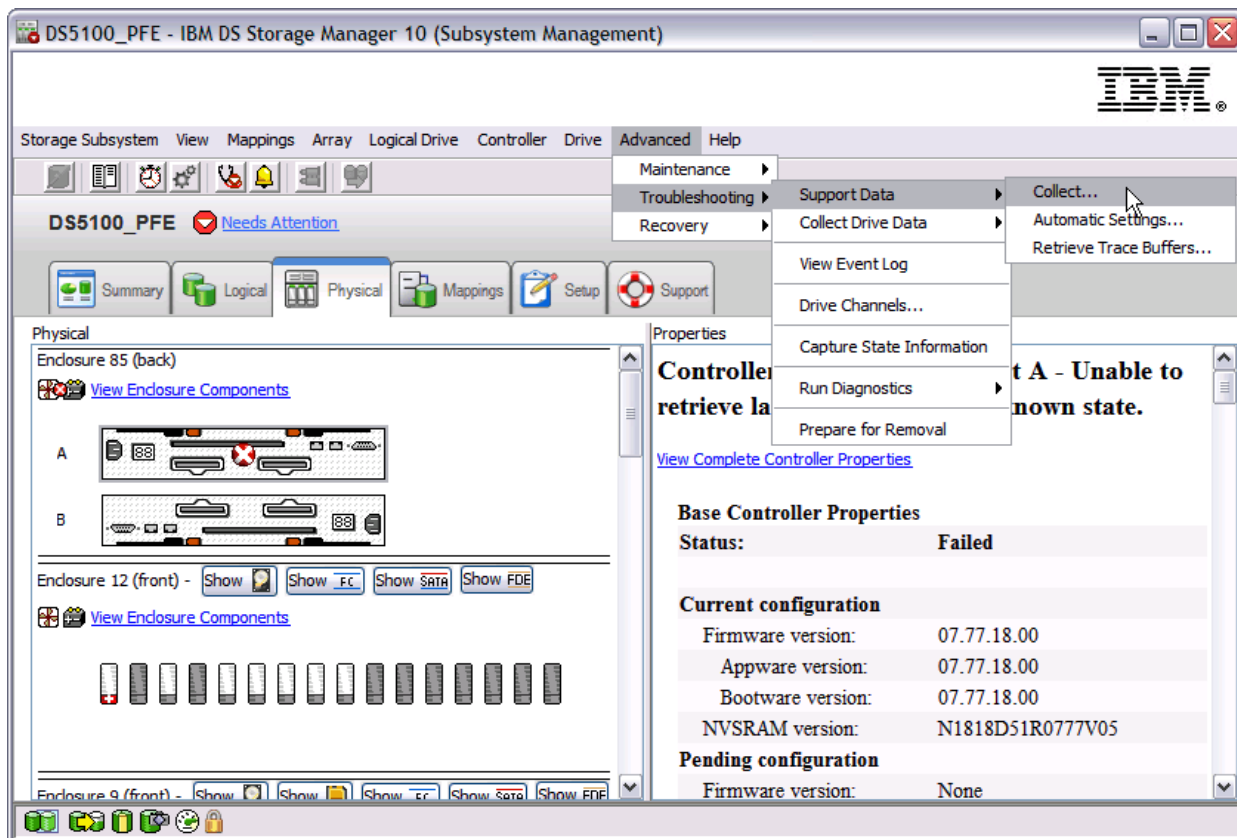


Figure 5-64 Collect All Support Data

2. The Collect All Support Data window (Figure 2-55) opens. Specify the name and location of the zip file that you want to create and then click **Start** to begin the collection.

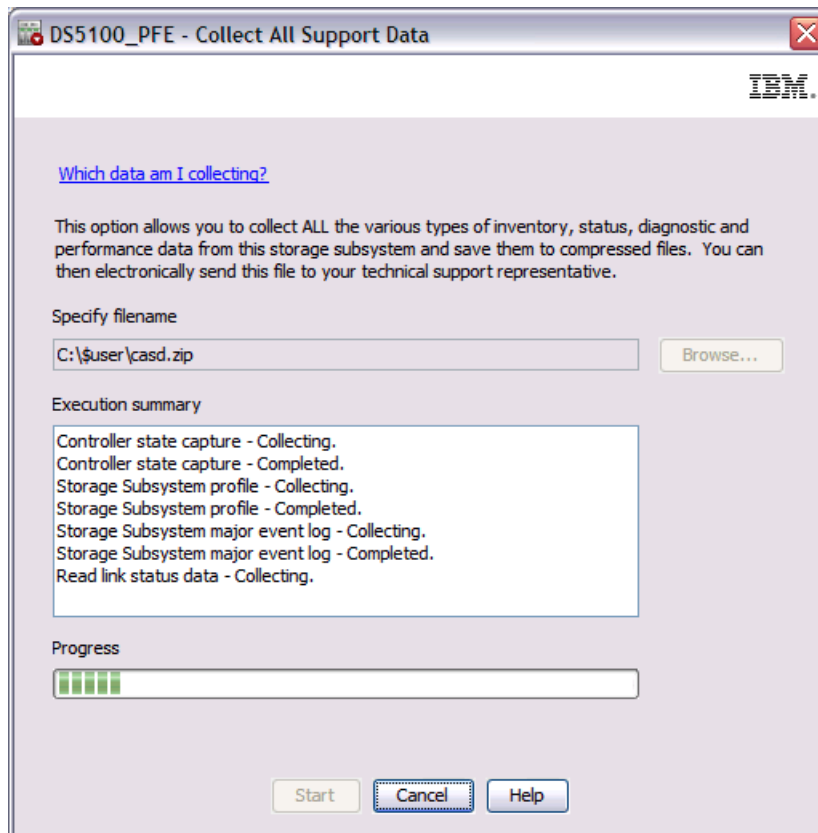


Figure 5-65 Collect All Support Data

A progress bar and execution summary is displayed throughout the data collection period. Click on **OK** when collecting of data is completed as shown in Figure 5-66 on page 367. The compressed file size will typically be around 2-3 MB, depending on the configuration, making it convenient to send to IBM Support as an e-mail attachment.

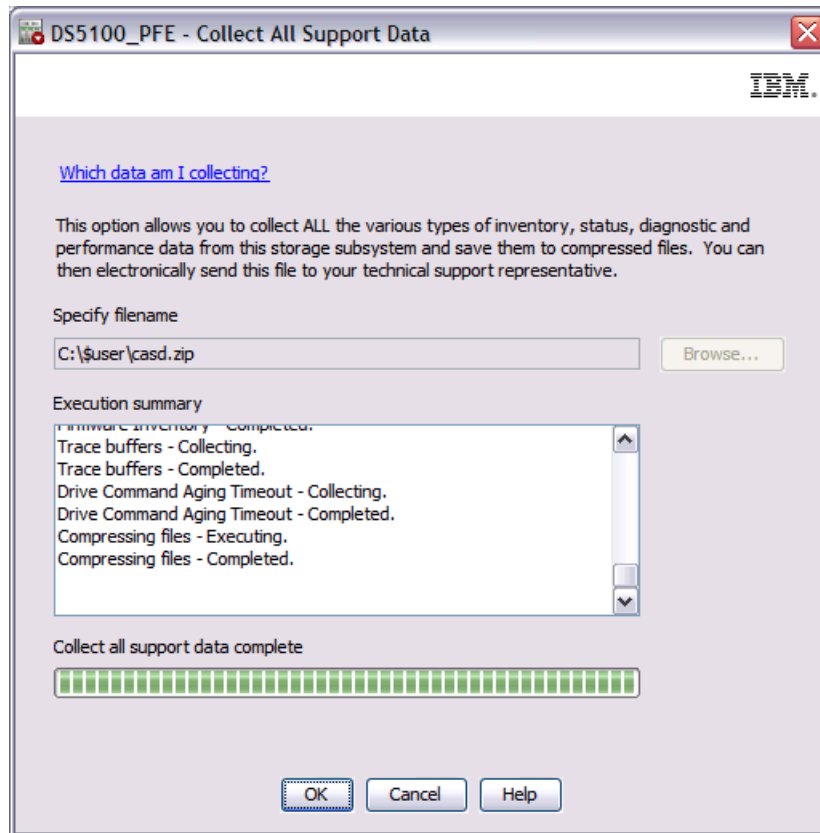


Figure 5-66 Collect All Support Data

Running collect all support data from script editor or SMCLI

There is an alternate way to manually generate the Collect All Support Data bundle through the script editor or SMCLI. The command to run is:

```
save storageSubsystem supportData file="c:\temp\filename.zip";
```

5.8.7 Retrieve trace buffers

The firmware uses the trace buffers to record processing, including exception conditions, that might be useful for debugging.

In some particular cases, it could be requested to retrieve controllers trace by IBM Technical Support representative. You can retrieve trace buffers, without interrupting the operation of the storage subsystem and with minimal effect on performance, from Subsystem Management Window by selecting **Advanced** → **Troubleshooting** → **Support Data** → **Retrieve Trace Buffers...** as shown in Figure 5-67 on page 368

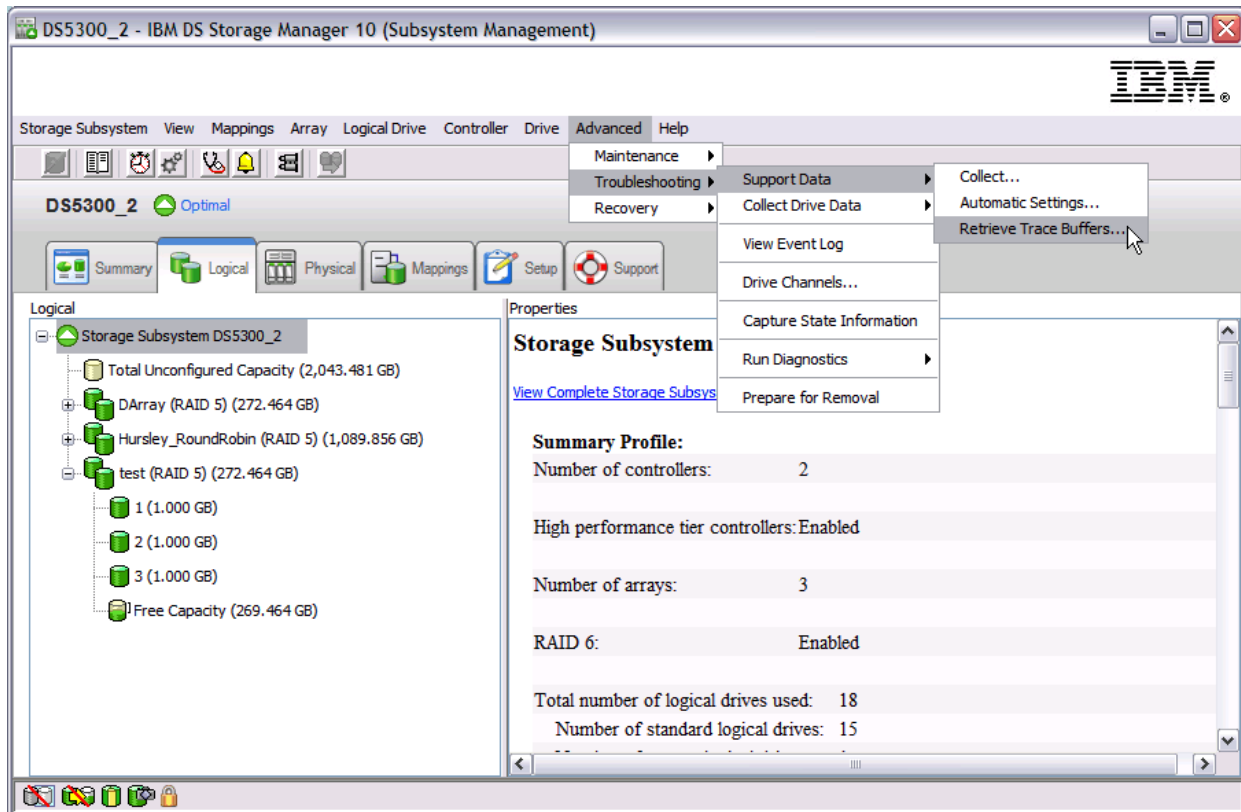


Figure 5-67 Retrieve Trace Buffer

Trace buffer window opens as shown in Figure 5-68 on page 369.

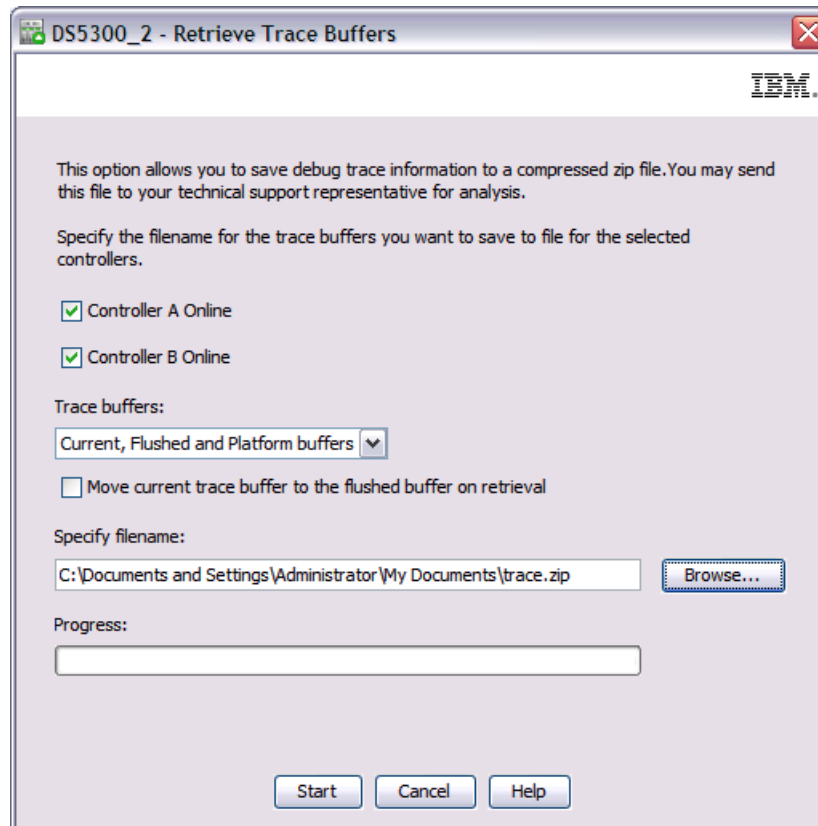


Figure 5-68 Trace buffers window

Select the Controller A and Controller B check boxes. From the Trace Buffers drop-down list, select Current buffer, Flushed buffer, Current and flushed buffers, or Current, flushed, and platform buffers. Enter a name for the file to be saved or browse to if you want to change the default path. Click **Start** to archive the trace buffer information to the specified file. When the retrieval process is finished, click on **Close** button.

Note: If the controller status message to the right of a check box is Failed or Disabled, the check box is disabled.

Trace buffers are also included in All Support Data bundle. You can also retrieve trace buffers through the script editor or SMCLI. The command to run is:

```
start controller [both] trace dataType=all forceFlush=FALSE file="C:\TBTest2.zip";
```

5.8.8 Configuration database validation

SM Version 10.77 adds a new Configuration Database Diagnostic feature.

The configuration database, also called "dacstore", stores information that is used by the storage subsystem to manage the controller firmware. Automatic DB check will be performed before CFW download is started.

To perform the validation manually, select a controller on the Physical Tab, then select **Advanced** → **Troubleshooting** → **Run Diagnostics** → **Configuration Database** as shown in Figure 5-69 on page 370.

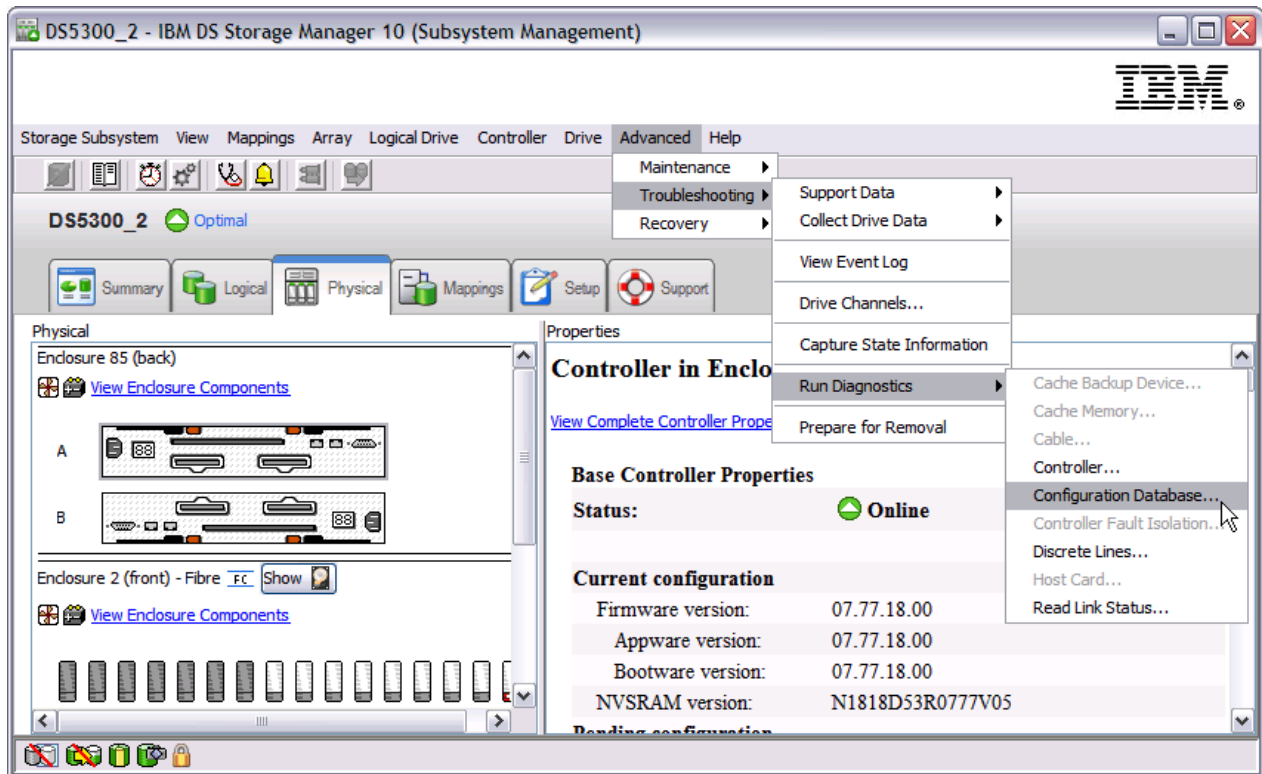


Figure 5-69 Configuration database validation

Configuration Database Diagnostic window opens as shown in Figure 5-70.

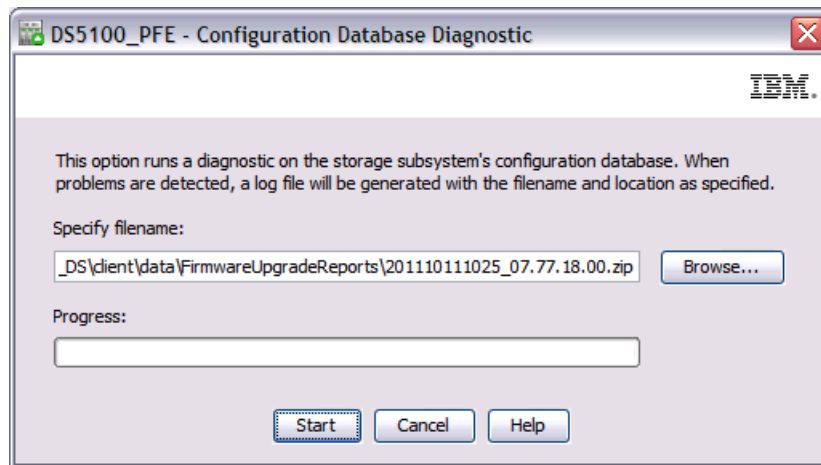


Figure 5-70 Configuration database validation window

Enter a name for the file to be saved or browse to if you want to change path and click on **Start** button. When validation process is finished, click on **OK** to close.

If validation fails, a zip file is created containing a text file with a description of the error and a Diagnostic file for troubleshooting.

5.8.9 Database save/restore

This procedure and functionality is intended to be used in recovering systems that have lost their configuration or their configuration was required to be removed in order to recover from failure. Restoring the configuration using this functionality will restore portions of the database containing the volume configuration, volume WWNs, controller WWNs, Premium Features and mappings. It will not restore other areas such as the MEL.

Note: The Storage Subsystem must be accessible through Storage Manager before starting this procedure. All drives also need to be inserted into the system at this time.

Warning: If there is an active database on the Storage Subsystem, this will be deleted during this process.

Save database configuration

Storage Monitor Service automatically saves the configuration DB from subsystem a in ...\\client\\data\\monitor\\dbcapture folder.

All captured DB files are zipped and named as RetrievedRecords_SSID_Date_Time.dbm.zip. Following an example of DB configuration file:

RetrievedRecords_60080e500017b8de000000004be47b12_2011_9_20_14_48_27.dbm.zip

CLI can be used to save a DB manually by using command

```
save storageSubsystem dbmDatabase file="C:\\path\\filename.zip";
```

Restore database configuration

A “Valedictory String” is needed to restore the configuration DB. Validator is obtained from IBM Support by sending the config DB zip file and the system profile.

The restore is done using CLI command:

```
load storageSubsystem dbmDatabase file="<configuration_DB_file>"  
validator="<validator_string>;
```

5.8.10 Media Scan

Media Scan is a background process that runs on all logical drives in the storage subsystem for which it has been enabled. A media scan provides error detection on the drive media. The Media Scan process scans all logical drive data to verify that it can be accessed. This is enabled by default when creating a new logical drive. There is also an option to scan the logical drive redundancy data during the Media Scan cycle.

To modify the Media Scan settings, you need to be in the logical view in the Storage Manager Subsystem Management window. Then either right-click a logical drive or select **Logical Drive** → **Change** → **Media Scan Settings...** to bring up the Change Media Scan Settings window shown in Figure 5-71.

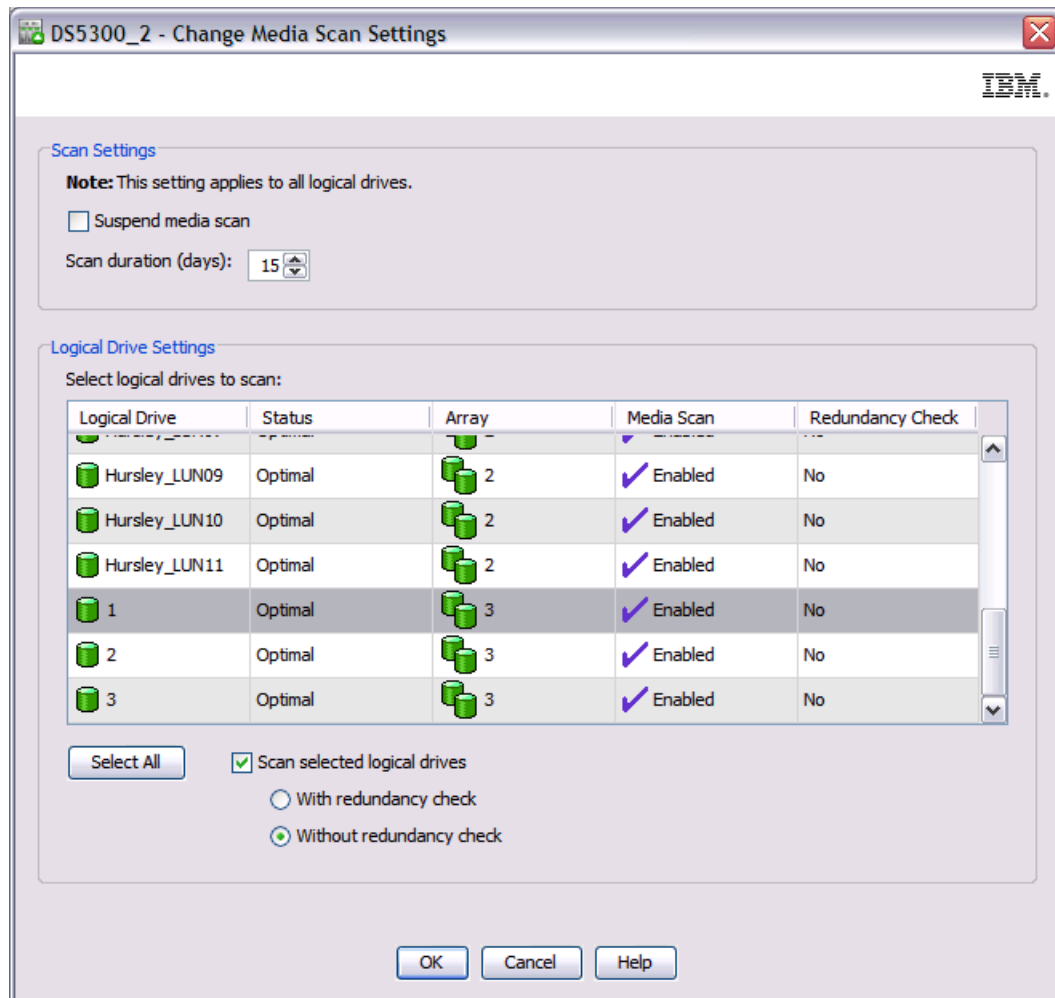


Figure 5-71 Media Scan settings

The options displayed at the top, Suspend media scan and Scan duration (days), are global settings. The logical drive settings at the bottom of the window apply to individual logical drives, although there is an option to set all logical drives identically by clicking the **Select All** button.

To specify the duration (in days) of the media scan, select a number in the Scan duration (days) box. The media scan duration specifies the number of days over which the media scan can run on the eligible logical drives. The controller uses the duration period, with its knowledge of which logical drives must be scanned, to determine a constant rate at which to perform media scan activities. This rate is maintained regardless of host I/O activity. Choosing a higher value for the duration will result in the media scan running for a longer period as a lower priority task.

A redundancy check scans the blocks in a RAID 3, 5, or 6 logical drive and checks the redundancy information for each block. A redundancy check compares data blocks on RAID 1 mirrored disk drives. RAID 0 logical drives have no data redundancy. There might be a performance impact when redundancy check is enabled.

5.8.11 Pre-read redundancy check

The pre-read redundancy check verifies the redundancy information during every read I/O. A logical drive that has this feature enabled returns read errors if the data is determined to be inconsistent by the controller. You can enable this option for logical drives that contain redundancy information, that is, RAID 1, 3, 5, and 6. However, there is a severe performance impact with this feature enabled, so it is only enabled in exceptional cases.

To modify the Pre-read redundancy settings, you need to be in the logical view in the Storage Manager Subsystem Management window. Then either right-click a logical drive or select **Logical Drive** → **Change** → **Pre-read Redundancy Check...** to bring up the Pre-read redundancy settings window as shown in Figure 5-72.

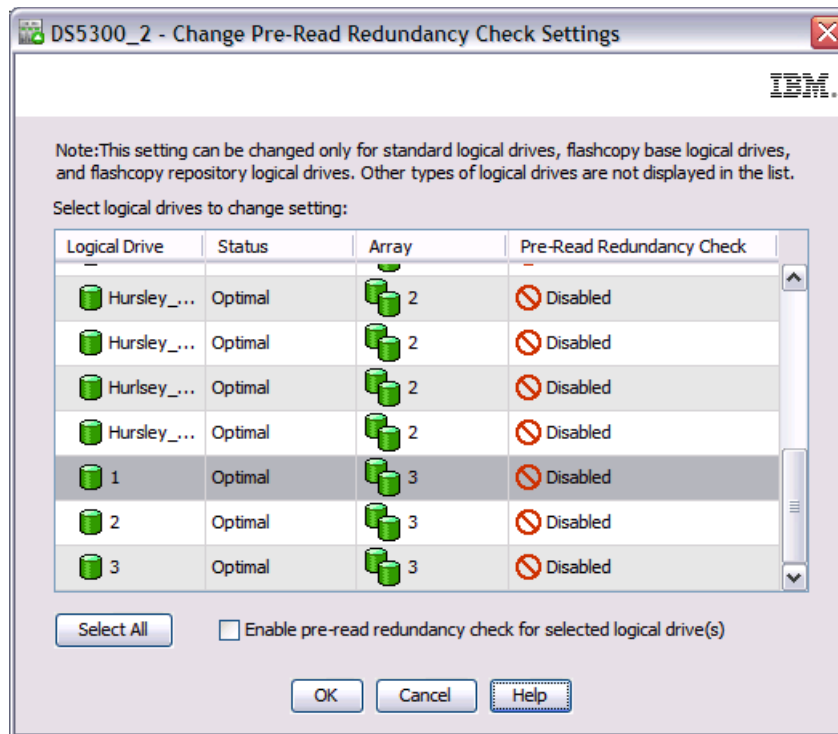


Figure 5-72 Pre-read redundancy settings

Note: Enabling the option on logical drives without redundancy does not affect the logical drive.

5.9 Problem determination

In this section, we explore some of the tools and methods used to diagnose:

- ▶ Drive-side problems
- ▶ Host-side problems
- ▶ Storage Manager communication problems

We only include techniques for determining faults using the Storage Manager Client and SMCli interface. Additional tools are available through the controller shell, although these are outside the scope of this book. A password is required for accessing the shell through either

the serial port or a telnet session. It is only intended to be used by the IBM Support representative during problem determination.

However, there is a Capture State Information option in Storage Manager (also included within the Collect all Support Data bundle) that collects shell data from both controllers in the DS5000 storage subsystem. We will explore some of the included commands that might be relevant to fault finding.

With any suspected fault, it is essential to first rule out the possibility of a code mismatch or configuration error. This is particularly important when fault symptoms are detected following an installation or upgrade. Check that all prerequisites and configuration rules are adhered to before logging a hardware support call.

In many cases, Recovery Guru will assist in identifying cabling configuration errors with an explanation of the fault together with advice on correcting it, for example:

Channel miswired Two or more drive channels are connected to the same Fibre Channel loop. The Recovery Guru Details area provides specific information that you will need as you follow the recovery steps.

Drive enclosures not cabled correctly

There are drive enclosures in the storage subsystem that are not cabled correctly because they have ESM canisters that must be cabled sequentially together. The Recovery Guru Details area provides specific information that you will need as you follow the recovery steps.

For limitations and version specific requirements, see the readme documents associated with the current code files, which can be found at the following address:

<http://www.ibm.com/support/entry/portal/>

For details of tested and supported configurations, see the System Storage Interoperation Center at the following address:

<http://www.ibm.com/systems/support/storage/ssic/interoperability.wss>

For cabling and configuration rules, see the following documents:

- ▶ *Installation, User's, and Maintenance Guide - IBM System Storage DS5100 and DS5300 - GA32-0955 (MIGR-5084430).*
- ▶ *Installation and Host Support Guide for DS Storage Manager v10 - GA32-0963 (MIGR-5075652).*
- ▶ *Installation and Migration Guide for Hard Drive and Storage Expansion Enclosure - GA32-0962 (MIGR-57818)*

5.9.1 Diagnosing drive-side problems

In order to accurately diagnose drive-side problems, it is important to understand how the DS5000 storage subsystems work on backend side. Although the communication protocol is fundamentally unchanged in that, they all use the Fibre Channel protocol for communication between the controllers and the back-end drives, the way it is implemented is different.

Unlike the earlier models which used arbitrated loop (ALPA) technology, the DS5000 storage subsystems and expansion enclosures include a switch-on-chip (SOC) built in to each ESM and controller. This allows the Fibre Channel frames to be passed between the controllers and ESM and then forwarded directly to the destination disk device via a point-to-point link.

This improves performance, adds error diagnostic capability at the SOC, and eliminates the risk of a single drive disrupting the loop by causing downstream devices to fail.

Figure 5-73 illustrates the drive-side connections for one redundant channel pair in a 16 enclosure configuration. On the DS5300, each drive channel is associated with two ports. There are four drive channels and eight associated ports per controller. One channel from each controller combines to form a *redundant drive channel pair*.

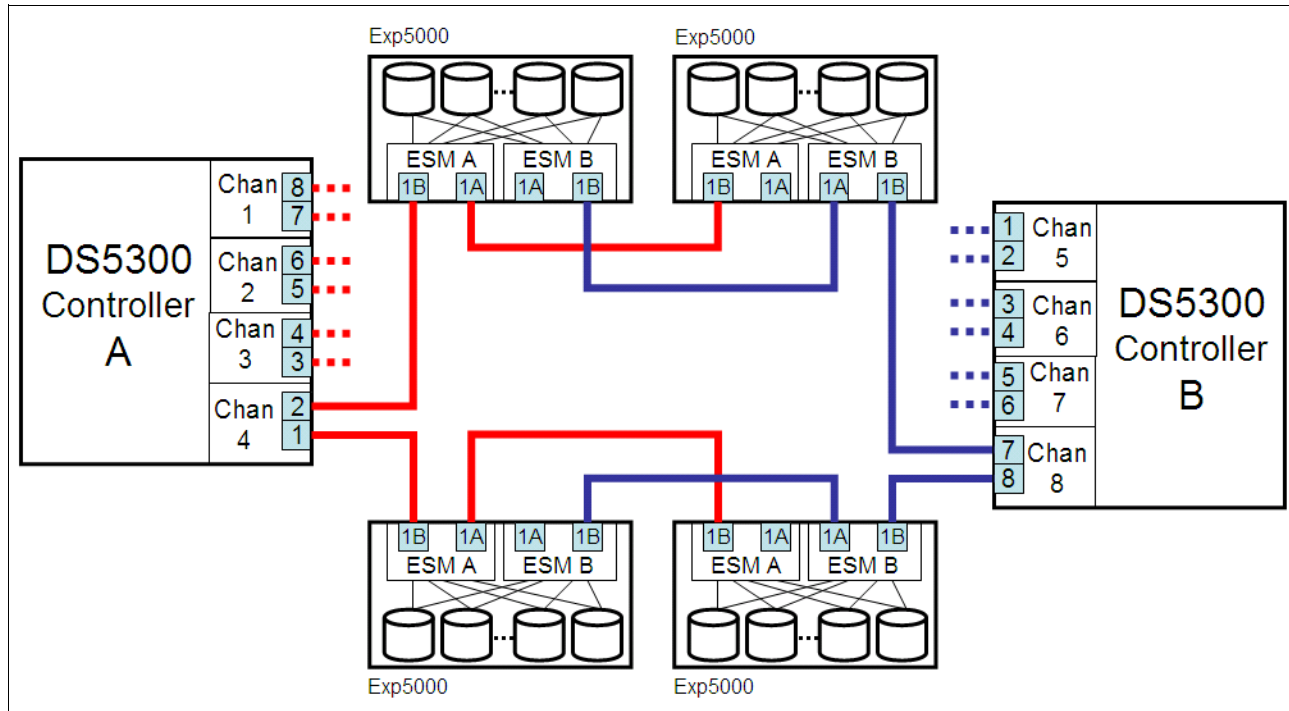


Figure 5-73 Drive-side connections

Degraded drive channel

The controller automatically fails a disk or ESM whenever an error threshold is exceeded. However, if there are excessive errors detected on a drive channel, then the controller will mark the channel as *degraded*. In this state, the channel is still available, but all I/Os are routed via the alternate channel in the redundant channel pair until the problem is identified and resolved. This is where we need to use available tools to determine which storage subsystem (enclosure) or component (cable, SFP, or ESM) on the channel is causing the excessive errors.

The main tools for diagnosing drive-side problems include:

- ▶ View Connections
- ▶ Storage Subsystem Profile
- ▶ Major Event Log (MEL)
- ▶ Read Link Status Diagnostics
- ▶ SOC Statistics
- ▶ Capture State Information

View Connections

Before starting any analysis of drive-side channel problems, it is essential to have a clear understanding of the cabling topology. By selecting **Storage Subsystem** → **View** → **Connections** from the Storage Manager Subsystem Management window, we are presented with a list of drive-side cable connections, as shown in Figure 5-74. This can be used to compile a topology diagram.

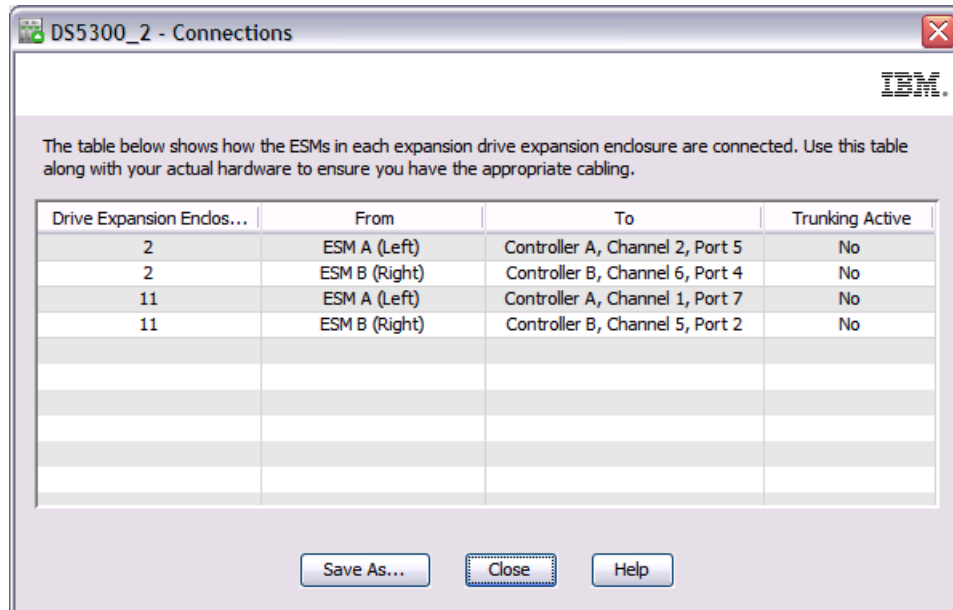


Figure 5-74 View Connections window

Storage Subsystem Profile

The Storage Subsystem Profile (Example 5-8) includes a section on drive channels. This provides a useful summary of status together with cumulative errors accumulated on each drive channel since the last controller reset (or since the counters were cleared).

Example 5-8 Storage Subsystem Profile

SUMMARY						
	CHANNEL	PORT	STATUS	CTRL A LINK	CTRL B LINK	TRUNKING
1	8,7,ESM A 1B	Optimal	Up	Up	No	
2	6,5,ESM A 1B	Optimal	Up	Up	No	
3	4,3	Optimal	Up	Up	No	
4	2,1	Optimal	Up	Up	No	
5	1,2,ESM B 1B	Optimal	Up	Up	No	
6	3,4,ESM B 1B	Optimal	Up	Up	No	
7	5,6	Optimal	Up	Up	No	
8	7,8	Optimal	Up	Up	No	

DETAILS

DRIVE CHANNEL 1

Port: 8, 7, ESM A 1B
 Status: Optimal
 Max. Rate: 4 Gbps
 Current Rate: 4 Gbps
 Rate Control: Auto
 Controller A link status: Up
 Controller B link status: Up
 Trunking active: No

DRIVE COUNTS

Total # of attached drives: 16
 Connected to: Controller A, Port 7
 Attached drives: 16
 Drive expansion enclosure: 11 (16 drives)

CUMULATIVE ERROR COUNTS**Controller A**

Baseline time set: 10/7/11 1:55:25 PM
 Sample period (days, hh:mm:ss): 2 days, 23:52:24
 Controller detected errors: 7
 Drive detected errors: 60
 Timeout errors: 0
 Link down errors: N/A
 Total I/O count: 163290

Controller B

Baseline time set: 10/7/11 1:54:10 PM
 Sample period (days, hh:mm:ss): 2 days, 23:53:41
 Controller detected errors: 0
 Drive detected errors: 94
 Timeout errors: 0
 Link down errors: N/A
 Total I/O count: 177377

The same information is available in the Storage Manager Subsystem Management window by selecting **Advanced** → **Troubleshooting** → **Drive Channels...**, as shown in Figure 5-75.

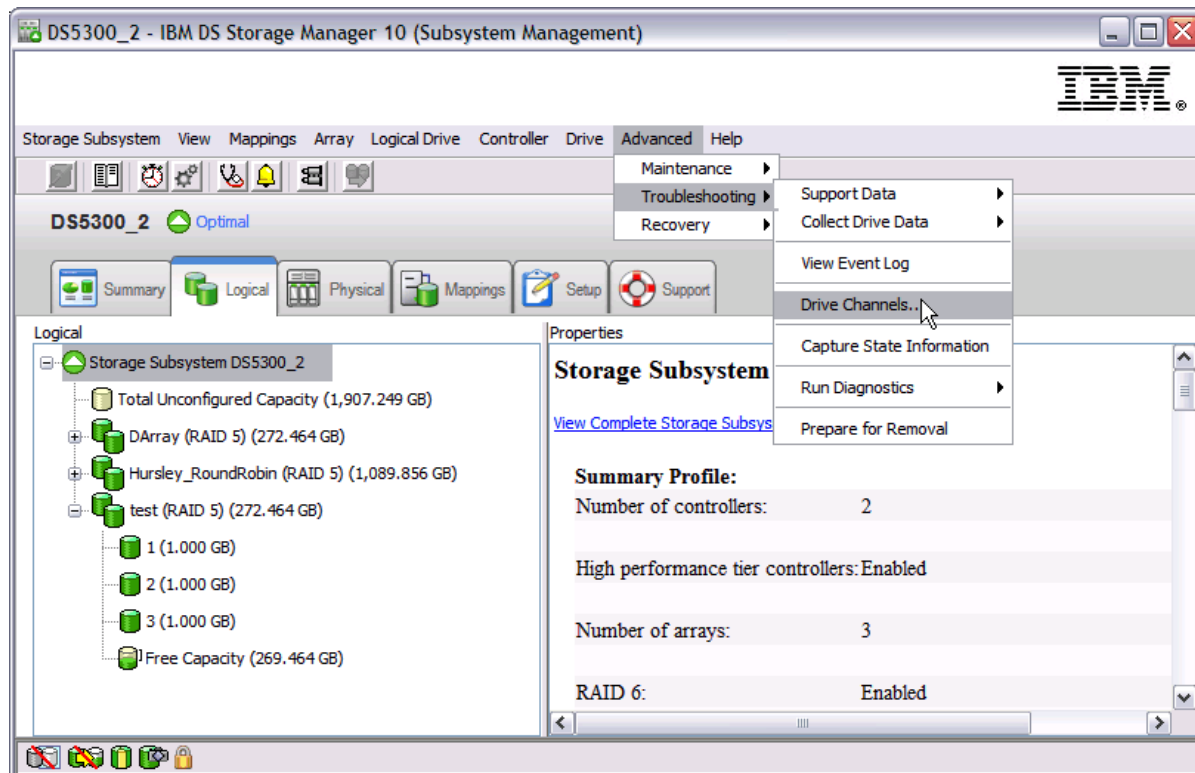


Figure 5-75 Drive Channels window

The Drive channels summary window is opened, as shown on Figure 5-76.

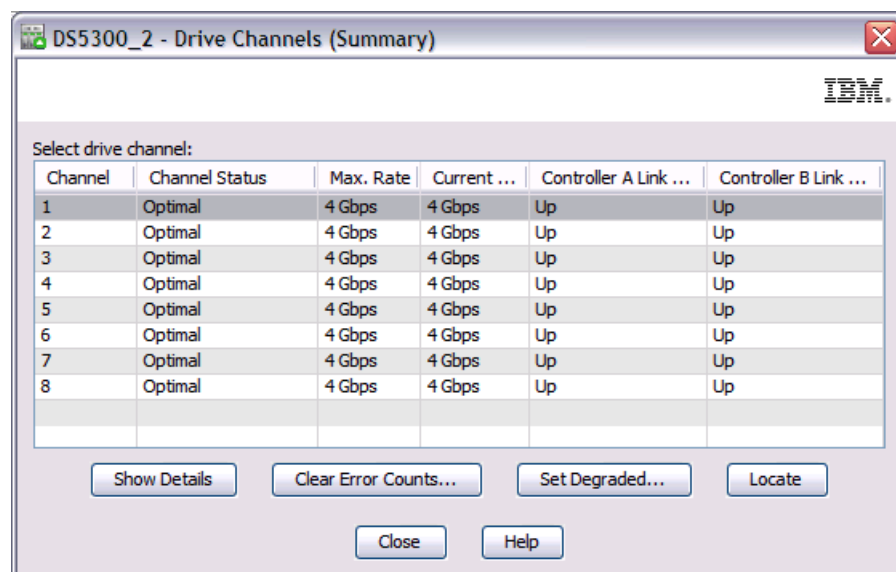


Figure 5-76 Drive channels (Summary)

Highlight the drive channel you want to check and click the **Show Details** button to get more details like the cumulative error statistics as shown on Figure 5-77 on page 379.

There is also an option to toggle the drive channel state between Optimal and Degraded. This action is not necessary, as the channel automatically returns to an Optimal state when the problem device is identified and excluded.

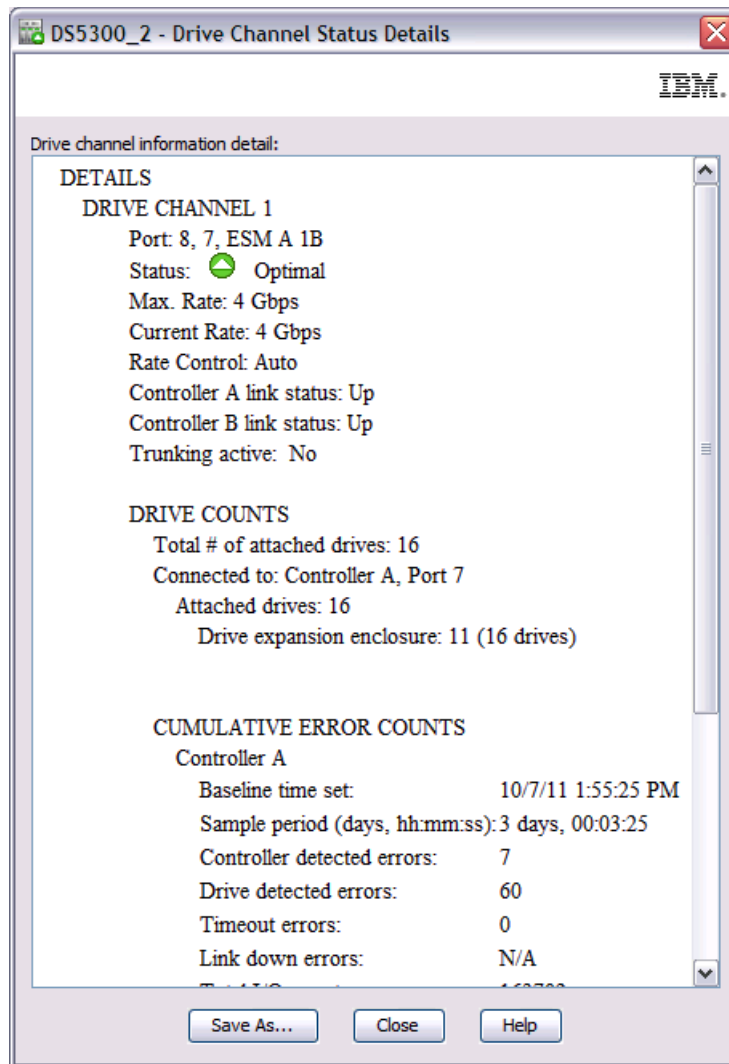


Figure 5-77 Drive Channel Status Details

The Clear Error Counters option can be used to reset the counters. A sampling time of around 24 hours is normally sufficient to show any errors on a degraded drive-side loop. In some cases, the pattern of errors will begin to emerge within minutes of resetting the counters. If the counters have not been reset for an extended period, then the values might be historic rather than reflecting the current status.

Major Event Log (MEL)

The MEL is always likely to hold some clues to drive-side problems. Quite often, we see events logged against a faulty disk well before the error threshold is exceeded to mark it as failed. If there is a pattern of repeated errors against a single device, then it is worth removing it as a first step in diagnosing a degraded channel problem. It is also worth checking when the errors first started, as this might point to some other activity that was in progress at the time. Select View All Events while debugging drive problems. This let us view the sequence of all events and help us to figure out the cause of issue.

Read Link Status Diagnostics

The Read Link Status error counts refer to link errors that have been detected in the traffic flow of a Fibre Channel drive-side loop. The Read Link Status Diagnostics dialog retrieves the error counts and shows the controllers, disk drives, ESMs, and Fibre Channel ports in channel order.

By analyzing the error counts retrieved, you can determine the components on a drive-side channel that might be experiencing problems communicating with the storage subsystems on the loop. A high error count for a particular component might indicate that it is experiencing problems and should be given immediate attention.

To run Read Link Status Diagnostics, select **Advanced** → **Troubleshooting** → **Run Diagnostics** → **Read Link Status...** as shown in Figure 5-78

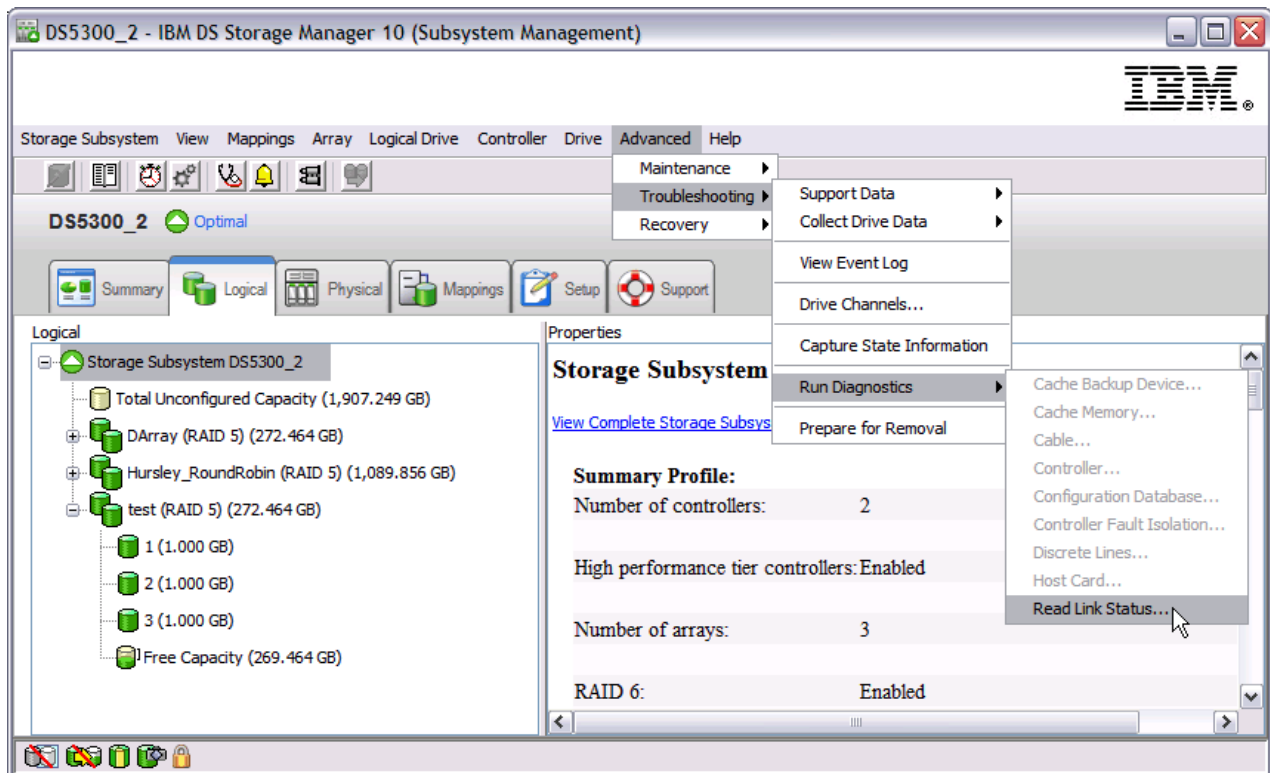


Figure 5-78 Read Link Status Diagnostics

The Read Link Status Diagnostics window will appear, as shown in Figure 5-79 on page 381.

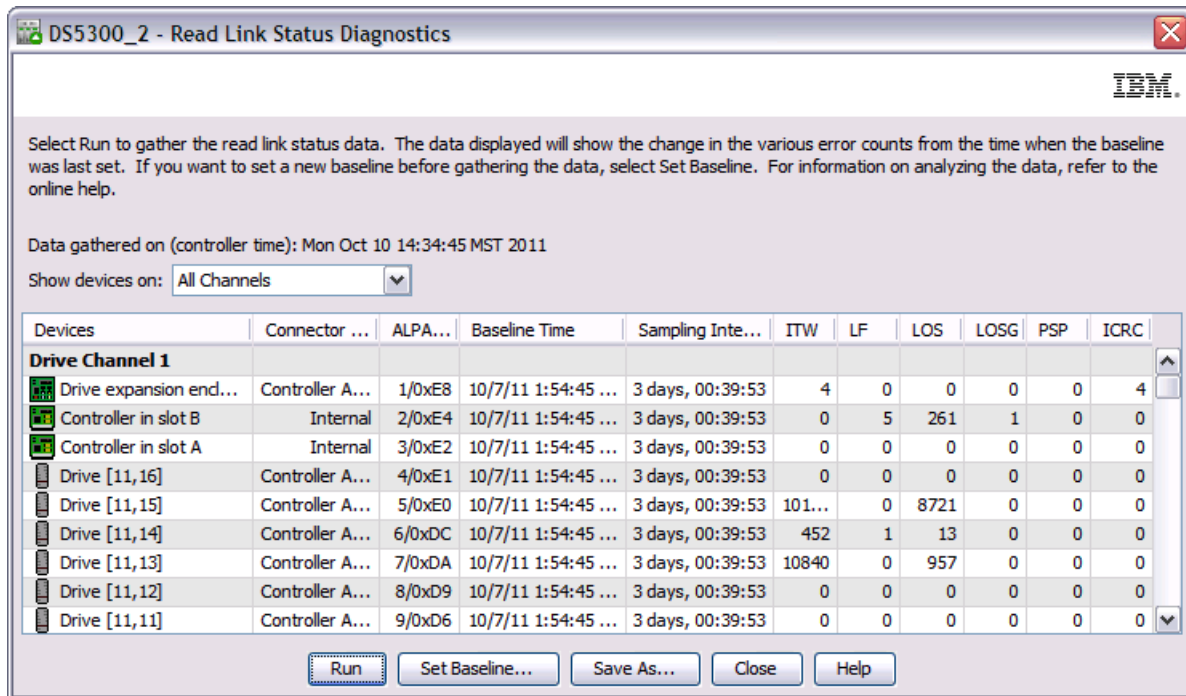


Figure 5-79 Read Link Status Diagnostics window

Error counts are calculated from a baseline. The baseline can be manually reset by pressing the **Set Baseline** button.

The columns displayed in the Read Link Status Diagnostics output are:

Devices	A list of all of the storage subsystems on the Fibre Channel loop. The storage subsystems appear in channel order, and within each channel they are sorted according to the storage subsystem's position within the loop.
Controller/Port	The controller ID or the port ID of the device.
ALPA ID	The arbitrated loop physical address of the device.
Baseline Time	The date and time of when the baseline was last set.
Sampling Interval	The elapsed time between when the baseline time was set and when the read link status data was gathered using the Run option.
ITW	The total number of invalid transmission word (ITW) errors detected on the Fibre Channel loop from the baseline time to the current date and time. ITW might be referred to as the "Received Bad Character Count."
LF	The total number of link failure (LF) errors detected on the Fibre Channel loop from the baseline time to the current date and time.
LOS	The total number of loss of synchronization (LOS) errors detected on the Fibre Channel loop from the baseline time to the current date and time.
LOGS	The total number of loss of signal (LOGS) errors detected on the Fibre Channel loop from the baseline time to the current date and time.
PSP	The total number of primitive sequence protocol (PSP) errors detected on the Fibre Channel loop from the baseline time to the current date and time.

ICRC The total number of invalid cyclic redundancy check (ICRC) errors detected on the Fibre Channel loop from the baseline time to the current date and time.

A sampling time of around 24 hours is normally sufficient to show any errors on a degraded drive-side loop. In some cases, the pattern of errors will begin to emerge within minutes of resetting the baseline. If the baseline has not been reset for an extended period, then the values might be historic rather than reflecting the current status.

ITW is the key error count to be used when analyzing the error count data. In a switched (SOC) ESM environment, a high ITW error count is likely to indicate a problem on the associated device.

The Read Link Status file can be saved as a comma separated file. It is included within the Collect all Support Data bundle.

SOC Statistics File (socStatistics.csv)

While RLSD error statistics are measured at the Fibre Channel port on the actual device, that is, the controller port, ESM port or disk, the SOC statistics are measured by the Switch-on-Chip (SOC) chip. Therefore, interpreting the differences between the two sets of output can be vital to accurately determine the root cause of a degraded drive-side channel.

The SOC statistics file can be generated with the following script command:

```
save storageSubsystem SOCCounts file="c:\socStatistics.csv";
```

It is also included within the Collect all Support Data bundle.

The columns displayed in the socStatistics file include:

OPM	This is the Operating Port Mode (OPM). Valid states include non-cascade, tree, or string.
PS	The state of the port (PS). Valid values could be inserted, loopback, unknown, or various bypassed states.
PIC	Port Insertion Count (PIC) is the number of times the device has been inserted into this port.
LS	Loop State (LS) is the condition of the loop between the SOC and component. Possible states include up, down, or various transition states.
LUC	Loop Up Count (LUC) is the number of times the loop has changed from Down to Up.
CRCEC	CRC Error Count (CRCEC) is the number of Cyclic Redundancy Check errors that are detected in frames.
RFDEA	Relative Frequency Drift Error Average (RFDEA) is the difference between the port-received data rate and the internal clock of the SOC. A value in the 1,000s indicates a problem device.
LCC	Loop Cycle Count (LCC) is the number of LIPs seen by the reference port.
OSEC	Ordered Set Error Count (OSEC) is the number of invalid FC transmit words seen at the receiver of the port.
PCAC	Port Connections Attempted Count (PCAC) is the number of times the port attempted to make a connection due to ARB connection requests.

PCHOC

Port Connections Held Off Count (PCHOC) is the number of times the port attempted to make a connection but it was held off by a busy port.

PUP

Port Utilization Percentage (PUP) is the percentage of time that frames are seen on the port, or percentage of time that a port is used if in switching mode.

A sampling time of around 24 hours is normally sufficient to show any errors on a degraded drive-side loop. In some cases, the pattern of errors will begin to emerge within minutes of resetting of SOS statistics. If the SOC statistics have not been reset for an extended period, then the values might be historic rather than reflecting the current status.

The SOC statistics can be reset with the following script command:

```
reset storageSubsystem SOCBaseline;
```

During loop initialization (LIP), the SOC chips temporarily change to hub mode to allow all devices to see each other in an environment resembling a simple arbitrated loop topology. This skews some of the error statistics. Therefore, they can only be treated as reliable after a period of normal activity when no devices have been added, removed, or changed on the drive-side channels.

Capture State Information

This is a collection of shell commands executed on each controller. It can be started from the Storage Manager Subsystem Management window by selecting **Advanced** → **Troubleshooting** → **Capture State Information** as shown in Figure 5-80.

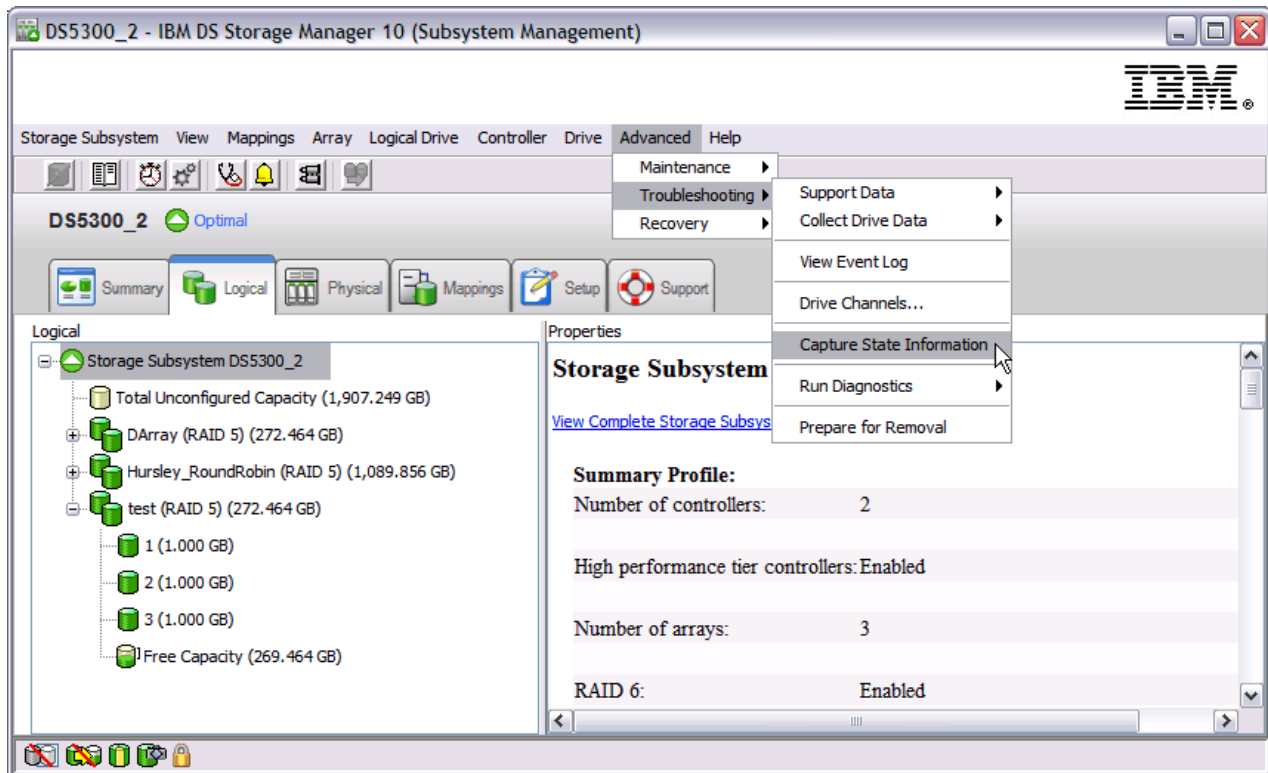


Figure 5-80 Capture state information

The state capture window appears as shown in Figure 5-81 on page 384.

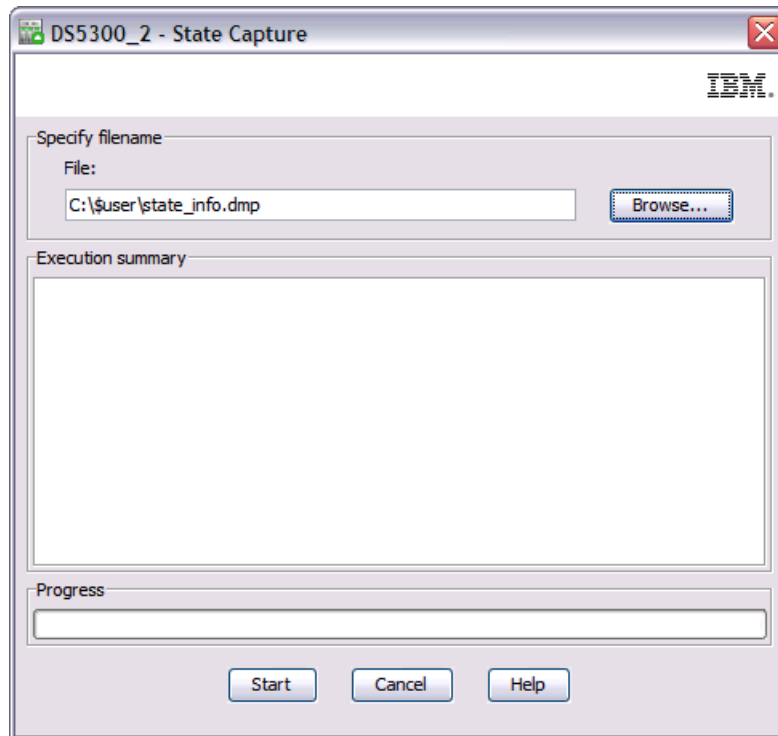


Figure 5-81 State capture information window

Specify the name and location of the dmp file that you want to create and then click Start button. Type Yes and click OK on confirmation window to begin collection. A progress bar and execution summary is displayed throughout the data collection period as shown in Figure 5-82. Click on OK when collecting of data is completed.

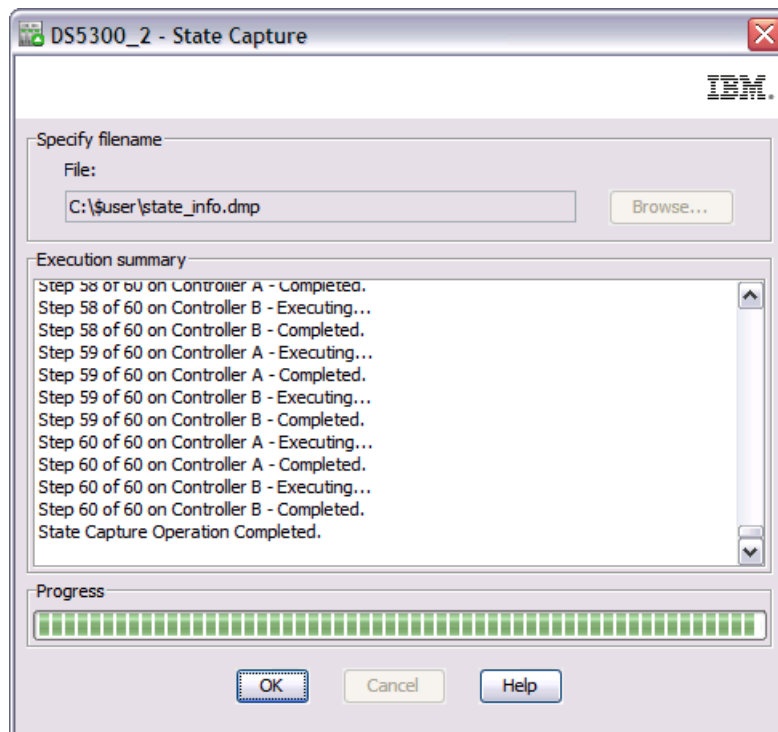


Figure 5-82 State capture information window

A large uncompressed text file is generated with a .dmp file name suffix.

This file is also included in the Collect all Support Data bundle.

Each command appears twice within the Capture State Information file, once on each controller. Each command is shown on a separate line with the following syntax:

Executing <command> on controller <A or B>

The file includes a few commands that might be useful for investigating drive-side problems:

fcDump	An incrementing number of fc exchange errors suggests that there is a problematic device on the loop. This is often a quick and easy check that can be carried out after excluding a suspect device from the loop.
chAll	Similar output to fcDump, just in a slightly different format.
luAll	This command provides a summary of logical unit information. For our purposes, the important information is in the ORP and Channels columns. ORP represents Operation, Redundancy and Performance. These normally are +++ for all disk devices. The Channels column displays a + for the preferred path to the device and * for the alternate path.
showEnclosuresPage81	This provides data similar to the SOC statistics file with a few additional items.

Clearing all error counters

We have already mentioned that there are options in Storage Manager to reset RLSD baseline, SOC statistics and clear drive channel error counters. Another way is to reset all of these with a simple script that can be executed from the Storage Manager Enterprise Management window (select **Tools** → **Execute Script** to open this window):

```
//Clear Drive Channel Statistics
clear allDriveChannels stats;
//
//Reset Storage Subsystem SOC Baseline
reset storageSubsystem SOCBaseline;
//
//Reset RLS baseline
reset storageSubsystem RLSBaseline;
```

The IBM Support representative handling your case might request that this script be run and that a new Collect all Support Data file be captured the next day.

Multiple drive failures

We highly recommend logging an call whenever multiple drives fail simultaneously. Sometimes, the root cause is clearly understood and we can be reasonably confident that there are no underlying hardware defects. For example, if there was an unexpected loss of power to an expansion enclosure, then this could result in multiple disks remaining in a failed state. Those arrays that only lost RAID redundancy will remain online, but in a degraded state, and reconstruction or copyback will start automatically when power is restored to the enclosure. This can be observed in the Storage Manager Subsystem Management window physical view. The missing drives first re-appear in a replaced state. The associated logical drives return to an optimal state when reconstruction is complete without any intervention.

Any arrays and logical drives where the outage resulted in a failed array remain in a failed state after power is restored to the enclosure. This applies if two or more drives in the same

RAID 5 array reside in the missing enclosure. Before taking any recovery action, it is important to understand the order in which the drives failed. Ideally, the failed drives should be revived in the opposite order in which they failed. With a power failure affecting a single enclosure, we can sometimes assume that all drives failed simultaneously. However, if a drive was in a failed state prior to the power outage, then it could contain stale data and therefore needs to be excluded from the array during recovery. Failing to do so might result in data corruption. If there is any doubt, then the IBM Support representative can determine the order in which the drives failed by reviewing the MEL and shell data.

Recovery actions: Multiple disks failures

To recover after multiple disks fail, perform these steps:

1. Determine the order in which the disks failed.
2. Unassign any standby hotspare drives.
3. Revive each disk starting with the drive that failed last until the associated logical drives change from a Failed to Degraded state. With a RAID 5 array, this means that one disk still remains in a failed state.

The Revive option is available through the Storage Manager Subsystem Management window by highlighting the drive and then selecting **Advanced** → **Recovery** → **Revive** → **Drive...**

In this case, reviving a failed drive results in it being returned to an Optimal state.

4. Reboot the host(s) or rescan for the previously missing LUNs.
5. Check the data. If possible, avoid making any changes on the volume until it is clear that there is no data corruption, that is, mount the file system as read-only and perform **fsck** or **chkdsk** without attempting to fix errors. If data appears to be corrupt, then contact your IBM Support representative before taking any further actions.
6. After confirming data integrity, we can reconstruct the remaining failed disk(s) in the array. When complete, the associated logical drives return to an Optimal state.

The Reconstruct option is available through the Storage Manager Subsystem Management window by highlighting the drive and then selecting **Advanced** → **Recovery** → **Reconstruct Drive...**

Reconstructing a failed disk results in data being regenerated on it from the remaining drives in the RAID array.

7. Reassign the hotspare drives.

Note: Extreme care should be taken when selecting the Revive Drive option on an assigned drive. The function behaves differently depending on whether another drive is sparing for the drive being revived. If a hotspare has taken over, then reviving the drive will force a copyback to start. If there is no hotspare in use, then it will return the drive into an Optimal state as a member of the array, irrespective of whether it contains valid data or not.

Note: Be careful that wrong revive sequence could cause data corruption.

Sometimes, following a power or channel incident, some drives return to a Replaced state even though there is no reconstruction or copyback in progress. In this case, it could be need to change the drive to a failed state before to be revived or reconstructed.

To fail a drive through the Storage Manager Subsystem Management window, highlight the drive and then select **Advanced** → **Recovery** → **Fail Drive**.

Checking RAID redundancy

We have already mentioned earlier in the 5.8, "Preventative maintenance and data collection" on page 356 that Media Scan includes an option to perform a RAID redundancy check. By default, the redundancy check is normally disabled for all logical drives. If enabled, Media Scan schedules to complete the check as a low priority task within the preset duration period (default of 30 days). However, there is also an option to perform an immediate data redundancy check on an array from Storage Manager.

This can be started from the Logical view in the Storage Subsystem window. Highlight the array to be checked in the left-hand pane and select **Advanced** → **Recovery** → **Check Array Redundancy** as shown in Figure 5-83.

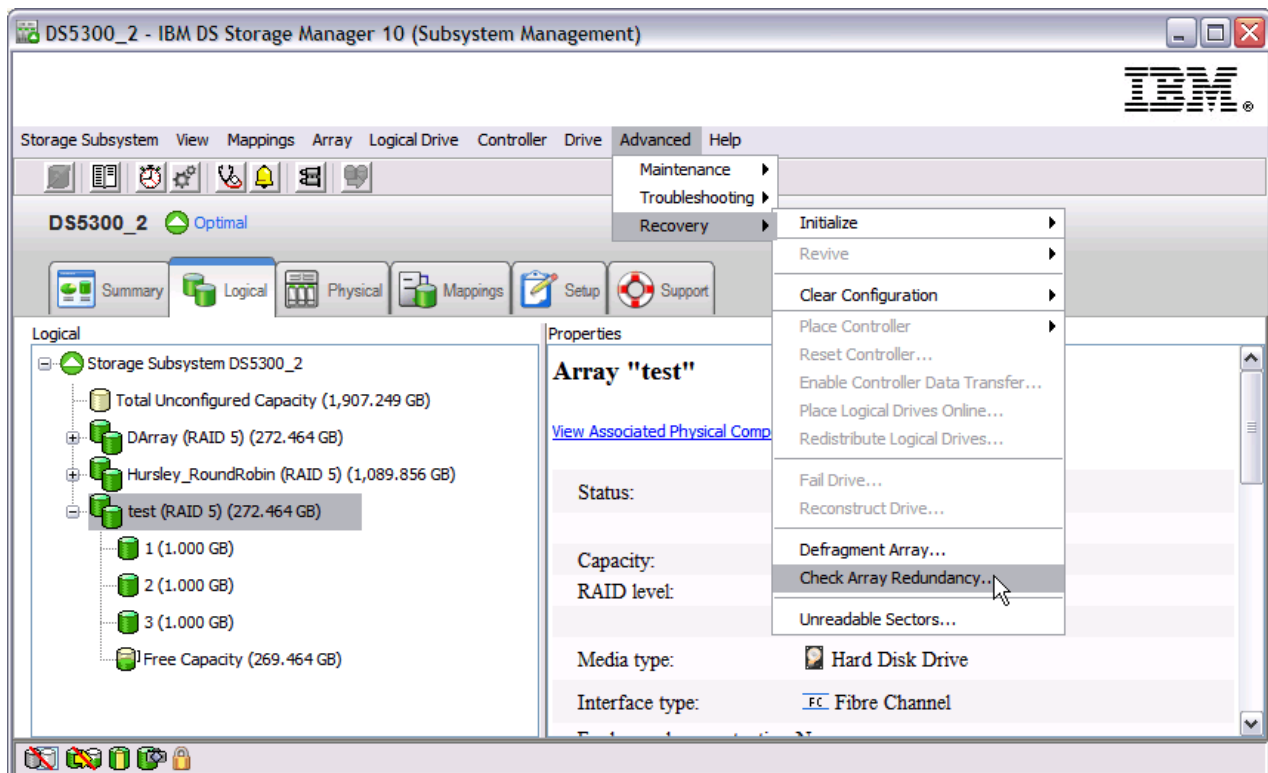


Figure 5-83 Check of array redundancy

The Check Redundancy window opens. The array test starts after clicking the **Start** button. A progress bar and execution summary is displayed throughout the check period. Click on OK when redundancy check is completed as shown in Figure 5-84 on page 388.

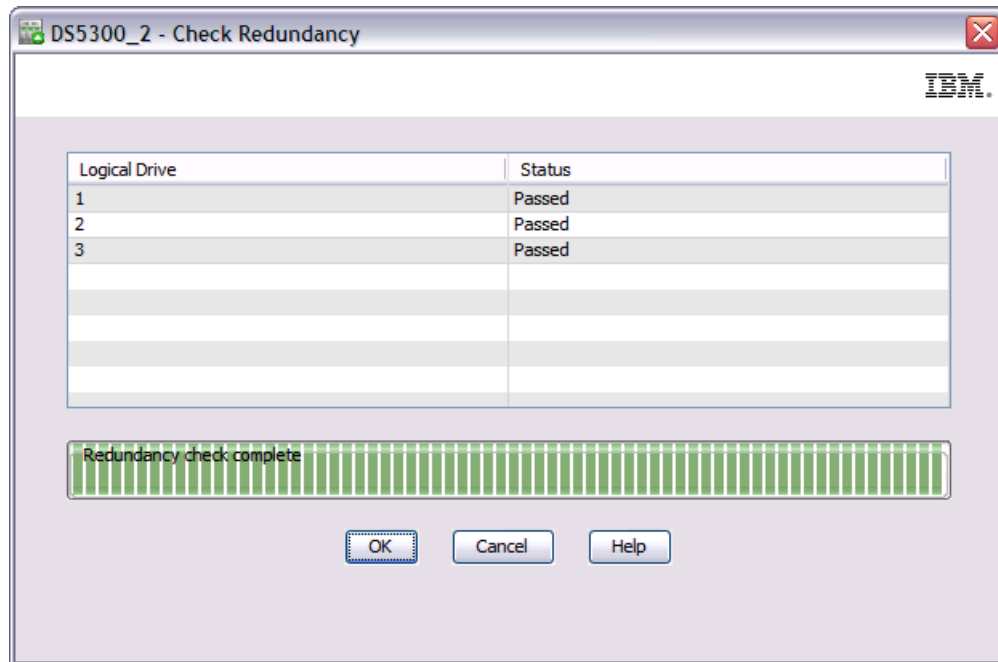


Figure 5-84 Check redundancy window

The utility will return a status for each logical drive associated with the array:

- Passed** The logical drive passed the redundancy check. No inconsistencies were detected in the redundancy information.
- Media error** The disk drive media is defective and is unreadable.
- Parity error** The parity is not what it should be for a given portion of the data.

If parity errors are detected, then it is important to determine the root cause. Contact your IBM Support representative for assistance.

A similar utility can also be run on an individual logical drive through the script editor in the Storage Manager Enterprise Management window. The command syntax is:

```
check logicalDrive ["logicalDriveName"] parity [parityErrorFile="filename"]
[mediaErrorFile="filename"] [priority=(highest | high | medium | low | lowest)]
[startingLBA=LBAvalue] [endingLBA=LBAvalue] [verbose=(TRUE | FALSE)];
```

Here is a typical usage example:

```
check logicalDrive ["LUN01"] parity parityErrorFile="c:\LUN01.parity.txt"
mediaErrorFile="c:\LUN01.media.txt" priority=high verbose=TRUE;
```

This runs the RAID redundancy check on the entire logical drive named LUN01 with parity errors being logged in the file c:\LUN01.parity.txt and any media errors in c:\LUN01.media.txt.

This command adds some flexibility to the redundancy check. It is never easy to predict how long the utility will take to complete and what impact it will have. Therefore, it is advisable to perform a quick test first by timing how long it takes to complete the check on the first 10 GB of data. The time to complete execution on the entire logical drive can then be estimated with some accuracy. If there are performance concerns, then the priority level can be reduced. The test command looks like this:

```
check logicalDrive ["LUN01"] parity parityErrorFile="c:\LUN01.parity.txt"
mediaErrorFile="c:\LUN01.media.txt" priority=low verbose=TRUE startingLBA=0
endingLBA=20000000;
```

Repairing RAID redundancy errors

If RAID parity errors are detected during execution of the logical drive parity check script, then there is another script command that can be run to fix them:

```
repair logicaldrive [logicalDriveName] parity parityErrorFile="filename"
[verbose=(TRUE | FALSE)];
```

So, our usage example looks like this:

```
repair logicalDrive ["LUN01"] parity parityErrorFile="c:\temp\LUN01.parity.txt"
verbose=TRUE;
```

This generates the following output in the bottom pane of the script editor while the sectors with invalid parity are being corrected:

```
Executing script...
Repair Logical Drive Parity called on logical drive: "LUN01" at LBA: 2,032
Repair Logical Drive Parity called on logical drive: "LUN01" at LBA: 2,033
Repair Logical Drive Parity called on logical drive: "LUN01" at LBA: 2,034
Repair Logical Drive Parity called on logical drive: "LUN01" at LBA: 2,035
Repair Logical Drive Parity called on logical drive: "LUN01" at LBA: 2,036
Repair Logical Drive Parity called on logical drive: "LUN01" at LBA: 2,037
Repair Logical Drive Parity called on logical drive: "LUN01" at LBA: 2,038
Repair Logical Drive Parity called on logical drive: "LUN01" at LBA: 2,039
Repair Logical Drive Parity called on logical drive: "LUN01" at LBA: 2,040
Script execution complete.
```

This command corrects the RAID parity information on the logical drive where errors were detected, but it has no way to determine which disk(s) have valid data and which are incorrect. Therefore, it is always safer to identify the root cause of the RAID parity corruption and repair it by forcing a reconstruction of data on the disk most likely to have contributed to the problem. The script command should only be used when the affected data area is known to occupy non-critical data or unused space. We recommend to perform above action under guidance of IBM service representative.

Disk media errors

Over time, there will be a degree of deterioration on mechanical and Solid State Drive devices. The logic on the disks themselves will automatically re-map deteriorating sectors without the DS5000 controller even being aware. This extends the life and reliability of the media quite considerably. When enabled, the background Media Scan function forces a read of every sector in a logical drive over a preset period.

It is only when data on the sector becomes unreadable that the DS5000 controller must intercept by filling in the gaps using RAID redundancy data from the remaining drives in the array. If an error threshold is exceeded, then the drive is marked as failed and spun down awaiting replacement. At this point, if the array has RAID redundancy, there needs to be a reconstruction of data either to a standby hotspare drive, if available, or onto a replacement drive. With RAID 1 arrays, this involves a full copy of every sector for all logical drives from just the partner drive in the mirrored pair. With RAID 3 or 5 arrays, this involves a full copy of every sector for all logical drives from data and parity information about every remaining drive in the array.

Although extremely rare, it is nonetheless possible that an unreadable sector is detected on one of the source drives during this reconstruction. With RAID 3 and 5 arrays, the risk increases proportionally with the number of drives in the array. The type and capacity of the drives can also be a factor. RAID 6 arrays have two parity drives, so the potential exposure to this problem is statistically negligible.

When this occurs, there is no way to recover the data from the affected sector(s). The DS5000 controllers then remap the bad block without taking a prior copy of the data, while appending a log entry to the unreadable sector list. This allows the reconstruction process to complete, but data on the bad block is lost. Recovery Guru notifies the user of a non-optimal condition whenever there are any entries in the unreadable sector list. This list can be accessed from the Storage Manager Subsystem Management window by selecting **Advanced** → **Recovery** → **Unreadable Sectors** as shown in Figure 5-85.

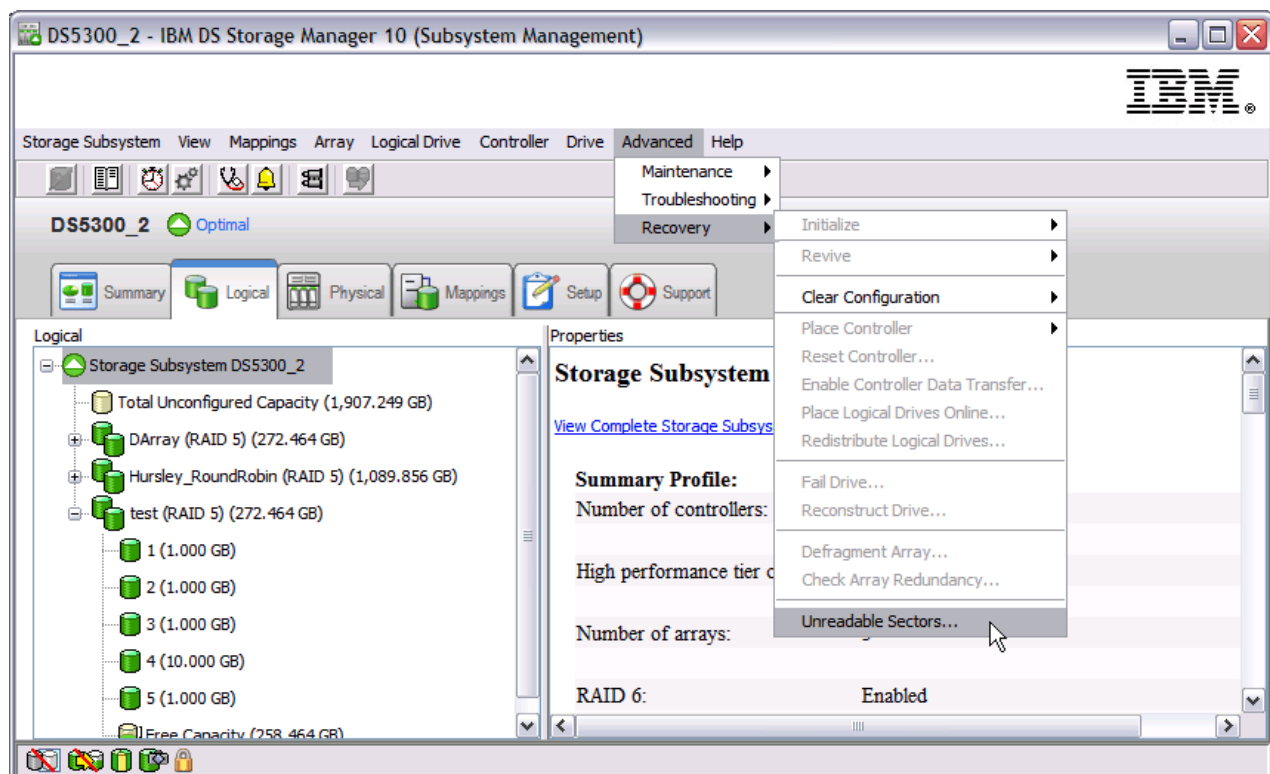


Figure 5-85 Unreadable sectors

By reviewing the LBAs in the list, it might be possible to determine whether the bad block(s) are in unconfigured space or in a logical drive space. This could assist any decision on recovery action.

The DS5000 unit remains in a non-optimal condition until the Clear option is selected in the Unreadable Sectors window. However, make sure that a Collect All Support Data file is captured before doing so.

Checking the Data Redundancy on an Array

Use the Check Array Redundancy option to check the redundancy on a selected array only when instructed to do so by the Recovery Guru or under the guidance of your IBM Technical Support representative.

It is the procedure to check parity for a case dealing with data corruption reported by the host and you suspect an issue on the storage.

Note: Checking parity does cause some performance impact, recommend to perform this action in low workload timeframe.

Keep these important guidelines in mind before you check data redundancy on an array:

- ▶ You cannot use this option on RAID Level 0 arrays that have no redundancy.
- ▶ If you use this option on a RAID Level 1 array, the redundancy check compares the data on the mirrored drives.
- ▶ If you perform this operation on a RAID Level 3, RAID Level 5, or RAID Level 6 array, the redundancy check inspects the parity information that is striped across the drives.

To successfully perform this operation, these conditions must be present:

- ▶ The logical drives in the array must be in Optimal status.
- ▶ The array must have no logical drive modification operations in progress.
- ▶ You can perform this operation only on one array at a time. However, you can perform a redundancy check on selected logical drives during a media scan operation. You can enable a media scan redundancy check on one or more logical drives in the storage subsystem.

To run data redundancy check manually on Storage manager client, select the array you want to check and select **Select Advanced → Recovery → Check Array Redundancy** as shown in Figure 5-86 on page 392.

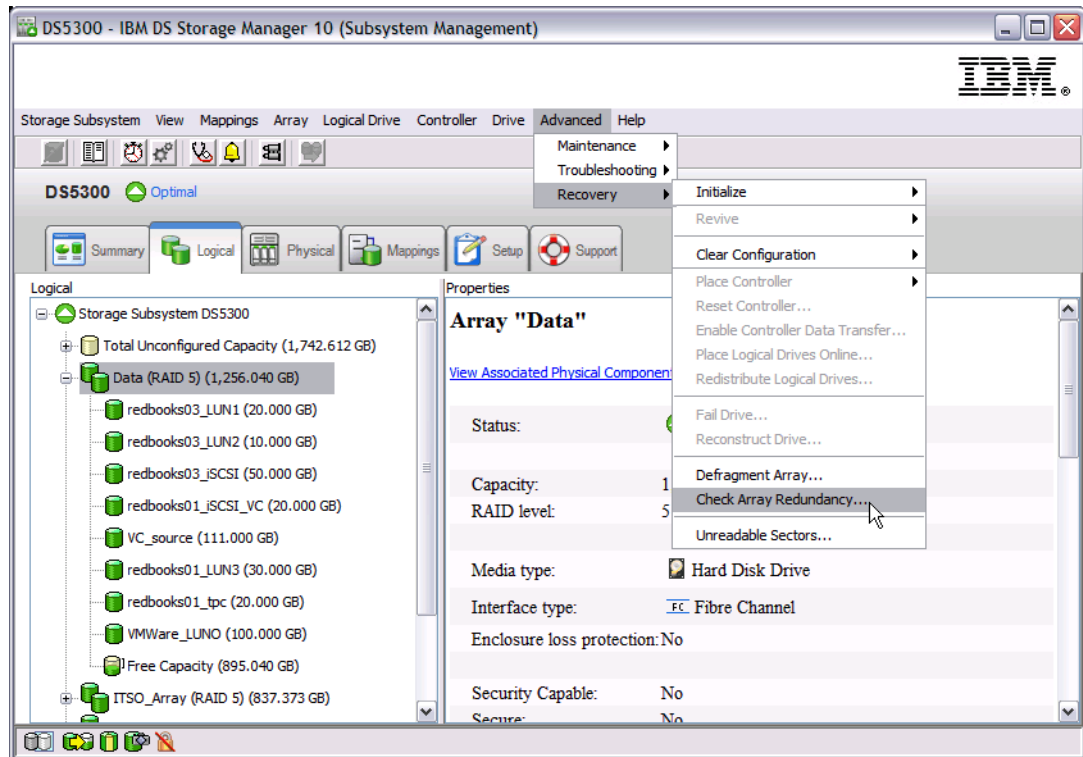


Figure 5-86 Check array redundancy

The check redundancy window opens listing all logical drive that belong to the selected array. Click on **Start** button to begin the redundancy check as shown in Figure 5-87.

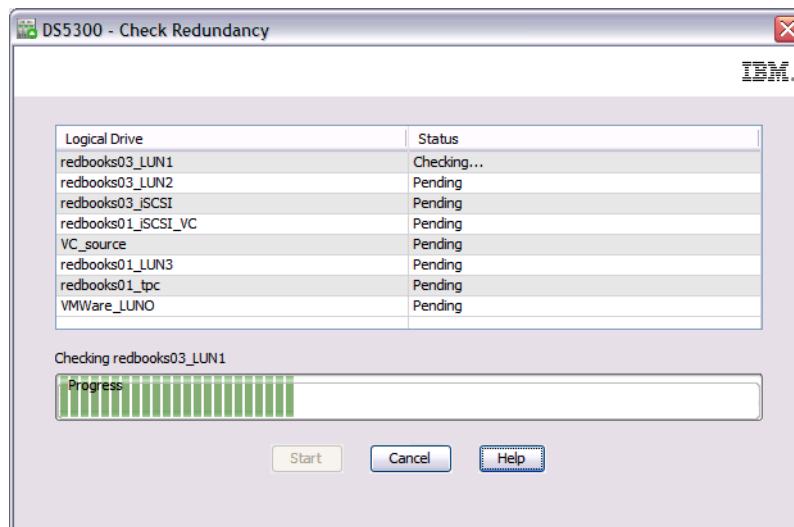


Figure 5-87 Check redundancy window

The progress bar shows the completion percentage of the redundancy check for a single logical drive, with 100 percent being complete. If an operation error occurs before the redundancy check completes, an error message appears.

Once check is completed, If you get errors send them to IBM Technical Support representative, and then click on **OK** to close the window.

5.9.2 Diagnosing host-side problems

A significant amount of support calls logged for host-side problems are found to be due to either misconfiguration or faults external to the DS5000. In this section, we look at some areas to check when attempting to identify host related problems.

Some of the more common host-side problems on the DS5000 include:

- ▶ Logical drive not on preferred path
- ▶ LUN bouncing
- ▶ Persistent reservations
- ▶ Target reset

Checking host configuration rules

The host configuration rules are described in detail in the *IBM System Storage DS Storage Manager Version 10 Installation and Host Support Guide*, GC53-1135. The latest operating system and code version specific updates are available in the readme files that accompany the Storage Manager download files. You can find these files at the following address:

<http://www.storage.ibm.com/support>

Supported configurations can be checked at the System Storage Interoperation Center at the following address:

<http://www.ibm.com/systems/support/storage/config/ssic>

Previously, there were different host cable configuration rules and recommendations for the different implementations of the RDAC multipath driver which is no longer supported. In most cases, these were restricted to a maximum of two paths.

With MPIO and other native multipath drivers multiple paths to DS5000 storage subsystem are supported. There is a single highly resilient recommended configuration for Dual-HBA hosts attached through switched Fibre Channel SAN fabrics, as illustrated in Figure 5-88 on page 393.

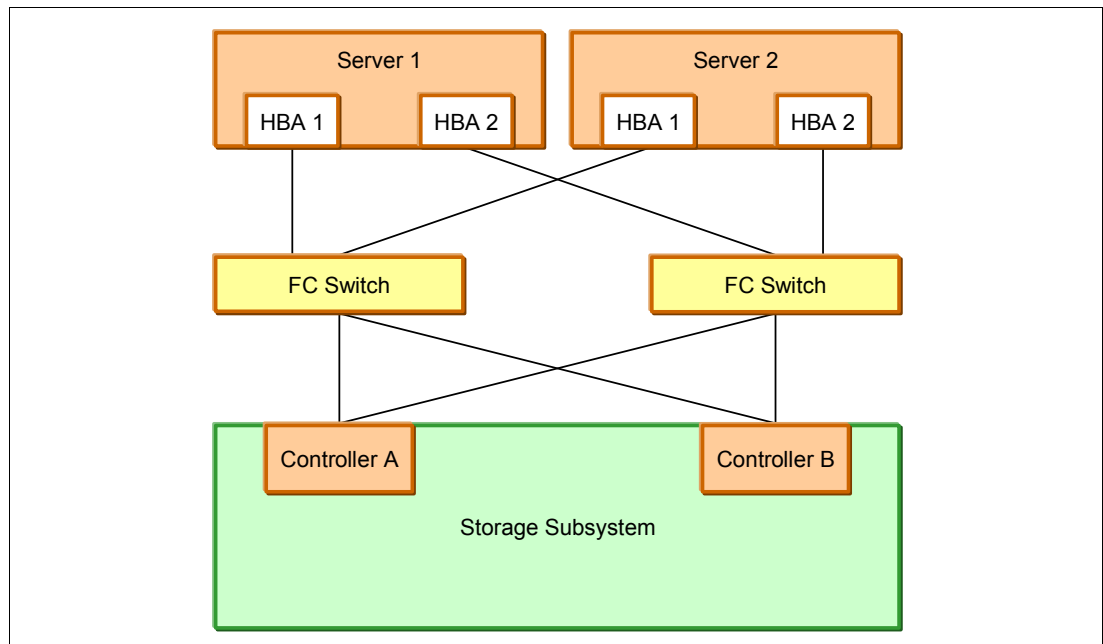


Figure 5-88 HBA to storage recommended configuration

Direct attached host configurations are permitted, although check the readme files for any operating system specific restrictions. Brocade HBAs do not support direct attached connections, a FC switch is required.

Single HBA configurations are permitted through a switch. The HBA must be zoned to have access to both controllers.

Logical drive not on preferred path

Each logical drive on the DS5000 storage subsystem is assigned to a preferred controller. The owning controller will service all I/O requests for this logical drive, while the alternate controller will act as a standby in case of failure. Whenever a logical drive failover occurs, a critical event is logged in MEL and Recovery Guru reports a non-optimal condition due to the logical drive not being on the preferred path. In the majority of cases, this does not indicate a fault on the DS5000 storage subsystem, but simply that the controllers behaved exactly as designed in transferring ownership when requested. Usually, the root cause of the failover is external to DS5000 storage subsystem.

Selecting the correct host type definition

The DS5000 storage subsystem automatically moves a logical drive onto the alternate controller for host types where Automatic Drive Transfer (ADT) is enabled whenever an I/O is received down the non-preferred path. Otherwise, it relies on the host multipath driver to issue a command (SCSI Mode Select 2C) to instruct the DS5000 storage subsystem when a failover is required. For these mechanisms to work, it is essential that the host type is set correctly to match the operating system and multipath driver on the host.

With controller firmware Version 07.77.xx, the host types shown in Table 5-3 are recognized.

Table 5-3 Host types

Host type	ADT status
AIX	Disabled
AIX (with Veritas DMP)	Enabled
Base	Disabled
HP-UX	Enabled
HPXTPGS	Disabled
IBM TS SAN VCE	Enabled
i Series	Disabled
Irix	Disabled
LNXAVT	Enabled
LNXCLUSTER	Disabled
Linux	Disabled
MacOS	Disabled
NetWare Failover	Disabled
Onstor	Enabled
Solaris (with Veritas DMP)	Enabled
Solaris (with or without MPXIO)	Disabled
VMWARE	Disabled
Windows 2000/Server 2003/Server 2008 Clustered	Disabled
Windows 2000/Server 2003/Server 2008 Clustered (supports DMP)	Enabled
Windows 2000/Server 2003/Server 2008 Non-Clustered	Disabled
Windows 2000/Server 2003/Server 2008 Non-Clustered (supports DMP)	Enabled

Note: There are two host type definitions for Windows 2000/Server 2003/Server 2008 Clustered and Windows 2000/Server 2003/Server 2008 Clustered Non-Clustered. The entries with the (supports DMP) suffix are only valid if VERITAS DMP is used as the multipath driver.

There are also scripts available to change the default ADT setting for specific host types. This might be required for SAN boot to work correctly. See the relevant documentation for usage instructions in *IBM System Storage DS5000 Series Implementation and Best Practices Guide*, SG24-8024.

Missing path(s) to host

When multiple logical drives associated with different hosts (or host groups) suddenly failover onto their non-preferred controllers in the same direction, then the fault is likely to be closer to the DS5000 storage subsystem. In this case, the first place to check is the Recovery Guru summary of problems to see whether there are any other outstanding failures, such as failed SFP. If not, then take a look in the Major Event Log (MEL) for a possible controller reset or other host-side incidents at the time of failover. It is also worth checking the status and error count on the Fibre Channel switch ports that connect to the DS5000 storage subsystem. This could expose some marginal links to the host port(s) on the DS5000 controllers.

If logical drive(s) associated with a single host or host group fail over onto their non-preferred controllers while other logical drives remain unaffected, then the fault is likely to be closer to the host itself. In this instance, we need to focus just on the affected host(s) and paths to it. It means physical connection as well as SAN and multipath policy configurations.

Apply following procedure to figure out where the problem is:

1. If storage partitions are used, the first step is to show the WWPN of each HBA device in a host that the controllers are configured to see. To do so one of following procedure can be used:
 - a. Storage Subsystem profile as shown in Example 5-9:

Example 5-9 Host definition

Host:	X3650-U
Host type:	Windows Server 2003/Server 2008 Non-Clusterer
Interface type:	Fibre Channel
Host port identifier:	10:00:00:05:1e:59:04:35
Alias:	X3650-UP0
Host port identifier:	10:00:00:05:1e:57:1a:6e
Alias:	X3650-UP1

- b. Host properties in the Mappings section by right clicking on host and selecting **Manage Host Port Identifier...** as shown in Figure 5-89 on page 397.

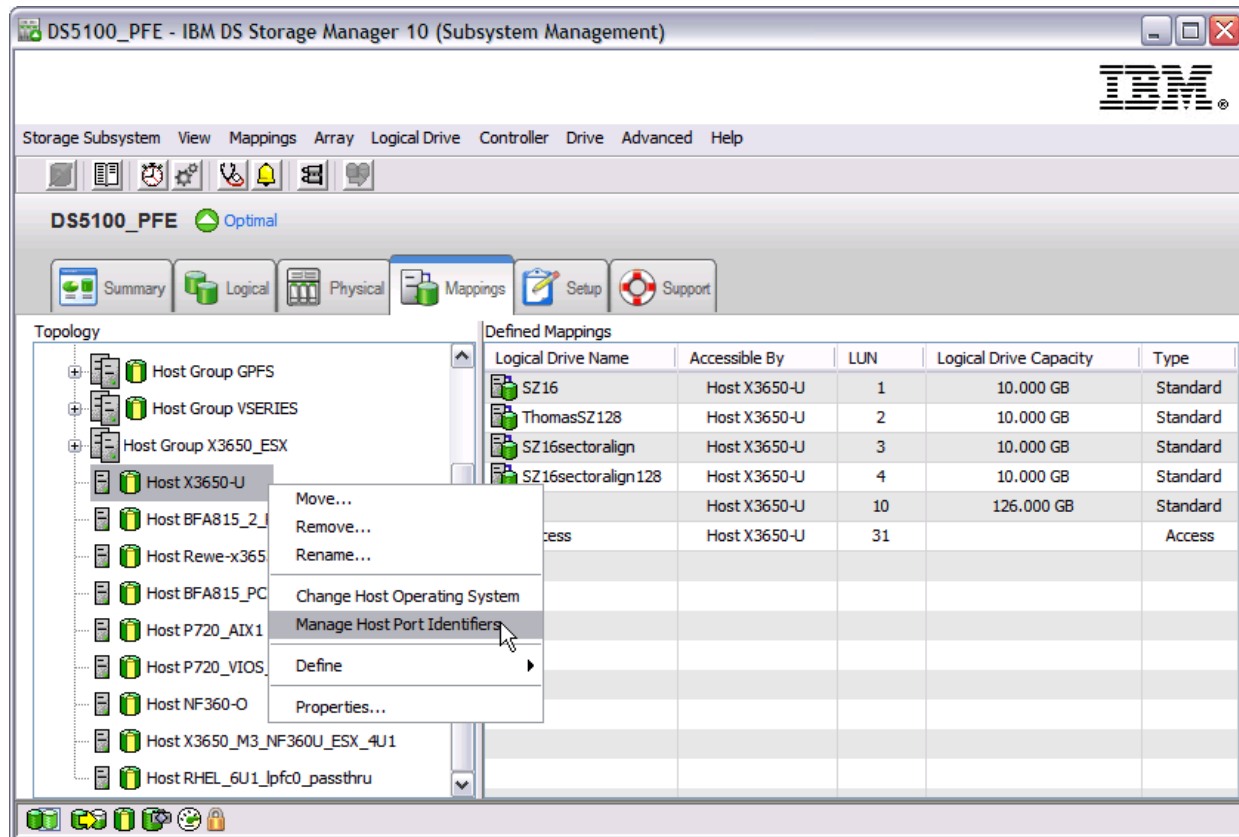


Figure 5-89 Managing host ports

The manage port identifiers window shows host ports information as shown in Figure 5-90.

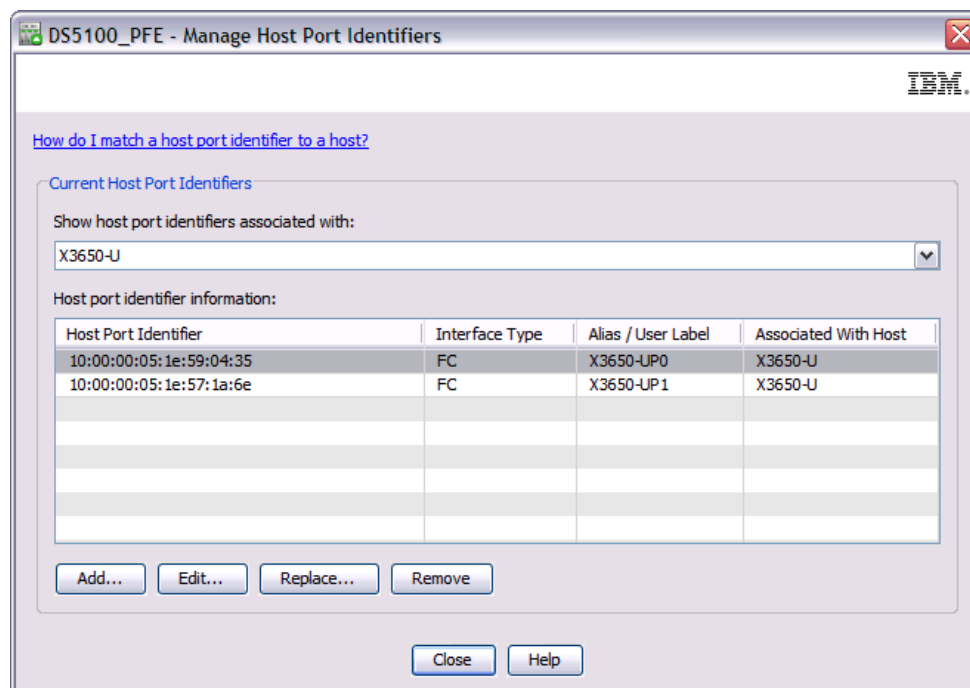


Figure 5-90 Host ports properties

- Obtain a real-time view of devices accessible from each controller by analyzing the Capture State Information output. This is a text file containing low-level shell data from both controllers. The Capture State Information file can be generated from the Storage Manager Subsystem Management window by selecting **Advanced** → **Troubleshooting** → **Capture State Information**.

Use a text editor such as Notepad to view the Capture State Information file. The only command we need to check is **spmShow** from each controller. The sections we need to search for begin with:

Executing spmShow(0,0,0,0,0,0,0,0,0) on controller A

and

Executing spmShow(0,0,0,0,0,0,0,0,0) on controller B

From there, we need to page down to a subsection with the following heading:

---I-T-Nexus (PORT) Objects (ITN)---

This provides a list of initiator devices that are currently seen by this controller. The HBA ports can be recognized by either the alias name, which matches the alias defined in the Storage Manager mappings view or Host_XXXXXXXXXXXXXXX, where XXXXXXXXXXXXXXXXXX represents the WWPN of the undefined HBA. For each Dual-HBA host configured in the recommended way shown in Figure 5-90 on page 397, we expect to see one entry for each HBA on each controller. The following output shows an example of how **spmShow** can be used to troubleshoot host-side problems:

Controller A spmShow output:

---I-T-Nexus (PORT) Objects (ITN)---

ITNID	InitiatorPort	TargetPort	Online
x001f	X3650-UP1	FC_TargetPort_Ah_ch10	on
x0020	X3650-UP0	FC_TargetPort_Bh_ch11	off

Controller B spmShow output:

---I-T-Nexus (PORT) Objects (ITN)---

ITNID	InitiatorPort	TargetPort	Online
x0020	X3650-UP1	FC_TargetPort_Ah_ch11	on
x0021	X3650-UP0	FC_TargetPort_Bh_ch10	off

The Online column shows a status of either on or off:

on Device is currently accessible from this controller.

off Device was recognized on this channel previously but is no longer accessible.

The output confirms that we need to focus on the HBA named X3650-UP0 for the root cause of the logical drive moving onto the non-preferred path. This might be due to a zoning or configuration change, a hardware failure on the HBA card itself, or the fiber link to it.

- Check the host logs and switch port status to reveal more information.

Note: This same technique can be used during initial configuration to confirm that all HBAs are zoned correctly. It is also good practice to simulate link failures during installation in order to verify that path failover is configured correctly on each host. Often, misconfiguration is only detected following a genuine failure when path failover does not behave as expected.

Managing a replaced HBA from Storage Manager

If an HBA is replaced in a host, then changes might need to be made in the switch zoning and Storage Manager host definition mappings. Once switch zoning has been changed open the Storage Manager Subsystem Management window and select the **Mappings** tab, highlight the host with the new HBA in the left-hand pane and then select **Mappings** → **Manager Host Port Identifiers** as shown in Figure 5-91 on page 399.

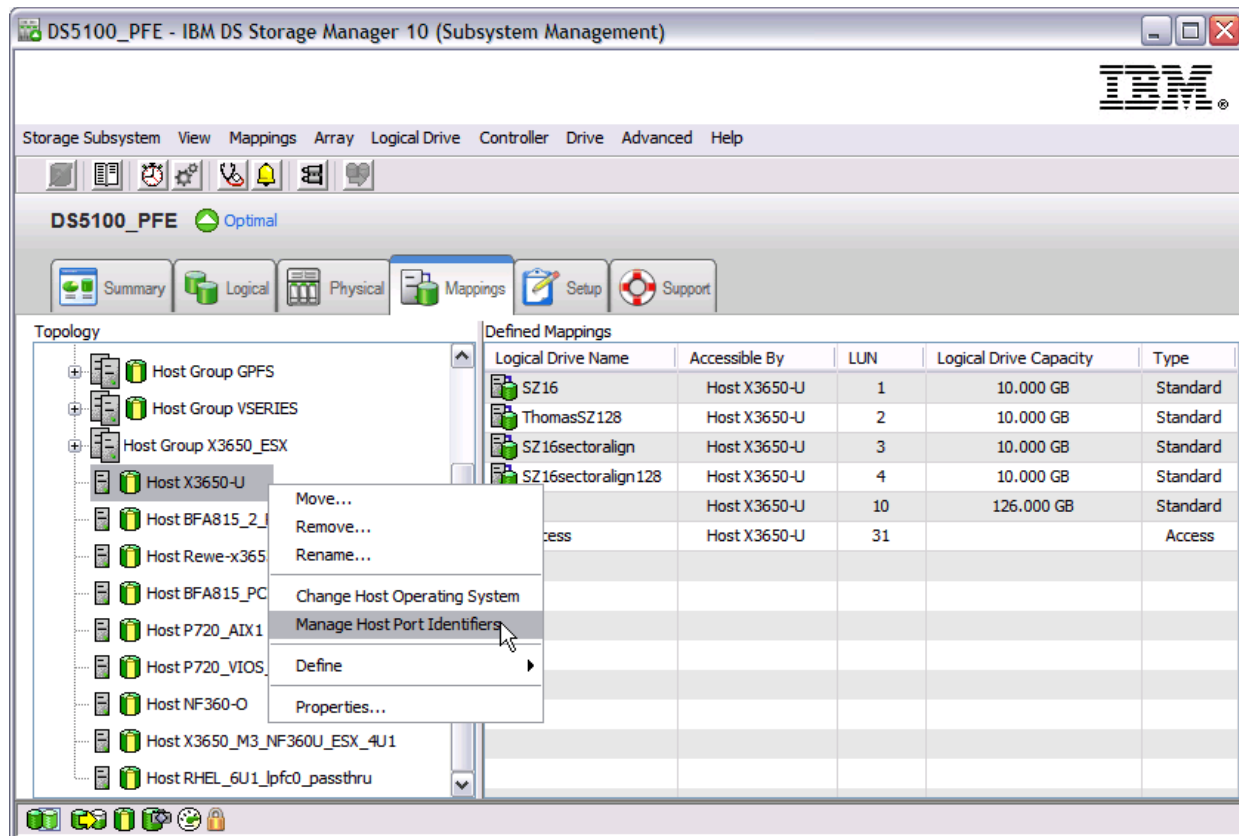


Figure 5-91 Managing host ports

The Host Port Identifiers window opens, as shown in Figure 5-92 on page 400.

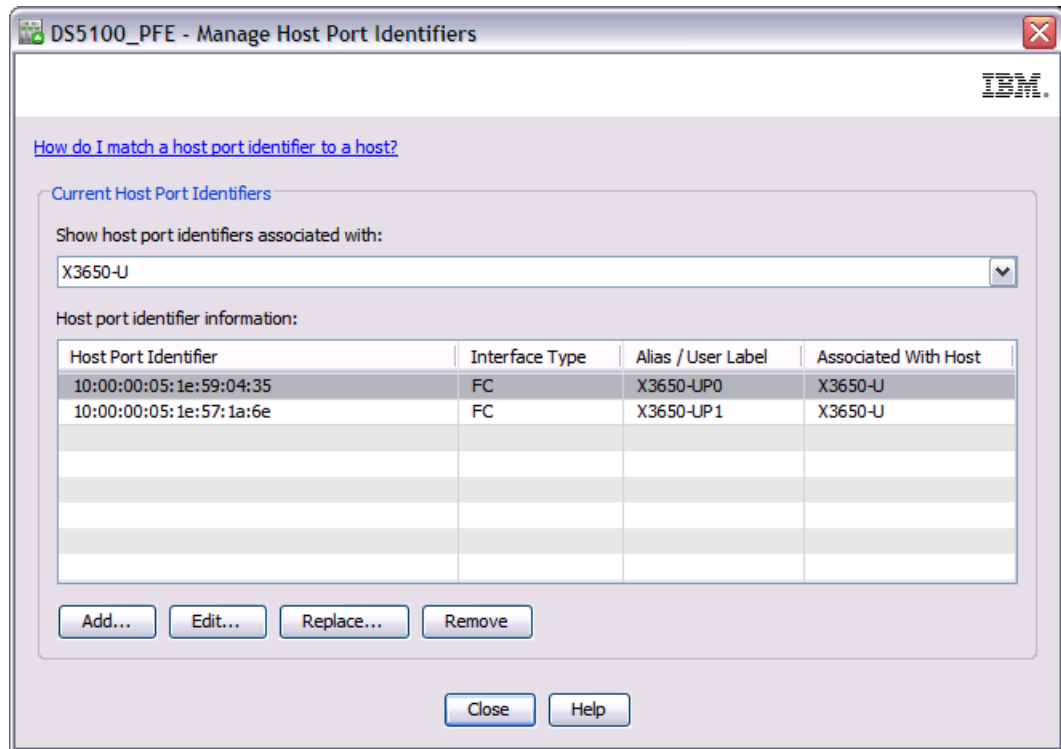


Figure 5-92 Host Port Identifiers window

By clicking the **Replace** button, we are given the option to select the host interface type as shown in Figure 5-93 on page 401.

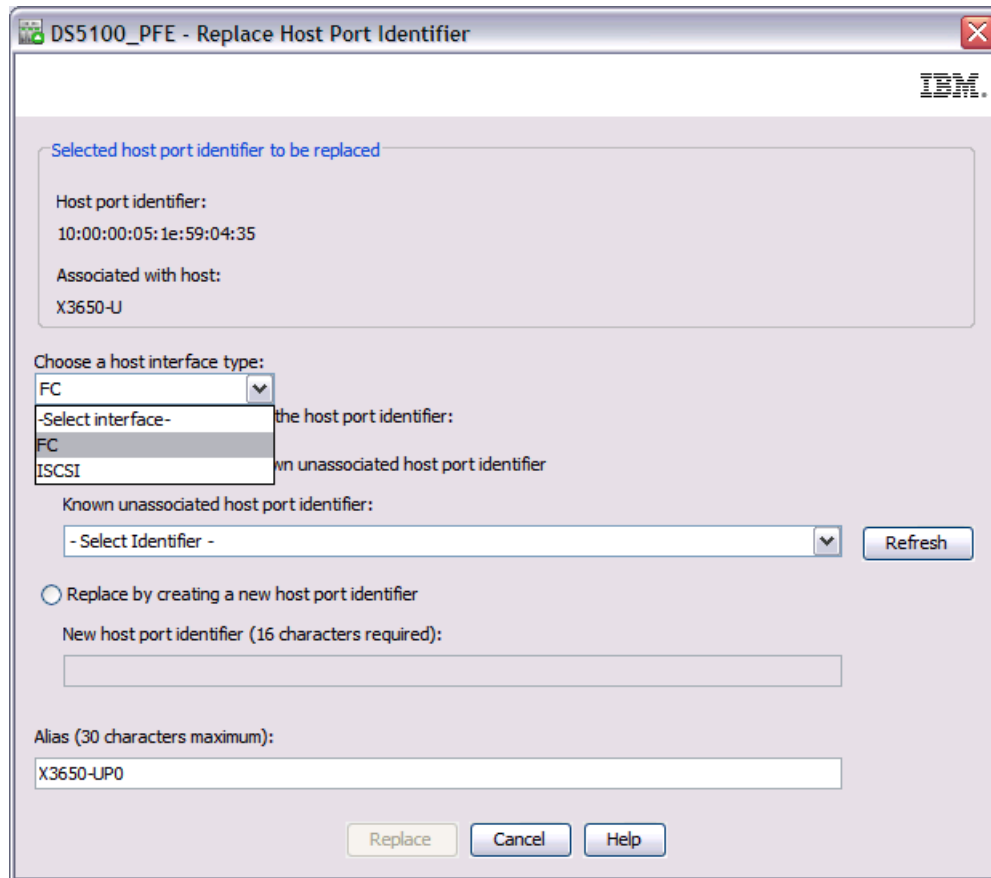


Figure 5-93 Replace host port identifier window

The option to select the new WWPN for this device from a drop-down list of known unassociated host port identifier as shown in Figure 5-94 on page 402.

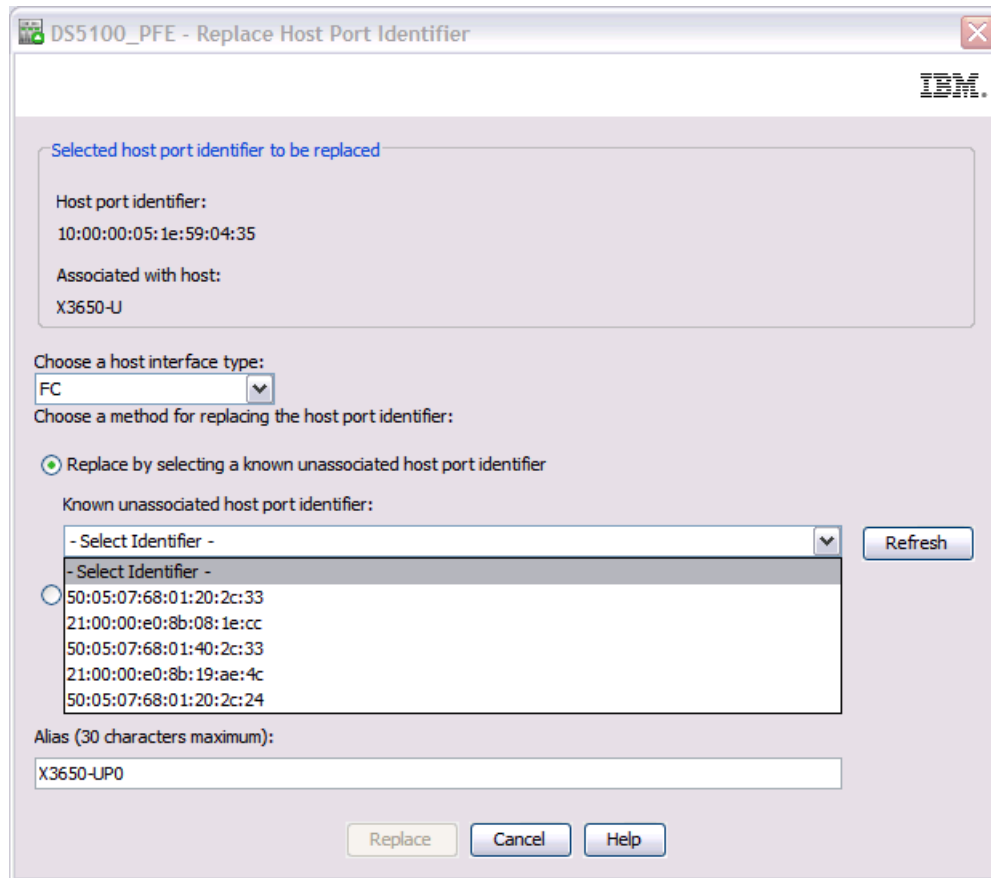


Figure 5-94 Replace host port identifier window

Any logical drives might remain on the non-preferred controller while all available paths to the preferred controller are inaccessible.

Checking host configuration

If logical drives remain on the non-preferred path even though all paths have been confirmed to be accessible, then the focus must switch to the host itself. Here, we need to check that:

- ▶ Supported versions of the HBA driver, HBA BIOS, and multipath drivers are installed.
- ▶ HBA parameters are set correctly (see *Appendix A. HBA settings on Installation and Host Support Guide GA32-0963*).
- ▶ Operating system parameters (that is, the Windows registry) are set correctly.
- ▶ Multipath policies are set correctly.
- ▶ All operating system specific rules, limitations, and prerequisites are met.

For hosts running SDDPCM/MPIO, the following commands are available for further troubleshooting:

```
pcmpath query adapter
pcmpath query adaptstats
pcmpath query device
pcmpath query devstats
pcmpath query essmap
pcmpath query portmap
pcmpath query wwpn
```

Returning logical drives back to their preferred paths

Once the underlying root cause of the logical drives switching to non-preferred path has been identified and resolved, then it is possible to return them back to their normal preferred paths. This can be done from the Storage Manager Subsystem Management window by selecting **Advanced** → **Recovery** → **Redistribute Logical Drives...** as shown in Figure 5-95.

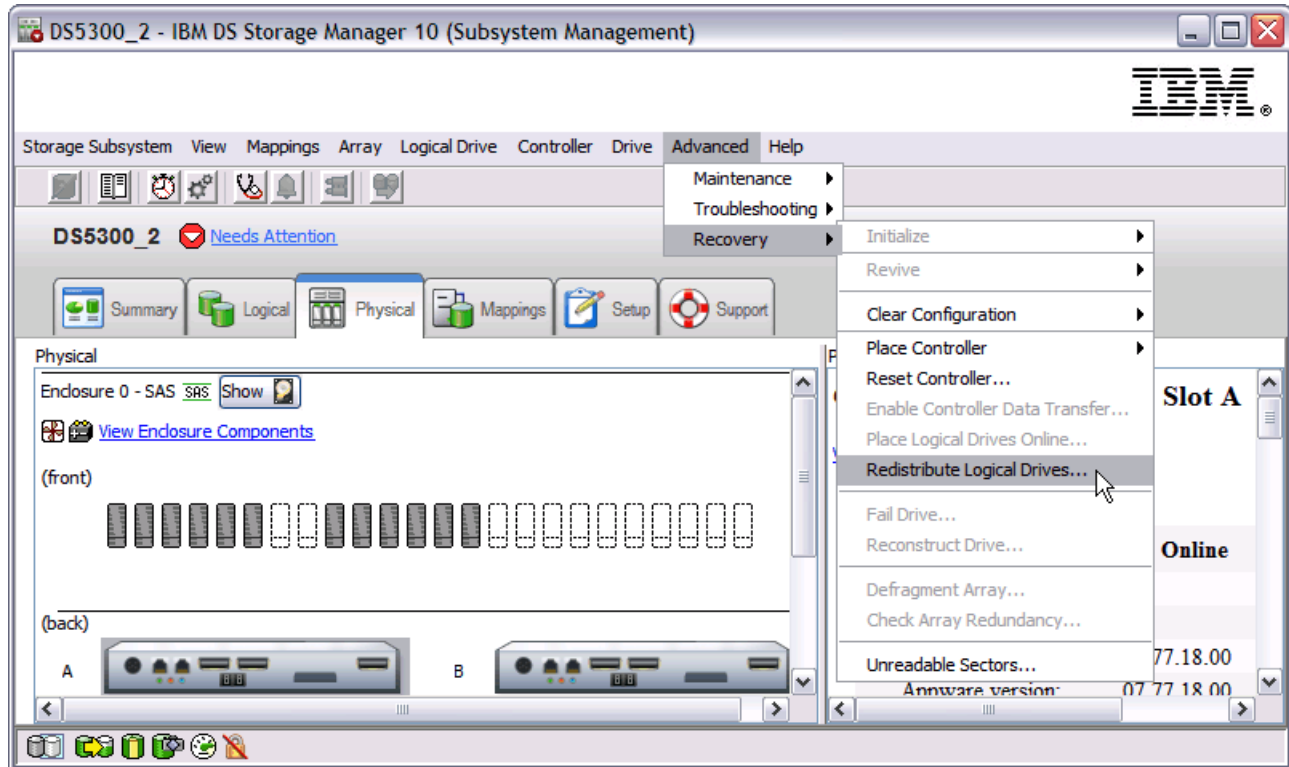


Figure 5-95 Redistribute Logical drives

Figure 5-96 shows the Redistribute Logical Drives window with a progress bar that appears during the procedure.

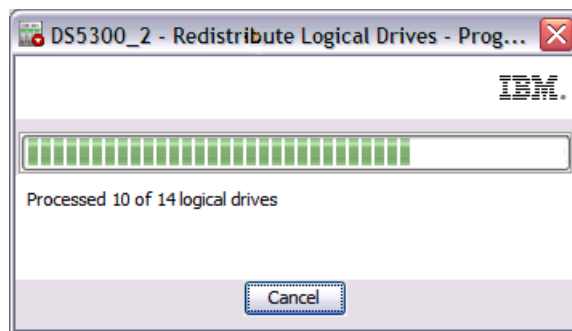


Figure 5-96 Redistribute Logical Drives window

When complete, the DS5000 unit returns to an Optimal state in Storage Manager. If any problems remain unresolved, the affected logical drives will fail back onto their non-preferred paths.

Note: The message "Controller cache not enabled or was internally disabled" is logged each time a Logical Drive ownership changes between the controllers. The message only indicates that the cache for the Logical Drive being moved is disabled during the transfer. It does not mean that the cache is permanently disabled.

Logical drive bouncing

The constant transfer of logical drives back and forth between the two controllers can be caused by a number of reasons. It can result in a severe performance degradation and should be corrected. It is more likely to be a host configuration issue. In order to find evidence of logical drive bouncing, we need to check the Major Event Log (MEL), looking for a constant stream of non-critical event type 300D errors with a description of "Mode select for redundant controller page 2C received", as shown in Figure 5-97.

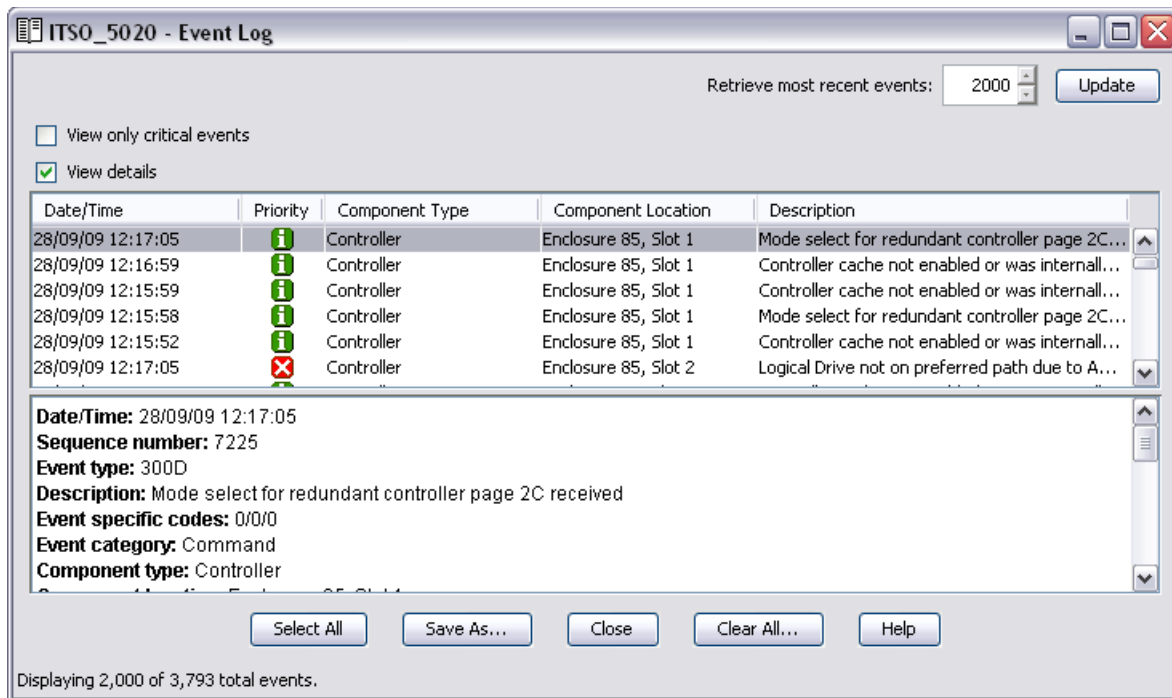


Figure 5-97 Mode Select 2C events

The DisableLunRebalance parameter

If the events appear exactly every 60 seconds, then it is possible that the DisableLunRebalance parameter is set incorrectly in an MPP clustered environment. If a host in a cluster server configuration lost a physical path to a DS5000 storage subsystem controller, the logical drives that are mapped to the cluster group will periodically fail over and then fail back between cluster nodes until the failed path is restored. This behavior is the result of the automatic logical drive failback feature of the MPIO/DSM multipath driver. The cluster node with a failed path to a DS5000 controller will issue a failover command of all logical drives that were mapped to the cluster group to the controller that it can access. After a programmed interval (normally 60 seconds), the nodes that did not have a failed path will issue a **failback** command for the logical drives because they can access the logical drives both controllers, resulting in the cluster node with the failed path not being able to access certain logical drives. This cluster node will then issue a **failover** command for all logical drives, repeating the logical drives failover/failback cycle.

The workaround is to disable this automatic failback feature in all clustered configurations. In Windows, change the DisableLunRebalance registry setting of the [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ds4dsm\Parameters] registry key from 0 to 3 in each cluster node. Then, reboot each node for the changes to take effect.

For Linux cluster (SteelEye) environments change DisableLUNRebalance=3 in /etc/mpp.conf and run following command to active new parameter:

```
# mppUtil -o DisableLunRebalance=0x3
# mppUpdate
```

Missing paths in a cluster environment

LUN bouncing can be caused by an incorrect configuration in which one cluster node can access the shared logical drives only through one controller and another node can only access the same shared logical drives through the alternate controller.

The missing paths can be identified using the same method described in “Missing path(s) to host” on page 396.

Persistent reservations

A host may issue a SCSI persistent reservation command to restrict which other HBA ports can access a particular LUN. These commands can be used by a server to prevent HBA ports in other servers from accessing the LUN and thereby prevent accidental data corruption caused by one server overwriting another server's data. “Reserve” and “Persistent Reserve” are often used by clustering software to control access to shared logical disks.

If a server is not shut down or removed from the server cluster in a controlled way, its reserves and persistent reserves can sometimes be left in place, preventing other servers from accessing data that is no longer in use by the server holding the reservation. In this situation, a storage administrator or server administrator might want to break the reservation and allow a new server to access the virtual disk.

The safest thing to do is to have the server that owns the reservation explicitly release the reservation, as this ensures that the server concerned has flushed its caches and its software is aware that it has lost access to the disk. In some circumstances where this is not possible, then most operating systems provide operating system specific tools to allow reservations to be removed. Consult the operating system documentation for details.

It is possible to view the Logical Drive Reservations and Logical Drive Registrations from the Storage Manager Subsystem Management window by selecting **Advanced** → **Maintenance** → **Persistent Reservations**. The dialog shows any logical drives in the storage subsystem that have registrations, with the first logical drive in the list highlighted by default. This table describes the information and buttons shown in the Persistent Reservation dialog:

Logical drive name	Shows the user label of the logical drive with persistent reservations. Logical drives are listed in alphabetical order. If a logical drive user label is not available, then its World Wide Identifier (WWID) appears.
LUN	Shows the assigned LUN number for the particular logical drive.
Registrants	Shows the number of registrations for the particular logical drive.
Reservation type	Shows an abbreviated form of the associated reservation type for the particular logical drive. Each addressable logical drive can have one reservation. Each reservation can grant access rights to one or more registrants, depending on the reservation type. You can reserve a logical drive for a specific access level by a group of registrants. All of

the registrants within a group are restricted to the access level defined by the reservation type. This list shows reservation types as follows:

None	The logical drive has registrants, but it currently has no reservation.
WE	Write exclusive: Only the host port that reserved the logical drive may write to the logical drive. Reads shared: Any host port may read from the logical drive.
EA	Exclusive Access: Only the host port that reserved the logical drive may read from or write to the logical drive.
WE-RO	Write Exclusive - Registrants Only: Writes exclusive: All registered host ports may write to the logical drive. Reads shared: Any host port may read from the logical drive.
EA-RO	Exclusive Access - Registrants Only: Only registered host ports may read from or write to the logical drive.
WE-AR	Write Exclusive - All Registrants: Writes exclusive: All registered host ports may write to the logical drive. Reads shared: Any host port may read from the logical drive.
EA-AR	Exclusive Access - All Registrants: Only a host port may read from or write to the logical drive.

PTPL Shows Yes if the registrations are set to persist through a power loss.

To view the registrations that are associated with the logical drive reservation, either double-click the desired logical drive, or highlight the logical drive and check the **View Associated Registrations** check box in the upper left of the dialog. The following information is then presented:

Interface type	Shows the type of interface: SATA, SAS, or Fibre.
Host (initiator) port	Shows the associated user label for the particular host port. If the host port alias has not been provided, then Not Available appears.
Associated host	Shows the host associated with the specific logical drive.
Controller (target) ports	Shows the port name of the target port.
Holds Reservation?	Shows either Yes or No, depending on whether the specific host port is the reservation holder.

Clearing persistent reservations

Sometimes it is not possible to clear the persistent reservation from the host. This is the case if a cluster host had been decommissioned without being shut down cleanly. Any persistent reservations prevent the associated logical drives from being deleted or changed in any way. There is an option to clear the logical drive reservations from the Storage Manager Subsystem Management window by selecting **Advanced** → **Maintenance** → **Persistent Reservations**.

1. In the upper-left corner of the Persistent Reservations window, make sure that the View Associated Registrations check box is cleared.
2. Click one or more desired logical drives. To select all of the logical drives, click **Select All**.
3. Click **Clear**.
4. In the text box in the Clear Registrations/Reservations dialog, type yes, and click **OK**. If you do not want to clear any reservations, click **Cancel** to return to the Persistent Reservations dialog.

The reservation and registrations that were associated with the logical drives that you highlighted in the upper pane are now cleared.

Target reset

It is normal to see TGT Reset events logged in the Major Event Log (MEL) during a host cluster failover. Basically it indicate a reset SCSI command issued by the host and could be related to wrong HBA settings. A support call will need to be logged for any unexplained target reset events.

5.9.3 Storage Manager communication problems

If Storage Manager shows the status of DS5000 storage subsystems as unresponsive, then there are some recovery procedures to be followed.

In-Band management

To recover the storage subsystems using in-band management, perform these steps:

1. Close all Storage Manager windows.
2. Check to make sure that the Access LUN is presented to the Storage Manager station.
Use this utility SMDDevices to determine whether the Access LUN is visible. The default LUN number is 31. If the Access LUN is not mapped to the Storage Manager station, then in-band management will not be possible.
3. Restart the host agent software. On Windows 2003 and 2008 hosts, this can be done by performing these steps:
 - a. Select **Start** → **Administrative Tools** → **Services**. The Services window opens.
 - b. Right-click **IBM DS Storage Manager Agent**.
 - c. Click **Restart**. The IBM DS Storage Manager Agent stops and then starts again.
 - d. Close the Services window.
4. Restart the Storage Manager client.

Out-of-Band management

To recover the storage subsystems using out-of-band management, perform these steps:

1. Ping both controllers from the Storage Manager station.
 - a. If the controllers respond to a ping, but Storage Manager remains unresponsive, then your firewall settings should be checked.
 - b. If the controllers do not respond to a ping, then there might be local network problems. Try using another mobile computer or host with a direct cable connection to one of the controllers. The default IP addresses for the controller A Ethernet ports 1 and 2 are 192.168.128.101 and 192.168.129.101, respectively. The default IP addresses for the controller B Ethernet ports 1 and 2 are 192.168.128.102 and 192.168.129.102, respectively. The default subnet mask for all four Ethernet ports is 255.255.255.0.
2. If the problem persists, then contact IBM Support for further assistance. A controller reset might be required.

5.9.4 Connecting to the Controller via the Shell interface

If the DS5000 is not reachable via Storage Manager Client and you don't know the Controller's IP address to add it to Storage Manager GUI, you may establish a direct access to the controllers via serial connection in order to check for IP address settings of each controller and change it if required.

What's needed to connect to the Serial Port interface?

Be sure to have following stuff before start to establish a serial interface connection to DS5000 controllers:

1. Server, Workstation, or Laptop installed with Windows 95,98,2000 XP/Vista, Windows Server 2003/2008.
2. Null Modem female-female DB9 cable.

PS/2-to-DB9 (Male) Serial adapter (IBM FRU # 39M5942) is required to connect to the DS5020 only.

Note: Customer may have this adapter. It is shipped with DS units that require PS/2 to DB9 connections.

3. Terminal Emulator software (i.e. Putty, HyperTerminal, NetTerm).

How to get serial interface shell

In our case we used Putty release 0.60.

Once determined which COM Port is being used to communicate with DS System, connect the serial cable to controller interface (refer to Figure 5-98 and Figure 5-99 to identify port) and perform following steps to access the controller shell:

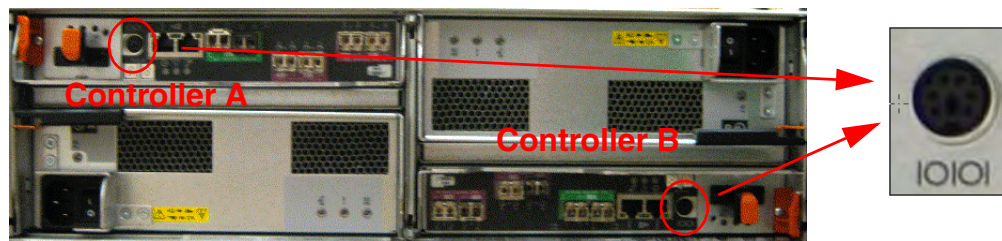


Figure 5-98 Serial port on DS5020 controller

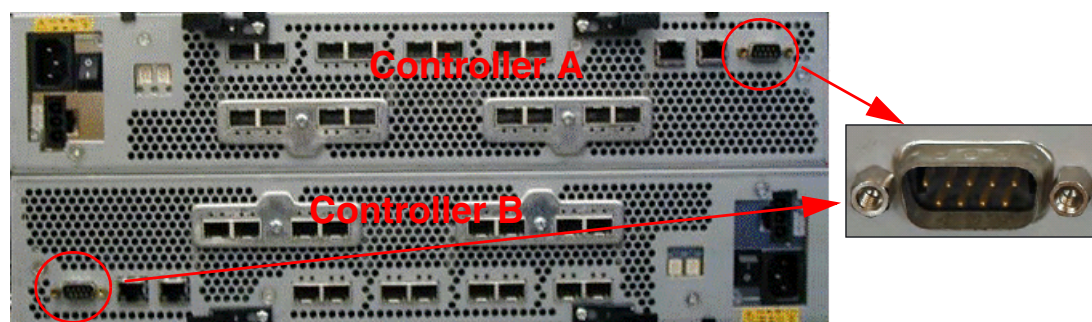


Figure 5-99 Serial port on DS5000 controller

1. Start Putty, select serial as connection type, specify the serial port and speed (at least 38400) and click on Open button.
2. Press Ctrl+Break (It is possible that you have to press this more time because when you send the Ctrl+Break command that random characters will appear on the screen each time you press Ctrl+Break. This is a normal synchronization procedure. The random characters are a result of the controller and terminal program communicating at different baud rates. Each time you press "CTRL+BREAK", the controller steps it's baud rate up in

an attempt to sync with the terminal program's baud rate. Press CTRL+BREAK until you get message in Figure 5-100 on page 409:

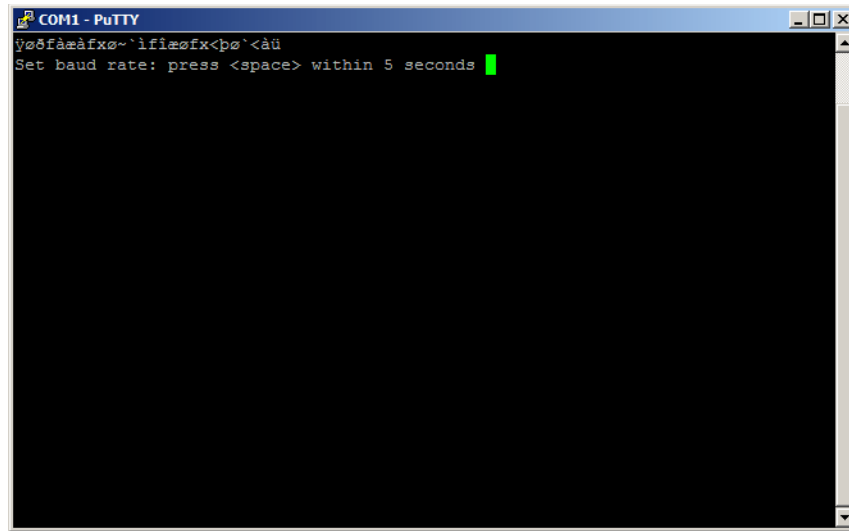


Figure 5-100 Baud rate synchronization process

3. Pressing SPACE bar with 5 seconds to set Baud rate you get the message “Baud rate set to 115200”. The speed is the one you set in step 1 on page 408.
4. Press again CTRL+BREAK, you get message in Figure 5-101:

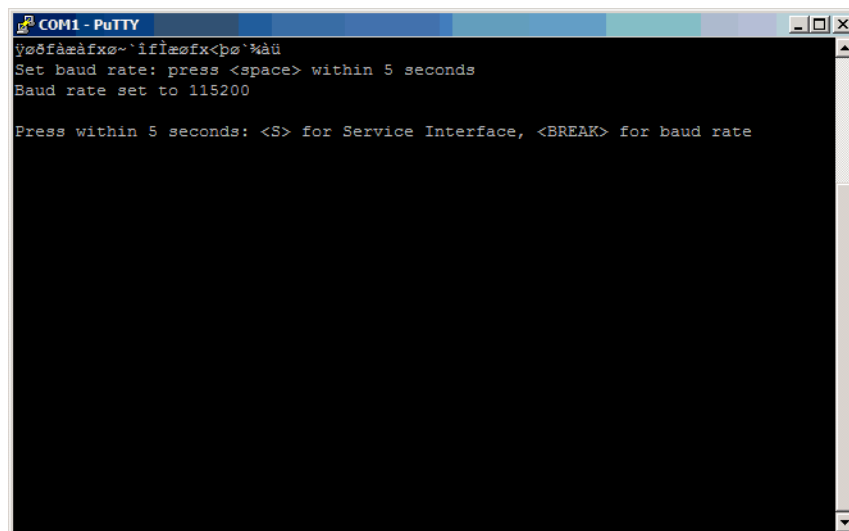


Figure 5-101 Serial login process

5. Press ESC within 5 seconds to get the login. You get login prompt as shown in Figure 5-102 on page 410:

Note: Some firmware version show the message “press within 5 seconds: <S> for Service interface” (see above). This is for developer matter. Please Press ESC otherwise you cannot log into controller.

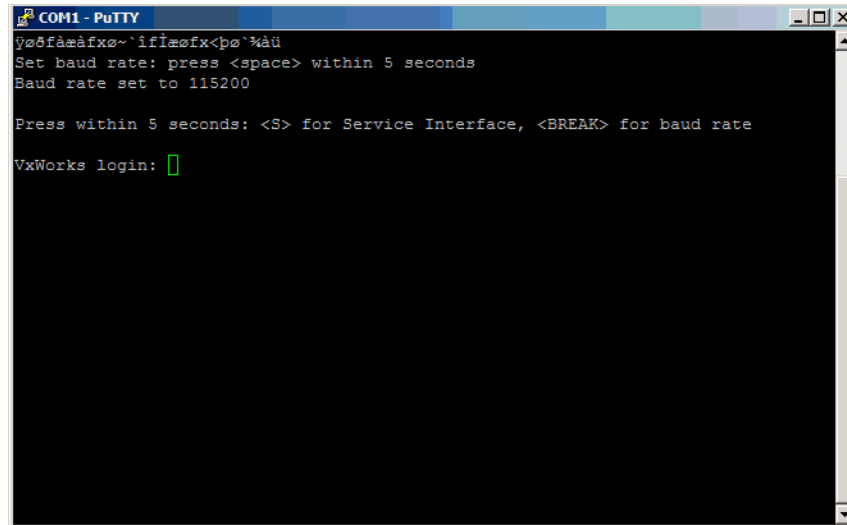


Figure 5-102 Serial login prompt

6. Enter Shell User and Password to log into controller as shown Figure 5-103

Note: For Controller Shell Login Credentials contact your IBM service support representative.

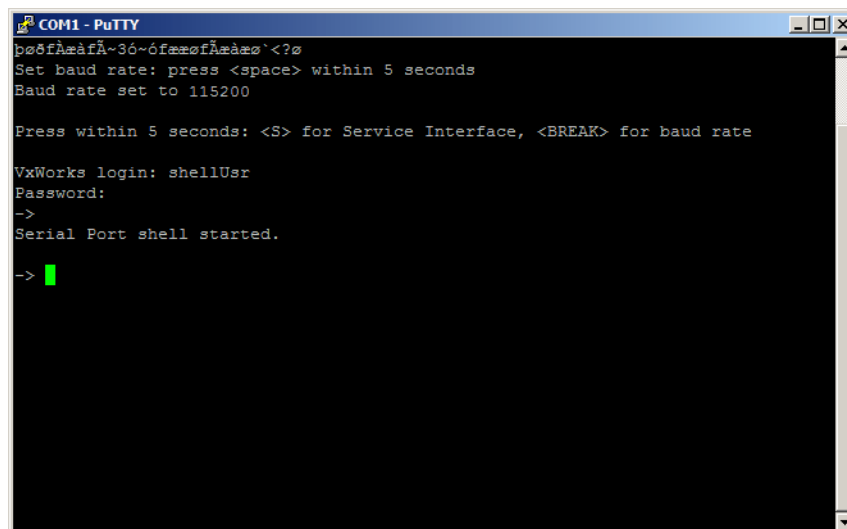


Figure 5-103 Serial shell command prompt

Show Controller IP address

To show the ethernet settings run the netCfgShow command. You get output as shown in Example 5-10:

Example 5-10 show ethernet port settings

```
-> netCfgShow

==== CURRENT NETWORK CONFIGURATION ====
My Host Name           : host
Interface Name    if0 : gei0
```

```

MAC Address      if0 : 00:80:e5:17:cc:74
IP Address      if0 : 9.11.218.191
Subnet Mask    if0 : 255.255.255.0
Config Flags     if0 : 0x81 - IPV4_EN
NIC Speed/Duplex if0 : 0x0000 - AUTO
Interface Name   if1 : gei1
MAC Address      if1 : 00:80:e5:17:cc:75
IP Address       if1 : 192.168.207.101
Subnet Mask      if1 : 255.255.255.0
Config Flags     if1 : 0x81 - IPV4_EN
NIC Speed/Duplex if1 : 0x0000 - AUTO
Server Host Name : server
Server IP Address : 192.168.11.176
Gateway IP Address : 9.11.218.1
Network Init Flags : 0x80 - TELNET_EN
User Name        : lsiuser
User Password    : *****

```

'*' indicates a dynamically assigned or default address
 value = 58 = 0x3a = ':'
 ->

In the output you have the ethernet ports settings. We recommend to use the port 1 (if0) for management via Storage manager client. Port 2 is usually for maintenance purpose.

Change Controller IP address

If you need to change the ethernet settings run the netCfgSet command as shown in Example 5-11:

Example 5-11 Change the ethernet port settings

```
-> netCfgSet
```

Please wait...

'.' = clear field; '-' = to previous field; '?' = help
 ^D = quit (keep changes); ESC = quit (discard changes)

```

==== STORED NETWORK CONFIGURATION ====
My Host Name      : host >
IP Address      if0 : 9.11.218.191 > 9.11.218.181
Subnet Mask    if0 : 255.255.255.0 > 255.255.254.0
IPv6 Local Addr   if0 : :: >
IPv6 Routable Addr if0 : :: >
IPv6 Router Addr  if0 : :: >
Config Flags      if0 :
    IPv4 Enable    : true >
    IPv6 Enable    : false >
    IPv6 Autoconf Enable : false >
NIC Speed/Duplex  if0 : 0x0000 >
IP Address        if1 : 192.168.207.101 >
Subnet Mask       if1 : 255.255.255.0 >
IPv6 Local Addr   if1 : :: >
IPv6 Routable Addr if1 : :: >

```

```

IPv6 Router Addr   if1 : ::                >
Config Flags      if1 :
  IPv4 Enable      : true                >
  IPv6 Enable      : false               >
  IPv6 Autoconf Enable : false           >
NIC Speed/Duplex   if1 : 0x0000          >
Server Host Name   : server              >
Server IP Address  : 192.168.11.176      >
Server IPv6 Address : ::                 >
Gateway IP Address : 9.11.218.1         > 9.11.218.10
Network Init Flags :
  Prefer IPv6 Host : false               >
  FTP Disable      : false               >
  Telnet Enable    : true                >
User Name          : lsiuser             >
User Password      : *****            >

Network Configuration successfully written to NVSRAM.
value = 0 = 0x0
->

```

You will get the prompt to change the values for each field one line at time. Enter the new value if you want to change it or just press enter to leave the actual value unchanged and go to the next field. In Example 5-11 on page 411 we changed port 1 and gateway IP addresses and mask as well.

5.10 Replacement and maintenance procedures

In this section, we discuss how to resolve some hardware failures on the DS5000 storage subsystem. See the *Installation, User's and Maintenance Guide* for your DS5000 storage subsystem for detailed parts replacement procedures. These publications can be downloaded from the Documents section on the IBM Storage Support Web site at the following address:

<http://www.ibm.com/support/entry/portal/>

5.10.1 Managing disk failures

The DS5000 controllers are constantly monitoring the status of the disk drives. Whenever an error threshold is exceeded, then the disk is marked as failed. This triggers the audible enclosure alarm to sound (unless disabled) and the subsystem appears in a non-optimal state. A critical event is logged in MEL and the Recovery Guru button starts flashing. All critical events are sent to the SNMP management console or to the e-mail recipient that you have configured to receive alert notifications by selecting **Edit** → **Configure Alerts** in the Enterprise Management window. The amber FAULT LED is illuminated on the faulty drive.

If the array has been configured with redundancy protection (RAID 1, 3, 5, or 6), then the drive failure will cause the array and associated logical drives to change to a degraded state. This indicates that the array has lost RAID redundancy. For RAID 1 or 6 arrays, this is only a partial loss of redundancy.

If a standby hotspare drive with the same (or greater) capacity and performance characteristics is available, then it takes over from the failed drive. Reconstruction of data

onto the hotspare starts automatically. Once reconstruction of all associated logical drives is complete, the array returns to an Optimal state. At this point, the failed drive slot is still associated with the array. The hotspare drive remains assigned as a hotspare, but assumes a temporary association with the array.

Figure 5-104 shows both the physical and logical views in Storage Manager when a disk fails in a redundant array. There is a clock symbol next to one of the logical drives associated with the degraded array indicating that reconstruction is in progress on that logical drive. A progress bar is displayed when the logical drive is selected.

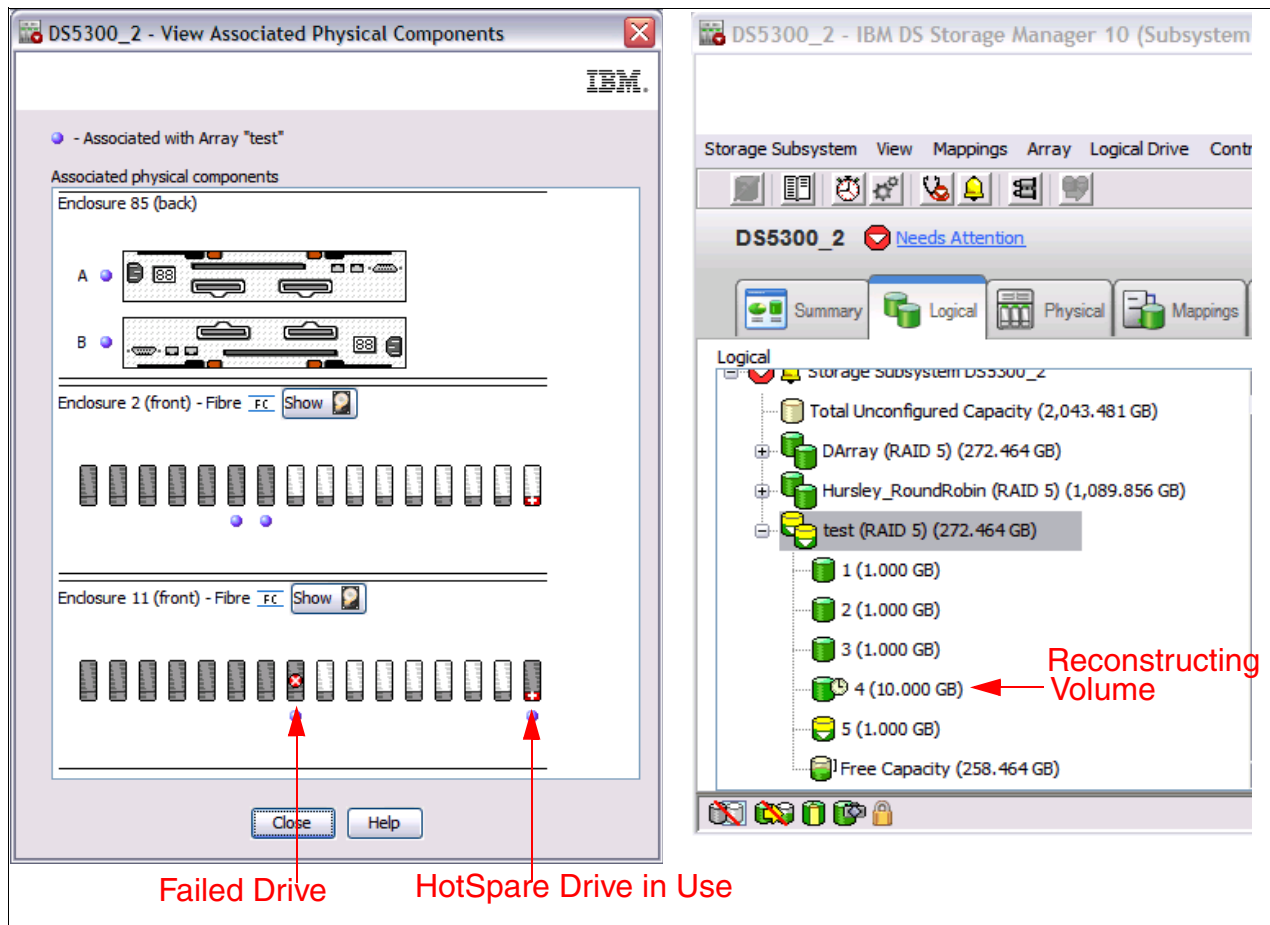


Figure 5-104 Storage Manager view after disk failure

At this point, we have a choice:

- ▶ The simplest and most common solution is to physically replace the failed disk. This results in an automatic copyback operation from the hotspare onto the new drive. When complete, the hotspare returns to an unassigned hotspare role.
- ▶ The alternate solution is to make another disk a permanent replacement for the failed drive. When we right-click the icon for the array with the failed disk in the logical view, we are given the Replace Drives option, as shown in Figure 5-105 on page 414. This menu option is normally grayed out when all drives in the array are optimal.

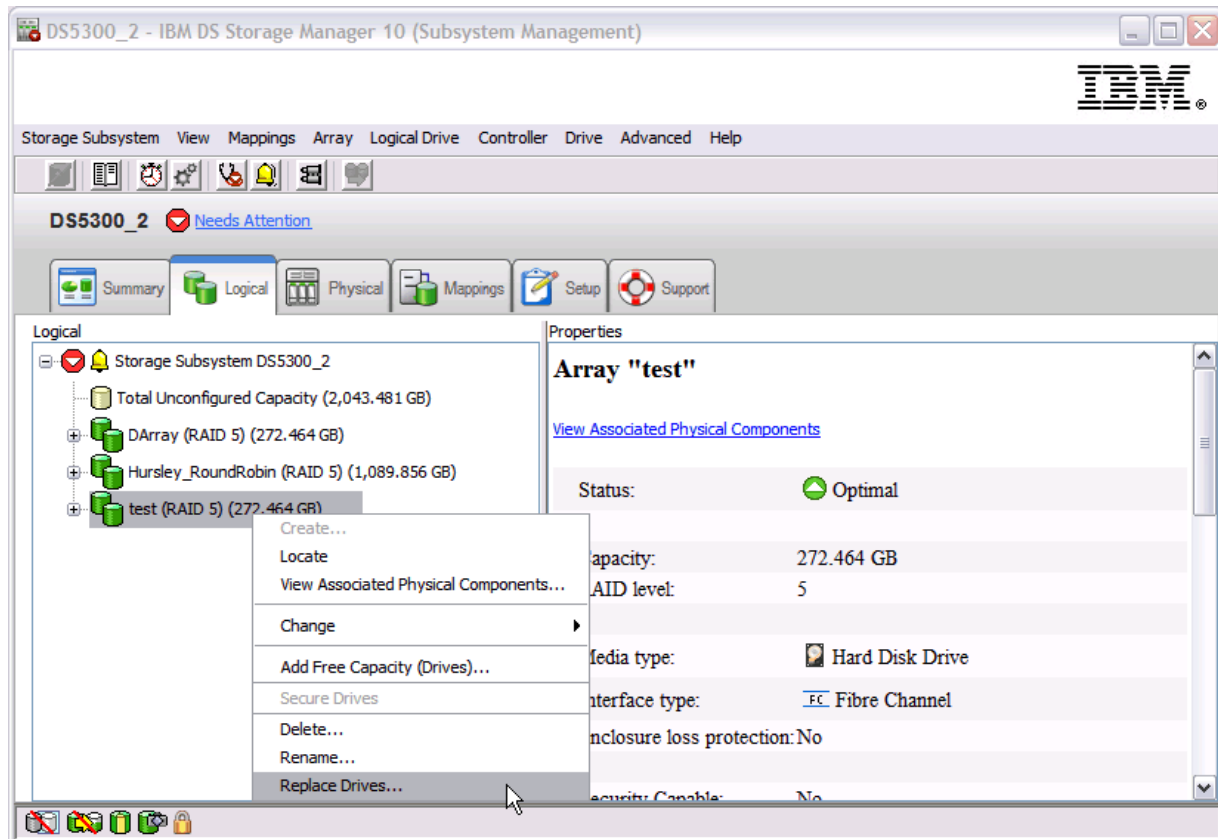


Figure 5-105 Replace drive

A new window appears showing the failed drive at the top and a list of potential replacement drives beneath, as shown in Figure 5-106 on page 415. This allows us to make the hotspare drive or any other drive of equal capacity and type (FC, SATA, or SSD) a permanent replacement for the failed drive by selecting the drive and click on **Replace Drive** button.

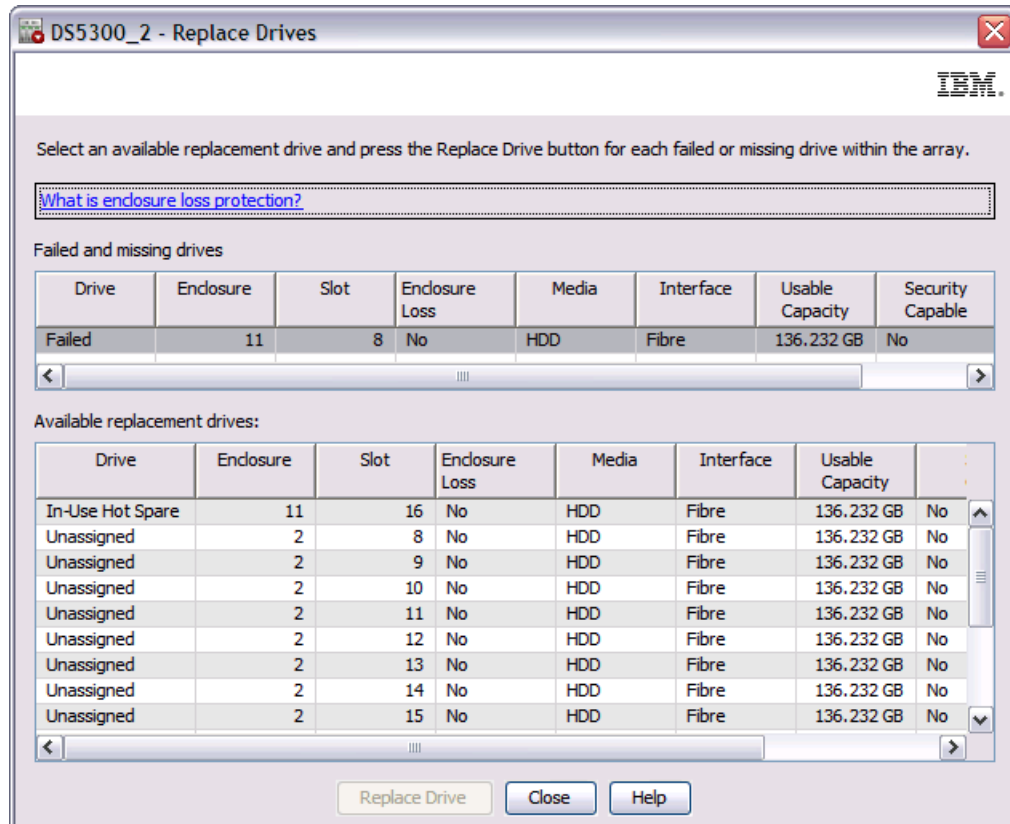


Figure 5-106 Replace Drives window

The straightforward option #1 is preferred in most cases, as all disks in the array remain in unchanged positions after the drive replacement. However, if drive positions were not an important factor during the initial planning, then option #2 might be considered.

The Replace Drives option can also be used as a concurrent method of migrating individual drives to new locations within the same storage subsystem. To do so, we need to ensure that the target drive is the only hotspare of the same capacity and type as the source. Then we can fail the source drive from Storage Manager by selecting it and navigating to **Advanced** → **Recovery** → **Fail drive**. When the target hotspare drive takes over, we can use the same procedure described in step #2 to make it the permanent replacement.

Disk replacement

The amber fault LED on the front of the drive indicates that it is in a powered down state and ready for replacement. To replace the disk, perform these steps:

1. Release the latch on the disk by pressing on the inside of the bottom of the tray handle.
2. Pull the tray handle out into the open position and slide the drive out.
3. Wait for at least 60 seconds before inserting the replacement drive. Gently push the new disk into the empty bay until the hinge of the tray handle latches beneath the storage subsystem enclosure bezel and then push the tray handle down into the closed (latched) position.

The amber fault LED on the front of the drive will flash while the drive is spinning up. When complete, the new drive appears in the Storage Manager physical view and copyback from hotspare starts automatically.

In cold climates, we recommend allowing the replacement disk to acclimatize within the drive slot for at least one hour before pushing it in fully. This reduces the risk of early life failures as the CRU drive is introduced into a controlled data center environment from a delivery vehicle. The sudden change in temperature and humidity can result in a buildup of condensation. The drive bays must never be left empty for an extended period, as this affects the internal airflow within the enclosure.

Note: Be sure that drive status is Failed before remove it otherwise the new drive inserted result as By-passed drive.

5.10.2 Managing disks with an impending drive failure error

The DS5000 controllers are constantly monitoring the status of the disk drives. A Predictive Failure Analysis (PFA) error is logged against the drive whenever a sufficient level of errors are detected and regarded as a concern yet the drive remains usable. This should be regarded as a warning that the drive is deteriorating and likely to fail in the near future. This triggers the audible enclosure alarm to sound (unless disabled) and the subsystem appears in a non-optimal state. A critical event is logged in MEL and the Recovery Guru button starts flashing. All critical events are sent to the SNMP management console or to the e-mail recipient that you have configured to receive alert notifications (you set these notifications by selecting **Edit** → **Configure Alerts** in the Enterprise Management window).

Recovery Guru reports three levels of impending drive failure:

Low risk	This is when a PFA threshold is exceeded on an unassigned drive or standby hotspare drive. The suspect drive should be replaced whenever possible.
Medium risk	When a PFA threshold is exceeded on a drive that is a member of a RAID 1, 3, 5, or 6 array. If the drive fails, then you might lose redundancy. The suspect drive should be replaced at the earliest opportunity.
High risk	When a PFA threshold is exceeded on a drive that is a member of an array where no more drives can fail without losing data. This is either a RAID 0 array or a degraded RAID 1, 3, 5, or 6 array. Immediate action should be taken to avoid data loss. We discuss some of the possible recovery actions later in this section.

When impending drive failure is detected, the affected disk remains powered and spinning.

With low or medium risk PFAs, the recovery actions are nondisruptive. The affected drive needs to be manually failed before it can be safely replaced. This is performed in the Storage Manager Subsystem Management window physical view by highlighting the affected drive and selecting **Advanced** → **Recovery** → **Fail drive**. Once in a failed state, the drive can be handled as a normal faulty drive with the procedure described in 5.10.1, “Managing disk failures” on page 412.

The recovery options for High Data Availability Risk are different. It is a good idea to back up all data on the affected logical drives and then proceed with the steps in either “PFA warning on a disk in a RAID 0 array” or “PFA warning on a disk in a degraded array” on page 417.

PFA warning on a disk in a RAID 0 array

An array is configured without redundancy (RAID 0) with the understanding that a single disk failure results in data loss. Only temporary or non-critical data should be stored on the associated logical drives. Therefore, the main PFA recovery action for RAID 0 arrays is a

disruptive procedure with all associated LUNs being inaccessible while the affected drive is replaced and data restored.

Perform these steps:

1. Stop all I/O to the affected logical drives.
2. Volume Copy can be used as an alternative to tape backup and restore. This function is only available with the optional premium feature. If any of the affected logical drives are also source or target logical drives in a Volume Copy operation that is either Pending or In Progress, you must stop the copy operation before continuing. Go to the Copy Manager by selecting **Logical Drive** → **VolumeCopy** → **Copy Manager**, highlight each copy pair that contains an affected logical drive, and select **Copy** → **Stop**.
3. If you have FlashCopy logical drives associated with the affected logical drives, these FlashCopy logical drives will no longer be valid. Perform any necessary operations (such as backup) on the FlashCopy logical drives and then delete them.
4. Highlight the affected drive in the Physical View of the Subsystem Management window and select **Advanced** → **Recovery** → **Fail Drive**. The amber fault LED illuminates on the affected disk. The affected logical drives become Failed.
5. Replace the failed drive.
6. Highlight the array associated with the replaced drive in the Logical View of the Subsystem Management window and select **Advanced** → **Recovery** → **Initialize** → **Array**. The logical drives in the array are initialized, one at a time.

To monitor initialization progress for a logical drive, highlight the logical drive in the Logical View of the Subsystem Management window and select **Logical Drive** → **Properties**. Note that after the operation in progress has completed, the progress bar is no longer displayed in the Properties dialog.

When initialization is completed, all logical drives in the array have the Optimal status.

7. Use operating system tools to re-discover the initialized LUNs.
8. Restore data from backup or recreate any Volume Copy relationships by highlighting the copy pairs in the Copy Manager (select **Logical Drive** → **VolumeCopy** → **Copy Manager**) and selecting **Copy** → **Re-Copy**.

It might also be possible to add redundancy by changing the RAID level if sufficient spare drives are available. If successful, this alters the PFA risk level from high to medium, allowing the disk to be replaced without disruption. However, there will be data loss if the affected disk fails during this operation.

PFA warning on a disk in a degraded array

For the array to be in a degraded state, there must already be a failed disk when the PFA is detected on another disk in the same array. Reconstruction to a hotspare might already be in progress. Two replacement disks will be required. In this scenario, it is important to replace the failed disk as soon as possible by performing the following steps:

1. Although not required, I/O to the affected logical drives should be stopped to reduce the possibility of inducing a failure on the PFA disk before the failed disk is replaced.
2. If a standby hotspare drive is not available, replace the failed disk.
3. Monitor the progress of reconstruction on the affected logical drives or change the reconstruction rate by highlighting the logical drive in the Logical View of the Subsystem Management window and then selecting **Logical Drive** → **Properties**. Note that after the operation in progress has completed, the progress bar is no longer displayed in the Properties dialog.

4. When all affected logical drives have returned to the Optimal status, the PFA risk level reduces from high to medium. At this point, it safe to resume I/O to the affected logical drives.
5. Highlight the PFA flagged drive in the Physical View of the Subsystem Management window and select **Advanced** → **Recovery** → **Fail Drive**. The amber fault LED for the affected disk illuminates. The affected logical drives become degraded until reconstruction is complete.
6. Replace the failed drive(s).

5.10.3 Monitoring Solid State Drives (SSD)

When we look at the SSD drive properties in the Storage Manager Subsystem Management physical view, we see some parameters that are unique to SSD drives (see Figure 5-107).


Media type:	 Solid State Disk
Interface type:	FC Fibre Channel
Drive path redundancy:	OK
Wear life monitoring:	Enabled
Average erase count:	0%
Spare blocks remaining:	99%

Figure 5-107 SSD drive properties

A flash-based SSD has a limited wear life before individual memory locations can no longer reliably persist data. The disk drive continuously monitors itself and reports its wear life status to the controller. Two mechanisms exist to alert you that an SSD is nearing the end of its useful life: average erase count and spare blocks remaining. You can find these two pieces of information in the disk drive properties, which you can see in the storage management software by selecting a disk drive on the Physical tab.

The average erase count is reported as a percentage of the rated lifetime. When the average erase count reaches 80 percent, an informational event is logged to the Major Event Log (MEL). At this time, schedule the replacement of the SSD. When the average erase count reaches 90 percent, a critical event is logged, and a Needs Attention condition occurs. At this time, replace the SSD as soon as possible.

The spare blocks remaining are reported as a percentage of the total blocks. When the spare blocks remaining falls below 20 percent, an informational event is logged to the MEL. At this time, schedule the replacement of the SSD. When the spare blocks remaining falls below 10 percent, a critical event is logged, and a Needs Attention condition occurs. At this time, replace the SSD as soon as possible.

5.10.4 Managing battery issues

On DS5000 storage subsystems, the battery unit contains lithium-ion battery packs that can maintain power to the RAID controller caches for up to thirty minutes to flush cache memory to flash memory modules in the event of a power loss.

This battery unit provides backup power to each controller's cache memory. Each battery unit contains a sealed, rechargeable lithium-ion battery. The battery unit can maintain data in the cache for three days.

On both the DS5000 storage subsystems, the battery should not be replaced until it is marked failed by the controller. If the batteries are shown as expired, use the reset battery age function in the Storage Manager Subsystem Management window to reset the age.

5.11 Replacing adapters (HBA) and storage controllers

The logical volumes created in the DS5000 are mapped to the hosts Fibre Channel adapters worldwide name (WWN). Replacing an HBA affects the mappings in both the DS5000 and the SAN zoning configuration if the HBAs are not directly attached.

Consider the following items:

- ▶ Host adapter replacement

If for any reason an HBA is replaced and you are not using the default group to map your logical volumes in the DS5000, you will not see any disks through the new controller until the mappings are regenerated by replacing the old HBA WWPN with the new adapter WWPN.

Also, update your SAN zoning configuration after changing the HBA to allow the new WWPN to communicate with the target DS5000.

- ▶ DS5000 controller replacement

Under rare circumstances, it is possible that after replacing a failed DS5000 controller, the World Wide Port Names could be changed on the resident as well as the replaced controller. If a user has his Fibre Channel switch zoned by WWPN, this will cause a loss of access. The zoning configuration on Fibre Channel switches must be adjusted. It is also possible to see this exceptional condition after performing a DS5000 controller firmware upgrade.

There is a feature for automatic code synchronization of the controllers in case one is replaced. This ensures that both controllers execute the same level of firmware.

5.12 HBAs and operating system tools

This section provides practical information for problem determination on specific OS platforms and HBAs when you use Storage Manager utilities such as mppUtil and SMDevices, and other common operating system (OS) dependent commands used for reviewing disks status and data collection.

5.12.1 Brocade HBA and Brocade Host Configuration Manager (HCM)

This section gives a brief introduction to the Host Configuration Manager (HCM) for Brocade FC HBAs.

Brocade offers different software to manage their HBAs. A list of software bundles that are downloadable from the Web can be found at the following address:

http://www.brocade.com/sites/dotcom/services-support/drivers-downloads/HBA/HBA_IBM.page

The software bundles consist of the following items:

- ▶ Brocade Adapter Software installer

This package enables a single step installation for all software components, including Host Connectivity Manager (HCM), Drivers, Firmware, Agent, Brocade Command Utility (BCU), and APIs.

- ▶ Driver

This is a single driver package (per OS and server platform) for supporting all Brocade HBAs. The drivers will be packaged appropriately for each operating system.

- ▶ Firmware

The adapter firmware is bundled as part of the driver, and will be automatically updated after the driver is updated.

- ▶ Multi-boot code image

A multi-boot code image (BIOS/EFI) allows an adapter to be plugged into a server to support boot from SAN functionality for x86, IEM64T, AMD64, and IA64 server platforms. Server administrators can set up a bootable LUN in the SAN through an easy to use configuration utility menu.

- ▶ Driver Update Disks (DUDs)

DUDs (provided in ISO and zip format) are needed to install the drivers during an OS installation of a LUN attached to the SAN.

- ▶ LiveCD

The LiveCD can be used to boot up diskless or OS-less servers. The Brocade Command Utility (BCU) can then be used to update the boot code.

- ▶ Agent

The management agent is automatically installed as part of the driver installation process and can be started manually or automatically. This agent is required to manage Brocade HBAs through HCM.

- ▶ Host Connectivity Manager (HCM)

HCM is the Brocade Adapter management tool that has an intuitive and easy-to-use graphical user interface (GUI). This is a Java based application and can run on standard servers and workstations or a dedicated management server. HCM is used to install, configure, and manage local as well as remote adapters from a single interface. In addition, data center administrators can use the tool for detailed configuration tasks, driver and firmware upgrades, device level monitoring, and comprehensive diagnostics.

- ▶ Brocade Command Line Utility (BCU)

Brocade also includes the Brocade BCU, which is a command-line utility used to configure and manage local HBAs from the console. Many of the GUI configuration options are also available through the BCU. Run the **bcu -help** command to obtain more information about BCU options.

- ▶ APIs

SNIA HBA API V2.0 is supported. For both Windows and Solaris, the SNIA HBA API libraries are part of the OS. For Linux and VMware, separate API libraries are provided as part of the driver package.

Using HCM

The minimum set of requirements to support HCM include:

- ▶ Brocade FC HBAs (BR-815, and BR-825).
- ▶ A single-processor or multiprocessor server or workstation.

- ▶ Pentium III with 450 MHz (or equivalent) or greater for Windows, Red Hat, Novell, Solaris x86, and VMware.
- ▶ Sun Ultra 60 for Solaris SPARC.
- ▶ Internet Explorer (6.0 or later), or Firefox (2.0 or greater).
- ▶ TCP/IP protocol stack for communicating with the management agents.

After installing Brocade HCM, you can start it from the Windows Start menu.

HCM is secured by user and password, as shown in Figure 5-108. The default user is *administrator* with the default password of *password*.

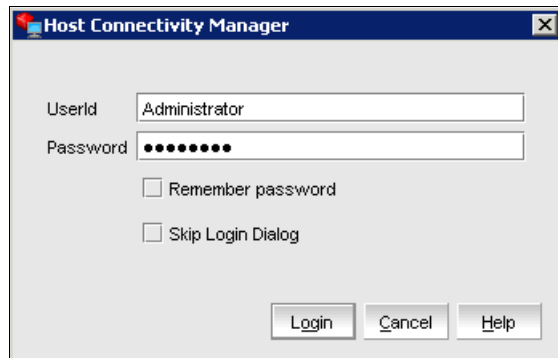


Figure 5-108 Agent login window

After a successful login, the HCM main window opens as shown in Figure 5-109 on page 422.

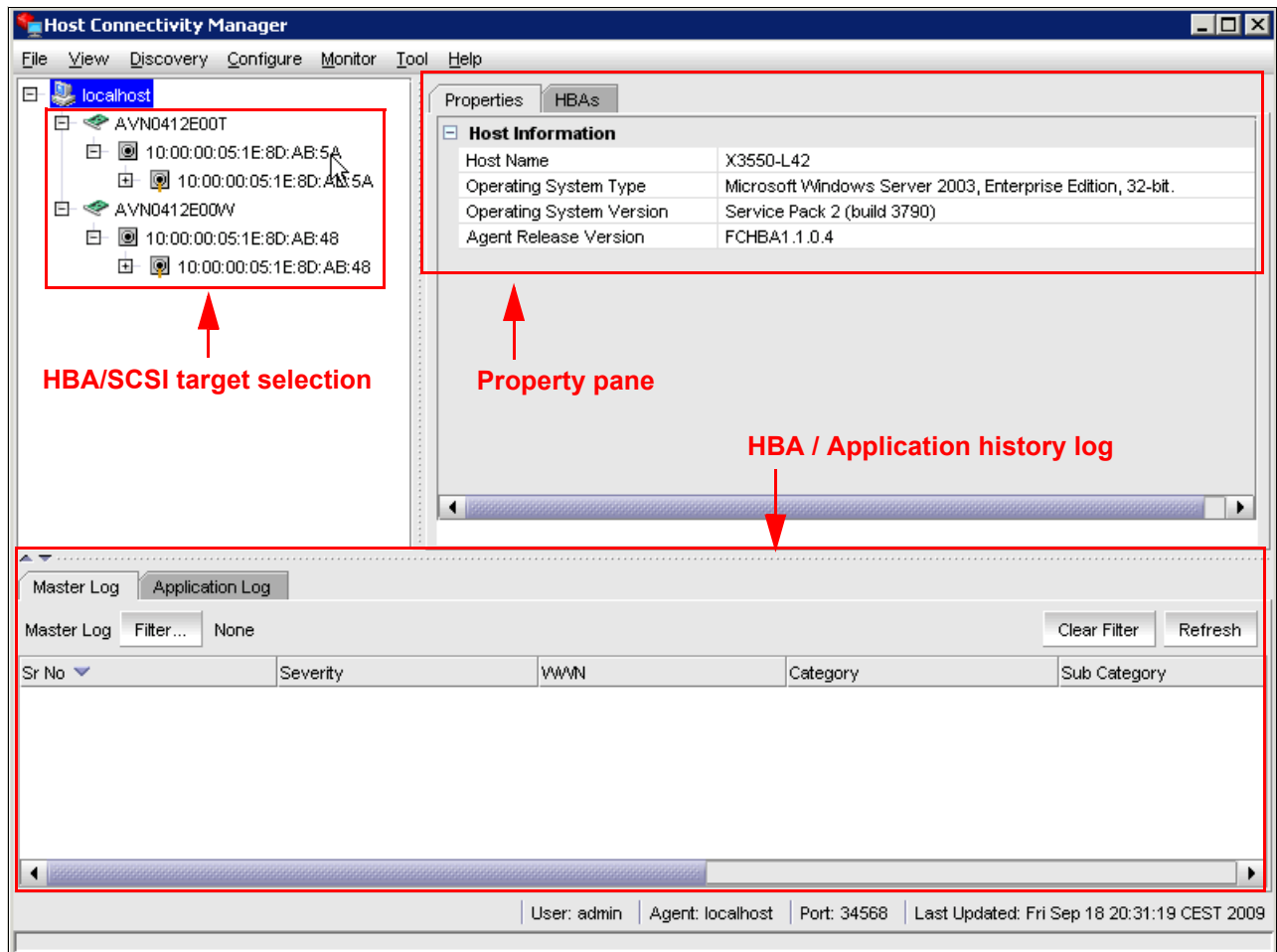


Figure 5-109 HCM main window

HMC window shows, in the left pane, all the adapters and all ports, as well as all current connected targets with their available LUNs. Upon selecting a HBA, port, or target, the right pane will show the corresponding properties for that object. The bottom pane displays a change history of the configuration done by the user. By going through the menu items, you can perform various actions on the adapter and ports and retrieve much information from the targets.

With HCM, you can:

- ▶ Perform HBA firmware update, also known as Boot Code Image (Figure 5-110 on page 423).
- ▶ Perform data collection (Support Save) and HBA settings backup (Figure 5-111 on page 423).
- ▶ Configure HBA/port settings, persistent binding, and diagnostics (Figure 5-112 on page 423).

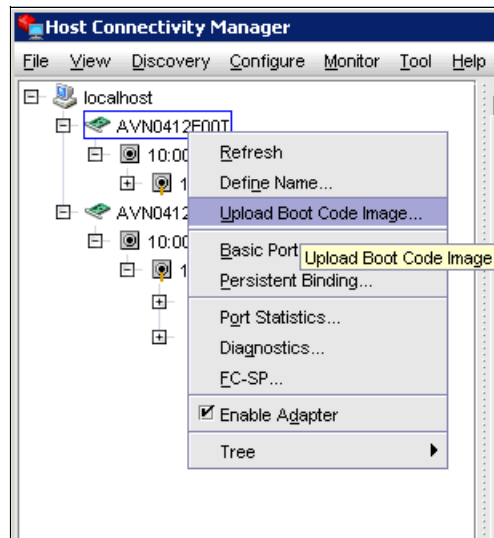


Figure 5-110 HCM Update HBA firmware

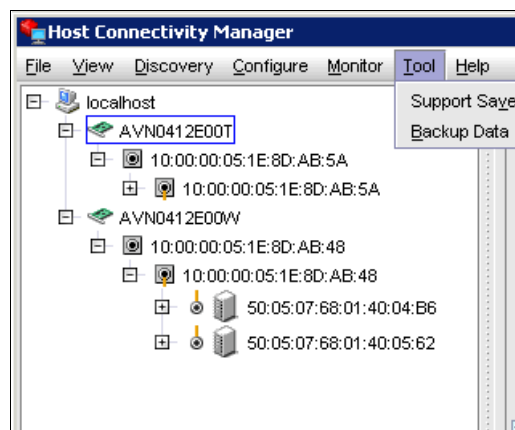


Figure 5-111 HCM Tool menu

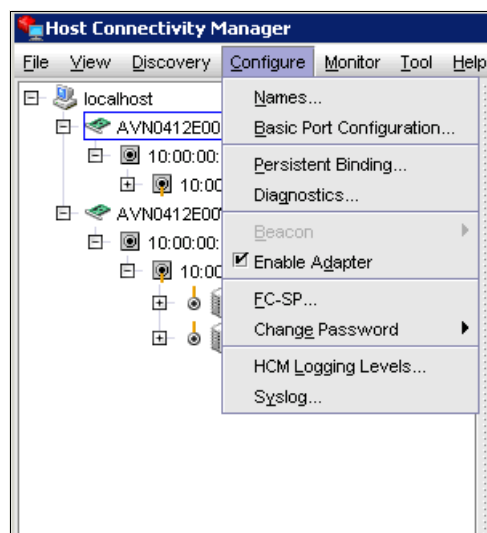


Figure 5-112 HCM Configure menu

Data collection

You can collect a variety of information about installed Brocade adapters, such as the firmware version installed, operational status, port speed, WWN, PCI data, configuration data, flash status, and other details, in order to troubleshoot the use of BCU commands, HCM menu options, and host operating system commands. This function is named Support Save.

Support Save

The Support Save feature is an important tool for collecting debug information from the driver, internal libraries, and firmware. You can save this information to the local file system and send it to support personnel for further investigation.

Use one of the following options to launch this feature:

- ▶ In HCM, launch Support Save from the Tools menu (see Figure 5-113).
- ▶ Using the Brocade Command Line Utility (BCU), run the **bfa_supportsave** command.
- ▶ Using your Internet browser (Internet Explorer 6 or later or Firefox 2.0 or later), you can collect **bfa_supportsave** output if you do not have root access, do not have access to file transfer methods such as FTP and SCP, or do not have access to the Host Configuration Manager (HCM).
- ▶ A **bfa_supportsave** collection can also occur automatically for a port crash event.

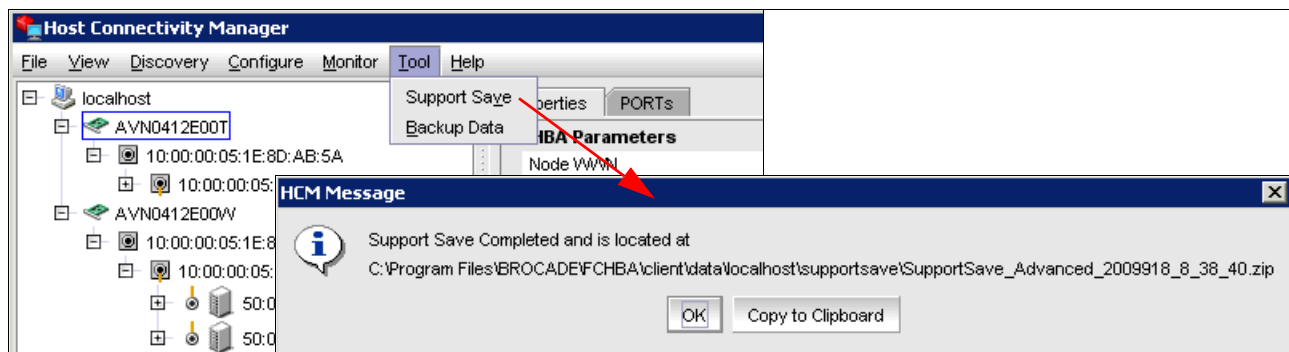


Figure 5-113 HCM Support Save

The Support Save feature saves the following information:

- ▶ Adapter model and serial number
- ▶ Adapter firmware version
- ▶ Host model and hardware revision
- ▶ All support information
- ▶ Adapter configuration data
- ▶ All operating system and adapter information needed to diagnose field issues
- ▶ Information about all adapters in the system
- ▶ Firmware and driver traces
- ▶ Syslog message logs
- ▶ Windows System Event log .evt file
- ▶ HCM GUI-related engineering logs
- ▶ Events
- ▶ Adapter configuration data
- ▶ Environment information
- ▶ Data.xml file
- ▶ Vital CPU, memory, and network resources
- ▶ HCM Agent (logs and configuration)
- ▶ Driver logs
- ▶ Status and states of all adapter ports

5.12.2 Emulex HBA tools

This section briefly describes the tools used to maintain IBM branded Emulex HBAs.

Emulex offers this software to drive and manage the HBAs, and it includes the following tools:

- ▶ **Driver**
A host computer software component that controls the operation of peripheral controllers or HBAs attached to the host computer. Drivers manage communication and data transfer between applications and I/O devices, using HBAs as agents.
- ▶ **The HBAnywareutility (HBAnyware)**
This utility allows you to perform installation and configuration tasks on remote and local HBAs.
- ▶ **Security Configurator**
The HBAnyware security package allows you to control which HBAnyware systems can remotely access and manage HBAs on other systems in a Fibre Channel (FC) network.
- ▶ **LightPulse utility (lputilnt)**
This driver-specific utility for the Storport Miniport and SCSIport Miniport drivers provides a user-friendly interface that allows you to examine, manage, and configure installed HBAs. lputilnt is automatically installed when you install the HBAnyware utility.

To obtain the latest information for Emulex HBAs, go to the following address:

<http://www.ibm.com/support/entry/portal/>

Installation instructions can be obtained from the Emulex Web site at the following address:

<http://www.emulex.com/downloads/ibm/fw-and-bootcode.html>

HBAnyware utility (HBAnyware)

The HBAnyware utility (HBAnyware) is a user-friendly graphical environment. Use HBAnyware to do any of the following actions:

- ▶ Discover local and remote hosts, host bus adapters (HBAs), targets, and LUNs.
- ▶ Reset HBAs.
- ▶ Set up persistent binding.
- ▶ Set HBA driver parameters.
- ▶ Set driver parameters simultaneously to multiple HBAs using Batch Update.
- ▶ Set global driver parameters to HBAs.
- ▶ Update firmware on the single HBA or multiple HBAs using Batch Update.
- ▶ Enable boot code.
- ▶ Run diagnostic tests on HBAs.
- ▶ Manage out-of-band HBAs.
- ▶ Manage local and in-band remote HBAs.
- ▶ Update EFIBoot (64-bit only).

To start HBAnyware for Windows, perform the following steps:

1. On the Windows desktop, select **Start** → **Programs** → **Emulex** → **HBAnyware**.
2. The initial discovery information for the host appears, as shown in Figure 5-114 on page 426.

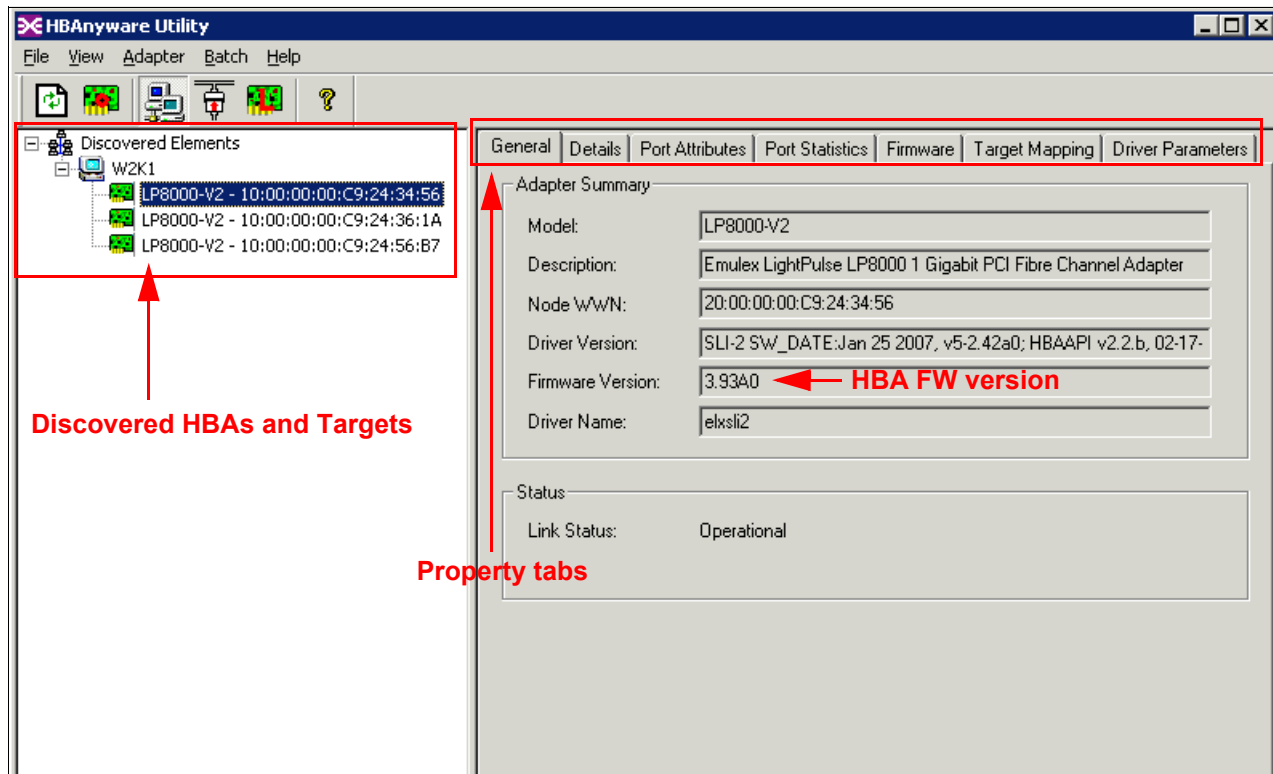


Figure 5-114 HBAAnyware Utility main window

The HBAAnyware utility contains five basic elements:

- ▶ Menu bar
- ▶ Toolbar
- ▶ Discovery tree
- ▶ Property tabs
- ▶ Status bar

5.12.3 Qlogic HBAs and SANsurfer (Windows/Linux)

The Qlogic SANsurfer is a graphical management interface program used to manage, configure, and diagnose Host Bus Adapters in servers running the Qlogic SANsurfer agent, which is available for Windows or Linux hosts. It is especially useful if you have hosts that are directly connected to the DS5000, as you can check for errors on the FC link of the HBA and troubleshoot path problems. Some of the features include:

- ▶ Timely and accurate detection of I/O failures
- ▶ Local and remote management of adapters
- ▶ Performance statistics
- ▶ Central control point in a network environment
- ▶ Diagnostics and utilities
- ▶ Firmware update

In this section, we provide an overview about how to use the tool with the DS5000 storage subsystem.

Setting the Qlogic SANsurfer client

You can find the latest version of the Qlogic SANsurfer at the IBM Disk Support Web site:

<http://www.ibm.com/support/entry/portal/>

Select your DS5000 model from the appropriate drop-down menu and select the **Download** tab on the right side of the page. Under the Drivers section for Qlogic FC2/4/8, you will find different packages for the Qlogic SANsurfer tool that correspond to different processor platforms with Linux or Windows.

Proceed with the installation. You have the option to install the agent and the manager separately. You can run the client from any workstation, while the agent must be installed on all the servers for which you want to manage the HBAs.

When you launch the SANsurfer application, you are prompted to specify a host to manage. Enter the IP or host name of the host running the agent, or leave the default as localhost if you are running the SANsurfer client from the server that you want to manage, as shown in Figure 5-115.

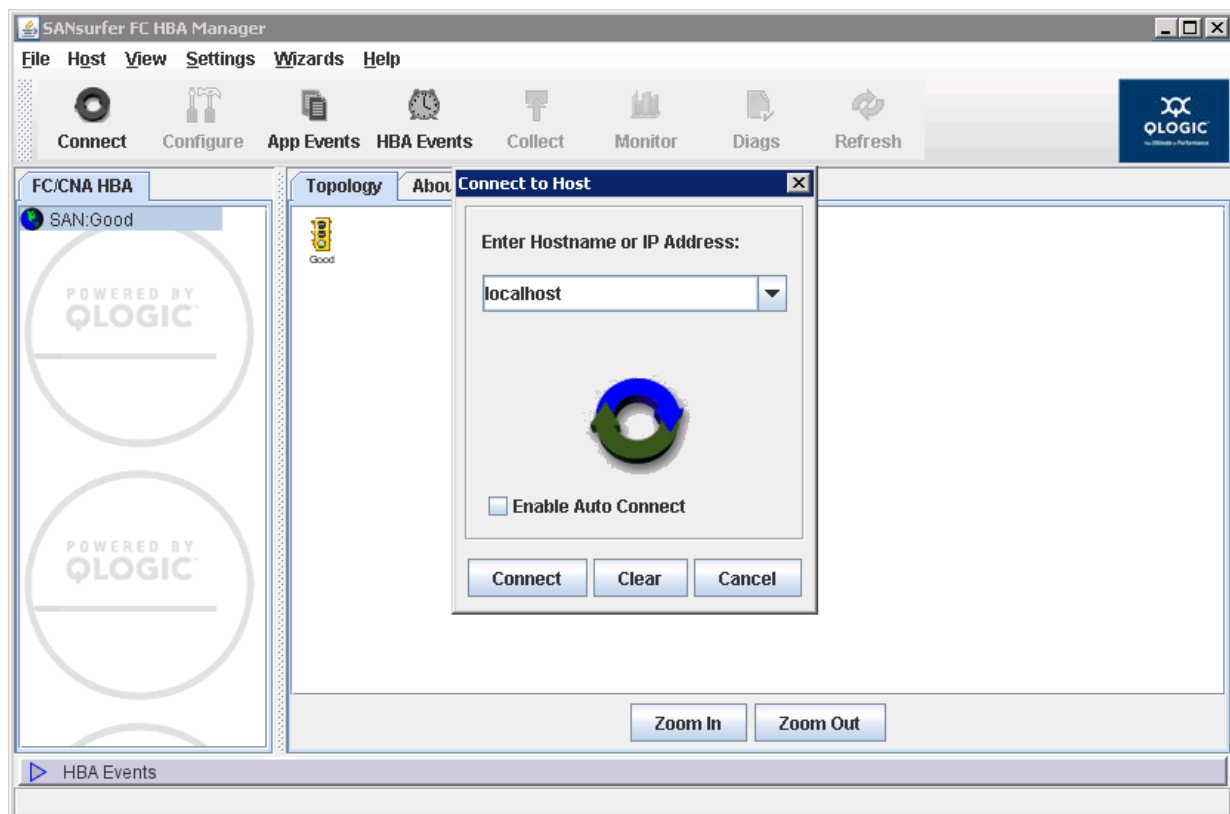


Figure 5-115 Qlogic SANsurfer FC HBA Manager view

Click **Connect** to start managing the HBAs on the specified host. At this point, you are returned to the HBA View window, and the host that you specified in the previous window is now displayed in the left pane (known as the HBA tree pane). The host bus adapters installed in the server appear below the host name as shown in Figure 5-116.

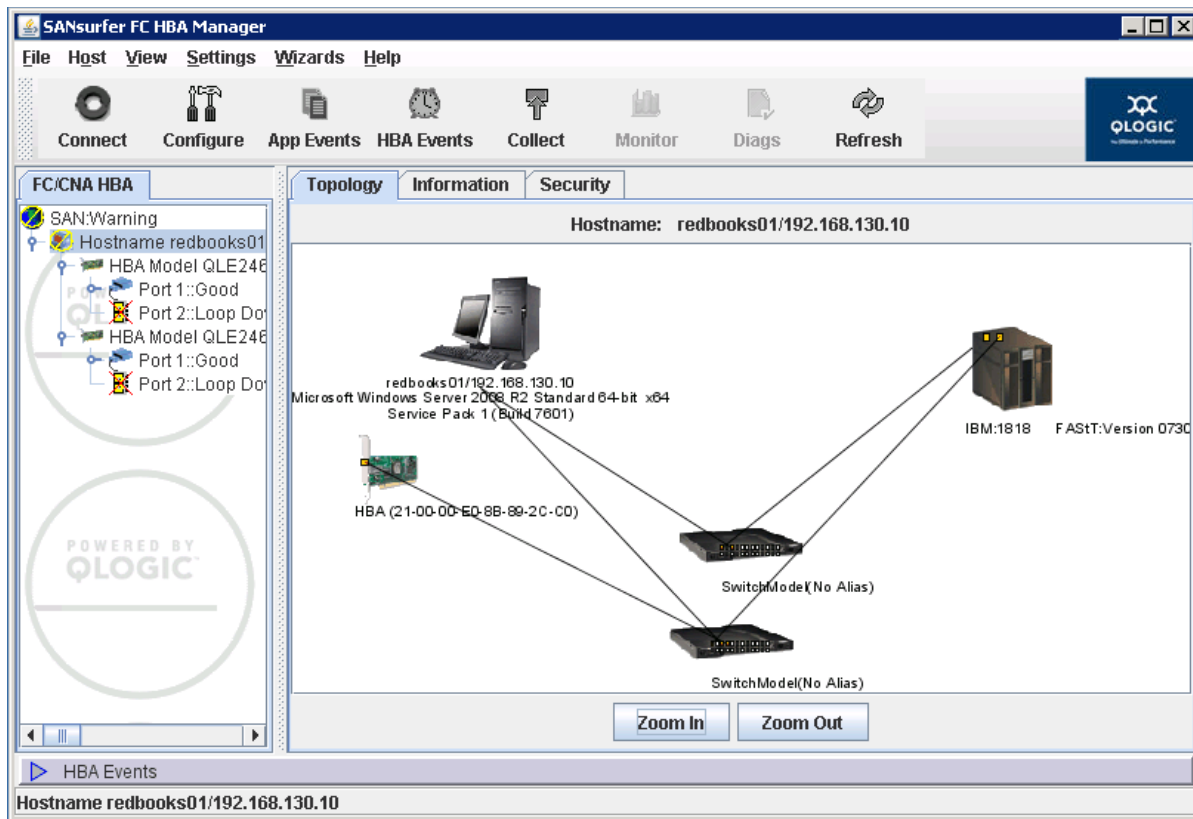


Figure 5-116 Qlogic SANsurfer Host view

Three tabs are displayed in the right pane (known as the Tab pane). They are:

- ▶ **Topology:** Contains a basic view of the topology of the currently connected server.
- ▶ **Information:** Contains basic information about the currently connected server, agent version running on the connected host, and OS version.
- ▶ **Security:** Contains security settings for the connected agent. This lets you set host security and application security.
 - Host access defines the authorized user with administrator or root privileges.
 - Application access specifies the password for changing settings on the HBAs (for firmware download or BIOS settings).

Viewing event and alarm logs

The Qlogic SANsurfer records an extensive amount of information to the event and alarm logs. The logs are saved as text files (alarms.txt and events.txt) in the folder where Qlogic SANsurfer is installed. Qlogic SANsurfer can parse and view these logs in a window. To view these logs, click **Application Event Log** or **HBA Event Log** from the view menu, or click the appropriate button on the button bar.

Using the Qlogic SANsurfer tools

When you click one of the host bus adapter ports in the HBA tree pane, the tab pane displays eight tabs, as shown in Figure 5-117.

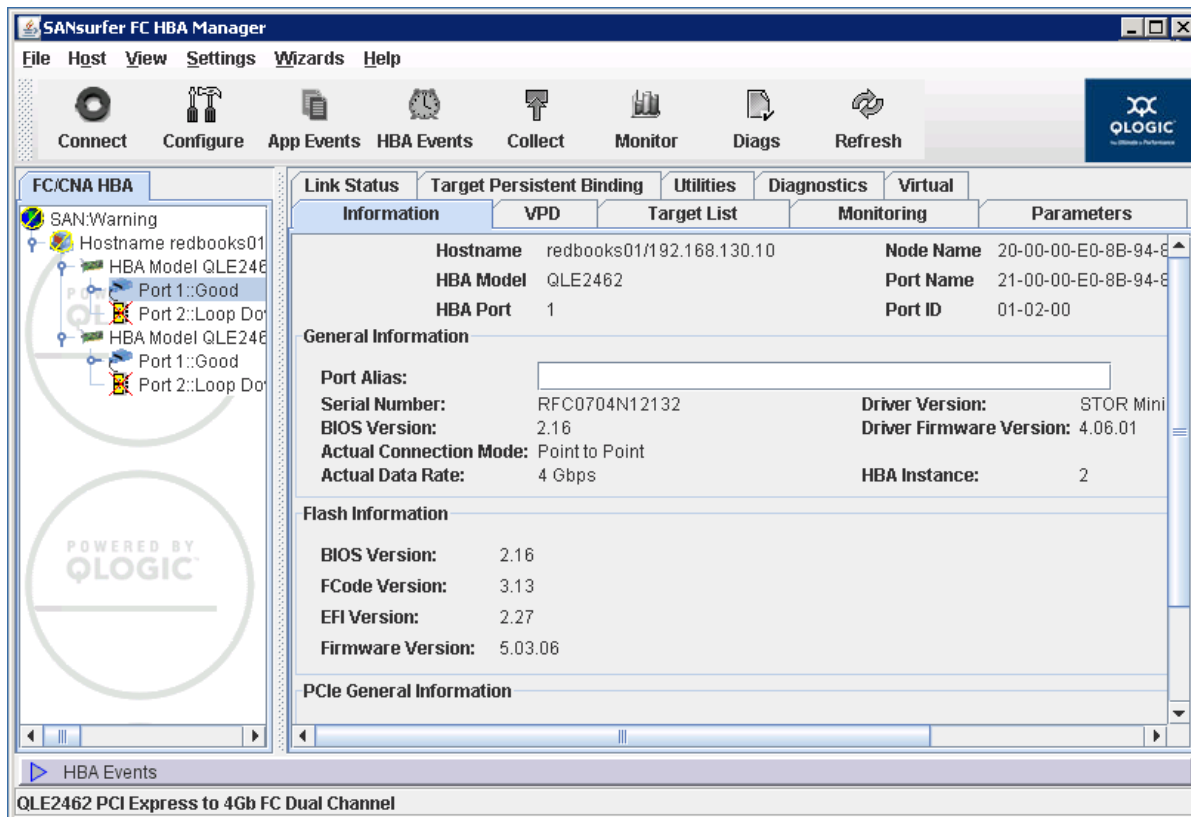


Figure 5-117 Qlogic SANsurfer FC HBA Manager view

The Qlogic SANsurfer has several tabs for the HBAs:

- ▶ **Information:** Displays general information about the server and Host Bus Adapters, such as worldwide name, BIOS, NVRAM, and driver version.
- ▶ **VPD:** Displays the Host Bus Adapter Vital Product Data.
- ▶ **Target List:** Displays the devices currently available to the host bus adapter.
- ▶ **Monitoring:** Displays a graph of the performance and errors on the host bus adapters over a period of time.
- ▶ **Parameters:** Displays the current settings and allows you to make remote configuration changes to the BIOS of the adapters.
- ▶ **Link Status:** Displays link information for the devices attached to an adapter connected to a host.
- ▶ **Target Persistent Binding:** Allows you to bind a device to a specific LUN.
- ▶ **Utilities:** Allows you to update the flash memory and HBA Parameters remotely.
- ▶ **Diagnostics:** Allows you to run diagnostic tests remotely.
- ▶ **Virtual:** Display defined virtual ports created for a single physical adapter port.

Monitoring

The Monitoring tab (Figure 5-118) displays the following information:

- ▶ HBA port errors: The number of port errors reported by the adapter device driver (connection problem from or to switches or hubs).
- ▶ Device errors: The number of device errors reported by the adapter device driver (I/O problems to the storage subsystem, and so on). This item usually gives the first hint about what path to the storage subsystem controller has a problem.
- ▶ Reset: The number of LIP resets reported by the adapter's driver. If you get increasing numbers, there might be a communication problem between the HBAs and storage.
- ▶ I/O count: Total numbers of I/Os reported by the adapter's driver.
- ▶ IOPS (I/O per second): The current number of I/Os processed by the adapter.
- ▶ BPS (bytes per second): The current numbers of bytes processed by the adapter.

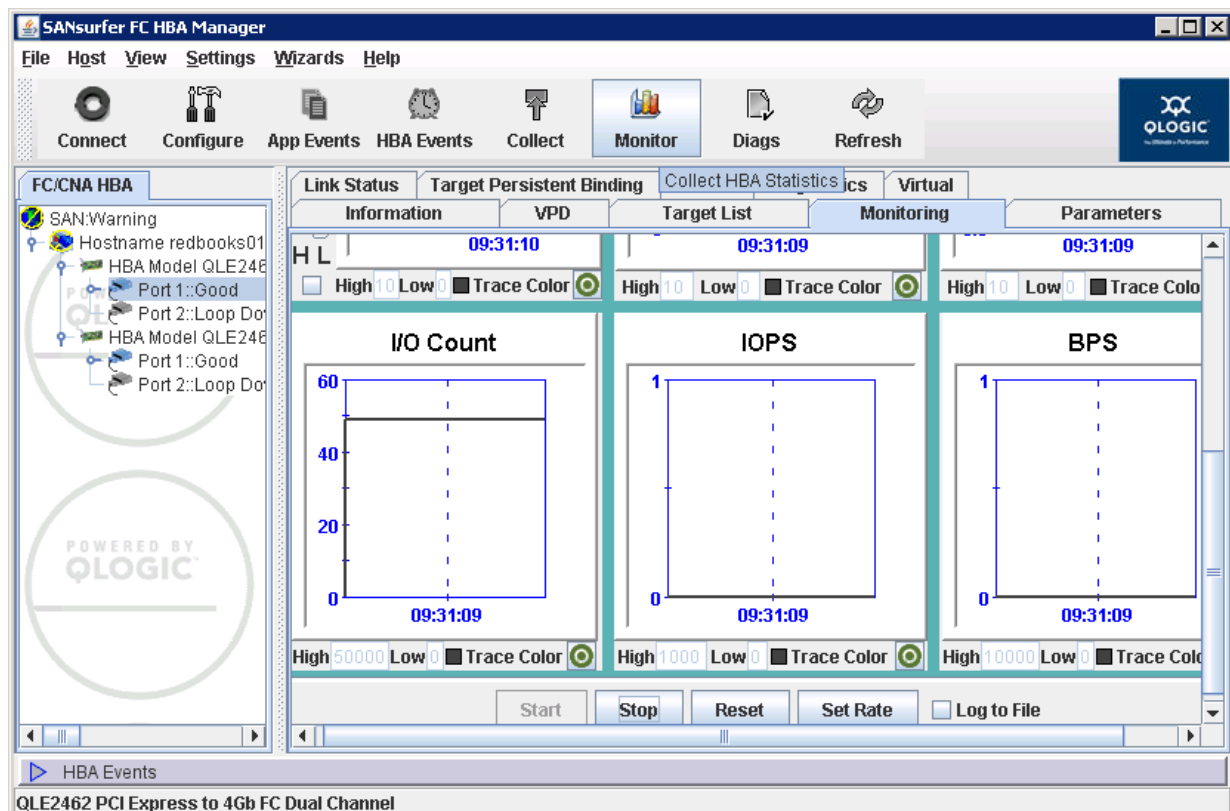


Figure 5-118 Monitoring tab

Link status

If you experience problems with connectivity or performance or you see entries from Multipath or HBA drivers, use the Link Status tab (Figure 5-119) to narrow down the device causing problems (faulty cable, SFPs, and so on).

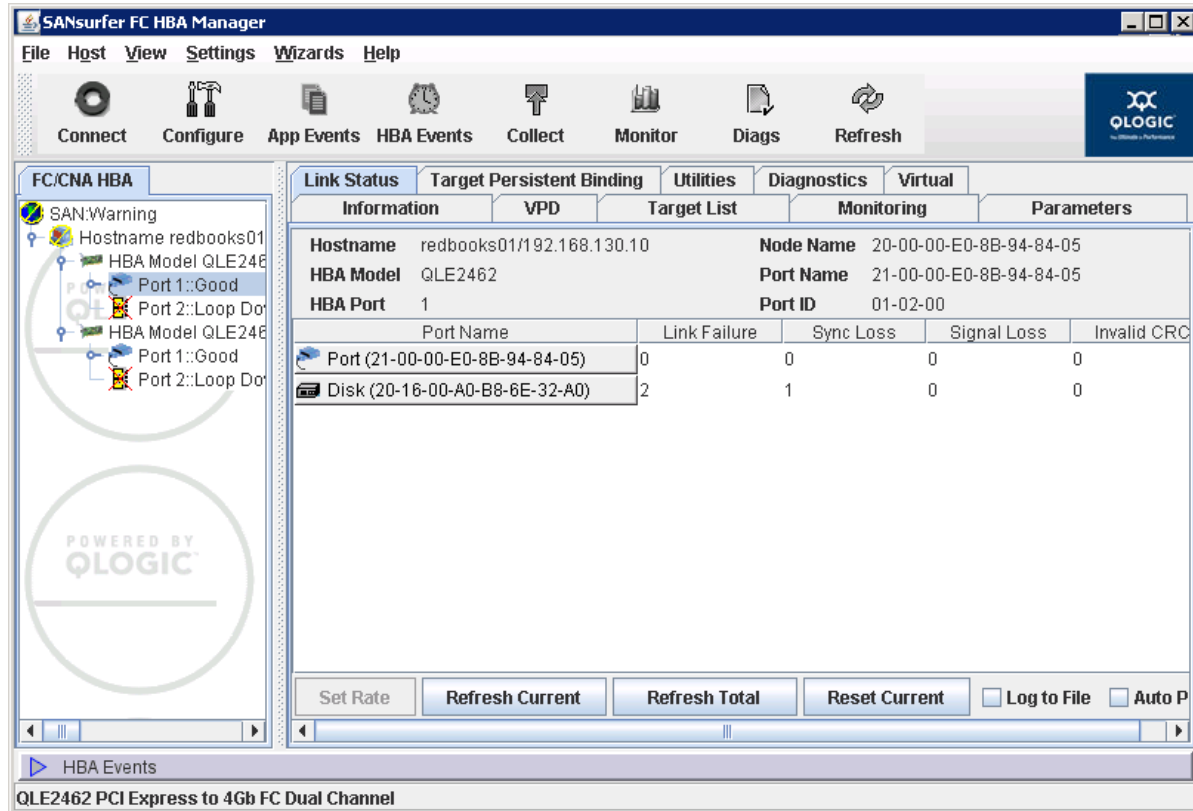


Figure 5-119 Link status tab

The following information can be retrieved from the Link Status window:

- ▶ Link failure: The number of times that the link failed. A link failure is a possible cause for a timeout (see the Windows Event Log).
- ▶ Sync Loss: The number of times that the adapter had to re-synchronize the link.
- ▶ Signal Loss: The number of times the signal was lost (dropped and re-connected).
- ▶ Invalid CRC: The number of cyclic redundancy check (CRC) errors that were detected by the device.

Diagnostics

You can use the Diagnostics tab to perform loopback and read/write buffer tests as shown in Figure 5-120 on page 432.

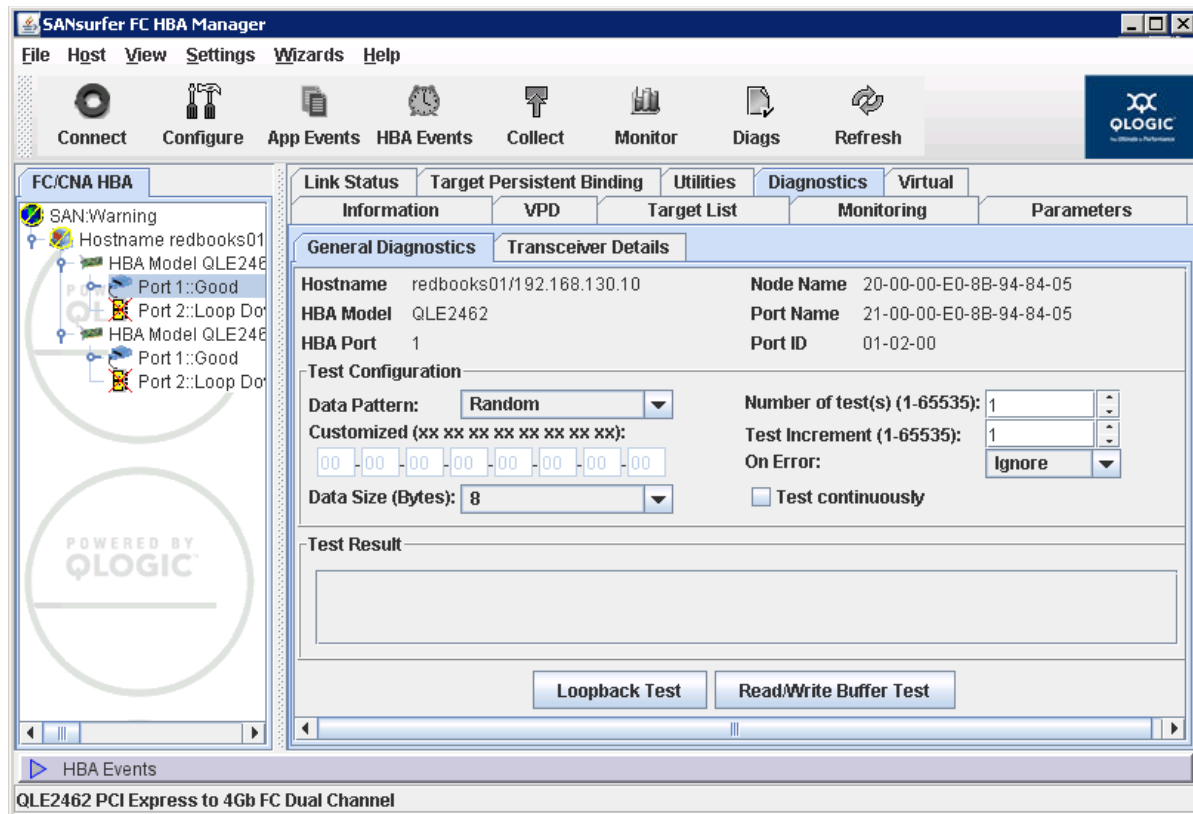


Figure 5-120 Qlogic SANsurfer Diagnostics tab

- ▶ The **Loopback Test** is internal to the adapter. The test evaluates the Fibre Channel loop stability and error rate. The test transmits and receives (loops back) the specified data and checks for frame CRC, disparity, and length errors.
- ▶ The **Read/Write Buffer Test** sends data through the SCSI Write Buffer command to a target device, reads the data back through the SCSI Read Buffer command, and compares the data for errors. The test also compares the link status of the device before and after the read/write buffer test. If errors occur, the test indicates a broken or unreliable link between the adapter and the device.

The Diagnostics tab has two sub tabs:

- ▶ General Diagnostics:
 - Identifying Information: Displays information about the adapter being tested.
 - Test Configuration: Contains testing options (like data patterns, number of tests, and test increments).
 - Loopback Test Results: Displays the results of a test showing whether the test passed or failed and error counters.
 - Test Buttons.
- ▶ Transceiver Details has two sub tabs:
 - General:
 - Media Information: shows transceiver details.
 - Diagnostic Data: shows temperature, Voltage, Tx and Rx powers value and thresholds.
 - Details: shows Optical Transceiver Digital Diagnostic Data.

Utilities

Qlogic SANsurfer can also be used to update the Flash Image, HBA driver and the HBA Parameters as shown in Figure 5-121. See “Update the HBA firmware using QLogic SANsurfer” on page 313 for instructions about updating the HBA firmware.

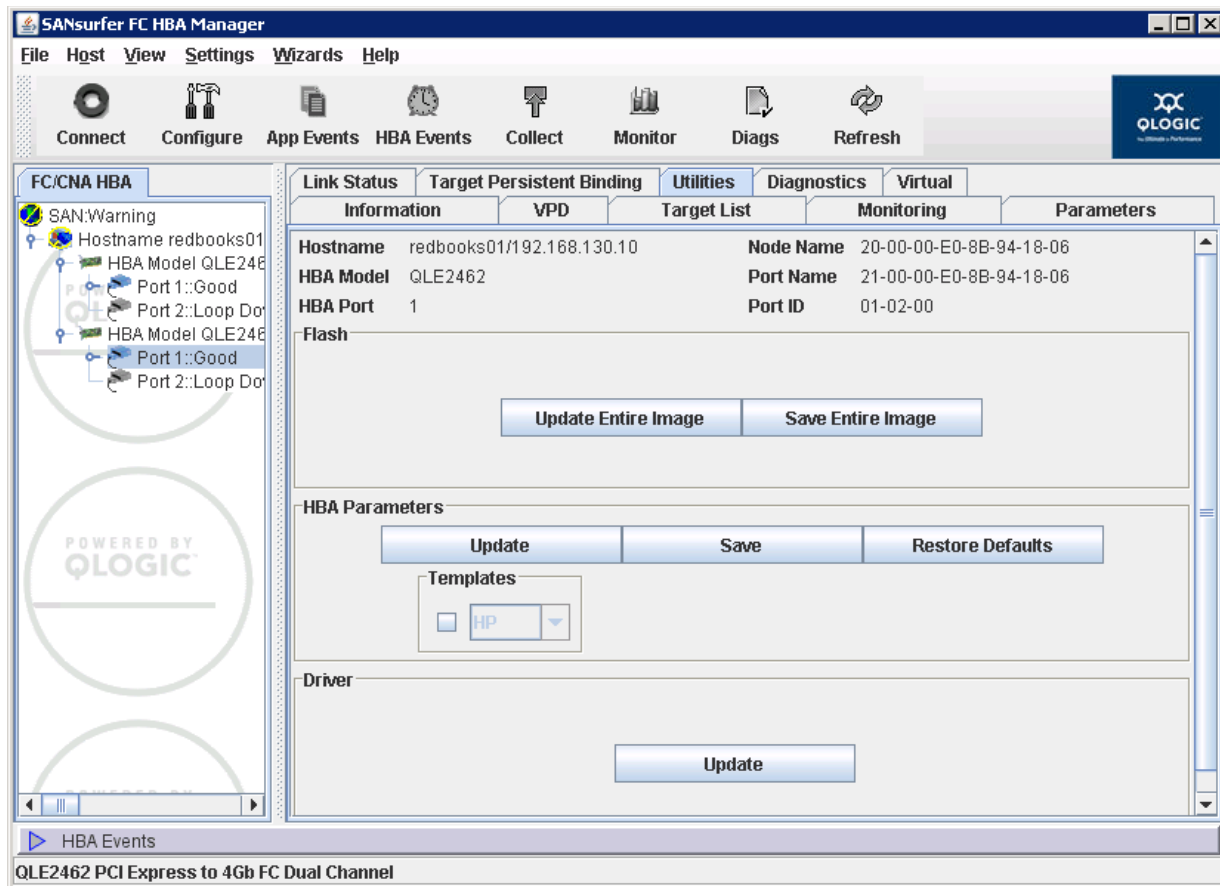


Figure 5-121 Qlogic SANsurfer utilities tab

Note: If you are installing your DS5000 for the first time, it's a Best Practice to update the HBA to the latest supported levels to minimize future exposures.

Displaying LUNs detected

The LUNs recognized by the HBAs are visible in the HBA tree view in the left pane and in LUN List tab, as shown in Figure 5-122.

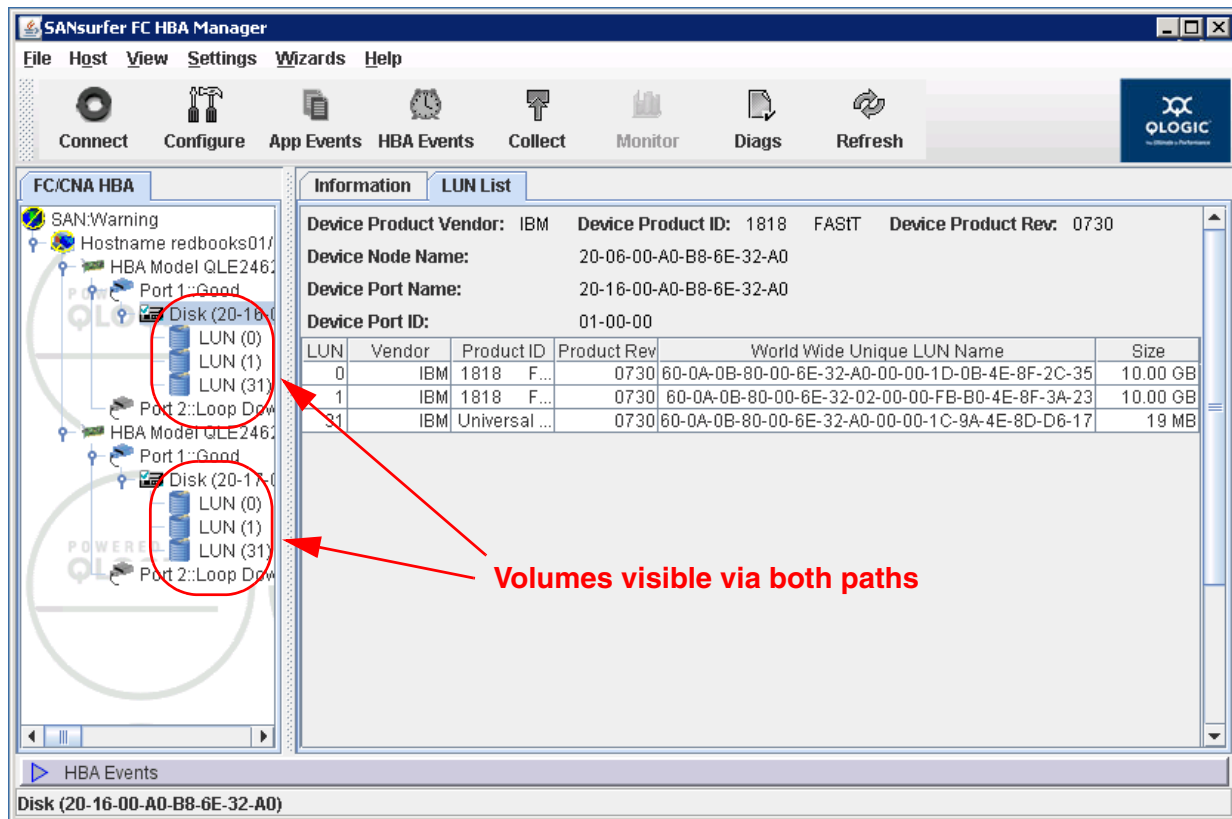


Figure 5-122 Displaying LUNs with SANsurfer

Note: In a good configuration, you see the same LUN on both HBAs or HBA ports.

5.12.4 Windows Server 2008

The drivers used for failover in Windows environments are MPIO together with DSM installed by the Storage Manager installation package.

The former RDAC drivers for Windows are no longer supported, starting with IBM DS Storage Manager V10.10 (firmware V7.10).

Determining the driver and version in use

You can use the Windows Device Manager to check the driver and version being used:

- If you are running MPIO, as shown in Figure 5-123, there is a module under the Storage controllers tree that identifies the driver. Right-click it and select Properties to see the version of the driver installed under the Driver tab.

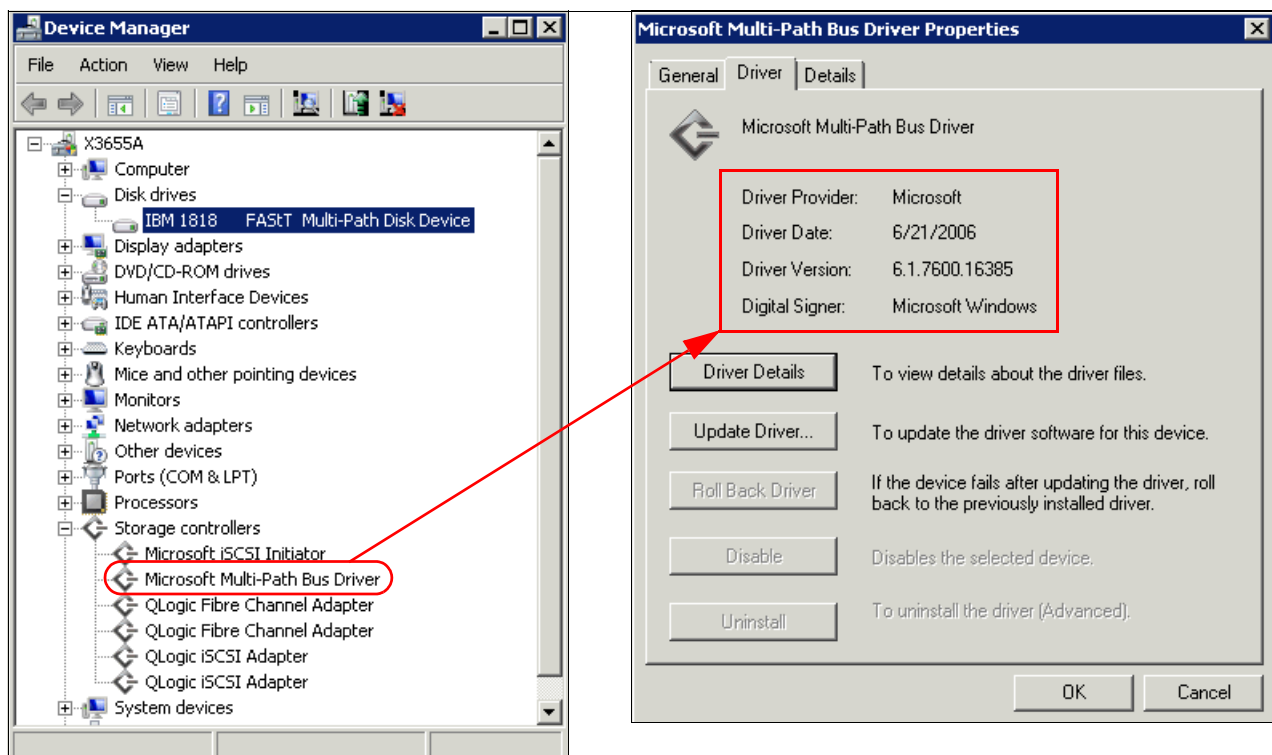


Figure 5-123 Determining the device driver in use

- If running the IBM Storage Manager 10 Failover driver, you will find, under System devices, an entry named IBM DS3000/DS4000/DS5000 series Device Specific Module, as shown in Figure 5-124 on page 436. This entry is used to set the failover policies.

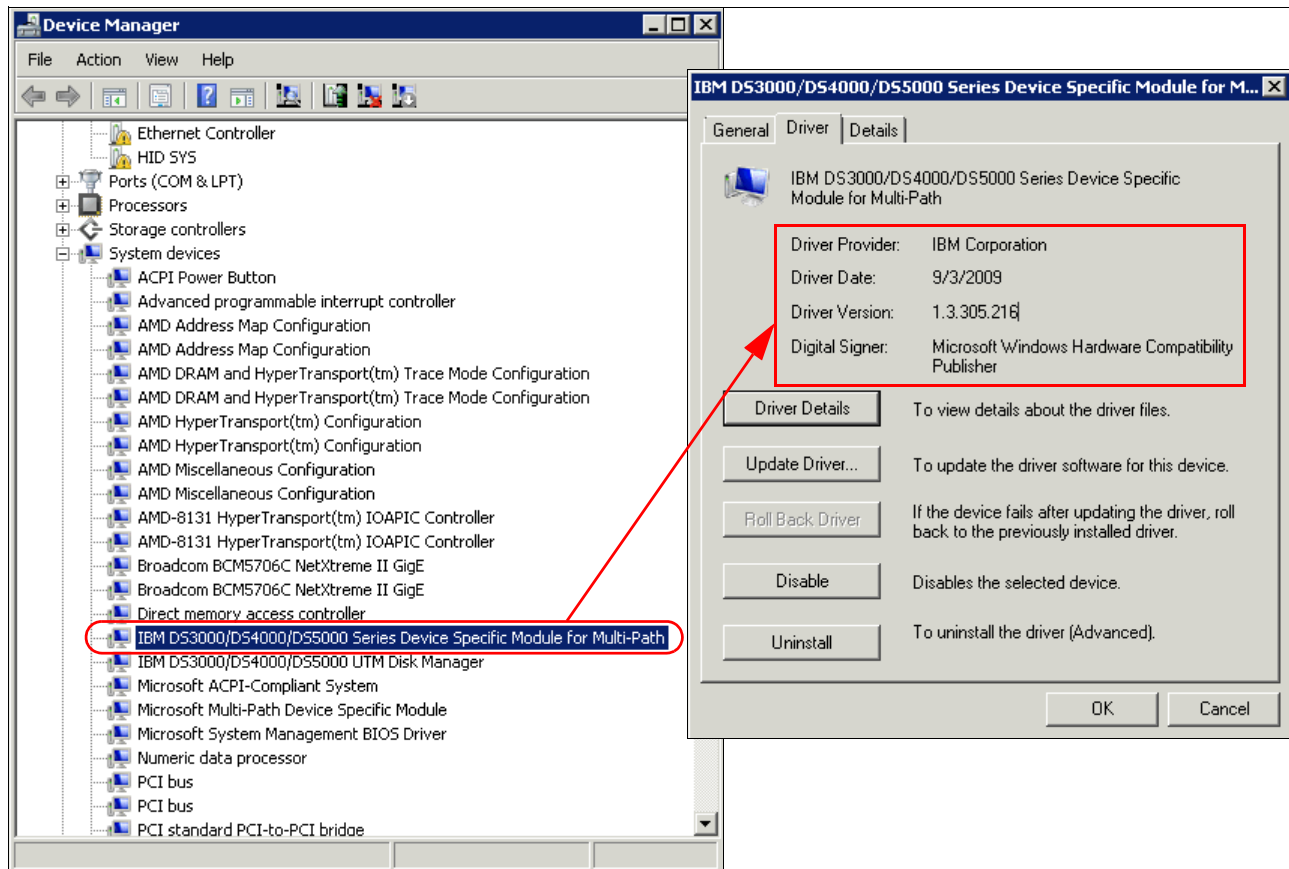


Figure 5-124 Windows Device Manager/DSM

DS5000 logical drive representation in Windows Server 2008

The DS5000 logical drives mapped to a Windows host are presented in the Windows Device Manager under the Disk drives section.

When using the device specific module (DSM) of the IBM Storage Manager together with Microsoft's MPIO architecture, the device is represented under the Device Manager as shown in Figure 5-125.

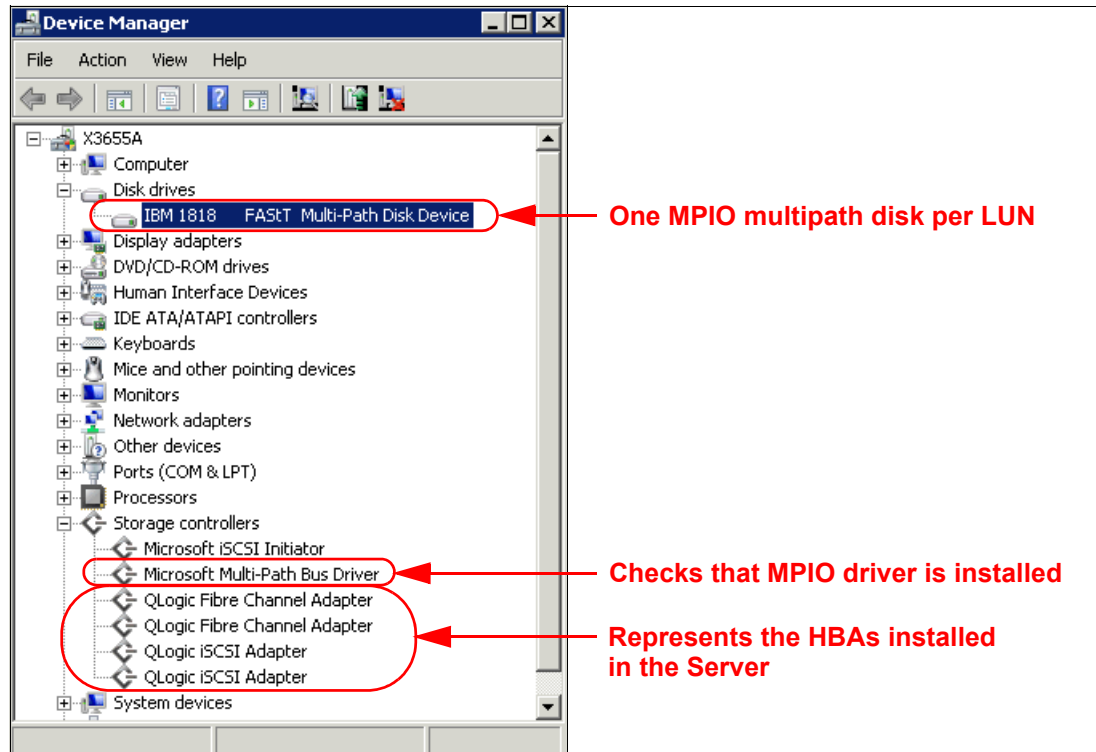


Figure 5-125 Device representation either using MPIO or SDDDSM

In the example above, the DS5300 is configured with only one LUN. The Access LUN is not mapped to the server. Therefore, we see in the Disk drives list only one IBM 1818 Multi-path Disk Device that represents each logical drive mapped.

The physical paths are not represented, as was done with RDAC or Windows Server 2003 in the past. The best practise to verify the paths is to use the SANsurfer or other HBA utilities to verify the paths, as shown in Figure 5-122 on page 434.

However, there is also a way to gather this information in Windows. From the Windows Device Manager, under Disk devices, right-click the MPIO disk that represents the DS5000 LUN and select Properties, as shown in Figure 5-126 on page 438.



Figure 5-126 Disk drive properties

In our example in Figure 5-127, we see:

- ▶ A IBM 1818 Multi-Path Disk Device.
- ▶ MPIO counts two paths. One path is Active/Optimized, and the other one is Standby.
 - Active path on HBA port 4
 - Standby path on HBA port 5 (port number does not refer the hardware port number of the HBA)

Depending on the SAN/iSCSI topology, you might have more paths, but you usually have an equal number of active and standby paths.

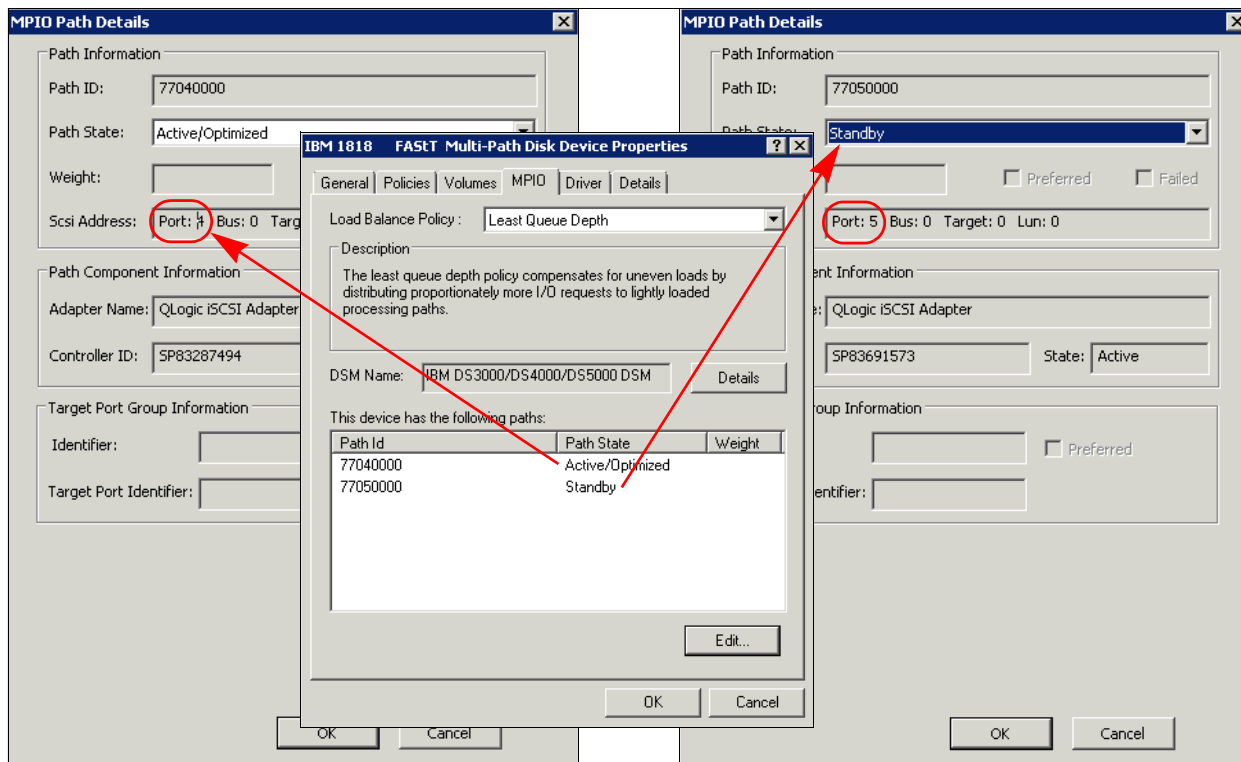


Figure 5-127 MPIO Path details

If the Access LUN is mapped to the server, an IBM Universal Xport SCSI Disk Device appears in the Disk drives list. There is one for each DS5000 connected to the server.

Matching DS5000 logical drives with Windows disks

You can cross-reference the disks represented in the Windows Device Manager list with the logical drives in the DS5000 Mapping view. Right-click the multi-path disk representation in the Device Manager and select **Properties** to display the information in the MPIO tab shown in Figure 5-128. If you select your host in the Mapping tab of SM, you see the matching LUN.

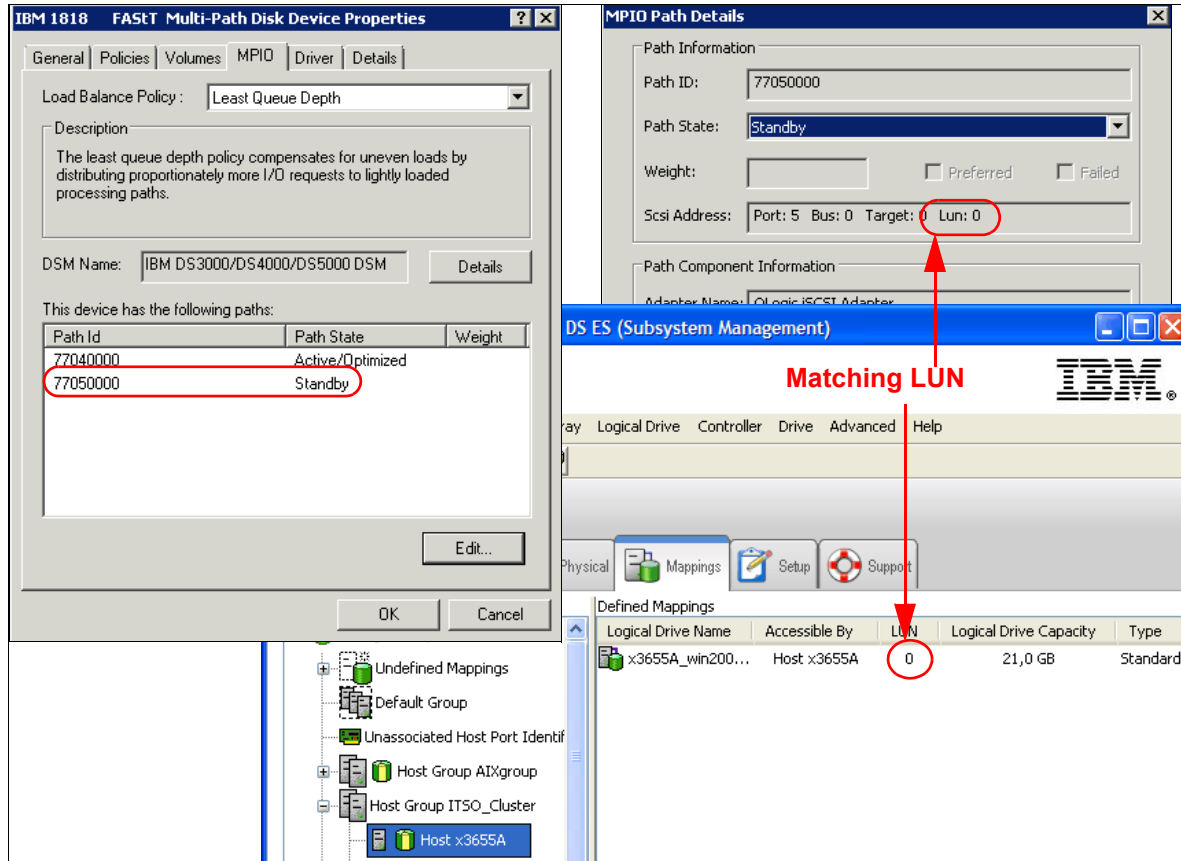


Figure 5-128 Matching disks in Windows and SM

You can access the disk device properties in Windows from either the Device Manager (Figure 5-126 on page 438) or, in Windows 2008, by selecting **Server Manager** → **Storage** → **Disk Management**. In the Disk Management window, select the disk to match from the lower right pane, then right-click and select **Properties**, as shown in Figure 5-129. The disk properties window opens, as shown in Figure 5-128 on page 439.

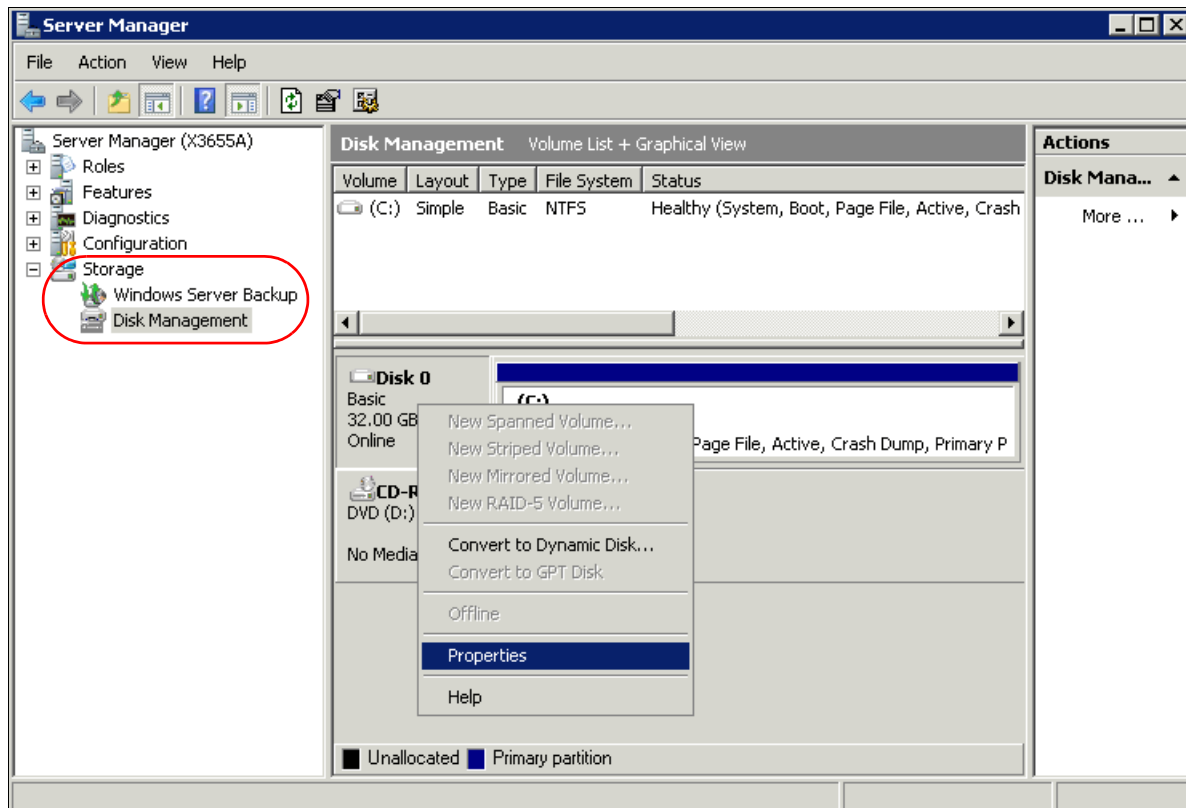


Figure 5-129 Disk Management

Using SM utilities to match disks

There are two commands provided by the Storage Manager to help you manage devices:

- ▶ **hot_add**: Invokes a hardware rescan to search for new DS5000 attached devices.
- ▶ **SMdevices**: Lists devices recognized by Windows, indicating DS5000 names and logical volume names as configured in the DS5000. It is very helpful to relate Windows devices with the logical drives set from Storage Manager.

SMdevices is installed under the util folder in the same directory where the SM Client is installed, and works with all DS5000 drivers (Figure 5-130).

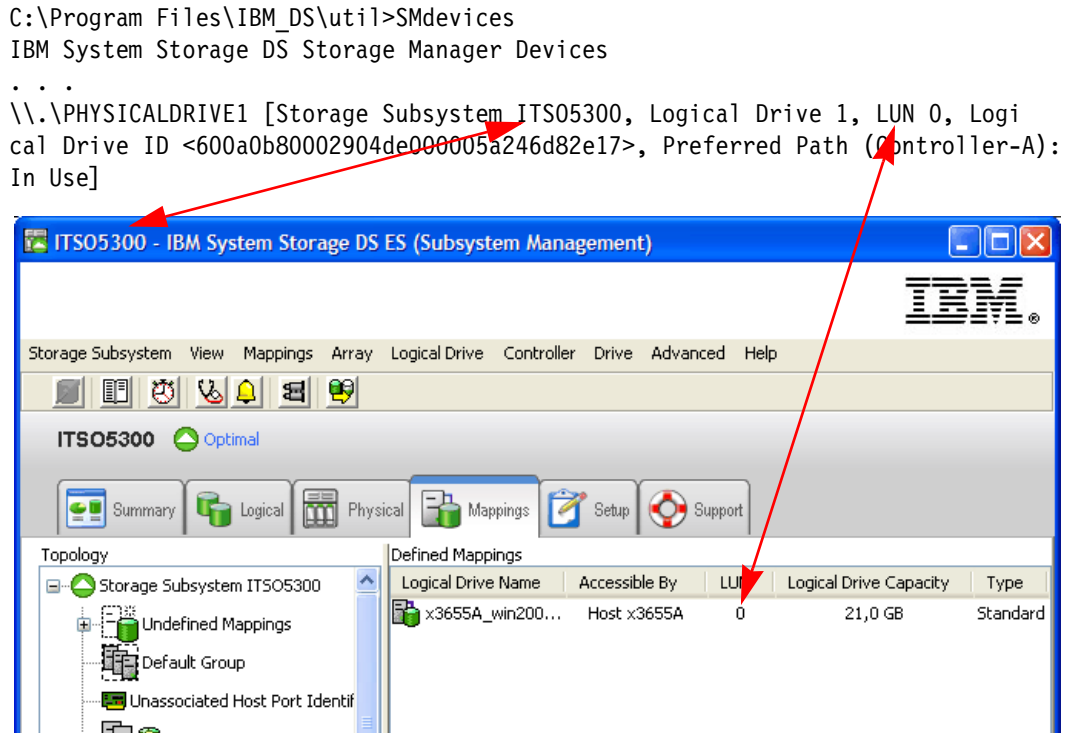


Figure 5-130 Using SMdevices utility

You can also use the drive ID string provided by the **SMdevices** output to identify your logical drive in the DS5000.

Collecting information

In addition to the information given in 5.8.6, “Collect All Support Data option” on page 362, also consider evaluating or sending your service provider the following information from your Windows host system to perform problem determination for certain failures:

- ▶ System event log: Right-click the **My Computer** icon on your desktop and select **Manage** to open the System Management window. From the System Tools option under Computer Management, select **Event Viewer** → **System**. Now click **Action** from the drop-down menu, and select **Save Log File as** to save the event view log file.
- ▶ Application log: Proceed as for the system event log, but this time select the application log.
- ▶ Dynamic system analysis (DSA log): IBM Dynamic System Analysis (DSA) collects and analyzes system information to aid in diagnosing system problems. This is a tool developed initially for IBM System x servers that not only collects the system event and application logs, but also information from your adapters, drivers, and configuration. This allows you to easily provide all the information that your support representative needs in one package. This tool is available at the following address:

www-947.ibm.com/support/entry/portal/docdisplay?lnocid=SERV-DSA

5.12.5 Linux

There are two available driver options to manage a DS5000 storage subsystem in Linux:

- ▶ The RDAC/MPP driver.
- ▶ The Linux Device Mapper Multipath (DMM).

To install RDAC/MPP, a specific kernel version is required. The RDAC driver readme has information about all the supported kernel versions. We currently recommend using RDAC as the failover driver.

The Linux Device Mapper Multipath (DMM) is supported by latest OS version.

RDAC provides additional functions and utilities to obtain much better information about the DS5000 from the operating system. Once the RDAC driver is installed, you have access to several commands that are useful for problem determination and correction. The utilities are:

- ▶ **mppUtil**: This utility is used with the Linux RDAC driver to perform the various functions provided by the driver.
- ▶ **hot_add**: This utility rescans your HBA to detect and configure new devices on SAN.
- ▶ **mppBusRescan**: This utility is equivalent to **hot_add** and also probes the physical bus hardware to discover any newly attached DS5000 devices. These can either be new LUNs on an existing system or a new storage subsystem. All the physical buses are scanned for new devices or LUNs. Any that are found are registered with the OS and attached to the RDAC driver. This utility should be run any time that new storage subsystem devices are connected or new LUNs are mapped to a system.
- ▶ **mppUpdate**: This utility uses the **mppUtil** utility to discover the RDAC-assigned virtual target IDs of the attached subsystems. It then updates the RDAC driver configuration file (`/var/mpp/devicemapping`) so that the entries will be persistent after a reboot. The first time that the RDAC driver sees a storage subsystem, it will arbitrarily assign a target ID for the virtual target that represents the storage subsystem. At this point, the target ID assignment is not persistent. It could change on a reboot. The **mppUpdate** utility updates the RDAC driver configuration files so that these target ID assignments are persistent and do not change across reboots. Once made persistent, the user does not have to worry about the possibility of device names changing and invalidating mount points.

mppUpdate must be executed after a DS5000 is added to or removed from the system. If a storage subsystem is added to the installation, **mppBusRescan** also must be run before **mppUpdate** is run. **mppUpdate** must also be executed whenever a user changes the RDAC configuration file `/etc/mpp.conf` to rebuild the new configuration file into the RAM Disk image that will be used for the next reboot.

Note: Linux RDAC supports rescan of a newly mapped LUN without rebooting the server. The utility program is packaged with the Linux RDAC driver. Rescan can be invoked by either the **hot_add** or the **mppBusRescan** command. **hot_add** is a symbolic link to **mppBusRescan**. There are man pages for both commands. However, the Linux RDAC driver does not support LUN deletion. You must reboot the server after deleting the mapped logical drives.

Listing DS5000 subsystems in Linux

If you want to scan for all the DS5000s that are attached to your Linux host, you must use the **mpputil -a** command, as shown in Example 5-12.

Example 5-12 mppUtil -a

```
[root@TC-2008 /]# mppUtil -a
Hostname      = TC-2008
Domainname    = (none)
Time          = GMT 10/12/2011 11:34:27
```

```
-----
Info of Array Module's seen by this Host.
-----
```

ID	WWN	Type	Name
0	60080e500017b5bc000000004a955e3b	FC	ITS0_5020
1	600a0b80004777d8000000004a956964	FC	ITS05300

--FC connected subsystem = ID #0

In Example 5-12, two DS5000s are presented to the Linux host. Each one has an ID number assigned. You use that number to query for specific details of the subsystem.

Displaying DS storage devices from Linux

In addition to the RDAC utilities, installing the Storage Manager host software gives you access to the same utilities as in other operating systems, such as SMdevices.

In Example 5-13, we show the SMdevices output for the same system shown in Example 5-12.

Example 5-13 SMdevices output

```
[root@TC-2008 /]# SMdevices
DS Storage Manager Utilities Version 10.00.A5.13
...
..
/dev/sda (/dev/sg0) [Storage Subsystem ITS0_5020, Logical Drive TC-2008-1, LUN 0, Logical
Drive ID <60080e500017b5bc000047d04aaa2559>, Preferred Path (Controller-A): In Use]
/dev/sdb (/dev/sg1) [Storage Subsystem ITS0_5020, Logical Drive TC-2008-2, LUN 1, Logical
Drive ID <60080e500017b5bc000048444aafd60a>, Preferred Path (Controller-B): In Use]
<n/a> (/dev/sg2) [Storage Subsystem ITS0_5020, Logical Drive Access, LUN 31, Logical
Drive ID <60080e500017b5bc000043834a955f8a>]
<n/a> (/dev/sg3) [Storage Subsystem ITS0_5020, Logical Drive Access, LUN 31, Logical
Drive ID <60080e500017b5bc000043834a955f8a>]
<n/a> (/dev/sg4) [Storage Subsystem ITS0_5020, Logical Drive Access, LUN 31, Logical
Drive ID <60080e500017b5bc000043834a955f8a>]
<n/a> (/dev/sg5) [Storage Subsystem ITS0_5020, Logical Drive Access, LUN 31, Logical
Drive ID <60080e500017b5bc000043834a955f8a>]
/dev/sdc (/dev/sg6) [Storage Subsystem ITS05300, Logical Drive TC-2008-Vol1, LUN 0,
Logical Drive ID <600a0b800047709c0000852c4abb84f4>, Preferred Path (Controller-A): In Use]
/dev/sdd (/dev/sg7) [Storage Subsystem ITS05300, Logical Drive TC-2008-Vol2, LUN 1,
Logical Drive ID <600a0b80004777d800007e764abb86b6>, Preferred Path (Controller-B): In Use]
```

Notice the SMdevices output lists all the volumes found from any DS storage subsystem with LUNs mapped to this host.

Using the LUN Logical Drive ID

To display the Linux name assigned to each of the logical volumes, use the `lsdev` utility, as shown in Example 5-14.

Example 5-14 Displaying Linux disk names with `lsdev`

```
[root@TC-2008 mpp]# ./lsdev
      Array Name      Lun      sd device
      -----
      ITS0_5020        0      -> /dev/sda
      ITS0_5020        1      -> /dev/sdb
      ITS0_5020        2      -> /dev/sde
      ITS05300         0      -> /dev/sdc
      ITS05300         1      -> /dev/sdd
```

Use the `mppUtil` command, as shown in Example 5-15, to list the DS devices found together with their characteristics. Use the parameter `-g#`, where `#` specifies the DS Subsystem ID previously obtained by using the `mppUtil -a` command, as shown in Example 5-12 on page 443.

Example 5-15 `mppUtil -g0` - good condition

```
[root@TC-2008 ~]# mppUtil -g0
Hostname      = TC-2008
Domainname    = (none)
Time          = GMT 10/01/2009 19:25:59

MPP Information:<-----DS5000 general information
-----
      ModuleName: ITS0_5020                      SingleController: N
      VirtualTargetID: 0x000                      ScanTriggered: N
      ObjectCount: 0x000                          AVTEnabled: Y
      WWN: 60080e500017b5bc000000004a955e3b      RestoreCfg: N
      ModuleHandle: none                          Page2CSubPage: Y
      FirmwareVersion: 7.60.13.xx
      ScanTaskState: 0x00000000
      LBPolicy: LeastQueueDepth

Controller 'A' Status:<----- Controller A breakdown view with path information
-----
      ControllerHandle: none                      ControllerPresent: Y
      UTMunExists: N                              Failed: N
      NumberOfPaths: 2                           FailoverInProg: N
                                              ServiceMode: N

      Path #1
      -----
      DirectoryVertex: present                    Present: Y
      PathState: OPTIMAL<-----first Path to CTRL A
      PathId: 77020000 (hostId: 2, channelId: 0, targetId: 0)

      Path #2
      -----
      DirectoryVertex: present                    Present: Y
      PathState: OPTIMAL<-----second Path to CTRL A
      PathId: 77030000 (hostId: 3, channelId: 0, targetId: 0)
```

```

Controller 'B' Status:<----- Controller Bbreakdown view with path information
-----
ControllerHandle: none                      ControllerPresent: Y
      UTMLunExists: N                      Failed: N
      NumberOfPaths: 2                    FailoverInProg: N
                                           ServiceMode: N

      Path #1
      -----
DirectoryVertex: present                      Present: Y
      PathState: OPTIMAL<-----first Path to CTRL A
      PathId: 77020001 (hostId: 2, channelId: 0, targetId: 1)

      Path #2
      -----
DirectoryVertex: present                      Present: Y
      PathState: OPTIMAL<-----second Path to CTRL A
      PathId: 77030001 (hostId: 3, channelId: 0, targetId: 1)

Lun Information
-----
Lun #0 - WWN: 60080e500017b5bc00004be94ac48ff9<-----LUN0 breakdown
-----
      LunObject: present                      CurrentOwningPath: A<---
      RemoveEligible: N                      BootOwningPath: A<---
      NotConfigured: N                      PreferredPath: A<---
      DevState: OPTIMAL                      ReportedPresent: Y
                                           ReportedMissing: N
                                           NeedsReservationCheck: N
                                           TASBitSet: Y
                                           NotReady: N
                                           Busy: N
                                           Quiescent: N

      Controller 'A' Path<-----LUN0 Path information for CTRL A
      -----
      NumLunObjects: 2                      RoundRobinIndex: 0
      Path #1: LunPathDevice: present
      DevState: OPTIMAL
      RemoveState: 0x0 StartState: 0x1 PowerState: 0x0
      Path #2: LunPathDevice: present
      DevState: OPTIMAL
      RemoveState: 0x0 StartState: 0x1 PowerState: 0x0

      Controller 'B' Path<-----LUN0 Path information for CTRL B
      -----
      NumLunObjects: 2                      RoundRobinIndex: 0
      Path #1: LunPathDevice: present
      DevState: OPTIMAL
      RemoveState: 0x0 StartState: 0x1 PowerState: 0x0
      Path #2: LunPathDevice: present
      DevState: OPTIMAL
      RemoveState: 0x0 StartState: 0x1 PowerState: 0x0

```

Example 5-15 on page 444 shows an example of Linux with one LUN connected to a DS5020 via Fibre Channel. Both HBAs see both controllers, which results in two paths per controller.

In Example 5-16, we see a bad condition example, where:

- ▶ Both paths to controller B failed.
- ▶ LUN0 is owned by controller A, which is in the Optimal state.
- ▶ LUN1 is owned by controller B, which is in the failed state. LUN1 has been taken over by controller A.

To correct these path issues, set the paths to controller B.

To relate the devices detected by Linux to the logical drives configured and mapped to your host in the DS5000, use the mppUtil utility. You can use the LUN number listed and the WWN string to determine the corresponding logical drive in your DS5000.

Example 5-16 mppUtil -g1 - controller failover

```
[root@TC-2008 ~]# mppUtil -g0
```

```
Hostname    = TC-2008
```

```
Domainname  = (none)
```

```
Time        = GMT 10/01/2009 19:27:28
```

MPP Information:

ModuleName: ITS0_5020	SingleController: N
VirtualTargetID: 0x000	ScanTriggered: N
ObjectCount: 0x000	AVTEnabled: Y
WWN: 60080e500017b5bc000000004a955e3b	RestoreCfg: N
ModuleHandle: none	Page2CSubPage: Y
FirmwareVersion: 7.60.13.xx	
ScanTaskState: 0x00000000	
LBPoly: LeastQueueDepth	

Controller 'A' Status:

ControllerHandle: none	ControllerPresent: Y
UTMLunExists: N	Failed: N
NumberOfPaths: 2	FailoverInProg: N
	ServiceMode: N

Path #1

DirectoryVertex: present	Present: Y
PathState: OPTIMAL	
PathId: 77020000 (hostId: 2, channelId: 0, targetId: 0)	

Path #2

DirectoryVertex: present	Present: Y
PathState: OPTIMAL	
PathId: 77030000 (hostId: 3, channelId: 0, targetId: 0)	

Controller 'B' Status:

ControllerHandle: none	ControllerPresent: Y
UTMLunExists: N	Failed: Y<--indicates
HW problem	
NumberOfPaths: 2	FailoverInProg: N
	ServiceMode: N

```

Path #1
-----
DirectoryVertex: present                                Present: Y
PathState: FAILED_NEED_CHECK<-----results out of the HW problem
PathId: 77020001 (hostId: 2, channelId: 0, targetId: 1)

```

```

Path #2
-----
DirectoryVertex: present                                Present: Y
PathState: FAILED_NEED_CHECK<-----results out of the HW problem
PathId: 77030001 (hostId: 3, channelId: 0, targetId: 1)

```

Lun Information

```

Lun #0 - WWN: 60080e500017b5bc00004be94ac48ff9<-----not affected, owning CTRL optimal
-----

```

```

LunObject: present                                     CurrentOwningPath: A
RemoveEligible: N                                       BootOwningPath: A
NotConfigured: N                                         PreferredPath: A
DevState: OPTIMAL                                         ReportedPresent: Y
                                                         ReportedMissing: N
                                                         NeedsReservationCheck: N
                                                         TASBitSet: Y
                                                         NotReady: N
                                                         Busy: N
                                                         Quiescent: N

```

Controller 'A' Path

```

-----
NumLunObjects: 2                                         RoundRobinIndex: 0
Path #1: LunPathDevice: present
DevState: OPTIMAL
RemoveState: 0x0 StartState: 0x1 PowerState: 0x0
Path #2: LunPathDevice: present
DevState: OPTIMAL
RemoveState: 0x0 StartState: 0x1 PowerState: 0x0

```

Controller 'B' Path <-----recognise path failure

```

-----
NumLunObjects: 2                                         RoundRobinIndex: 0
Path #1: LunPathDevice: present
DevState: FAILED_NEED_CHECK<-----Failed
RemoveState: 0x0 StartState: 0x1 PowerState: 0x0
Path #2: LunPathDevice: present
DevState: FAILED_NEED_CHECK<-----Failed
RemoveState: 0x0 StartState: 0x1 PowerState: 0x0

```

```

Lun #1 - WWN: 60080e500017b5bc00004beb4ac4901c<---- affected LUN because CTRL B failed
-----

```

```

LunObject: present                                     CurrentOwningPath: A<--failover
RemoveEligible: N                                       BootOwningPath: B
NotConfigured: N                                         PreferredPath: B
DevState: OPTIMAL                                         ReportedPresent: Y
                                                         ReportedMissing: N
                                                         NeedsReservationCheck: N
                                                         TASBitSet: Y
                                                         NotReady: N
                                                         Busy: N
                                                         Quiescent: N

```

```

Controller 'A' Path
-----
NumLunObjects: 2                                RoundRobinIndex: 0
  Path #1: LunPathDevice: present
            DevState: OPTIMAL
            RemoveState: 0x0 StartState: 0x1 PowerState: 0x0
  Path #2: LunPathDevice: present
            DevState: OPTIMAL
            RemoveState: 0x0 StartState: 0x1 PowerState: 0x0

Controller 'B' Path
-----
NumLunObjects: 2                                RoundRobinIndex: 0
  Path #1: LunPathDevice: present
            DevState: FAILED_NEED_CHECK<-----Failed
            RemoveState: 0x0 StartState: 0x1 PowerState: 0x0
  Path #2: LunPathDevice: present
            DevState: FAILED_NEED_CHECK<-----Failed
            RemoveState: 0x0 StartState: 0x1 PowerState: 0x0

```

Verify RDAC installation

To verify the installation of RDAC, you have many different commands available. Chose the right command that displays the output you want. You can use one of the following options:

- Type the following command to list the installed modules:

```
# lsmod
```

Verify that the module entries are included in the lsmod list, as follows:

- Module entries for SLES or RHEL:
 - mppVhba
 - mppUpper
 - lpfc for Emulex HBAs
 - qla2xxx for Qlogic HBAs
 - lpfcdfc (if ioctl module for Emulex HBAs is installed)
- mppVhba and MppUpper are RDAC modules.

Note: If you do not see the mpp_Vhba module, the likely cause is that the server was rebooted before the LUNs were assigned, so the mpp_Vhba module was not installed. If this is the case, assign the LUNs now, reboot the server, and repeat this step.

- Type the following command to verify the RDAC/MPP driver version:

```
# mppUtil -V
```

The Linux multipath driver version displays, as shown in Example 5-17.

Example 5-17 mppUtil -V

```
[root@TC-2008 ~]# mppUtil -V
Linux MPP Driver Version: 09.03.0C05.0214
```

- Type the following command to verify that the devices are configured with the RDAC driver:

```
# ls -lR /proc/mpp
```

The output similar to the one shown in Example 5-18 displays:

Example 5-18 ls -lR /proc/mpp

```
/proc/mpp:
total 0
dr-xr-xr-x 4 root root 0 Oct 24 02:56 DS5020-sys1
crwxrwxrwx 1 root root 254, 0 Oct 24 02:56 mppVBusNode
/proc/mpp/ DS5020-sys1:
total 0
dr-xr-xr-x 3 root root 0 Oct 24 02:56 controllerA
dr-xr-xr-x 3 root root 0 Oct 24 02:56 controllerB
-rw-r--r-- 1 root root 0 Oct 24 02:56 virtualLun0
/proc/mpp/ DS5020-sys1/controllerA:
total 0
dr-xr-xr-x 2 root root 0 Oct 24 02:56 lpfc_h6c0t2
/proc/mpp/ DS5020-sys1/controllerA/lpfc_h6c0t2:
total 0
-rw-r--r-- 1 root root 0 Oct 24 02:56 LUN0
/proc/mpp/ DS5020-sys1/controllerB:
total 0
dr-xr-xr-x 2 root root 0 Oct 24 02:56 lpfc_h5c0t0
/proc/mpp/ DS5020-sys1/controllerB/lpfc_h5c0t0:
total 0
-rw-r--r-- 1 root root 0 Oct 24 02:56 LUN0
```

After you install the RDAC driver, the following commands and man pages are available:

- **mpUtil**
- **mpBusRescan**
- **mpUpdate**
- **RDAC**

HBA parameters in Linux

The 2.6.11 Linux kernel introduced certain changes to the lpfc (Emulex driver) and qla2xxx (Qlogic driver) Fibre Channel Host Bus Adapter (HBA) drivers; these changes removed the following entries from the proc pseudo-file system:

- /proc/scsi/qla2xxx
- /proc/scsi/lpfc

These entries provided a centralized repository of information about the drivers and connected hardware. After the changes, the drivers started storing all this information within the `/sys` file system. Since Red Hat Enterprise Linux 5 uses Version 2.6.18 of the Linux kernel, it is affected by this change.

Using the `/sys` file system means that all the Fibre Channel drivers now use a unified and consistent manner to report data. However, it also means that the data previously available in a single file is now scattered across a myriad of files in different parts of the `/sys` file system.

It is impractical to search through the `/sys` file system for the relevant files when there is a large variety of Fibre Channel-related information. Instead of using a manual search, use the **systool** command, which provides a simple but powerful means of examining and analyzing this information. We show several commands in this section that demonstrates what type of information that the **systool** command can be used to examine.

For example, to examine information about the Fibre Channel HBAs in a system, use the command **systool -c fc_host -v**, which shows:

- ▶ The WWN of a FC adapter
- ▶ The FC PortID
- ▶ The online state
- ▶ The HBA driver and firmware level

Figure 2-95 shows an example of this command.

```
[root@TC-2008 ~]# systool -c fc_host -v
Class = "fc_host"
Class Device = "host2" first fc adapter
Class Device path = "/sys/class/fc_host/host2"
    fabric_name      = "0x100500341e7096"
    issue_lip        = <store method only>
    node_name        = "0x200000e08b18208b"
    port_id          = "0x070100"
    port_name        = "0x210000e08b18208b"
    port_state       = "Online"
    port_type        = "NPort (fabric via point-to-point)"
    speed            = "2 Gbit"
    supported_classes = "Class 3"
    symbolic_name     = "QLA2340 FW:v3.03.26 DVR:v8.02.00.06.05.03-k"
    system_hostname   = ""
    tgtid_bind_type   = "wwpn (World Wide Port Name)"
    uevent            = <store method only>
[ content removed ]
Class Device = "host3" second fc adapter
Class Device path = "/sys/class/fc_host/host3"
    fabric_name      = "0x100500341e7096"
    issue_lip        = <store method only>
    node_name        = "0x200000e08b892cc0"
    port_id          = "0x070500"
    port_name        = "0x210000e08b892cc0"
    port_state       = "Online"
    port_type        = "NPort (fabric via point-to-point)"
    speed            = "2 Gbit"
    supported_classes = "Class 3"
    symbolic_name     = "QLA2340 FW:v3.03.26 DVR:v8.02.00.06.05.03-k"
    system_hostname   = ""
    tgtid_bind_type   = "wwpn (World Wide Port Name)"
    uevent            = <store method only>
[ content removed ]
```

Figure 5-131 HBA information in Linux: `systool -c`

Collecting information

In addition to the information mentioned in 5.8.6, “Collect All Support Data option” on page 362, you can also send additional information about the Linux host server to your service provider. This information can be collected by using the following commands:

- ▶ **SMdevices**: Lists the DS5000 recognized by your server (if SMutil is installed).
- ▶ **rpm -qa**: Lists installed software.
- ▶ **yum list installed**: Lists installed software if yum is installed.
- ▶ **mppUtil -V**: Lists the installed disk driver version.
- ▶ **ls -lR /proc/mpp**: Lists the devices recognized by the RDAC driver.
- ▶ **cat /proc/scsi/scsi**: Lists the LUNs recognized by the HBAs.
- ▶ **/opt/mpp/mppSupport**: Script provided by RDAC to collect information. Generates a compressed file in the /tmp folder.

www-947.ibm.com/support/entry/portal/docdisplay?lnodocid=SERV-DSA

Loss of Signal: 0
 Primitive Seq Protocol Error Count: 0
 Invalid Tx Word Count: 4
 Invalid CRC Count: 0

IP over FC Adapter Driver Information
 No DMA Resource Count: 0
 No Adapter Elements Count: 0

FC SCSI Adapter Driver Information
 No DMA Resource Count: 0
 No Adapter Elements Count: 0
 No Command Resource Count: 0

IP over FC Traffic Statistics
 Input Requests: 0
 Output Requests: 0
 Control Requests: 0
 Input Bytes: 0
 Output Bytes: 0

FC SCSI Traffic Statistics
Input Requests: 28955
Output Requests: 22520
Control Requests: 172
Input Bytes: 2755219663

The text marked in red in Example 5-19 on page 452 indicates particularly important information, that is:

- ▶ HBA firmware level
- ▶ HBA WWNN and WWPN
- ▶ FCP information, such as FC attachment (Fabric or AL) and speed
- ▶ FC SCSI I/O statistics

Checking the installed AIX level

You must check that your AIX hosts meet the minimum recommended AIX OS level, maintenance level, and service pack level. You can check for this information by issuing the commands shown in Figure 5-132.

```
# oslevel
6.1.0.0      ← AIX 6.1 installed

# oslevel -r ← Technology level 3
6100-03

# oslevel -s
6100-03-01-0921 ← Service pack 1
```

Figure 5-132 #oslevel

Collecting information

Execute the following sequence of commands to capture information to send to your IBM Support representative for problem analysis:

1. **snap -r**: This removes previous data collections from `/tmp/ibmsupt`.
2. **snap -gfikL6c**: This collects information from your system and generates a compressed file in the `/tmp/ibmsupt` directory named `snap.pax.Z`. Send the compressed file output to your IBM Support representative for review.
3. **mpio_get_config -Av**: This command shows how your specific DS5000 is recognized by your MPIO AIX driver (this command does not work with SDDPCM).

Commands to display disk usage

The commands to display your disk usage are:

- ▶ **lspv**: Displays all disks and their usage per volume group (even volume groups that are not active).
- ▶ **lsvg -o**: Displays only online volume groups.
- ▶ **mount**: Displays file systems currently in use.
- ▶ **lsvg -l vgroupname**: Lists file systems for the *vgroupname* volume group (only if the volume group is active).
- ▶ **lspv -l hdisk***: Lists file systems in disk *hdisk**.

Other useful commands

Other useful commands are:

- ▶ **fcstat fcs***: Provides a complete listing of FC parameters of the HBA. Replaces **lsattr** and **lscfg**.
- ▶ **errpt -a**: Displays error log information.
- ▶ **lsdev -Cc disks**: Displays all disks recognized.
- ▶ **cfgmgr -v**: Invokes AIX scans for hardware changes.
- ▶ **lsslot -c pci**: Lists all PCI adapters in your system, and provides their physical locations.
- ▶ **lscfg -l hdisk***: Lists all recognized disks, and provides their physical locations.
- ▶ **lscfg -vl fcs***: Displays adapter *fcs**, which is used for the WWN, and the firmware level.
- ▶ **lsmcode -cd fcs***: Displays the adapter *fcs** microcode.
- ▶ **hot_add**: Similar to **cfgmgr**, but only for DS4000 devices (only if SMutil installed).
- ▶ **oslevel**: Displays the AIX version (**oslevel -s** also displays the maintenance level).
- ▶ **lspp -l**: Lists all installed file sets.
- ▶ **lspath**: Lists all paths and states for MPIO disks.
- ▶ **chpath -s enabled -l hdisk***: Enables paths for the *hdisk** device.

For additional information regarding AIX error messages, see your AIX software documentation or consult the Web site at the following address:

<http://publib16.boulder.ibm.com/pseries/index.htm>

6



IBM Remote Support Manager for Storage

In this chapter, we describe how to use IBM Remote Support Manager (RSM) for Storage with the IBM DS5000 Storage subsystem.

6.1 IBM Remote Support Manager for Storage

The IBM Remote Support Manager for Storage (RSM for Storage) software is a no-charge software package that is installed on an IBM System x server running Novell SUSE Linux Enterprise Server 9, SUSE Linux Enterprise Server 10, SUSE Linux Enterprise Server 11, Red Hat Enterprise Linux 4 Advanced Server, or Red Hat Enterprise Linux 5. It provides problem reporting and remote access for IBM Service for the IBM System Storage DS3000, DS4000, and DS5000 families.

The problem reporting utility provided by RSM for Storage automatically creates an entry in the IBM call management system for each subsystem that reports a problem. This is the equivalent of placing a voice call to IBM Service for a problem. Once in the system, problems are responded to with the priority specified by the maintenance agreement in place for the product.

Note: During off-shift hours, in addition to RSM reporting a problem, please call your local IBM Service Support.

For support telephone numbers in your country or region, navigate to the following URL:
<http://www.ibm.com/planetwide>

RSM for Storage controls security for remote access by managing hardware and software components of the server on which it is installed. After it is installed, the server should be considered a single purpose appliance for problem reporting and remote access support for your storage subsystems. Only applications approved by IBM and specified in this document should be installed. (Management of the internal firewall and other configuration changes made by the software might prevent other applications from working.) There is no guarantee that applications that work with the current version of RSM for Storage will continue to work with future releases.

Remote access to the RSM for Storage system by IBM Service is provided by either an external modem attached to the server or through an external SSH connection. This connection provides IBM Service with a command-line interface to the server. All bulk data transfers for logs and other problem determination files are sent to IBM through email using the server's Ethernet interface as shown in Figure 6-1. An internal firewall that is managed by the RSM for Storage software keeps remote and local users of the system from accessing other devices on your intranet. Local and remote IBM users of the system do not have the ability to change any security features of the software.

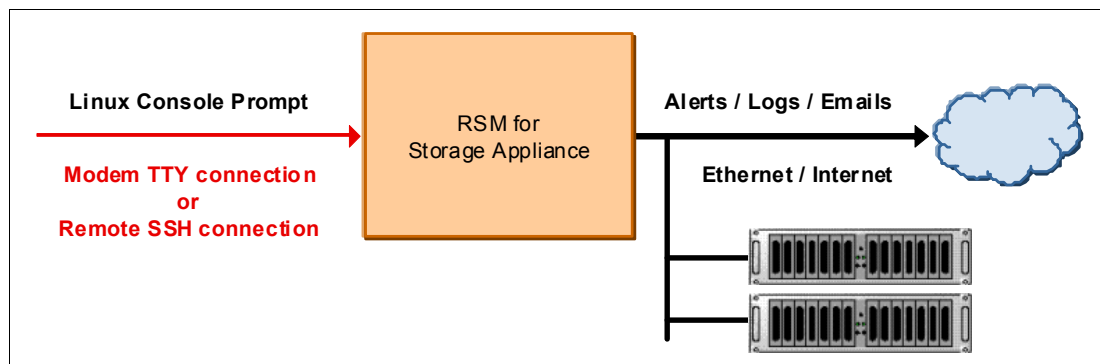


Figure 6-1 RSM layout

Your existing IBM System Storage DS Storage Manager v10, also known as Storage Manager software monitors the storage subsystems. This software is configured to send SNMP traps to the Remote Support Manager when critical events are detected. Configuration of the management application is discussed in 6.2.4, “Configuring SNMP traps in Storage Manager” on page 480.

The RSM for Storage user interface allows you to control and view the status of four management areas:

- ▶ System configuration
- ▶ Reporting
- ▶ Remote access
- ▶ Internal firewall

Your contact person for RSM for Storage will also receive emails about status changes in these areas.

One RSM for Storage server can support up to fifty DS5000, DS4000, DS3000, FASTT 200, and FASTT 500 storage servers. Only IP connectivity to the Ethernet management ports of the subsystems is required: serial cables are not needed for access to the disk subsystems. The storage subsystems must be under a warranty or a current IBM maintenance agreement to be eligible to use the RSM for Storage software. There are no annual fees for RSM.

Note: Documentation and installation code is available at the following URL:

<http://www.ibm.com/storage/disk/rsm>

6.1.1 RSM for Storage Documentation and installation code

RSM for Storage code changes with every new release of the Storage Manager software (as it contains SMCLI part of Storage Manager software). Update the RSM for Storage code along with updating the Storage Manager software on your management hosts. Check the Change History document described below for information on included Storage Manager code.

Note: RSM for Storage depends on SMCLI to communicate and gather information from storage subsystems. Updating the storage subsystem controller firmware on storage subsystems often requires updating the Storage Manager software to support the new firmware features. Please check the appropriate storage subsystem controller firmware Readme documents for information.

There are several documents that cover RSM for Storage:

- ▶ *IBM RSM for Storage Compatibility Guide* - lists all the hardware and software requirements.
- ▶ *IBM RSM for Storage Installation Hints and Tips* - collection of procedures and information necessary to configure your servers and environment to be able to use RSM for Storage.
- ▶ *Change History* - lists all the changes in RSM for Storage versions.
- ▶ *Readme* - short installation and support information.
- ▶ *IBM RSM for Storage Planning, Installation and User's Guide* - comprehensive guide detailing the process of planning, installation and using RSM for Storage

Documentation and installation code changes periodically. Always verify that you are using the latest version available at the following URL:

<http://www.ibm.com/storage/disk/rsm>

6.1.2 Hardware and software requirements

RSM for Storage has the following hardware and software requirements.

Hardware requirements

IBM internal databases that support RSM for Storage use the IBM Machine Type and Serial Numbers of the servers, and therefore an IBM System x server must be used. This is required to properly register heartbeat records from the RSM for Storage system in IBM tracking databases. RSM for Storage can be run on a dedicated System x server or in a VMware client running on a System x server. See the *IBM RSM for Storage Compatibility Guide* listed under 6.1.1, “RSM for Storage Documentation and installation code” on page 457 for the minimum server requirements and a list of the specific servers that have been tested with the RSM software.

Suggested servers

The following servers have been tested with the RSM for Storage software, and installation instructions are available for configuring and using them with RSM for Storage software:

- ▶ IBM System x3250 4364
- ▶ IBM System x306m 8849
- ▶ IBM System x3550 7978
- ▶ IBM System x3550m2 7946
- ▶ IBM System x3550m3 7944

The *IBM RSM for Storage: Installation Hints and Tips* document listed under 6.1.1, “RSM for Storage Documentation and installation code” on page 457 contains specific information about the BIOS configuration and device drivers that might be required to install the Linux OS on the above servers.

Other IBM servers

You can use other System x servers that meet the following requirements:

- ▶ 512 MB memory.
- ▶ 20 GB disk space.
- ▶ Serial port: The serial port must be on the server system board. Some servers have a build-in Remote Supervisor Adapter (RSA) that also includes a serial port. The serial port on the RSA cannot be accessed by the RSM for Storage software.
- ▶ Ethernet port: If your SAN devices are on a private management LAN, a second Ethernet port for accessing your company's SMTP server and the Internet will be required if your selected server only has a single Ethernet port.

Note: To use servers other than those specifically tested with RSM for Storage, you will need to see the System x server support website for technical information about BIOS configuration and device drivers that might be required to install the Linux OS or configure the server's internal RAID capability.

The *IBM RSM for Storage Compatibility Guide* listed under 6.1.1, “RSM for Storage Documentation and installation code” on page 457 also contains the setup required for a VMware client that will host the Linux operating system running RSM for Storage.

RSM for Storage in a VMware virtual client

RSM for Storage has been tested for operation in a VMware virtual client. See the *IBM RSM for Storage Compatibility Guide* for specific configurations.

In setting up the virtual client, allocate the following resources:

- ▶ Storage: 20 GB HDD.
- ▶ Memory: 512 MB.
- ▶ If using an external modem, assign exclusive physical ownership of the host system's first serial port to the virtual client as `/dev/ttyS0`.

The client must be configured to automatically start when the host reboots.

Note: Two additional fields must be provided in the RSM for Storage configuration pages.

When a VMware environment is detected by the RSM for Storage software, you will be prompted to enter the IBM machine type and serial number of the hosting system on the RSM for Storage Connections configuration page.

The IBM server type and serial number are required in order to properly register heartbeat records from the RSM for Storage system in IBM tracking databases.

To avoid reporting problems set the machine type to: 1818-RS3.

Software requirements

The RSM for Storage software requires the following prerequisite software to monitor an IBM System Storage DS subsystem:

- ▶ IBM System Storage DS Storage Manager V10.77 or later (the latest version is preferable) with Event Monitor installed on a management station in a separate server.
- ▶ Storage subsystems with controller firmware supported by Storage Manager V10.77 or later. The latest supported firmware version is suggested.
- ▶ One of the following operating systems to install the RSM for Storage software:
 - Novell SUSE Linux Enterprise Server 9 (SP3 or SP4)
 - Novell SUSE Linux Enterprise Server 10 (Base, Update 1, 2, 3)
 - Novell SUSE Linux Enterprise Server 11 (Base and Update 1)
 - Red Hat Enterprise Linux 4 AS (Update 4, 5, or 6)
 - Red Hat Enterprise Linux 5 (Base, Update 1, 2, 3, 4, 5)

RSM for Storage software receives SNMP traps from the Event Monitor included with the Storage Manager. RSM for Storage software cannot be installed on the same system used to manage your storage network.

Note: See the *IBM RSM for Storage Compatibility Guide* for the latest update of supported servers, modem, and operating systems. Check chapter 6.1.1, "RSM for Storage Documentation and installation code" on page 457 for details.

6.1.3 How RSM for Storage works

RSM for Storage uses an Ethernet connection for problem reporting and a modem (optional) or SSH for remote access by IBM Service as shown in Figure 6-2. The storage system can be any supported IBM System Storage DS subsystem.

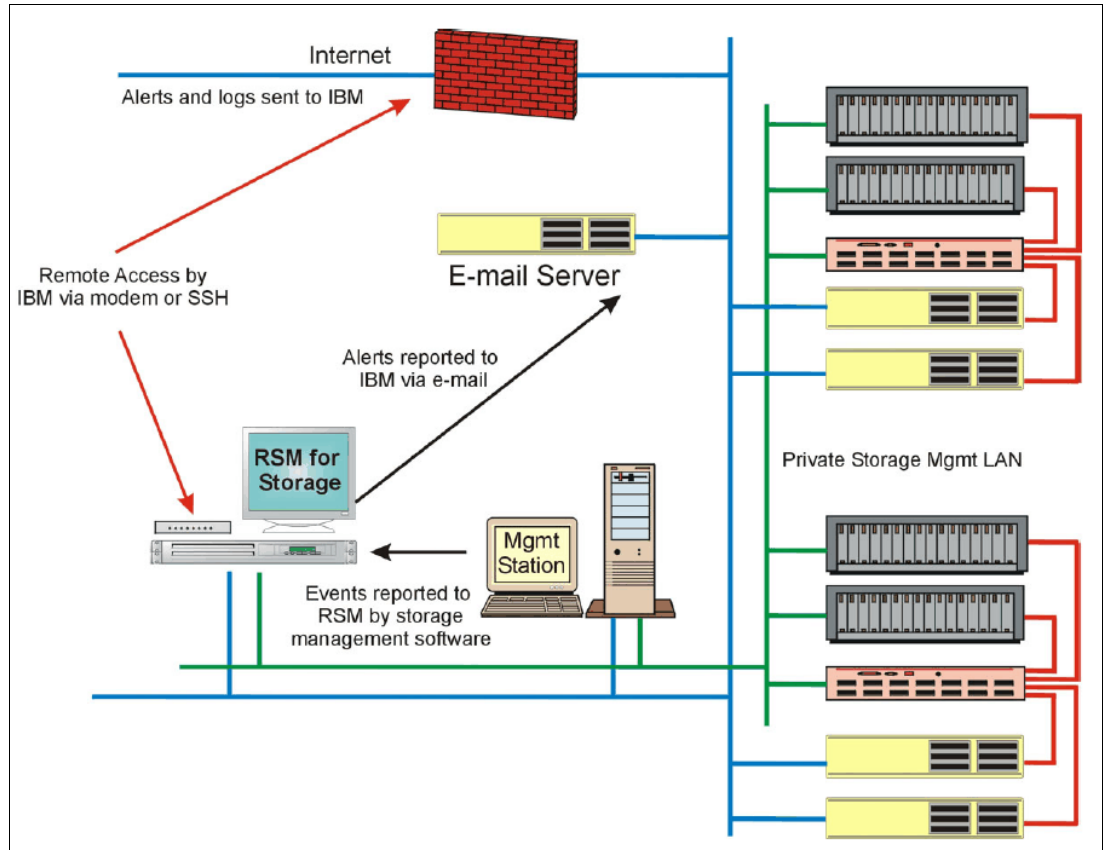


Figure 6-2 RSM for Storage connection

The RSM for Storage server must have IP connectivity to the Ethernet management ports of the storage subsystems to be monitored and the management station must be running IBM Storage Manager's Event Monitor. All the storage subsystems, the management station, the email server, and Internet gateway must be accessible from the RSM server without requiring authorization through a firewall.

If your managed storage subsystems or other SAN devices are on a private management LAN, a second Ethernet port for accessing your company's SMTP server and the Internet will be required if your selected RSM server has only a single Ethernet port (see Figure 6-2).

Figure 6-2 shows that some storage subsystems and other SAN devices are managed through a private management LAN and others that are managed through the customer intranet. Therefore, the RSM server in this instance needs at least two network adapters.

RSM for Storage can send alerts to IBM by two methods. The primary method is to establish a HTTPS connection directly to the IBM Problem Reporting and Status Reporting Servers. This method provides confirmation of receipt and encryption of all information. This method uses the IBM Electronic Customer Care (ECC) client. ECC client also creates new status values which will be seen on the browser management pages. If a direct connection cannot be established, RSM for Storage will send alerts to IBM's email gateway with log files as attachments.

After RSM is installed, configured, and activated, here is an example scenario for RSM. See Figure 6-2 on page 460 to understand the flow:

1. An error occurs on one of the storage subsystems and a critical event is logged in the management station running Storage Manager.
2. The management station reports the critical event to the RSM server through an SNMP trap. The RSM system receives notification of the critical event and sends an alert to IBM Service.

When an alert is received from the management station, RSM downloads All Support Data zip package using the out-of-band Ethernet interface, and sends it along with the alert to IBM Service using ECC (if ECC fails, RSM will try to send the package using email).

SNMP traps are sent by the Storage Manager client or the Storage Manager's Event Monitor service. As the Storage Manager Client might not always be running, Event Monitor should be installed. See the Storage Manager documentation to learn about the installation of Event Monitor.

See 6.1.4, "Notification email and events filtering" on page 461 to configure the SNMP traps in Storage Manager.

3. IBM Service does problem determination based on the information sent by the alert along with the All Support Data package. If the problem can be fixed with the existing information, IBM Service contacts the customer either by phone or email to resolve the problem. After the problem is solved, either IBM Service or the customer must indicate *Service Complete* for all alerts in the RSM. IBM Service can dial in the RSM using a modem or use an SSH connection to acknowledge and indicate *Service Complete* for all alerts for the subsystem.
4. If the problem cannot be fixed with the existing information, IBM Service dials in the RSM using a modem or uses an SSH connection, acknowledges the alert, and performs troubleshooting by connecting to the storage subsystem using the Storage Manager command-line interface (SMcli) included with RSM code or TELNET. IBM Service might need to contact the customer to obtain the password for the storage subsystem to use SMcli. IBM might also have to contact the customer to enable TELNET access.

If IBM Service needs to send or upload logs or other information from the RSM server to IBM, they can use FTP or email commands from the Linux shell of the RSM server while connected through the modem line or using SSH connection. Any data connected is sent to an IBM server through a customer network, not through the modem line (the modem connection is a TTY serial console, not an IP connection).

5. After the problem is resolved, all alerts must be closed either by IBM Service or the customer before reporting will resume for that subsystem.

Note: After the RSM for Storage reports a problem to IBM for a given subsystem, no additional problems will be reported to IBM for that particular subsystem until all existing alerts are closed.

6.1.4 Notification email and events filtering

The RSM for Storage software sends e-mails to notify you about important changes in status. Up to 20 contact people can be configured. One will be the primary contact for RSM related events and will receive all notifications about RSM system operation and problems. Additional contacts can be configured for subsystems located at other sites. They only receive notifications related to subsystem problems. See Table 6-1 on page 462 for information about the notifications.

Table 6-1 E-Mail notifications

Notification	Primary contact	Subsystem contact
Remote Access is enabled or disabled.	x	
Remote User connects and logs into the RSM for Storage system or logs out.	x	
Firewall is enabled or disabled.	x	
Remote Access is about to expire or has expired.	x	x
An alert occurs for a subsystem.	x	x
Daily status updates at local noon.	x	
Daily status updates at local noon when a subsystem has an active alert.	x	x
Daily phone line check fails.	x	
Ping Check fails.	x	
RSM receives an event it is configured to ignore.	x	x
Notifications from IBM Support or RSM for Storage Development about the availability of updates to RSM for Storage software.	x	

There are several types of notifications sent by RSM to the primary contact or subsystem contact, as configured in the RSM:

- ▶ *Remote Access notifications* are sent when:
 - Remote access is enabled or disabled.
 - A remote user connects or disconnects from the system.
 - The remote access automatic timeout is about to expire and the system has one or more active alerts. Timeout warnings are sent at 4 hours, 2 hours, and 1 hour before the timeout occurs.
- ▶ *Alerts Status notifications* are sent when an alert has been sent to IBM Service.
- ▶ *Daily Status emails* serve as a heartbeat notification that the RSM for Storage system is operational. This includes the summary status for the system and status for alerts that might be active for storage subsystems.
- ▶ *Firewall Status notifications* are sent when the internal firewall is enabled or disabled by a root or admin user.
- ▶ *Ping check notifications* are sent when two ping checks in a row fail. Ping checks of the configured SMTP sever and Management Station are performed every half hour.
- ▶ *Ignored Event notifications* are sent when an event is received that is configured to be ignored by the RSM for Storage system, and is therefore not reported to IBM Service. These are events for which a response by IBM Service is not usually required as shown in Table 6-2.

Table 6-2 Filtered events

Event code	Event text
6200	FlashCopy repository logical drive capacity - threshold.

Event code	Event text
6202	FlashCopy logical drive failed.
None	The persistent monitor running on Host xxxxxxxx cannot reach the indicated Storage Subsystem.
None	The persistent monitor running on Host xxxxxxxx can now reach the indicated Storage Subsystem.
4011	Logical drive not on preferred path due to ADT/RDAC.

- *Phone Line Check notification* is sent if the RSM for Storage system cannot verify that an active phone line is connected to the modem. The check is run daily after midnight local time.

RSM and Storage Manager email alerts

Storage Manager in the management station can be configured to send email notifications when a problem is detected. However, this feature *must be disabled* when RSM for Storage is installed if the email contact configured in the Storage Manager is the same as the email contact configured in the RSM Contact List. Otherwise, you will receive multiple notification emails about the same problem: one notification from RSM and another one from Storage Manager.

To disable email alerts in Storage Manager, perform the following steps:

1. Right-click your management station in the Storage Manager Enterprise window and select **Configure Alerts** to select all storage subsystems.
2. On the Email tab, delete any configured email destinations.

If there are email addresses already configured to receive emails from Storage Manager but are not listed in the RSM Contact List (see Figure 6-9 on page 470 for the Contact List), it is not necessary to delete them in Storage Manager.

6.1.5 Remote access methods

The required Remote Access for IBM Service can be provided by one or both of two methods: An external modem can be attached to the server's serial port, or remote access through an SSH client can be enabled.

Remote access by modem

The functional requirements for the modem are minimal: it is only used for remote access by IBM Service. Most "Hayes-compatible" external modems can be used. Any V.92 56K modem supporting the common AT command set will work.

The RSM for Storage software has been tested with the following modems:

- Multitech MultiModem II MT5600BA
- Multitech MultiModem ZBA MT5634ZBA

See the *IBM RSM for Storage Compatibility Guide* listed under 6.1.1, "RSM for Storage Documentation and installation code" on page 457 for updated information about which modems are supported. You will need to contact your IT support staff for installation and problem resolutions related to the modem.

Remote access by SSH

Instead of using a modem for external access to the RSM for Storage system, you can allow remote access by an external SSH connection. To do this, you will need to map a port on your external firewall to the IP address and SSH port (typically 22, but this can be configured) on the RSM for Storage system. Although the RSM for Storage system has several layers of login protection on the SSH port, you can also require firewall authentication (typically using a browser) before the external firewall makes a connection to the RSM for Storage system.

You can also choose to allow remote access by both methods. More information about setting up and using an SSH connection is available in the *IBM RSM for Storage Planning, Installation, and User's Guide*, and the supplement *IBM RSM for Storage: Installation Hints and Tips*. For details, check the chapter 6.1.1, "RSM for Storage Documentation and installation code" on page 457.

6.1.6 RSM management interface

The RSM management interface can be accessed through a web browser pointing to the IP address or host name of the RSM server using HTTPS. You can use the web interface to check the status and configure RSM settings. For IBM Service, the interface is a command-line interface when connected to the RSM server through a modem or SSH connection.

Figure 6-3 shows an example of a System Configuration menu for an already configured and not activated RSM system.

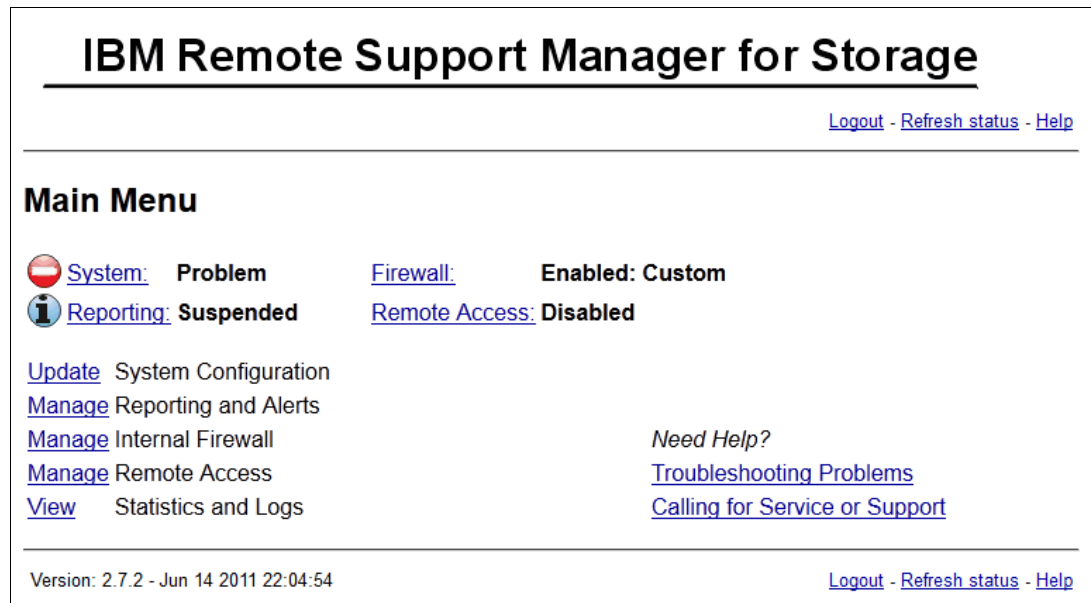


Figure 6-3 RSM System Configuration menu

Under System Configuration, there are links at the top of the page that provide a summary status of the RSM system. Depending on the status, various icons might be displayed to the left of each link. The status values for each of these are as follows:

- ▶ System:
 - OK: Remote Support Manager is operating properly.
 - Incomplete: One or more required configuration settings are missing or incorrect.
 - Problem: There is a problem that is preventing correct operation.

Note: Reporting is disabled until all configuration problems are fixed.

- ▶ Reporting:
 - All Subsystems: Reporting is enabled for all configured subsystems.
 - Standby: Reporting has been disabled for all subsystems.
 - Partial: Reporting has been disabled for some but not all subsystems.
 - Suspended: Reporting is not performed while a configuration problem exists.
 - Storage Problem: A problem has been reported by one or more subsystems.
- ▶ Firewall:
 - Enabled:Closed: The firewall is enabled. Only connections required for reporting are allowed.
 - Enabled:Open: The firewall is enabled. Connections are open to one or more devices being serviced.
 - Enabled:Custom: The firewall is enabled. Only connections required for reporting and permitted by the custom rules defined in `/etc/rsm/rsm-firewall.conf` are allowed.
 - Disabled: The firewall is disabled. There are no restrictions on access to the networks connected to the RSM.
- ▶ Remote Access:
 - Disabled: Modem answer and remote user login is disabled.
 - Enabled: Modem is enabled and remote user login is allowed.
 - Active: A remote user is logged into the system.

6.1.7 RSM security considerations

RSM for Storage controls security for remote access by managing the hardware and software components of the server on which it is installed. After it is installed, the server should be considered a single purpose appliance for problem reporting and remote access support for your storage subsystems. Do not use it for other applications.

Remote access to your system has the following four layers of control:

- ▶ The modem is configured to only answer when Remote Access is enabled by the RSM for Storage software. Likewise, the SSH daemon is only allowed to respond to connection attempts when Remote Access is enabled.

You can manually enable and disable remote access, or you can choose to have remote access automatically enabled when a storage subsystem reports a problem. When remote access is enabled, a timer is started that will automatically disable remote access when it expires. You do not have to remember to make the system secure after service has been completed.

The person identified as the primary contact for the RSM for Storage system is notified by email whenever a change in the remote access settings occurs, and all state changes are written to the security log.

- ▶ The user ID reserved for remote access (`rservice`) is only valid when Remote Access is enabled. Attempts to log in using the `root`, `admin`, or `lservice` user IDs are rejected.

Note: For this reason, do not create additional users on this system.

- ▶ The initial login password is changed daily at midnight UTC. IBM Service has an internal tool that provides the current password for RSM for Storage systems.
- ▶ After validation of the initial login password, remote users are presented with a challenge string, which also requires access to an internal IBM tool to obtain the correct response. The response also includes an IBM employee user name that is recorded in the RSM for Storage security log.

User ID

During installation, the RSM software creates three user IDs:

- ▶ **admin**: This is the administrative user that can perform management and configuration tasks.
- ▶ **lservice**: This is the local service user intended for use by IBM Service when on site. This User ID has restrictions regarding the directories it can access. This is to prevent any configuration change that might affect the security of the system.
- ▶ **rservice**: This is the remote service (IBM Service) user that is used exclusively for remote access to the system and only valid when Remote Access is enabled. This user ID also does not have the ability to change any of the RSM security features.

Passwords for user ID *admin* and *lservice* for the RSM for Storage browser user interface can be changed by the Linux *root* user using the command **rsm-passwd admin** or **rsm-passwd lservice**. For security reasons, set a separate password for each user ID.

For the remote user (*rservice*), the password is automatically generated by RSM and it is changed daily at midnight UTC. IBM Service has an internal tool that provides the current password so you do not need to provide the current RSM password to IBM Service.

The Switch User (**su**) command is disabled to prevent a normal user from attempting to become “root” and have unrestricted access to the system. The RSM for Storage software makes other changes in program and directory permissions to limit what programs and files these users can access.

Internal firewall

RSM for Storage includes an internal firewall to limit the scope of access a remote user has to your network. Without an internal firewall, the remote user will have unrestricted access to your network. The RSM software configures an internal firewall on the RSM system to limit the scope of access that users of the RSM system have to your network, as shown in Figure 6-4 on page 467. When no alerts are active, the firewall only allows incoming SNMP traps and outbound SMTP email. When an alert occurs, a rule is automatically added to the firewall to allow access to the configured controllers for the storage subsystem reporting the problem. There might be times when you want to allow IBM Service to be able to access a device to troubleshoot a problem (such as a performance issue) for a subsystem that is not reporting a failure. You can manually enable “service access” for any configured storage subsystem. Service Access settings have a configurable timeout from 12 to 96 hours, after which the firewall rules for access are removed.

Firewall rules that are added for a device that is reporting an alert are removed when the alert is closed on the RSM for Storage system.

Although the internal firewall effectively limits the scope of access for remote users, at the same time it also limits the access of any program running on the server. Because management applications such as Storage Manager or IBM Director require access to all devices being managed, the presence of this internal firewall prevents the use of the RSM server as a management station. Therefore, the RSM for Storage system should be

considered to be a single purpose appliance dedicated to problem reporting and remote access for IBM Service.

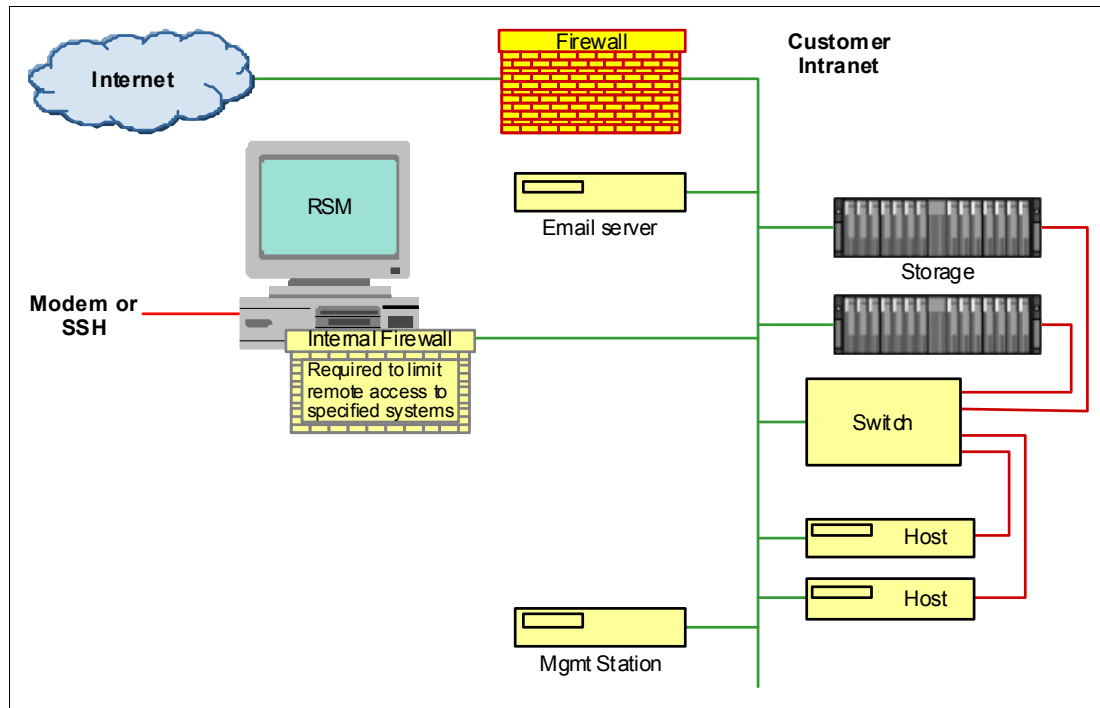


Figure 6-4 RSM internal firewall

6.2 Installing and setting up RSM

In this section, we show how to install and configure RSM. Before beginning this task, go to the RSM support website and carefully review the *IBM RSM for Storage* documents *Planning*, *Installation and Users Guide*, and *Installation Hints and Tips*. For details, check the chapter 6.1.1, “RSM for Storage Documentation and installation code” on page 457.

Tip: Do not use a remote connection when installing the RSM for Storage on the workstation. Log on locally to the Graphical User Interface of the workstation because RSM resets the firewall settings to prevent remote access to the Linux workstation and will be configured later.

6.2.1 Installing the host OS

There are various operating systems supported for the RSM host as shown in “Software requirements” on page 459. In our example, we used Novell SUSE Linux Enterprise Server (SLES) 11 as the host operating system on the RSM server. When installing SLES 11, we selected the following additional packages:

- ▶ KDE Desktop Environment for Server
- ▶ mgetty
- ▶ expect
- ▶ net-snmp
- ▶ minicom

See *IBM RSM for Storage: Planing, Installation, and User's Guide*, found in chapter 6.1.1, "RSM for Storage Documentation and installation code" on page 457 for specific operating system installation instructions.

6.2.2 Installing RSM

The RSM software can be downloaded from:

<http://www.ibm.com/storage/disk/rsm>

We installed RSM according to the instructions in *IBM RSM for Storage: Planing, Installation, and User's Guide* (listed under 6.1.1, "RSM for Storage Documentation and installation code" on page 457). After the installation, you have to define the admin and lservice user IDs.

6.2.3 Setting up RSM

After the installation is complete, we have to set up RSM by performing the following steps:

1. On the Linux login window, perform the following steps:
 - a. Click **Session** and select **KDE**.
 - b. Log in as the admin user.
 - c. Click the **Manage** icon on the Desktop to open a web browser that shows the main administration window as shown in Figure 6-5. Click **Login**.

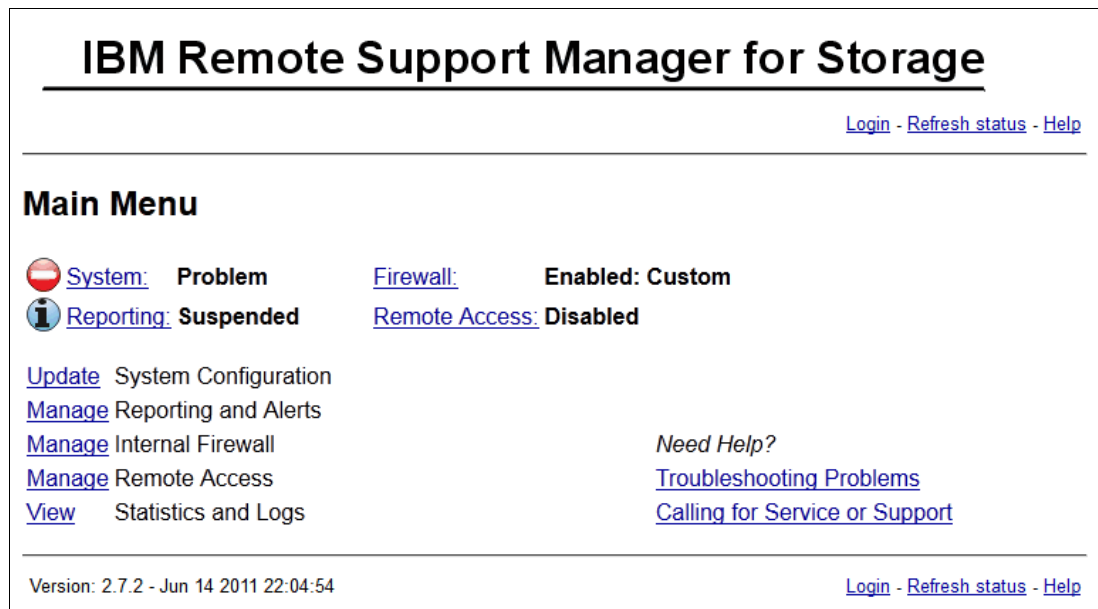


Figure 6-5 RSM administration window

2. Click **Login** and enter the user name and password of the RSM administrator. This account is named admin and the password was defined during the installation of RSM. See Figure 6-6 on page 469.

Figure 6-6 RSM login window

3. You return to the Main Menu. To start the setup, click **System** as shown in Figure 6-7.


Figure 6-7 RSM main menu

4. The System Configuration window shows incomplete tasks that need to be accomplished before the RSM system can be used as shown in Figure 6-8 on page 470.


IBM Remote Support Manager for Storage

[Main](#)
[Logout](#) - [Refresh status](#) - [Help](#)

System Configuration

 [System:](#) **Problem**

[Firewall:](#) **Enabled: Custom**

 [Reporting:](#) **Suspended**

[Remote Access:](#) **Disabled**

View and define information for: **redbooks-rsm.ibm.com** Type: **1818-RS3** Serial: **LKMTPA0**

[Contact Information:](#) **Incomplete**
[Company Information:](#) **Incomplete**
[Connection Information:](#) **Configuration Incomplete**
[Storage Subsystems:](#) **Configuration Incomplete** (0 subsystems currently defined)
[Other SAN Devices:](#) **OK** (0 switches currently defined)
[System Activated:](#) **No**
[Options](#)


Figure 6-8 System Configuration

- Click **Contact Information** to access the contact list to add a new contact (Figure 6-9).


IBM Remote Support Manager for Storage

[Main > Configuration](#)
[Logout](#) - [Refresh status](#) - [Help](#)

Contact List

 [System:](#) **Problem**

[Firewall:](#) **Enabled: Custom**

 [Reporting:](#) **Suspended**

[Remote Access:](#) **Disabled**

Who should IBM Support contact:

View/Configure
 1 [Select to add](#)

[Main > Configuration](#)
[Logout](#) - [Refresh status](#) - [Help](#)

Figure 6-9 RSM contact list


- Click **Select to add**, fill out the form, and click **Update configuration**. This information is important: when a DS Storage Subsystem reports a problem, IBM Service will contact the person specified here. See Figure 6-10 on page 471.


IBM Remote Support Manager for Storage

[Main](#) > [Configuration](#) > [Contact List](#)

[Logout](#) - [Refresh status](#) - [Help](#)

Contact Person Information

 [System:](#) **Problem**
[Firewall:](#) **Enabled: Custom**

 [Reporting:](#) **Suspended**
[Remote Access:](#) **Disabled**

Who should IBM Support contact:

Contact Name
 E-mail address
 Phone number
 Hours to call.
 Time Zone

Alternate phone number (optional)
 Hours to call or other information (optional).

☒ Make this person the primary contact for the RSM for Storage system
 Country or region

[Update configuration](#)
[Delete this contact](#) To remove this contact from the configuration:

[Main](#) > [Configuration](#) > [Contact List](#)

[Logout](#) - [Refresh status](#) - [Help](#)

Figure 6-10 RSM contact person information



7. The specified contact will be added to the contact list. Multiple contacts can be defined and assigned to different storage subsystems. Click **Configuration** to return to System Configuration as shown in Figure 6-11 on page 472.

IBM Remote Support Manager for Storage

[Main](#) > [Configuration](#)

[Logout](#) - [Refresh status](#) - [Help](#)

Contact List

 [System](#): **Problem**
[Firewall](#): **Enabled: Custom**
 [Reporting](#): **Suspended**
[Remote Access](#): **Disabled**

Who should IBM Support contact:

View/Configure

1 [John Doe](#) United States (Primary contact for RSM for Storage)

2 [Select to add](#)

[Main](#) > [Configuration](#)

[Logout](#) - [Refresh status](#) - [Help](#)

Figure 6-11 RSM contact list with contacts



8. The task Contact Information in System Configuration will be marked OK. Click **Company Information** as shown in Figure 6-8 on page 470.
9. Complete the form with the appropriate information and click **Update configuration** as shown in Figure 6-12.

IBM Remote Support Manager for Storage

[Main](#) > [Configuration](#)

[Logout](#) - [Refresh status](#) - [Help](#)

Company Information

 [System](#): **Problem**
[Firewall](#): **Enabled: Custom**
 [Reporting](#): **Suspended**
[Remote Access](#): **Disabled**

Company Information:

* next to an entry indicates missing or incorrect information

IBM	* Company name
Street	* Street Address 1
	Address 2
City	* City
State	* State or Province
10000	* Postal Code
United States	Country or region

[Update configuration](#)

[Main](#) > [Configuration](#)

[Logout](#) - [Refresh status](#) - [Help](#)

Figure 6-12 RSM company information

10. The task Company Information in System Configuration will be marked OK. Click **Connection Information** as shown in Figure 6-8 on page 470.
11. Complete the form with the appropriate information and click **Update configuration** as shown in Figure 6-13.

* next to an entry indicates missing or incorrect information

DIRECT	IP address of SMTP server, or DIRECT (See Help page)
9.11.218.143	IP address of Management Station (optional, see help)
IBM Lab	* Location of RSM for Storage system
Street	* Street Address
City	* City
State	* State or Province
10000	* Postal Code
United States	Country or region

Reporting Connection to IBM

The current Reporting Transmit Method is: **ECC with Email backup**.

Note: You can change the method of sending reports to IBM on the [Options configuration page](#).

IBM ECC Client Status: **Unknown, assumed OK** (Run test to update).

A change has been made to the configuration. Run this (or the full configuration test again).

The ECC Client Connection Test is a shorter version of the Configuration Test. Refresh the main configuration page until the test results are displayed.

[ECC Client Connection Test](#)

ECC HTTPS Proxy Configuration (if required by your network)

	Proxy IP Address (blank if not required)
0	Proxy Port Number
	Proxy User ID (optional)
	Proxy Password (optional)
	Proxy Password Confirm

Remote Access Connections - you must configure one or both of the following:

For a remote modem connection:

NOMODEM	* Modem phone number (0...9 and spaces) or "NOMODEM"
DISABLE	Phone Line Check number. (See Help page.)

For a remote SSH connection:

9.11.218.201	* External IP Address IBM should use (blank to disable)
2222	External Port IBM should use
	External Firewall User ID (optional)
	External Firewall Password (optional)
	External Firewall Password Confirm
22	SSH Port RSM will listen on for remote access (default: 22)

[Update configuration](#)

[Main > Configuration](#) [Logout](#) - [Refresh status](#) - [Help](#)


Figure 6-13 RSM connection information

12. The task Connection Information in System Configuration will be marked OK. Click **Storage Subsystems** as shown in Figure 6-8 on page 470.
13. Click **Select to add** to define a storage subsystem in RSM (Figure 6-14).


IBM Remote Support Manager for Storage

[Main](#) > [Configuration](#)
[Logout](#) - [Refresh](#) - [Help](#)

Configure Storage Subsystems

 [System](#): **Incomplete**

[Firewall](#): **Enabled: Custom**

 [Reporting](#): **Standby**

[Remote Access](#): **Disabled**

There are currently 0 storage subsystems configured:
View/Configure Firmware

1 [Select to add](#)

[Main](#) > [Configuration](#)
[Logout](#) - [Refresh](#) - [Help](#)

Figure 6-14 RSM configure storage subsystem

RSM for Storage reports DS Storage System Expansion units as well, and therefore the configuration of drive expansion units is required. During the configuration test, the profile for each subsystem will be downloaded. This will verify connectivity to the subsystem, verify that this version of RSM for Storage software is compatible with the firmware on the subsystem, and determine if there are any drive expansion units attached to the controller. If any drive expansion units are detected, the configuration status for the subsystem will change to Configuration Incomplete and additional configuration fields will be available for setting the IBM machine type and serial numbers of each detected drive expansion unit.

Complete the form with the following fields:

- a. The name of a storage subsystem, as shown in the DS Storage Manager.
- b. The country where the storage subsystem is located.
- c. A description of where to find the storage subsystem, for example, room number or rack number, in the location field.
- d. Management interface IP addresses of all controllers in the subsystem. If only one controller is installed, use only one IP address.
- e. Type, model, and the serial number. This information can be found on the front bezel of the DS storage subsystem. Select an entry from the contact list.

Click **Update configuration**. Figure 6-15 shows the completed form with sample data.

Machine Description:

* next to an entry indicates missing or incorrect information

DS5020 Hostname (Defined in Storage Manager)

Firmware: **Not available at this time**

9.11.218.190 IP Address #1

9.11.218.191 IP Address #2 (If present)

1814-20A * IBM Product ID (TTTT-MMM) or MTM. Refer to the [Help Page](#) for this field.

78K0DZ8 IBM Serial Number (7 characters)

..... Storage Manager Password

..... Confirm Password

(May be required in order for RSM for Storage to be able to automatically collect a full set of log files. See [Help](#) for more information).

Part of an IBM Solution: **None** (Must be set by IBM Support. Refer to the Help for this page.)

Location where service is required:

123-4567890 * Phone (Rings where service is required)

IBM Lab * Location: Building, Floor, Room

Street * Street Address

City * City

State * State or Province

10000 * Postal Code

United States * Country or region

Contact Information:

John Doe * Who to contact about a problem with this subsystem.

[Update configuration](#)

[Delete this device](#) To remove this subsystem from the configuration:



Figure 6-15 RSM storage subsystem information

14. Repeat the procedure for all the storage subsystems you have attached.
15. If there is an Expansion cabinet attached, the System Configuration shows that the Configuration is still incomplete. The Storage Subsystem Information must be added for the enclosure too as shown in Figure 6-16 on page 476.

IBM Remote Support Manager for Storage

[Main](#) > [Configuration](#)
[Logout](#) - [Refresh](#) - [Help](#)

Configure Storage Subsystems

 [System:](#) **Incomplete**
[Firewall:](#) **Enabled: Custom**
 [Reporting:](#) **Configuration Problem**
[Remote Access:](#) **Disabled**

There are currently 2 storage subsystems configured:

View/Configure	Firmware
1 DS5020	07.77.20.00
2 DS5300 Configuration Incomplete	07.77.18.00
3 Select to add	

[Main](#) > [Configuration](#)
[Logout](#) - [Refresh](#) - [Help](#)

Figure 6-16 RSM Configure Storage Subsystem incomplete

16. Select the Storage Subsystem again as shown in Figure 6-16.

17. Now you will be able to fill in the necessary information for the additional enclosure as shown in Figure 6-17. Click the **Copy this form** button to add more enclosures.

Drive Expansion Units

Expansion Unit ID: 6

* IBM Product ID (TTTT-MMM) or MTM.
 * IBM Serial Number (7 characters)

To remove this subsystem from the configuration:

To define a new subsystem based on this configuration:

[Main](#) > [Configuration](#) > [Storage Subsystems](#)
[Logout](#) - [Help](#)


Figure 6-17 RSM Configure Storage Subsystem continued

18. The storage subsystem will be added to the list of configured storage subsystems as shown in Figure 6-18. Up to 50 storage subsystems and SAN switches can be added. Click **Configuration** to return to the System Configuration.


IBM Remote Support Manager for Storage

[Main](#) > [Configuration](#)
[Logout](#) - [Refresh](#) - [Help](#)

Configure Storage Subsystems

 [System:](#) **Incomplete**

[Firewall:](#) **Enabled: Custom**

 [Reporting:](#) **All Subsystems**

[Remote Access:](#) **Disabled**

There are currently 2 storage subsystems configured:

View/Configure Firmware

1	DS5020	07.77.20.00
2	DS5300	07.77.18.00
3	Select to add	

[Main](#) > [Configuration](#)
[Logout](#) - [Refresh](#) - [Help](#)


Figure 6-18 RSM Configure Storage Subsystem continued

19. Now we want to add other SAN Devices. Click the **Other SAN Devices** button as seen in Figure 6-8 on page 470.
20. Click on Select to add as shown in Figure 6-19.


IBM Remote Support Manager for Storage

[Main](#) > [Configuration](#)
[Logout](#) - [Help](#)

Configure Other Devices

 [System:](#) **Incomplete**

[Firewall:](#) **Enabled: Custom**

 [Reporting:](#) **All Subsystems**

[Remote Access:](#) **Disabled**

Configuration of other SAN devices is optional. See the help page for more information.

There are currently 0 devices defined.

View/Configure Management IP Address

1 [Select to add](#)

[Main](#) > [Configuration](#)
[Logout](#) - [Help](#)

Figure 6-19 RSM Configure Other Devices

21. Fill in the description and the Management IP Address for the SAN Device as shown in Figure 6-20 on page 478. After entering the required Information, press **Update configuration**.

IBM Remote Support Manager for Storage

[Main](#) > [Configuration](#) > [Other SAN Devices](#) [Logout](#) - [Help](#)

Other SAN Devices Information

[System](#): **Incomplete** [Firewall](#): **Enabled: Custom**
[Reporting](#): **All Subsystems** [Remote Access](#): **Disabled**

* Name
 * Management IP Address

[Update configuration](#)
[Delete this device](#) To remove this switch from the configuration:

[Main](#) > [Configuration](#) > [Other SAN Devices](#) [Logout](#) - [Help](#)

Figure 6-20 RSM Other SAN Devices

22. The newly added SAN Device is now added as shown Figure 6-21.

IBM Remote Support Manager for Storage

[Main](#) > [Configuration](#) [Logout](#) - [Help](#)

Configure Other Devices

[System](#): **Incomplete** [Firewall](#): **Enabled: Custom**
[Reporting](#): **All Subsystems** [Remote Access](#): **Disabled**

Configuration of other SAN devices is optional. See the help page for more information.

There are currently 1 devices defined.

View/Configure Management IP Address

1 [IBM2498B40](#) 9.11.218.188

2 [Select to add](#)

[Main](#) > [Configuration](#) [Logout](#) - [Help](#)

Figure 6-21 RSM Add other SAN Devices continued

23. After entering all the desired information, you can verify the information by clicking the **Run Configuration Test** button as shown in Figure 6-22 on page 479.

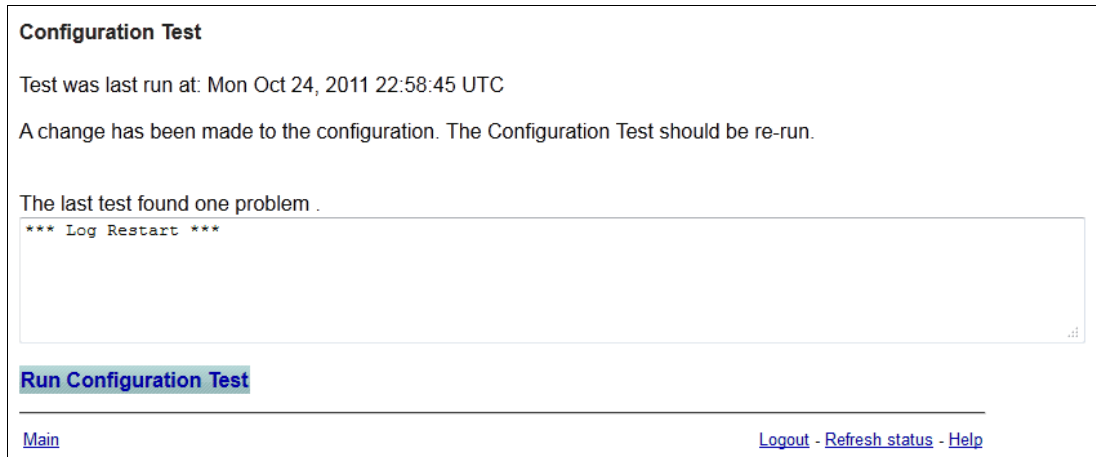


Figure 6-22 RSM Run Configuration Test

24. Click **Refresh status** to see the progress of the test as shown in Figure 6-23.

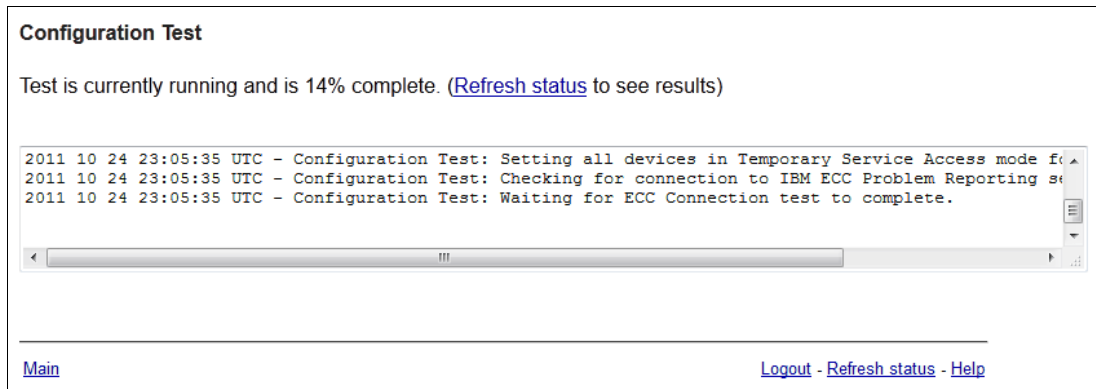


Figure 6-23 RSM Run configuration Test

25. The results from this test are logged in the activity log. You can access the activity log by using an icon on the KDE desktop or you can use the command `tail -fn 10000 /var/log/rsm/activity.txt` to see the contents of the log file as shown in Example 6-1.

Example 6-1 Activity log example

```
2011 10 24 23:05:35 UTC - Starting Configuration Test...
2011 10 24 23:05:35 UTC - Configuration Test: Checking for Modem
2011 10 24 23:05:35 UTC - Configuration Test: NOMODEM specified, skipping modem checks
2011 10 24 23:05:35 UTC - Configuration Test: Setting all devices in Temporary Service Access mode for duration of test.
2011 10 24 23:05:35 UTC - Configuration Test: Checking for connection to IBM ECC Problem Reporting servers.
2011 10 24 23:08:40 UTC - The ECC Connection test is running.
2011 10 24 23:08:43 UTC - The ECC Connection test was successful.
2011 10 24 23:08:44 UTC - Configuration Test: Checking connectivity to Management Station at 9.11.218.143
2011 10 24 23:08:44 UTC - Configuration Test: Checking connectivity to DS5020
2011 10 24 23:08:44 UTC - Configuration Test: Validating subsystem name for DS5020
```

```

2011 10 24 23:08:44 UTC - Configuration Test: Waiting for results of SMcli:
"show storagesubsystem profile"
2011 10 24 23:08:49 UTC - Configuration Test: Checking results of SMcli command
2011 10 24 23:08:50 UTC - History file has been updated
2011 10 24 23:08:50 UTC - Found 0 drive expansion boxes for DS5020
2011 10 24 23:08:50 UTC - Configuration Test: Checking connectivity to DS5300
2011 10 24 23:08:50 UTC - Configuration Test: Validating subsystem name for
DS5300
2011 10 24 23:08:50 UTC - Configuration Test: Waiting for results of SMcli:
"show storagesubsystem profile"
2011 10 24 23:08:55 UTC - Configuration Test: Checking results of SMcli command
2011 10 24 23:08:55 UTC - History file has been updated
2011 10 24 23:08:55 UTC - Found 1 drive expansion boxes for DS5300
2011 10 24 23:08:55 UTC - Configuration Test: No problems detected.
2011 10 24 23:08:55 UTC - Configuration Test: Restoring firewall to original
state.

```

26. When the test is complete, the date and time of the last run is displayed as shown in Figure 6-24.

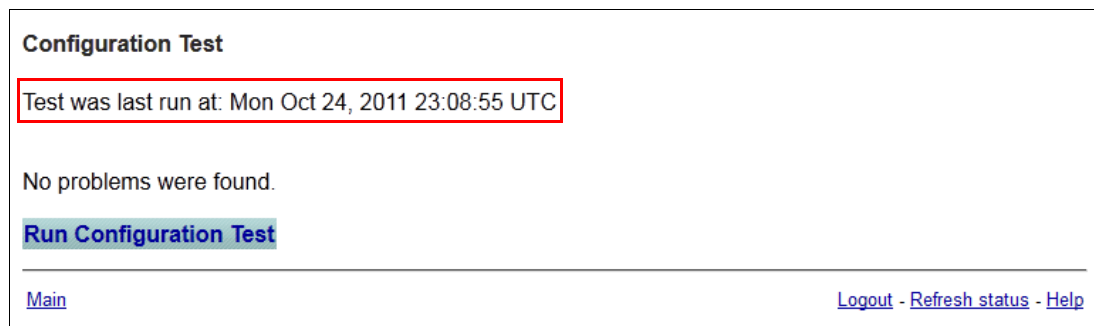


Figure 6-24 RSM configuration test complete

6.2.4 Configuring SNMP traps in Storage Manager

To allow the DS storage subsystem management workstation to send SNMP traps to the RSM server, set the RSM server as your SNMP traps destination in the Storage Manager client.

To configure the Storage Manager to send SNMP alerts for each defined storage subsystem in RSM to the RSM host, perform these steps:

1. Open the Enterprise management window of the Storage Manager.
2. Right-click a DS storage subsystem. In the Connect menu, select **Configure Alerts**.
3. In the Configure Alerts window, click the **SNMP** tab.
4. Type the host name or the IP address of the RSM host in the trap destination field and click **Add** (Figure 6-25 on page 481). Do not change the SNMP community name (the default is *public*).

Configure Alerts

Alerts are generated for all events.

Mail Server | Email | **SNMP**

Alerts for: All storage subsystems

Configured SNMP addresses:

Community Name	Trap Destination
----------------	------------------

Community name (maximum 20 characters):

public

Trap destination (host name, IPv4 address, or IPv6 address):

9.11.218.201

Add Replace Delete Test

OK Cancel Help

Figure 6-25 Storage Manager Configure SNMP Alerts

If you have an existing SNMP infrastructure and there is already an SNMP trap destination set, you can add the IP address of the RSM server as an additional SNMP trap destination without having to delete the existing SNMP trap destination setting.

Validate SNMP configuration

To validate the SNMP configuration, select the SNMP trap destination and click **Test** to send a test trap to the RSM host (Figure 6-26).

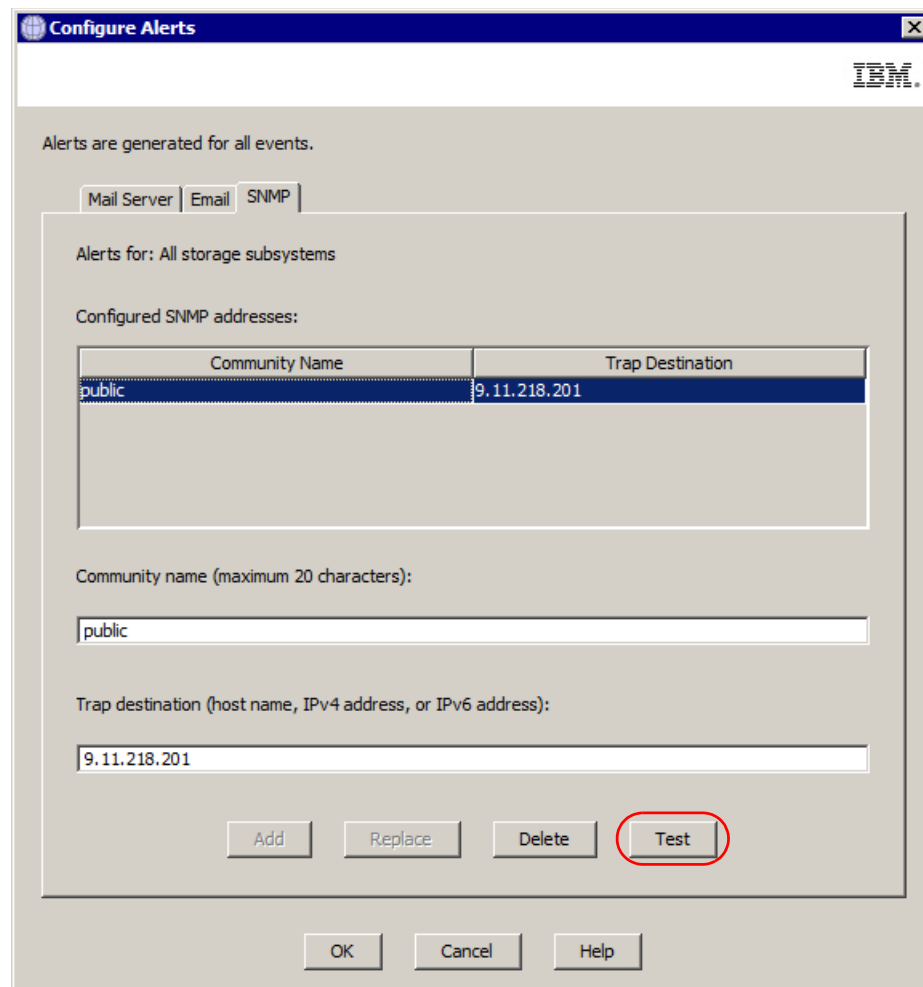


Figure 6-26 RSM Send test trap

Check the activity log (as shown in Figure 6-24 on page 480) and verify that the trap was received. The activity log will contain a entry as shown in Example 6-2.

Example 6-2 Test alert received

2011 10 24 23:10:12 UTC - Received a test alert for DS5300 from 9.11.218.143

6.2.5 Activating RSM

The final step is to activate your system. Complete all the other configurations and run a successful Configuration Test before contacting IBM Service to activate RSM.

To activate RSM, perform these steps:

1. Make sure Remote Access is enabled. Click **Remote Access** in the main RSM window and the **Enable Remote Access** to activate it, if required as shown in Figure 6-27 on page 483. For a complete description, see 6.2.6, “Remote access security” on page 484.

IBM Remote Support Manager for Storage

[Main](#) [Logout](#) - [Refresh status](#) - [Help](#)

Remote Access

[System:](#) Incomplete [Firewall:](#) Enabled: Custom
[Reporting:](#) All Subsystems [Remote Access:](#) Disabled

Manage Remote Access

Remote Access is: Disabled [Enable Remote Access](#)

The Remote Access Timeout is: N/A

Select one of the following to change the current (and default) Remote Access Timeout:

☐ 12 hours ☐ 24 hours ☒ 36 hours ☐ 48 hours ☐ 72 hours ☐ 96 hours [Update Timeout Value](#)

Figure 6-27 RSM Remote access

2. Call the number for IBM Service for your region and give the IBM Machine Type and Serial Number of one of the DS storage subsystems to be monitored by RSM for Storage. For support telephone numbers in your country or region, navigate to the following URL:
<http://www.ibm.com/planetwide>
3. Tell the disk support contact person that you are activating an RSM for Storage system.
4. Provide IBM Service with the phone number of the modem attached to the RSM for Storage system (if used). IBM Service will connect to the system, verify that the configuration is correct, send a test alert through email, verify receipt of the alert and associated attachments, and then activate the system.

When the RSM for Storage system is ready to receive events, the System Status will be OK. See Figure 6-28 on page 484.

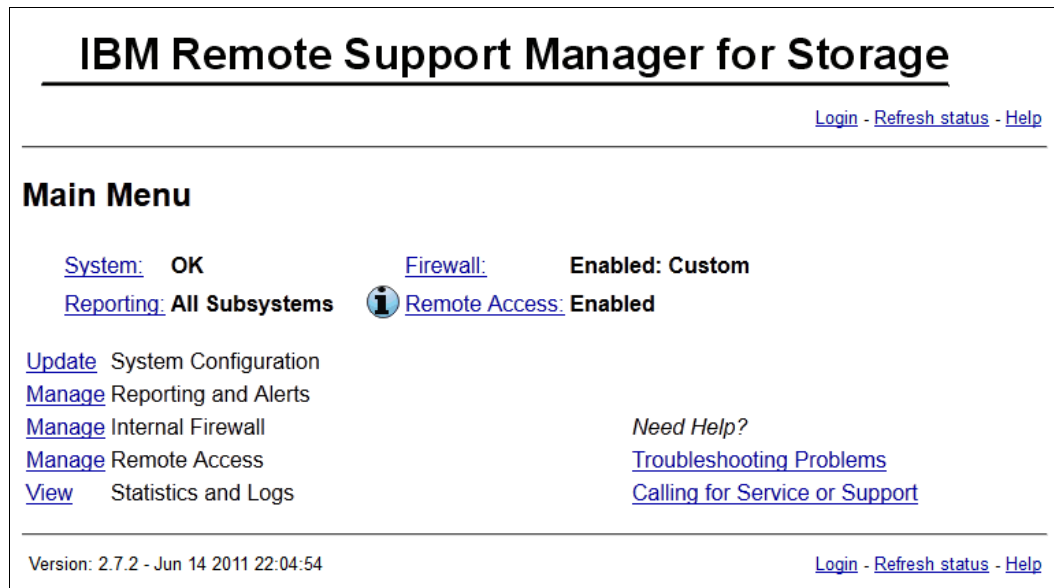


Figure 6-28 RSM main menu: Configured

Note: If you decide to install the RSM for Storage software on another server, you will need to contact IBM Service to obtain a new activation key for the new server.

6.2.6 Remote access security

This section will cover how to secure your IBM System Storage DS subsystem from unauthorized access.

SSH connectivity

In the RSM for Storage Remote Access window, click **Enable Remote Access**. This will reconfigure the RSM for Storage internal firewall to allow connections through SSH port 22.

Verify connectivity using the following steps:

1. From inside your network, open an SSH client and connect to the RSM for Storage system on port 22. (Remember, if you perform these connectivity checks over several days, that the RSM for Storage Remote Access control has a timeout that might need to be reset.) Verify that you are able to obtain a login prompt from the RSM for Storage system.
2. From outside your network, open an SSH client and connect to your external IP address port that has been assigned (port mapped) to the RSM for Storage system.

You should be connected to the RSM for Storage system and receive a login prompt.

Note: You will not be able to complete the login. Authentication requires a special tool only available to IBM Remote Support.

If an authentication process has been put in place by your firewall administrator, verify that the user ID and password for the external firewall is specified in the RSM for Storage Connections configuration.

3. Verify that the SSH connection is correctly configured on the Connections Configuration page. This information will be encrypted and sent with each alert to IBM.

Modem connectivity

Adding a modem to one of your systems creates a potential entry point for unauthorized access to your network. RSM for Storage modifies many characteristics and behaviors of the system it is installed on to protect this entry point and to maximize the amount of control you have in managing remote access.

In RSM, the modem used for remote access by IBM Service will not answer unless one of the storage subsystems has an active alert or Remote Access has manually been enabled.

Normally, Remote Access is enabled automatically when an alert is sent to IBM, but you can choose to wait for IBM Service to contact you when an alert is received and manually enable Remote Access at that time.

On the RSM for Storage Remote Access window, click **Enable Remote Access**. This will enable the modem to answer when called. Verify modem connectivity by calling the modem phone number from a voice phone:

1. Most modems will either flash an LED or you might hear a sound when a call is being received. If there is no indication that a call is being received:
 - a. Plug the phone cable into an analog voice phone and verify that a dial tone is present.
 - b. If a dial tone is present, hang up and then call this phone number from another phone and verify that the phone you just connected rings.
 - c. Reconnect the phone cord to the modem connector labeled line #1.
2. Try again to verify the modem connectivity by calling the modem phone number from a voice phone.
3. Check the instructions that came with the modem and review any troubleshooting information.

To configure the Remote Access policy, perform the following steps:


1. Click **Remote Access** from the Main Menu as shown in Figure 6-28 on page 484.
2. In the Remote Access setting window, you can enable/disable the Remote Access service and enable/disable the option to automatically enable the Remote Access when an alert is sent to IBM. This is shown in Figure 6-29 on page 486.

IBM Remote Support Manager for Storage

[Main](#)
[Logout](#) - [Refresh status](#) - [Help](#)

Remote Access

[System:](#) OK
[Reporting:](#) All Subsystems

[Firewall:](#) Enabled: Custom
 [Remote Access:](#) Enabled

Manage Remote Access

Remote Access is: **Enabled** [Disable Remote Access](#)

The Remote Access Timeout is: **35:39 (hh:mm)**

Select one of the following to change the current (and default) Remote Access Timeout:

☐ 12 hours
 ☐ 24 hours
 ☒ 36 hours
 ☐ 48 hours
 ☐ 72 hours
 ☐ 96 hours

[Update Timeout Value](#)

Option to Enable Remote Access on Alert

You can choose to have the RSM for Storage system automatically enable remote access when an alert is sent to IBM. If this option is disabled, IBM Service will contact you and request that Remote Access be manually enabled so they can access the RSM for Storage system.

The option to automatically enable remote access when an alert occurs is: **Enabled**

[Disable remote access on alert](#)

Additional Information:

If you need to send the modem phone number or SSH connection information to IBM in an email, you can send this string instead of the actual information:

E40E3-12225-D3355-99FF5-55522-5D3A9-9D40B-8E3AD-BDBD5-62434-3E791-62B9B-0F861-52B0F-7E5DB-0C9C7-E2400-D45D3-A9C7E-221E2-40

IBM Service does not need to be sent the remote login password, it is provided here so you can test the remote login function. Note however that following a successful login, a Challenge/Response (that can only be answered correctly using an internal IBM system) will block further access.

Remote user: **rservice**, password: **RdxTeoUL**

[Main](#)
[Logout](#) - [Refresh status](#) - [Help](#)

Figure 6-29 Remote Access settings

3. Remote Access also has a configurable timeout between 12 to 96 hours. You can manually disable remote access when the service is complete or allow it to time out. After the timeout period has elapsed, the system is guaranteed to return to a secure state without intervention.

To configure the timeout value, scroll down the Remote Access settings window, select the desired timeout value, and click **Update Timeout Value**, as shown in Figure 6-29 on page 486.

Note: You do not need to provide the rservice user ID password to IBM Service because IBM Service has an internal tool that provides the current rservice password. You only need to provide passwords of your storage subsystems or your other SAN devices, if required.

Internal firewall

RSM for Storage includes an internal firewall to limit the scope of access a remote user has to your network. It also limits the IP destinations that can be accessed by local and remote users of the system. The rules for inbound and outbound IP traffic that control the internal firewall are managed dynamically by the RSM for Storage software.

- ▶ The normal state for the firewall is Enabled:Closed, which means that the firewall is operational and configured to allow SNMP traps to be received and emails to be sent. However, access to other devices on your network is not allowed.
- ▶ The Enabled: Custom state indicates that one or more custom rules have been added to `/etc/rsm/rsm-firewall.ibm.conf`. These rules will be active any time the firewall is enabled.
- ▶ The Enabled: Open state means that access to one or more other devices has been enabled. The firewall allows access to any storage subsystem that has an active alert, and also storage subsystems and other SAN devices that have been placed in Service Access mode.

Service Access mode allows you to manually allow access to a device from the RSM for Storage system. You can select storage subsystems that you have previously configured.

Disabling the firewall allows unrestricted access from the RSM for Storage system to your network. To maintain the security of your network, disabling the firewall also disables remote access. Likewise, enabling Remote Access will automatically enable the firewall.

Note: Subsystems with active alerts are automatically allowed access from the Remote Support Manager while the alert is active and do not need to be enabled for Service Access.

To manage the RSM internal firewall and service access of your managed storage subsystems (and other SAN devices) from the web interface, perform the following steps:

1. Click **Firewall** on the Main Menu, as shown in Figure 6-28 on page 484.
2. In the Internal Firewall and Service Access window, you can change the internal firewall status and service access mode of your managed storage subsystems as shown in Figure 6-30 on page 488.

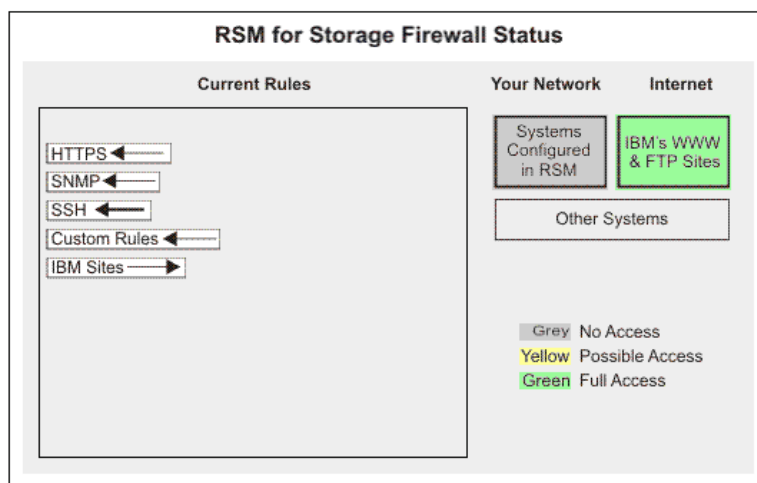
Manage Internal Firewall

Firewall is **Enabled**

- Custom rules for the firewall have been configured.

Note: Disabling the firewall will also disable remote access.

[Disable Firewall](#)



Custom Firewall Rules:

Firewall rules from /etc/rsm/rsm-firewall.ibmecf.conf:

```
OUTPUT -o eth+ -d 170.225.15.41 -j ACCEPT
OUTPUT -o eth+ -d 192.109.81.20 -j ACCEPT
OUTPUT -o eth+ -d 170.225.15.28 -j ACCEPT
OUTPUT -o eth+ -d 170.225.15.107 -j ACCEPT
OUTPUT -o eth+ -d 129.35.224.107 -j ACCEPT
OUTPUT -o eth+ -d 170.225.15.104 -j ACCEPT
OUTPUT -o eth+ -d 129.35.224.104 -j ACCEPT
OUTPUT -o eth+ -d 129.35.224.115 -j ACCEPT
OUTPUT -o eth+ -d 170.225.15.115 -j ACCEPT
```

Manage Service Access

Any configured device may be placed in temporary in Service Access mode. This creates a rule for the internal firewall that will allow connections to that device from the RSM for Storage system. These temporary firewall rules will be removed when the Service Access Timeout expires.

[Manage](#) Service Access for storage subsystems. (0 - currently enabled)

[Manage](#) Service Access for other SAN devices (0 - currently enabled)

[Disable Service Access for all devices](#)

The Service Access Timeout is: **N/A**

Select one of the following to change the current (and default) Service Access Timeout:

- ☐ 12 hours
 ☐ 24 hours
 ☒ 36 hours
 ☐ 48 hours
 ☐ 72 hours
 ☐ 96 hours

[Update Timeout Value](#)

[Main](#)

[Logout](#) - [Refresh status](#) - [Help](#)

Figure 6-30 Internal Firewall and Service Access window

Placing a device into Service Access mode will create a rule for the internal firewall that will allow connections to that device from the RSM server. For subsystems with active alerts, they are automatically allowed access from the Remote Support Manager while the alert is active and do not need to be enabled for Service Access.

3. Similar to Remote Access, you can also modify the Service Access Timeout. To set the Service Access Timeout, go to the Manage Service Access section in the Internal Firewall and Service Access window, select the desired Service Access Timeout value, and click **Update Timeout Value** as shown in Figure 6-30 on page 488.

IBM System Storage DS security

The Storage Manager has the ability to require an administrative password to make changes to the subsystem configuration. We suggest configuring this password.

The IBM System Storage DS subsystems also have a controller shell environment that is accessible using a TELNET client. Storage Manager has an option to disable TELNET, and we suggest that it be disabled and only used under IBM Service personnel guidance.

6.2.7 Managing alerts

To manage alerts, perform these steps:

1. When RSM receives SNMP alerts from one of the defined storage subsystems, an attention mark (!) is shown next to the reporting link, as shown in Figure 6-31. Click **Reporting** to see the alerts.

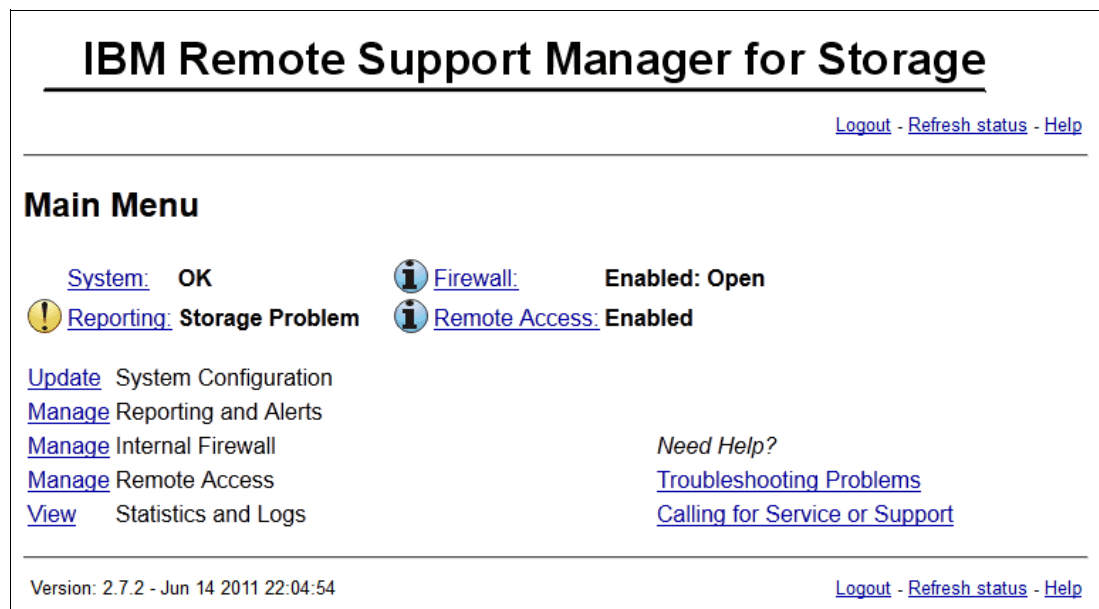


Figure 6-31 Main Menu: Storage Problem


2. The reporting and alert window shows all those subsystems that have sent alerts sent to RSM (Figure 6-32 on page 490). Click **View or Close Alerts**.


IBM Remote Support Manager for Storage


[Main](#)
[Logout](#) - [Refresh status](#) - [Help](#)

Reporting and Alerts

[System:](#) **OK**

 [Firewall:](#) **Enabled: Open**

 [Reporting:](#) **Storage Problem**

 [Remote Access:](#) **Enabled**

Products with Active Alerts: 1	Alerts sent to IBM: 1
Products with Reporting Enabled: 2	Alerts Pending: 0
Products with Reporting Disabled: 0	Alerts Acknowledged: 0

[View/Change](#) reporting state for each subsystem

Events waiting to be processed: **7**

[View Closed Alerts](#) (**0**)

Active Alerts:		Sent	Acknowledged	Pending	Firmware
View or Close Alerts for: DS5020	1	0	0	0	07.77.20.00

[Main](#)
[Logout](#) - [Refresh status](#) - [Help](#)


Figure 6-32 RSM storage subsystem with alerts


3. The alert list for the selected storage subsystem (Figure 6-33) shows all alerts that were received by RSM. Click **View** to see the details of an alert.


IBM Remote Support Manager for Storage


[Main](#) > [Reporting and Alerts](#)
[Logout](#) - [Refresh Status](#) - [Help](#)

Alert List for DS5020

 **System:** OK

 **Firewall:** Enabled: Open

 **Reporting:** Storage Problem

 **Remote Access:** Enabled

Subsystem: DS5020, 9.11.218.190 9.11.218.191
IBM Type/Serial: 1814-20A / 78K0DZ8
Firmware Version: 07.77.20.00 (as of Mon Oct 24, 2011 16:56:36)
Location: IBM Lab, Street, City, 10000, United States
Contact: John Doe

Total alerts for this subsystem: **2**

NOTE: Do not close alerts unless IBM Service has contacted you about the problem. See the help page for more information.

	Date and Time	State	Duplicates	Event Code
View - Close	Mon Oct 24, 2011 23:54:41 UTC	Submitted	5	103
View - Close	Mon Oct 24, 2011 23:54:42 UTC	Holding	1	104

[Close all active alerts for DS5020](#)

[Main](#) > [Reporting and Alerts](#)
[Refresh Status](#) - [Help](#)

Figure 6-33 RSM list of alerts

4. The alert details and an error message are shown in Figure 6-34.

IBM Remote Support Manager for Storage

[Main](#) > [Reporting and Alerts](#) > [DS5020](#)
[Logout](#) - [Refresh Status](#) [Help](#)

Alert Details

[System:](#) **OK**

[Reporting:](#) **Storage Problem**

[Firewall:](#) **Enabled: Open**

[Remote Access:](#) **Enabled**

Subsystem Name: **DS5020**

Type and Model: **1814-20A**

Serial number: **78K0DZ8**

Alert Status: **Submitted**

IBM Service logged in? **No**

Time of alert: **Mon Oct 24, 2011 23:54:41 UTC**

Sent to IBM at **not available**

Duplicates: **5**

Time of last duplicate: **Mon Oct 24, 2011 23:54:43 UTC**

Alert Event Code: **103**

Alert Description: **A needs attention condition has been raised by the controller firmware..
Controller.
Enclosure 85, Slot A**

Log File Available: **Log files could not be downloaded**

NOTE: Do not close alerts unless you have talked with IBM Service

[Close this alert](#) (Service is complete)

[Main](#) > [Reporting and Alerts](#) > [DS5020](#) >
[Refresh Status](#) [Help](#)

Figure 6-34 RSM alert details

5. When the problem is solved, click **Close this alert**.
6. After the alert is closed, it disappears from the alert list. The main menu status changes so that the attention mark disappears after all problems are solved (Figure 6-35 on page 493).

IBM Remote Support Manager for Storage


[Main](#)[Logout](#) - [Refresh status](#) - [Help](#)

Reporting and Alerts

[System:](#) OK

[Firewall:](#) Enabled: Custom

[Reporting:](#) All Subsystems

 [Remote Access:](#) Enabled

Products with Active Alerts: 0

Alerts sent to IBM: 0

Products with Reporting Enabled: 2

Alerts Pending: 0

Products with Reporting Disabled: 0

Alerts Acknowledged: 0

[View/Change](#) reporting state for each subsystem

There are no active alerts.

[View Closed Alerts \(2 \)](#)

[Main](#)[Logout](#) - [Refresh status](#) - [Help](#)

Figure 6-35 RSM main menu



Command-line interface and Script Editor

All Storage Manager functions available through the Subsystem Management window can also be performed and sent to an IBM System Storage DS storage subsystem using statements in scripts. The Script Editor can be used to create or edit a script file, save a script file to the Storage Manager station's local disk, or load a script file from disk. The command-line interface (CLI) can also be used to issue individual commands to the scripting engine from the host operating system command line or to invoke complete, pre-written scripts.

This chapter explains how to work with the command-line interface and the Script Editor. For detailed information about all the CLI parameters, consult the Command Line reference included in the SMclient online help or the guide *IBM System Storage DS3000, DS4000, and DS5000 Command Line Interface and Script Commands Programming Guide*, GC52-1275.

7.1 Command-line interface (CLI)

The Script Engine is built into the Storage Manager software and processes commands one at a time. It is invoked through one of three different methods:

- ▶ Interactive command-line interface
- ▶ Batch command-line interface
- ▶ Script Editor

Both the interactive and batch command-line interfaces use the **SMcli** command, which is packaged with the SMclient GUI. The *interactive command-line interface* connects to a storage subsystem and returns to a command prompt to await typed instructions. This interface is useful for basic storage subsystem configuration, command testing, and connectivity testing.

The *batch command-line interface* uses the **SMcli -f <scriptfile>** form of the command, where scriptfile is simply a series of commands that can be executed. This simple feature gives you the ability to create platform independent script files to execute on the DS5000 storage subsystem. The format of the commands that are put in this file are exactly as those entered on the interactive command-line interface.

The *Script Editor* is accessed from the GUI and provides a simple way to manage a single storage subsystem or test command syntax and execution. It is covered in more detail in 7.2, “Script Editor” on page 522.

Any of these methods provide an efficient way to edit, send, and execute Storage Manager commands on multiple network storage subsystems. The script engine makes it possible to automate many tasks, such as backup procedures or firmware upgrades on the storage subsystem.

The SMclient software must be installed on the station that will be used for command-line instructions. Detailed instructions about the installation of the SMclient can be found in 3.2, “Installing IBM System Storage DS Storage Manager” on page 128.

7.1.1 Using CLI commands

The basic syntax of a CLI command is:

```
command parameter;
```

The most important part of this syntax is the semicolon (;) at the end of the command. This terminates the command and causes the script engine to process it. A typical command looks like this:

```
show storagesubsystem;
```

Before a command can be executed, the user must connect SMcli to the storage subsystem. Both the interactive and batch command-line interfaces can address the target storage subsystem using a number of different identifiers, depending on the management method used:

- ▶ Directly managed (out-of-band): Use the *host name* or *IP address* of either or both controllers. The format is as follows:
SMcli <IP address of one controller> <IP address of second controller>

If the storage subsystem is configured in the Enterprise Management window, the storage subsystem can be specified by its user-supplied name only by using the -n option. The name must be unique to the Enterprise Management window, for example:

```
SMcli -n <name of the DS5000 storage subsystem>
```

If the name of the DS5000 storage subsystem consists of spaces and special characters, double quotes (") have to be used around the name, for example:

```
SMcli -n "Remote DS5100"
```

- Host-agent managed (in-band): Use the *host name* or *IP address* of the managing host (the host that is running the SAgent). For example:

```
SMcli <hostname of managing station>
```

The -n option must be used if more than one host-agent managed storage subsystem is connected to the host, for example:

```
SMcli <hostname of managing station> -n <name of the DS5000 storage subsystem>
```

If the world-wide name of the storage subsystem is specified, use the -w option instead of the -n option, for example:

```
SMcli -w 600A0B800029ED2200000000489C6F56
```

The interactive command-line mode is entered after executing one of the above commands, where one or more commands can be entered. **SMcli** verifies the existence of the specified storage subsystems and returns to a command prompt to await your instructions. Once you have entered the commands, press Ctrl-c to return to the operating system command prompt.

7.1.2 CLI parameters

Example 7-1 shows the help information that is displayed after executing **SMcli -?** in the command prompt window of a WIN platform; a similar output will be seen from a UNIX command line prompt.

Example 7-1 Help on SMcli

```

SMcli <DNS-network-name-or-IP-address>
    [<DNS-network-name-or-IP-address>]
    [-c "<command>;<command2>;..."]
    [-n <storage-array-name> | -w <WWID>]
    [-o <outputfile>] [-p <password>] [-e] [-S] [-quick]
SMcli <DNS-network-name-or-IP-address>
    [<DNS-network-name-or-IP-address>]
    [-f <scriptfile>]
    [-n <storage-array-name> | -w <WWID>]
    [-o <outputfile>] [-p <password>] [-e] [-S] [-quick]
SMcli {-n <storage-array-name> | -w <WWID>}
    [-c "<command>;<command2>;..."]
    [-o <outputfile>] [-p <password>] [-e] [-S] [-quick]
SMcli {-n <storage-array-name> | -w <WWID>}
    [-f <scriptfile>]
    [-o <outputfile>] [-p <password>] [-e] [-S] [-quick]
SMcli -d [-i] [-s] [-w] [-v] [-S]
SMcli -A [<DNS-network-name-or-IP-address1> [<DNS-network-name-or-IP-address2>]] [-S]
SMcli -X (-n <storage-array-name> | -w <WWID> | -h <hostName>)
SMcli -m <ip address> -F <e-mail address> [-g <contactInfoFile>] [-S]
SMcli -x email:<e-mail address>
    [<hostname or IP address1> [<hostname or IP address2>]]
    [-n <storage-array-name> | -w <WWID> | -h <hostName>]
    [-S]
SMcli -a email:<e-mail address>
    [<hostname or IP address1> [<hostname or IP address2>]]
    [-n <storage-array-name> | -w <WWID> | -h <hostName>]}
    [-I <informationToInclude>] [-q <frequency>] [-S]
SMcli {-a | -x} trap:<community>,<hostname or IP address>
    [<hostname or IP address1> [<hostname or IP address2>]]
    [-n <storage-array-name> | -w <WWID> | -h <hostName>]
    [-S]
SMcli -?

```

For additional information, refer to your Command Line Interface documentation

SMcli completed successfully.

Note: The method of accessing help on a CLI interface can vary depending on the operating systems. Enter **SMcli** without any parameters to display a short help message.

The command-line interface supports the command line parameters shown in Table 7-1.

Table 7-1 CLI parameters

Command-line parameter	Description
<IP address> or <hostname>	Specifies an IP address (xx.xx.xx.xx) or host name (of host-agent or controller) of a storage subsystem managed through the host-agent or directly managed method.
-a	<p>Adds a Simple Network Management Protocol (SNMP) trap destination or an e-mail address alert destination.</p> <p>When you add an SNMP trap destination, the SNMP community is automatically defined as the community name for the trap, and the host is the IP address or Domain Name Server (DNS) host name of the system to which the trap will be sent.</p> <p>When you add an e-mail address for an alert destination, the e-mail address is the e-mail address to which you want the alert message to be sent.</p>
-A	<p>Specifies a storage subsystem to add to the management domain. Specify an IP address (xx.xx.xx.xx) for each controller in the storage subsystem.</p> <p>Important: If you specify one IP address, the storage subsystem will be partially managed. If no IP address is specified, an automatic discovery is performed for storage subsystems attached to the local subnet.</p>
-c	<p>Specifies the list of commands to be performed on the specified storage subsystem.</p> <p>Important: Note the following usage requirements:</p> <ul style="list-style-type: none"> ▶ You cannot place multiple -c parameters on the same command line. However, you can include multiple commands after the -c parameter. ▶ Each command must be terminated with a semicolon (;). ▶ Windows: The entire command string must be enclosed in double quotes ("). Each command must be terminated with a semicolon (;). ▶ UNIX: The entire command string must be enclosed in single quotes ('). Each command must be terminated with a semicolon (;). <p>Note: Any errors encountered when executing the list of commands, by default, cause the execution to stop. Use the on error continue; command first in the list of commands to override this behavior.</p>
-d	<p>Displays the contents of the configuration file in the following format:</p> <p><storageSubsystemName> <hostname> <hostname></p> <p>The configuration file lists all known storage subsystems that are currently configured in the Enterprise Management window.</p>
-e	Executes the commands only, without performing a syntax check first.
-f	<p>Specifies the name of a file containing script engine commands to be performed on the specified storage subsystem. Use the -f parameter in place of the -c parameter.</p> <p>Note: Any errors encountered when executing the list of commands, by default, cause the execution to stop. Use the on error continue; command in the script file to override this behavior.</p>
-F	Specifies the e-mail address that sends the alerts.
-g	Specifies an ASCII file that contains e-mail sender contact information that will be included in all e-mail alert notifications. The CLI assumes that the ASCII file is text only, without delimiters or any expected format. Do not use this terminal if a userdata.txt file exists.
-h	Use this parameter to specify the host name that is running the SNMP agent to which the storage subsystem is connected. Use this parameter with the -a and -x parameters.
-l	<p>Specifies the type of information to be included in the e-mail alert notifications. You can select these values:</p> <ul style="list-style-type: none"> ▶ eventOnly ▶ profile ▶ supportBundle

Command-line parameter	Description
-i	Shows the IP address of the known storage subsystems. Use this terminal with the -d terminal. The file's contents use the format storage-system-name IP-address1 IPAddress2.
-m	Specifies the IP address or host name of the mail/SNMP server that will send the alerts.
-n	Specifies the storage subsystem name on which you want to perform the script commands. This name is optional when a <hostname> or <IP address> is used. However, if you are managing the storage subsystem using the host-agent management method, you must use the -n option if more than one storage subsystem is connected to the host at the specified address. This name is required when the <hostname> or <IP address> is not used. However, the storage subsystem name must be configured for use in the Enterprise Management window and must not be a duplicate of any other configured storage subsystem name.
-o	Specifies a file name for all output text from the script engine. If this parameter is not used, the output goes to stdout.
-p	Specifies the password for the storage subsystem on which you want to run commands. A password is not necessary under these conditions: <ul style="list-style-type: none"> ▶ A password has not been set on the storage subsystem. ▶ The password is specified in a script file that you are running. ▶ You specify the password by using the -c terminal and the set session password= password command.
-q	Specifies the frequency at which you want to include additional profile or support bundle information in the e-mail alert notifications. An e-mail alert notification containing at least the basic event information is always generated for every critical event. If you set the -l terminal to eventOnly, the only valid value for the -q terminal is everyEvent. If you set the -l terminal to either the profile value or the supportBundle value, this information is included with the e-mails with the frequency specified by the -q terminal. These values are valid frequency values: <ul style="list-style-type: none"> ▶ everyEvent: Information is returned with every e-mail alert notification. ▶ 2: Information is returned no more than once every two hours. ▶ 4: Information is returned no more than once every four hours. ▶ 8: Information is returned no more than once every eight hours. ▶ 12: Information is returned no more than once every 12 hours. ▶ 24: Information is returned no more than once every 24 hours.
-quick	Reduces the amount of time that is required to run a single-line operation. An example of a single-line operation is the recreate flashcopy logicalDrive command. This terminal reduces time by not running background processes for the duration of the command. Do not use this terminal for operations that involve more than one single-line operation. Extensive use of this command can overrun the controller with more commands than the controller can process, which causes operational failure. Also, status updates and configuration updates that are usually collected from background processes will not be available to the CLI. This terminal causes operations that depend on background information to fail.
-s	Displays the alert settings for the storage subsystems currently configured in the Enterprise Management window.
-S	Use this parameter to suppress informational messages describing command progress that appear when running script commands. (Suppressing informational messages is also called "silent mode.") This parameter suppresses the following messages: <ul style="list-style-type: none"> ▶ Performance syntax check. ▶ Syntax check complete. ▶ Executing script. ▶ Script execution complete. ▶ SMcli completed successfully.
-v	Use this parameter with the -d parameter to display the current global status of the known devices in a configuration file.

Command-line parameter	Description
-w	Specifies the storage subsystem, using its world-wide name (WWN), on which you want to perform the script commands. Note: The WWN is optional when a <hostname> is used or if the -n option is used to identify the storage subsystem with its <storagearrayname>. Use this option <i>instead</i> of the -n option.
-x	Delete an SNMP trap destination or e-mail alert destination. To delete an SNMP trap destination, enter: -x trap:Community, HOST Here COMMUNITY is the SNMP Community Name, and HOST is the IP address or the host name of a station running an SNMP service. To delete an e-mail alert destination, enter: -x email:MAILADDRESS Here MAILADDRESS is the fully qualified e-mail address to which the alert message will no longer be sent.
-X	Use this parameter to delete a storage subsystem from a configuration.
-?	Displays usage information.

Basic interactive command-line execution examples are shown in Example 7-2. In the example, the user runs the command **show storagesubsystem time;**. Note that the user presses Ctrl-c to exit the interactive mode and return to the command line prompt, which is the same for both UNIX and Windows.

Example 7-2 SMcli command in interactive mode

```
C:\temp>"C:\Program Files\IBM_DS\client\SMcli" 9.11.218.183 9.11.218.182 -p
xxxxxxx
Executing script...
```

```
show storagesubsystem time;
Controller in Slot A
Date/Time: Tue Sep 15 11:38:35 GMT-07:00 2009
Controller in Slot B
Date/Time: Tue Sep 15 11:38:32 GMT-07:00 2009
^C
Script execution complete.
```

```
C:\temp>
```

The interactive command-line method can also be invoked using the -c option, which allows a command to execute immediately. This method will execute the specified command and return to the operating system command prompt:

```
SMcli <IP address of one controller> <IP address of second controller> -c
"<command>;"
```

This executes the command that is found after the -c parameter. See Example 7-3 for more details.

Example 7-3 Non-interactive commands

```
C:\temp>"C:\Program Files\IBM_DS\client\SMcli" 9.11.218.183 9.11.218.182 -p xxxx  
xxxx -c "show storagesubsystem time;"  
Performing syntax check...
```

Syntax check complete.

Executing script...

```
Controller in Slot A  
Date/Time: Tue Sep 15 11:48:21 GMT-07:00 2009  
Controller in Slot B  
Date/Time: Tue Sep 15 11:48:17 GMT-07:00 2009  
Script execution complete.
```

SMcli completed successfully.

```
C:\temp>
```

If the batch command-line interface method is used, a script file can also be specified. The **SMcli** command will verify the file location and syntax of the commands. Each of the commands will be executed one at a time. When the commands are all executed, the **SMcli** command returns to the operating system command prompt. The command has the following format:

```
SMcli <IP address of one controller> <IP address of second controller> -f <script  
file name>
```

This executes the commands contained in the script file. If the script file is not in the SMclient directory or the path to the SMclient in the system environment settings, the full path to the script must be specified. See Example 7-4 on page 503, where the command **show StorageSubsystem time; show StorageSubsystem lunmappings;** is embedded in the pre-written script (script11.txt).

Example 7-4 Sending scripts to SMclient

```
C:\temp>"C:\Program Files\IBM_DS\client\SMcli" 9.11.218.183 9.11.218.182 -p xxx
xxxx -S -f "C:\temp\script11.txt"
Controller in Slot A
Date/Time: Tue Sep 15 15:11:46 GMT-07:00 2009
Controller in Slot B
Date/Time: Tue Sep 15 15:11:43 GMT-07:00 2009
MAPPINGS (Storage Partitioning - Enabled (3 of 8 used))-----
```

Logical Drive Name	LUN	Controller	Accessible by	Logical Drive status
AIX_Boot	3	A	Host Group AIX_ITS0	Optimal
Secured1	2	A	Host Group AIX_ITS0	Optimal
test3	4	A	Host Group AIX_ITS0	Optimal
RAID1_SATA_00	0	B	Host Group LAB_SVC_Cluster_1	Optimal
Access Logical Drive	31	A,B	Host WinITS0	Optimal
TC-2008-1	0	B	Host WinITS0	Optimal

```
C:\temp>
```

This method can be used, for example, to automatically create (by combining native operating system commands with CLI commands) a FlashCopy logical drive, mount it under the operating system, and create a backup of it.

For detailed information about the CLI parameters, consult the Command Line reference included in the SMclient online help or the guide *IBM System Storage DS3000, DS4000, and DS5000 Command Line Interface and Script Commands Programming Guide*, GC52-1275.

7.1.3 Syntax requirements

The **SMcli** command has some specialized syntax requirements, but most of them can be simplified by using the batch command-line interface. A script file simply contains the list of commands that are normally run from the command line, so no special formatting is required. The script can be used by any **SMcli** command on any platform without modification.

SMcli has the following usage and formatting requirements:

- ▶ Usage requirements that apply to all operating systems:
 - All statements must end with a semi-colon (;).
 - Separate each base command and any parameters with a space.
 - Separate each parameter and its parameter value with an equal sign.
 - The Script Editor and command-line interface are not case-sensitive. Any combination of upper- and lowercase letters can be entered.
 - Invoking **SMcli** with no arguments or with an unrecognized parameter will cause usage information to be displayed.
 - Arguments used after the -n, -o, -f, and -p options that contain a space, a number, or a special character (<, >, ', !, *, for example) need to be enclosed in single quotes (') or double quotes ("), depending on the operating system being used.
 - Arguments used after the -n, -o, -f, and -p options that contain a single quote character (') need to be enclosed in double quotes (").

- Invoking **SMcli** and specifying a storage subsystem, but not specifying the commands or script file to execute, will cause **SMcli** to run in interactive mode. Use Ctrl-c to stop **SMcli** execution.
- ▶ Usage requirements that apply to Windows operating systems only:
 - Insert a backslash (\) before each double quote character (") when the double quotes are used as part of a name or command syntax (for example, -c "set storageSubsystem userLabel=\"string\";").
 - Insert a backslash (\) before each quote around a user label that contains spaces (for example, -c "start logical driveCopy source=\"Mirror Repository 1\" target=trg9 priority=high;").
 - Insert three backslashes (\\\) in front of the (") to display the backslash when used with the -n, -o, -f, or -p option (for example, -n "Jason\\\" to specify storage subsystem named Jason\).VolumeCopy
 - Insert five backslashes (\\\\\) in front of the (") to use the backslash character as part of the literal command string (for example, -c "set storageSubsystem userLabel=\"Jason\\\\\"," to change the name of the storage subsystem to Jason\).
 - Insert a caret (^) before each special script character (^, &, |, <, >) when that character is used with the -n, -o, -f, and -p options (for example, -n "CLI^&CLIENT" to specify storage subsystem "CLI&CLIENT"). See the appropriate operating system scripting documentation for a list of special script characters.
 - Insert three carets (^^^) before each special script character when used within a literal script command string (for example, -c "set storageSubsystem userLabel=\"Finance^^^&payroll\";" to change the name of the storage subsystem to Finance&Payroll).
- ▶ Usage requirements that apply to UNIX operating systems only:
 - The entire command string must be enclosed in single quotes ('), although some simple commands might also work with double quotes (").

Important: As a general recommendation, it is better to avoid using special characters in order to stick to a simple command syntax.

7.1.4 Error reporting

When the CLI encounters an error, it writes information describing the error directly to the command line and sets a return code. Depending on the return code, the CLI might also write additional information about which parameter caused the error. The CLI will also write information about what it was expecting in the command syntax to help you identify any syntax errors you might have entered.

When an exception occurs while a command is running, the CLI captures the error and, at the end of processing the command (after the command processing information has been written to the command line), the CLI automatically saves the error information to a file.

Special command-line options are not required to save the error data. Additionally, if the CLI must abnormally end CLI and script commands, error data is collected and saved before the CLI finishes.

The name of the file to which error information is saved is `excp rpt.txt`. It is located in Windows directory `C:\Program Files\IBM_DS\client\data`. The file name or location cannot be changed. The file is overwritten every time an exception occurs. To save the information in the file, copy it to a new file or directory.

7.1.5 Commands overview

This section shows all of the available commands, and are classified in the following categories:

- ▶ Storage subsystem
- ▶ Controller
- ▶ Physical disk drive
- ▶ Enclosure
- ▶ Array
- ▶ Logical drive
- ▶ Host topology
- ▶ FlashCopy
- ▶ Remote Mirror
- ▶ VolumeCopy
- ▶ Session
- ▶ Other

Throughout the command listings, we have highlighted the most useful commands in **bold**.

Please be advised that the list of commands you see in the following sections are an overview; for a complete list of the commands and syntax, see *IBM System Storage DS3000, DS4000, and DS5000 Command Line Interface and Script Commands Programming Guide*, MIGR-5076792.

Tip: While the Script Editor and command-line interface syntax have undergone some revisions, the former syntax is still supported. Any scripts that adhere to previous syntax rules will still pass the Script Editor syntax check and will execute.

Storage subsystem commands

Table 7-2 lists the storage subsystem commands.

Table 7-2 Storage subsystem commands

Command	Description
activate storageSubsystem firmware	This command activates firmware that you have previously downloaded to the pending configuration area on the controllers in the storage subsystem.
autoConfigure storageSubsystem	This command automatically configures a storage subsystem. Before entering the autoConfigure storageSubsystem command, enter the show storageSubsystem autoConfiguration command.
autoConfigure storageSubsystem hotSpares	This command automatically defines and configures the hot spares in a storage subsystem.
clear storageSubsystem configuration	This command clears the entire configuration from the controllers in a storage subsystem. There is potential storage subsystem configuration damage.

Command	Description
clear storageSubsystem eventLog	This command clears the storage subsystem event log by deleting the data in the event log buffer. There is potential storage subsystem configuration damage.
clear storageSubsystem firmwarePendingArea	This command deletes, from the pending area buffer, a firmware image or NVSRAM values you have previously downloaded. There is potential storage subsystem configuration damage.
disable storageSubsystem featurePack	This command disables a storage subsystem premium feature.
download storageSubsystem driveFirmware	This command downloads firmware images to all physical disks in the storage subsystem.
download storageSubsystem firmware	This command downloads firmware and, optionally, NVSRAM values for the storage subsystem controller.
download storageSubsystem NVSRAM	This command downloads NVSRAM values for the storage subsystem controller.
enable storageSubsystem featureKey	This command enables a feature using a feature key file.
reset storageSubsystem batteryInstallDate	This command resets the age of the batteries in a storage subsystem to zero days.
reset storageSubsystem RLSBaseline	This command resets the Read Link Status (RLS) baseline for all devices.
reset storageSubsystem logicalDriveDistribution	This command reassigns (moves) all logical drives to their preferred controller.
save storageSubsystem configuration	This command creates a script file that you can use to create the current storage subsystem logical drive configuration.
save storageSubsystem allEvents	This command saves events from the Major Event Log (MEL) to a file. You can save either all the events or only the critical events.
save storageSubsystem performanceStats	This command saves the performance statistics to a file. Before you use this command, issue the set session performanceMonitorInterval and set session performanceMonitorIterations commands to specify how often statistics are collected.
save storageSubsystem RLSCounts	This command saves the RLS counters to a file. Before using this command, issue the reset storageSubsystem RLSBaseline command to get current data.
save storageSubsystem stateCapture	This command saves the state capture to a file.

Command	Description
save storageSubsystem supportData	This command saves the support related information to a file. Support related information includes: <ul style="list-style-type: none"> ▶ Storage subsystem profile ▶ Major Event Log (MEL) information ▶ Read Link Status (RLS) data ▶ NVSRAM data ▶ Current problems and associated recovery information ▶ Performance statistics for the entire storage subsystem ▶ Persistent registration and reservation information ▶ Detailed information about the current status of the storage subsystem ▶ Physical disk diagnostic data ▶ A recovery profile for the storage subsystem ▶ Unreadable sectors detected on the storage subsystem ▶ State capture data
set storageSubsystem	This command defines the properties of the storage subsystem.
set storageSubsystem redundancyMode	This command sets the storage subsystem redundancy mode to either simplex or duplex. Use simplex mode when you have a single controller. Use duplex mode when you have two controllers.
set storageSubsystem time	This command sets the clocks on both controllers in a storage subsystem by synchronizing the controller clocks with the clock of the host from which you issue this command.
set storageSubsystem alarm	This command sets the alarm on or off.
set enclosure id	This command sets the enclosure ID of a controller module or a expansion drawer in a storage subsystem.
set storageSubsystem enclosurePositions	This command defines the position of all enclosures in the storage subsystem.
show storageSubsystem autoConfiguration	This command displays the default autoconfiguration that the storage subsystem will create if you issue the autoConfigure storageSubsystem command.
show storageSubsystem connections	This command lists where drive channel ports are located and where drive channels are connected.
show storageSubsystem	This command returns configuration information about the storage subsystem.
show storageSubsystem hostTopology	This command returns storage partition topology, host type labels, and host type index for the host storage subsystem.
show storageSubsystem lunMappings	This command returns information from the array profile about the storage subsystem LUN mappings.
show storageSubsystem unreadableSectors	This command returns a table of the addresses of all sectors in the storage subsystem that cannot be read.
start storageSubsystem locate	This command locates a storage subsystem by turning on the indicator lights for the storage subsystem.
stop storageSubsystem driveFirmwareDownload	This command stops a firmware download to the physical disks in a storage subsystem that was started with the download storageSubsystem driveFirmware command.
stop storageSubsystem locate	This command turns off the storage subsystem indicator lights that were turned on by the start storageSubsystem locate command.

Controller commands

Table 7-3 lists the controller commands.

Table 7-3 Controller commands

Command	Description
clear allDriveChannels stats	This command resets the statistics for all physical disk channels.
diagnose controller	This command runs diagnostic tests on the controller.
enable controller	This command revives a controller that has become quiesced while running diagnostics.
reset controller	This command resets a controller.
save controller NVSRAM	This command saves a copy of the controller NVSRAM values to a file.
set controller	This command defines the properties for the controllers.
set controller serviceAllowedIndicator	This command turns on or turns off the Service Action Allowed indicator light on a DS4800 82A/84A command module controller. This command is valid only for the DS4800 command modules.
set driveChannel status	This command defines how the physical disk channel performs.
set hostChannel	This command defines the loop ID for the host channel.
show controller	For each controller in a storage subsystem, this command returns: <ul style="list-style-type: none"> ▶ Status (online, offline) ▶ Current firmware and NVSRAM configuration ▶ Pending firmware and NVSRAM configuration configurations (if any) ▶ Board ID ▶ Product ID ▶ Product revision ▶ Serial Number ▶ Date of manufacture ▶ Cache/processor size ▶ Date/time to which the controller is set ▶ Associated logical drives (including preferred owner) ▶ Ethernet port ▶ Physical disk interface ▶ Host interface (this applies only to Fibre Channel host interfaces)
show controller NVSRAM	This command returns the NVSRAM bytes for the specified host type.
show driveChannel stats	This command displays cumulative physical disk channel data transfer and error information.
start driveChannel locate	This command identifies the physical disk enclosures connected to a specific physical disk channel by turning on the indicator lights for the physical disk enclosure connected.
stop driveChannel locate	This command turns off the physical disk enclosure indicator lights that were turned on by the start driveChannel locate command.

Physical disk drive commands

Table 7-4 lists these commands.

Table 7-4 Physical disk drive commands

Command	Description
download drive firmware	This command downloads a firmware image to a physical disk. There can be potential storage subsystem configuration damage.
revive drive	This command forces the specified physical disk to the Optimal state.
save allDrives logFile	This command saves the log sense data to a file. Log sense data is maintained by the storage subsystem for each physical disk.
set Drive hotSpare	This command assigns or unassigns one or more physical disks as a hot spare.
set Drive operationalState	This command sets a physical disk to the failed state.
show Drive	For each physical disk in the storage subsystem, this command returns: <ul style="list-style-type: none"> ▶ Total number of physical disks ▶ Type of physical disk (Fibre or SATA) ▶ Basic physical disk information: ▶ Enclosure and slot location ▶ Status ▶ Capacity ▶ Data transfer rate ▶ Product ID ▶ Firmware level ▶ Physical disk channel information ▶ Enclosure and slot location ▶ Preferred channel ▶ Redundant channel ▶ Hot spare coverage ▶ Details for each physical disk
show allDrives downloadProgress	This command returns the status of firmware downloads for the physical disks targeted by the download drive firmware or download storageSubsystem driveFirmware commands.
start Drive initialize	This command starts physical disk initialization. There can be potential storage subsystem configuration damage.
start Drive locate	This command locates a physical disk by turning on the physical disk indicator lights.
start Drive reconstruct	This command starts reconstructing a physical disk.
stop drive locate	This command turns off the physical disk indicator lights that were turned on by the start drive locate command.

Enclosure commands

Table 7-5 lists these commands.

Table 7-5 Enclosure commands

Command	Description
download enclosure firmware	This command downloads ESM firmware.
set enclosure id	This command sets the ID of a DS4800 82A/84A storage subsystem. The range of valid IDs is from 80 through 99. This range avoids conflicts with existing drive module IDs used for attached expansion enclosures.
set enclosure serviceAllowedIndicator	This command turns on or turns off the Service Action Allowed indicator light on the power-fan canister or interconnect module in a DS4800 82A/84A subsystem.
start enclosure locate	This command locates an enclosure by turning on the indicator lights.
stop enclosure locate	This command turns off the enclosure indicator lights that were turned on by the start enclosure locate command.

Array commands

Table 7-6 lists these commands.

Table 7-6 Array commands

Command	Description
delete array	This command deletes an entire array and its associated logical drives. There can be potential storage subsystem configuration damage.
revive array	This command forces the specified array and associated failed physical disks to the Optimal state.
set array	This command defines the properties for an array.
show array	This command returns the following information about an array: <ul style="list-style-type: none"> ▶ Status (online or offline) ▶ Drive type (Fibre or SATA) ▶ Enclosure loss protection (yes or no) ▶ Current owner (controller slot A or slot B) ▶ Associated logical drives and free capacity ▶ Associated physical disks (drives)
start array defragment	This command starts a defragment operation on the specified array.

Logical drive commands

Table 7-7 lists these commands.

Table 7-7 Logical drive commands

Command	Description
check logicalDrive parity	This command checks a logical drive for parity and media errors, and writes the results of the check to a file.
clear logicalDrive reservations	This command clears persistent logical drive reservations.
clear logicalDrives unreadableSectors	This command clears unreadable sector information from one or more logical drives.
create logicalDrive driveCount= (Automatic Drive Select)	This command creates an array across the storage subsystem physical disks, and a new logical drive in the array. The storage subsystem controllers choose the physical disks to be included in the logical drive.
create logicalDrive drives= (Manual Drive Select)	This command creates a new array and logical drive, and enables you to specify the physical disks for the logical drive.
create logicalDrive array= (Free Capacity Base Select)	This command creates a logical drive in the free space of an array.
delete logicalDrive	This command deletes one or more standard logical drives or FlashCopy and FlashCopy repository logical drives. There can be potential storage subsystem configuration damage.
recover logicalDrive	This command creates a RAID logical drive with the given properties without initializing any of the user data areas on the disks.
remove logicalDrive lunMapping	This command removes the logical unit number mapping.
repair logicalDrive parity	This command repairs the parity errors on a logical drive.
set logicalDrive	This command defines the properties for a logical drive.

Command	Description
show logicalDrive	<p>For the logical drives in a storage subsystem, this command returns:</p> <ul style="list-style-type: none"> ▶ Number of logical drives ▶ Name ▶ Status ▶ Capacity ▶ RAID level ▶ Array where the logical drive is located ▶ Details ▶ Logical Drive ID ▶ Subsystem ID ▶ Physical disk type (Fibre or SATA) ▶ Enclosure loss protection ▶ Preferred owner ▶ Current owner ▶ Segment size ▶ Modification priority ▶ Read cache status (enabled or disabled) ▶ Write cache status (enabled or disabled) ▶ Write cache without batteries status (enabled or disabled) ▶ Write cache with mirroring status (enabled or disabled) ▶ Flush write cache after time ▶ Cache read ahead multiplier ▶ Enable background Media scan status (enabled or disabled) ▶ Media scan with redundancy check status (enabled or disabled) ▶ Pre-Read redundancy check (enabled or disabled) ▶ FlashCopy repository logical drives ▶ Mirror repository logical drives ▶ FlashCopy logical drives ▶ Copies
show logicalDrive actionProgress	<p>For a long-running operation that is currently running on a logical drive, this command returns information about the logical drive action and amount of the long-running operation completed. The amount of the long-running operation that is completed is shown as a percentage.</p>
show logicalDrive performanceStats	<p>This command returns information about the performance of the logical drives in a storage subsystem.</p>
show logicalDrive reservations	<p>This command returns information about the logical drives that have reservations.</p>
start logicalDrive initialize	<p>This command starts the formatting of a logical drive in a storage subsystem.</p>

Host topology commands

Table 7-8 lists these commands.

Table 7-8 Host topology commands

Command	Description
create host	This command creates a new host.
create hostGroup	This command creates a new host group.
create hostPort	This command creates a new host port.
delete host	This command deletes a host.
delete hostGroup	This command deletes a host group.
delete hostPort	This command deletes a host port.
set host	This command assigns a host to a host group or moves a host to a different host group.
set hostGroup	This command renames a host group.
set hostPort	This command changes the host type for a host port.
show allHostPorts	For all host ports connected to a storage subsystem, this command returns the following information: <ul style="list-style-type: none"> ▶ Host port identifier ▶ Host port name ▶ Host type

FlashCopy commands

Table 7-9 lists these commands.

Table 7-9 FlashCopy commands

Command	Description
create FlashCopyLogicalDrive	This command creates a FlashCopy logical drive.
recreate FlashCopy	This command starts a fresh copy-on-write operation using an existing FlashCopy logical drive.
set logicalDrive	This command defines the properties for a FlashCopy logical drive and enables you to rename a FlashCopy logical drive.
stop flashcopy	This command stops a copy-on-write operation.

Remote Mirror commands

Table 7-10 lists these commands.

Table 7-10 Remote Mirror commands

Command	Description
activate storageSubsystem feature=remoteMirror	This command creates the mirror repository logical drive and activates the Remote Mirror feature.
create remoteMirror	This command creates both the primary and secondary logical drives for a Remote Mirror.
deactivate storageSubsystem feature=remoteMirror	This command deactivates the Remote Mirror feature and tears down the mirror repository logical drive.
diagnose remoteMirror	This command tests the connection between the specified primary logical drives and mirror logical drives on a storage subsystem with the Remote Mirror feature installed.
recreate storageSubsystem mirrorRepository	This command creates a new Remote Mirror repository logical drive using the parameters defined for a previous Remote Mirror repository logical drive.
remove remoteMirror	This command removes the mirror relationship between the primary logical drive and secondary logical drive.
resume remoteMirror	This command resumes a suspended Remote Mirror operation.
set remoteMirror	This command defines the properties for a Remote Mirror pair.
show remoteMirror candidates	This command returns information about the candidate logical drives on the remote storage subsystem that you can use as secondary logical drives for a primary logical drive.
show remoteMirror localLogicalDrive synchronizationProgress	This command returns the progress of data synchronization between the primary logical drive and secondary logical drive in a Remote Mirror.
start remoteMirror primary synchronize	This command starts Remote Mirror synchronization.
suspend remoteMirror	This command suspends a Remote Mirror operation.

VolumeCopy commands

Table 7-11 lists these commands.

Table 7-11 Logical drive copy commands

Command	Description
create volumeCopy	This command creates a logical drive copy and starts the logical drive copy operation.
recopy volumeCopy	This command reinitiates a logical drive copy operation using an existing logical drive copy pair.
remove volumeCopy	This command removes a logical drive copy pair.
set volumeCopy	This command defines the properties for a logical drive copy pair.
show volumeCopy	This command returns information about logical drive copy operations. The information returned is: <ul style="list-style-type: none"> ▶ Copy status ▶ Start time stamp ▶ Completion time stamp ▶ Copy priority ▶ Source or target logical drive WWN ▶ Target logical drive read-only attribute setting ▶ Percent completed, if a logical drive copy operation is in progress
show VolumeCopy sourceCandidates	This command returns information about the candidate logical drives that you can use as the source for a logical drive copy operation.
show volumeCopy targetCandidates	This command returns information about the candidate logical drives that you can use as the target for a logical drive copy operation.
stop volumeCopy	This command stops a logical drive copy operation.

Note: Some earlier versions of Storage Manager used “LogicalDriveCopy” instead of the “VolumeCopy” command above. If you are updating to SM V10.6 and are using CLI scripting, we recommend that you check for usage in your scripts.

Other commands

Table 7-12 lists some other available commands.

Table 7-12 Other commands

Command	Description
show “string”	This command shows a string of text from a script file. This command is similar to the echo command in MS DOS and UNIX.
set session	This command defines how you want the current script engine session to run.

7.1.6 CLI examples

Here are examples of how CLI can be used to access and execute script engine commands. Note that the usage for the **-c** parameter varies depending on your operating system (enclosed in single quotation marks (') in UNIX or double quotation marks (") in Windows).

Upgrading the DS5000 controller, ESM, and disk drive firmware

The script in Example 7-5 can be used during a maintenance window to automate the upgrade of all components of the DS5000 storage subsystem. It should only be run in a maintenance window, because firmware updates require a quiescing of the I/O bus. This script is platform independent except for the specification of file names and assumes that the firmware has been downloaded to a local directory. The order for applying the updates is:

1. Controller
2. ESM
3. Drives

Example 7-5 SMcli script to download firmware updates to a DS5000 storage subsystem

On command line:

```
SMcli <AcontrollerIP> <BcontrollerIP> -f firmwareupgrade.scr
```

In the firmwareupgrade.scr file:

```
download storagesubsystem firmware,NVSRAM
file="C:\FW_06100600_06100100.dlp","C:\N1742F700R910V03.dlp";

download alltrays firmware file="C:\esm9326.s3r";

download storagesubsystem drivefirmware file="C:\ST136403FC.LOD"
file="C:\ST173404FC.LOD" file="C:\ST3146807FC.LOD" file="C:\ST318203FC.LOD";
```

The script example assumes that all types of supported drives are present in the storage subsystem. In a specific environment, change the file names to only those updates that are required for that environment. Note that the command for parallel firmware download is different from the command for single drive firmware download.

The first command (**download storagesubsystem firmware, NVSRAM**) will download the firmware and NVSRAM to the controllers. The next command (**download all trays firmware**) downloads the firmware to the ESMs. The final command (**download storagesubsystem drive firmware**) uses the parallel drive download feature. There are 20 different drive types and associated file names, so this last command is be modified to suit the environment.

Staging an upgrade of DS5000 controller firmware and NVSRAM

The script in Example 7-6 stages an upgrade of the firmware for the controller and NVSRAM to be activated at another time.

Example 7-6 SMcli script to stage a controller and NVSRAM firmware update

On command line:

```
SMcli <AcontrollerIP> <BcontrollerIP> -f "c:\stagedfirmwareupgrade.scr"
```

In the c:\stagedfirmwareupgrade.scr file:

```
download storagesubsystem firmware,NVSRAM
file="C:\FW_06100600_06100100.dlp","C:\N1742F700R910V03.dlp" activatenow=FALSE;
```

To activate the upgrade:

```
SMcli 9.11.218.163 9.11.218.164 -c "activate storagesubsystem firmware;"
```

Upgrading individual components in the DS5000 storage controller

The script in Example 7-7 can be useful for testing a new firmware level on a subset of the environment. It is included to show the slight differences in the commands that are required. In particular, the **drive update** command is different when you are not using the parallel upgrade functionality.

Example 7-7 SMcli script to update individual components in the DS5000 storage subsystem

To update the controller only:

```
SMcli 9.11.218.163 9.11.218.164 -c "download storagesubsystem firmware  
file=\"C:\FW_06100600_06100100.dlp\";"
```

To update the NVSRAM only:

```
SMcli 9.11.218.163 9.11.218.164 -c "download storagesubsystem NVSRAM  
file=\"C:\N1742F700R910V03.dlp\";"
```

To update a particular ESM:

```
SMcli 9.11.218.163 9.11.218.164 -c "download tray [1] firmware file=\"C:\esm9326.s3r\";"
```

To update a single drive:

```
SMcli 9.11.218.163 9.11.218.164 -c "download drive [2,3] firmware  
file=\"C:\ST336732FC.LOD\";"
```

Creating and mapping logical drives on AIX

The script in Example 7-8 on page 518 automates the creation of a logical drive and maps it to a storage partition for use by a specified hostgroup. The **SMcli** commands are platform independent, but the script example is from an AIX host and includes some recommended steps to make the storage available to the operating system. This example can be used if a large number of LUNs need to be created from predefined arrays and to existing hosts.

Example 7-8 Script to create and map a logical drives for AIX

```
#!/usr/bin/ksh
#
# -----
#
# Script:      Create LUN on DS5000
# Purpose:     Create several LUNs on DS5000 and allocate to a specific hostgroup.
#              If error message is detected, script will terminate
#
# -----
set -x
#
DATE=`date '+%y%m%d'`
FCMD=/usr/SMclient/SMcli
IP="9.11.218.183 9.11.218.182"
PWDD=xxxxxxx

Create_LUN()
{
LUNNO=$7
$FCMD $IP -p $PWDD -c "create logicaldrive array=$2 userlabel=\"\$1\" capacity=$3 GB
owner=$6 segmentsize=$4;"
error_chk $? Create_$1 quit

# Note we are attaching to a 'hostgroup', this can be changed to 'host' below
$FCMD $IP -p $PWDD -c "set logicaldrive [$1] logicalunitnumber=$7 hostgroup=\"\$5\";"
error_chk $? Allocate_$1 quit

}

error_chk()
{
TIME=`date '+%T'`
if [ $1 -eq 0 ]
then
echo "Process $2 completed Successfully at $TIME"
else
echo "Warning process $2 completed with code $1 at $TIME "
if [ "$3" = "quit" ]
then
echo " ##### ERROR
#####\n"
echo "Process $2 terminating at $TIME"
echo " ##### ERROR
#####\n"
exit 1
fi
fi
}

# Passed variables used below
# LUN name=$1
# ARRAY name $2
# LUN size $3
# Segment size $4
# Host to map to $5
# Preferred Controller a or b $6
# Host LUN number when mapped $7

Create_LUN AIX_A Data_FC 20 64 AIX_ITS0 a 10
```

```
Create_LUN AIX_B Data_FC 20 64 AIX_ITS0 b 11
Create_LUN AIX_C Data_FC 20 128 AIX_ITS0 a 12
Create_LUN AIX_D Data_FC 20 128 AIX_ITS0 b 13

# Run cfgmgr and check final LUN configuration
/usr/sbin/cfgmgr
# For AIX 5.3 use /usr/bin/fget_config command
/usr/bin/mpio_get_config -Av
```

Renaming a DS5000 storage subsystem

Example 7-9, Example 7-10, and Example 7-11 demonstrate the differences between running a command with the -c and -f options. The -c option requires you to be aware of specialized parsing syntax for your particular platform. The -f option eliminates that need.

Example 7-9 Windows command line with -c option

```
C:\temp>"C:\Program Files\IBM_DS\client\SMcli.exe" 9.11.218.183 9.11.218.182 -p
xxxxxxx -c "set storagesubsystem userlabel=\"Tucson_5020\";"
Performing syntax check...
```

Syntax check complete.

Executing script...

Script execution complete.

SMcli completed successfully.

```
C:\temp>
```

Example 7-10 UNIX command line with -c option

```
/usr/SMclient/SMcli 9.11.218.183 9.11.218.182 -p xxxxxxx -c "set storagesubsystem
userlabel=\"ITS0_5020\";" <
Performing syntax check...
```

Syntax check complete.

Executing script...

Script execution complete.

SMcli completed successfully.

```
root@itsop630:/root
#
```

Example 7-11 Script file alternative on Windows or UNIX

```
In userlabel.scr:
set storageSubsystem userlabel="Test DS5020";
```

```
On Windows or UNIX:
SMcli 9.11.218.163 9.11.218.164 -f userlabel.scr
```

Deleting a logical drive

Example 7-12, Example 7-13, and Example 7-14 show the same set of commands being executed on Windows, UNIX, and a script file alternative. The tasks are:

- ▶ Remove mapping of the logical drive named AIX_D.
- ▶ Delete logical drive AIX_D.
- ▶ Show the health status of the storage subsystem, which is managed through the direct management method.

Example 7-12 Windows command line with -c option

```
C:\temp>"C:\Program Files\IBM_DS\client\SMcli.exe" 9.11.218.183 9.11.218.182 -p
passw0rd -c "remove logicaldrive ["AIX_B"] lunmapping hostgroup=\"AIX_ITS0\"
delete logicaldrive ["AIX_B"] ;"
Performing syntax check...
```

Syntax check complete.

Executing script...

Script execution complete.

SMcli completed successfully.

C:\temp>

Example 7-13 UNIX command line with -c option deleting logical drive

```
# /usr/SMclient/SMcli 9.11.218.183 9.11.218.182 -p passw0rd -c "remove
logicaldrive ["AIX_B"] lunmapping hostgroup=\"AIX_ITS0\";"
Performing syntax check...
```

Syntax check complete.

Executing script...

Script execution complete.

SMcli completed successfully.

root@itsop630:/root

Example 7-14 Script file alternative on Windows or UNIX

```
In deletelogicaldrive.scr:
remove logicaldrive ["AIX_A"] lunmapping hostgroup="AIX_ITS0";
delete logicaldrive ["AIX_A"] ;
show storageSubsystem healthStatus;
```

On Windows or UNIX:

```
SMcli 9.11.218.183 9.11.218.182 -p xxxxxxxx -f deletelogicaldrive.scr
```

Configuration Script example 1

Example 7-15 creates a new logical drive using the **create logicalDrive** command in the free space of a array.

Example 7-15 Creating logical drives

```
Show "Create RAID 5 Logical Drive WIN-1 on existing Array Data_FC";

//Create logicalDrive on array created by the create logicalDrive drives command

//Note: For arrays that use all available capacity, the last logicalDrive on the
// group is created using all remaining capacity by omitting the
capacity=logicalDrive
// creation parameter

create logicalDrive array=Data_FC RAIDLevel=5 userLabel="WIN-1" owner=A
segmentSize=16 capacity=20 GB;
show "Setting additional attributes for logicalDrive WIN-1";
//Configuration settings that cannot be set during logicalDrive creation
set logicalDrive["WIN-1"] cacheFlushModifier=10;
set logicalDrive["WIN-1"] cacheWithoutBatteryEnabled=false;
set logicalDrive["WIN-1"] mirrorEnabled=true; set logicalDrive["WIN-1"]
readCacheEnabled=true; set logicalDrive["WIN-1"] writeCacheEnabled=true; set logicalDrive["WIN-1"] mediaScanEnabled=false;
set logicalDrive["WIN-1"] redundancyCheckEnabled=false; set logicalDrive["WIN-1"]
modificationPriority=high;
```

The line beginning with `//Create` is a comment explaining that the purpose of this script file is to create a new logical drive using the **create logicalDrive** command on an existing array.

Tip: For an example of how to set up an entire storage subsystem and the commands required to do this task, look at the output of a saved configuration (select **Storage Subsystem** → **Configuration** → **Save...**) of a configured DS5000 storage subsystem. The output from this configuration will have all the commands and steps to duplicate the configuration or modified to create a different storage controller. It is an excellent source of example commands to complete individual tasks.

Collecting all Support Data example

Example 7-16 gathers the most comprehensive information about the storage subsystem. The command collects data for remote troubleshooting and analysis of problems with the storage management software. All of the files gathered are compressed into a single archive in a zipped file format. The output file should be specified in the **file** string. The output file will be placed in the current directory if no path is specified.

Example 7-16 Collecting support data

```
save storageSubsystem supportData file="DS5300SupportData";
```

Collecting Performance Data example

Example 7-17 on page 522 gathers performance data of the storage subsystem through the use of a script file. All data will be saved in the output file called `CustomerPerfOut.txt`. All error data will be output to a file called `PerfScript_ErrOutput.txt`.

Example 7-17 Script file for collecting performance data

```
In CustomerPerf.scr:
//Performance stats SMcli script: built for W2K customer environments to use

set session performanceMonitorInterval=15 performanceMonitorIterations=120;
save storageSubsystem performanceStats file="CustomerPerfOut.txt";

On Windows:
SMcli -e 10.140.18.216 10.140.18.218 -S -f .\CustomerPerf.scr
>PerfScript_ErrOutput.txt;
```

7.2 Script Editor

The Script Editor is a powerful tool to create and edit scripts. It can verify syntax, run a script, or both, and the scripts can also be saved and later executed to automate storage management procedures.

7.2.1 Using the Script Editor

To open the Script Editor, perform these steps:

1. Select a storage subsystem in the Device Tree View or Device Table from the Enterprise Management window in the Storage Manager Client.

2. Select **Tools** → **Execute Script**, as shown in Figure 7-1, or right-click and select **Execute Script**.

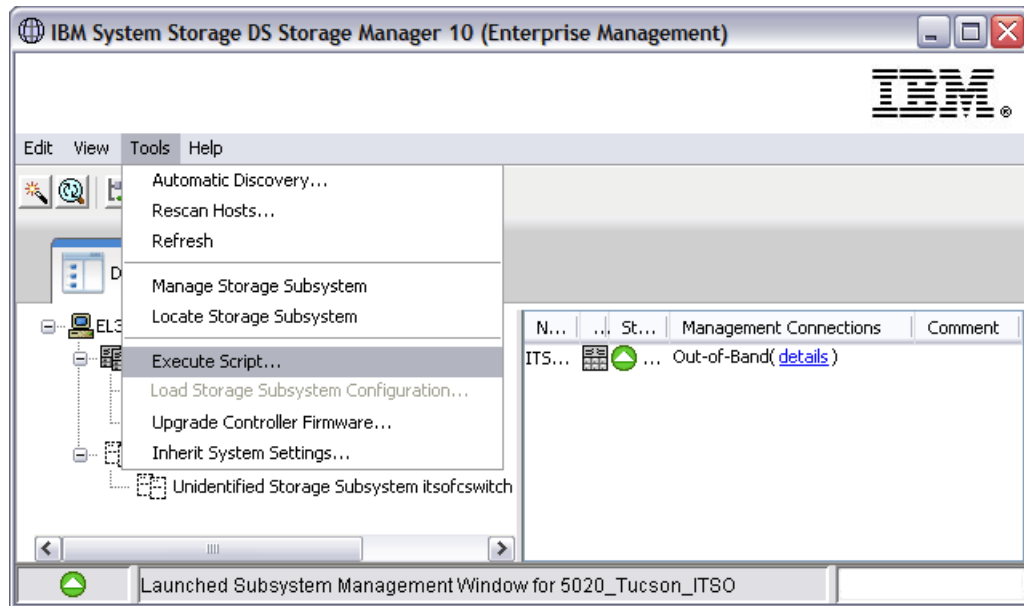


Figure 7-1 Starting the Script Editor

The Script Editor opens, as shown in Figure 7-2. There are two views in the window:

- ▶ Script view: Provides an area for inputting/editing script commands.
- ▶ Output view: Displays verification or execution results.

A splitter bar divides the window between Script View and Output View. You can use the splitter bar to resize the views.



Figure 7-2 The Script Editor

Usage guidelines

Follow these guidelines when using the Script Editor:

- ▶ All statements must end with a semicolon (;).
- ▶ Each base command and its associated primary and secondary parameters must be separated with a space.
- ▶ The Script Editor is not case-sensitive.
- ▶ Each statement must be on a separate line.
- ▶ Comments can be added to the scripts to make it easier for future reference and to understand the purpose of the command statements.

Adding comments to a script

The Script Editor supports the following comment formats:

- ▶ Text contained after two forward-slashes // until an enter character is reached.

For example, the comment The following command assigns hot spare drives is included for clarification and is not processed by the Script Editor:

```
//The following command assigns hot spare drives.  
set drives [1,2 1,3] hotspare=true;
```

Important: A comment beginning with // must end with an end-of-line character, which is inserted by pressing the Enter key. If the script engine does not find an end-of-line character in the script after processing a comment, an error message is displayed and the script execution is terminated. This error commonly occurs when a comment is placed at the end of a script.

- ▶ Text contained between the characters /* and */.

For example, the comment The following command assigns hot spare drives is included for clarification and is not processed by the Script Editor:

```
/* The following command assigns hot spare drives.*/  
set drives [1,2 1,3] hotspare=true;
```

Important: The comment must start with /* and end with */. If the script engine does not find both a beginning and ending comment notation, an error message is displayed and the script execution is terminated.

Using the show command

Use the **show** command with a string (enclosed in a double quotes) and no options to embed in your script comments that display in the output view during script execution. For example, including a **show "START of the script"** command in your script results in the display of START of the script in the output view when this line is processed during script execution. Including **show** statements can help you when writing longer scripts where intermediate steps can make troubleshooting easier, as shown in Figure 7-3.

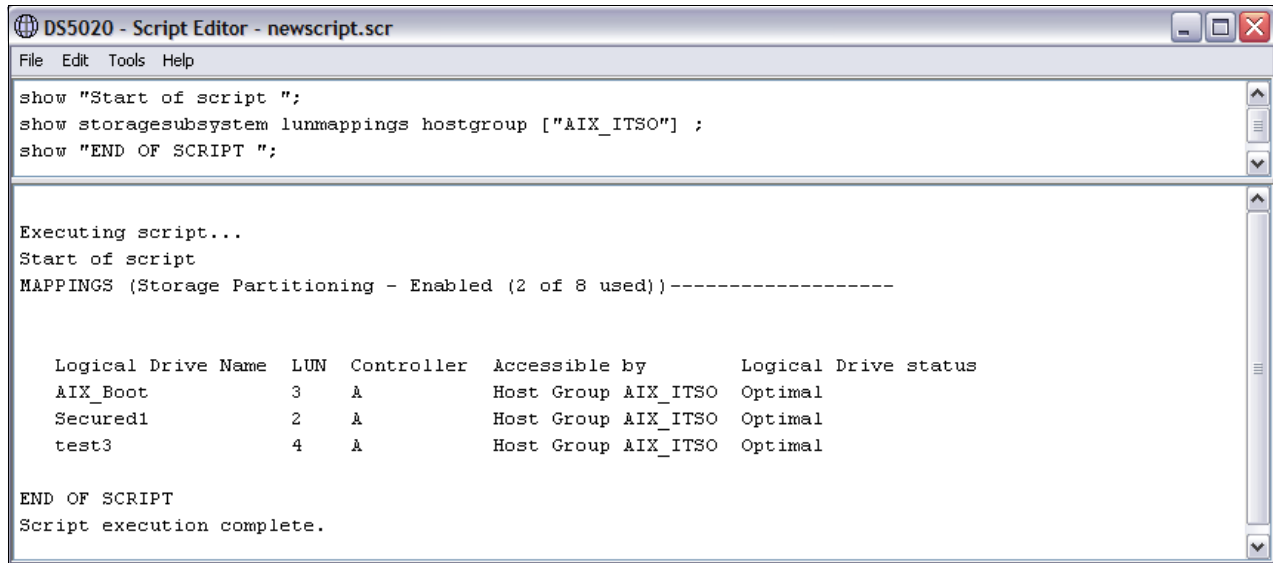


Figure 7-3 Show command in Script Editor

Script Editor tools

The Script Editor offers the following tools to help you when writing scripts:

► Verify Syntax

To run this option, select **Tools** → **Verify Syntax** from the drop-down menu. The Script Editor engine parses the statements in the script file one line at a time and verifies that it has the correct syntax. Any syntax errors are displayed in the output view, reporting the line number of the error and a description of the error. If the Script Editor encounters a syntax error, no further syntax verification is performed on the script. Fix the syntax error and rerun the **Verify Syntax** command to validate the error correction and check the remainder of the statements in the script.

► Verify and Execute

To run this option, select the **Tools** → **Verify and Execute** option. The Script Editor engine parses the command statements in the script, interprets and converts the statements to the appropriate commands, and sends the commands to the storage subsystem.

If a *syntax error* is encountered, the execution stops and an error message is displayed. Fix the error, then use the Verify Syntax or Verify and Execute options to validate the error correction.

If an *execution error* occurs, the script might or might not continue to execute depending on the included On Error script statement. The On Error Stop statement stops the script if an execution error is encountered. The On Error Continue statement allows the script to continue even after an execution error is encountered. (This is the default.)

► Execute Only

To run this option, select the **Tools** → **Execute Only** option. The Script Editor engine executes a script. It displays an error message if a syntax error is encountered.

If an execution error occurs, the script might or might not continue to execute depending on the included On Error script statement. The On Error Stop statement stops the script if an execution error is encountered. The On Error Continue statement allows the script to continue even after an execution error is encountered. (This is the default.)

Note: Certain execution errors, including the inability to communicate with the storage subsystem, always cause the script execution to halt. In these cases, execution stops even if you have used the On Error Continue statement.

Interpreting the script execution results

During script execution, messages are displayed in the output view, beginning with:

Executing script...

After a successful script execution, you see the message:

Script execution complete.

If there is an error during the parse phase, an error indication is displayed in the Output View, giving the line and column number and a description of the syntax error.

If there is an error during execution, a message is displayed in the Output View stating that the command failed and reporting a description of the error.

7.2.2 Embedding commands in batch files

Due to the business demand for higher availability of data, the time window allocated to make backups is shrinking. Customers can no longer afford the daily downtime on their production server to perform backups. This becomes especially true as databases become larger and larger. Online backups improve the availability of the database, but cost CPU, disk, and network resources. Even with the use of incremental and differential backups, the time necessary to perform a backup can be significant.

On the other hand, a feature such FlashCopy enables customers to perform offline backups by creating a point in time copy of a logical device, which can then be presented to a host and backed up. A script can be written, such as the example in Example 7-8 on page 518, which will execute a FlashCopy procedure from the host at a chosen time of day using UNIX “cron” scheduling, for example. Thus, CLI and scripting can become an important tool in managing the DS5000 and host operations.



Deploying iSCSI with the IBM System Storage DS5000 series

This appendix reviews planning considerations when deploying IBM System Storage DS5000 storage subsystems in environments with mixed-host-interface requirements. The Internet Small Computer Systems Interface (iSCSI) Host Interface Card (HIC) is a feature that has been added to the IBM System Storage DS5300 and IBM System Storage DS5100, and included in the IBM System Storage DS5020. Therefore, a specific considerations need to be taken when deploying the storage subsystems with planning to use iSCSI, either on 1 Gbps or 10 Gbps Ethernet. In the mixed interface environment, we review the other iSCSI requirements such as networking, performance, and security.

The DS5000 series of storage subsystems now support intermixed iSCSI and FC host interfaces. Usage of both interfaces provides a greater degree of flexibility in configuration and deployment of a consolidated storage solution to individual servers or hosts attached to a SAN.

iSCSI technology

iSCSI is a protocol that transmits SCSI commands and data over a standard Transmission Control Protocol/Internet Protocol (TCP/IP) based network. The advantage to using a TCP/IP-based network instead of an Fibre Channel based infrastructure is largely based on the cost associated with implementation and support of a Fibre Channel (FC) SAN. In many organizations, a TCP/IP based network already exists and is already being utilized for IP traffic over Local Area Network (LAN) and Wide Area Network (WAN). More recently, the TCP/IP network has also been used for voice traffic with the development of Voice over IP (VoIP). So for some organizations, further use of this existing resource with iSCSI makes sound economic sense.

The iSCSI protocol can be used to transmit data from the connected server to the storage subsystem and vice versa. Generically, the servers are called *initiators*, and the storage subsystem iSCSI ports, such as those available on the IBM DS5000 storage subsystems, are known as *targets*. The targets will listen for connection requests using TCP port 3260 (you can use another port if necessary). You may create other Ethernet ports to handle subsequent communications after a connection between initiator and target is established. An active iSCSI connection is called a *session*, and a session is required for actual data transfer to occur. The basic components of iSCSI communication layer are shown in Figure A-1.

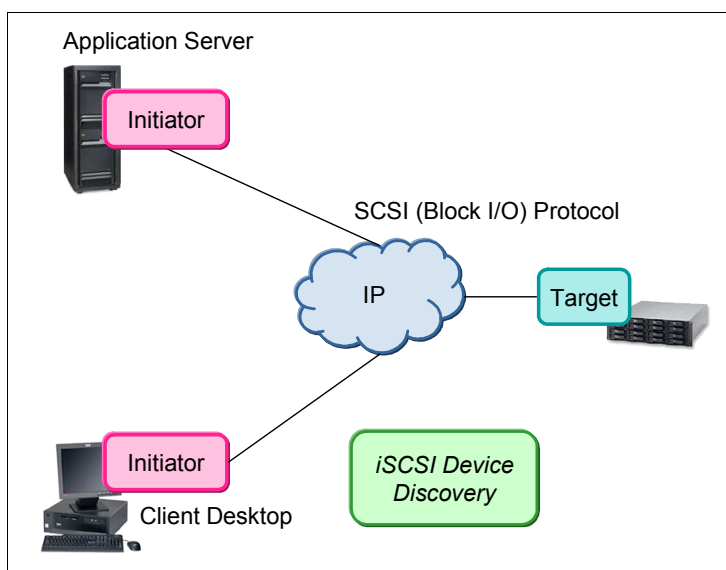


Figure A-1 iSCSI communication components

For the initiator to communicate with the target, you must assign a unique name to both, so that this communication layer can be established. Two types of naming conventions are associated with iSCSI: the IQN, or iSCSI qualified name, and the EUI, or the IEEE EUI-64 identifier.

The IBM DS5000 series of storage subsystems support IQN names.

iSCSI Qualified Name (IQN)

Four major sections comprise an IQN:

- ▶ Type
- ▶ Date
- ▶ Naming authority
- ▶ Unique string

The first section, the type, is the “IQN” string, which indicates that this is an iSCSI qualified name. A period delineates the next field, which is a date code. This date corresponds to the next field, which is a reversed domain name. The date should be the point in time at which the domain name was registered. See an example of IQN in Figure A-2.

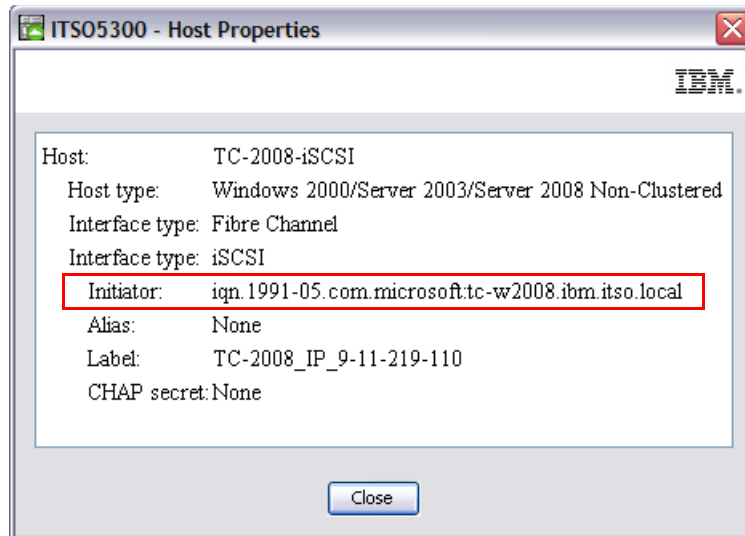


Figure A-2 Example of an IQN name in a defined host

The combination of the domain name and date indicate that the name is based on registered authority. A colon separates the first three fields (the qualification) from the unique string that identifies the device. Many initiators and targets allow you to alter the iSCSI target name, although you cannot alter iSCSI target names in the IBM DS5000 platform. Note that even though iSCSI is in use, the underlying communication protocol is still TCP/IP, so you still need to assign valid IP addresses, along with normal associated IP configuration parameters to all of the appropriate iSCSI initiator and target ports. IQNs are used with iSCSI to allow for name translation services in the event that an underlying IP address were to change for a given initiator or target, for example, using Dynamic Host Control Protocol (DHCP).

After a session has been established between the target and the initiator, you can continue storage provisioning and usage in a manner similar to that of an FC-based storage subsystem.

iSCSI physical components

When planning of the DS5000 as iSCSI target storage subsystem, there are several other components that you use to configure an iSCSI SAN. Of particular interest is the connectivity point for the iSCSI communications within the physical host server itself. You can use several different options to allow iSCSI network traffic to interface with the underlying server hardware. These eventually connect to the operating system and application by using hardware-accelerated host bus adapters (HBAs) and software initiators. Generally, three types of options are available, as detailed in Table A-1.

Table A-1 Adapter technologies comparison

	NIC	TOE	iSCSI HBA
Description	Network Interface Card: Provides Ethernet connectivity.	TCP Offload Engine: A specialized NIC that provides additional functionality.	An HBA that provides Ethernet connectivity and additional functionality.

	NIC	TOE	iSCSI HBA
Function	Physical and data link communications.	TCP physical and data link communications.	iSCSI read/write processing, TCP/IP processing, and physical and data link communication.
Server CPU resource required	iSCSI protocol management and TCP/IP protocol management.	iSCSI protocol management.	None.
Requires Software based initiator	Yes.	Yes.	No.
Performance	Fair.	Good.	Best.

TCP Offload Engine

It is obvious, that the processing of TCP packets from an Ethernet connection consumes many processor resources, and iSCSI protocol only adds another layer of processing. With the number of packets and their corresponding interrupts required for iSCSI, the software iSCSI packet processing can burden the host system with 50–65% processor usage. Depending upon signaling options used, high processor usage might even render certain host applications unusable.

Therefore, it is important that efficient iSCSI systems depend on a hardware *TCP Offload Engine* (TOE) to handle the transportation protocols of iSCSI. A TOE network interface card (NIC) is a dedicated interface card specifically designed for interfacing a server to the IP-SAN including iSCSI offloading and additionally TCP/IP encapsulation from the server processors. A hardware TOE implements the entire standard TCP and iSCSI protocol stacks on the hardware layer. This approach completely offloads the iSCSI protocol from the primary processors, leveraging storage communications efficiently and enabling applications to run faster and more reliable. By using the TCP Offload Engine, a single system can run multiple initiators for improved throughput.

Attention: While deployment of TCP Offload Engine is highly recommended when 1 Gbps iSCSI adapter is used, it is a **must** in environments with 10 Gbps iSCSI adapter connected to 10 GbE Ethernet. Otherwise your processor resources would be seriously saturated.

10 Gigabit iSCSI

Ethernet entered the networking world as a simple 10 Mbps data communication solution tens of years ago, utilizing coaxial cables and BNC connectors. Successive generations have delivered powerful 100 Mbps and 1 Gbps networks at very low cost.

With the continuous development of networking products (host adapters, Ethernet switches, copper and optical cables, etc.), the new standard - 10 Gbps Ethernet (10 GbE) - has emerged as a viable technology to enter the storage networking market. With the 64/66b encoding ratio, it complies with the standards of lossless Ethernet and provides theoretically up to 2450 MB/s of data transfer rate in full duplex mode.

The IBM DS5100 and DS5300 Storage Subsystems offer the 10 GbE Host Interface Cards (HIC) - leveraging the existing lossless 10 GbE network.

Network considerations

You can run the iSCSI protocol on the DS5000 series of storage subsystems, but you must consider a number of areas with regard to network traffic. With normal FC SAN configuration, little planning is required because of the capacity and robustness of the switching and connectivity infrastructure or fabric. This is because a Fibre Channel provides a very low latency and high bandwidth communications medium between the initiator and the target. It has been specifically designed and implemented for high speed data (disk and tape) traffic. With iSCSI, these same statements might not be true and can be subject to external influences outside the traditional SAN itself, such as the existing aforementioned workload of the TCP/IP network.

Because iSCSI utilizes a traditional Ethernet network, many of the same considerations that apply to file-level Networked Attached Storage (NAS) devices, are also true. You should analyze and understand the impact of the network into which an iSCSI target is to be deployed prior to the actual installation and configuration of a DS5000 storage subsystem.

Before beginning an iSCSI deployment, understand and document the network topology that will be used for the SAN. A poorly understood or inadequate networking infrastructure will inevitably lead to what is perceived as poor storage performance. Ensure that you connect a DS5000 storage subsystem with iSCSI host connectivity to the desired initiator using a dedicated Ethernet network with as few “hops,” or switched and routed connections, as possible due to propagation loss and latency. Typically, approximately 1 ms of latency is added for every 100 miles of networked infrastructure, as well as additional latency of up to 1 ms for every routed connection. Thus, connectivity between an iSCSI initiator and an iSCSI target over a LAN is considered ideal and allows for adequate response time metrics between a given application and the underlying storage being used.

Furthermore, 10 Gbps iSCSI deployment on 10 GbE significantly reduces the risk of latency and improves the storage traffic on existing datacenter networking solution.

Several utilities, including ping and trace route, are available at the operating-system level that can be used to help determine network latency between two devices. In addition, you can use other more comprehensive utilities, such as Ethereal, to provide additional insight into the networking infrastructure. In particular, special attention must be paid to Address Resolution Protocol (ARP) packets being sent on the desired iSCSI SAN. ARP requests force a response from all of the devices located on the subnet from which they are broadcast and can have a serious impact on network performance and the underlying iSCSI-based storage subsystem.

iSCSI configurations on the DS5000 series

As well as the basic iSCSI connectivity parameters, such as IP address per target Ethernet port and associated IQN, as detailed in “iSCSI Qualified Name (IQN)” on page 528, you might modify several optional configuration parameters within the context of an iSCSI-enabled DS5000 storage subsystem, including enablement of jumbo frames, configuration of a VLAN, and setting a specific Ethernet priority.

Jumbo frames

Most enterprise 1 GbE and 10 GbE equipment provide some degree of support for jumbo frames, or frames larger than the standard 1500-byte payload limit. Enabling jumbo frames has the following effects:

- ▶ They can accelerate iSCSI performance by about 5 percent.
- ▶ They reduce server processor utilization by 2 percent to 3 percent with standard NICs.

Since TOE cards or HBAs already perform off-loading, the processor savings from jumbo frames is negligible when jumbo frames are used with a TOE or an HBA. However, jumbo frames can still accelerate performance. When using jumbo frames, ensure that all of the devices on your iSCSI network, including switches, initiators, and targets, are configured to use the same maximum jumbo frame size. Jumbo frame sizes are not standardized and can vary from 1501 bytes to 9000 bytes. If the frame size maximum differs between these components, a potentially serious I/O performance problem can be experienced by the hosts.

For example, if the servers, the storage subsystem, or both are set to a maximum frame size that is larger than the setting to which the switches are configured, a DS5000 storage subsystem might appear to be working perfectly. However, if you start performing large data transfers that exceed the switch's maximum frame size, I/O errors might result. Therefore, if jumbo frames are used, make sure to set up and configure jumbo frames across all devices with an agreed maximum size.

If jumbo frames have been enabled and performance appears to be substantially less than expected, disabling jumbo frames on the DS5000 storage subsystem is a simple and quick troubleshooting step, as shown in Figure A-3. We found that, based on empirical tests of several varieties of iSCSI HBAs, that using jumbo frames led to, on occasion, degraded performance.

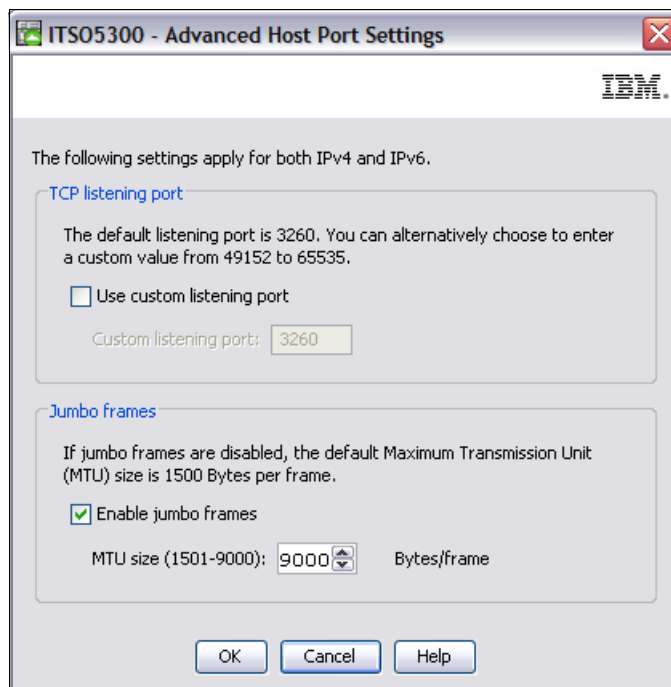


Figure A-3 Jumbo frames enabled on the iSCSI host port

Virtual Local Area Networks

Virtual Local Area Networks (VLANs) are a grouping of devices that communicate on dedicated broadcast network, even though they might be physically separate. A VLAN has the same basic characteristics of a normal LAN, but it allows for a greater degree of flexibility within a networked infrastructure, and it allows reconfiguration using software instead of physical movement of devices. On the other hand, many networking devices connected to the same, common VLAN, could cause additional latency when switching the storage packets between multiple devices in your 1 GbE or 10 GbE network.

In the DS5000 storage subsystems that are connected using iSCSI, you can use an option that enables VLAN support and provides a valid VLAN ID, as shown in Figure A-4. If it is not possible to segregate an iSCSI storage subsystem onto a physically separate LAN, use a VLAN to maximize potential performance.

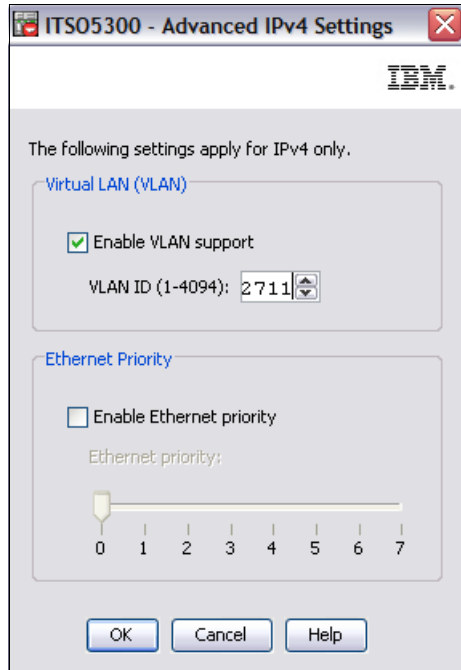


Figure A-4 Ethernet priority and VLAN support for iSCSI port

Ethernet priority

Ethernet priority, sometimes referred to as Quality of Service (QoS) or class of service, is a relatively recent addition to the Ethernet specification. The 802.1 Ethernet standards working group has defined an extension to the Media Access Control (MAC) layer that can take into account a user-defined class of service. The 802.1p specification is a standard for traffic prioritization where network frames are tagged with one of eight priority levels using a 3-bit value added to the Tag Control Info (TCI) inside of a standard Ethernet frame, where 7 is high and 0 is low. Switches and routers that are 802.1p compliant can give traffic that is time-sensitive preferential treatment if the priority tag has been set to a higher value than other traffic. Generically, the seven levels are defined as shown in Figure A-4. The seven levels are:

0	Routine (default)
1	Priority
2	Immediate
3	Flash
4	Flash Override
5	Critical
6	Internetwork Control
7	Network Control

For the DS5000 storage subsystem, you can modify the Ethernet priority of the target iSCSI interfaces to increase the class of service received within the network itself. Use Ethernet priority on isolated networks, both LANs and VLANs, only where multiple hosts and devices exist. Modifying this value can and will impact the performance of other devices located on the network. Avoid using a priority setting of 7, which is the highest priority.

Security

Several security mechanisms are provided by the DS5000 storage subsystem when an iSCSI Host Interface Card (HIC) is present that is not applicable to standard FC communications. Because the storage subsystems can now be employed on a relatively unsecure Ethernet network topology, additional security might be required to comply with organizational or corporate network security guidelines. You can configure both Internet Storage Name Service (iSNS) and Challenge Handshake Authentication Protocol (CHAP) authentication on the DS5000 storage subsystems.

Internet Storage Name Service

The Internet Storage Name Service (iSNS) protocol allows for automated discovery, management, and configuration of iSCSI devices on TCP/IP network. In a typical iSCSI-based storage subsystem without iSNS configured, any and all iSCSI session requests to the target may be allowed from devices on the iSCSI SAN subject to restrictions in place using the partitioning element of the DS5000 series of storage subsystems. The iSNS servers offer additional security services through explicitly defined initiator-to-target mappings and simplified asset locators, similar to that provided by DNS and WINS for IP address lookup facilities. Most modern operating systems allow iSNS services to be established. The DS5000 series of storage subsystems support this capability as well. Figure A-5 shows the configurations settings where the iSNS box has been checked, allowing the iSNS server to be defined.

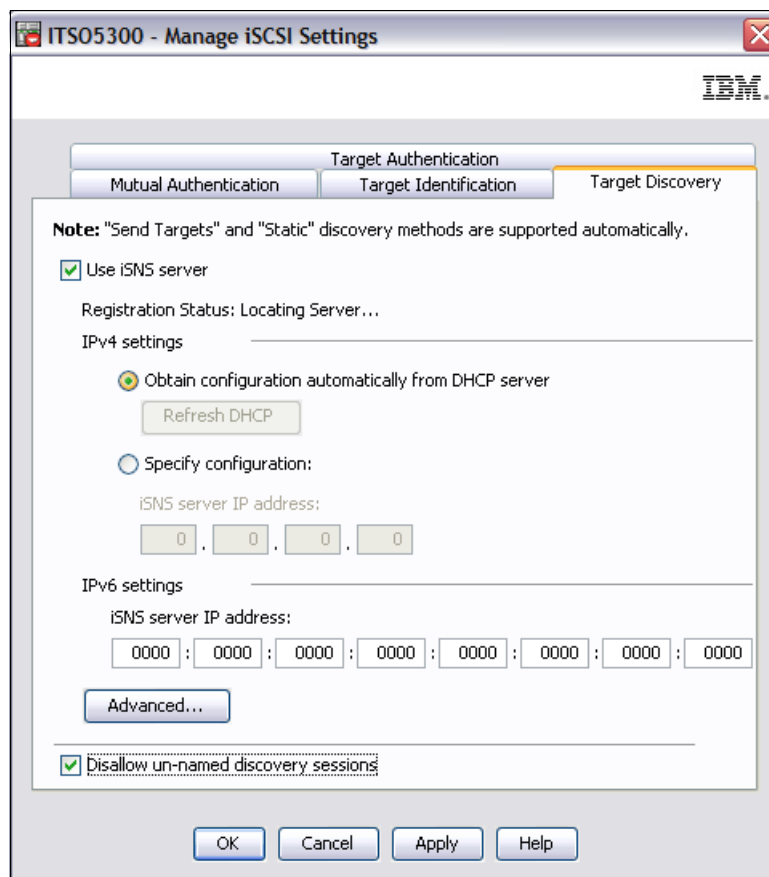


Figure A-5 iSNS settings

The iSNS server listening port is the TCP port number that the controller tries to connect to a server. This process lets the iSNS server register the storage subsystem with the iSCSI target and the iSCSI portals so that the host initiators can find the storage subsystem. The default value for this listening port is 3205.

Challenge Handshake Authentication Protocol

The Challenge Handshake Authentication Protocol (CHAP) provides an additional security layer within the iSCSI SAN on the DS5000 storage subsystems. When CHAP is enabled, the initiator sends the target a random value and an ID value. Both the initiator and the target share a predefined “secret,” or password. The peer then concatenates the random value, the ID, and the secret to calculate a one-way hash using the MD5 hash function. This hash value is then sent back to the initiator, which in turn builds the same string, calculates the MD5 sum, and compares the result with the value received by the target. If the values match, then the iSCSI session is considered established and future communication proceeds with subsequent increases of the ID value to prevent possible replay attacks. By default, CHAP is not enabled nor enforced on the DS5000 storage subsystem and this method is highly recommended for enhanced security. Figure A-6 shows the CHAP setup in the iSCSI settings window.

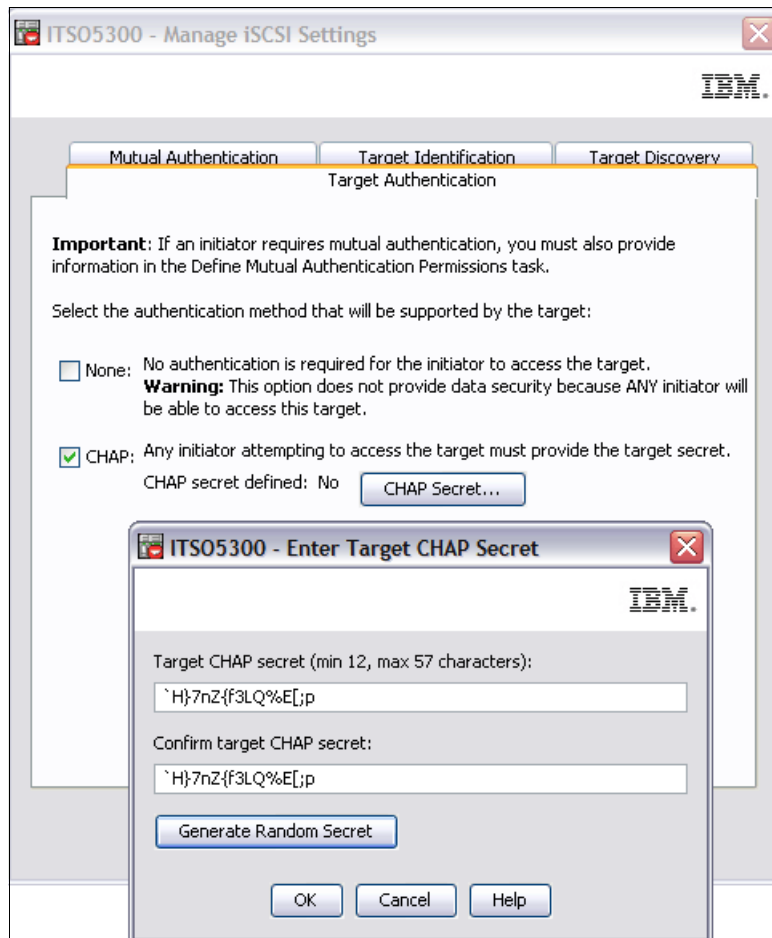


Figure A-6 Configuring CHAP and secret

The CHAP secret must be between 12 characters and 57 characters. The CHAP secret must use ASCII code characters with a decimal value between 32 and 126. In Figure A-6, the utility is used to generate a “secret”.

iSCSI performance considerations

A Fibre Channel SAN almost always yields higher performance than an iSCSI SAN. FC does not suffer from congestion and oversubscription problems as readily as iSCSI due to both the FC protocol and the general segregation of FC traffic itself. FC includes a mechanism for port-to-port throttling, not just end-to-end throttling, and can limit the amount of data that a connected system sends. This mechanism avoids situations in which information must be dropped and avoids degradation into a retransmission recovery scheme that can limit the storage network's performance. For this reason, and many others, including general protocol efficiency, FC is more capable of operating near-wire speed than iSCSI is likely to be.

From the host perspective, you must consider several elements before deploying an iSCSI SAN. These considerations include the number of physical NICs that will be installed in the hosts themselves, the types of NICs (see Table A-1 on page 529), whether a software initiator or a hardware initiator will be used, how many paths will exist between the initiator and the target, which failover, load-balancing driver, or both may be used and, most importantly, what speed will the infrastructure operate. Generically speaking, iSCSI solutions might be a good fit for those environments where the bulk of the data processing activity is considered to be of the random, small-block variety. Given the relatively modest throughput available within a current iSCSI SAN compared to 8 Gbps FC fabrics, it is not likely that adequate throughput will be available within an Ethernet network or the specific target ports to handle workloads that consist primarily of large, sequential transactions. This behavior can be more easily seen using the following simplified equation:

Throughput = IOPS x I/O size

Thus, as the size of the inbound I/Os decrease and typically become more random in nature, as in some applications, databases and general file sharing, the amount of throughput required also is reduced. Conversely, as the size of the inbound I/Os increase and typically become more sequential in nature, such as video editing or disk-to-disk backup, the amount of throughput required greatly increases.

Initial testing of the DS5000 storage subsystems configured with 1 Gbps iSCSI HICs has shown that a heavily configured storage subsystem will likely offer a greater proportion of the "small block random I/O" performance to an 8 Gbps FC configuration. Alternatively, given the maximum of four 1 Gbps iSCSI target ports currently available on the DS5000 series of storage subsystems, enough available bandwidth might not be available to provide high levels of "large block sequential" performance relative to what will potentially be available using multiple 8 Gbps FC interfaces. The performance difference between the two interface types can become very large in this type of environment.

One of the most remarkable conclusions given is that, typically, 1 Gbps iSCSI is not a good fit for the environments or applications that require high throughput.

This dogma is being obviously changed with the implementation of 10 Gbps iSCSI HICs connected into the native 10 GbE network. The network bandwidth, data throughput and enhanced encoding scheme (64/66b) enable iSCSI to be at least equal competitor to the FC deployment. With correctly configured and tuned 10 GbE network and 10 Gbps iSCSI components, we see performance results on a level similar to 8 Gbps FC (where 8/10b encoding is still in place). It is not a surprise, that 10 GbE is a good candidate to compete widely used typical FC-based datacenter networking with dedicated SAN switches, directors, or multiprotocol routers. The 10 GbE (40 and 100 GbE standards already available) gives IT architects and decision makers an option to significantly reduce hardware, operational, and maintenance cost on drastically lower level. With the deployment of iSCSI or Fiber Channel over Ethernet (FCoE) the overall number of managed ports, devices, and cables drops tremendously.

After it has been determined whether a given application might not be a logical candidate for iSCSI connectivity based on throughput requirements, you need to consider whether you will use iSCSI HBAs or use on-board NICs with software initiators. The DS5000 storage subsystems support both methods, and you will make this determination on a cost to required performance basis. In principle, a software initiator performs nearly as well as a hardware initiator in terms of driving storage I/Os. The primary difference is largely in the amount of processor cycles that are required to become devoted to handling iSCSI traffic in the absence of a hardware-based initiator with the appropriate TOE support. Keep in mind that TCP Offload Engine is a must with 10 Gbps iSCSI implementation and I/O intensive applications.

Multipathing iSCSI

As with Fibre Channel SANs, iSCSI SANs, in concert with the DS5000 series, offer the ability to provide failover to the alternate controller in the event of an outage situation. In addition, many failover drivers, such as the native MPIO driver in the Windows 2003 and Windows 2008 operating systems, when combined with the IBM-provided DSM, also offer load-balancing across available iSCSI routes between the target and the initiator as well. Therefore, you still need to configure iSCSI with multiple NIC interfaces for optimal performance and reliability for initiators connecting to a DS5300, DS5100, or DS5020 storage subsystem.

Other iSCSI performance considerations

You must consider several other factors when working with a mixed-host interface environment due to various limitations on the intermixing of the physical protocols at the controller level and the host level.

- ▶ A given host group must not contain hosts that are FC-based as well as hosts that are iSCSI-based.
- ▶ A single host must not be configured for both iSCSI connections and FC connections to the storage subsystem.
- ▶ The Remote Mirroring premium feature is only supported using FC connectivity.
- ▶ TCP Offload Engine (TOE) has to be used with 10 Gbps iSCSI and I/O intensive applications to avoid processors' saturation.

Generically, even though both protocols are available within the storage subsystem itself, take care that at the host and host group level, these protocols remain independent and are used as a tiering strategy across the entire host pool rather than within a given host group or on a singular host itself.

As described previously, FC and iSCSI provide different latency and throughput capabilities, and this mixture within an initiator environment can be prone to failover driver conflict, performance degradation, and data loss.

**B**

Solid State Drives on the IBM System Storage DS5000 series

In this section, we discuss Solid State Drives (SSD), which are supported by the IBM DS System Storage with the DS5000 storage subsystems. We compare this technology to hard disk drives (HDD), and we base this comparison on tests we ran that compared SSDs to HDDs. Lab tests show a significant performance advantage with SSDs with a substantial reduction in the number of drives needed to meet the desired level of performance. Fewer drives translate into a smaller physical footprint, reduced energy consumption, and less hardware to maintain. Tests also showed better application response times using SSDs, which leads to increased productivity and higher customer satisfaction.

SSD technology was introduced more than two decades ago. Until recently, however, the high cost-per-gigabyte and limited capacity of SSDs restricted deployment of these drives to niche markets or military applications. Recent advances in SSD technology and economies of scale have driven down their cost, making them a viable storage option for many I/O intensive applications. While the cost of SSDs is trending downward, the dollar per gigabyte cost for SSDs is still substantially higher than that of HDDs. It is not cost-effective or necessary to replace all HDDs with SSDs. For example, infrequently accessed (cold) data can reside on lower cost HDDs, and frequently accessed (hot) data can be moved to SSDs for maximum performance. The appropriate mix of SSDs and HDDs can be used to strike a proper balance between performance and cost.

SSD technology

Solid State Drives are built mainly from flash memory and augmented with Dynamic Random Access Memory (DRAM) along with a sophisticated internal controller. Flash memory based on the NAND (the logical “Not And” operation) has been available for nearly two decades, and is used in several high-volume consumer electronics applications, including cell phones, PDAs, and MP3 players. Flash memory is non-volatile (it retains data without a power source), involves no mechanical parts, and can be manufactured as standard components in high volume.

Current flash technology manipulates a charge on the floating gate of specially designed transistors to allow representation of two (voltage) states, which translates to a single bit per cell, and is called single layer cell (SLC). SLC NAND-based flash has been dropping in price faster than DRAM and HDDs, and now sits between them in a price range approximately twenty to thirty times more expensive than HDDs but up to ten times cheaper than DRAM. At ten times the price and one hundred times the performance, the value proposition is very compelling for high IOPS applications. This explains why the technology has been around for some time but is just now being introduced in storage solutions, including the DS5000 series.

The flash technology is still evolving and we can expect to see a multiple layer cell or MLC in the future. MLC is designed to allow a more precise amount of charge on the floating gate of the transistor to represent four different states, so translating to two bits of information per cell. This higher density per cell and the potential to store three or more bits of information per cell provides for continuing cost improvement in the coming years. If MLC is successful, flash memory could reach down to only two to three times the price of high-performance HDDs (FC or SAS 15K RPM) in the foreseeable future, close enough to drive a significant substitution rate of low-capacity/high-performance HDDs.

Solid State Drives in tiered storage

Many storage environments have grown to support a diversity of needs and evolved into disparate technologies that have lead to storage sprawl. In a large-scale storage infrastructure, this yields a sub-optimal storage design that can be improved with a focus on data access characteristics analysis and management.

Tiered storage is an approach of utilizing different types of storage throughout the storage infrastructure. It is a mix of higher performing and higher cost storage with lower performing and lower cost storage and placing data accordingly based on specific characteristics, such as performance needs, age, and importance of data availability.

An example of an existing storage environment is shown in Figure B-1. The design results in a significantly increased cost associated with maintaining and supporting the infrastructure. In addition to the immediate effect associated with this balance, growth continues at an increased rate in the higher cost area of Tier 1. Thus, as the growth occurs, the distribution of data continues to grow in a non-optimal direction unless there is careful planning and discipline in deployment.

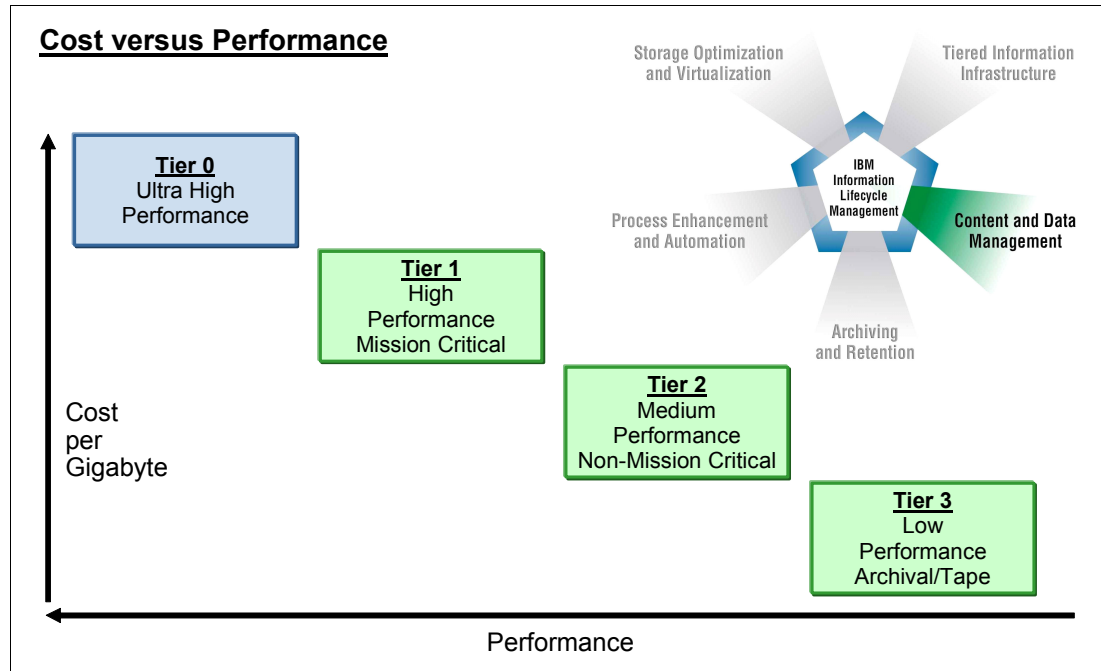


Figure B-1 Tiered Storage: Cost versus performance

Properly balancing these tiers leads to the minimal cost and best performance solution. Typically, an optimal design keeps the active operational data in Tier 0 and Tier 1 and uses Tiers 2 and 3 for less active data. An example is shown in Figure B-2. The benefits associated with a tiered storage approach are simple; it is all cost related. This approach will save significant cost associated with storage itself, as lower tiered storage is less expensive. Beyond that, there are the environmental savings, such as energy, footprint, and cooling reductions.

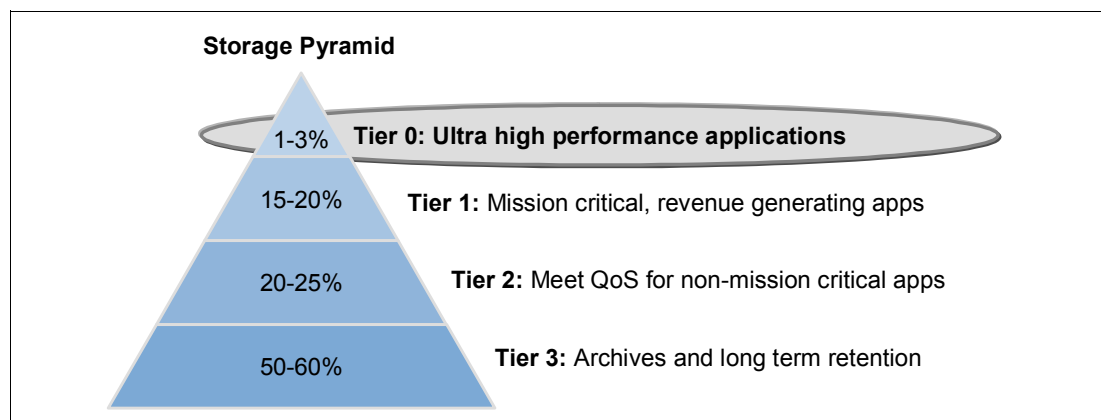


Figure B-2 Example of a tiered storage pyramid

On a DS5000 storage subsystem, delivering these tiers will be in the form of RAID level selection and disk types, so SDD will clearly be used for Tier 0 followed by FC 15k drives and

SATA for the lower tiers. Longer term retentions may even be put on cheaper, external, or transportable media, such as tape, to be kept in libraries or a storage facility away from the data center.

Implementing tiered storage

There are three areas of interest critical to implementing, maintaining, and leveraging a tiered storage solution. These areas are:

- ▶ software tools: For identification and reporting of all components of the tiered storage solution.
- ▶ virtualization: To enable control and allocation of your solution.
- ▶ Offerings that are designed to provide alignment with your specific needs for IT governance.

One useful methodology is Information Lifecycle Management (ILM). ILM is the process of managing information, from creation, through its useful life, to its eventual destruction, in a manner that aligns storage costs with the changing business value of information. A more recent IBM offering is the Novus - Intelligent Storage Service Catalog (ISSC) offering, which is a single framework aimed at providing storage optimization through more efficient provisioning, better analytics of the storage environment, and proper alignment of data to storage tiers. You can obtain more information about this topic at the following address:

<ftp://public.dhe.ibm.com/common/ssi/ecm/en/pow03025usen/POW03025USEN.PDF>

Solid State Drives on a DS5000 storage subsystem

This new, supported feature on the DS5000 series is supported as a base product on all DS5000 only with an EXP5000 expansion enclosure. To install SSDs on a DS5000 storage subsystem, there are some requirements and limitations.

The SSD emulates a conventional hard disk drive, thus easily replacing it in any application. SSDs are available with the same interfaces used by hard disk drives: Serial Advanced Technology Attachment (SATA) and Fibre Channel (FC).

The advantages of SSDs over hard disk drives in a DS5000 storage subsystem include:

- ▶ Faster start up (no spin up)
- ▶ Faster access to data (no rotational latency or seek time)
- ▶ Higher I/O operations per second (IOPS)
- ▶ Higher reliability
- ▶ Lower power usage
- ▶ Less heat produced and less cooling required

Your DS5000 storage subsystem must meet the following criteria to include SSDs:

- ▶ Firmware V7.60 or higher.
- ▶ Only twenty SSDs are supported in a DS5000 storage subsystem.
- ▶ At the time of this writing, 200 GB and 400 GB FC-SAS SSDs (using a FC to SAS interposer) are supported on the DS5000 storage subsystem. The previous 73 GB and 300 GB SSD's are no longer available.

Identifying SSD in Storage Manager

You can identify SSDs in Storage Manager either by the label “SSD” or an icon, as shown in Figure B-3, in the row “Media Type”.

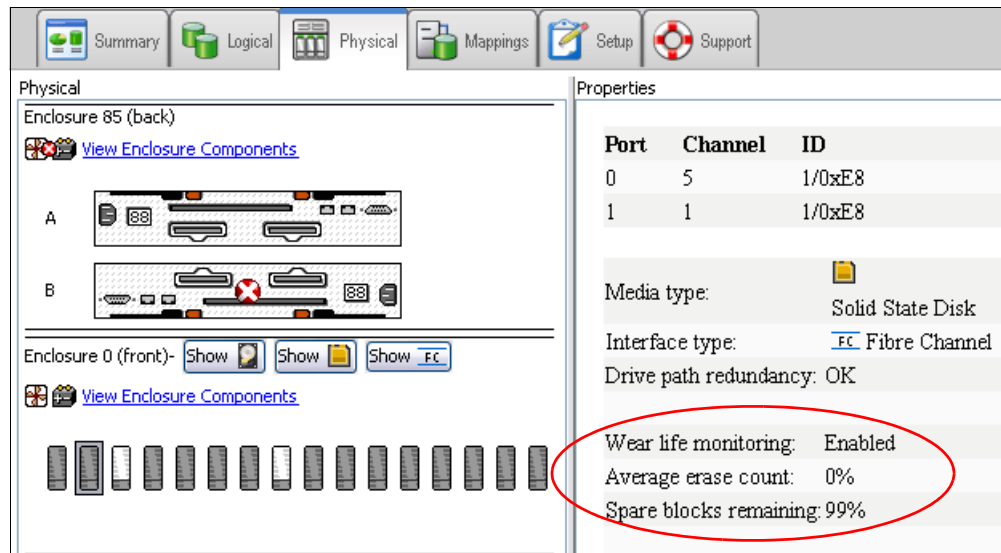


Figure B-3 SSD properties

SSD arrays

The same criteria for arrays apply to SSD as for other type disk drives. All of the disk drives in the SSD array must have the same media type (SSD) and the same interface type (FC only). Hot spare disk drives must also be SSD and be the same type as the disk drives they are protecting.

Wear life

The flash-based SSD has a limited wear life before individual memory locations can no longer reliably store data. The disk drive continuously monitors itself and reports its wear life status to the controller. Two mechanisms exist to alert you that an SSD is nearing the end of its useful life:

- ▶ Average erase count
- ▶ Spare blocks remaining

You can find these two pieces of information in the disk drive properties, which you can see in the storage management software by selecting a disk drive on the **Physical** tab. These are marked in Figure B-3.

The average erase count is reported as a percentage of the rated lifetime. When the average erase count reaches 80 percent, an informational event is logged to the Major Event Log (MEL). At this time, schedule the replacement of the SSD. When the average erase count reaches 90 percent, a critical event is logged, and a “Needs Attention” condition occurs on the DS5000. At this time, replace the SSD as soon as possible.

The spare blocks remaining are reported as a percentage of the total blocks. When the spare blocks remaining falls below 20 percent, an informational event is logged to the MEL. At this time, schedule the replacement of the SSD. When the spare blocks remaining falls below 10 percent, a critical event is logged, and a “Needs Attention” condition occurs. At this time, replace the SSD as soon as possible.

Write caching

Write caching will always be enabled for SSDs. Write caching improves performance and extends the life of the SSD

Background media scan

You cannot enable background media scans on SSDs. Background media scans are not needed for SSDs because of the high reliability of SSDs. Furthermore, background media scans will be detrimental because they increase wear on the SSDs.

SSD performance on DS5000 storage subsystems

In addition to capacity growth, there is an increasing need to process data quickly. In some cases, the high volume of users accessing a database can result in the need for a high IOPS rate. In other cases, there is a need to quickly process data, and to index the incoming streams to allow high-speed searches and retrieval of needed records. Within the database or file system middleware, there are directories, lock managers, and access control records that must be accessed and updated at rates that scale with the size of the data or the number of clients being served.

A need for high performance disks

There are some applications that simply cannot be run fast enough to satisfy business needs. These include trading algorithms, complex simulations in aerospace or pharmaceutical design, and security video analysis. Online transaction processing (OLTP) systems are the classic example of these applications. Many of these usages of data create a need to operate at high speed, often on indices or subsets of larger collections of information. In cases where the IOPS performance of the storage is the system bottleneck, there is a high value in faster storage and using SSDs.

Over the years, HDDs have maintained a dramatic rate of improvement in terms of dollar per gigabyte, which has enabled data center administrators to keep up with storage capacity demand without greatly increasing expenses. HDDs have also performed relatively well in achieving improvements to sustained bandwidths (GBps) with recent 15K RPM drives advertising greater than 170 MBps speeds. But the rate of improvement in IOPS has lagged far behind other system elements. While the dollar to gigabyte ratio has improved at a rate of 50 percent per year or more over the last decade, IOPS has only increased at a rate of 5 percent per year, and has slowed even further in recent years.

This parameter of performance is dominated by the mechanical elements of the drive: the drive's rotational speed and the seek time of the arm. Substantial improvements for each drive form factor (for example, 3.5") are no longer attainable. Although some minor improvement are possible by using smaller drives (for example, 2.5" at 15K RPM), this comes at a higher dollar to gigabyte cost. This lack of improvement in IOPS means that HDDs are actually getting worse in access density as defined by IO per GB per second (I/O / GBps).

Storage management, performance, and cost are big issues in the database world. Database workloads, both transactional and data warehousing, typically require lots of HDDs for I/O performance, both IOPS and bandwidth. Traditional enterprise HDDs, including the 15K RPM HDDs, are limited by the rate of head movement and deliver random I/O performance of approximately 150 -175 IOPS with a latency of about 5 -7 ms and sequential scan bandwidth of about 30 - 60 MBps for most database workloads. Write-intensive batch jobs are under pressure to complete within the increasingly shrinking time-window, leading to reduced uptime for transactional database systems.

SSDs offer game-changing performance for database applications by removing the limitations traditional rotating disks impose on database design. This revolutionizes database architectural design by removing the traditional I/O bottleneck. SSDs eliminate the need to have a large number of underutilized (short-stroked) HDDs to meet the heavy I/O demands of database applications.

Initial lab tests of SSDs on a DS5000 storage subsystem

Lab tests with a DS5000 storage subsystem were made in order to illustrate a comparison between SSDs on a DS5000 storage subsystem and the traditional SATA and Fibre Channel (FC) disks. The tools used to create the I/O have been created purely for a lab environment, and the results shown below do not indicate any expectation to what a commercial application or database can expect to achieve on a DS5000 storage subsystem. The lab environment ensures that the tests performed are identical and a realistic comparison between the different disk drive results can be made.

Random I/O performance

The SSD limitation of twenty disks per subsystem are compared to SATA limitation of 256 disks and the FC limitation of 256 disks that can be used in a single DS5000 storage subsystem. The first set results, shown in Figure B-4, compare random I/O reads and writes for all three types of disk. The arrays were set up in the following configurations:

- ▶ SSD: 4 x (4+1) volumes in a RAID 5 configuration
- ▶ FC: 32 x (7+1) volumes in a RAID 5 configuration
- ▶ SATA: 32 x (7+1) volumes in a RAID 5 configuration
- ▶ Read cache disabled
- ▶ Write cache disabled

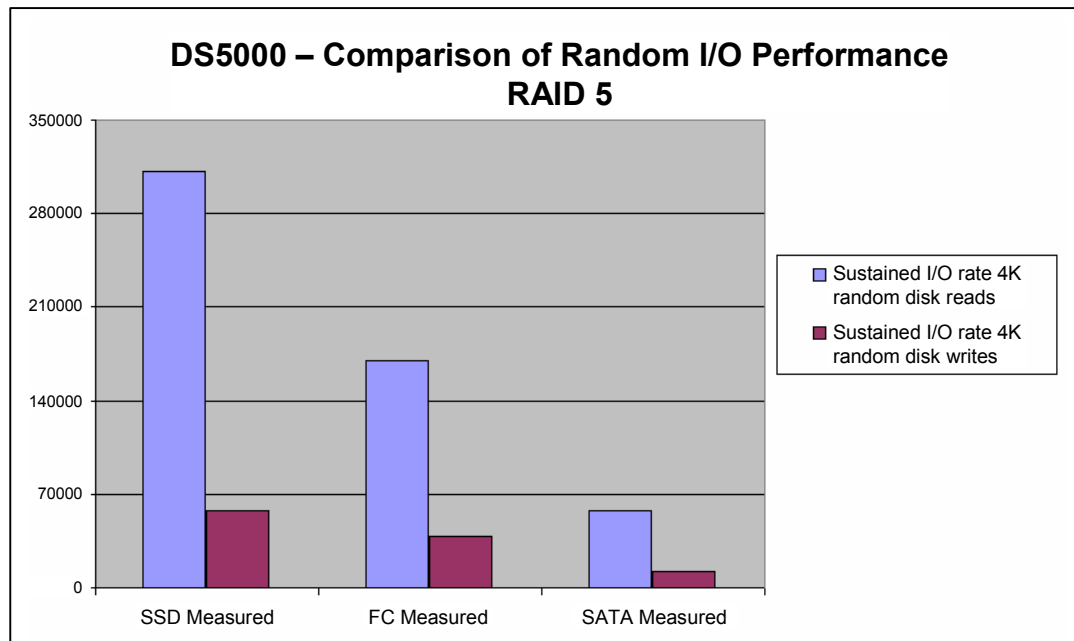


Figure B-4 Comparison of random I/O performance

Throughput performance

The second set of results show the throughput comparison. The arrays were set up in the following configurations:

- ▶ SSD: 4 x (4+1) volumes in a RAID 5 configuration
- ▶ FC: 16 x (8+1) volumes in a RAID 5 configuration
- ▶ SATA: 16 x (8+1) volumes in a RAID 5 configuration

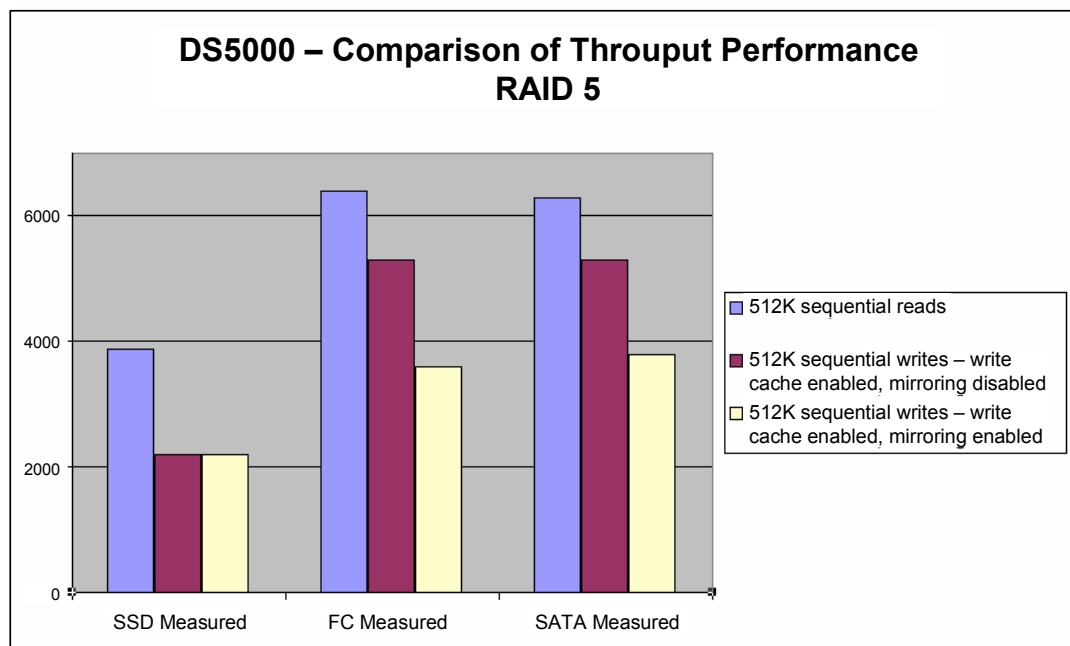


Figure B-5 Throughput performance comparison

SDD summary

From the comparisons given in Figure B-4 on page 545 and Figure B-5, SSD offers a greatly improved performance over HDDs, but SSD costs more. With such a performance, SDD usage can be increasingly justified for use in high performance tiered storage on a DS5000 storage subsystem. Also, SDD usage will be cost driven, and as the cost for SDD diminishes to only two to three times the price of high-performance HDDs, it will drive a significant substitution rate of low-capacity/high-performance HDDs.

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 System Storage DS5000 Series Implementation and Best Practices Guide*, SG24-8024
- ▶ *IBM System Storage DS Storage Manager Copy Services Guide*, SG24-7822
- ▶ *IBM Midrange System Storage Hardware Guide*, SG24-7676
- ▶ *IBM Midrange System Storage Implementation and Best Practices Guide*, SG24-6363
- ▶ *IBM System Storage b-type Multiprotocol Routing: An Introduction and Implementation*, SG24-7544
- ▶ *IBM System Storage Copy Services and IBM i: A Guide to Planning and Implementation*, SG24-7103
- ▶ *IBM System Storage DS3000: Introduction and Implementation Guide*, SG24-7065
- ▶ *IBM System Storage DS4000 and Storage Manager V10.30*, SG24-7010
- ▶ *Implementing an IBM b-type SAN with 8 Gbps Directors and Switches*, SG24-6116
- ▶ *Implementing an IBM/Cisco SAN*, SG24-7545
- ▶ *IBM System Storage DS3500 Introduction and Implementation Guide*, SG24-7914
- ▶ *VMware Implementation with IBM System Storage DS5000*, REDP-4609
- ▶ *IBM System Storage EXP5060 Storage Expansion Enclosure Planning Guide*, REDP-4679

You can search for, view, download or order these documents and other Redbooks, Redpapers, Web Docs, draft and additional materials, at the following website:

ibm.com/redbooks

Other publications

These publications are also relevant as further information sources:

- ▶ *IBM System Storage DS3000, DS4000, and DS5000 Command Line Interface and Script Commands Programming Guide*, GC52-1275
- ▶ *IBM System Storage DS4000 Concepts Guide*, GC26-7734
- ▶ *IBM System Storage DS4000/DS5000 EXP810 Storage Expansion Enclosure Installation, User's and Maintenance Guide*, GC26-7798

- ▶ *IBM System Storage DS4000/DS5000 Fibre Channel and Serial ATA Intermix Premium Feature Installation Overview*, GC53-1137
- ▶ *IBM System Storage DS4000/DS5000 Hard Drive and Storage Expansion Enclosure Installation and Migration Guide*, GC53-1139
- ▶ *IBM System Storage DS4800 Storage Subsystem Installation, User's, and Maintenance Guide*, GC26-7845
- ▶ *IBM System Storage DS4800 Storage Subsystem Quick Start Guide*, GC27-2148
- ▶ *IBM System Storage DS5000 EXP5000 Storage Expansion Enclosure Installation, User's, and Maintenance Guide*, GC53-1141
- ▶ *IBM System Storage DS5100, DS5300, and EXP5000 Quick Start Guide*, GC53-1134
- ▶ *IBM System Storage DS5100 and DS5300 Storage Subsystems Installation, User's, and Maintenance Guide*, GC53-1140
- ▶ *IBM System Storage DS Storage Manager Version 10 Installation and Host Support Guide*, GC53-1135
- ▶ *IBM System Storage DS Storage Manager Version 10.50 Copy Services User's Guide*, GC53-1136
- ▶ *IBM System Storage DS Storage Manager Version 10.60 Copy Services User's Guide*, GC53-1136

Online resources

These websites are also relevant as further information sources:

- ▶ System Storage Interoperation Center (SSIC):
http://www-03.ibm.com/systems/support/storage/config/ssic/displayessearchwithoutjs.wss?start_over=yes
- ▶ Support for IBM Disk systems: <http://www.ibm.com/systems/support/storage/disk>

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

To determine the spine width of a book, you divide the paper PPI into the number of pages in the book. An example is a 250 page book using Plainfield opaque 50# smooth which has a PPI of 526. Divided 250 by 526 which equals a spine width of .4752". In this case, you would use the .5" spine. Now select the Spine width for the book and hide the others: **Special>Conditional Text>Show/Hide>SpineSize(->Hide:)->Set** . Move the changed Conditional text settings to all files in your book by opening the book file with the spine:fm still open and **File>Import>Formats** the Conditional Text Settings (ONLY!) to the book files.

Draft Document for Review October 3, 2012 6:47 am

8023spine.fm 549



IBM System Storage DS5000 Series Hardware Guide

(1.5" spine)
1.5"<-> 1.998"
789 <-> 1051 pages



IBM System Storage DS5000 Series Hardware Guide

(1.0" spine)
0.875"<-> 1.498"
460 <-> 788 pages



IBM System Storage DS5000 Series Hardware Guide

(0.5" spine)
0.475"<-> 0.873"
250 <-> 459 pages



IBM System Storage DS5000 Series Hardware Guide

(0.2" spine)
0.17"<-> 0.473"
90<->249 pages

(0.1" spine)
0.1"<-> 0.169"
53<->89 pages

To determine the spine width of a book, you divide the paper PPI into the number of pages in the book. An example is a 250 page book using Plainfield opaque 50# smooth which has a PPI of 526. Divided 250 by 526 which equals a spine width of .4752". In this case, you would use the .5" spine. Now select the Spine width for the book and hide the others: **Special>Conditional Text>Show/Hide>SpineSize(->Hide:>Set** . Move the changed Conditional text settings to all files in your book by opening the book file with the spine:fm still open and **File>Import>Formats** the Conditional Text Settings (ONLY!) to the book files.

Draft Document for Review October 3, 2012 6:47 am

8023spine.fm 550



IBM System Storage DS5000 Series Hardware Guide

(2.5" spine)
2.5" <-> nnn.n"
1315<-> nnnn pages



IBM System Storage DS5000 Series Hardware Guide

(2.0" spine)
2.0" <-> 2.498"
1052 <-> 1314 pages



IBM System Storage DS5000 Series Hardware Guide



Introduction to IBM System Storage DS5000 series

Remote Support Manager (RSM) Configuration

Configuration, Maintenance, and Troubleshooting

This IBM® Redbooks® publication consolidates, in one document, detailed descriptions of the hardware configurations and options offered as part of the IBM System Storage DS5000 families of products.

This edition covers updates and additional functions available with the IBM System Storage DS Storage Manager Version 10.77 (firmware level 7.77). This book presents the concepts and functions used in planning and managing the storage servers, such as multipathing and path failover. The book offers a step-by-step guide to using the Storage Manager to create arrays, logical drives, and other basic (as well as advanced) management tasks.

This publication also contains practical information about diagnostics and troubleshooting, and includes practical examples of how to use scripts and the command-line interface.

This publication is intended for customers, IBM Business Partners, and IBM technical professionals who want to learn more about the capabilities and advanced functions of the DS5000 series of storage servers with Storage Manager Software V10.77. It also targets those who have a DS5000 storage subsystem and need detailed advice about how to configure it.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks