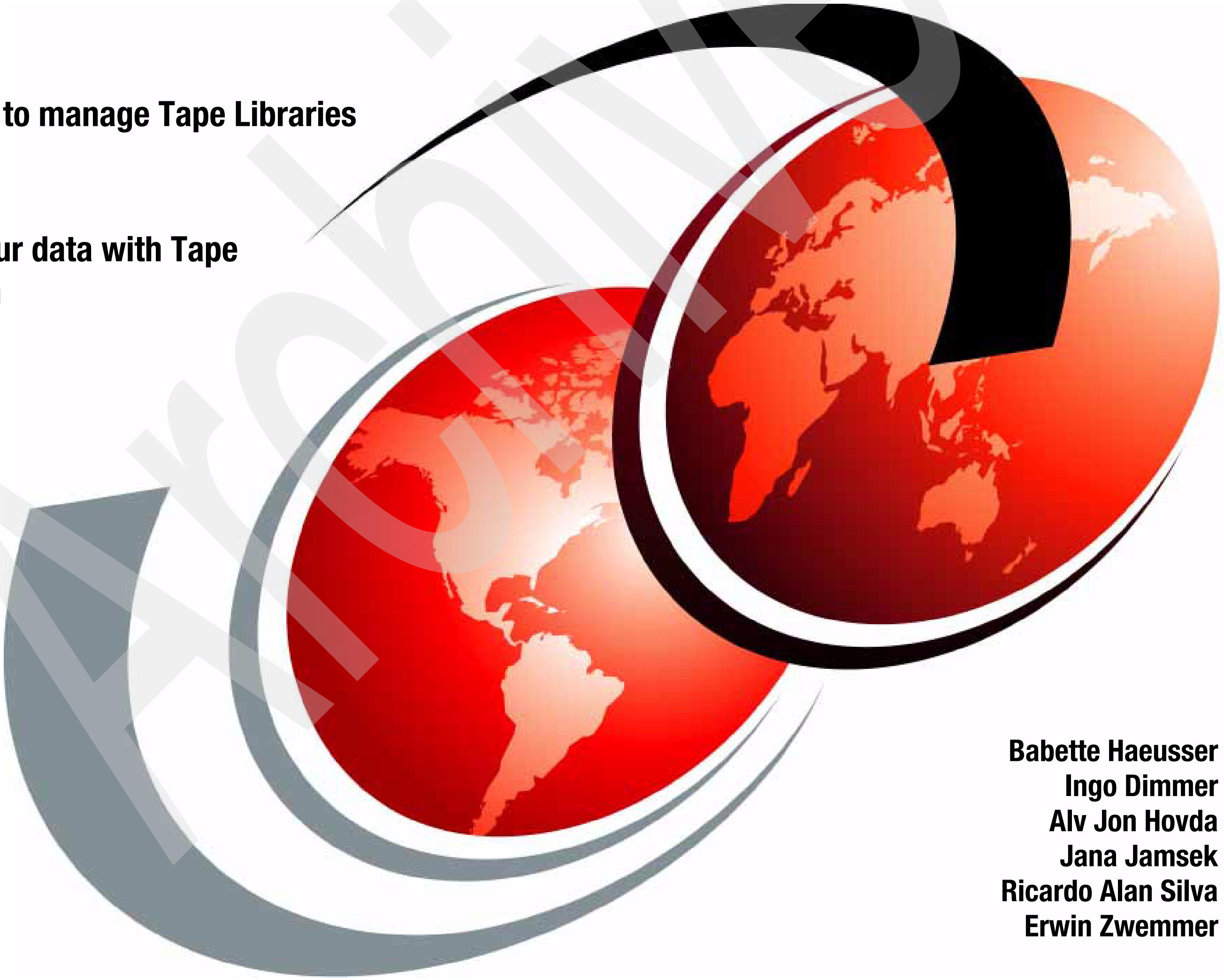
Implementing IBM Tape in i5/OS

Learn about IBM Tape Solutions

Use BRMS to manage Tape Libraries

Protect your data with Tape Encryption



Babette Haeusser
Ingo Dimmer
Alv Jon Hovda
Jana Jamsek
Ricardo Alan Silva
Erwin Zwemmer

Redbooks

ibm.com/redbooks

International Technical Support Organization

Implementing IBM Tape in i5/OS

February 2008

SG24-7440-00

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

First Edition (February 2008)

This edition applies to all IBM Tape Drive and Tape Library products current at the time of writing.

Contents

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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

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

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

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

AIX 5L™
AIX®
AS/400®
DB2®
DB2 Universal Database™
DFSMS™
Domino®
ESCON®
eServer™
FICON®
Hypervisor™
IBM®
iSeries®
i5/OS®
Lotus®
MVS™
NetView®
OS/400®
PowerPC®
POWER™
POWER Hypervisor™
POWER5™
POWER5+™
POWER6™
Redbooks®
Redbooks (logo) ®
System i™
System i5™
System p™
System Storage™
System x™
System/38™
Tivoli®
Tivoli Enterprise Console®
TotalStorage®
Virtualization Engine™
WebSphere®
xSeries®
z/OS®
zSeries®

The following terms are trademarks of other companies:

InfiniBand, and the InfiniBand design marks are trademarks and/or service marks of the InfiniBand Trade Association.

Java, JDBC, JDK, JVM, J2SE, Powderhorn, Solaris, StorageTek, Sun, Ultra, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

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

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

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

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

Preface

This IBM® Redbooks® publication follows *The IBM System Storage Tape Libraries Guide for Open Systems*, SG24-5946, and can help you plan, install, and configure IBM Ultrium LTO tape drives, as well as the TS1120 Tape Drive and libraries in i5/OS® environments. The book focuses on the setup and customization of these drives and libraries.

The first part of the book gives an overview of the System i™ family of servers and describes how to attach and configure the drives and libraries. It also covers basic installation and administration. We describe the sharing and partitioning of libraries and explain the concept and usage of the Advanced Library Management System (ALMS).

In the second part of the book, we document how to use these products with Backup Recovery and Media Services (BRMS), how to implement Tape Encryption, and how to use the IBM TS7520 Virtualization Engine™ with i5/OS.

This book can help IBM personnel, Business Partners, and customers to better understand and implement the IBM Ultrium LTO product line, and also the TS1120 Tape Drive attached to System i servers. We assume that the reader is familiar with tape drives and libraries and has a basic understanding of System i servers and i5/OS.

The team that wrote this IBM Redbooks publication

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

Babette Haeusser is an IBM Certified IT Specialist at the International Technical Support Organization, San Jose Center. She writes extensively and teaches IBM classes worldwide on all areas of Enterprise and Open Systems Tape Drives (including Tape Encryption), Tape Libraries, and Tape Virtualization. Babette joined IBM in 1973 as an application programmer. In 1987, she became an MVS™ Systems Engineer and specialized in IBM Storage Hardware and Software, which she has supported in various job roles since then. Before joining the ITSO in early 2005, Babette worked in the Advanced Technical Sales Support EMEA. She led a team of specialists for Enterprise Storage, while she focused on Enterprise Tape including tape libraries and Virtual Tape Servers.

Ingo Dimmer is an IBM Advisory IT Specialist for System i and a PMI Project Management Professional working in the IBM STG Europe storage support organization in Mainz, Germany. He has eight years of experience in enterprise storage support from working in IBM post-sales and pre-sales support. He holds a degree in Electrical Engineering from the Gerhard-Mercator University Duisburg. His areas of expertise include System i external disk storage solutions, I/O performance, and tape encryption, for which he has been an author of several White Papers and IBM Redbooks publications.

Alv Jon Hovda is a Senior IT Specialist for IBM ITS Norway. He has 12 years of experience in the Tivoli® Storage Manager field, working with a number of different tape libraries. He holds a Masters degree in Engineering Physics. He is Tivoli Storage Manager certified, and his areas of expertise include Tivoli Storage Manager and AIX®. He has been the author of several IBM Redbooks on Tivoli Storage Manager and IBM Open Systems tape.

Jana Jamsek is an IT Specialist in IBM Slovenia. She works in Storage Advanced Technical Support for EMEA as a specialist for Storage and IBM eServer™ System i™. Jana has eight years of experience in the System i, iSeries®, and IBM AS/400® areas, and five years of experience in Storage. She holds a Master's degree in Computer Science and a degree in mathematics from the University of Ljubljana, Slovenia. She has co-authored several IBM Redbooks and IBM Redpapers.

Ricardo Alan Silva is an IT Specialist for IBM GTS Brazil, working in the Tivoli Storage Manager team supporting Tivoli Storage Manager and all its complementary products. He has been working at IBM for five years. His areas of expertise include System Storage™ Disk and Tape solutions, Tivoli Storage products implementation and TPC. He is an IBM Certified Deployment Professional: Tivoli Storage Manager V5.3 and IBM Certified Storage Administrator: Tivoli Storage Manager V5.

Erwin Zwemmer is a Certified High End Tape Solution Specialist working at the Tape Support Centre in Mainz, Germany, since 2001. In his current job, Erwin provides EMEA support to colleagues for the complete spectrum of IBM TotalStorage® and System Storage tape and optical products. Prior to his position with IBM Germany, he worked as an AS/400 Technical Support Member. He joined IBM Holland in 1995 as an IBM Customer Engineer for AS/400 systems and multivendor products.

The Team: Ingo, Jana, Erwin, Babette, Ricardo Alan, and Alv Jon

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

Leslie Parham, Emma Jacobs, Sangam Racherla, Yvonne Lyon
International Technical Support Organization, San Jose Center

Jim Cook, Nick Harris
International Technical Support Organization, Rochester Center

Scott Maxson, Sanjay Patel, Mervyn Venter, Barbara Smith, Glen Nelson
IBM Systems and Development Group

Jennifer Bappert, John Morganti, Paul Greco, Tommy de Jesus, Timothy Cook,
Alan Ishikawa, Linda Muller
IBM Development and Marketing, Tucson

Jim Fisher, Nancy Roper, Jeff Ziehm
IBM Advanced Technical Support AG

Thomas Barlen, Edelgard Schittko
IBM Germany

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbooks publication dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You will have the opportunity to team with IBM technical professionals, Business Partners, and Clients.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

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 Redbooks to be as helpful as possible. Send us your comments about this book or other Redbooks in one of the following ways:

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

  ibm.com/redbooks

- Send your comments in an e-mail 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

Part 1

Setting up IBM tape in i5/OS

In this part of the book, we introduce the IBM System Storage tape products (LTO Ultrium products and 3592 Enterprise Tape Drive) and describe how to set them up in i5/OS environments. Both native SCSI and SAN (Fibre Channel) attachments are presented. We also show how to use the administration tools, such as the IBM Library Specialist.

We cover the following topics:

- Introduction to IBM Open Systems Tape
- Tape Library sharing and partitioning
- Overview of the IBM System i platform
- Planning considerations
- Setup for IBM tape

1

Introduction to IBM Open Systems Tape

This chapter provides an overview of the Linear Tape-Open (LTO) initiative and the corresponding IBM System Storage LTO Ultrium product line.

This includes:

- An overview of the IBM System Storage Tape LTO models available:
  - IBM TS2230 Tape Drive
  - IBM TS2340 Tape Drive
  - IBM TS3100 Tape Library
  - IBM TS3200 Tape Library
  - IBM TS3310 Tape Library
  - IBM TS3500 Tape Library
- An overview of the other IBM System Storage Enterprise Tape models:
  - IBM TS1120 Tape Drive
  - IBM TS3400 Tape Library

1.1 LTO overview

The Linear Tape-Open (LTO) program is a joint initiative of Hewlett-Packard, IBM, and Seagate Technology. In 1997, the three companies set out to enable the development of best-of-breed tape storage products by consolidating state-of-the-art technologies from numerous sources. The three companies also took steps to protect client investment by providing a four-generation road map and establishing an infrastructure to enable compatibility between competitive products. This road map has been extended to six generations later.

The LTO technology objective was to establish new open-format specifications for high capacity, high performance tape storage products for use in the midrange and network server computing environments, and to enable superior tape product options.

LTO program cooperation goes beyond the initial three companies. LTO format specifications have been made available to all who want to participate through standard licensing provisions. LTO program technology has already attracted a number of other industry leaders, so that LTO-specified products (tape drives and tape storage cartridges) can reach the market from multiple manufacturers, not just the Technology Provider Companies. This is critical to meeting an open market objective, and is accomplished through open licensing of the technology.

Cooperation is also evident in the LTO program requirement that all products produced by licensees be technically certified annually. The primary objective of this certification is to help determine whether LTO format cartridges can be exchangeable across drives produced by different LTO Ultrium manufacturers. In other words, LTO compliant media from any vendor can be read and written in LTO compliant drives from any vendor.

All three consortium members (IBM, HP, and Certance LLC[1]) are now shipping LTO Ultrium products, and numerous other licensees are shipping hardware and media.

The Linear Tape-Open organization home page is:

http://www.lto.org

For more information about LTO technology, see the *IBM System Storage Tape Libraries Guide for Open Systems,* SG24-5946.

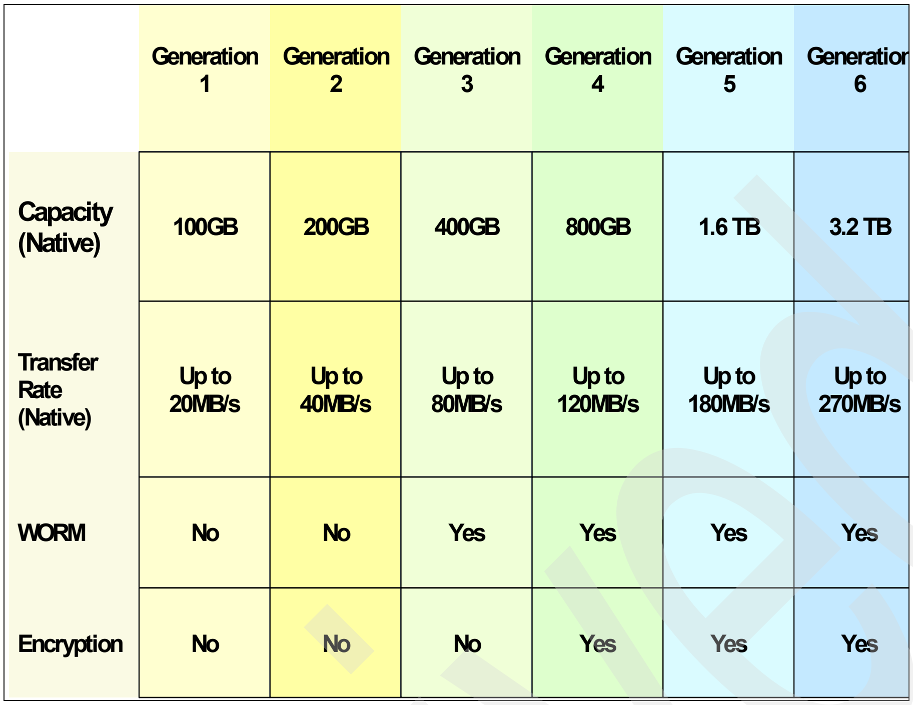
The IBM LTO home page is:

http://www.ibm.com/storage/lto

The LTO Ultrium road map (Figure 1-1) shows the evolution of LTO technology. At the time of writing, IBM Ultrium generation 3 and 4 products are offered. The information in the road map is given as an indication of future developments by the three consortium members, and is subject to change.

Important: Hewlett-Packard, IBM, and Certance reserve the right to change the information in this migration path without notice.

[1] Seagate RRS became Certance and is now owned by Quantum.



	Generation 1	Generation 2	Generation 3	Generation 4	Generation 5	Generation 6
Capacity (Native)	100GB	200GB	400GB	800GB	1.6 TB	3.2 TB
Transfer Rate (Native)	Up to 20MB/s	Up to 40MB/s	Up to 80MB/s	Up to 120MB/s	Up to 180MB/s	Up to 270MB/s
WORM	No	No	Yes	Yes	Yes	Yes
Encryption	No	No	No	Yes	Yes	Yes

Figure 1-1 LTO Ultrium road map

1.1.1 LTO Ultrium models

For the remainder of this book, we use the term LTO as a generic term for different generations of the LTO Ultrium tape drives.

As the specific reference to the IBM System Storage TS1040 LTO Ultrium 4 Tape Drive, we use the term LTO4.

The IBM System Storage LTO family consists of:

- IBM TS2230 Tape Drive
- IBM TS2340 Tape Drive
- IBM TS3100 Tape Library
- IBM TS3200 Tape Library
- IBM TS3310 Tape Library
- IBM TS3500 Tape Library

These are shown in Figure 1-2.

Figure 1-2 The LTO product family

We describe these models in more detail starting in 1.1.2, “IBM System Storage TS2230 Tape Drive” on page 8.

Some existing models have two drive options: IBM LTO3 and LTO4.

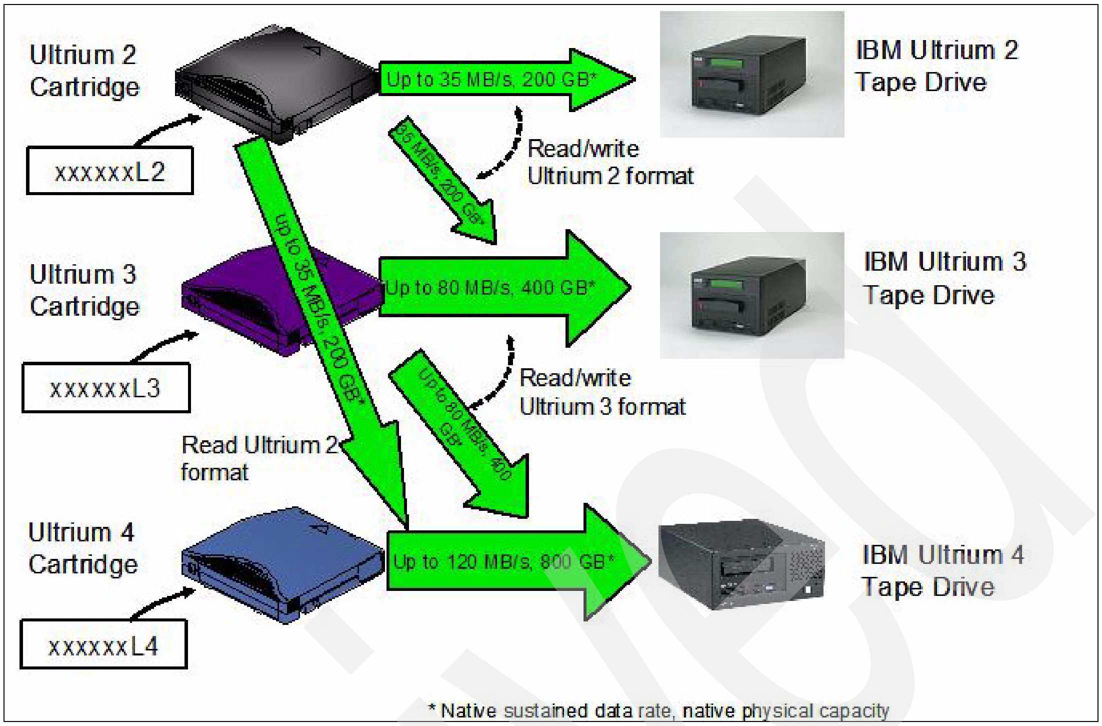
LTO1 was the first generation of the LTO technology with a tape capacity of 100 GB per cartridge in a native format, and capacity of 200 GB using 2:1 compression.

LTO2 is the second generation of the LTO technology with a tape capacity of 200 GB per cartridge in native format, and capacity of 400 GB using 2:1 compression.

LTO3 is the third generation of the LTO technology with a tape capacity of 400 GB per cartridge in native format, and capacity of 800 GB using 2:1 compression. A WORM (write-once, read-many) version of the LTO3 cartridge is also available.

LTO4 is the fourth generation of the LTO technology with a tape capacity of 800 GB per cartridge in native format, and capacity of 1600 GB using 2:1 compression. A WORM (write-once, read-many) version of the LTO4 cartridge is also available.Media compatibility.

Figure 1-3 depicts the media compatibility characteristics for the last three generations of LTO tape.



* Native sustained data rate, native physical capacity

Figure 1-3 LTO generation media compatibility

LTO2

The LTO2 Tape Drive is compatible with the cartridges of its predecessor, the LTO1 Tape Drive. Cartridge compatibility for the LTO2 Tape Drive is as follows:

- Reads and writes LTO2 format on LTO2 cartridges
- Reads and writes LTO1 format on LTO1 cartridges
- Does not write LTO2 format on LTO1 cartridges
- Does not write LTO1 format on LTO2 cartridges

LTO3

The LTO3 Tape Drive is compatible with the cartridges of its predecessors, the LTO2 and LTO1 Tape Drive. Cartridge compatibility for the LTO3 Tape Drive is as follows:

- Reads and writes LTO3 format on LTO3 cartridges
- Reads and writes LTO2 format on LTO2 cartridges
- Reads LTO1 format on LTO1 cartridges
- Does not write LTO3 format on LTO2 cartridges
- Does not write LTO2 format on LTO3 cartridges

LTO4

The LTO4 Tape Drive is compatible with the cartridges of its immediate predecessors, the LTO3 and LTO2 Tape Drives. Cartridge compatibility for the LTO4 Tape Drive is as follows:

- Reads and writes LTO4 format on LTO4 cartridges
- Reads and writes LTO3 format on LTO3 cartridges
- Reads LTO2 format on LTO2 cartridges
- Does not write LTO4 format on LTO3 cartridges
- Does not write LTO3 format on LTO4 cartridges
- Does not write or read on LTO1 cartridges

WORM tape format

Beginning with LTO3, Write Once Read Many (WORM) functionality provides for non-erasable, non-rewritable operation with tape media and is designed for long term tamper resistant record retention.

The IBM LTO3 specification for WORM includes the use of low level encoding in the Cartridge Memory (CM), which is also mastered into the servo pattern as part of the manufacturing process. This encoding is designed to prevent tampering.

Data can be appended at the end of a WORM cartridge to which data was previously written, allowing the full use of the high capacity tape media.

LTO3 WORM cartridges can be used with any LTO3 tape drive with the appropriate microcode and firmware. LTO3 non-WORM and WORM cartridges can coexist in the same library.

The same description holds for the LTO4 WORM cartridges. They can be used by any LTO4 tape drive, and can coexist with non-WORM cartridges. Additionally, the LTO4 drive can read and write WORM and non-WORM LTO3 cartridges.

1.1.2 IBM System Storage TS2230 Tape Drive

The IBM System Storage TS2230 Tape Drive (3580 Model H3L or H3S) is an external stand-alone or rack mountable unit and is the entry point to the family of IBM Linear Tape-Open (LTO) Tape products. The IBM System Storage TS2230 Tape Drive is designed for backup and restore of midrange Open Systems applications. The IBM System Storage TS2230 Tape Drive incorporates the IBM System Storage LTO3 half-high T880V Tape Drive, which has a native physical capacity of 400GB, or 800GB with 2:1 compression.

The TS2230 is the first member of the IBM LTO Tape Family that uses the new half-high LTO3 Tape Drive. It has the same characteristics of the full-high tape drive except the native transfer rate, which is 60 MB/s compared to 80 MB/s for the full-high LTO3 drive. In addition to the standard LTO3 data cartridges, Write Once Read Many (WORM) cartridges are supported and recognized when loaded.

The IBM System Storage TS2230 Tape Drive Model H3L is available with a Low Voltage Differential (LVD) Small Computer System Interface (SCSI). The LVD SCSI interface has a native maximum data transfer rate of up to 60 MB/s. The IBM System Storage TS2230 Model H3S comes with a 3 Gbps Serial-Attached SCSI (SAS) interface.

The TS2230 can be attached to IBM System p™, IBM System i, IBM System p, IBM System x™, Microsoft® Windows®, HP-UX, Sun™ Solaris™, UNIX®, Linux®, and PC servers. To determine the latest update of supported servers, visit the Web at:

http://www-03.ibm.com/servers/storage/tape/compatibility

Figure 1-4 shows the front view of the TS2230.

Figure 1-4 Front view of IBM TS2230 Tape Drive

For more information about the IBM TS2230 Tape Drive, see the *IBM System Storage Tape Libraries Guide for Open Systems,* SG24-5946.

1.1.3 IBM System Storage TS2340 Tape Drive

The TS2340 Tape Drive is an external stand-alone or rackmountable unit and is the entry point for the family of IBM LTO tape products. The TS2340 Tape Drive provides an excellent migration path from digital linear tape (DLT or SDLT), 1/4-inch, 4mm, or 8mm tape drives.

IBM TS2340 is an LTO tape drive designed to increase maximum tape drive throughput native data rate performance up to 120 MB/s In addition, with the use of the LTO4 data cartridge, the LTO4 Tape Drive doubles the tape cartridge capacity up to 800 GB native physical capacity (1600 GB with 2:1 compression). IBM LTO4 Tape Drives can read and write LTO3 data cartridges and can read LTO2 data cartridges. In addition, the LTO4 SAS Tape Drive is encryption-capable and designed to support Application-Managed Encryption.

The TS2340 Tape Drive Model L43 uses a SCSI Ultra160 LVD attachment, and the Model S43 uses a 3 Gbps Serial-Attached SCSI (SAS) interface for connections to a wide spectrum of Open Systems servers. The new models attach to IBM System p, IBM System i, IBM System p, IBM System x, MicroSoft Windows, HP-UX, Sun Solaris, UNIX, and PC servers.

Figure 1-5 shows the IBM TS2340 Tape Drive.

Figure 1-5 IBM TS2340 Tape Drive

For more information about the IBM TS2340 Tape Drive, see the *IBM System Storage Tape Libraries Guide for Open Systems,* SG24-5946.

1.1.4 IBM System Storage TS3100 Tape Library

The TS3100 Tape Library (Machine Type 3573, Model L2U), is a single drive or a dual drive entry level desktop or a rack mounted unit (requiring two rack units of a industry standard 19 inch rack). A total of 22 cartridges can be stored in two removable magazines. A single dedicated mail slot (I/O Station) is available for importing and exporting cartridges. The TS3100 Tape Library is available with a choice of two tape drive interfaces, either SCSI LVD or 4 Gbps Native Fibre Channel.

IBM TS3100 supports either one IBM LTO3 full-high tape drive with a native capacity of 400 GB, two IBM LTO3 half-high tape drives with a native capacity of 400 GB, or one IBM LTO4 tape drive with a native capacity of 800 GB. With IBM LTO4 tape drive, the IBM TS3100 also has 3 GB SAS (Serial Attached SCSI) attachment interface. Standard features are a barcode reader and a remote management unit (RMU).

The IBM TS3100 also supports Application-Managed Encryption (AME) on SAS and Fibre Channel LTO4 drives using LTO4 media.

The TS3100 Tape Library can be attached to IBM System p, IBM System i, IBM System x, Microsoft Windows, HP-UX, Sun Solaris, UNIX, Linux, and PC servers.

It provides the ability to configure the number of logical libraries up to the number of tape drives. This provides a maximum capability of two logical libraries for the TS3100 with two half-high drives.

Available as a standard feature, a *Remote Management Unit* (RMU) provides an Ethernet port, so that the library can be configured as a TCP/IP device in the network. Library status can be sent to the network as Simple Network Management Protocol (SNMP) traps. The IBM System Storage Tape Library Specialist enables network access (via Web browser) to the library for more detailed status and for updating the firmware of the library. All library Operator panel functions can be accessed using the IBM System Storage Tape Library Specialist.

Figure 1-6 shows the IBM TS3100 Tape Library.

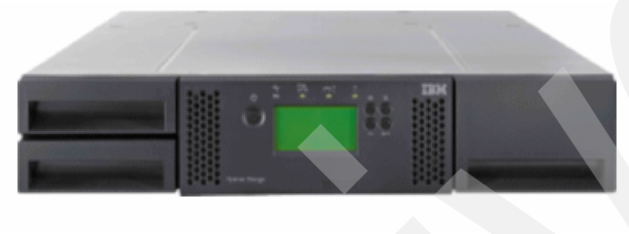


Figure 1-6 IBM TS3100 Tape Library

For more information about the IBM TS3100 Tape Library, see the *IBM System Storage Tape Libraries Guide for Open Systems,* SG24-5946.

1.1.5 IBM System Storage TS3200 Tape Library

The TS3200 Tape Library (Machine Type 3573, Model L4U), is a midrange level desktop or a rack mounted unit (requiring four rack units of an industry standard 19 inch rack). A total of 44 cartridges can be stored in four removable magazines. A single dedicated mail slot (I/O Station) is available for importing and exporting cartridges. The TS3200 Tape Library is available with a choice of two tape drive interfaces, either SCSI LVD or 4 Gbps Native Fibre Channel.

IBM TS3200 supports either two IBM LTO3 full-high tape drives with a native capacity of 400 GB, four IBM LTO3 half-high tape drives with a native capacity of 400 GB, two IBM LTO4 tape drives with a native capacity of 800 GB or a mix of IBM LTO3 and LTO4 full-high tape drives. With IBM LTO4 tape drive, the IBM TS3200 also has 3 GB Serial-Attached SCSI (SAS) attachment interface. Standard features are a barcode reader and a remote management unit (RMU).

The IBM TS3200 also supports Application-Managed Encryption (AME) on SAS and Fibre Channel LTO4 drives using LTO4 media. Designed for high system availability, the optional control path feature can assure continued host connectivity even if one path goes down.

The TS3200 Tape Library can be attached to IBM System p, IBM System i, IBM System x, Microsoft Windows, HP-UX, Sun Solaris, UNIX, Linux, and PC servers.

It provides the ability to configure the number of logical libraries up to the number of tape drives. This provides a maximum capability of four logical libraries for the TS3200 with four half-high drives.

Available as a standard feature, a *Remote Management Unit* (RMU) provides an Ethernet port, so that the library can be configured as a TCP/IP device in the network. Library status can be sent to the network as Simple Network Management Protocol (SNMP) traps. The IBM System Storage Tape Library Specialist enables network access (via Web browser) to the library for more detailed status and for updating the firmware of the library. All library Operator panel functions can be accessed using the IBM System Storage Tape Library Specialist.

Figure 1-7 shows the IBM TS3200 Tape Library.

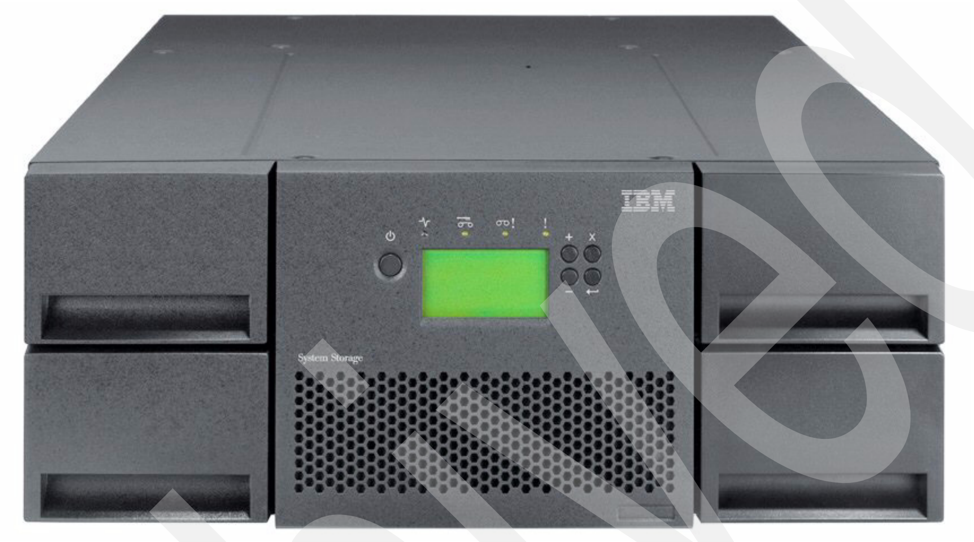


Figure 1-7 IBM TS3200 Tape Library

For more information about the IBM TS3200 Tape Library, see the *IBM System Storage Tape Libraries Guide for Open Systems,* SG24-5946.

1.1.6 IBM System Storage TS3310 Tape Library

The TS3310 Tape Library is a highly expandable IBM LTO library which allows you to start small with a 5U base unit available in desktop or rack mounted configurations. Over time, as your requirements for tape backup expands, you can add additional 9U expansion modules, each of which contains space for additional cartridges, tape drives and a redundant power supply. The entire system grows vertically. Available configurations include the 5U base library module alone or with up to four 9U modules.

The TS3310 Tape Library offers a broad range of configuration possibilities. The smallest configuration includes a base unit with one or two tape drives, either IBM LTO3, LTO4 or a mix, 30 storage slots and 6 I/O slots. This is upgradeable to a fully configured rack mounted library 41U high with up to 18 IBM LTO3 or LTO4 tape drives, tape storage (402 slots), and up to 54 I/O slots.

The IBM TS3310 also supports Application Managed Encryption (AME), System Managed Encryption (SME) and Library Managed Encryption (LME) on SAS and Fibre Channel LTO4 drives using LTO4 media. Designed for high system availability, the optional control path feature can assure continued host connectivity even if one path goes down.

The TS3310 Tape Library can be attached to IBM System p, IBM System i, IBM System x, Microsoft Windows, HP-UX, Sun Solaris, UNIX, Linux, and PC servers.

It provides the ability to configure the number of logical libraries up to the number of tape drives. This provides a maximum capability of 18 logical libraries for the IBM TS3310.

Available as a standard feature, a *Remote Management Unit* (RMU) provides an Ethernet port, so that the library can be configured as a TCP/IP device in the network. Library status can be sent to the network as Simple Network Management Protocol (SNMP) traps. The IBM System Storage Tape Library Specialist enables network access (via Web browser) to the library for more detailed status and for updating the firmware of the library. All library Operator panel functions can be accessed using the IBM System Storage Tape Library Specialist.

Figure 1-8 shows the IBM TS3310 Tape Library 5U base unit.

Figure 1-8 IBM TS3310 Tape Library 5U base unit

For more information about the IBM TS3310 Tape Library, see the *IBM System Storage Tape Libraries Guide for Open Systems,* SG24-5946.

1.1.7 IBM System Storage TS3500 Tape Library

The IBM System Storage TS3500 Tape Library (Figure 1-9) leverages the LTO and Enterprise 3592 drive technologies within the same library. The TS3500 was previously known as the IBM TotalStorage 3584 Tape Library and still has the machine type 3584.

The IBM System Storage TS3500 Tape Library provides tape storage solutions for the large, unattended storage requirements from today's mid-range up to enterprise (z/OS® and Open Systems) environment. This chapter only covers information relating to the TS3500 Tape Library library attachment in an Open Systems environment. For information about TS3500 Tape Library attachment to a z/Series environment, refer to *IBM TotalStorage 3584 Tape Library for zSeries Hosts: Planning and Implementation*, SG24-6789.

Combining reliable, automated tape handling and storage with reliable, high-performance IBM LTO tape and TS1120 drives, the TS3500 Tape Library offers outstanding retrieval performance with typical cartridge move times of less than three seconds.

The TS3500 Tape Library can be partitioned into multiple logical libraries. This makes it an excellent choice for consolidating tape workloads from multiple heterogeneous open-system servers and enables the support for z/Series attachment in the same library.

In addition, the TS3500 Tape Library provides outstanding reliability and redundancy, through the provision of redundant power supplies in each frame, an optional second cartridge accessor, control and data path failover, and dual grippers within each cartridge accessor. Both library and drive firmware can now be upgraded non-disruptively, that is without interrupting the normal operations of the library.

The TS3500 supports Tape Encryption on the following tape drives: IBM System StorageTS1040 Tape Drive, and the IBM System StorageTS1120 Tape Drive. The three different Encryption methods are supported by the TS3500: Application-Managed Encryption (AME), System-Managed Encryption (SME), and Library-Managed Encryption (LME).

Figure 1-9 IBM System Storage TS3500 Tape Library

1.1.8 TS3500 frames L53 and D53 for IBM LTO Fibre Channel drives

The TS3500 Tape Library Models L53 and D53 integrate the TS1030 and TS1040 LTO 4 Gbps Fibre Channel Tape Drive. The Model L53 frame includes an enhanced Frame Controller Assembly (FCA) with two power supplies (for redundancy), an optimized dual-gripper cartridge accessor, on-demand storage slot capacity, and 16-slot I/O stations. The Model D23 frame can be attached to current or installed frame models.

TS3500 Tape Library Model L53

The L53 can be installed on its own as a complete library enclosure, or it can have up to 15 expansion frames attached to it. This frame provides the major library components for the whole library, whether it has single or multiple frames. It also provides cartridge storage capacity for LTO media and it can be equipped with IBM LTO 1, 2, 3, and 4 tape drives. The expansion frames must be added to the right of the L53 frame.

The number of LTO cartridge storage slots ranges from 64 to 287. With the minimum configuration, there are just 64 slots available for use, but the maximum of 287 slots are already physically installed. Additional slots can be added for use by simply enabling through a license key.

The Intermediate Capacity feature (FC1643) gives a total amount of usable cartridge slots of 129. This feature is required to add a Full Capacity feature (FC1644), which gives the capacity of 287 cartridge slots. The full capacity feature is in turn required to add an Additional I/O Slots feature (FC1658 for LTO or FC1659 for 3592) or to attach an optional expansion frame.

This gives a maximum data capacity for the L53 of 229 TB native (up to 458 TB with 2:1 data compression).

Up to 12 IBM LTO drives can be installed. LTO1, LTO2, LTO3, and LTO4 tape drives can be installed in the same frame. As you add more than four drives or install the additional I/O station, there is an incremental reduction in storage slots. It is also possible to install the LTO FC Drive Mounting Kit (FC1514) in advance, to simplify future tape drive installation, but it also reduces the number of available slots.

Each TS3500 Model L53 has a standard 16-slot LTO cartridge input/output station for importing or exporting cartridges from the library without requiring re-inventory or interruption of library operations. Optional features can provide 16 additional input/output slots for LTO (FC1658) or 3592 media (FC1659). The lockable library door can be opened for bulk-loading IBM LTO tape cartridges. Re-inventory of the cartridges is done in fewer than 60 seconds per frame each time the library door is closed. A barcode reader mounted on the autochanger scans the cartridge labels at less than one minute per frame. A door lock is included to restrict physical access to cartridges in the library.

TS3500 Tape Library Model D53

The D53 frame has the same footprint as the model L53.

The D53 cannot be installed on its own. It must be connected to a library with a base frame and optionally multiple expansion frames. Up to 16 frames can be connected together.

If one or more tape drives are installed in the D53, then the Enhanced Frame Control Assembly Feature (FC1451) is required along with the LTO Fibre Drive Mounting Kit (FC1514). This feature provides the hardware and firmware required to support IBM LTO drives within the D53 and also provides a redundant AC line feed for the L frame accessor. The Frame Control Assembly Feature is also required if LTO Fibre Drive Mounting Kit (FC1504) is installed.

You can easily configure D53 frames according to future requirements. By installing the Enhanced Frame Control Assembly (FC1451), the D53 frame is ready to host LTO drives. The LTO Fibre Drive Mounting Kit (FC1514) prepares the drive slots for hosting an LTO drive. This enables you to install or move LTO drives without any additional hardware changes.

A fully configured IBM TS3500 Tape Library with one L53 frame and 15 D53 frames supports up to 192 drives. An L53 base frame and 15 D53 expansion frames with a minimal drive configuration provides a maximum capacity of 6887 storage slots with a total capacity of 5.5 PB without compression.

The base L23 or L53 is always on the left and as many as 15 additional D53 and/or D23 expansion frames can be added to the right side. During the installation of additional D53 frames, the x-rail of the L frame where the accessor resides is extended, so that the accessor can move through the new installed frame.

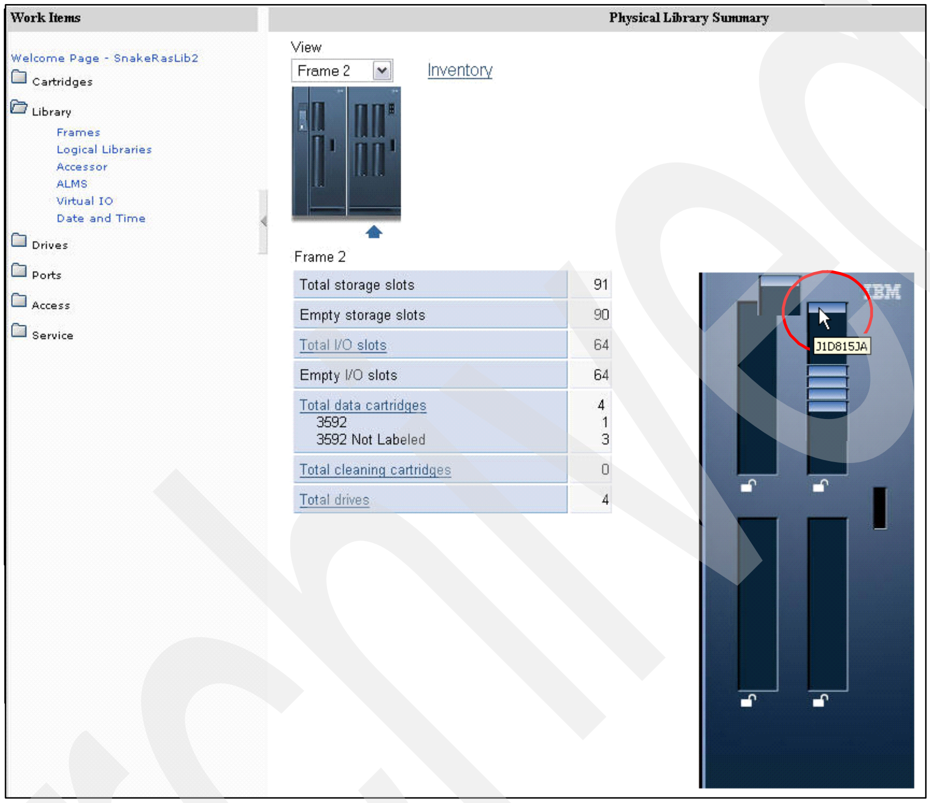
If a D53 is being added to an installed L32 or D32 frame, feature FC1610 is required, because the D53 is a shorter frame. This feature includes a short rear side cover for the Model D32/L32 frame and the Model D23/D53 front and rear side covers.

An additional 16-slot input/output station for LTO media should be ordered via feature FC1658 if attaching a D53 expansion frame to an L23 base frame.

An additional 4 I/O station door can be installed in a Dx3 frame. This requires Feature Code 1451, and up to three Dx3 frames can be installed with this feature. Figure 1-10 shows the 4 I/O Station D-Frame. On the right upper corner, a LED status panel is located. The LEDs represent the amount of cartridges per I/O station and indicate if the I/O station is locked. The I/O door has a total amount of 64 slots, 16 slots per I/O station.

The 4 I/O station door reduces the frame storage slot capacity by 176 for a model D53. The I/O stations increase the maximum library I/O station slots from 32 to 224 due to a maximum of three D23 or D53 I/O frames in a sixteen frame library. The D53 models are compatible with existing models L22, L32, L52, D22, D32, and D52.

Figure 1-10 shows a graphical overview of the 4 I/O station door using the Web user interface. In our example there are five cartridges imported in the upper right I/O station, and when you put your cursor on the data cartridge, it shows you the volume label.



Frame 2

Total storage slots	91
Empty storage slots	90
Total I/O slots	64
Empty I/O slots	64
Total data cartridges	4
3592	1
3592 Not Labeled	3
Total cleaning cartridges	0
Total drives	4

Figure 1-10 A graphical overview of the 4 I/0 door using the Web user interface

1.1.9 IBM TS3500 Tape Library frames L23 and D23

The Model L23 and D23 frames integrate the IBM TotalStorage 3592 Tape Drive with 4 Gbps dual-ported switched fabric Fibre Channel attachment. The TS3500 Tape Library Model L23 and D23 frames can be attached to LTO Frames (L53 and D53), and, therefore, TS1120 and LTO tape drives can be intermixed within the same TS3500 Tape Library.

The TS1120 Tape Drive used in the IBM TS3500 Tape Library Models L23 and D23 is designed for automation and uses a tape cartridge with a form factor similar to the IBM 3590 tape cartridges. The TS1120 Tape Drive has a dual-ported 4 Gbps Fibre Channel interface and has a native data rate of up to 100 MB/s. The TS1120 Tape Drives are designed to provide high levels of performance, functionality, and cartridge capacity supporting the 3592 tape format, including Write Once Read Many (WORM) media support.

IBM System Storage TS3500 Model L23 Frame

The TS3500 Model L23 provides cartridge slots for 3592 media and support for up to twelve TS1120. This model has the same footprint as the model L53. Data capacity for the model

L23 using 3592 data cartridges is 17 to 78 TB native. The L23 can be installed on its own as a complete library enclosure, or up to 15 Model D23 or D53 can be attached to it. The library capacity and number of drives can be expanded to meet changing requirements.

The L23 frame provides the major library components for the whole library, whether it has single or multiple frames. The expansion frames must be added to the right of the L53 frame.

The number of 3592 cartridge storage slots ranges from 58 to 260. The minimum configuration provides 58 slots available for actual use, although all 260 slots are already physically installed. To enable the additional slots for use (up to the total of 260), obtain an additional license key by ordering one of the following Capacity On Demand features. The Intermediate Capacity feature (FC1643) gives a total amount of usable cartridge slots of 117. This feature is required to add a Full Capacity feature (FC1644), which gives the capacity of 260 cartridge slots. The Full Capacity feature is required to add an additional I/O Slots feature (FC1658 or FC1659) or to attach the optional expansion frame models D23 or D53.

Up to 12 IBM TS1120 Tape Drives can be installed. Adding more than four drives or drive mounting kits, or installing the additional I/O station, reduces the number of storage slots available for use. You can also install the 3592 FC Drive Mounting Kit (FC1513) in advance, which simplifies future tape drive installation. This kit reduces the storage slots to the appropriate number and provides the power supply and necessary cables for installing a TS1120 drive.

Each L23 has a standard 16-slot 3592 cartridge input/output station for importing or exporting cartridges from the library without requiring re-inventory or interruption of library operations. Optional features can provide 16 additional input/output slots for LTO media. The lockable library door can be opened for bulk-loading cartridges. Re-inventory of the cartridges is done in fewer than 60 seconds per frame each time the library door is closed. A barcode reader mounted on the autochanger scans the cartridge labels at less than one minute per frame. A door lock is included to restrict physical access to cartridges in the library.

IBM System Storage TS3500 Model D23 frame

The D23 frame has the same footprint as the Model L23. The D53 cannot be installed on its own. It must be connected to a base frame and optionally other expansion frames. Up to 16 frames can be connected.

If one or more tape drives are installed in the D23, then the Enhanced Frame Control Assembly Feature is also required (FC1451). This feature provides the hardware and firmware required to support IBM 3592 drives within the D23 and provides a redundant line feed for the L23 or L53 accessor.

You can easily configure D23 frames according to future requirements. By installing the Enhanced Frame Control Assembly (FC1451), the D23 frame is ready to host TS1120 tape drives. The 3592 Fibre Drive Mounting Kit (FC1513) prepares the drive slots for hosting a TS1120 Tape Drive. This enables you to install or move 3592 drives without any additional hardware changes.

A fully configured IBM TS3500 Tape Library with one L23 frame and 15 D23 frames supports up to 192 drives. An L23 base frame and 15 D23 expansion frames with a minimal drive configuration provides a maximum capacity of 6260 storage slots with a total capacity of 4,382 PB without compression and using the TS1120 Tape Drive and 700GB cartridges.

The base frame (mode Lxx) is always on the left and as many as 15 additional expansion frames (Dxx) can be added to the right side. During the installation of additional D23 frames, the x-rail of the L frame where the accessor resides is extended, so that the accessor can move through the newly installed frame.

If a D23 is being added to an installed L32 or D32 frame, feature FC1610 is required, because the D23 is a shorter frame. This feature includes a short rear side cover for the Model D32/L32 frame and the Model D23/D53 front and rear side covers.

If attaching a D23 frame to an L53 frame, the First Expansion Frame Attachment Feature (FC9002) for the L53 must be specified. Subsequent expansion requires the Additional Expansion Frame Attachment feature (FC9003).

Additional 16-slot I/O stations for 3592 media should be ordered via feature FC1659 if attaching a D23 frame to a L53.

An additional 4 I/O station door can be installed in a D23 frame. This requires Feature Code 1451, and up to three Dx3 frames can be installed with this feature. Figure 1-10 on page 15 shows the 4 I/O Station D-Frame. On the right upper corner, a LED status panel is located. The LEDs represent the amount of cartridges per I/O station and indicate if the I/O station is locked. The I/O door has a total amount of 64 slots, 16 slots per I/O station.

The 4 I/O station door reduces the frame storage slot capacity by 160 for a model D23. The I/O stations increase the maximum library I/O station slots from 32 to 224 due to a maximum of three D53 I/O frames in a sixteen frame library. The D23 models are compatible with existing models L22, L32, L52, D22, D32, and D52.

1.1.10 IBM TS3500 High Availability Unit HA1

The IBM TS3500 High Availability Frame Model HA1 can be added to the IBM TS3500 Tape Library Base Frame Models. In conjunction with a service bay feature on the TS3500 Tape Library Model D23 or L23, the Model HA1 provides for the installation and operation of a second library accessor that is designed to operate simultaneously with the first accessor and service mount requests in the IBM TS3500 Tape Library. It is designed to non-disruptively fail over to a redundant accessor when any component of either accessor fails, which helps maintain availability and reliability. This design also includes the ability to add one or more Model D53 or D23 frames to an IBM TS3500 Tape Library that has an attached Model HA1 with minimal disruption.

Dual active accessor support is provided in a mixed media library. This includes any combination of 3592 and LTO media types. For example, a single library can have 3592, LTO1, LTO2, LTO3, and LTO4 media installed and configured. The Advanced Library Management Systems (ALMS) (see 1.1.15, "ALMS" on page 21) is required for support of dual accessors and two or more media types.

When dual accessors are installed and an attached host issues a command for cartridge movement, the library automatically determines which accessor can perform the mount in the most timely manner. If the library's primary accessor fails, the second accessor assumes control and eliminates system outage or the requirement for operator intervention.

A dual accessor library has two garage areas called service bays (see Figure 1-11). Service Bay A (the TS3500 High Availability Frame Model HA1) is to the left of and adjacent to the L-frame, when facing the front door. Service Bay B (a modified TS3500 Tape Library Model D23 or D53) is located to the right of the last active frame in the library.

The TS3500 Tape Library Model HA1 itself provides only a frame, which serves as Service Bay A for the original accessor for the TS3500 Tape Library Model Lxx. The second accessor is provided by ordering the Service Bay B Configuration and Dual Accessor feature (FC1440) on a TS3500 Tape Library Expansion Frame Model D23 or D53. When this feature is ordered on a Model D23 or D53, that expansion frame is reserved and functions as a Service Bay B for the second accessor. This feature should initially be installed on a new Model D23 or D53 frame that is added to the IBM TS3500 Tape Library when ordering the Model HA1. If your library already contains the service bays and you decide to add one or more D23 or D53 expansion frames, Service Bay B is converted to an expansion frame, the new frame, or frames are added to the right, and the last frame on the right is converted to Service Bay B. The downtime for this process is designed to be less than an hour.

The service bays are regular library frames but they do not have drives, power supplies, or node cards. Storage slots within the service bays are only used to test service actions. Figure 1-11 demonstrates how the Service Bays surround the other library frames.

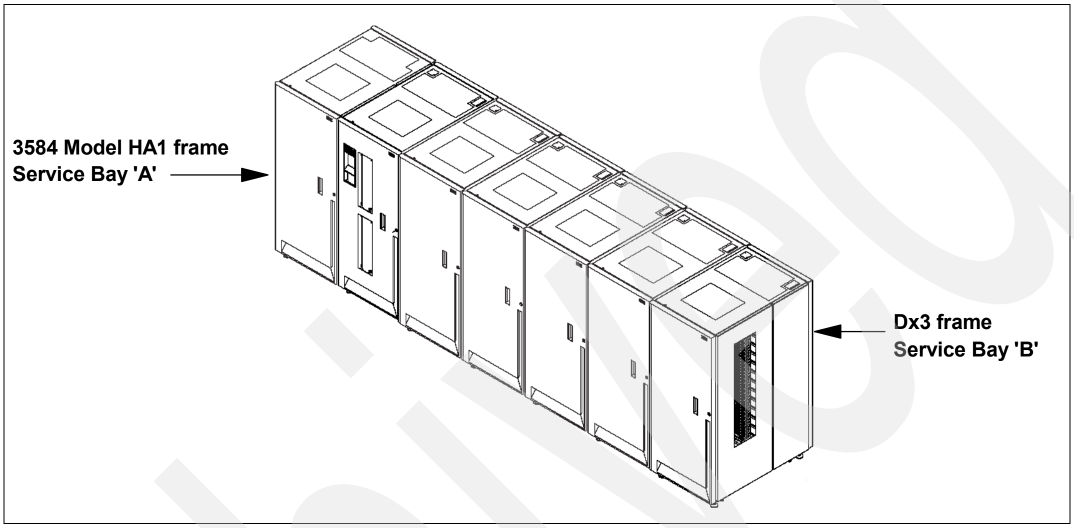


Figure 1-11 Location of service bays in the IBM TS3500 Tape Library

To summarize, to implement non-disruptive accessor failover, the following components are required:

- A TS3500 Model HA1 frame to act as Service Bay A
- High Availability Library feature (FC9040) for the Lxx frame
- Advanced Library Management System feature (FC1690)
- A D53 or D23 frame to operate as Service Bay B for the second accessor
- Additional expansion frame Attachment (FC9003)
- Service Bay B Configuration with Accessor (FC1440)

1.1.11 Control path failover

Control path failover, currently available for AIX, Linux, Solaris, HP-UX, and Windows hosts, configures multiple physical control paths to the same logical library within the device driver and provides automatic failover to an alternate control path when a permanent error occurs on one path. This is transparent to the running application.

For example, consider a simple multi-path architecture connection consisting of two HBAs in a host that are connected to a library with two or more drives. Two drives have the control ports enabled. The two HBAs are connected to the first and second control port drives, respectively. This simple configuration provides two physical control paths to the library for redundancy if one path from an HBA to the library fails. When the server boots, each HBA detects a control port to the library, and two medium changer devices (smc0 and smc1) are configured. Each logical device is a physical path to the same library; however, an application can open and use only one logical device at a time, either smc0 or smc1.

Without the device driver alternate pathing support, if an application opens smc0 and a permanent path error occurs (because of an HBA, cable, switch, or drive control port failure), the current command to the library fails. It is possible to initiate manual failover by changing the device path to the alternate path (smc1), but this is a manual operation and the last failing command has to be resent.

When the alternate pathing support is enabled on both smc0 and smc1, the device driver configures them internally as a single device with multiple paths. The application can still open and use only one logical device at a time (either smc0 or smc1). If an application opens smc0 and a permanent path error occurs, the current operation continues on the alternate path without interrupting the application.

Activation of control path failover is done by entering a license key at the library Operator Panel. Control path failover is provided by an optional FC1680 for Lx2 frame models and requires the use of the IBM Atape device driver. For Lx3 models, control path failover and data path failover are available with the optional Path Failover feature (FC1682).

1.1.12 Data path failover

Data path failover and load balancing exclusively support native Fibre Channel LTO and IBM 3592 tape drives in the IBM TS3500 Tape Library using the IBM device driver. Data path failover is now supported for AIX, Linux, HP, Solaris, and Windows hosts. Load balancing is supported for AIX, Linux, and Solaris. Refer to the *IBM Ultrium Device Drivers Installation and User's Guide*, GA32-0430*,* for current support and implementation details.

Data path failover provides a failover mechanism in the IBM device driver, so that you can configure multiple redundant paths in a SAN environment. If a path or component fails, the failover mechanism is designed to provide automatic error recovery to retry the current operation using an alternate, preconfigured path without stopping the current job in progress. This improves flexibility in SAN configuration, availability, and management. When accessing a tape drive device that has been configured with alternate pathing across multiple host ports, the IBM device driver automatically selects a path through the HBA that has the fewest open tape devices and assigns that path to the application. This autonomic self-optimizing capability is called *load balancing*.

The dynamic load balancing support is designed to optimize resources for devices that have physical connections to multiple HBAs in the same machine. The device driver is designed to dynamically track the usage on each HBA as applications open and close devices, and balance the number of applications using each HBA in the machine. This can help optimize HBA resources and improve overall performance. Further, data path failover provides autonomic self-healing capabilities similar to control path failover, with transparent failover to an alternate data path in the event of a failure in the primary host-side path.

Data path failover and load balancing for Linux and Solaris are provided by an optional feature (FC1681) for Lx2 models. Data path failover is included in the Path Failover feature (FC1682) for Lx3 models, which also includes control path failover.

Data path failover and load balancing support for IBM 3592 tape drives do not require this feature.

1.1.13 SNMP

Occasionally, the IBM TS3500 Tape Library might encounter a situation that should be reported, such as an open door that causes the library to stop. Because many servers can attach to the IBM TS3500 Tape Library by differing attachment methods, the library provides a standard TCP/IP protocol called Simple Network Management Protocol (SNMP) to send alerts about conditions (such as an opened door) over a TCP/IP LAN network to an SNMP monitoring server. These alerts are called *SNMP traps*. Using the information supplied in each SNMP trap, the monitoring server (together with customer-supplied software) can alert operations staff of possible problems or operator interventions that occur. Many monitoring servers (such as IBM Tivoli NetView®) can be used to send e-mail or pager notifications when they receive an SNMP alert.

1.1.14 SMI-S support

This section describes how the IBM TS3500 Tape Library uses the Storage Management Initiative - Specification (SMI-S) to communicate in a SAN environment.

To communicate with storage devices in a SAN, management software can use other software known as the Storage Management Initiative - Specification (SMI-S) Agent for Tape. The SMI-S Agent for Tape is available for Intel®-based SuSE LINUX Enterprise Server 9. The SMI-S Agent for Tape communicates by using the Web-Based Enterprise Management (WBEM) protocol, which allows management software to communicate with the IBM TS3500 Tape Library.

The SMI-S Agent for Tape is designed for compliance with the Storage Management Initiative - Specification. The SMI-S is a design specification of the Storage Management Initiative (SMI) that was launched by the Storage Networking Industry Association (SNIA). The SMI-S specifies a secure and reliable interface that allows storage management systems to identify, classify, monitor, and control physical and logical resources in a Storage Area Network (SAN). The interface is intended as a solution that integrates the various devices to be managed in a SAN and the tools used to manage them. The SMI-S was developed to address the problems that many vendors face in managing heterogeneous storage environments. It creates a management interface protocol for multivendor storage networking products. By enabling the integration of diverse multivendor storage networks, the initiative is able to expand the overall market for storage networking technology.

For detailed information about SMI-S, see the *IBM TotalStorage SMI-S Agent for Tape Installation Guide*, GC35-0512.

The SMI-S agent ran normally on a separate LINUX PC but from library firmware level 7050 SMI-S, in a limited form, is running on the MCP. The level of SMI-S is 1.1 and the following functions are supported within the Server Profile:

- Library code level:
  - Use IBMTSSML3584_SoftwareIdentity VersionString.
- Library name:
  - Use IBMTSSML3584_TapeLibrary ElementName.
- Administrator and Contact information:
  - Use IBMTSSML3584_TapeLibrary PrimaryOwnerName and PrimaryOwnerContact.

There is no support for Service Location Protocol (SLP) and Secure Socket Layer (SSL) at the time of writing this publication.

The external LINUX PC supports the following protocols:

- Server Profile SMI-I Version 2
- Storage Media Library Version 2
  - Limited Access Port 1.1
  - Chassis 1.1
  - FC Port 1.1
  - Software 1.1
  - Physical Package 1.1

In the future, the imbedded SMI-S should have the same functions as the external LINUX PC.

Note: The imbedded SMI-S function requires an Lx3 Frame and a library firmware level that supports SMI-S.

1.1.15 ALMS

The Advanced Library Management System (ALMS), an optional extension to the IBM patented multi-path architecture (FC1690), provides enhanced flexibility and capabilities for partitioning the IBM TS3500 Tape Library. ALMS virtualizes the SCSI element addresses while maintaining the approach of the multi-path architecture and using SCSI Medium Changer commands. Without ALMS, everything is based on the SCSI element address (location-centric) and partitioning is based on real cartridge slots and drive slots. With ALMS, there is no affinity between a real slot address and a SCSI Element address reported to the server and used by the server. Instead there is now an affinity with the VOLSER (volume serial numbers on the barcode label of the cartridge). For further information and examples of using ALMS, see 2.3, “Partitioning the TS3500 with ALMS enabled” on page 60.

Note ALMS is available only for the IBM TS3500 Tape Library and requires FC1690 for enablement.

1.1.16 Virtual I/O

The IBM TS3500 Tape Library has I/O stations and I/O slots that enable you to import and export up to 32 cartridges at any given time. The I/O slots are also known as *import/export elements (IEEs)*. As a feature of ALMS, Virtual I/O (VIO) slots increase the quantity of available I/O slots by allowing storage slots to appear to the host as I/O slots. Storage slots that appear to the host as I/O slots are called *virtual import/export elements (VIEEs)*. The goal of virtual I/O slots is to reduce the dependencies between the system administrator and library operator so that each performs their import and export tasks without requiring the other to perform any actions. With virtual I/O slots, the library automatically moves cartridges from the I/O stations to physical storage slots and from physical storage slots to the I/O stations. For further description of Virtual I/O, refer to 2.3.2, “Virtual I/O” on page 65.

1.1.17 Element number

Element numbers identify the physical location within the library. This information is required mostly for storage applications, such as IBM Tivoli Storage Manager, which translate the device to a name that the robotic system understands.

In the IBM TS3500 Tape Library, each SCSI storage element is assigned a SCSI element address. A SCSI storage element is a physical location capable of holding a tape cartridge (such as an I/O slot, drive, or storage slot). The element numbering is grouped in:

- Tape drive sequence
- I/O station sequence
- Cartridge slot sequence

Note: The numbering is contiguous for the cartridge slot sequence. However, the addition, removal, or movement of one or more tape drives can affect the element numbering of the cartridge slots.

Figure 1-1 shows the element numbers for tape drives in each IBM TS3500 Tape Library frame up to six frames. For element numbers up to the maximum 16 frames, see the *IBM System Storage TS3500 Tape Library Operator Guide*, GA32-0560 for further information.

Table 1-1 IBM TS3500 Tape Library tape drive element numbers

Drive number	**Frame 1 (Lx3)**	**Frame 2 (Dx3)**	**Frame 3 (Dx3)**	**Frame 4 (Dx3)**	**Frame 5 (Dx3)**	**Frame 6 (Dx3)**
1	257	269	281	293	305	317
2	258	270	282	294	306	318
3	259	271	283	295	307	319
4	260	272	284	296	308	320
5	261	273	285	297	309	321
6	262	274	286	298	310	322
7	263	275	287	299	311	323
8	264	276	288	300	312	324
9	265	277	289	301	313	325
10	266	278	290	302	314	326
11	267	279	291	303	315	327
12	268	280	292	304	316	328

Each element in the IBM TS3500 Tape Library (the cartridge storage slots, I/O storage slots, and tape drives) has two addresses:

- Physical address
- SCSI element address

When initiating an operation such as moving a tape cartridge or performing manual cleaning, you can use the physical or logical address to specify a location in the library.

The physical address consists of frame, column, and row identifiers that define a unique physical location in the library. The address is represented as:

- Fx,Cyy,Rzz for a storage slot (where F equals the frame and x equals its number, C equals the column and yy equals its number, and R equals the row and zz equals its number)
- Fx,Rzz for a tape drive and I/O storage slot (where F equals the frame and x equals its number, and R equals the row and zz equals its number)

The SCSI element address consists of a bit and hex value that defines to the SCSI interface a logical location in the library. This logical address is represented as xxxx (X'yyy'), where xxxx is a bit value and yyy is a hex value. It is assigned and used by the host when the host processes SCSI commands. The SCSI element address is not unique to a storage slot, drive, or I/O slot; it varies, depending on the quantity of drives in the library.

For example, the storage slot address F2,C03,R22 means:

- F2: Frame 2 (first expansion frame)
- C03: Column 3 (second column from left on drive side)
- R22: Row 22 (22nd position down from the top of the column)

Each drive has a unique address to indicate its physical location. The drive address consists of two values, a frame number and a row number:

- Frame number: Represented as Fx, where F equals the frame and x equals its number. Regardless of whether any drives are installed, the frame number for the base frame is 1 and increments by one for each adjacent expansion frame.
- Row number: Represented as Rzz, where R equals the row and zz equals its number. The row number is 1 for the top drive position in the frame, and increments by one for each row beneath the top drive. Regardless of whether drives are installed, the row numbering is the same for every frame.

A drive address of F2,R10 means frame 2 (that is, the first expansion frame), row 10 (tenth drive position from the top of the column).

Note: ALMS virtualizes a SCSI element address. Therefore, there is no relationship between physical location and SCSI element address if using ALMS.

1.2 Other IBM System Storage Tape Models

Here we describe the two models of IBM Open Systems Tape that belongs to the IBM System Storage Enterprise Tape Family. They are the IBM TS1120 Tape Drive and IBM TS3400 Tape Library.

1.2.1 IBM System Storage TS1120

The TS1120 Tape Drive is the follow-on to the IBM 3592 Tape Drive Model J1A and the highly successful 3590 Enterprise Tape Drive. The TS1120 Tape Drive can be installed in the IBM System Storage TS3500, the IBM TotalStorage 3494 Tape Library, the IBM System Storage TS3400 and in a StorageTek™ 9310 Powderhorn™.

The tape drive uses IBM 3592 Cartridges, which are available in limited capacity (100GB) for fast access to data, standard capacity (500GB) or extended capacity (700GB). All three cartridges are available in re-writable or Write Once Read Many (WORM) format.

The TS1120 Tape Drive is supported in a wide range of environments including selected IBM System i, System p, xSeries®, IBM mainframe Linux, Sun, and Hewlett Packard servers, as well as Intel-compatible servers running Linux, Microsoft Windows 2000, or Windows Server® 2003. A tape controller is required for attachment to ESCON® or FICON® channels on IBM mainframe servers. Sharing drives optimizes drive utilization and helps reduce infrastructure requirements.

The TS1120 tape drive supports a native data transfer rate of up to 104 MBps. In Open Systems environments where data typically compresses at 2:1, the TS1120 tape drive can transfer data up to 200 MBps. In a mainframe environment where data typically compresses at 3:1, a single tape drive can transfer data up to 260 MBps. This high transfer rate help reduce backup and recovery times.

Figure 1-12 shows the IBM System Storage TS1120 Tape Drive.

Figure 1-12 IBM System Storage TS1120 Tape Drive

For more information about the IBM TS1120 Tape Drive, see the *IBM System Storage Tape Libraries Guide for Open Systems,* SG24-5946.

1.2.2 IBM System Storage TS3400 Tape Library

The IBM System Storage TS3400 Tape Library (Machine type 3577, Model 5LU) is designed to offer high performance drive technology and automation for the Open Systems environment. The IBM System Storage TS3400 Tape Library is a five unit (5U) external desktop or rackmountable tape library that incorporates one or two IBM System Storage TS1120 Tape Drives Model E05.

The IBM System Storage TS1120 Tape Drive has a native capacity of 700 GB, when using the IBM Extended Data Cartridge (JB) or 500 GB when using the IBM Data cartridge (JA). The only attachment to the host is a 4 GB/s switch fabric Fibre Channel connection. The tape drives must be ordered separately with the final order.

The IBM System Storage TS3400 Tape Library supports the IBM System Storage TS1120 Tape Drive built-in encryption capabilities. The encryption methods are Application-Managed-Encryption (AME), System-Managed-Encryption (SME), and Library Managed Encryption (LME).

The previous IBM System Storage 3592 J1A Tape Drive is not supported in the IBM System Storage TS3400 Tape Library.

Designed for tape automation, the IBM System Storage TS3400 Tape Library can be attached to BM System p, IBM System i, IBM System x, Microsoft Windows, HP-UX, Sun Solaris, UNIX, Linux, and PC servers.

The IBM System Storage TS3400 Tape Library has two removable cartridge magazines providing 18 data cartridges slots including a 3 slot I/O station. The total native storage capacity is 12.6 TB when using the 700 GB data cartridges.

The IBM System Storage TS3400 Tape Library incorporates IBM´s Multi-Path Architecture with one or two logical libraries. The TS1120 has two FC ports (dual ported) to make a connection to the host. The TS1120 provides a sustained native data transfer rate of 100MB/s.

Standard features for the IBM System Storage TS3400 Tape Library: Control path and data path fail over, barcode reader, dual power supplies, remote management and the possibility to use the IBM System Storage TS3400 Tape Library in sequential or random access mode.

Figure 1-13 shows the front view of the IBM TS3400 System Storage Tape Library.

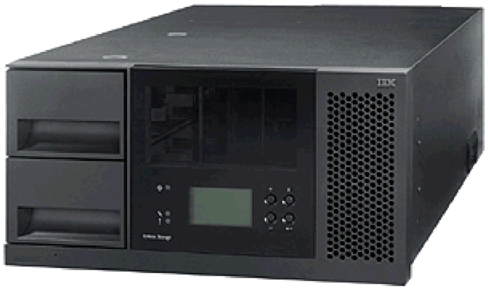


Figure 1-13 Front view of the IBM TS3400 System Storage Tape Library

For more information about the IBM TS3400 Tape Library, see the *IBM System Storage Tape Libraries Guide for Open Systems,* SG24-5946.

2

IBM Open Systems Tape Library sharing and partitioning

In this chapter we describe the sharing and partitioning of the following IBM tape libraries:

- IBM System Storage TS3100 Tape Library
- IBM System Storage TS3200 Tape Library
- IBM System Storage TS3310 Tape Library
- IBM System Storage TS3400 Tape Library
- IBM System Storage TS3500 Tape Library.

The topics covered in this context are:

- Tape library sharing and partitioning definitions
- Tape Library Specialist
- Advanced Library Management System - ALMS
- Using the Tape Library Specialist for partitioning the tape libraries
- Using the operator panel for partitioning the IBM System Storage TS3500 Tape Library
- Using and partitioning the IBM System Storage TS3500 Tape Library with ALMS

For additional discussions on tape library sharing, refer to *Get More Out of Your SAN with IBM Tivoli Storage Manager*, SG24-6687.

Details about the ALMS functionality and setup can be found in the TS3500 manuals:

- *IBM System Storage TS3500 Tape Library Operator Guide*, GA32-0560
- *IBM System Storage TS3500 Tape Library Introduction and Planning Guide*, GA32-0559

2.1 Definitions

In general, the sharing of devices improves the utilization of the devices and can reduce the total cost of ownership. Sharing of disk subsystems among multiple host systems is a common practice. Similar sharing of a tape device can improve the utilization of the tape drive because normally it is not used 100% of the time by a single client (host). In the Open Systems world there are different possible ways to share either a tape library or tape drives among multiple hosts. The most basic requirement in sharing any library between backup applications and servers is the ability to control the medium changer. The tape drives and media might or might not be shared, but the medium changer must be available to be manipulated by all of the backup applications and servers.

2.1.1 Library sharing

We differentiate between outboard library management and the multipath approach.

Outboard library management

One approach is to share the library but not the tape drives. Multiple servers attached to a tape library can share the library robotics. Drives and cartridges are pooled, and such a drive and cartridge pool belong to one set of servers (one server or multiple servers) and cannot be shared with another set of servers.

Some applications, like IBM Tivoli Storage Manager use the name “library sharing” if they share drives and library. We explain drive sharing later.

Some technique is necessary to share the library robotics. The most common way is to use an outboard library manager that controls the library. The library manager receives the commands from the attached servers, controls the resources inside the library, and executes the commands received from the servers. The communication between the library manager and attached servers normally takes place over the LAN using a proprietary command set.

The *tape library manager* controls access to and sequencing of the medium changer. The medium changer is physically available to all backup and application servers. The IBM 3494 Tape Library uses this type of library sharing. Support for communication with the IBM 3494 Tape Library manager is built into the i5/OS operating system while for Unix systems a command set called mtlib from the IBM tape device driver must be used (see Figure 2-1). Other examples are STK with ACSLS, or ADIC with Scalar DLC.

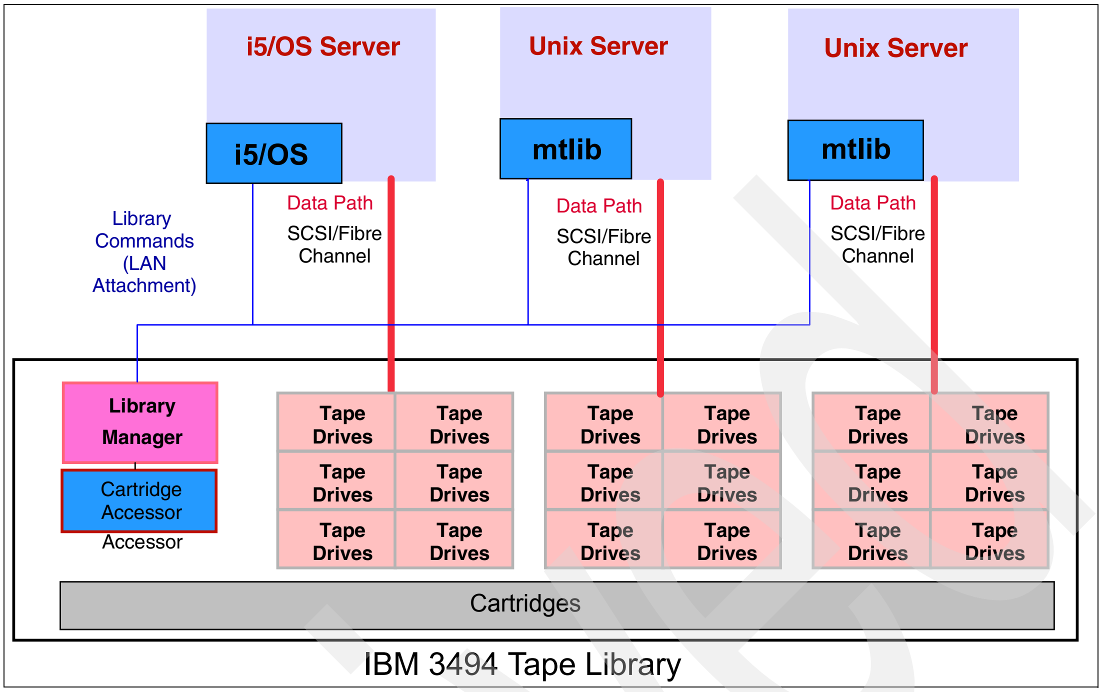


Figure 2-1 IBM 3494 Tape Library sharing

The IBM 3494 Tape Library pools cartridges by using categories. Drives, on the other hand, are pooled by simply connecting them to one set of servers.

Multi-path SCSI Medium Changer Library

The disadvantage of the outboard library management is that it introduces an additional software layer for the library manager. The IBM patented multi-path architecture eliminates this disadvantage.

Multi-path architecture is the capability of a tape library to provide multiple paths to the library robotics without requiring a library manager. This capability allows the *partitioning* of the physical library into several logical libraries. A logical partition (logical library) contains tape drives and storage slots. The library robotics are shared among all logical partitions and the tape library controls access and sequencing to the medium changer. All IBM LTO Tape Libraries with more than one tape drive, including the high-end IBM System Storage TS3500 Tape Library, offer this partitioning capability at no additional cost. Partitioning is available for SCSI and FC drives.

Figure 2-2 shows the multipath design of all IBM TS3xxx Tape Libraries. Every drive can have a path defined to the SCSI medium changer. The library in this example has been partitioned into three logical libraries. Each logical partition has two tape drives and a set of cartridge slots. All the servers share the library robotics, but not the drives or the cartridges.

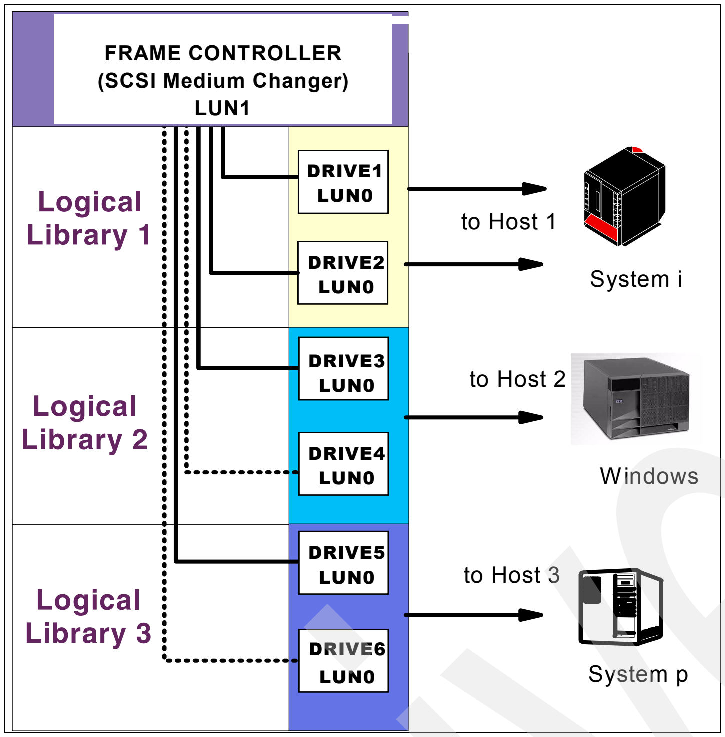


Figure 2-2 IBM multipath architecture and logical partitioning

This kind of partitioning uses static assigned resources. There is no sharing of these resources (tape drives and cartridge slots), which means servers from one partition cannot access tape drives or cartridges in another partition. The assignment of resources to the different logical partitions is defined through static rules and must use contiguous resources. In other words, you create barriers around the logical library. This type of partitioning is also called first generation of multipath architecture.

Advanced Library Management System (ALMS), which is the second generation of multipath architecture, does not have to partition the library using static rules and contiguous resources. ALMS virtualizes the affinity to physical resources.

This second type of partitioning allows heterogeneous applications to share the library robotics independent of each other. ALMS is offered as a feature for the TS3500. For further detail, see 2.3, “Partitioning the TS3500 with ALMS enabled” on page 60.

2.1.2 Homogenous drive sharing in an Open Systems environment

Because a tape drive cannot be accessed simultaneously by several servers, a mechanism is required to manage and control access. Currently, there are different solutions available that allow some kind of tape drive sharing. The most common way in the Open Systems world is to do a homogenous drive sharing. Homogenous means that one master host takes care of the access control, and allows other servers that are running the same backup application to share the tape drives. All servers access the medium changer through the master such as multiple IBM Tivoli Storage Manager servers communicating through one IBM Tivoli Storage Manager Library Manager server being the master. The master server controls physical access (such as mount and demount cartridges) and sequencing to the medium changer (see Figure 2-3).

The tape drives appear to each Tivoli Storage Manager server as locally attached devices. When a server requests a tape to be loaded for a tape operation, the server contacts the master with the request. The master mounts the tape, then passes control back to the requesting server. The server then reserves (SCSI reserve) the same drive to itself (to ensure that no other server can access the tape drive and overwrite data). When the operation is complete, the server unloads the cartridge, releases (SCSI release) the reserve on the drive, and notifies the master to demount the cartridge. The master then demounts the media.

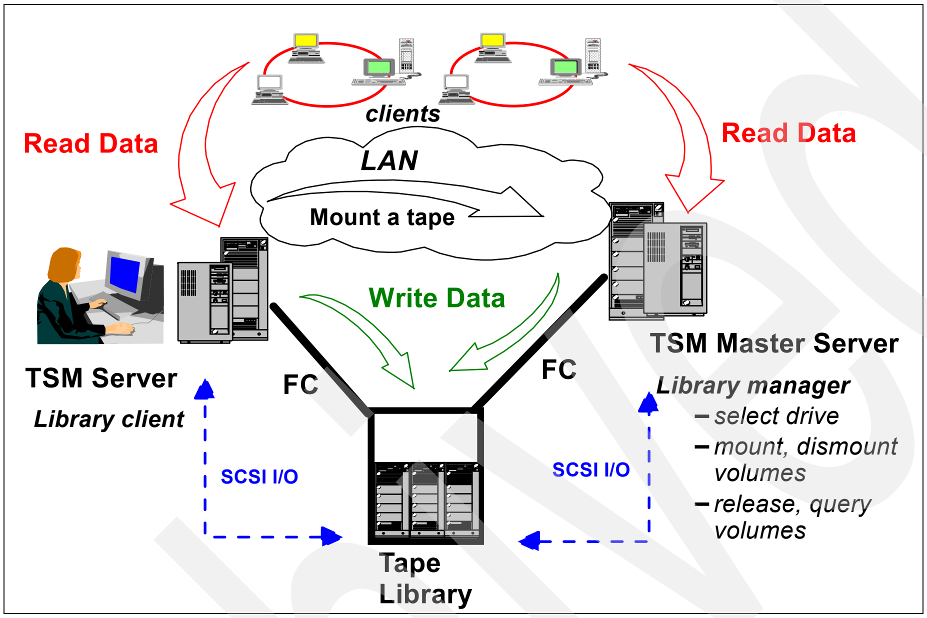


Figure 2-3 Tivoli Storage Manager library sharing

Homogeneous drive sharing is also commonly used for LAN-free backups where a kind of light-weight Tivoli Storage Manager server provided with the Tivoli Data Protection (TDP) client is installed on each client for direct access to the tape drives as shown in Figure 2-4.

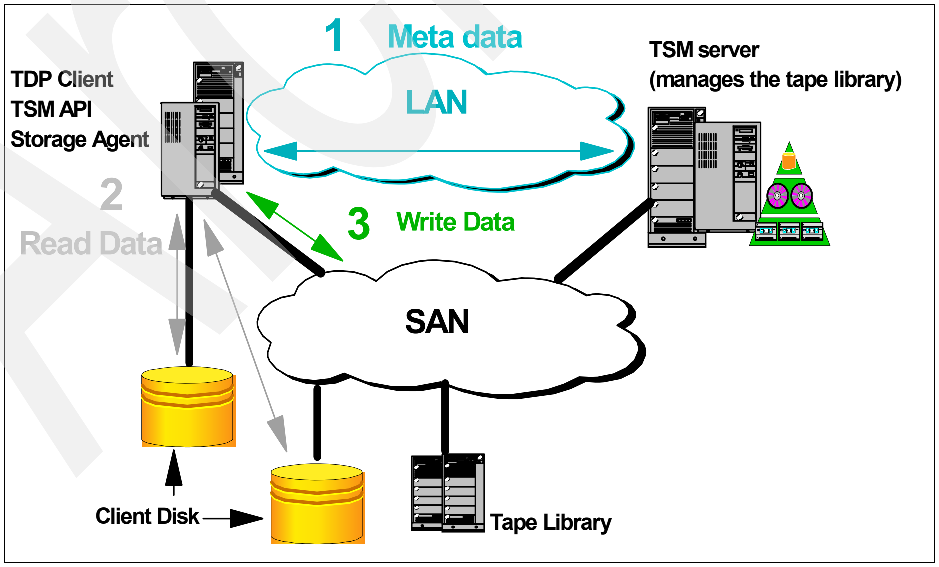


Figure 2-4 LAN-free backup

2.1.3 Deciding which Library Sharing method to use

Whenever multiple Open Systems servers running the same storage management (homogenous) application have to share the same tape library, we suggest using the application's own sharing capabilities. This ensures the most efficient library and drive sharing. In an Open Systems environment, the master server can normally provide sharing functions for all tape drives to all client servers. The master server also manages the cartridges in the library; so that you require only one scratch pool, instead of several scratch pools (one for each server).

Figure 2-5 shows an example of how sharing capabilities from the application can address the sharing requirements. This example is built on IBM Tivoli Storage Manager, but it works also with other applications such as VERITAS NetBackup or EMC Legato NetWorker. There are two locations in the example, each with its own data processing application, server, and storage. The SAN spans over both locations. There are three backup servers, with many clients attached to them performing the backup jobs.

For disaster recovery reasons, all backup data is copied to the second location. One or more tape libraries are installed in each location. In every location, one backup server manages the tape library (library manager) and handles all mount requests issued by the other backup servers. Any backup server from location 1 asks Library Manager Server 1 (Tivoli Storage Manager Server 1) to assign a tape to it and mount a cartridge in Library 1. If a backup server from location 1 copies the data to location 2, then it asks Library Manager Server 2 (Tivoli Storage Manager Server 2) to mount a tape on Library 2.

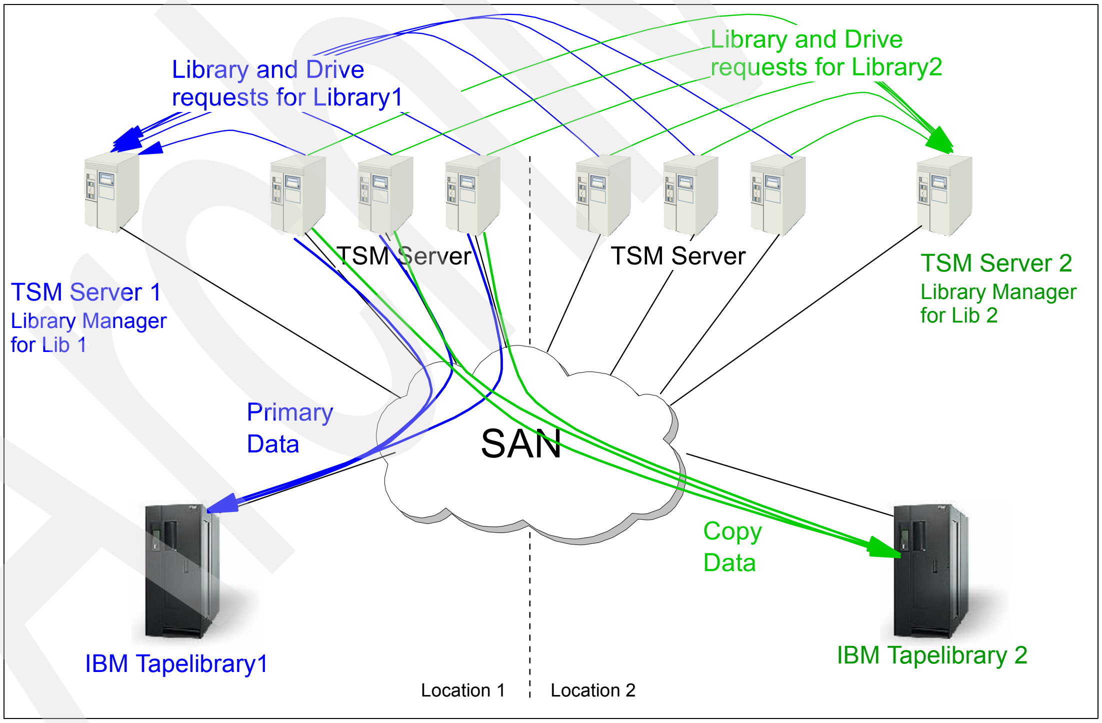


Figure 2-5 Library sharing in an Open Systems environment done by Tivoli Storage Manager

However, in some cases, even if you use one homogenous backup application, it might not be adequate to use the sharing option of the application itself, and instead use the partitioning capabilities of the library. This is the case if for security reasons you have to separate the data coming from the different backup servers; in this situation you require the partitioning function of the library to guarantee separation of the data.

Also, if different backup applications are used, it becomes mandatory to use the partitioning function of the library, such as for System i on the one hand and Tivoli Storage Manager running on Windows or UNIX on the other hand connected to the same library.

Backup Recovery and Media Services (BRMS) is the recommended and strategic solution for planning and managing backups on the System i platform. Refer to Chapter 6, “Implementing tape with Backup Recovery and Media Services” on page 153 for further details about BRMS and its implementation.

> **Note:** The available *BRMS Tivoli Storage Manager client* does not support save-while-active or save of system data. Since the system cannot be recovered from Tivoli Storage Manager, a local save is enforced for system data. For further information about using BRMS with Tivoli Storage Manager, refer to Appendix B, “BRMS and Tivoli Storage Manager” on page 301.
>
> i5/OS uses SCSI reserve/release commands to support sharing of its tape drives among multiple servers. However, the operator still has to plan the schedule of the servers’ backups to ensure that shared tape drives are available to each server when required.

2.1.4 Tape Library Specialist

The IBM *Tape Library Specialist* is a Web-based graphical user interface for configuring, updating, and administering IBM tape libraries. The Tape Library Specialist is an embedded functionality with the IBM TS3000 family of tape libraries.

The communication is through an Ethernet connection between the Web browser and the tape library. The Ethernet speed is 10/100MB full duplex, and it is auto-negotiated with the host or switch. Once the library is set up for using the IBM Tape Library Specialist, you can connect to the Library using a Web browser, for example, Microsoft Internet Explorer®. We recommend that you upgrade your Java™ runtime environment to the latest available version, which is available at:

http://java.com/en/

In the following sections, we describe in more detail the IBM Tape Library Specialist applications for the IBM TS3100/TS3200, TS3310, TS3400, and TS3500. When the library has been connected to the network, use the Operator Panel to establish the IP address. It can then be accessed from the Web browser using a default user ID and password.

> **Note:** In all our examples, we are using the default user ID and password to connect to the library. However, for obvious security reasons, we recommend that you change the default password, and also establish your own ID and password.
>
> Make sure to update the password to secure the access.

The layout of the Tape Library Specialist varies between the libraries, but the general content is similar. It includes functions such as these:

- Monitor the library
- Configure the library
- Manage the library
- Manage access to the library
- Service the library

This layout is exemplified in the library tasks for the TS3400 library; see Figure 2-6.

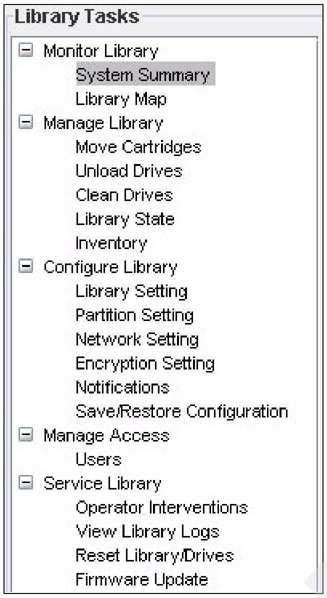


Figure 2-6 TS3400 Tape Library Specialist - Library Tasks

2.2 Partitioning multi-path tape libraries

The IBM TS3100, TS3200, TS3310, TS3400, and TS3500 Tape Libraries all use the patented multi-path architecture, and those libraries can be partitioned. You can use multiple logical libraries to share the physical library between applications, or when allowed by the library (as for TS3500), to support mixed drive types for any application. You can create multiple logical libraries by partitioning the physical library storage slots and tape drives into two or more logical libraries. They can all be partitioned into as many libraries as there are tape drives installed.

Each logical library consists of:

- Tape drives
- Storage slots
- Input/output (I/O) slots
- Cartridge accessor

Each logical library has its own *control path*, which is a logical path into the library through which a server sends standard SCSI medium changer commands to control the logical library. Each logical library control path is available to servers through a Logical Unit Number 1 (LUN 1) of the first drive that is defined within that logical library. A logical library cannot share another logical library’s tape drives and storage slots, therefore, a tape library must have at least two tape drives installed so that it can be partitioned. However, it does share the I/O slots, and the cartridge accessor on a first-come, first-served basis.

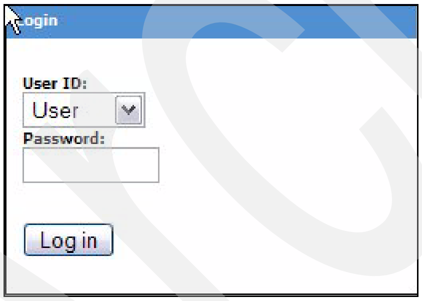
2.2.1 Setting up and configuring the IBM TS3100 / TS3200

Attach your library to the network. Using the TS3100/TS3200 operator panel, set the IP address, subnet mask, and gateway address. See the *IBM System Storage TS3100 Tape Library and TS3200 Tape Library Installation Quick Reference*, GA32-0548 for setup details.

Follow these steps:

1. Enter the Network Settings using the Operator Control Panel Configuration menu. We recommend setting a fixed IP address. Press **down** to highlight the Network menu, and **enter** to display.
2. Press **down** to select IP Address:
   a. Press **enter** to highlight the IP Address field
   b. Press **up** or **down** to select the digit(s) of your library's IP Address
   c. Press **enter** to highlight the next digit(s) in your IP Address
   d. After entering the final digits, press **enter** to apply your entries.
3. Press **down** to select Netmask. Continue as for the IP address.
4. Press **down** to select Gateway. Continue as for the IP address.
5. After entering the final digits in your Gateway address, press **down** and select one of the following choices:
   – **Save:** To save your network settings.
   – **Cancel:** To cancel all of your entries and leave the settings as they were.
6. Press **enter** to return to the Configure menu. and **cancel** twice to return to the home panel.

You are now able to access the Tape Library Specialist from a Web browser by entering the tape library IP address. Figure 2-7 shows the Login panel.

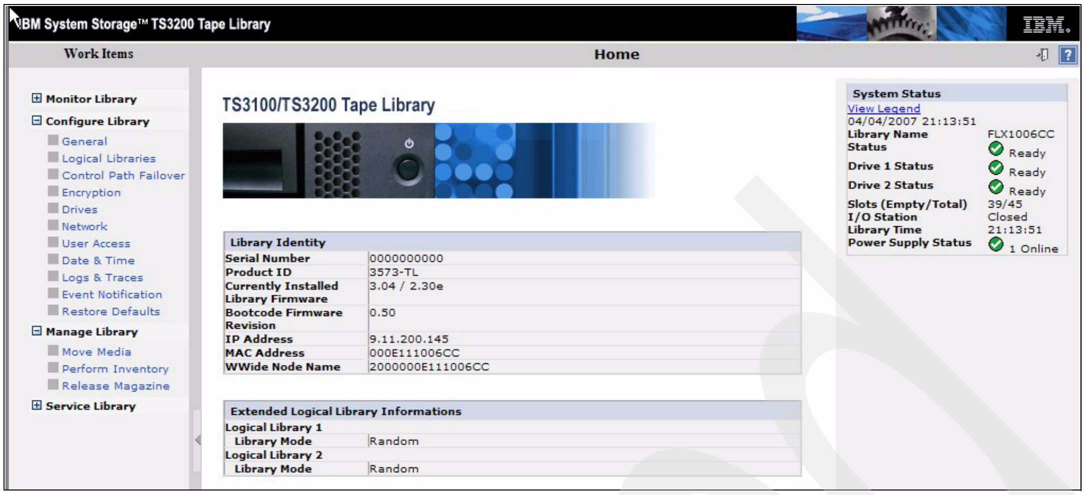


User ID: User

Figure 2-7 IBM TS3200 Tape Library Login panel

Log in as an Administrator; the default password is `secure`. When logged in as a standard user, you can only access the Status and Information functions; configuration changes cannot be made. If you cannot log on, check that the library is not in offline mode.

Click the **Login** button to log in. This shows the Home menu, and you can now perform any operations on the library; see Figure 2-8.



Library Identity

Serial Number	0000000000
Product ID	3573-TL
Currently Installed Library Firmware	3.04 / 2.30e
Bootcode Firmware Revision	0.50
IP Address	9.11.200.145
MAC Address	000E111006CC
WWide Node Name	2000000E111006CC

Extended Logical Library Informations

Logical Library 1	
Library Mode	Random
Logical Library 2	
Library Mode	Random

System Status

View Legend

04/04/2007 21:13:51

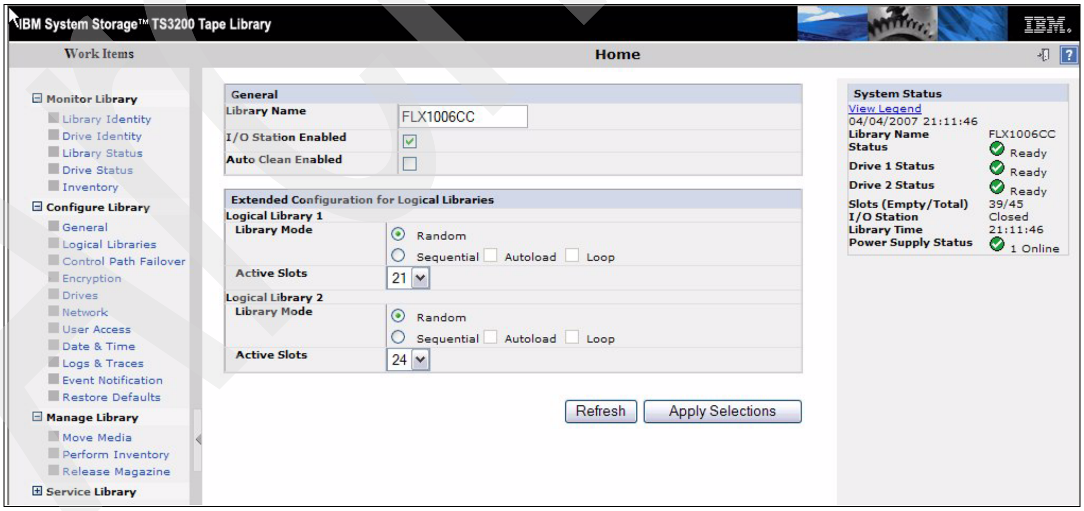
Library Name	FLX1006CC
Status	✓ Ready
Drive 1 Status	✓ Ready
Drive 2 Status	✓ Ready
Slots (Empty/Total)	39/45
I/O Station	Closed
Library Time	21:13:51
Power Supply Status	✓ 1 Online

Figure 2-8 IBM TS3200 Home menu

2.2.2 Partitioning the IBM TS3100 and TS3200

The IBM TS3200 library can accommodate two full-high drives or four half-high drives, and can accordingly be partitioned into multiple libraries. Similarly, the TS3100 can accommodate two half-high drives and can then also be partitioned. They use the same Tape Library Specialist.

1. Start the Tape Library Specialist.
2. In the Home panel (see Figure 2-8), select the **Configure Library** → **Logical Libraries** to define one or more partitions. Select the partitions, and **submit**. You are asked to verify the update, and then the reconfiguration starts, taking some minutes.
3. Verify the definitions selecting **Configure Library** → **General**; see Figure 2-9.



General

Library Name	FLX1006CC
I/O Station Enabled	☑
Auto Clean Enabled	□

Extended Configuration for Logical Libraries

Logical Library 1	
Library Mode	● Random ○ Sequential □ Autoload □ Loop
Active Slots	21
Logical Library 2	
Library Mode	● Random ○ Sequential □ Autoload □ Loop
Active Slots	24

System Status

View Legend

04/04/2007 21:11:46

Library Name	FLX1006CC
Status	✓ Ready
Drive 1 Status	✓ Ready
Drive 2 Status	✓ Ready
Slots (Empty/Total)	39/45
I/O Station	Closed
Library Time	21:11:46
Power Supply Status	✓ 1 Online

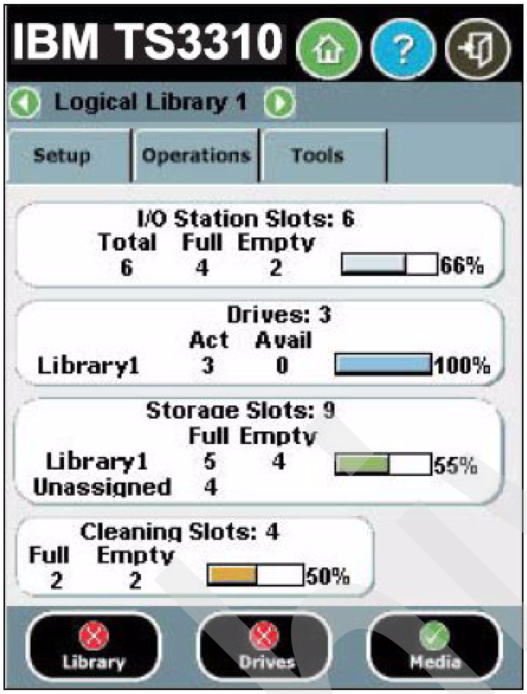
Figure 2-9 IBM TS3200 Partition details

For further description of how to configure the logical partitions, see the *IBM System Storage TS3100 Tape Library and TS3200 Tape Library Setup, Operator and Service Guide,* GA32-0545, available at:

http://www-1.ibm.com/servers/storage/tape/resource-library.html#publications

2.2.3 Setting up and configuring the IBM TS3310

Attach your library to the network. The TS3310 Operator panel is a touchscreen interface. Tap it slightly to get the login panel and login as default user admin, password secure. Remember to change this password, and define your own user ids and passwords. The main panel appears; see Figure 2-10.



I/O Station Slots: 6

Total	Full	Empty	
6	4	2	66%

Drives: 3

	Act	Avail	
Library1	3	0	100%

Storage Slots: 9

	Full	Empty	
Library1	5	4	55%
Unassigned	4		

Cleaning Slots: 4

Full	Empty	
2	2	50%

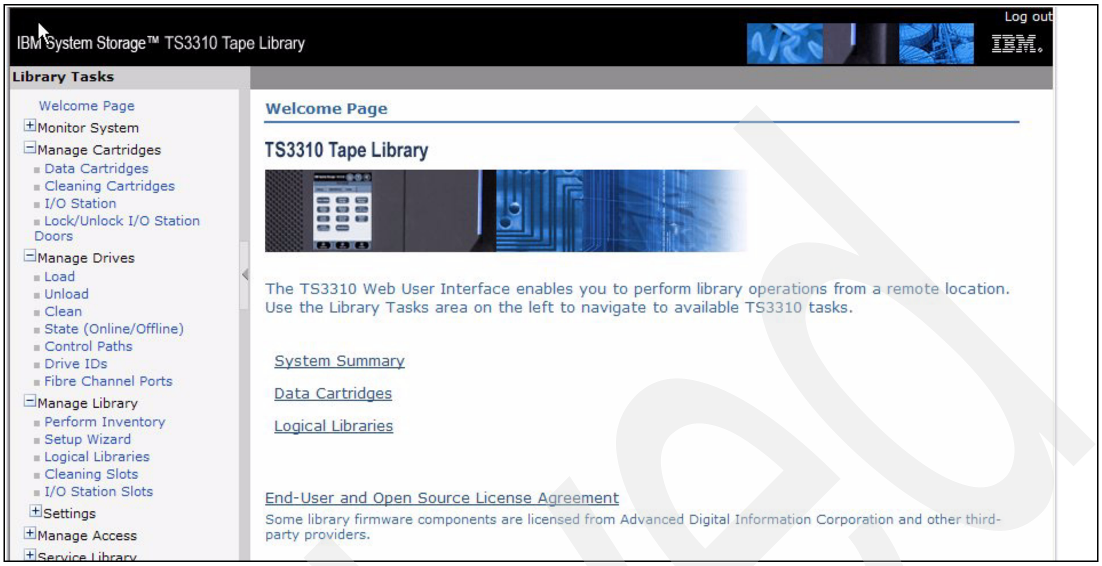
Figure 2-10 TS3310 Home Screen Capacity View

To modify the network settings, select **setup**, and **network config**. The network settings must be set through the Operator Panel.

You have to provide the data for the following fields:

- Library Name is the network name you want to assign to the library. The library name can be up to a maximum of twelve characters long.
- Dynamic Host Configuration Protocol (DHCP) setting defaults to enabled. We recommend using a fixed IP address. Set DHCP to *Disable* to make the IP Address, Subnet Mask, and Default Gateway text boxes available for you to manually set the library network settings.
- Set IP Address as the IP Address of the library, and set *Default Gateway* and *Subnet Mask*.

You are now able to access the Tape Library Specialist from a browser by entering the IP address. Figure 2-11 shows the welcome window of the IBM TS3310 Tape Library Specialist.



The TS3310 Web User Interface enables you to perform library operations from a remote location. Use the Library Tasks area on the left to navigate to available TS3310 tasks.

Some library firmware components are licensed from Advanced Digital Information Corporation and other third-party providers.

Figure 2-11 TS3310 tape Library Specialist welcome panel

The first time you use the Specialist, log in as `admin` with the password `secure`. Then you can access the Configuration menu to add any additional users that require access. Remember that every user defined can potentially access every option available on the IBM TS3310 operator panel.

In the configuration panel shown in Figure 2-10 on page 37, you can set the network configuration parameters, as well as Simple Network Management Protocol (SNMP) settings to send the alerts generated by the library to an SNMP server in your private network. The configuration panel also provides user management for the Specialist interface.

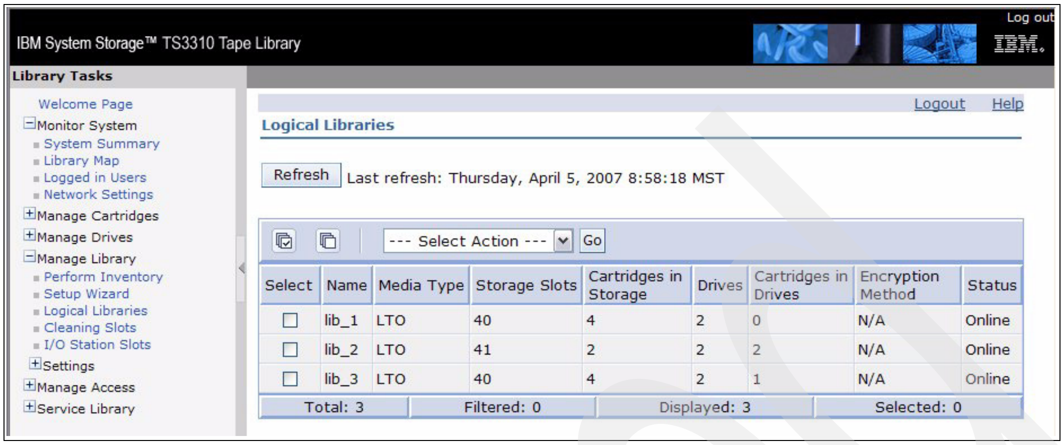
2.2.4 Partitioning the IBM TS3310

The IBM TS3310 can be partitioned into as many logical libraries as there are tape drives installed. Each partition provides its own separate and distinct drive, control path, and storage slots. The input/output (I/O) slots are shared on a first-come-first-served basis. This type of partitioning allows heterogeneous applications to share the library robotics independent of each other. Cartridges under library control are not shared between logical libraries, nor can they be moved between logical libraries.

Follow these steps:

1. Connect to the Tape Library Specialist, and login with default ID and password: *admin / secure*. Remember to change the password for security. The welcome panel displays, as already shown in Figure 2-11.

2. Select **Manage Library** → **Logical Libraries** to display the present setting of logical libraries, as shown in Figure 2-12.



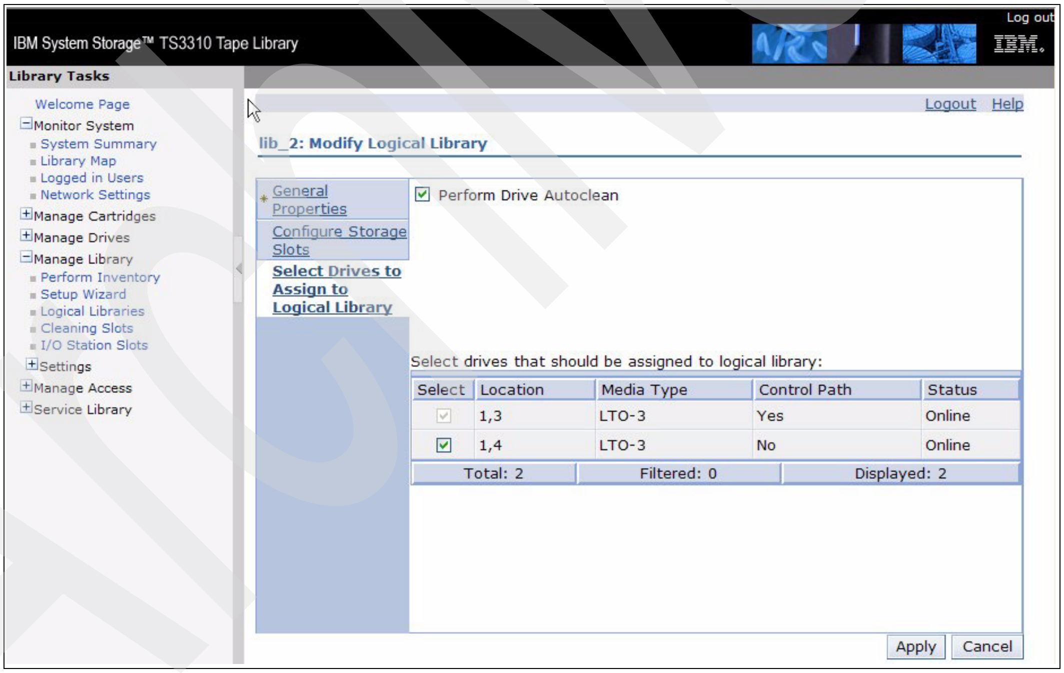
Last refresh: Thursday, April 5, 2007 8:58:18 MST

Select	Name	Media Type	Storage Slots	Cartridges in Storage	Drives	Cartridges in Drives	Encryption Method	Status
☐	lib_1	LTO	40	4	2	0	N/A	Online
☐	lib_2	LTO	41	2	2	2	N/A	Online
☐	lib_3	LTO	40	4	2	1	N/A	Online

Total: 3 Filtered: 0 Displayed: 3 Selected: 0

Figure 2-12 IBM TS3310 Logical Libraries.

3. From the drop-down menu, select **create** to add new logical libraries, or **modify** to change a defined library. Modify gives you several choices; see Figure 2-13. You can modify general properties, change storage slots, and assign tapes. Click **Apply** to activate.



lib_2: Modify Logical Library

☑ Perform Drive Autoclean

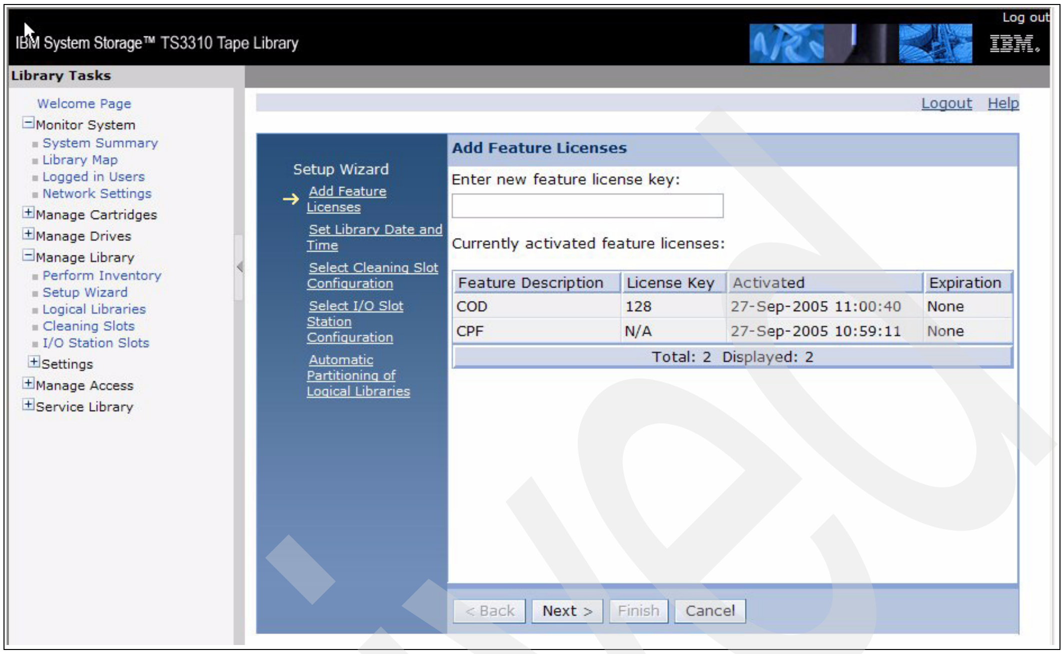
Select drives that should be assigned to logical library:

Select	Location	Media Type	Control Path	Status
☑	1,3	LTO-3	Yes	Online
☑	1,4	LTO-3	No	Online

Total: 2 Filtered: 0 Displayed: 2

Figure 2-13 Modify a logical library

4. With a new library, you can use the configuration wizard to automate some of the initial setup definitions. Select **Manage Library** → **Setup Wizard**; see Figure 2-14.



Add Feature Licenses

Enter new feature license key:

Currently activated feature licenses:

Feature Description	License Key	Activated	Expiration
COD	128	27-Sep-2005 11:00:40	None
CPF	N/A	27-Sep-2005 10:59:11	None

Total: 2 Displayed: 2

Figure 2-14 IBM TS3310 Setup Wizard

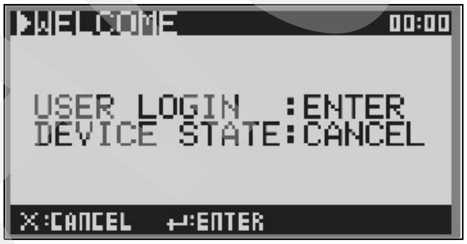
For further description of how to configure the logical partitions, see the *IBM System Storage TS3310 Tape Library Setup and Operator Guide,* GA32-0477, available at:

`http://www-1.ibm.com/servers/storage/tape/resource-library.html#publications`

2.2.5 Setting up and configuring the IBM TS3400

The IBM Tape Library Specialist is embedded in the firmware as a standard feature in the IBM TS3400. Set up the network connection using the operator panel and complete the following procedure:

1. At library power on, the login Welcome panel displays; see Figure 2-15.



USER LOGIN :ENTER
DEVICE STATE:CANCEL

Figure 2-15 IBM TS3400 Welcome panel

2. Press **enter**, and provide the default password **0000**. Remember to change this password from the Configuring Panel. This displays the Top Menu panel; see Figure 2-16.

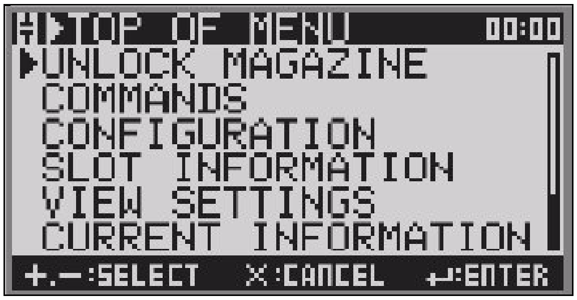
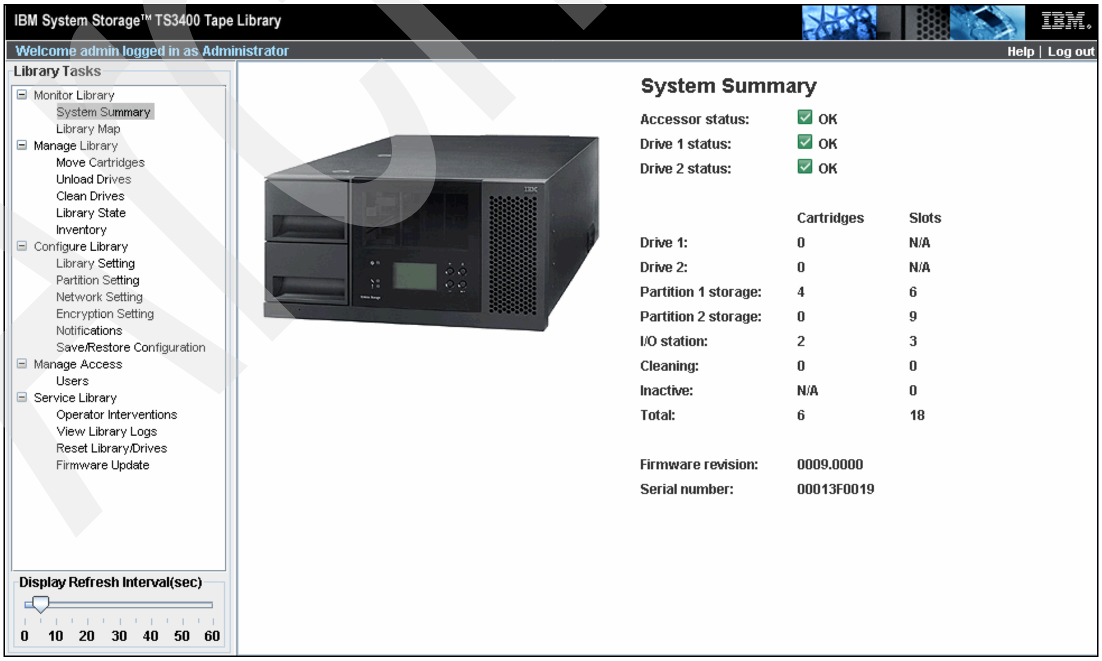


Figure 2-16 TS3400 Top Menu panel

3. To set the network settings using the Operator Panel, press **down** to select *Configuration*, and press **enter**.
4. Select *Network Settings*, and press **enter**.
5. Press **down** to select *IP Address*, and press **enter**.
6. Press **up** or **down** to select the digit(s) of your library's IP Address. Press **enter** to select each digit. After the last digit press **enter** to apply.
7. Press **down** to select *Subnet Mask*, and press **enter**. Follow the same procedure as for IP address.
8. Press **down** to select *Gateway,* and press **enter**. Follow the same procedure as for IP address.
9. Press **cancel** 3 times to return to the top menu panel.

You are now ready to log in to the Tape Library Specialist using a Web browser. You must have at least Java 1.5.0 installed on your computer. Log in using the default id Admin with password secure. Remember to change this password, and establish your own user ids and passwords. The Welcome panel displays; see Figure 2-17.



System Summary

Accessor status: ✓ OK
Drive 1 status: ✓ OK
Drive 2 status: ✓ OK

	Cartridges	Slots
Drive 1:	0	N/A
Drive 2:	0	N/A
Partition 1 storage:	4	6
Partition 2 storage:	0	9
I/O station:	2	3
Cleaning:	0	0
Inactive:	N/A	0
Total:	6	18

Firmware revision: 0009.0000
Serial number: 00013F0019

Figure 2-17 TS3400 Welcome panel - System Summary

You can now view or update the configuration, move tape cartridges, vary drives offline, and perform all other Operator panel tasks remotely from any browser window.

2.2.6 Partitioning the IBM TS3400

The IBM TS3400 can be partitioned into two logical libraries. Each logical library has its own drive, storage slots, and control paths. When Input/Output (I/O) slots are configured, they are shared on a first-come, first-served basis.

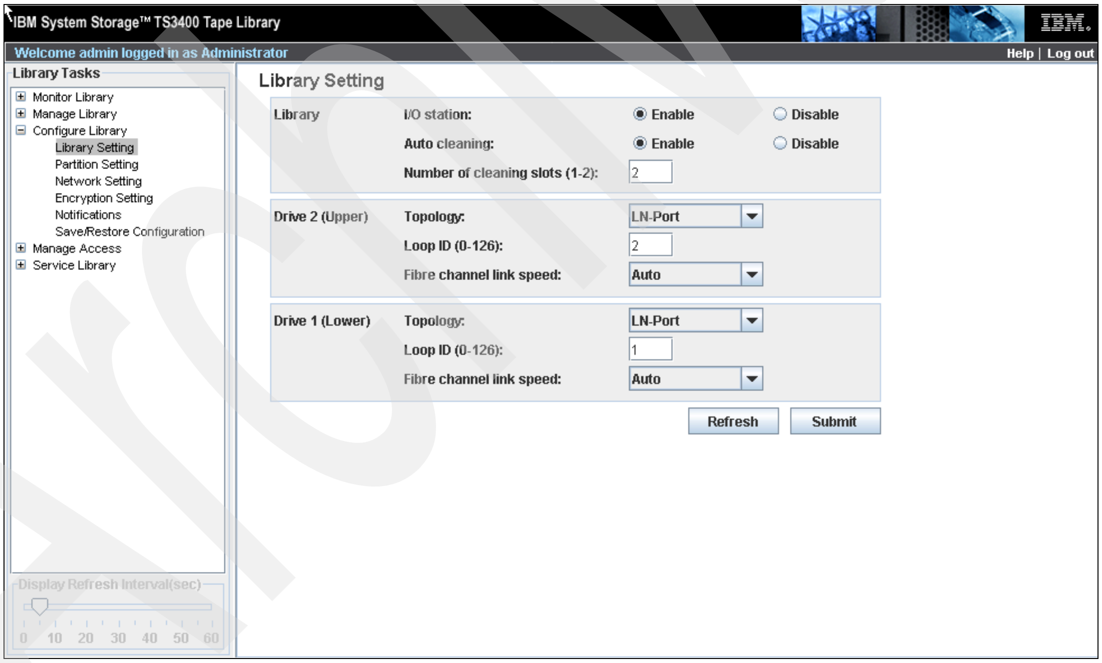
This library is using the IBM TS1120 drives, which provides built-in multipathing.

Guidelines for partitioning the IBM TS3400

We recommend that you follow these guidelines:

- The library can have one or two drives. With two drives they can either be in the same partition, or two partitions of one drive each.
- When there are two partitions, one drive uses the upper storage canister, and one drive the lower storage canister. If I/O and cleaning slots are defined, these are common for both partitions.
- If encryption is enabled, it must be enabled for both drives.

For an overview of the IBM TS3400 library settings, see Figure 2-18.



IBM System Storage™ TS3400 Tape Library

Welcome admin logged in as Administrator

Library Setting

Library
I/O station: ● Enable ○ Disable
Auto cleaning: ● Enable ○ Disable
Number of cleaning slots (1-2): 2

Drive 2 (Upper)
Topology: LN-Port
Loop ID (0-126): 2
Fibre channel link speed: Auto

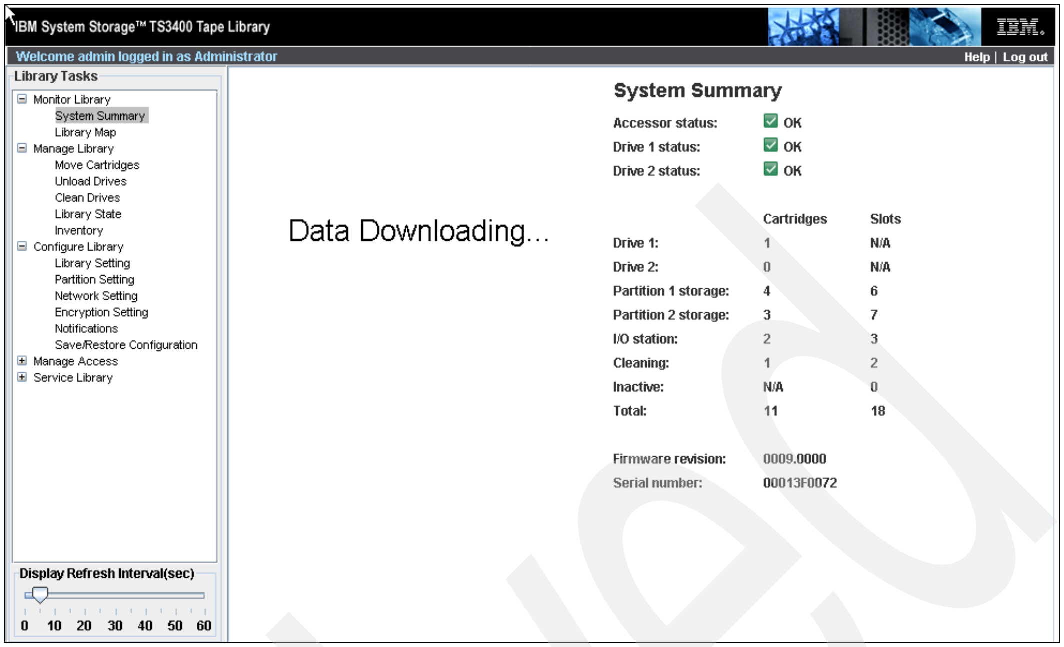
Drive 1 (Lower)
Topology: LN-Port
Loop ID (0-126): 1
Fibre channel link speed: Auto

Figure 2-18 IBM TS3400 Library Setting example

Partitioning the IBM TS3400 with the Tape Library Specialist

Partitioning is set up using the Tape Library Specialist Web interface.

1. Using the TS3400 Tape Library Specialist, you are asked to authenticate, and then see the summary panel shown in Figure 2-19.



System Summary

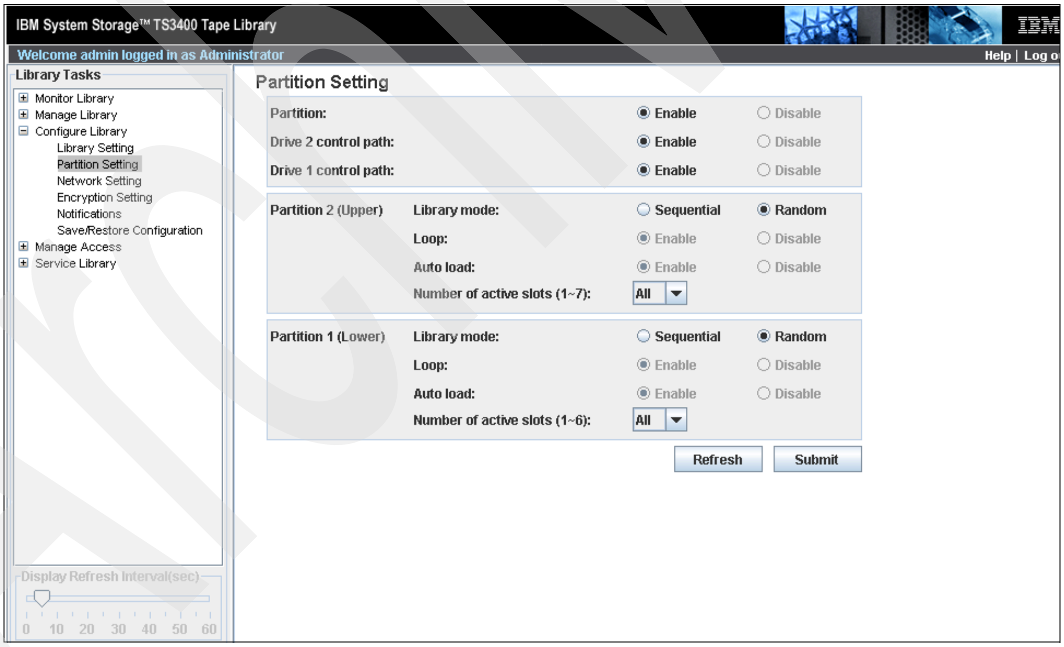
Accessor status: ☑ OK
Drive 1 status: ☑ OK
Drive 2 status: ☑ OK

	Cartridges	Slots
Drive 1:	1	N/A
Drive 2:	0	N/A
Partition 1 storage:	4	6
Partition 2 storage:	3	7
I/O station:	2	3
Cleaning:	1	2
Inactive:	N/A	0
Total:	11	18

Firmware revision: 0009.0000
Serial number: 00013F0072

Figure 2-19 IBM TS3400Tape Library Specialist Summary panel

2. Select the **Partition Setting**, and you see the map shown in Figure 2-20.



Partition Setting

Partition: ● Enable ○ Disable
Drive 2 control path: ● Enable ○ Disable
Drive 1 control path: ● Enable ○ Disable

Partition 2 (Upper)
Library mode: ○ Sequential ● Random
Loop: ● Enable ○ Disable
Auto load: ● Enable ○ Disable
Number of active slots (1~7): All

Partition 1 (Lower)
Library mode: ○ Sequential ● Random
Loop: ● Enable ○ Disable
Auto load: ● Enable ○ Disable
Number of active slots (1~6): All

Figure 2-20 IBM TS3400 Partition Setting example

3. To enable partitions, you require at least one tape drive and control path enabled for each partition.The panel indicates that both drives are enabled as a control path.

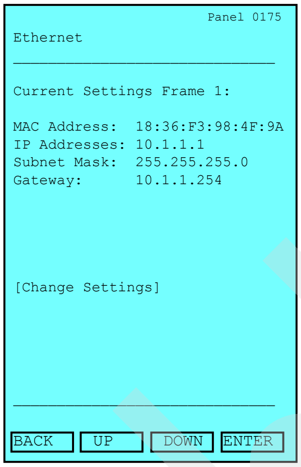
For more details about configuring partitions, see The *IBM System Storage TS3400 Tape Library Planning and Operator Guide*, GC27-2107, and:

http://www-03.ibm.com/systems/storage/tape/ts3400/index.html

2.2.7 Setting up and configuring the IBM TS3500 Tape Library

The IBM TS3500 Tape Library Specialist is embedded in the library firmware. Attach the Ethernet port to your network and configure the TCP/IP address information from the library Operator Panel:

1. Choose **Settings** → **Network** → **Ethernet.** You see the current interface MAC address (which cannot be changed), and the assigned TCP/IP address, subnet mask, and gateway. If the library has more than one frame, and you want to use several connections, then each frame requires a separate address. Use the **Up** and **Down** buttons to access the panels for the additional frames. The current configuration window is shown in Figure 2-21.

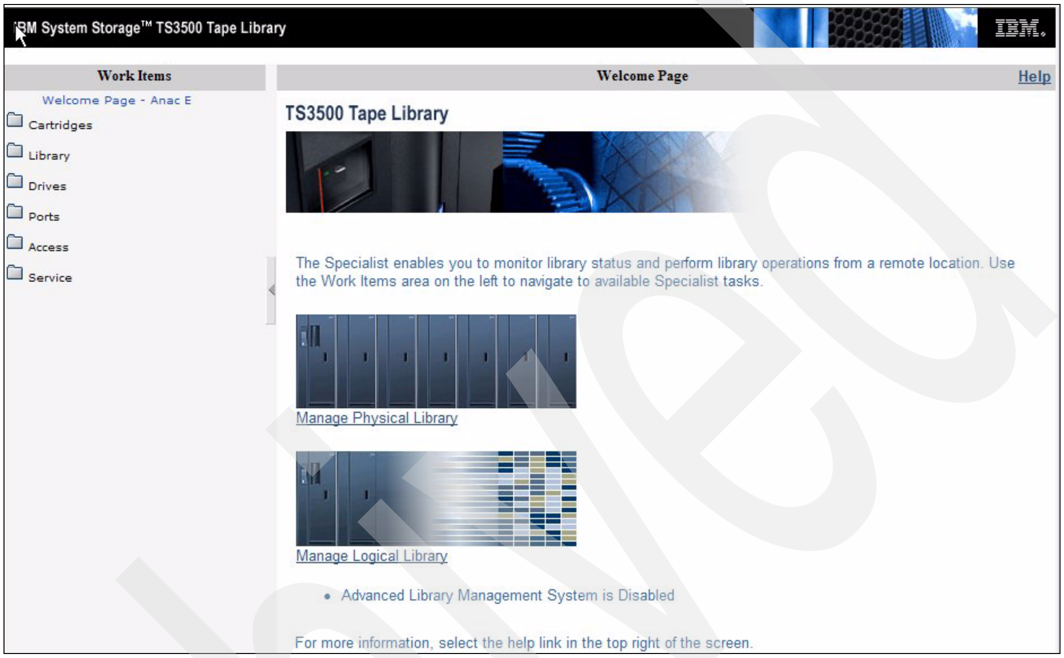


```
                              Panel 0175
Ethernet
______________________________

Current Settings Frame 1:

MAC Address:  18:36:F3:98:4F:9A
IP Addresses: 10.1.1.1
Subnet Mask:  255.255.255.0
Gateway:      10.1.1.254



[Change Settings]
```

Figure 2-21 Change Ethernet parameters on IBM TS3500

2. Click **Enter** to make the changes. You can select to disable the Ethernet interface, use DHCP to automatically assign an address (if supported in your network), or manually configure the parameters. We recommend that you define a fixed IP address.

3. After configuring the network connection for the IBM Tape Library Specialist, enter the TCP/IP address of the library in your browser. The welcome page of the IBM TS3500 Tape Library Specialist Web interface displays, as shown in Figure 2-22. With the Specialist, you can monitor library status and perform library operations from a remote location. Use the Work Items area on the left to navigate to available Specialist tasks. For more information, click the **Help** button in the top right of the panel.



The Specialist enables you to monitor library status and perform library operations from a remote location. Use the Work Items area on the left to navigate to available Specialist tasks.

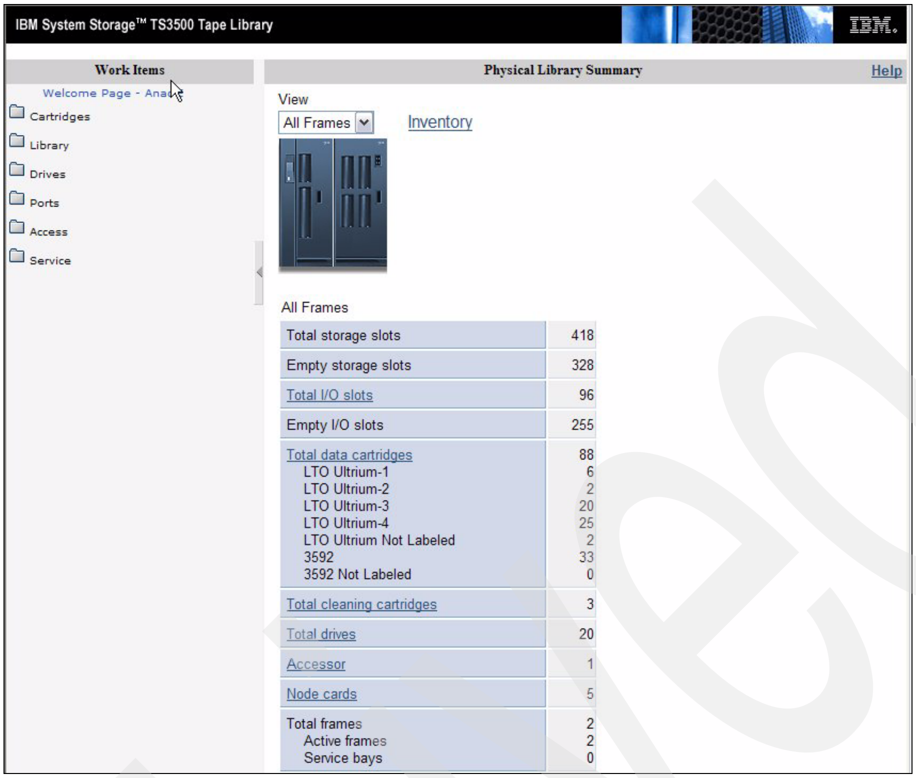
- Advanced Library Management System is Disabled

For more information, select the help link in the top right of the screen.

Figure 2-22 IBM TS3500 Tape Library Specialist: Welcome page

4. You now have complete operational control of the TS3500 Tape Library. The library might have implemented the Advanced Library Management Services, ALMS. For more information about ALMS, see 2.3, “Partitioning the TS3500 with ALMS enabled” on page 60.

   With the IBM TS3500 Tape Library Specialist, you can easily configure and monitor the library operations with graphics and tables like those shown in Figure 2-23.



All Frames

Total storage slots	418
Empty storage slots	328
Total I/O slots	96
Empty I/O slots	255
Total data cartridges	88
LTO Ultrium-1	6
LTO Ultrium-2	2
LTO Ultrium-3	20
LTO Ultrium-4	25
LTO Ultrium Not Labeled	2
3592	33
3592 Not Labeled	0
Total cleaning cartridges	3
Total drives	20
Accessor	1
Node cards	5
Total frames	2
Active frames	2
Service bays	0

Figure 2-23 IBM TS3500 Physical Library summary panel

The IBM TS3500 Tape Library Specialist has menus to manage the cartridges, drives, and library. The available menus vary depending upon whether ALMS is installed or not. For further examples, see the specific chapters for partitioning with or without ALMS. In the following discussion, all examples assumes that ALMS is installed and active.

For an example with ALMS, to view a list of the cartridges in the library, select **Cartridges** → **Data Cartridges**. Using the drop-down boxes, you can filter the cartridges displayed by frame or logical library. Figure 2-54 on page 71 lists the cartridges for all logical libraries. After selecting a cartridge, you can move it to a tape drive, remove it from the library, or assign it to a logical library.

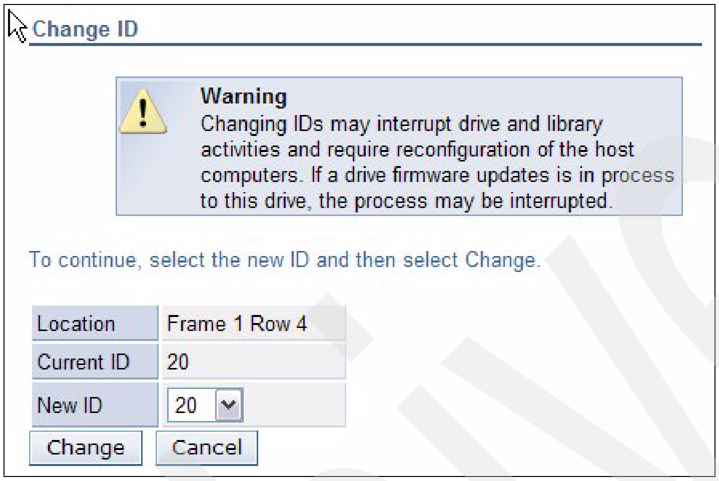
For information about Cartridge Assignment Policy, see “Cartridge assignment policy” on page 69.

To view a list of the drives in the library, select **Drives** → **Drive Summary.** On the **Drives** panel, you can use the drop-down boxes to limit the drives selected to a specific frame or a specific logical library, or you can select all frames or all logical libraries. In Figure 2-59 on page 75, you see for example logical library Redbook1 with LTO4 tape drives.

From the drop-down menu, after selecting a tape drive, you can clean it, change its SCSI ID (or Loop ID if FC), view drive details, move a cartridge, or do a power cycle of a drive. This last feature can be especially useful when sharing drives in a SAN (for example, LAN-free backup). In this circumstance, when a server is using a drive, it issues a SCSI `reserve` command, which blocks it from other servers. The drive is unavailable to other jobs until the server with the `reserve` sends a `release` command to the tape drive.

> **Note:** If the server which holds a SCSI `reserve` on a tape drive cannot `release` it, for example, because it is powered down, a power cycle of the tape drive is required to release the reservation and make the drive available for use with other servers.

To change a drive's settings, select that drive from the Drives panel and click **Change ID**. You get a warning (Figure 2-24) stating that this function might interrupt the library activity. Indeed, changing the Drive SCSI/Loop ID interrupts library and drive activities and might require reconfiguring the host computers.



Change ID

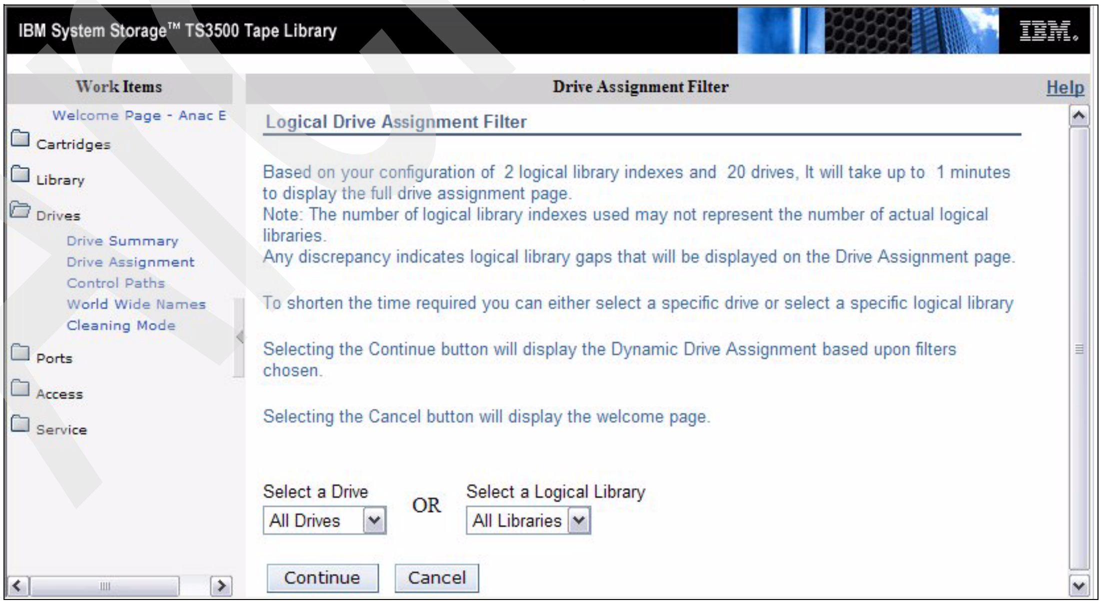
Warning
Changing IDs may interrupt drive and library activities and require reconfiguration of the host computers. If a drive firmware updates is in process to this drive, the process may be interrupted.

To continue, select the new ID and then select Change.

Location	Frame 1 Row 4
Current ID	20
New ID	20

Figure 2-24 IBM TS3500 Tape Library Specialist: ID change warning

Select **Drives** → **Drive Assignment** to display the Drive Assignment Filter panel, which is used for displaying the assignment of the drives to their logical libraries. You can select all drives or a specific drive, and all logical libraries or a specific logical library. In Figure 2-25, all drives are selected for display.



Logical Drive Assignment Filter

Based on your configuration of 2 logical library indexes and 20 drives, It will take up to 1 minutes to display the full drive assignment page.
Note: The number of logical library indexes used may not represent the number of actual logical libraries.
Any discrepancy indicates logical library gaps that will be displayed on the Drive Assignment page.

To shorten the time required you can either select a specific drive or select a specific logical library

Selecting the Continue button will display the Dynamic Drive Assignment based upon filters chosen.

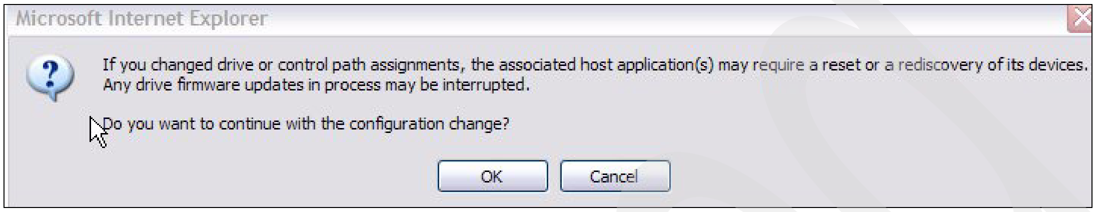
Selecting the Cancel button will display the welcome page.

Select a Drive: All Drives OR Select a Logical Library: All Libraries

Figure 2-25 IBM TS3500 Tape Library Specialist: Drive Assignment Filter

As shown in Figure 2-57 on page 73, after selecting a tape drive, you can unassign the drive or assign the drive as a control path. To assign a drive as a control path, click the block to the left of the check box for the drive and click the **Apply** button above the Drives column. In Figure 2-57 on page 73, drive 30010E611 is a control path, as is indicated by the icon shown on the left of the check box in the **Tucson** column.

Adding a control path, you see a warning (Figure 2-26) that changing a drive or control path assignment might affect the associated host applications, and that a reset or rediscovery of its devices might be required.



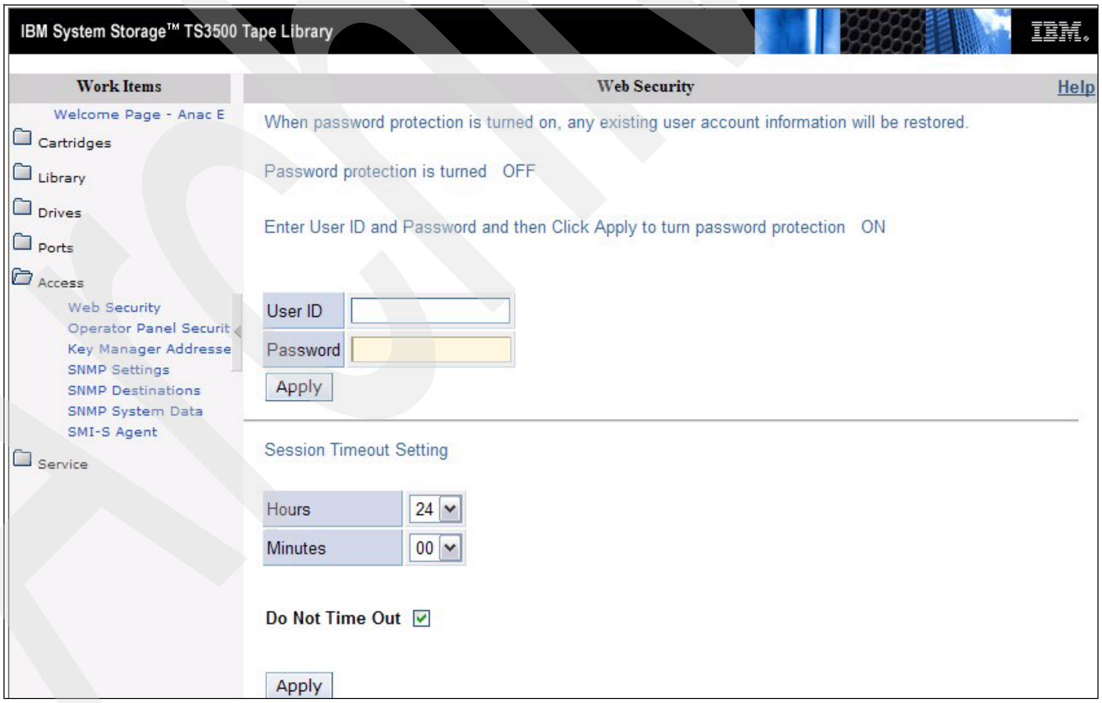
If you changed drive or control path assignments, the associated host application(s) may require a reset or a rediscovery of its devices. Any drive firmware updates in process may be interrupted.

Do you want to continue with the configuration change?

Figure 2-26 IBM TS3500 Tape Library Specialist: Assignment change warning

You can make any configuration of the library directly from the Tape Library Specialist panels. Note, however, that the initial TCP/IP configuration function is not available from the IBM Tape Library Specialist. This must be done from the Operator Panel.

You should always set password protection on to assure secure access to the library. To turn it on, select **Access** → **Web Security**; see Figure 2-27. Once password security is set on, use the same selection to control users and passwords.



When password protection is turned on, any existing user account information will be restored.

Password protection is turned OFF

Enter User ID and Password and then Click Apply to turn password protection ON

User ID

Password

Session Timeout Setting

Hours 24

Minutes 00

Do Not Time Out ☑

Figure 2-27 Set Password panel

For firmware update of the IBM TS3500 Tape Library, see Appendix C, “Firmware upgrades” on page 307.

2.2.8 Planning and partitioning the IBM TS3500 (ALMS not enabled)

You can partition the IBM TS3500 into multiple logical libraries. Each logical library requires at least one tape drive and one storage slot. Therefore, you can theoretically configure as many logical libraries as there are tape drives installed in the library, for example, the IBM TS3500 supports up to 192 logical libraries. LTO2, 3 and 4 drive types can be mixed in a logical library if the backup application supports it, but LTO and IBM 3592 tape drives cannot be mixed within a logical library, and they must be installed in different frames.

Note: If using mixed media and drives (LTO and 3592) within one TS3500, then at least two logical libraries (one for LTO and one for 3592) must be created.

Storage slots within one logical library must be in contiguous order, but can span over different frames. Also, tape drives within one logical library must be in contiguous order, but can be in different frames, and can contain gaps in the order (such as having two drives installed in frame 1 and two drives in frame 2; then you have a gap of 10 drives).

However, although the TS3500 allows you to have gaps in the tape drive order, some applications like EMC Legato NetWorker or VERITAS NetBackup do not support such gaps.

Note: For i5/OS gaps in the data transfer element address do not matter so there is no requirement for assignment of drives from consecutive locations to a logical library.

When using the ALMS feature, the tape drives are always defined as consecutive. For details about ALMS, see 2.3, “Partitioning the TS3500 with ALMS enabled” on page 60.

Plan your logical library configuration carefully, because the requirement for contiguous storage slots and drives makes future changes to the configuration very difficult. For instance, if you have an TS3500 with six logical libraries defined, and you have to change the configuration of the first library, then all of the five remaining libraries must be changed as well. Consequently, plan your logical library configuration according to these rules:

- Put the logical library that has the most expected growth at the end of the library.
- Put the logical library that is the least likely to grow in the front.
- Do not configure logical libraries with just the required minimum of resources (tape drives and storage slots); instead configure logical libraries with a buffer (reserve) of storage slots.
- Do not put the first drive of a logical library just behind the last drive of the preceding logical library. Keep some free drive locations between two logical libraries in order to install additional drives if required.

Figure 2-28 shows an example. This is an L53 frame with nine LTO drives installed, and with a capacity of 261 storage slots. Three logical libraries are required: logical library 1 requires 40 slots and two drives; logical library 2 requires 60 slots and two drives; logical library 3 requires 120 slots and five drives. The third library is expected to grow heavily.

The first logical library was configured with 60 slots and two tape drives.

The second logical library was configured with 81 slots and two tape drives. The first tape drive for logical library 2 was installed in the fourth drive location; this gives the possibility to install one additional drive in the first logical library if required.

The library with the highest expected growth was put at the end. If required, an additional D-frame can be added to the library, and logical library 3 can be expanded to the next frame without changing the configuration of the first two libraries (Figure 2-28).

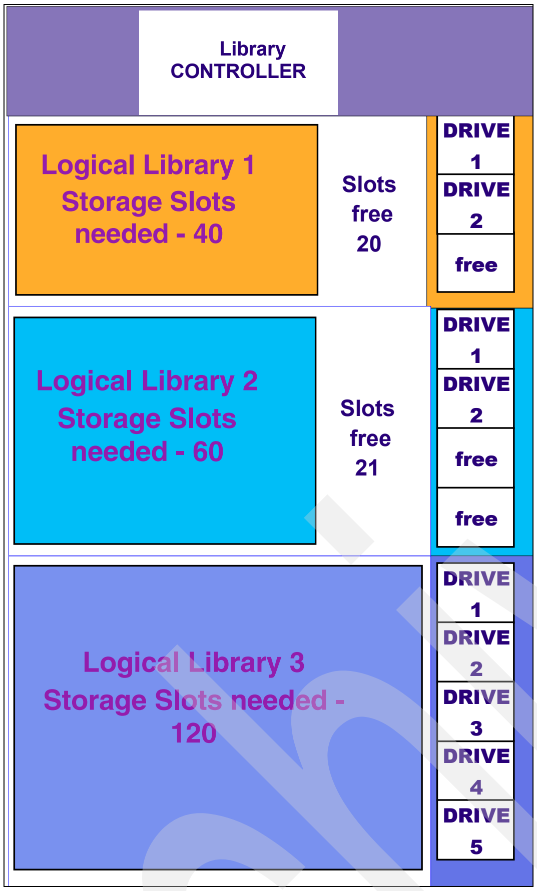


Figure 2-28 IBM TS3500 partitioning example

You can partition the TS3500 into multiple logical libraries by using menus. You can choose the exact number of storage elements that you want by selecting them from the library operator panel display **Advanced Configuration** menu selection, or using the **Tape Library Specialist** menu.

In both cases, the library is set offline while configuring. For further details about setting up partitions using the Operator Panel, see the *IBM System Storage TS3500 Tape Library Operator Guide*, GA32-0560.

2.2.9 Partitioning the TS3500 using the wizard (ALMS not enabled)

First, plan the number and location of storage slot columns and tape drives that you want in each logical library. Now, the logical libraries can be configured from the Tape Library Specialist using the configuration wizard or the menu system.

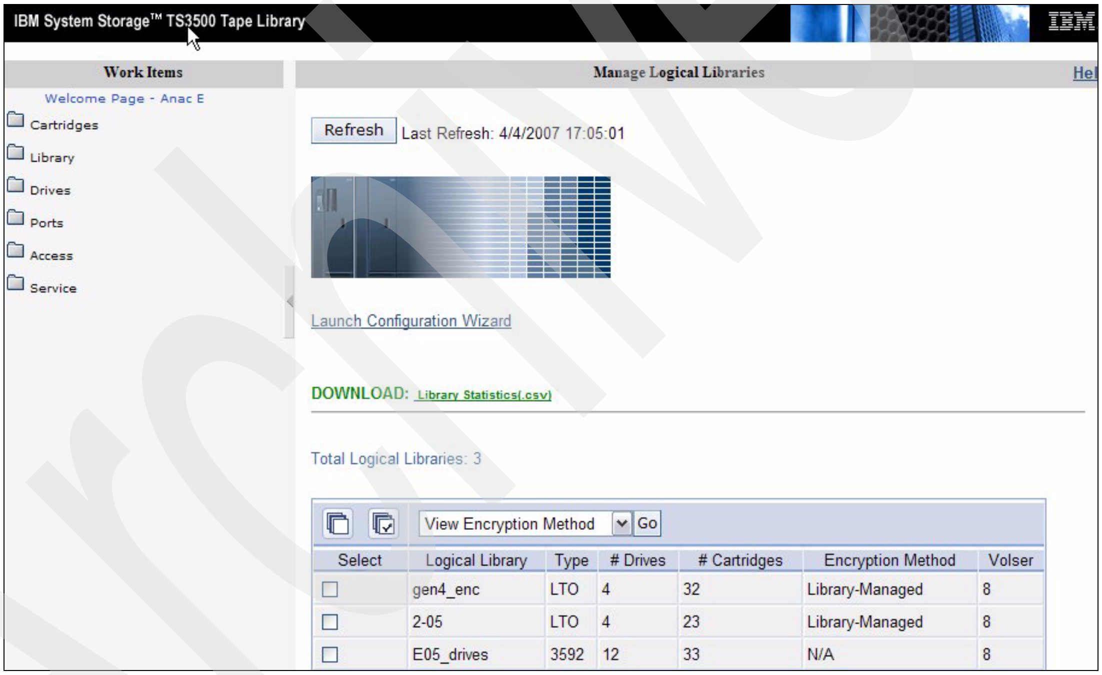
Using the Tape Library Specialist

In this example, we have a 2-frame library with one LTO frame and one 3592 frame. There are eight LTO4 drives, and twelve 3592 drives already installed. It is defined as three logical libraries, but we reconfigure the logical libraries using the configuration wizard, to achieve this configuration:

- Logical library ‘Redbook1’, 4 LTO drives, 100 cartridge slots
- Logical library ‘Mt Lemon’, 4 LTO drives, 119 cartridge slots
- Logical library ‘Tucson’, 8 3592 drives, 120 cartridge slots
- Logical library ‘Tombstone’, 4 3592 drives, 79 cartridge slots.

To use the TS3500 Tape Library Specialist Web interface, do the following steps:

1. Enter the library’s IP address as a Web site in your browser window; the introduction window displays (see Figure 2-22 on page 45). If login security is enabled, there is a login prompt first.
2. Click **Manage Logical Library** on the main pane, or select **Library** and **Logical Libraries** on the left side. The Manage Logical Libraries window displays; see Figure 2-29.



Last Refresh: 4/4/2007 17:05:01

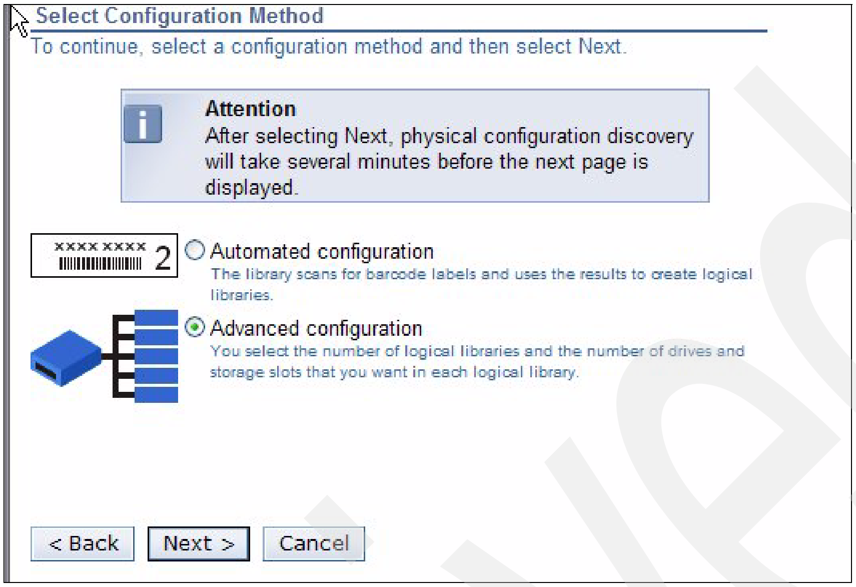
Total Logical Libraries: 3

Select	Logical Library	Type	# Drives	# Cartridges	Encryption Method	Volser
□	gen4_enc	LTO	4	32	Library-Managed	8
□	2-05	LTO	4	23	Library-Managed	8
□	E05_drives	3592	12	33	N/A	8

Figure 2-29 IBM TS3500 Tape Library Specialist Logical Libraries entry panel

3. This shows the library’s current configuration. Select the **Launch Configuration Wizard**. A warning window informs you that the library goes offline and that it might take up to 30 minutes to complete, depending on the library configuration (a small library with just one or two frames and a few drives can take less than a minute). Click **Next** to continue.

4. The **Select Configuration Method** window displays (Figure 2-30), showing the alternatives: **Automated configuration** (configuration with barcode labels) or **Advanced configuration**. Select **Advanced configuration** and click **Next.**



Select Configuration Method

To continue, select a configuration method and then select Next.

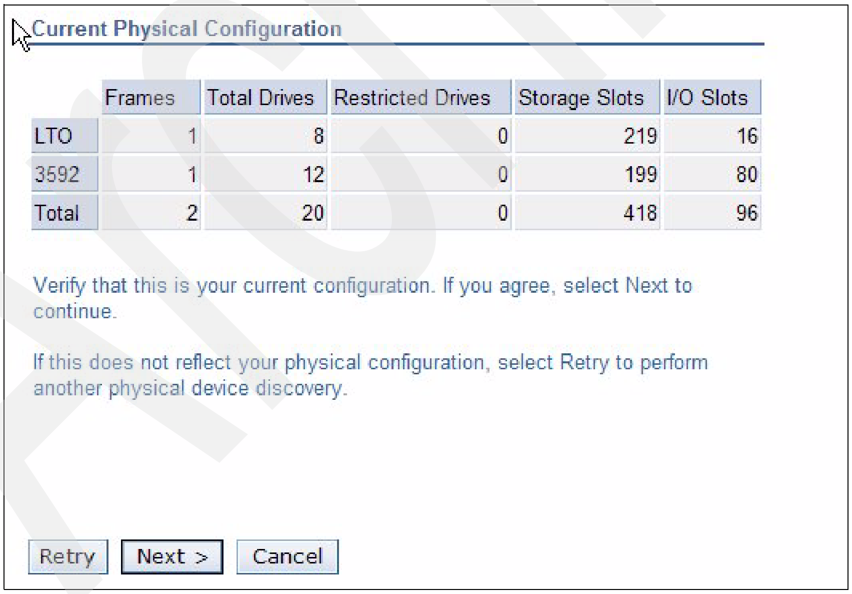
Attention
After selecting Next, physical configuration discovery will take several minutes before the next page is displayed.

○ Automated configuration
The library scans for barcode labels and uses the results to create logical libraries.

● Advanced configuration
You select the number of logical libraries and the number of drives and storage slots that you want in each logical library.

Figure 2-30 IBM TS3500 Tape Library Specialist configuration wizard

5. The library starts its configuration discovery, which can take several minutes. The current configuration is displayed. Check that the displayed configuration matches the real configuration (Figure 2-31). If not, then stop here and try the configuration discovery again. If the problem is still not solved, call your service representative.



Current Physical Configuration

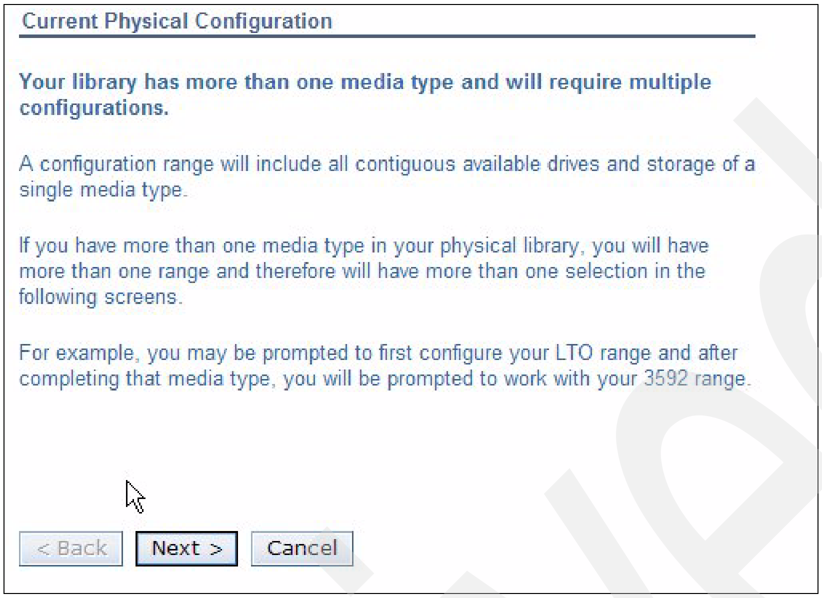
	Frames	Total Drives	Restricted Drives	Storage Slots	I/O Slots
LTO	1	8	0	219	16
3592	1	12	0	199	80
Total	2	20	0	418	96

Verify that this is your current configuration. If you agree, select Next to continue.

If this does not reflect your physical configuration, select Retry to perform another physical device discovery.

Figure 2-31 Current physical configuration

6. Click **Next**. As this is a mixed device library, you get a warning about this, and that multiple configurations are necessary; see Figure 2-32.



Current Physical Configuration

Your library has more than one media type and will require multiple configurations.

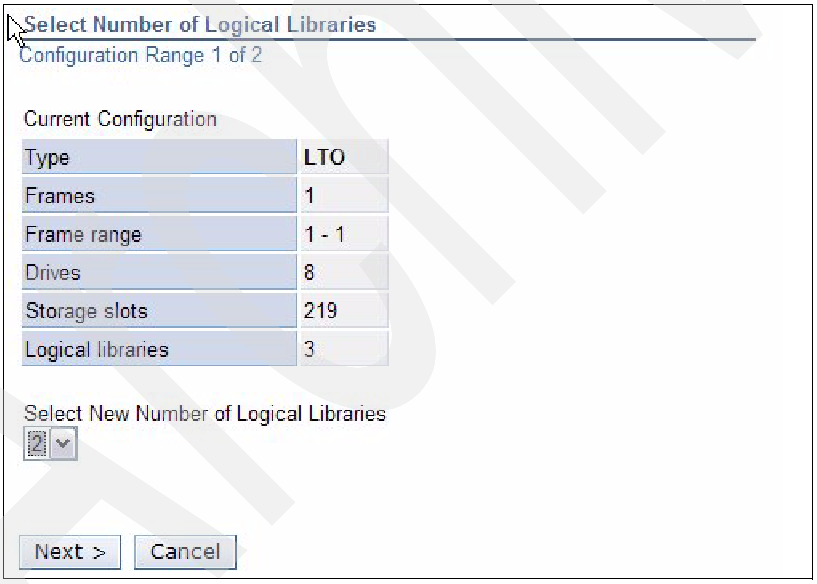
A configuration range will include all contiguous available drives and storage of a single media type.

If you have more than one media type in your physical library, you will have more than one range and therefore will have more than one selection in the following screens.

For example, you may be prompted to first configure your LTO range and after completing that media type, you will be prompted to work with your 3592 range.

Figure 2-32 Multiple configurations warning.

7. **Click Next.** The number of logical partitions can now be selected (Figure 2-33).



Select Number of Logical Libraries

Configuration Range 1 of 2

Current Configuration

Type	LTO
Frames	1
Frame range	1 - 1
Drives	8
Storage slots	219
Logical libraries	3

Select New Number of Logical Libraries

2

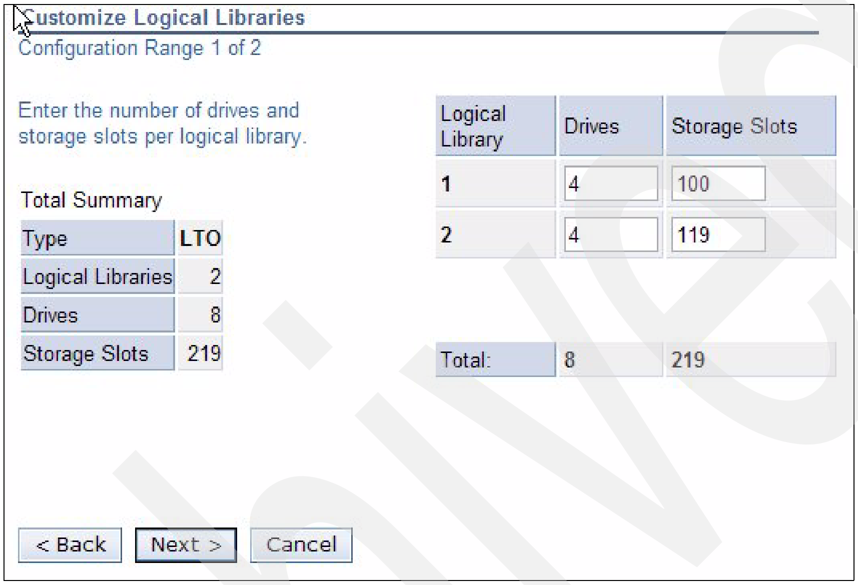
Figure 2-33 IBM TS3500 Tape Library Specialist Logical Libraries

8. Select the number of logical libraries for the displayed media type from the pull-down list. Click **Next**. The desired number of drives and slots can now be assigned to each logical library (Figure 2-34). Begin with the first logical library and use the Tab key to jump from one field to the other. Every time you press the Tab key, the remaining number of drives and storage slots is re-calculated.

Note: All resources (tape drives and cartridge slots) must be assigned!

If you have both LTO and 3592 in the physical library, there are more than one configuration range, and more than one set of selection and configuration details in the panels. That means you can first configure a range of LTO elements, and then a range of 3592 elements.

In the panel shown in Figure 2-34, click **Next** when finished.



Customize Logical Libraries

Configuration Range 1 of 2

Enter the number of drives and storage slots per logical library.

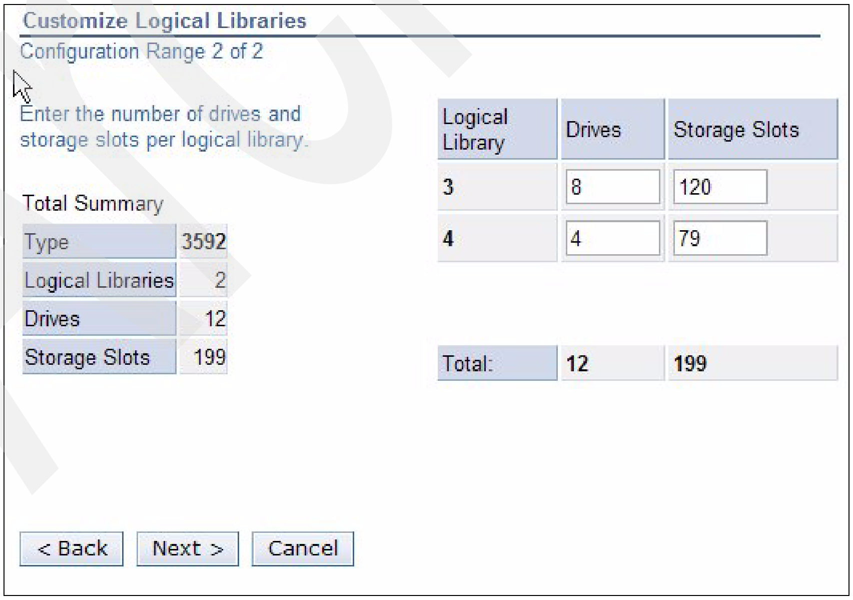
Total Summary

Type	LTO
Logical Libraries	2
Drives	8
Storage Slots	219

Logical Library	Drives	Storage Slots
1	4	100
2	4	119
Total:	8	219

Figure 2-34 IBM TS3500 Tape Library Specialist customize drives and slots - LTO

9. In the same way, select and customize the 3592 libraries as shown in Figure 2-35.



Customize Logical Libraries

Configuration Range 2 of 2

Enter the number of drives and storage slots per logical library.

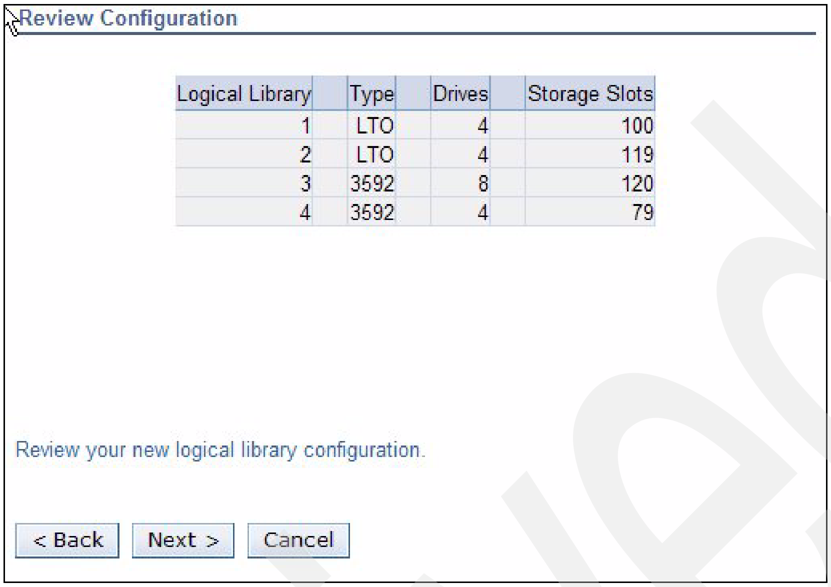
Total Summary

Type	3592
Logical Libraries	2
Drives	12
Storage Slots	199

Logical Library	Drives	Storage Slots
3	8	120
4	4	79
Total:	12	199

Figure 2-35 Customize drives and slots - 3592

10. A new window shows the selections. The configuration can now be reviewed before being applied; see Figure 2-36.



Review Configuration

Logical Library	Type	Drives	Storage Slots
1	LTO	4	100
2	LTO	4	119
3	3592	8	120
4	3592	4	79

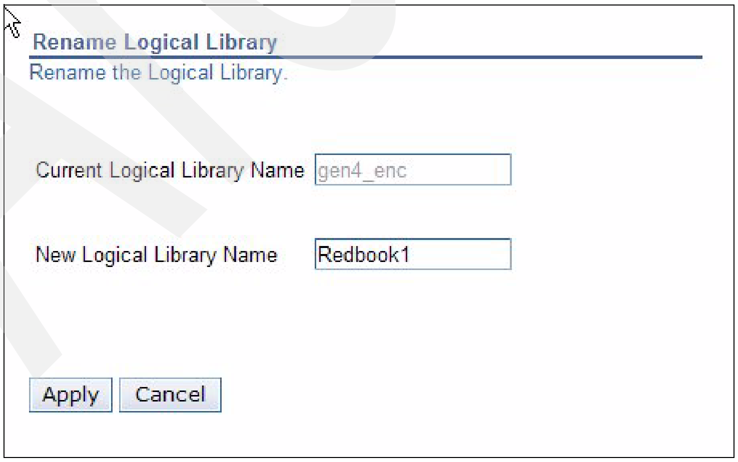
Review your new logical library configuration.

Figure 2-36 Review configuration

11. Click **Next** to accept the configuration, and then click **Finish** to apply the new configuration, which takes some minutes. After completion, the library informs you with a `Library configuration successful` message.

12. After setting a new configuration, the new logical libraries are simply named using numbers. You can change this to more meaningful names: From the Manage Logical Libraries panel (Figure 2-29 on page 51), select the library to be renamed and click **rename**. On the next panel (Figure 2-37) enter a new logical library name.

> **Note:** The logical library name is only used by the Library Specialist, and has no effect on the communication with your backup application.



Rename Logical Library

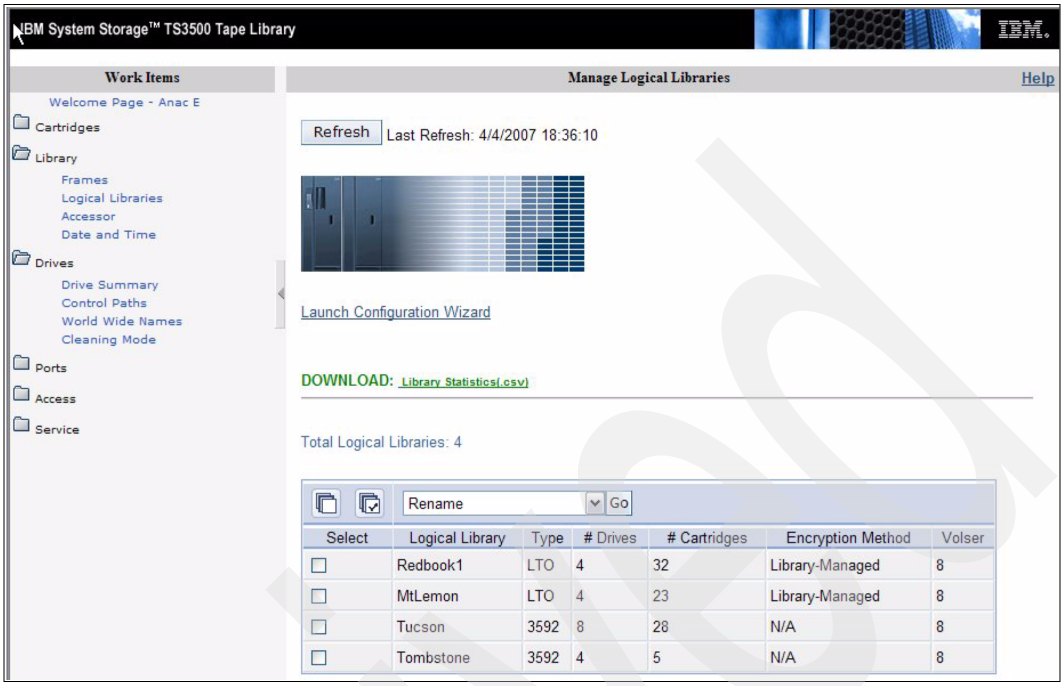
Rename the Logical Library.

Current Logical Library Name: gen4_enc

New Logical Library Name: Redbook1

Figure 2-37 Rename logical library

13.When all logical libraries are renamed, we have our library layout; see Figure 2-38.



Last Refresh: 4/4/2007 18:36:10

DOWNLOAD: Library Statistics(.csv)

Total Logical Libraries: 4

Select	Logical Library	Type	# Drives	# Cartridges	Encryption Method	Volser
□	Redbook1	LTO	4	32	Library-Managed	8
□	MtLemon	LTO	4	23	Library-Managed	8
□	Tucson	3592	8	28	N/A	8
□	Tombstone	3592	4	5	N/A	8

Figure 2-38 IBM TS3500 Logical Library status

Before we can work again with the library, we have to adjust the logical library configuration with the backup application that uses this library. If the storage slot capacity on the logical library is increased or decreased, the backup application must reflect this change.

Note: For i5/OS, a change to the logical library configuration, such as an increase or decrease of the storage slot, requires an IOP reset to make it aware of the new number of available storage slots.

For other platforms, refer to your backup application manuals for information about how to change an existing library configuration. Some applications such as IBM Tivoli Storage Manager handle this easily; other applications such as Legato NetWorker require that you run configuration wizards (NetWorker's `jbconfig`) in order to reflect the changes.

Also, cartridges that belong to the logical library must be moved to the appropriate set of storage cells.

2.2.10 Partitioning the TS3500 using the operator panel (ALMS not enabled)

The following steps show the procedure to partition the TS3500 Tape Library using its operator panel.

(For further details using the operator panel, refer to the *IBM System Storage TS3500 Tape Library Operator Guide*, GA32-0560.)

Follow these steps:

1. From the library's operator panel Activity window, click **Menu**. The Main Menu displays as shown in Figure 2-39.

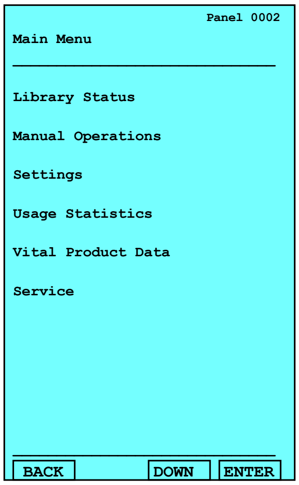


Figure 2-39 IBM TS3500 operator panel: Main Menu

2. Click **UP** or **DOWN** to highlight *Settings*, then click **ENTER**. The Settings menu displays.
3. Click **UP** or **DOWN** to highlight *Configuration* and click **ENTER**. The Configuration menu displays.
4. Click **UP** or **DOWN** to highlight *Advanced configuration* and click **ENTER** (Figure 2-40). The library displays the message: `If you continue with configuration the library will go offline.` Click **ENTER** to continue.

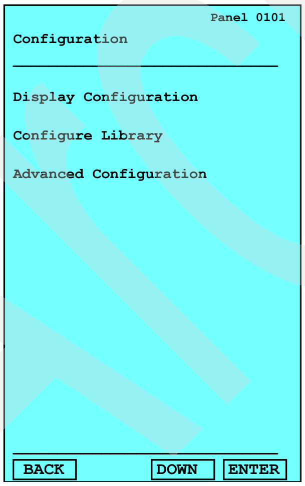
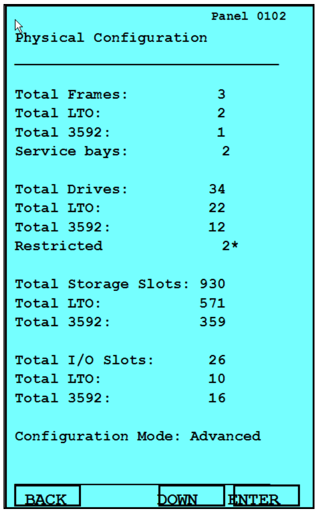


Figure 2-40 IBM TS3500 operator panel: Configuration

5. Click **ENTER** twice. The library displays the message: `Searching for installed devices` and might take several minutes to discover the physical configuration. The Physical Configuration panel displays, identifying the library's existing physical configuration (Figure 2-41). The panel shows the total quantity of drives, storage slots, and I/O slots in the library's physical configuration. If the configuration includes both LTO and 3592 drives, the list shows them separately.

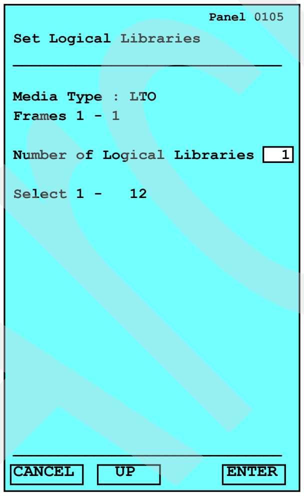
Check that the displayed configuration matches the real configuration. If not, stop here, resolve the problem, and start again.



```
                       Panel 0102
Physical Configuration
______________________________

Total Frames:           3
Total LTO:              2
Total 3592:             1
Service bays:            2

Total Drives:          34
Total LTO:             22
Total 3592:            12
Restricted              2*

Total Storage Slots: 930
Total LTO:           571
Total 3592:          359

Total I/O Slots:      26
Total LTO:            10
Total 3592:           16

Configuration Mode: Advanced
```

Figure 2-41 IBM TS3500 Configuration display

6. Click **ENTER**. The library displays the message: `Do you want to commit the new physical configuration?`
7. Click **Yes** to accept the new physical configuration and to set up any logical library configurations. The Set Logical Libraries panel displays, indicating the type of media used by the logical library (Figure 2-42). The following panels do not display if the ALMS feature has been enabled.

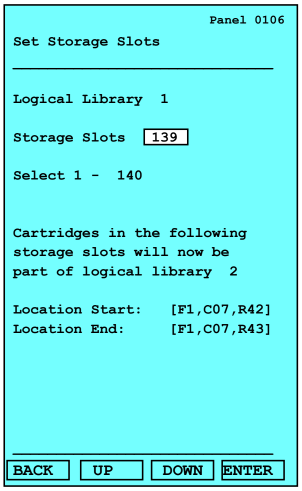


```
                        Panel 0105
Set Logical Libraries
______________________________

Media Type : LTO
Frames 1 - 1

Number of Logical Libraries  1

Select 1 -   12
```

Figure 2-42 IBM TS3500 operator panel: Set Logical Libraries

8. Specify the number of logical libraries that you want for the displayed media type by clicking **UP** or **DOWN** to increase or decrease the value.

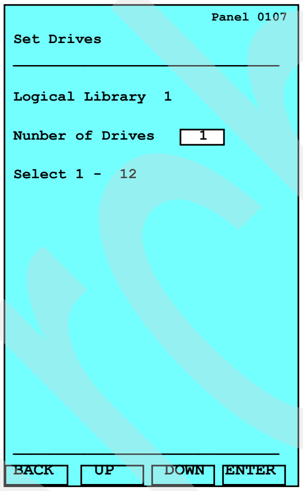
9. When the desired quantity of libraries displays, click **ENTER**. The Set Storage Slots panel displays (Figure 2-43).



```
                                Panel 0106
Set Storage Slots

Logical Library  1

Storage Slots  139

Select 1 -  140


Cartridges in the following
storage slots will now be
part of logical library  2

Location Start:    [F1,C07,R42]
Location End:      [F1,C07,R43]
```

Figure 2-43 IBM TS3500 operator panel: Set Storage Slots

10. Specify the quantity of storage slots that you want in the logical library by clicking **UP** or **DOWN** to increment or decrement the value. When the desired quantity of storage slots displays, click **ENTER**. The Set Drives panel displays (Figure 2-44).

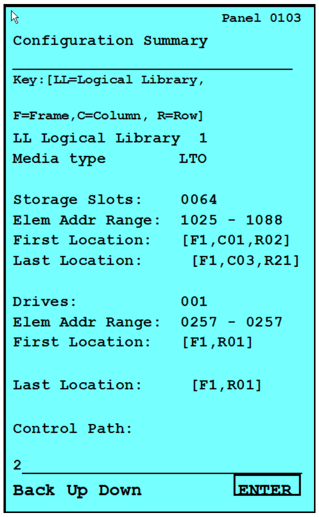


```
                                Panel 0107
Set Drives

Logical Library  1

Nunber of Drives     1

Select 1 -  12
```

Figure 2-44 IBM TS3500 operator panel: Set Drives

11. Specify the quantity of drives that you want in the logical library by clicking **UP** or **DOWN** to increment or decrement the value. When the desired quantity of drives displays, click **ENTER**.

12. The Configuration Summary panel for Logical Library 1 is displayed (Figure 2-45). The panel contains the range of SCSI element addresses for the cartridge storage slots and the drives.



```
                                   Panel 0103
Configuration Summary
_____________________________________
Key:[LL=Logical Library,

F=Frame,C=Column, R=Row]
LL Logical Library  1
Media type        LTO

Storage Slots:    0064
Elem Addr Range:  1025 - 1088
First Location:   [F1,C01,R02]
Last Location:     [F1,C03,R21]

Drives:           001
Elem Addr Range:  0257 - 0257
First Location:   [F1,R01]

Last Location:     [F1,R01]

Control Path:

2____________________________________
Back Up Down                  ENTER
```

Figure 2-45   IBM TS3500 operator panel: Configuration Summary

13. Click **ENTER** to display the Configuration Summary panel for each logical library. After displaying the panel of the last logical library, the library displays the message: `Do you want to commit the new logical configuration?`

14. Click **Yes** to accept the new configuration (the library might take several minutes to process). When finished, it displays the message: `The configuration process is complete.`

2.3 Partitioning the TS3500 with ALMS enabled

The *Advanced Library Management System* (ALMS), an optional extension to the IBM patented multi-path architecture (FC1690), provides enhanced flexibility and capabilities for partitioning the TS3500 Tape Library. ALMS virtualizes the SCSI element addresses while maintaining the approach of the multi-path architecture and using SCSI3 Medium Changer commands. Without ALMS tape handling is based on the SCSI element address (location-centric) and partitioning is based on real cartridge slots and drive slots. With ALMS, there is no affinity between a real slot address and a SCSI Element address reported to the server and used by the server. Instead there is now an affinity with the VOLSER (volume serial numbers on the barcode label of the cartridge). ALMS allows the following new capabilities on the TS3500 Tape Library:

- Dynamic partitioning:
  - Storage slot pooling
  - Flexible drive assignment
- Add/remove storage capacity transparent to any host application
- Configure drives or Lxx storage capacity without taking the library offline
- Virtualize I/O slots to automatically manage the movement of cartridges between I/O station slots and storage slots
- More flexible configuration options for using tape encryption (see 7.2.1, “Hardware prerequisites” on page 206)

The TS3500 Tape Library is compliant with the SCSI Medium Changer standard whether ALMS is enabled or not; when enabled, ALMS is completely transparent to the application. The SCSI Medium Changer can be thought of as a “location-centric” interface. The application controlling a SCSI Medium Changer device specifies a source and destination location for each request to move a cartridge. The traditional SCSI library does not have control of the cartridge locations; instead the SCSI library just acts on behalf of the server.

Restriction: ALMS is available only for the TS3500 Tape Library and requires FC1690 for enablement.

2.3.1 Functional description

In this section, we give a functional description of the ALMS features. The information is based on the *IBM TotalStorage UltraScalable Tape Library TS3500 Tape Library Advanced Library Management System Technology White Paper* by Lee Jesionowski, which can be found at:

http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101038

Storage slot virtualization

The host-view of a cartridge location is known as the *SCSI storage element address*. Without ALMS, the storage element address maps directly to a specific storage slot after the library is configured. With ALMS enabled, a given storage element address is no longer associated with a specific storage slot. Instead, storage slots are virtualized by dynamically associating them with element addresses, as required. An element address is associated with a storage slot, selected by the library, as cartridges are moved and inventoried. In the case of a storage element that is empty due to a move, that source element address becomes unassociated. Association of storage element addresses is accomplished in a way that is completely transparent to the application software.

The number of storage element addresses for a logical library (as reported to the host application software) is selectable by changing the Maximum Number of Cartridges setting for that logical library using the Web user interface (Tape Library Specialist). For each logical library, the default value for Maximum Number of Cartridges is the number of addressable storage slots that are installed in the library for that cartridge type at the time that ALMS is first enabled or, after ALMS is enabled, at the time the logical library is created. The Maximum Number of Cartridges setting can be changed for each logical library, but the value must always be greater than or equal to the number of actual cartridges currently assigned to that logical library.

It is possible to set Maximum Number of Cartridges to a value that is higher than the number of addressable storage slots installed at the time. This allows future library capacity expansion to be transparent to the host application software. However, application performance might degrade slightly due to the greater number of addresses. Care should be taken to not exceed the license limitations of the host application software. For i5/OS Backup Recovery and Media Services (BRMS) license limitations are no issue as licensing is tiered based on processor groups with support for an unlimited number of cartridges.

The starting element address for storage slots of each logical library is x'400' (1024) plus the associated logical library number. For example, logical library 1 would start at x'401' (1025), logical library 2 would start at x'402', and so on (see Figure 2-46 on page 62). The reason they do not all start at x'401' is because some applications have to be able to differentiate between different logical libraries from the same physical library.

Drive assignment

Using the ALMS flexible drive assignment capability, any drive in any position within any frame can be assigned to any logical library without creating any gaps in drive addresses. Drive (data transfer) element addresses are still mapped to specific drive locations when the drive is assigned, but any drive location can now be assigned to any logical library (intermix supported) using the Tape Library Specialist. Each drive added to a logical library is assigned to the lowest available element address, regardless of drive location.

When ALMS is first enabled, the *Data Transfer Element* (DTE) addresses of all installed and assigned drives are not changed from their previous values. However, after ALMS is enabled, the DTE addresses for any newly installed and assigned drives no longer depend on the drive's position. Instead, the DTE address for any newly installed or assigned drive is determined by the sequence in which the drive is assigned to each logical library. After enabling ALMS, drives are assigned to logical libraries using the Drive Assignment page of the Tape Library Specialist.

Using this interface, the DTE address for the first drive assigned to a new logical library is 257 (x'101'); see Figure 2-46. The DTE address for any other drive assigned to a logical library is based on the next available DTE address in that particular logical library. The next available DTE address is the lowest available DTE address after the starting DTE address. (This fills any gaps that are created when drives are unassigned and removed from a logical library.) When a drive is unassigned from a logical library using the Web interface, only that DTE address is made available for future usage, no other DTE addresses are affected.

The Drive Assignment page also supports the option to share a drive between two or more logical libraries. The drive is assigned a DTE address in more than one logical library. Note that the DTE addresses that are assigned to a shared drive can differ by logical library.

By using ALMS' dynamic Drive Assignment capability, any drive in any position in any frame is available to be assigned to any logical library without creating gaps in DTE addresses.

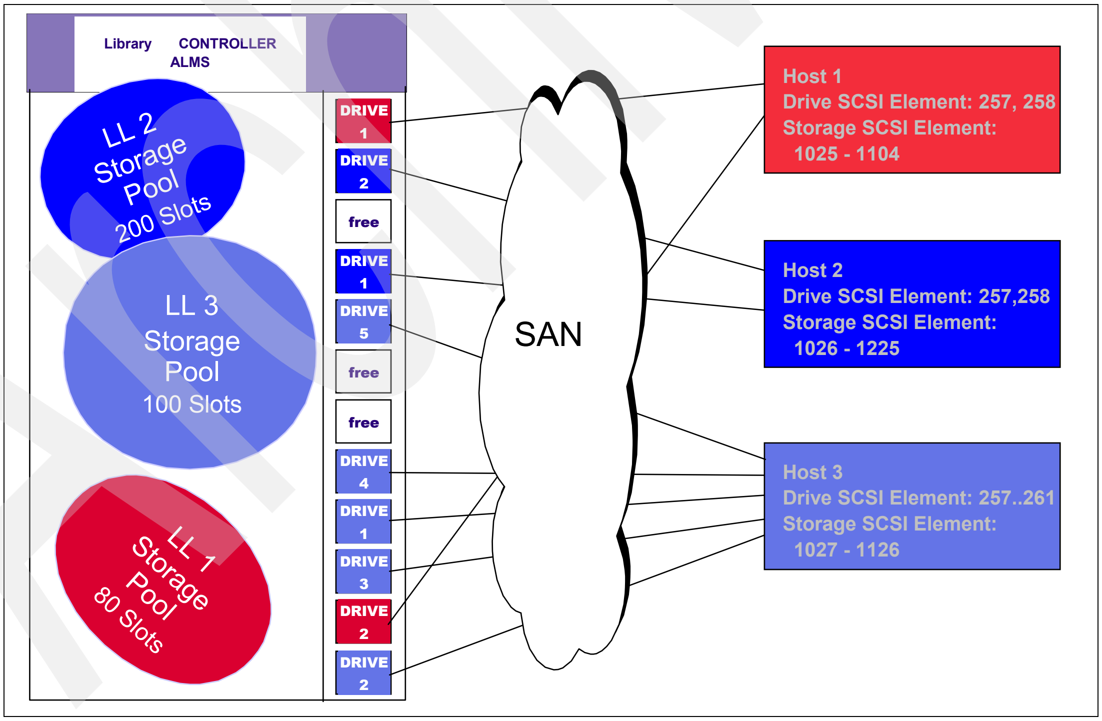


Figure 2-46 IBM TS3500 Tape Library with ALMS

Storage slot pooling

With ALMS, logical libraries can be added or deleted non-disruptively. All storage slots are first-come-first-served to each logical library based on cartridge insert operations. Therefore, storage slots are pooled as a shared resource such that changes to the capacity allocation for each logical library can occur without any down time or administrator involvement. Indications of a full or nearly full physical library continue to be provided via the Operator Panel, Tape Library Specialist, and SNMP traps.

The minimum logical library simply has a name and can be thought of as a file folder that has no content. Drives can be placed in the file folder using the Drive Assignment panel of the Tape Library Specialist. Cartridges can also be placed in the file folder, based on their volume serial (VOLSER) numbers and by using one of the following methods (in priority order):

- Migration from static partitioning (UI enablement of ALMS)
- Cartridge assignment policy (automatic at time of insertion)
- Insert notification (Operator Panel selection at time of insertion)
- Software application move from I/O station (based on source of command)
- Manual assignment using the Tape Library Specialist

The VOLSER assignment and physical location of cartridges are stored in non-volatile RAM (both primary and backup copies).

Shared drive assignment

Some customers require the ability to easily share a drive on an exception basis. For example, a drive might be required for a once-a-month job or as a temporary replacement for a failed drive. The Tape Library Specialist drive assignment UI supports the ability to assign a drive to multiple logical libraries. Therefore, each logical library consists of dedicated drives and shared drives. Each logical library maps a drive element address to the location of both dedicated and shared drives.

This option reduces the requirement to configure and unconfigure the tape drive every time it is required or not.

The Drive Assignment Web window supports the following point-and-click capabilities, which are non-disruptive to other logical libraries:

- Assign the drive
- Remove the drive assignment
- Reassign the drive

When a cartridge is mounted in a shared drive, the library only accepts a de-mount command requested via the source logical library; any de-mount command requested via other logical libraries is rejected.

However, the data path to the tape drive itself is not protected by the library. Therefore, the administrator must ensure that shared drives are not accessed by the wrong application via the data path.

On i5/OS the SCSI reserve and release option is used to ensure that no other server can synchronously access the tape drive – except for commands such as SCSI Inquiry – ensuring that data is not overwritten by any other host or application. Usage of SCSI reserve/release on i5/OS is achieved for stand-alone tape devices when they are varied on with a device description `ASSIGN *YES` parameter setting. Tape libraries in an `ALLOCATED` status have their corresponding drives permanently reserved while in the `UNPROTECTED` status the library's drive is only reserved while being actively used.

On Open Systems platforms, the SCSI reserve/release handling is done by the device driver and application, which must initiate a SCSI reserve on a device open, and after the device is closed, the application must send a SCSI release to the tape drive. Most Open Systems platform applications handle this, but it is best to check with the backup software provider to confirm.

SAN switch zoning can also be used to prevent access to the same tape drives by different servers.

When a tape drive is shared by different applications, any application using the drive has no knowledge of the other applications sharing the tape drive. Therefore, a cartridge could be loaded already and in use by application A, but if application B does not know it and tries to mount a cartridge in the same drive, application B would get a failure and the job that application B was executing would fail. For the i5/OS environment the BRMS network feature maintains a synchronized media inventory for all i5/OS systems within the BRMS network so that media conflicts are no issue. Some applications periodically scan all the tape drives and if they recognize that there is a cartridge mounted without initiation from the application itself, the application would consider this tape drive offline.

However, in general, we recommend not allowing multiple different applications with a non-sychronized media inventory to use shared tape drives concurrently. In this case set tape drives offline (or in service mode) from the application whenever they are not in use by that application.

The sharing option is mainly intended for environments where some drives are required only occasionally and must be preconfigured for the application.

Note: An application that occasionally leaves cartridges in drives or periodically scans all configured drives is not a good candidate for sharing drives between logical libraries.

Eliminates down time for total capacity changes

With ALMS enabled, the total library capacity (number of addressable storage slots) can be changed transparently to each application because the Maximum Number of Cartridges value is not affected by changes to the number of physical storage slots. The additional storage slots are simply new slot candidates for cartridges to be moved to upon insertion.

Furthermore, using the new Intermediate and Full Capacity on Demand capabilities of the TS3500 Tape Library Model L23 and L53, updates requires no down time at all for the change to total L-frame capacity.

Cartridge assignment policy

The cartridge assignment policy (CAP) of the TS3500 allows you to assign ranges of cartridge volume serial (VOLSER) numbers to specific logical libraries through the Tape Library Specialist. When a cartridge is inserted into the I/O station, the cartridge assignment policy is used to attempt to associate the cartridge with a logical library. If the cartridge is not in the CAP and insert notification (discussed in the next section) is enabled, you can assign the cartridge to a logical library by using the Insert Notification process on the library's operator panel or keep the cartridge as unassigned and assign it later using the Tape Library Specialist. If the insert notification feature is not enabled, and the cartridge was not in the CAP, the cartridge eventually becomes available to all hosts. Unassigned cartridges can also be assigned to a logical library by creating a new VOLSER range, then performing a manual inventory to assign those cartridges through the cartridge assignment policy.

The cartridge assignment policy is media-type specific. As such, it is based on the six most significant characters of the cartridge label, and the ranges of VOLSERs do not include the media-type indicator (L3, L4, JA, JJ and so forth). This means that two identical labels (except for the media-type indicator) could be assigned to two different logical libraries; for example, libraries that contain LTO or 3592 drives.

Note: The cartridge assignment policy does not reassign an assigned tape cartridge. To reassign a cartridge, use the procedure for assigning cartridges to a logical library.

Insert notification

Insert notification is an option that enables the TS3500 to monitor the I/O station for any new media which does not have a logical library assignment. This feature can be enabled through the Operator Panel or through the Tape Library Specialist. With Insert Notification enabled, when new media is detected the operator panel displays a message that asks to select a logical library. Any unassigned cartridges in the I/O station are assigned to the logical library that you select (and all other logical libraries are not able to access the cartridges). The library includes an option to defer any assignment and there is a time-out period when the deferral automatically takes effect.

2.3.2 Virtual I/O

The TS3500 Tape Library has I/O stations and I/O slots that enable you to import and export up to 32 cartridges at any given time. With the special 64-slot I/O frames, a total of 224 I/O slots can be available. The I/O slots are also known as *import/export elements (IEEs)*. Virtual I/O (VIO) slots increase the quantity of available I/O slots by allowing storage slots to appear to the host as I/O slots. Storage slots that appear to the host as I/O slots are called *virtual import/export elements (VIEEs)*. The goal of virtual I/O slots is to reduce the dependencies between the system administrator and library operator so that each performs their import and export tasks without requiring the other to perform any actions. With virtual I/O slots, the library automatically moves cartridges from the I/O stations to physical storage slots and from physical storage slots to the I/O stations.

With virtual I/O slots, you can configure up to 255 VIEEs per logical library. This can be set using the Specialist web GUI Max VIO Cartridges option for a logical libraries. Each logical library has a unique VIEE address space that is not accessible by other logical libraries.

New logical libraries are by default assigned the maximum number of virtual I/O slots, while logical libraries defined before ALMS is enabled initially have the number of physical I/O slots in the library.

Prior to virtual I/O slots, the IEE space was composed of physical I/O station slots in the L-frame (10, 30, 16, or 32 depending on the frame model type). Additionally, 3 times 64 slots are now available with the extended I/O frames. The I/O slots were shared by all logical libraries. If the application or system administrator did not explicitly import the cartridges from the I/O station into library storage, the cartridges would remain in the I/O station. This reduced the number of IEEs available to process imports and exports.

With virtual I/O slots, when cartridges are inserted into the I/O station, the library works with the cartridge assignment policy or insert notification to assign a cartridge to the correct logical library VIEE space, and cartridges are automatically moved into library storage slots. If there is no cartridge assignment policy assigned and insert notification is disabled for a particular cartridge, then that cartridge is inserted into the VIEE space of all logical libraries and automatically get moved into a library storage slot. The VIEE temporarily takes on the attributes of an IEE until a host moves the cartridge into a *storage element* (StE). When the host move occurs, if the cartridge is in a storage slot, no physical move is required and the element transitions from a VIEE to an StE. Similarly, when a host exports a cartridge from an StE, the physical storage slot is reported as a VIEE without moving the cartridge to the I/O station. The library monitors when free space is available in the physical I/O station and moves exported cartridges at the library’s convenience.

If a cartridge cannot be assigned, this is reported as *Assignment Pending*. This can occur if the assigned logical library does not have any available VIEE slots, or if all of the logical libraries do not have a common VIEE to share. To resolve this, either free up VIEE addresses so this is available in all libraries, or make a specific assignment of this cartridge to a logical library.

With VIO, there is an option to *Hide/Show Exports*. Show Exports, the default, shows a VIEE inventory of cartridges exported from the logical library. These cartridges then fill one of the VIEE slots for that logical library. Exporting a cartridge is reported as `Export in Progress` if there is no available VIEE and does not complete until one is available. `Export Complete` is shown when the exported cartridge is physically in an I/O station slot.

Selecting Hide Exports moves the exported cartridges to a library-maintained export queue, the VIEE is free immediately for other import/exports, and the exported cartridge disappears from the host application's inventory data.

Support for Virtual I/O slots is provided at library microcode level 5360 and above, and is enabled by default when ALMS is enabled. Existing customers who have already enabled ALMS on their TS3500 Tape Library have to install a newer level of library microcode that supports virtual I/O and then manually enable the virtual I/O slots.

For VIO examples, see also *IBM System Storage Tape Library Guide for Open Systems,* SG24-5946.

2.3.3 Configuring ALMS

The ALMS Feature Code #1690 is required for ALMS operation. This feature code provides a License Key that must be installed through the Operator panel (unless it was part of the initial order and was thus already installed by manufacturing.

Enter ALMS license key

To enter the ALMS license key, do the following steps:

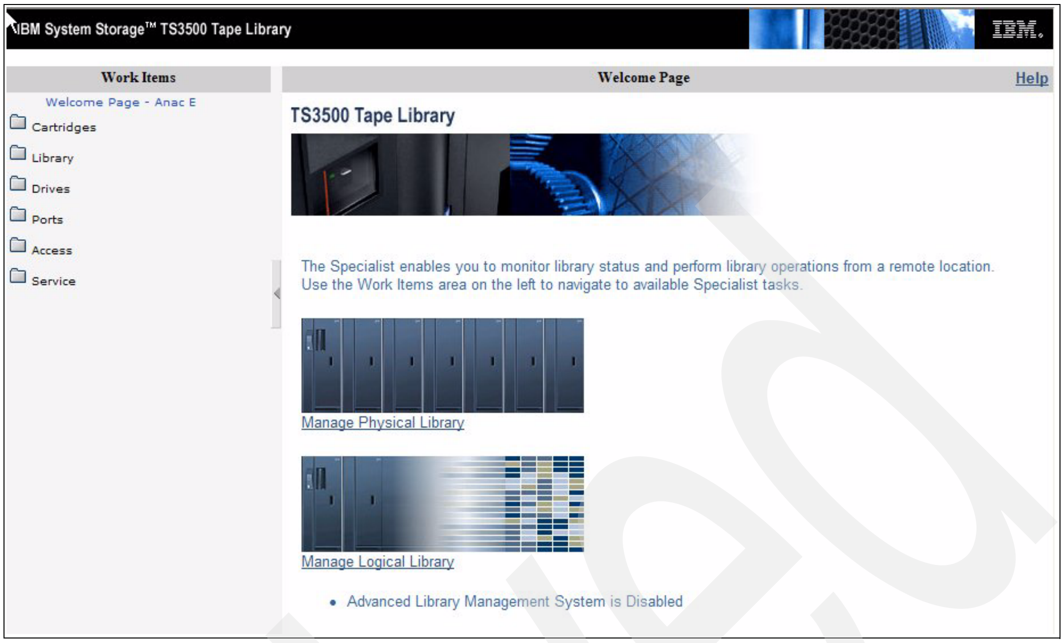
1. From the library Operator Panel, select **Menu** → **Service Library** → **Firmware Update** → **Features** → **Enter**. The Features panel displays a list of features, including the **Advanced Library Management System**. Select this and press Enter.
2. For each character of the license key, press **Up** or **Down** to select the value you want, and press **Enter** to move to the next digit. If you enter an incorrect number, press **Back** to return to the previous digit.
3. Press **Enter**. The Features panel now indicates `Advanced Library Management Feature Is Installed`.

Press **Back** until you return to the main panel.

Enable ALMS

After the License Key is installed, you can enable ALMS by using the Tape Library Specialist and performing the following steps:

1. Enter the library's IP address as a Web site in your browser. If login security has been enabled, there is a login prompt, and then you see the welcome panel with the message that ALMS is disabled at the bottom; see Figure 2-47.



IBM System Storage™ TS3500 Tape Library

Work Items

Welcome Page - Anac E

Cartridges

Library

Drives

Ports

Access

Service

Welcome Page

Help

TS3500 Tape Library

The Specialist enables you to monitor library status and perform library operations from a remote location. Use the Work Items area on the left to navigate to available Specialist tasks.

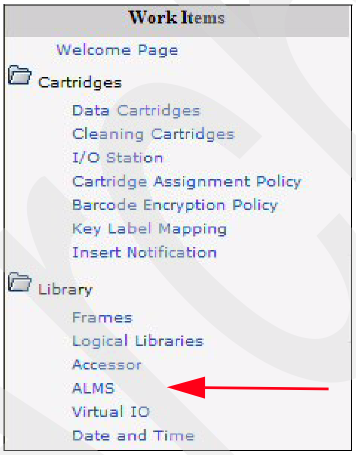
Manage Physical Library

Manage Logical Library

- Advanced Library Management System is Disabled

Figure 2-47 Welcome panel before enabling ALMS

2. On the left side of the panel, select **Library** → **ALMS**. This displays a warning and a specific selection to **Enable ALMS** (Figure 2-48). The operation can take many minutes, according to the size of your library.



Work Items

Welcome Page

Cartridges

Data Cartridges

Cleaning Cartridges

I/O Station

Cartridge Assignment Policy

Barcode Encryption Policy

Key Label Mapping

Insert Notification

Library

Frames

Logical Libraries

Accessor

ALMS

Virtual IO

Date and Time

Figure 2-48 Enable ALMS

Note: You can enable or disable ALMS in the TS3500 using the Tape Library Specialist, but not the operator panel.

When ALMS is enabled, you can easily:

- Name, add, and remove logical libraries.
- Reassign a cartridge to another logical library.
- Change the maximum quantity of cartridges that can be assigned to a logical library.

- Add, remove, and edit ranges of volume serial (VOLSER) numbers (also known as cartridge assignment policy).
- Assign shared drives, change control path drives, unassign drives, and assign new drives without using manual configuration methods.

ALMS can also be disabled, but this should done with care. After ALMS is enabled, the panel shown in Figure 2-48 on page 67 has the option **Disable ALMS** instead.

> **Important:** When you disable ALMS, the library returns to an unconfigured state and all cartridge and drive assignments are lost. You must manually reconfigure the library. However, switching between definitions, the library uses the previous definitions as a basic starting configuration.
>
> **Note:** If you manually configure the library, your changes might result in the loss of cartridge or logical library assignments, cartridge assignment policies, maximum cartridge assignments, and logical library names.

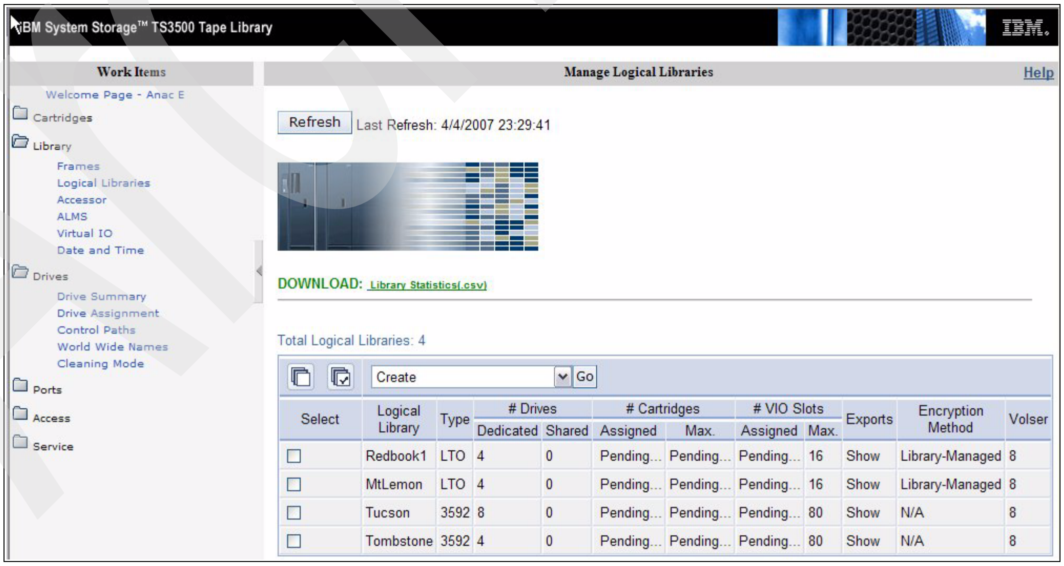
When using ALMS, cartridges belong to one logical library based on their VolSer. Without ALMS, logical libraries are based on physical boundaries within the library. This means that after disabling ALMS you might have to move several cartridges.

When switching from an environment with ALMS disabled, to one with ALMS enabled, the library uses the previous definitions as a basic starting configuration. The library performs an inventory operation similar to when the frame door has been opened. The library status during this inventory process shows a cartridge assignment status of pending (Figure 2-49).

Create and manage logical libraries

Follow these steps:

1. From the Tape Library Specialist (Figure 2-47 on page 67), select **Library** → **Logical Library** and on the next panel, Figure 2-49, click **Create**.



Last Refresh: 4/4/2007 23:29:41

DOWNLOAD: Library Statistics(.csv)

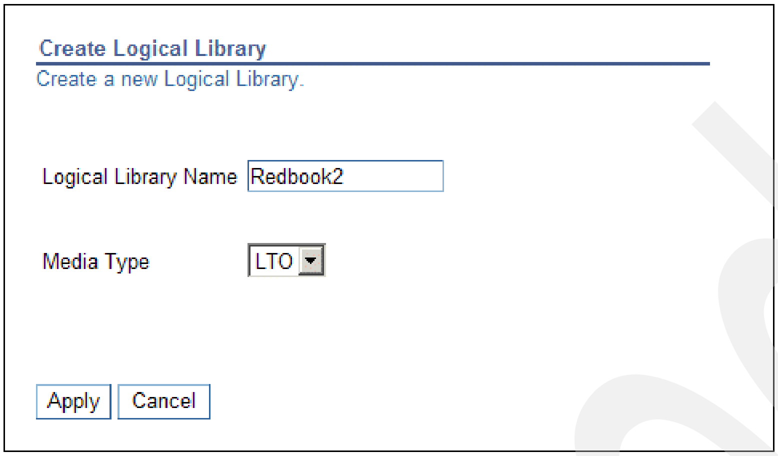
Total Logical Libraries: 4

Select	Logical Library	Type	# Drives		# Cartridges		# VIO Slots		Exports	Encryption Method	Volser
			Dedicated	Shared	Assigned	Max.	Assigned	Max.			
☐	Redbook1	LTO	4	0	Pending...	Pending...	Pending...	16	Show	Library-Managed	8
☐	MtLemon	LTO	4	0	Pending...	Pending...	Pending...	16	Show	Library-Managed	8
☐	Tucson	3592	8	0	Pending...	Pending...	Pending...	80	Show	N/A	8
☐	Tombstone	3592	4	0	Pending...	Pending...	Pending...	80	Show	N/A	8

Figure 2-49 Create Logical Library

2. Type a unique name (up to 15 characters) for your new logical library (in our case, `Redbook2`) and select a **Media Type** (LTO or 3592) for this logical library, as in Figure 2-50.

Click **Apply**. You cannot mix LTO and 3592 media types in one logical library, but you can have different LTO generations in one logical library, for example, LTO2, LTO3 and LTO4.



Create Logical Library

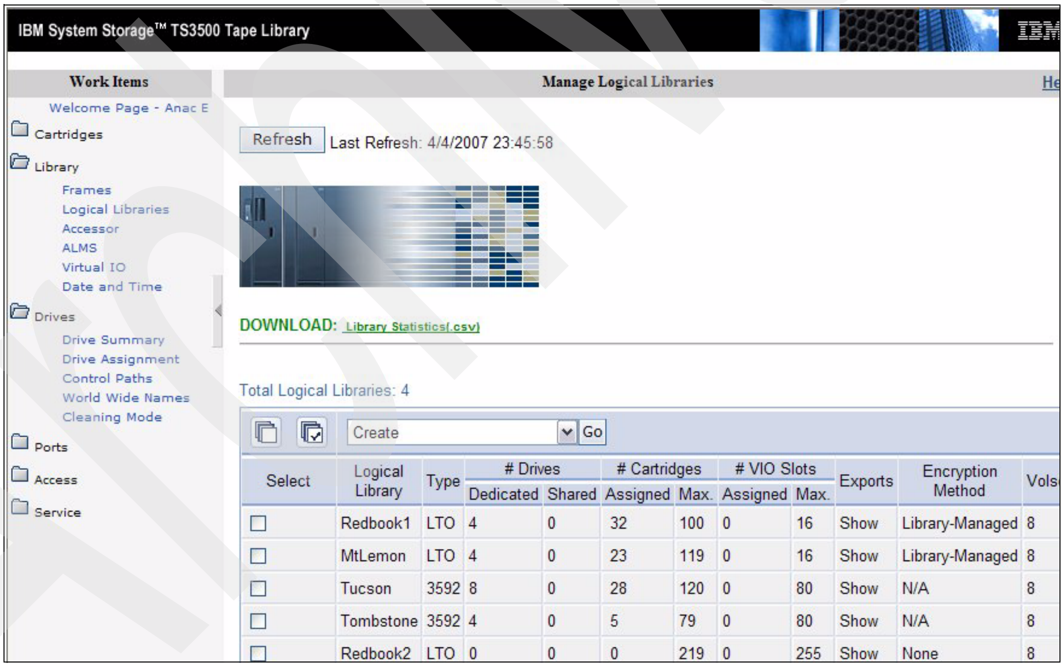
Create a new Logical Library.

Logical Library Name: Redbook2

Media Type: LTO

Figure 2-50   Create Logical Library

3. The library created appears in the Manage Logical Library display, as in Figure 2-51, but with no cartridges or drives assigned; these columns show a zero count. Therefore, after creating a new logical library, you have to add cartridge ranges and tape drives.



Last Refresh: 4/4/2007 23:45:58

DOWNLOAD: Library Statistics(.csv)

Total Logical Libraries: 4

Select	Logical Library	Type	# Drives		# Cartridges		# VIO Slots		Exports	Encryption Method	Vols
			Dedicated	Shared	Assigned	Max.	Assigned	Max.			
□	Redbook1	LTO	4	0	32	100	0	16	Show	Library-Managed	8
□	MtLemon	LTO	4	0	23	119	0	16	Show	Library-Managed	8
□	Tucson	3592	8	0	28	120	0	80	Show	N/A	8
□	Tombstone	3592	4	0	5	79	0	80	Show	N/A	8
□	Redbook2	LTO	0	0	0	219	0	255	Show	None	8

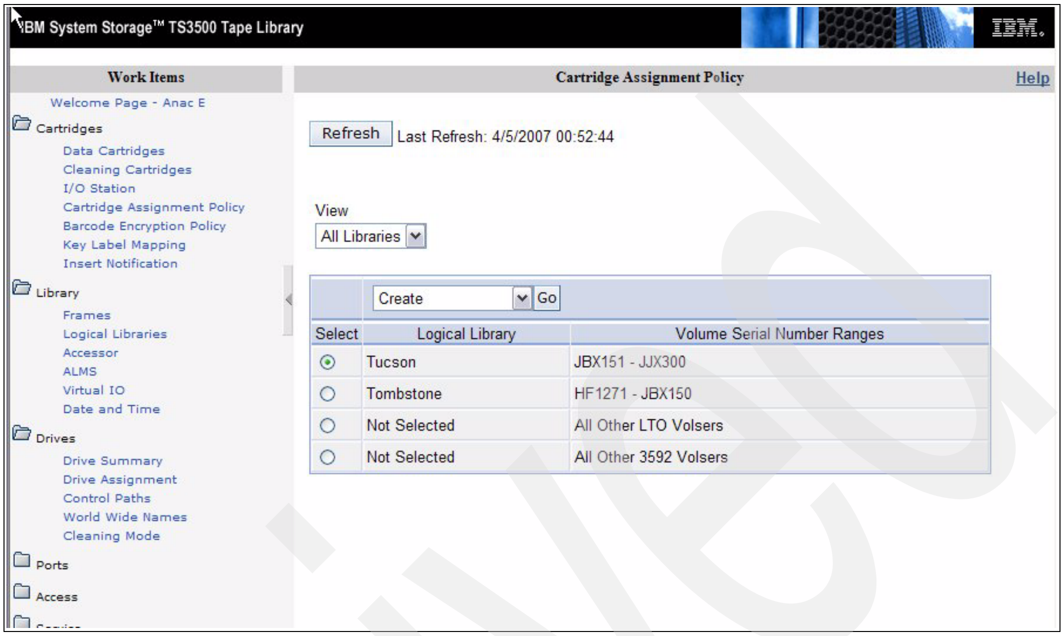
Figure 2-51   Added new logical library

Cartridge assignment policy

A new logical library does not have any cartridges assigned to it. You can assign single cartridges that are currently unassigned, or that are assigned to another logical library (the cartridge is then removed from this logical library).

Or, you can assign a range of unassigned cartridges (establish a *cartridge policy*) to the logical library. Such a *cartridge assignment policy* defines a range based on the VOLSER. Follow these steps:

1. To create a cartridge assignment policy, on the left-hand side, select **Cartridges** → **Cartridge Assignment Policy**. The Cartridge Assignment Policy window appears (Figure 2-52).

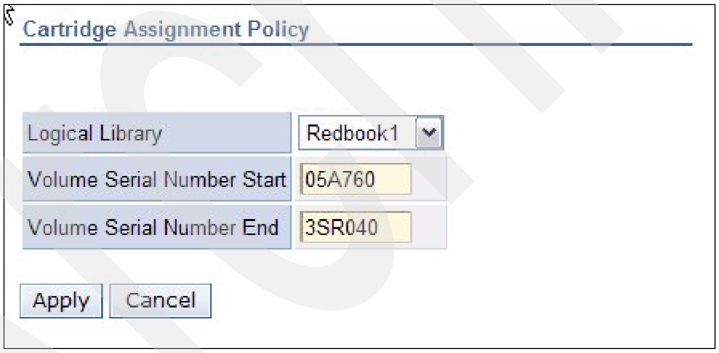


Last Refresh: 4/5/2007 00:52:44

Select	Logical Library	Volume Serial Number Ranges
●	Tucson	JBX151 - JJX300
○	Tombstone	HF1271 - JBX150
○	Not Selected	All Other LTO Volsers
○	Not Selected	All Other 3592 Volsers

Figure 2-52 Cartridge assignment policy main panel

2. Choose the logical library to which you want to assign the cartridge policy, enter the starting and ending VolSer for the range to be defined, see Figure 2-53, and click **Apply**.



Logical Library	Redbook1
Volume Serial Number Start	05A760
Volume Serial Number End	3SR040

Figure 2-53 Cartridge Assignment Policy assignments

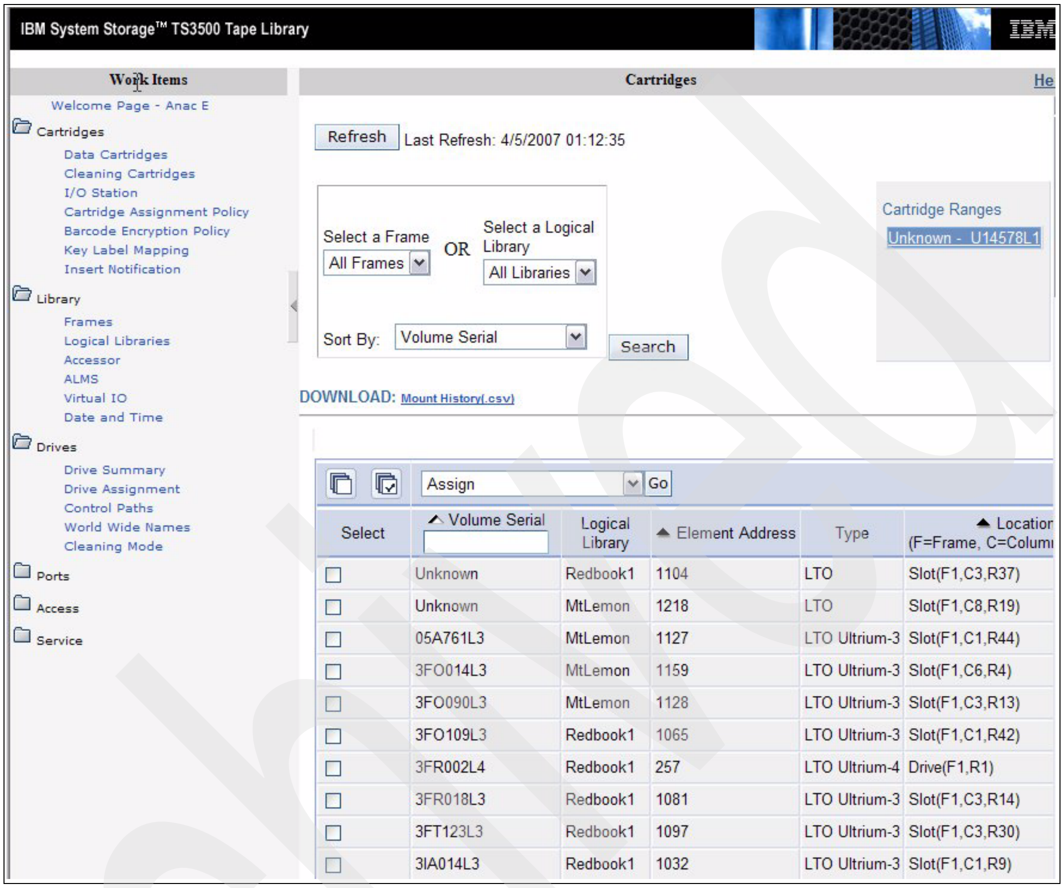
3. All unassigned cartridges and all new inserted cartridges within the specified range do now, by definition, belong to the specified logical library. However, new cartridges have to be inserted, or there must be a re-inventory to have existing unassigned cartridges in this range assigned into the logical library.

> **Note:** Previously assigned cartridges within the specified range remain untouched from changing the cartridge assignment policy.

Cartridge assignment

A single cartridge can be assigned to a specified logical library as well, or even be moved between libraries. Follow these steps:

1. To begin, navigate **Cartridges** → **Data Cartridges** (see Figure 2-54). Select the frame or logical library, select one or more cartridges to assign, and select **Assign** in the pull-down, and click **Go**.



Last Refresh: 4/5/2007 01:12:35

Select a Frame: All Frames OR Select a Logical Library: All Libraries

Sort By: Volume Serial

Cartridge Ranges: Unknown - U14578L1

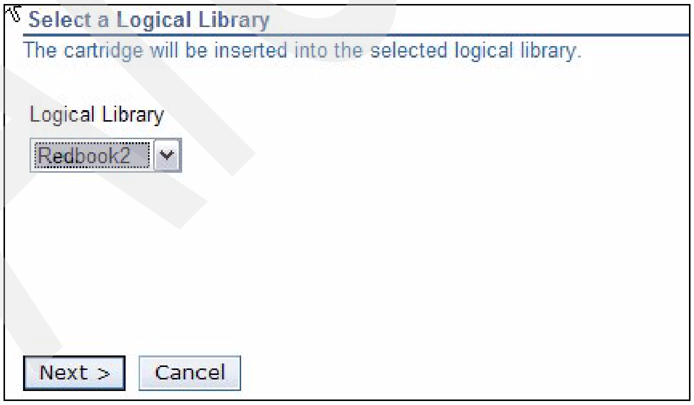
DOWNLOAD: Mount History(.csv)

Assign

Select	Volume Serial	Logical Library	Element Address	Type	Location (F=Frame, C=Colum
□	Unknown	Redbook1	1104	LTO	Slot(F1,C3,R37)
□	Unknown	MtLemon	1218	LTO	Slot(F1,C8,R19)
□	05A761L3	MtLemon	1127	LTO Ultrium-3	Slot(F1,C1,R44)
□	3FO014L3	MtLemon	1159	LTO Ultrium-3	Slot(F1,C6,R4)
□	3FO090L3	MtLemon	1128	LTO Ultrium-3	Slot(F1,C3,R13)
□	3FO109L3	Redbook1	1065	LTO Ultrium-3	Slot(F1,C1,R42)
□	3FR002L4	Redbook1	257	LTO Ultrium-4	Drive(F1,R1)
□	3FR018L3	Redbook1	1081	LTO Ultrium-3	Slot(F1,C3,R14)
□	3FT123L3	Redbook1	1097	LTO Ultrium-3	Slot(F1,C3,R30)
□	3IA014L3	Redbook1	1032	LTO Ultrium-3	Slot(F1,C1,R9)

Figure 2-54 Assign Data Cartridge menu

2. Select the library to which you want to assign the cartridge(s) (see Figure 2-55). Click **Next** to complete the operation. The cartridge is then logically moved to the new library.



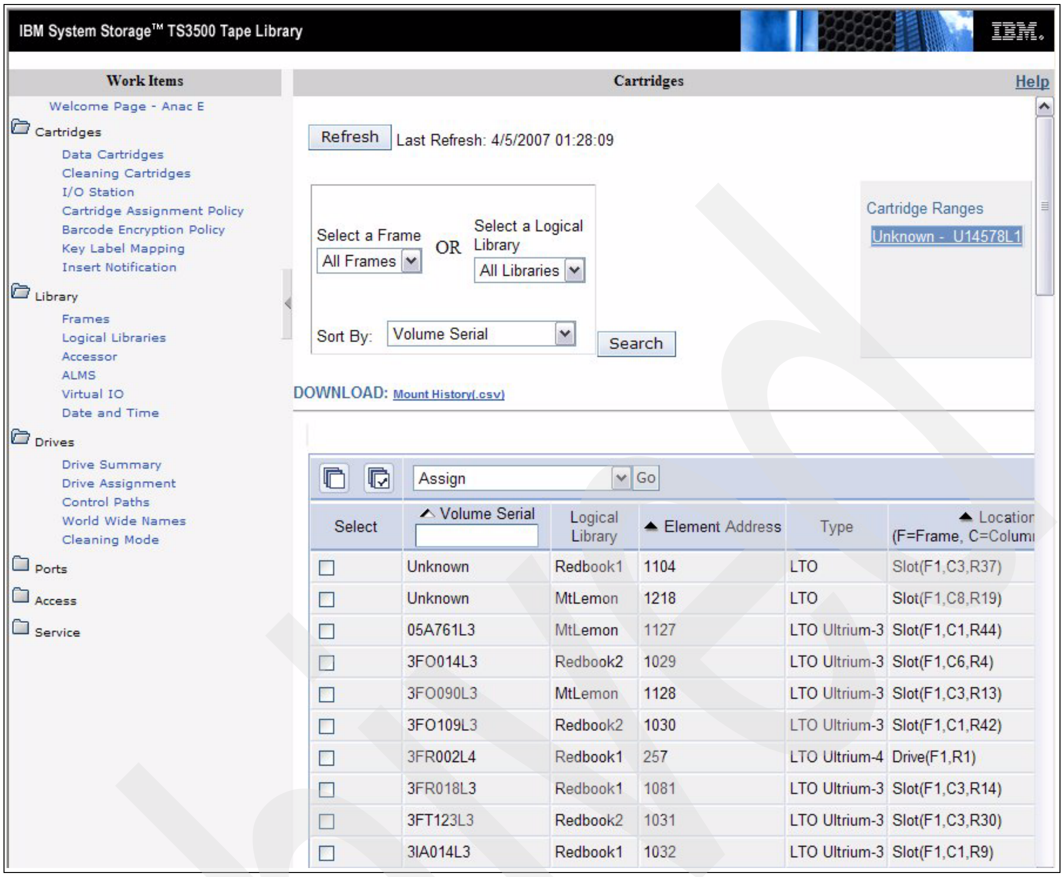
Select a Logical Library

The cartridge will be inserted into the selected logical library.

Logical Library: Redbook2

Figure 2-55 Assign cartridge to a logical library

3. In Figure 2-56, the Data Cartridges menu shows that the cartridge has moved to the new library. The cartridges has been given new element addresses according to the sequence of the new library, however, the cartridges remains in the same physical slots as before.



Last Refresh: 4/5/2007 01:28:09

Select a Frame: All Frames OR Select a Logical Library: All Libraries

Sort By: Volume Serial

Cartridge Ranges: Unknown - U14578L1

DOWNLOAD: Mount History(.csv)

Assign

Select	Volume Serial	Logical Library	Element Address	Type	Location (F=Frame, C=Colum
□	Unknown	Redbook1	1104	LTO	Slot(F1,C3,R37)
□	Unknown	MtLemon	1218	LTO	Slot(F1,C8,R19)
□	05A761L3	MtLemon	1127	LTO Ultrium-3	Slot(F1,C1,R44)
□	3FO014L3	Redbook2	1029	LTO Ultrium-3	Slot(F1,C6,R4)
□	3FO090L3	MtLemon	1128	LTO Ultrium-3	Slot(F1,C3,R13)
□	3FO109L3	Redbook2	1030	LTO Ultrium-3	Slot(F1,C1,R42)
□	3FR002L4	Redbook1	257	LTO Ultrium-4	Drive(F1,R1)
□	3FR018L3	Redbook1	1081	LTO Ultrium-3	Slot(F1,C3,R14)
□	3FT123L3	Redbook2	1031	LTO Ultrium-3	Slot(F1,C3,R30)
□	3IA014L3	Redbook1	1032	LTO Ultrium-3	Slot(F1,C1,R9)

Figure 2-56 Cartridge list

In our example, we now have cartridges assigned to the logical library, but no tape drives have been assigned. With ALMS, you can configure a logical library without any drives assigned to it. A driveless logical library can be used for:

- Tape vaulting, to move the cartridge to a location that cannot be accessed by the application.
- Use as a scratch pool.

Assign drives

The flexible drive assignment option supports the following capabilities:

- Assign drive (non-disruptive to other logical libraries)
- Unassign drive (non-disruptive to other logical libraries)
- Reassign drive (non-disruptive to other logical libraries)
- Assign drive to multiple logical libraries
- Change control paths

At least one assigned drive must have the control path enabled. Therefore, the first assigned tape drive gets the control path enabled by default. You can, however, enable or disable control paths for your drives. For i5/OS make sure that each System i tape IOA attached to the logical library has a control path configured. Drives with control path enabled cannot be shared with other logical libraries. You cannot assign LTO and IBM 3592 tape drives to the same logical library.

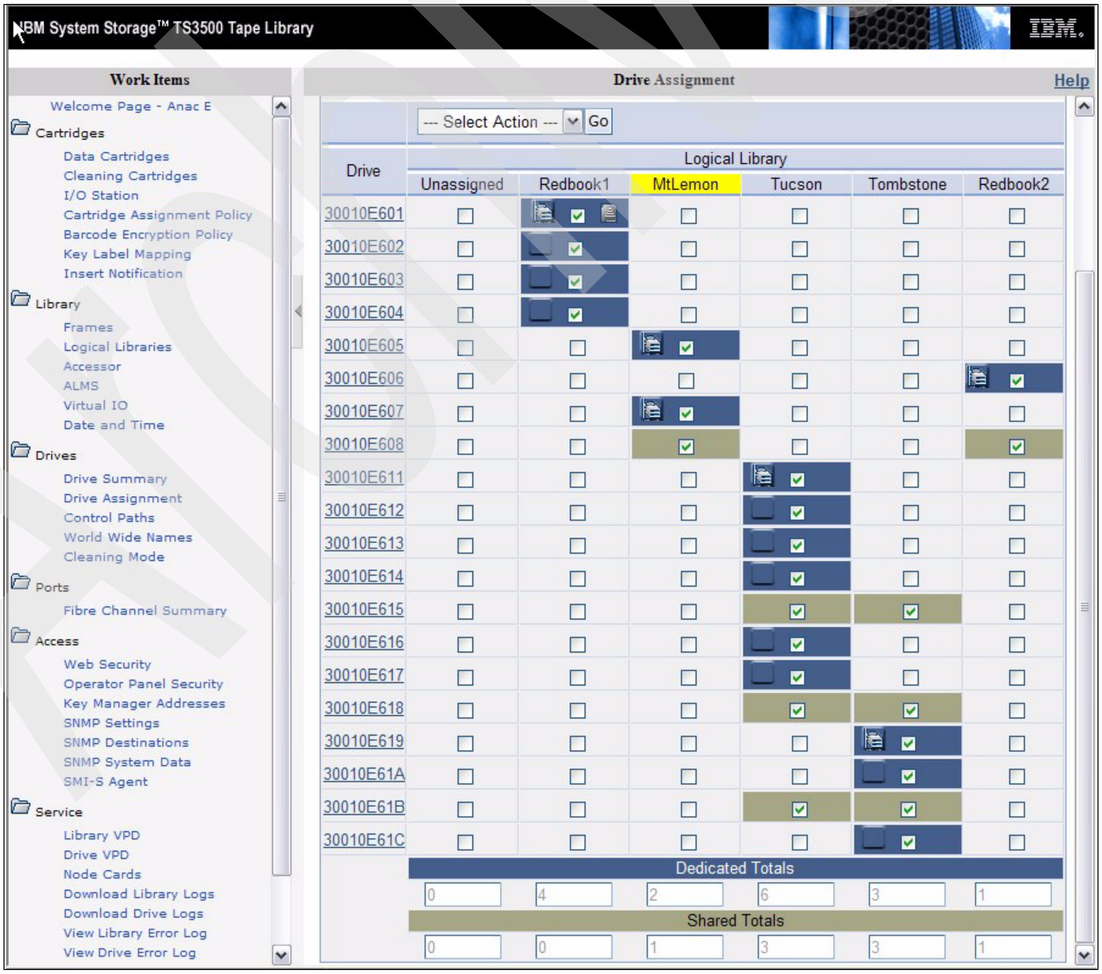
Although the drive assign procedure is non-disruptive, the application or server to which the drive is assigned must be configured. This server or application configuration might not necessarily be non-disruptive. In addition, a reconfiguration of the SAN might be required.

> **Note:** For i5/OS a reset of the corresponding IOP controlling the IOA the tape drive is attached to is required for library configuration changes.

Be sure that the drives you are working on do not have any cartridges loaded. The Tape Library Specialist does not allow you to change any assignment of tape drives with a cartridge loaded. Therefore, we suggest first running a manual inventory to be sure that there is not a forgotten cartridge in any drive.

To assign tape drives select **Drives** → **Drive Assignment**. On the introduction panel you can select specific drives or logical libraries, or a list of the full drive assignment. If you select the last option, the full assignment displays. On the drive assignment panel, you can easily assign and unassign tape drives to a logical library. On the left-hand side of the panel, you can see all available tape drives identified by their WWN. At the top, you see all the logical libraries. The first column is called Unassigned. All unassigned drives (such as newly installed drives) belong to this column. By simply clicking on the check boxes, you can easily assign tape drives to logical libraries, as has been done in Figure 2-57.

After you have completed your selections, select action **Apply** to make the changes effective.



Drive	Logical Library					
	Unassigned	Redbook1	MtLemon	Tucson	Tombstone	Redbook2
30010E601	□	☑	□	□	□	□
30010E602	□	☑	□	□	□	□
30010E603	□	☑	□	□	□	□
30010E604	□	☑	□	□	□	□
30010E605	□	□	☑	□	□	□
30010E606	□	□	□	□	□	☑
30010E607	□	□	☑	□	□	□
30010E608	□	□	☑	□	□	☑
30010E611	□	□	□	☑	□	□
30010E612	□	□	□	☑	□	□
30010E613	□	□	□	☑	□	□
30010E614	□	□	□	☑	□	□
30010E615	□	□	□	☑	☑	□
30010E616	□	□	□	☑	□	□
30010E617	□	□	□	☑	□	□
30010E618	□	□	□	☑	☑	□
30010E619	□	□	□	□	☑	□
30010E61A	□	□	□	□	☑	□
30010E61B	□	□	□	☑	☑	□
30010E61C	□	□	□	□	☑	□
Dedicated Totals	0	4	2	6	3	1
Shared Totals	0	0	1	3	3	1

Figure 2-57 Drive Assignment

Tape drives with control path enabled are indicated by the icon shown in Figure 2-58.

Figure 2-58 Drive with control path

The first tape drive assigned to a logical library automatically gets the control path enabled; if you want to enable more control paths, click the **placeholder** for the control path icon of the selected drive.

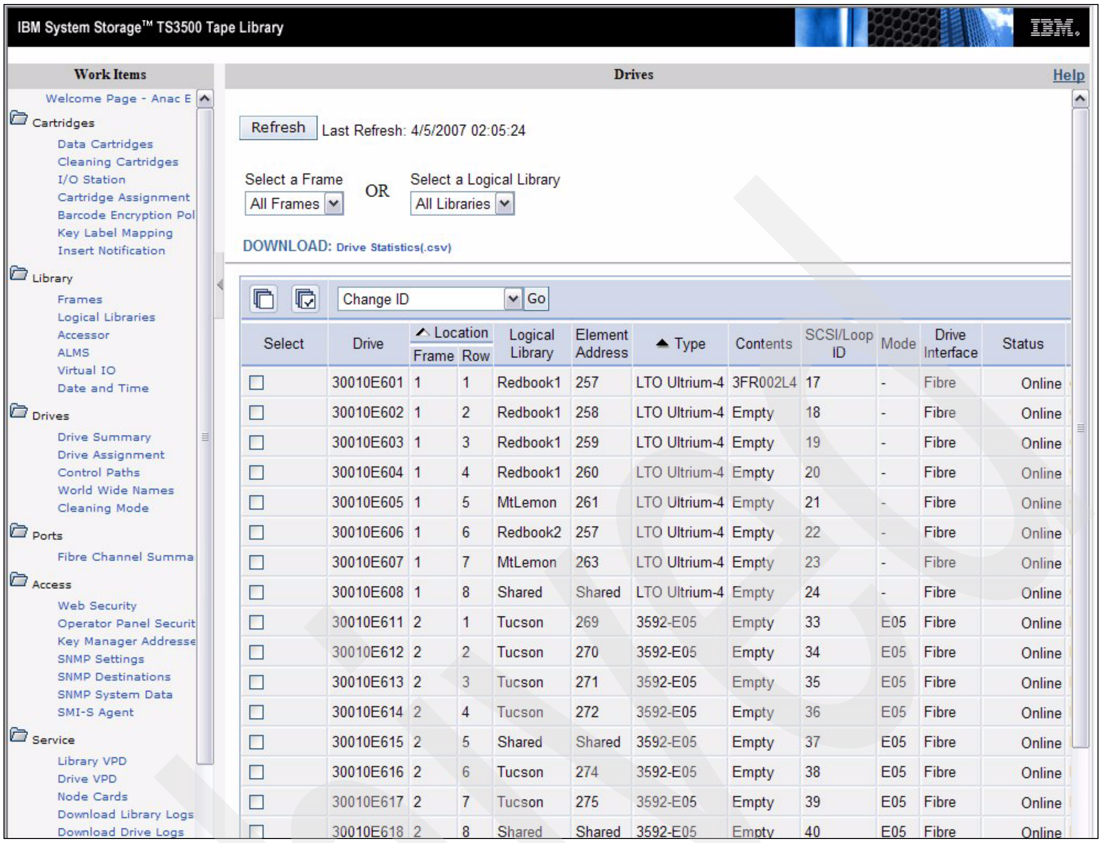
> **Note:** i5/OS supports no library control path failover so the rule is for each logical library to configure a single control path for each attached tape IOA. If IOAs are attached from different i5/OS servers, the control path(s) are shared.

If you want to delete a tape drive from one logical library, you have to set this tape drive to unassigned by checking the Unassigned check box for this tape drive.

We do not recommend that you assign a tape drive to multiple logical libraries unless required. If you have to share a tape drive, follow the recommendations given in “Shared drive assignment” on page 63. One drive can be shared by a maximum of 10 logical libraries.

In the example in Figure 2-57 on page 73, all logical libraries and applications require at least one tape drive to fulfill their backup jobs. Therefore, we assigned at least one tape drive to each logical library. In addition to the minimum required tape drive, we assigned some shared tape drives to some logical libraries. For all applications we thus configured at least two tape drives for use, but set the shared tape drive as offline, in service, or unavailable depending on the application. This enables us to easily use a shared tape drive (by setting it online, out of service, or available from the application) whenever it is required, for example, if one dedicated tape drive becomes defective, or one application temporarily requires more tape bandwidth due to additional workload (additional restores).

For any Open Systems backup applications that have to know the SCSI element address of the drive for configuring the library, check the SCSI element address of all tape drives by selecting **Drives** → **Drive Summary**. This displays the drive information as shown in Figure 2-59. Notice that this is now the virtualized element addresses, and that each logical library might show the same element address.



Last Refresh: 4/5/2007 02:05:24

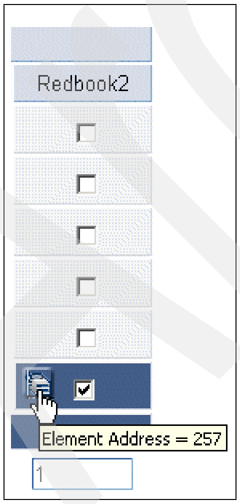
Select a Frame: All Frames OR Select a Logical Library: All Libraries

Change ID

Select	Drive	Location		Logical Library	Element Address	Type	Contents	SCSI/Loop ID	Mode	Drive Interface	Status
		Frame	Row								
□	30010E601	1	1	Redbook1	257	LTO Ultrium-4	3FR002L4	17	-	Fibre	Online
□	30010E602	1	2	Redbook1	258	LTO Ultrium-4	Empty	18	-	Fibre	Online
□	30010E603	1	3	Redbook1	259	LTO Ultrium-4	Empty	19	-	Fibre	Online
□	30010E604	1	4	Redbook1	260	LTO Ultrium-4	Empty	20	-	Fibre	Online
□	30010E605	1	5	MtLemon	261	LTO Ultrium-4	Empty	21	-	Fibre	Online
□	30010E606	1	6	Redbook2	257	LTO Ultrium-4	Empty	22	-	Fibre	Online
□	30010E607	1	7	MtLemon	263	LTO Ultrium-4	Empty	23	-	Fibre	Online
□	30010E608	1	8	Shared	Shared	LTO Ultrium-4	Empty	24	-	Fibre	Online
□	30010E611	2	1	Tucson	269	3592-E05	Empty	33	E05	Fibre	Online
□	30010E612	2	2	Tucson	270	3592-E05	Empty	34	E05	Fibre	Online
□	30010E613	2	3	Tucson	271	3592-E05	Empty	35	E05	Fibre	Online
□	30010E614	2	4	Tucson	272	3592-E05	Empty	36	E05	Fibre	Online
□	30010E615	2	5	Shared	Shared	3592-E05	Empty	37	E05	Fibre	Online
□	30010E616	2	6	Tucson	274	3592-E05	Empty	38	E05	Fibre	Online
□	30010E617	2	7	Tucson	275	3592-E05	Empty	39	E05	Fibre	Online
□	30010E618	2	8	Shared	Shared	3592-E05	Empty	40	E05	Fibre	Online

Figure 2-59 Drive details

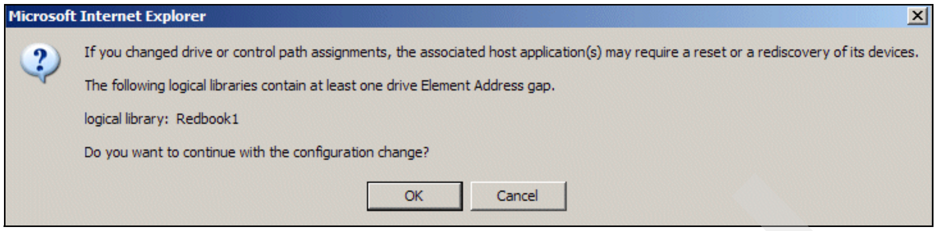
Alternatively, if you let the cursor hover over assigned element as in Figure 2-60, you get a small pop-up identifying the element number for that drive.



Element Address = 257

Figure 2-60 Display drive element number

By default, all drives are assigned the lowest available SCSI element address, which for Redbook1 are elements 257 to 260. It is possible that address gaps are created in the assignment. If Redbook1 drive 2 is set to unassigned, and you try to **Apply**, you get a warning message indicating that there might be an element gap, as shown in Figure 2-61.



Microsoft Internet Explorer

If you changed drive or control path assignments, the associated host application(s) may require a reset or a rediscovery of its devices.

The following logical libraries contain at least one drive Element Address gap.

logical library: Redbook1

Do you want to continue with the configuration change?

Figure 2-61   Drive gap warning

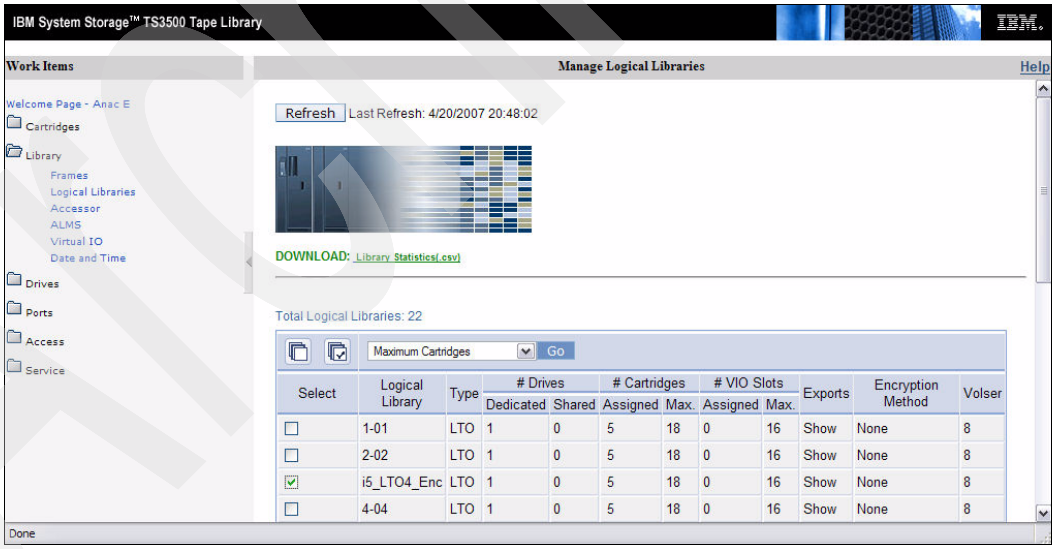
Although for i5/OS, gaps in the drive assignment do not matter, we generally recommend for other Open Systems hosts that you avoid having any gaps in the drive assignment. Gaps can easily be removed by simply unassigning and then reassigning the drive with the highest SCSI element address until all gaps are filled. Gaps in the drive SCSI element address can cause configuration problems on some backup applications such as EMC Legato NetWorker and VERITAS NetBackup.

Change the maximum number of storage slots

Since ALMS virtualizes the SCSI element address of the storage slots, the library is able to report any desired amounts of storage slots. Of course the number reported cannot be less than the actual number of cartridges in the library. The library allows the user to select a 16-frame maximum limit (6887). The default value is based on the physical slots currently in the library.

To change the Maximum Number:

1. Select **Library** → **Logical Libraries,** select the logical library and select **Maximum Cartridges** from the drop-down menu as shown in Figure 2-62.



Last Refresh: 4/20/2007 20:48:02

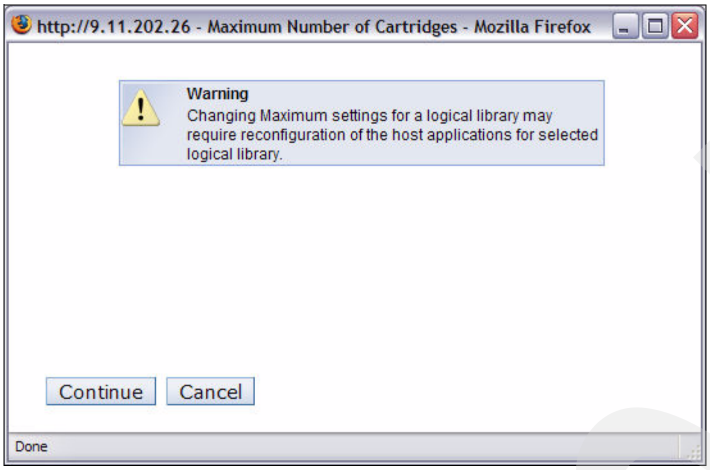
Total Logical Libraries: 22

Maximum Cartridges

Select	Logical Library	Type	# Drives		# Cartridges		# VIO Slots		Exports	Encryption Method	Volser
			Dedicated	Shared	Assigned	Max.	Assigned	Max.			
☐	1-01	LTO	1	0	5	18	0	16	Show	None	8
☐	2-02	LTO	1	0	5	18	0	16	Show	None	8
☑	i5_LTO4_Enc	LTO	1	0	5	18	0	16	Show	None	8
☐	4-04	LTO	1	0	5	18	0	16	Show	None	8

Figure 2-62   Manage Logical Libraries panel Maximum Cartridges option

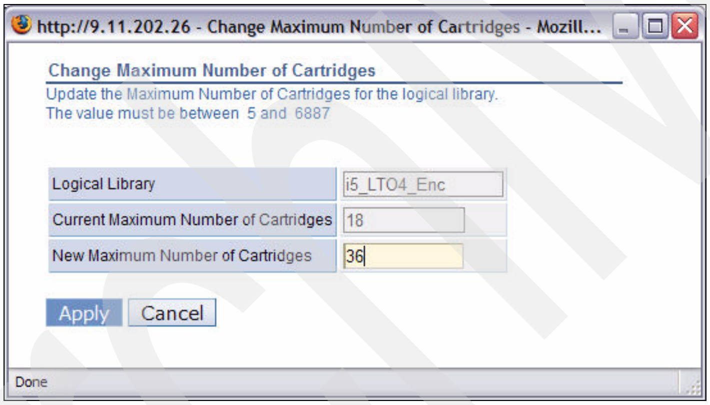
2. After clicking **Go**, a warning like the one shown in Figure 2-63 appears.


http://9.11.202.26 - Maximum Number of Cartridges - Mozilla Firefox

Warning
Changing Maximum settings for a logical library may require reconfiguration of the host applications for selected logical library.

Figure 2-63 Maximum Number of Cartridges Warning

3. After clicking **Continue**, enter the new maximum number of cartridges as shown Figure 2-64 and click **Apply**.


http://9.11.202.26 - Change Maximum Number of Cartridges - Mozill...

Change Maximum Number of Cartridges
Update the Maximum Number of Cartridges for the logical library.
The value must be between 5 and 6887

Logical Library	i5_LTO4_Enc
Current Maximum Number of Cartridges	18
New Maximum Number of Cartridges	36

Figure 2-64 Change Maximum Number of Cartridges window

> **Note:** For i5/OS, changes to the maximum number of storage slots require a reset of the IOP(s) the corresponding library is attached to. The new storage slot capacity can be viewed, for example, from the DSPTAPSTS command output.

While this change is non-disruptive for the library operation, this might not necessarily be the case for your Open Systems platform backup application. For example, with NetWorker you must run **jbconfig**, and with IBM Tivoli Storage Manager you must halt and re-start the server.

The ability to change the maximum number can be helpful if:

- You just have a license for a smaller library.
- You expect capacity growth, which forces you to enlarge your library physically over time, but want to avoid configuration changes in your application. Therefore, on the first setup, configure your logical library with a greater number of logical slots to avoid an outage later on, because you would then have to reconfigure the application.

However, a large number of reported storage slots can decrease the application performance in working with the library (such as an inventory or audit library, which takes longer from the application point of view).

Migration from partitioning without ALMS to ALMS

A library that was previously installed without ALMS can be upgraded to ALMS by enabling the ALMS license key. The license key must be entered using the operator panel; see “Enter ALMS license key” on page 66.

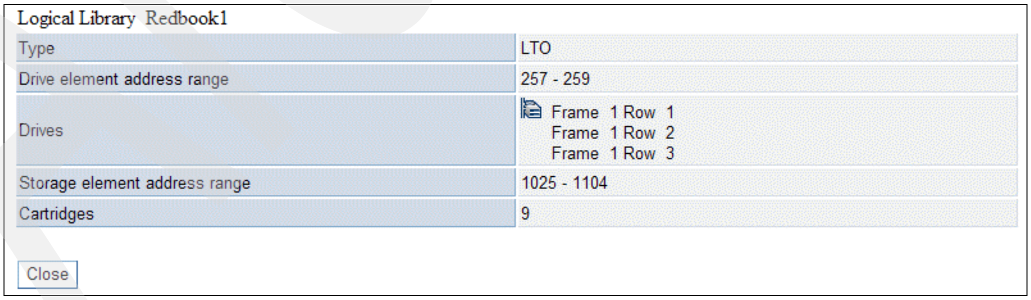
When enabling ALMS, it reuses the existing library configuration. This means that you get the same number of logical libraries. Cartridges and tape drives which were already assigned to the logical library remain assigned to the same logical library. Tape drives get the same SCSI element address (even if there was a gap in the SCSI element address) and all cartridges get the same SCSI element address as in the non-ALMS definition.

However, the storage element address of the storage slots for new logical libraries changes as described in “Storage slot virtualization” on page 61. For the first logical library, the storage address begins with 1025, for the second one with 1026, and so on. Adding a new logical library (Redbook2) to the four logical libraries that were already defined without ALMS, means that this library is number four, and accordingly, starts with a cartridge element address of 1029.

Also, in libraries with mixed media, the reported number of maximum storage slots might change to the number of currently installed cartridge slots. Consequently, when you enable ALMS, on i5/OS, the IOPs that the library is attached to must be reset. On other Open Systems platforms your application might also have to be reconfigured. For some applications, like the IBM Tivoli Storage Manager, you just have to stop and restart the server; for other applications, like EMC Legato NetWorker, you have to run a configuration wizard (run **jbconfig**).

You can enable ALMS using the Tape Library Specialist. Select **Library** → **ALMS** (refer to “Enable ALMS” on page 66 for details).

To illustrate how ALMS changes the configuration of the logical libraries, in Figure 2-65, we show the detailed information for a logical library named Redbook1. It indicates three tape drives with SCSI element addresses 257, 258, and 259. The storage element address range is 1025 to 1104 (80 storage slots). The physical library has 175 storage slots in total.



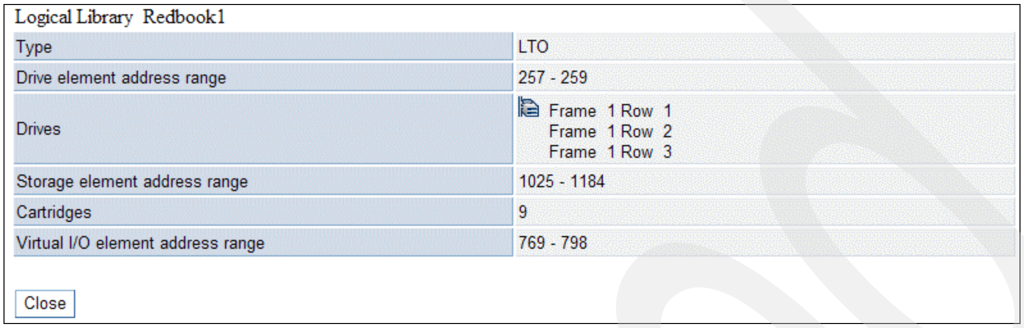
Logical Library Redbook1

Type	LTO
Drive element address range	257 - 259
Drives	Frame 1 Row 1 Frame 1 Row 2 Frame 1 Row 3
Storage element address range	1025 - 1104
Cartridges	9

Figure 2-65 Detailed information before ALMS is enabled

Then we enable ALMS.

In Figure 2-66 we again show the detailed view of the logical library. The drive element addresses are the same as before, but the storage element addresses were changed. Because it is seen as the first logical library, the storage element addresses begin with 1025. With ALMS, the physical limitation of 175 cartridge slots is removed, and we have assigned 160 slots to this one logical library. There is now also a listing of the default 30 Virtual IO elements.



Logical Library Redbook1

Type	LTO
Drive element address range	257 - 259
Drives	Frame 1 Row 1 Frame 1 Row 2 Frame 1 Row 3
Storage element address range	1025 - 1184
Cartridges	9
Virtual I/O element address range	769 - 798

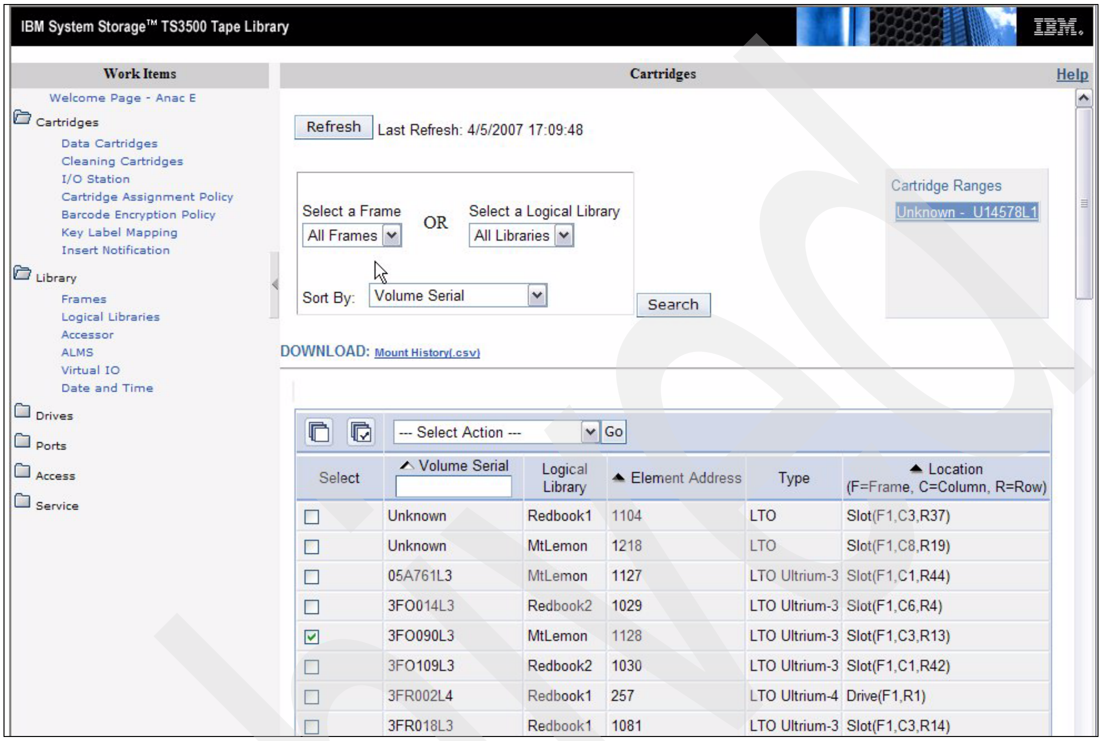
Figure 2-66 Detailed Information after ALMS enabled

2.3.4 Using ALMS

Because ALMS virtualizes the SCSI element addresses of the cartridge slots, some library commands do not generate a physical action on the library. If a move media command is issued the library replies with a new SCSI element address even though the cartridge was physically not moved.

Note: On i5/OS the SCSI element address is administered by the IOP and thus transparent for the user.

For example, suppose that we want to move the cartridge stored in Frame 1, Column 3, Row 13 (see Figure 2-67) from SCSI element address 1128 to a vacant SCSI element address. Use the menu selection **Cartridges** → **Data Cartridges**, and select from drop-down **Move** to move the cartridge.



IBM System Storage™ TS3500 Tape Library

Last Refresh: 4/5/2007 17:09:48

Select a Frame: All Frames OR Select a Logical Library: All Libraries

Sort By: Volume Serial

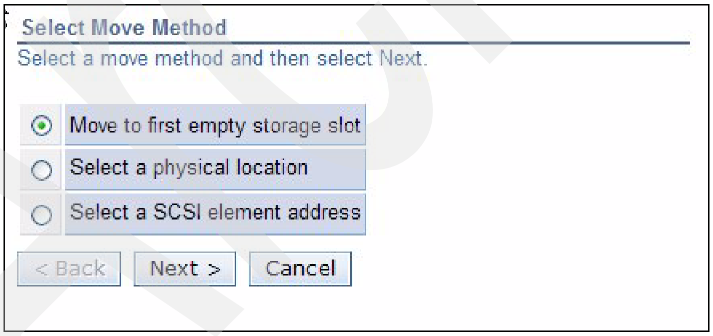
Cartridge Ranges: Unknown - U14578L1

DOWNLOAD: Mount History(.csv)

Select	Volume Serial	Logical Library	Element Address	Type	Location (F=Frame, C=Column, R=Row)
□	Unknown	Redbook1	1104	LTO	Slot(F1,C3,R37)
□	Unknown	MtLemon	1218	LTO	Slot(F1,C8,R19)
□	05A761L3	MtLemon	1127	LTO Ultrium-3	Slot(F1,C1,R44)
□	3FO014L3	Redbook2	1029	LTO Ultrium-3	Slot(F1,C6,R4)
☑	3FO090L3	MtLemon	1128	LTO Ultrium-3	Slot(F1,C3,R13)
□	3FO109L3	Redbook2	1030	LTO Ultrium-3	Slot(F1,C1,R42)
□	3FR002L4	Redbook1	257	LTO Ultrium-4	Drive(F1,R1)
□	3FR018L3	Redbook1	1081	LTO Ultrium-3	Slot(F1,C3,R14)

Figure 2-67 Inventory before move medium

A pop-up window lets you choose your move method. We select *first empty slot* as in Figure 2-68.



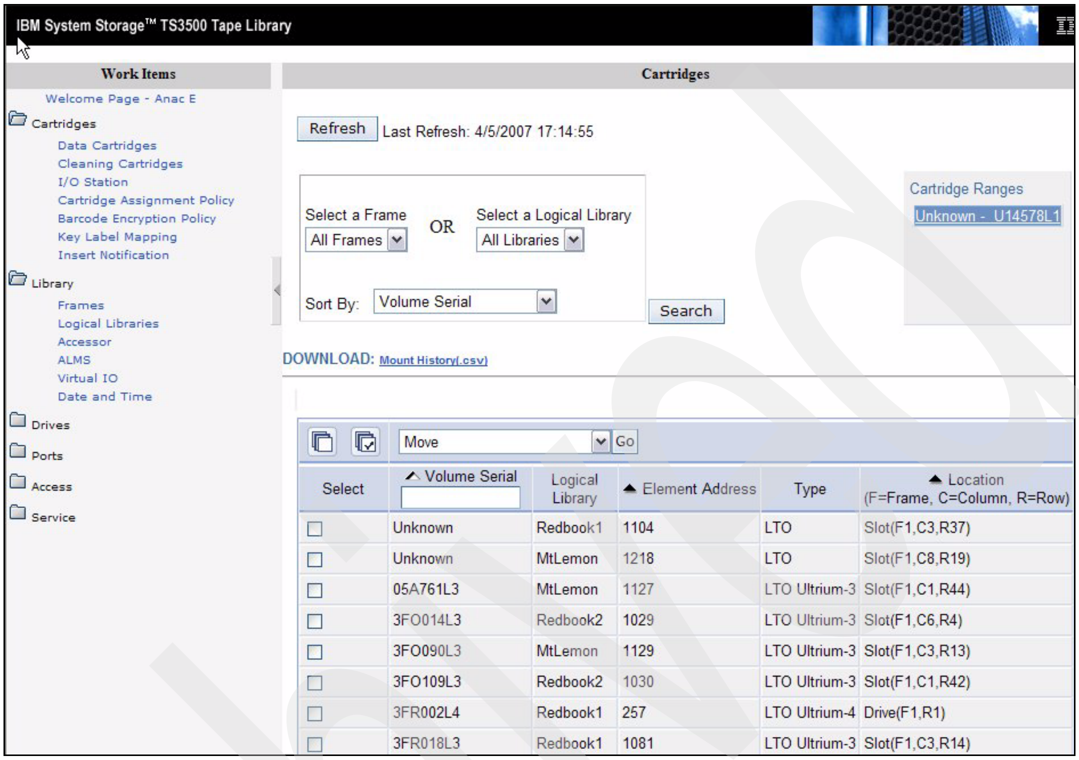
Select Move Method

Select a move method and then select Next.

● Move to first empty storage slot
○ Select a physical location
○ Select a SCSI element address

Figure 2-68 Select move method

Now, we again check the inventory of the library (see Figure 2-69). We see that the SCSI element address has changed to 1129, but the cartridge is still in the same physical location: Frame 1, Column 3, Row 13.



Last Refresh: 4/5/2007 17:14:55

Select a Frame: All Frames OR Select a Logical Library: All Libraries

Sort By: Volume Serial

Select	Volume Serial	Logical Library	Element Address	Type	Location (F=Frame, C=Column, R=Row)
□	Unknown	Redbook1	1104	LTO	Slot(F1,C3,R37)
□	Unknown	MtLemon	1218	LTO	Slot(F1,C8,R19)
□	05A761L3	MtLemon	1127	LTO Ultrium-3	Slot(F1,C1,R44)
□	3FO014L3	Redbook2	1029	LTO Ultrium-3	Slot(F1,C6,R4)
□	3FO090L3	MtLemon	1129	LTO Ultrium-3	Slot(F1,C3,R13)
□	3FO109L3	Redbook2	1030	LTO Ultrium-3	Slot(F1,C1,R42)
□	3FR002L4	Redbook1	257	LTO Ultrium-4	Drive(F1,R1)
□	3FR018L3	Redbook1	1081	LTO Ultrium-3	Slot(F1,C3,R14)

Figure 2-69 Inventory after moving cartridge

On a library without ALMS, you have to run a library inventory every time after moving some cartridges manually to get the application in a state consistent with the library. With ALMS this might no longer be required, as ALMS always tries to assign the same SCSI element address to the cartridge, even though the cartridge was moved manually.

Because ALMS is based on the affinity between VolSer (barcode label) and the reported SCSI element address, you have to make sure that the barcode label is readable. The library tries to keep the same SCSI element address for an unreadable barcode label if this cartridge is stored in the same physical slot. But, if the cartridge was moved manually, and the library does an inventory, a cartridge with an unreadable barcode label is placed in an unassigned status.

The same is true if you work with unlabeled cartridges (no barcode label). As long as you do not move this cartridge manually, the library tries to assign a SCSI element address. If you move such a cartridge manually, the cartridge is placed in an unassigned status.

The same happens with cartridges having duplicate barcode labels. Anyway, using duplicate barcode labels is generally not supported, and can easily lead to confusion.

It is possible that the storage capacity of the library, as reported by each logical library, might exceed the physical storage capacity of the library. As such, it is possible to run out of storage space while still reporting available space to a host. SNMP and operator panel messages notify the customer as the library approaches near full capacity. In addition, if cartridges are placed in the I/O station when a library has reached its capacity, the cartridges are marked inaccessible to all hosts to prevent the condition where the host tries to move the cartridge to storage that does not really exist.

When ALMS is enabled, auto clean is automatically enabled, and there is no mechanism to disable it. Cleaning cartridges are never associated to a logical library, so there is no host awareness that they exist in the library.

Static partitioning cannot be used when ALMS is enabled. The partitioning for the entire library is either static or dynamic.

3

Overview of the IBM System i platform

This chapter provides an introduction to the IBM System i server platform, primarily for those IT professionals with a storage background who are new to this platform.

Topics covered include:

- The unique architecture of the IBM System i platform, such as the Technology Independent Machine Interface
- Single-level storage
- Server consolidation
- Selected features of the i5/OS operating system, such as the integrated DB2® Universal Database™, journaling, the Integrated File System, and its server integration capabilities
- An IBM System i hardware overview and description of its tape I/O adapters

3.1 System i architecture

This section describes the main characteristics of the System i architecture.

3.1.1 System i I/O architecture

IBM System i servers are entirely designed for I/O intensive business computing. The latest POWER5+™ and POWER6™ microprocessor design and IBM System i unique processor hierarchy lay the foundation for an outstanding performance and scalability. Workload is offloaded from the CPU to dedicated input/output processors (IOPs) accommodated in I/O cards that fit into Peripheral Component Interconnect (PCI) type slots on the system buses.

The IOPs transfer data to/from main storage and control the input/output adapters (IOAs) which, for example, are the actual SCSI or Fiber Channel adapters for handling internal and external storage device communications. More and more new System i I/O adapters are now designed as IOP-less or smart IOAs which have the IOP functionality integrated into the IOA and Licensed Internal Code to achieve a higher package density with no PCI slot required anymore for an IOP.

The IBM System i^{TM} system busses are located in the Central Electronic Complex (CEC) and in optional expansion units (also known as I/O towers) connected via High-Speed-Link (HSL) copper or optical interfaces with which expansion units can be added concurrently to the system. With the POWER6 models, a new 12X loop technology has been introduced based on InfiniBand® technology offering up to 50% more bandwidth than previous HSL technology.

3.1.2 Technology Independent Machine Interface

A unique design going back to the early days of the System/38™ which sets the AS/400, iSeries and System i apart for other computer systems is the strict separation of *System Licensed Internal Code* (SLIC) and the operating system i5/OS by the *Technology Independent Machine Interface* (TIMI) shown in Figure 3-1.

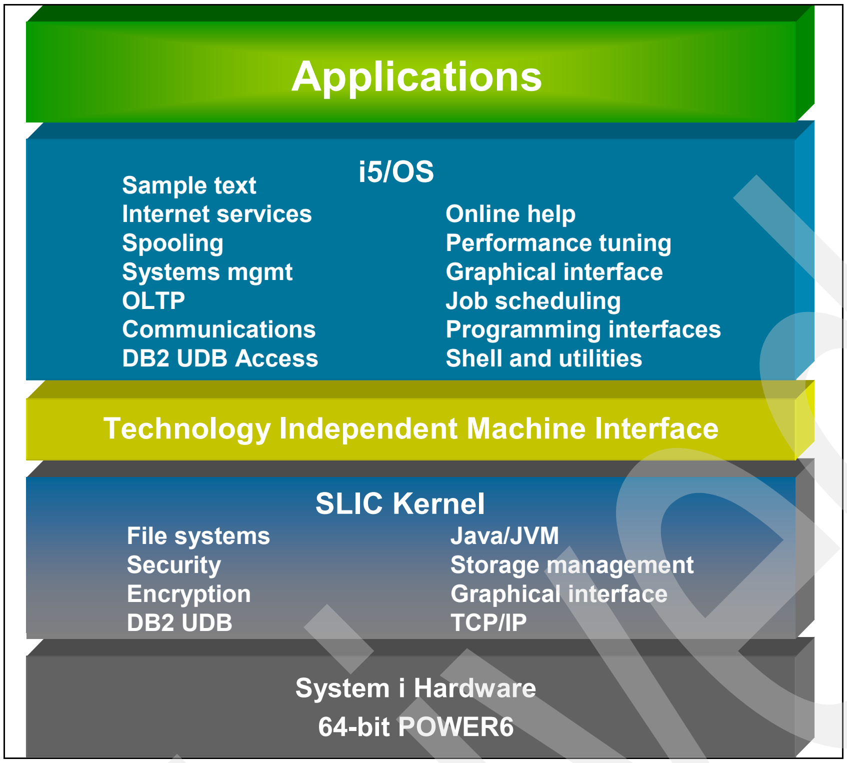


Figure 3-1 System i Technology Independent Machine Interface (TIMI)

This architecture makes both the i5/OS operating system itself and any user applications running above TIMI independent from any specific hardware implementation, which is completely being dealt with by SLIC. A classic example of the hardware independence was the transition from a 48 bit complex instruction set computing (CISC) to a 64 bit reduced instruction set computing (RISC) of the AS/400 in 1995 without requiring any recompiling or rewriting of user applications.

Clearly the benefits of the TIMI architecture are a very robust system design, because applications cannot directly communicate and therewith manipulate the hardware, as well as offering an excellent investment protection for any software applications being immune to underlying hardware changes.

3.1.3 Single-level storage

Another unique architecture of System i and its predecessors is the concept of single-level storage, shown in Figure 3-2.

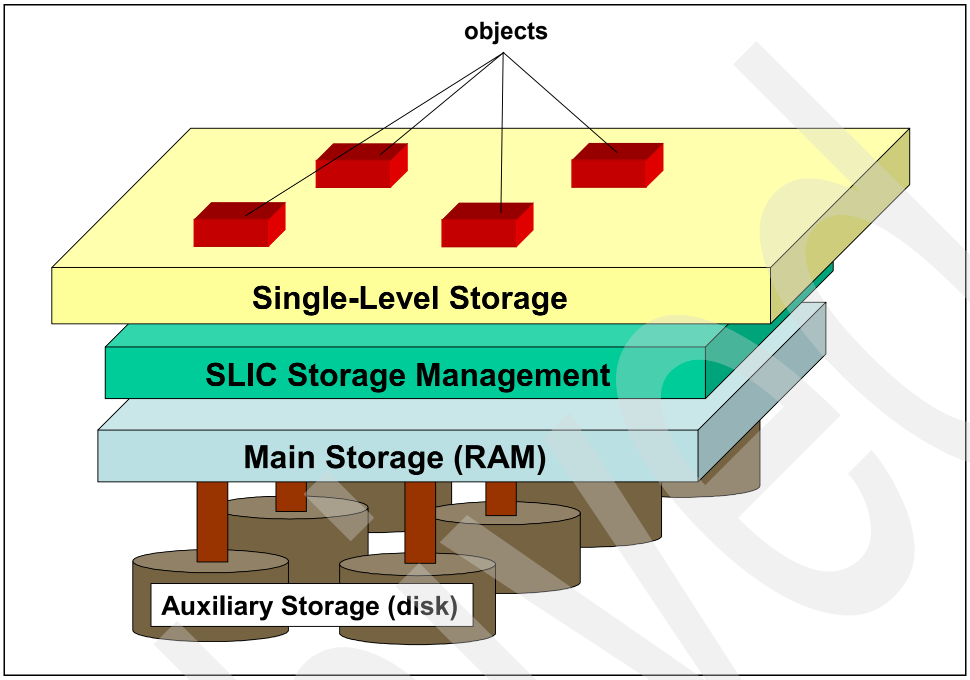


Figure 3-2 System i Single-Level Storage Architecture[1]

The knowledge of the underlying characteristics of storage hardware resides in the SLIC microcode layer, which uses a 64-bit address space for addressing both main memory and disk storage as a *single-level storage* space. The i5/OS operating system and applications on a System i server are completely unaware of the storage hardware characteristics because they are residing above TIMI and work with *virtual addresses*, which are 128-bit *MI pointers* containing the 64-bit single-level storage address and additional authority information.

The virtual address concept also makes i5/OS resistant to viruses, because any program trying to modify an integrity protected MI pointer immediately receives an exception. Also, by the virtual address concept, the system is already prepared to accommodate future 96-bit or 128-bit processors. To keep track of the unique virtual address for objects saved on disk, a 520 bytes per sector format is used with 512 bytes containing the actual user data and a 8-byte header used to save the virtual address spread across the eight headers of a 4K page.

System i application developers do not have to be concerned about main memory management with opening and closing files because, due to single-level storage, the whole System i main memory serves as a huge cache managed by SLIC storage management, which keeps objects in main memory or pages them out if no longer required. As every object has its unique virtual address, there is always only one instance of it, that is, each process using the object accesses it at its unique virtual address, and there is no necessity to have separate instances of an object loaded into memory for separate processes.

[1] Source: http://www-03.ibm.com/servers/enable/site/porting/iseries/overview/overview.html

Similarly, compared to other computer systems, disk storage administration for System i servers is almost effortless for System i administrators. This is so because, within the object-oriented i5/OS, there is no concept of filesystem spaces requiring to be managed, and the system automatically balances all data across the available disk units organized in an *auxiliary storage pool* (ASP).

For further information about the System i architecture, refer to:

- "*Fortress Rochester: The Inside Story of the IBM iSeries*" by Frank G. Soltis, 29th Street Press (2001), ISBN 1583040838

3.1.4 POWER Hypervisor architecture

The POWER™ Hypervisor™ is firmware that resides in flash memory on the System i server Service Processor. It performs the initialization and configuration of the System i hardware, as well as the virtualization support required to run up to 254 partitions concurrently on the System i servers.

Multiple operating systems are supported by the POWER Hypervisor to run on System i hardware which makes it an excellent platform for server consolidation. i5/OS, AIX 5L™, SuSE and Red Hat Linux for IBM POWER are supported natively in logical partitions (LPARs) on the System i platform. In addition to this POWER Hypervisor native LPAR support, like with the former AS/400 and iSeries Microsoft Windows Server or Linux is supported on the Integrated xSeries Server (IXS) and via Integrated xSeries Adapter (IXA) or iSCSI connected IBM xSeries or BladeCenter. The diverse System i operating system support is shown in Figure 3-3.

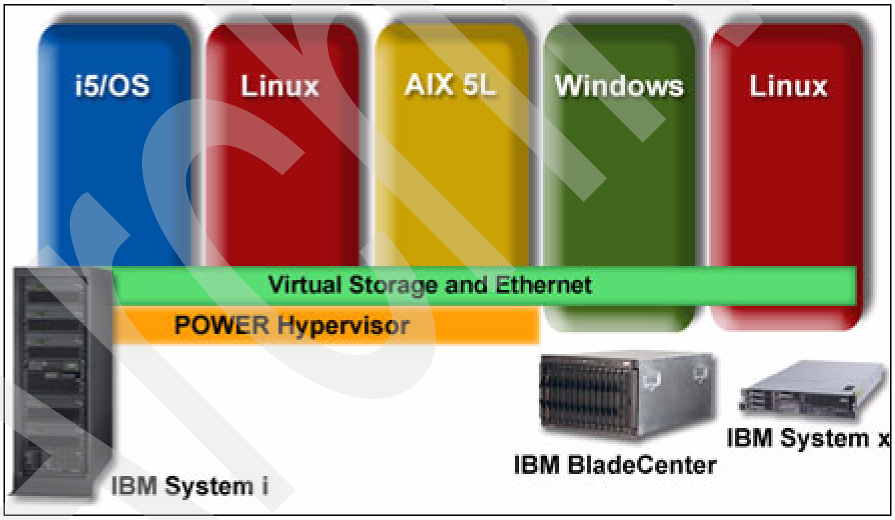


Figure 3-3 System i Server Consolidation[2]

The POWER Hypervisor also allows extensive dynamic and granular resource sharing of processors, memory, disk, tape, and other devices, including Virtual Ethernet and Virtual SCSI adapters across partitions. To illustrate these possibilities, for example, logical partitions can be defined with a minimum of a 0.1 share of one system processor, processors configured in an processor pool can be shared between partitions, disk storage space can be virtualized by Virtual SCSI adapters assigned to a server and client partition, tape adapters can be shared between partitions and dynamically be moved on a scheduled operation to another partition for running its backups.

[2] Source: http://www-03.ibm.com/systems/i/os

For more information about System i logical partitioning, refer to:

- *IBM Hardware Systems Information Center* section “Partitioning the server” at:

  http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp?topic=/iphat/iphatlparkickoff.htm

- “*Logical Partitions on System i5: A Guide to Planning and Configuring LPAR with HMC on System i*”, SG24-8000 at:

  http://www.redbooks.ibm.com/redbooks/pdfs/sg248000.pdf

3.2 System i hardware overview

The current System i server family comprises six models from the entry model 515 to the high-end model 595 as shown in Figure 3-4.

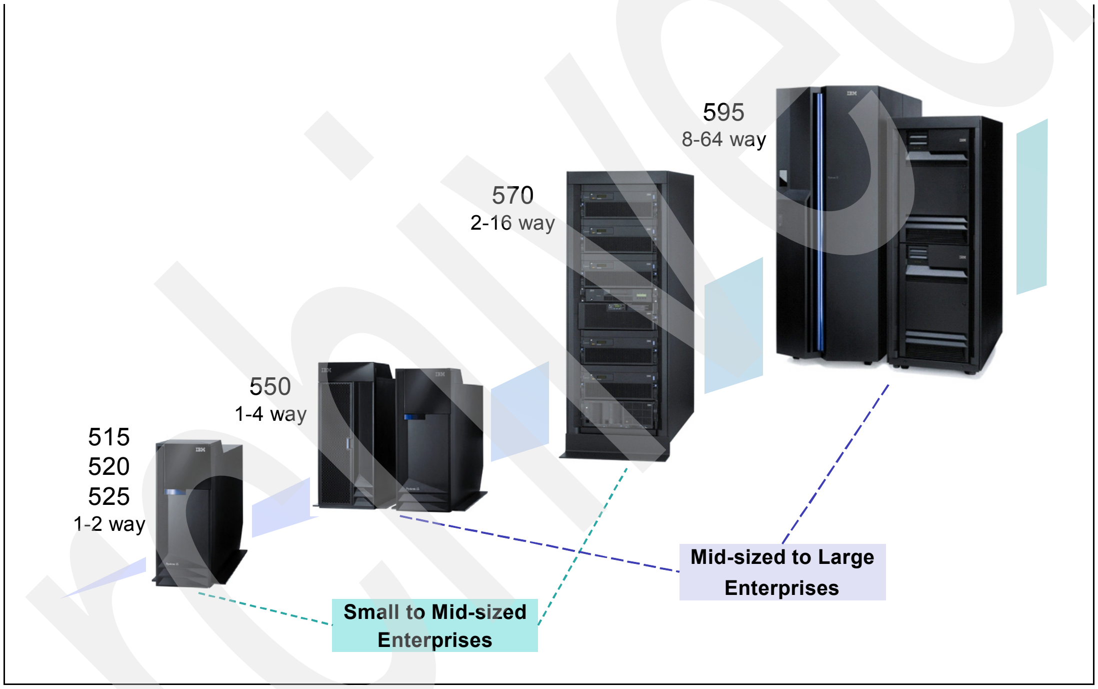

595
8-64 way
570
2-16 way
550
1-4 way
515
520
525
1-2 way
Mid-sized to Large Enterprises
Small to Mid-sized Enterprises

Figure 3-4 IBM System i Server Family

3.2.1 Server scalability

The System i server family provides an enormous range of scalability in both processor power and I/O capabilities. For example, the new POWER5+ entry models 515 and 525 Express provide up to unconstrained 7800 CPW in 2-way CPU configuration, the new POWER6 model 570 scales from 5500 CPW for the 1-way up to 76900 CPW for the 16-way CPU configuration and the high-end model 595 with 2*32-way CPUs provides 216.000 CPW.

Selected maximum system capabilities of current System i models are summarized in Table 3-1.

For more information about System i hardware configuration capabilities, refer to:

- *IBM System i Overview: Models 515, 520, 525, 570, 595, and More*, REDP-5052 at http://www.redbooks.ibm.com/Redbooks.nsf/RedpieceAbstracts/redp5052.html?Open

Table 3-1 Maximum System i system capacities

IBM System i	Model 515[a]	Models 520+ / 525[a]	POWER6 Model 570	Model 595+
Commercial Processing Workload (CPW)	3800 - 7100[b]	600 - 7100	8100 - 76900	8200 - 216000
Memory (max.)	16GB	32GB	768GB	2TB
Internal Disk Capacity (max.)	560GB	39TB	387TB	381TB[c]
Internal Disk Drives (max.)	8	278	1374	2700
I/O Loops (max.)	0	1	8	31
Expansion Towers (max.)	0	6	48	96
PCI Slots (max.)	6	90	692	1152
LPARs (i5/OS, AIX 5L or Linux - max.)	20	20	160	254
Integrated xSeries Servers (max.)	0	18	48	60
Integrated xSeries Adapters (max.)	0	8	57	57
iSCSI Adapters (max.)	5	21	168	125

[a] Models 515 / 525 are licensed for user-based pricing
[b] Constrained by limited number of disk arms
[c] Based on POWER5™ models assumed 141 GB max. drive capacity

These maximum system capabilities help in positioning and understanding the growth options for a selected System i server model. While they should be considered for sizing a System i external disk storage solution, such as for determining the available HSL bandwidth, they usually are not relevant for sizing System i tape storage solutions.

3.2.2 System i tape adapters

Attachment of high-performance external tapes such as LTO or 3592 to a System i server is accomplished either via a SCSI or a Fiber Channel I/O adapter (IOA) controlled by a *mandatory* I/O processor (IOP). Several System i IOAs for external tape attachment exist like the #2749, #5705, #5702, #5715, #5712 SCSI IOAs and the #2765, #5704 Fiber Channel IOAs, which are all withdrawn from marketing.

Currently only the #5736 PCI-X Ultra320 SCSI Disk/Tape Adapter and the #5761 4Gb Fiber Channel Tape Adapter are available for new orders.

The #5736 shown in Figure 3-5 is a dual bus Ultra320 SCSI adapter without write cache and without RAID support. It supports SCSI-connected tape, optical libraries, CD and DVD devices. From its two internal and two external LVD SCSI ports (VHDCI connectors), a combination of only up to two ports can be used due the two SCSI busses.

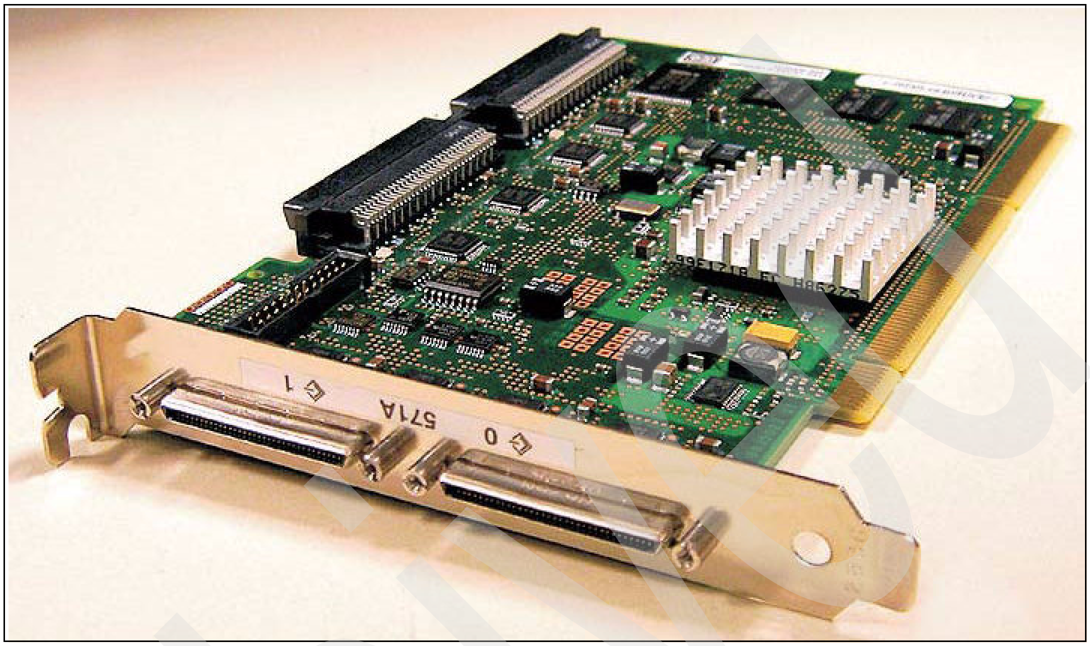


Figure 3-5 #5736 PCI-X Ultra320 SCSI Disk/Tape Adapter

The #5761 shown in Figure 3-6 is a single port Fiber Channel short form factor PCI-X 2.0 adapter supporting the Fiber Channel-Arbitrated Loop (FC-AL) and Fiber Channel-Switch Fabric (FC-SW) protocol with auto-negotiated speeds of 4Gb/s, 2Gb/s, and 1Gb/s and supported direct-connect distances up to 150m, 300m, and 500m.

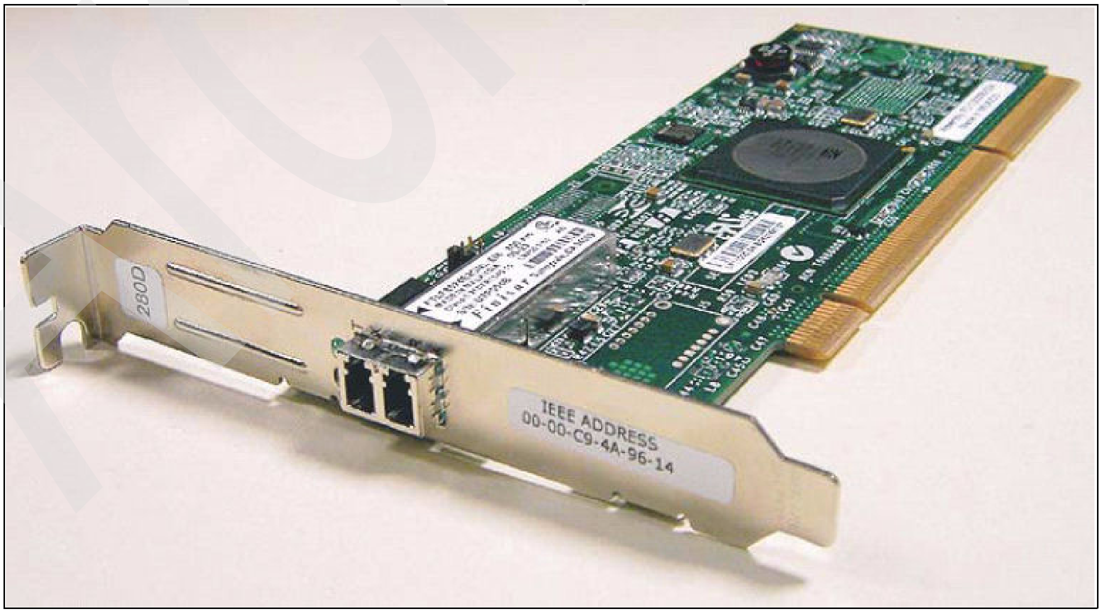


Figure 3-6 #5761 PCI-X 4Gb Fiber Channel Tape Adapter

For further details about the System i hardware, refer to:

- *IBM System i5 Handbook: IBM i5/OS Version 5 Release 4*, SG24-7486, at:

  http://www.redbooks.ibm.com/redpieces/abstracts/sg247486.html?Open

- *IBM System i5, eServer i5 and iSeries System Builder: IBM i5/OS Version 5 Release 4*, SG24-2155, at:

  http://www.redbooks.ibm.com/abstracts/sg242155.html?Open

- *IBM System i Overview: Models 515, 520, 525, 570, 595, and More*, REDP-5052, at:

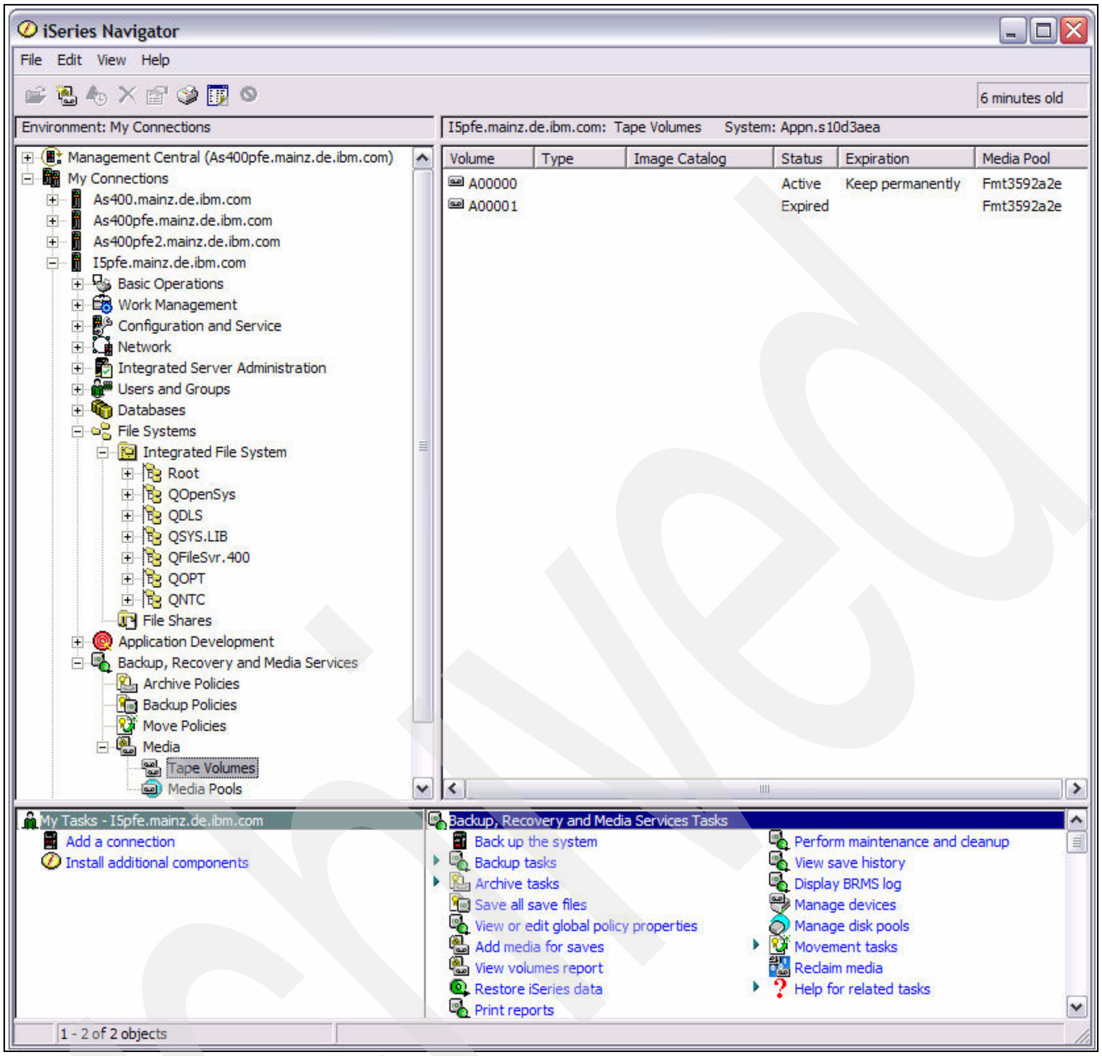
  http://www.redbooks.ibm.com/Redbooks.nsf/RedpieceAbstracts/redp5052.html?Open

3.3 System i5/OS overview

OS/400®, which has been renamed to *i5/OS* with Version 5 Release 3, is a 64-bit operating system that provides ease of implementation, management, and operation in one totally integrated object-oriented operating system. The benefit of this integrated approach is that all components such as system management, security, networking, internet services, the integrated DB2 Universal Database and SLIC hardware support functions are shipped as a fully integrated and tested solution so that System i customers do not have to be concerned about software incompatibility or hardware device driver support issues.

Selected i5/OS integrated features are as follows:

- Advanced *iSeries Navigator* GUI (see Figure 3-7) support to provide for:
  - Easy setup and management of the system, including TCP/IP functions
  - Database functions
  - User and printer job administration
  - System management
  - Software distribution
  - Performance monitoring
  - Centralized management of multiple systems
  - Plug-in support for Domino®, Backup Recovery and Media Services (BRMS), and others



Volume	Type	Image Catalog	Status	Expiration	Media Pool
A00000			Active	Keep permanently	Fmt3592a2e
A00001			Expired		Fmt3592a2e

Figure 3-7 iSeries Navigator GUI for Microsoft Windows clients

The iSeries Navigator nowadays is no longer just an alternative to the traditional System i 5250 terminal “green-screen,” because newer functions such as setup of independent Auxiliary Storage Pools (iASPs) actually require using the iSeries Navigator:

- Network computing
- *Integrated File System* (IFS) with industry standards:

  The IFS is a hierarchical directory structure that provides a common interface to support storing information in *stream files*, which are unstructured sequences of bytes stored in a file like known from PC and UNIX systems but also structured *database files*, documents, and other *objects* that are natively stored in *libraries* under i5/OS in the System i server.

  Figure 3-7 from the iSeries Navigator also shows the IFS directory structure with its common namespace supporting byte stream files stored under “Root” (/), a POSIX compliant case-sensitive filesystem under “QOpenSys”, i5/OS libraries, and objects stored under “QSYS.LIB” and Windows or Linux files from integrated Windows servers stored under “QNTC,” which enables file-level backup by i5/OS for these integrated servers.

- Multiple operating environments and logical partitions (LPARs):
  - Different versions and releases of i5/OS
  - Linux
  - AIX 5L
  - *Portable Application Solutions Environment* (PASE)
  - Resource sharing

  In addition to the support for native AIX 5L partitions on the IBM System i servers as outlined in "POWER Hypervisor architecture" on page 87 with PASE there is also an integrated runtime environment available for AIX applications under i5/OS. i5/OS PASE provides support for AIX shared libraries, shells and utilities. It runs on a System Licensed Internal Code (SLIC) kernel with direct processing of IBM PowerPC® machine instructions, so it does not have the drawbacks of an environment that only emulates the machine instructions.

- Clustering and shared resources:

  i5/OS natively supports clustering with up to 128 nodes in a cluster building the foundation for a System i high-availability solution. For using clustering with shared resources like independent Auxiliary Storage Pools the i5/OS option "HA Switchable Resources" is required.

- High system availability:

  High availability on i5/OS systems is implemented either using shared/switched *independent auxiliary storage pool* (iASP) resources in a cluster resource group, which can also be combined with storage system based physical data replication using the System i CopyServices Toolkit service offering or by using the i5/OS cross-site mirroring function (XSM) or by using logical replication software from an IBM HA business partner.

- Client/server connectivity
- DB2 Universal Database (UDB) for iSeries:

  Fully integrated into the system at no additional costs featuring journaling, distributed DB support, ODBC, JDBC™ connectivity and covering the core components of SQL 2003 standard DB2. Scalability in terms of performance is provided by the i5/OS option "DB2 Symmetric Multiprocessing," which allows multiple DB operations to be run in parallel on System i SMP systems.

- Transaction processing
- Batch processing
- Extensive run-time applications
- Openness standards
- PM eServer iSeries (performance modelling)
- Electronic Customer Support (ECS)
- Comprehensive security for system resources:

  i5/OS has extensive security features built-in, including different levels of object and data authorities, security auditing, intrusion detection, and different system-wide security level settings up to the Common Criteria CAPP/EAL4 security standard.

- Interfaces to system functions
- Connectivity to remote devices, systems, and networks
- Office services
- National language versions and multilingual support

- Comprehensive suite of application development tools:

  With IBM WebSphere® Development Studio (WDS), a comprehensive suite for application development is available for i5/OS supporting the native i5/OS Control Language (CL), COBOL, RPG and C/C++. The WDS client version for Windows also includes the IBM Web Facing Tool for source-code based transformation of 5250 applications into Web-enabled applications.

- IBM Java for i5/OS:

  Java applications utilize a JVM™ and Java compiler built into the i5/OS kernel (SLIC), which enables fast interpretation and execution of Java code on the System i servers. A class transformer enables the direct execution of Java on the system without the overhead of interpretation. The traditional 64-bit JVM supports JDK™ 1.3, 1.4, and 1.5, and with V5R4, an additional new 32-bit JVM for Java 5.0 with a smaller memory footprint was introduced.

- Backup Recovery & Media Services:

  Backup Recovery & Media Services (BRMS) is an i5/OS licensed program product, which is IBM's strategic solution for backup automation and media management with tape libraries on i5/OS systems. It supports policy-oriented setup and execution of archive, backup, recovery and other removable media-related operations. A BRMS network feature allows synchronization of policies and shared media inventories across multiple i5/OS systems. The traditional BRMS user interface is menu-driven, but a significant number of functions are GUI enabled through the optional BRMS iSeries Navigator plug-in (see Figure 3-7). For further information about BRMS, refer to Chapter 6, "Implementing tape with Backup Recovery and Media Services" on page 153

For further details about i5/OS features, refer to:

- *IBM System i5 Handbook: IBM i5/OS Version 5 Release 4*, SG24-7486, at:

  http://www.redbooks.ibm.com/redpieces/abstracts/sg247486.html?Open

- "*iSeries Information Center Version 5 Release 4*" at:

  http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp

4

Planning for IBM tape in i5/OS

In this chapter, we provide you with important planning information for sizing and implementing IBM tape systems with i5/OS. We describe the connectivity options and give you guidelines for connecting tape to i5/OS partitions and for sharing tape drives. In addition to general performance information, we also explain important factors that influence the overall throughput.

4.1 Prerequisites for tape with i5/OS

In this section we list required adapters, software level, and System i models for attachment of external tape drives.

4.1.1 Fibre Channel connection

Fibre Channel (FC) attachment of external tape devices to System i partition requires PCI-X Fibre Channel Tape Controller, feature number #5761.

The #5761 PCI-X Fibre Channel Tape Controller provides a 4 Gb/sec Single Port Fibre Channel PCI-X 2.0 adapter which attaches external tape devices. The #5761 is a 64-bit address/data, short form factor PCI-X adapter with an Lucent Connector (LC) type of connector.

Note: For more information about Fibre Channel connections and types of connectors, refer to *Introduction to Storage Area Networks,* SG24-5470.

The #5761 PCI-X Fibre Channel Tape Controller is supported on System i models 520+, 550+, 570+, 595 1.9 GHz, 520, 550, 570, 595, 800, 810, 825, 870, and 890.

The #5761 PCI-X Fibre Channel Tape Controller requires i5/OS version 5 Release 3 (V5R3) or later. Support for the #5761 PCI-X Fibre Channel Tape Controller is provided by i5/OS, it does not require you to install any driver.

Note: For more information about System i servers and i5/OS, refer to Chapter 3, "Overview of the IBM System i platform" on page 83.

Some customers with existing SAN configurations might want to connect external tape devices through the PCI-X Fibre Channel Tape Controller, feature #5704, although it is withdrawn from market since June, 2006. The #5704 PCI-X Fibre Channel Tape Controller provides 2 Gb/sec data rate.

The #5704 PCI-X Fibre Channel Tape Controller is supported on System i models 270, 520, 550, 570, 595, 800, 810, 820, 825, 830, 840, 870, 890, SB2, SB3, and 9411-100.

The #5704 PCI-X Fibre Channel Tape Controller requires i5/OS V5R2 or later. Support for the #5704 PCI-X Fibre Channel Tape Controller is provided by i5/OS or i5/OS, it does not require you to install any driver.

4.1.2 SCSI connection

SCSI LVD attachment of tape drives requires PCI-X Disk/Tape Controller with IOP, feature number #5736.

CI-X Disk/Tape Controller with IOP, feature #5736 requires minimum software level i5/OS V5R2.

Some customers with existing configuration of SCSI attached tape drives might want to connect external tape devices through one of the following controllers in System i partition, although they are withdrawn from market since June, 2006:

- PCI-X Tape/DASD Controller, feature number #5702
- PCI-X Tape/DASD Controller, feature number #5705
- PCI-X Tape/DASD Controller, feature number #5712
- PCI-X Tape/DASD Controller, feature number #5715
- PCI-X Disk/Tape Controller with IOP, feature number #5736

The listed SCSI adapters require minimum software level i5/OS V5R2.

4.1.3 Summary of required adapters and software

Table 4-1summarizes System i adapters and software level necessary to support different tape drives. Required adapters and software level for attaching a tape library depends on the tape drives installed in the tape library.

Table 4-1 System i prerequisites for tape drives

Tape drive	**SCSI LVD adapter featur**	**Min. SW level for SCSI LVD**	**Fibre Channel adapter feature**	**Min. SW level for Fibre Channel**
LTO3, TS1000				
3580 L33	#5736	i5/OS V5R2		
TS1030			#5761	i5/OS V5R3 i5/OS V5R3
TS2230	#5736	i5/OS V5R2		
3592, TS1100				
3592 J1A			#5761	i5/OS V5R3 i5/OS V5R3
TS1120			#5761	i5/OS V5R3 i5/OS V5R3
LTO4, TS100				
TS2340	#5736	i5/OS V5R2		
TS1040			#5761	i5/OS V5R3 i5/OS V5R3

> **Note:** We recommend that you install the latest Cumulative PTF package on System i, and also upgrade firmware on tape drive or tape library to the latest level, before connecting it to a System i partition.
>
> Later in this chapter, we refer to the #5704 PCI-X Fibre Channel Tape Controller and the #5761 PCI-X Fibre Channel Tape Controller, as *FC adapter*. However, if a subject refers to only one of them, we also note the feature number, for example: FC adapter #5761.

4.2 Guidelines for connecting tape to a System i partition

In order to properly plan tape drives and tape libraries for i5/OS, it is important to know the rules that apply when attaching Fibre Channel tape drives to a System i partition and the characteristics of such attachments.

The following guidelines apply when connecting Fibre Channel tape drives and tape libraries to System i:

- Fibre Channel connection protocols and speed
- Connecting more than one device per FC adapter
- Maximum one path visible to I5/OS for any tape drive
- Library control path enabled for each FC adapter in System i partition
- Extended distance
- Configuring an FC attached tape drive as an alternate IPL device
- Placement of adapters in System i partition

Next we describe each of the listed guidelines.

Fibre Channel connection protocols and speed

OS/400 and i5/OS support Switched Fabric, Arbitrated Loop, and Point to Point Fibre Channel protocols. We can connect tape drives to a System i FC adapter directly or via SAN switches.

When a tape drive is connected directly or via switches, FC adapter #5761 auto-negotiates for the highest data rate between adapter and an attaching tape device at 1 Gb/sec, 2 Gb/sec or 4 Gb/sec of which the device or switch is capable. So the achieved data rate between System i FC adapter and a tape drive is limited to the lowest bandwidth of FC adapter, switch, or tape drive. For example:

- An IBM TS1120 Tape Drive is connected to the FC adapter #5761 in a System i partition via a switch capable of 4 Gbps data rate. Because both tape drive and a switch provide a 4 Gbps data rate, the FC adapter auto-negotiates this data rate. 4 Gbps is the actually achieved bandwidth of this attachment.
- However, if the same tape drive is connected to 4 Gbps FC adapter via 2 Gbps switch, the achieved data rate is 2 Gbps.

Connecting more than one device per FC adapter

With System i and Fibre Channel connected tape devices, an *initiator* means a System i Fibre Channel adapter for tape, and a *target* means a Fibre Channel port on a tape drive in a tape library, or a Fibre Channel port on a standalone tape drive.

With i5/OS V5R2 and later, you can have multiple targets and up to 16 devices per one System i Fibre Channel tape adapter.

Although it is technically possible to connect up to 16 tape drives to an System i FC adapter, we recommend, for performance reasons, to connect only a few of them. We suggest that you connect to one FC adapter only such an amount of tape drives that the sum of their maximal data rates does not exceed the available bandwidth of an FC adapter. This way, we can ensure that every connected tape drive achieves its best performance. For example:

- FC adapter #5761 provides a bandwidth of approximately 400 MB/s when appropriately placed on the bus to achieve maximal performance. TS1120 attached through this FC adapter achieves a maximal data rate of approximately 250 MB/s. So you might want to plan one TS1120 per FC adapters #5761 to enable maximal performance of the drive.

- However, if you do not expect to achieve this high data rate with your System i workload, you can plan two TS1120 to connect to one FC adapter #5761.

For more information about achieved tape data rates with different System i workloads, refer to 4.3, “Performance” on page 100.

Maximum one path visible to i5/OS for any tape drive

i5/OS supports one path to a tape device. Configurations in i5/OS must have only one path from a System i partition to any tape device.

Even if a tape library with control or data path failover capability is connected to System i partition, it does not make sense to connect the same tape drive via multiple System i FC adapters to achieve failover and load balancing, since i5/OS does not support multiple paths to the same tape drive.

> **Note:** For more information about control and data path failover in a tape library, refer to the *IBM System Storage Tape Library Guide for Open Systems*, SG24-5946.

Library control path enabled for each FC adapter in System i partition

Every FC adapter must see at least one tape drive that has a tape library control path defined. the control path is used by the tape adapter to send commands to the library, such as: insert a data cartridge into the tape library, eject a data cartridge out of the tape library, mount a data cartridge on a tape drive in the tape library, etc.

> **Note:** For more information about control and data path failover in a tape library, refer to the *IBM System Storage Tape Library Guide for Open Systems*t, SG24-5946.

Extended distance

The maximal supported distance between FC adapter #5761 and a direct attached tape device or a switch depends on the achieved data rate. Following are maximal distances at different data rates:

- 500 meters at a data rate of 1 Gb/sec
- 300 meters at a data rate of 2 Gb/sec
- 150 meters at a data rate of 1 Gb/sec

To provide tape attachments to longer distance, switches and long wave Fibre Channel cables are used. Each FC adapter #5761 and a tape device are connected short wave to a switch, and between the switches, a long wave connection is established, as is shown in Figure 4-1. With such a configuration we achieve distances up to 10 km.

For connecting a tape drive to even longer distance, switches and Dense Wavelength Division Multiplexingor (DWDMs) or Directors are used, usually with dark fibre connection, or connection over IP network, as is shown in Figure 4-1. With such a configuration, we can connect a tape drive to a System i partition at a distance of up to 100 km.

> **Note:** For more information about required devices to enable data rate to long distances, refer to *Introduction to Storage Area Networks*, G24-5470.

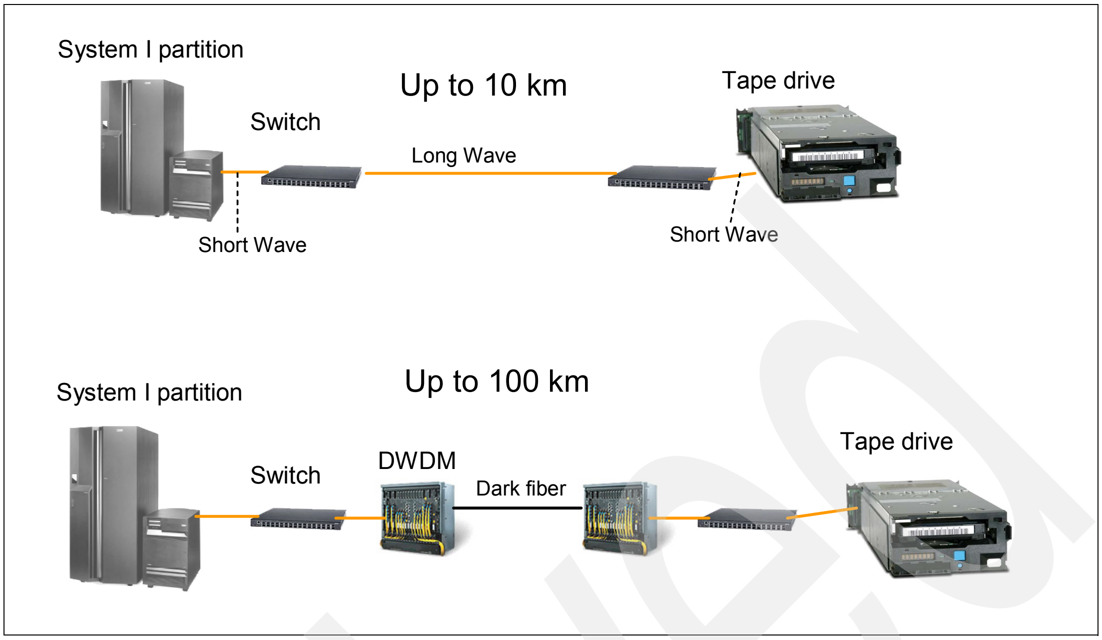


Figure 4-1 Remote tape

Configuring an FC attached tape drive as an alternate IPL device

In i5/OS, initial program load (IPL) uses programs that are stored on the primary IPL load source, which is typically a disk drive. Sometimes it is necessary to perform an IPL from another source, such as programs that are stored on tape. To do this, you must use IPL from the alternate IPL load source. Typically, alternate IPL must be done at i5/OS installation or a recovery procedure, or when IPl from disk fails.

Alternate IPL is not supported with Fibre Channel attached tapes drives; instead you should use *Alternate installation device support* when it is required to IPL from an FC connected tape drive. With alternate installation device function, the system is first loaded from a CD or DVD device. After enough of the Licensed Internal Code required to perform IPL is loaded, the system restore continues from the data cartridge on the alternate installation device.

For more information about alternate installation support, refer to *iSeries Backup and Recovery*, SC41-5304. More information about load source can be found in Chapter 3, “Overview of the IBM System i platform” on page 83.

4.3 Performance

Performance of a tape drive is becoming more and more important for a System i customer. With increasing business and spreading branches across the world, companies can afford less and less downtime of their business applications. The application outage required for daily save of the database library, or weekly save of the entire system, should be as short as possible. Also, they expect to quickly restore a database file, a library, or the entire system, to interrupt the working of critical applications as little as possible. Therefore durations of save and restore are critical factors for good IT support of the company’s business.

When designing their backup strategy, the customers should be aware about the duration of save and restore that they can expect from a particular tape drive. With System i customers, these performances depend very much on the type of workload being saved. For example, a save of many small files in the System i Integrated File System (IFS) can last much longer than doing a save of one big database file of the same capacity.

4.3.1 Workloads for measurement

To provide customers an estimation of tape performances with their systems, System i development performs regular measurements of save and restore on different types of workload, which are considered to be typical for i5/OS. Following are some of the measured workloads:

User Mix User Mix 3GB, User Mix 12GB: The User Mix data is contained in a single library and made up of a combination of source files, database files, programs, command objects, and so on. User Mix 12GB contains 49,500 objects and User Mix 3GB contains 12,300 objects.

Source File Source File 1GB: There are 96 source files with approximately 30,000 members.

Large Database File Large File 4GB, 32GB, 64GB, 320GB: The Large Database File workload is a single database file. The members in the 4GB and 32GB files are 4GB in size. The Members in the 64GB and 320GB files are 64GB in size.

For more information about i5/OS database files and members, refer to Chapter 3, “Overview of the IBM System i platform” on page 83.

A customer’s workload typically consists of different types, so we usually cannot estimate it with only one measured workload. When estimating duration of save and restore of the entire system, the best approximation might be somewhere between User Mix and Large Database Files.

4.3.2 Factors that influence performance

Performance of save and restore operations do not depend only on tape drive data rate, but also on other resources in System i partition.

Enough *processor power* should be provided to the System i partition where the save is performed, to fully utilize the tape drive speed. For User Mix workload, plan about 1.3 processors in the System i partition per one LTO3 tape drive.

It is also important to provide *enough disk arms* for save and restore operations to fully utilize the tape drive. Consider a minimum of 40 disk arms for save and restore of the Large Database File operations to the LTO3 drive, and consider a minimum of 50 disk arms to fully utilize LTO3 tape drive at the User Mix workload.

4.3.3 Measured performance

The charts in Figure 4-2 and Figure 4-3 show data rates of LTO3 and TS1120 tape drives for System i for the Large Database File workload and a User Mix workload. The measurements were done on a System i5™ Model 570 with 4 processors, and 180 15K rotation per minute (rpm) disk units in Raid-5. On the charts, you can observe the difference between connecting LTO3 and TS1120 drives via 2 Gbit System i adapter #5704 and 4 Gbit System i adapter #5761.

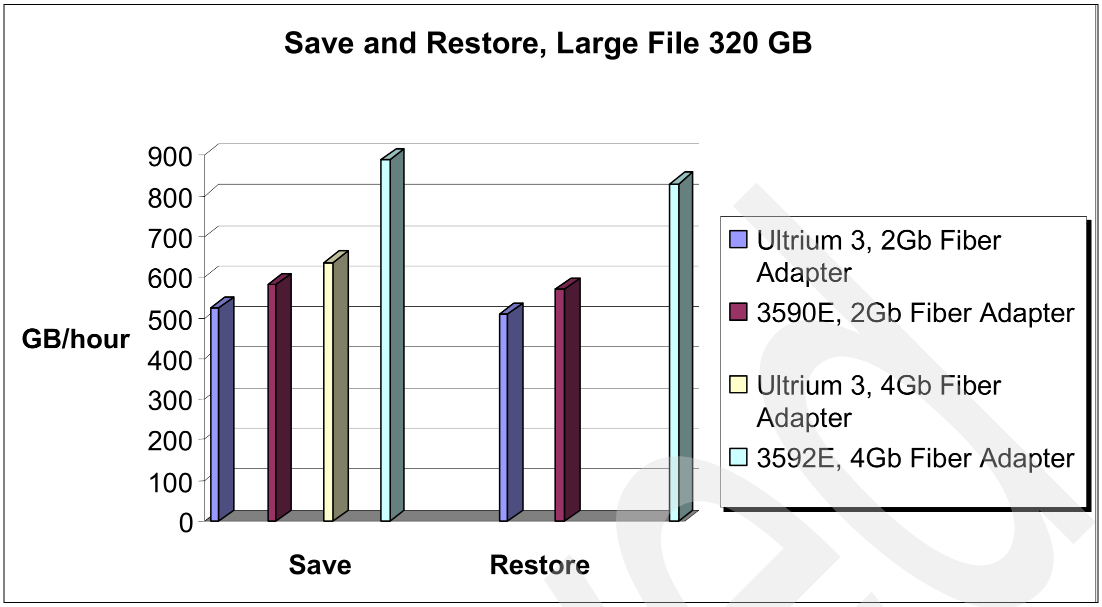


Figure 4-2 LTO3 and TS1120 performance - Large Database Files

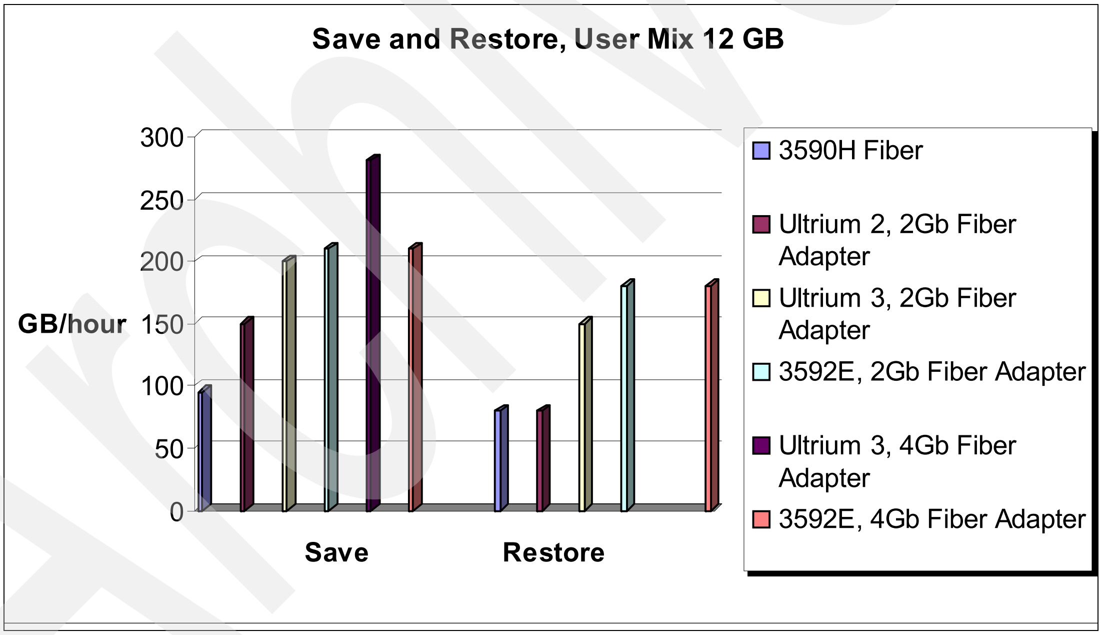


Figure 4-3 LTO3 and TS1120 performance - User Mix

As you can observe on the forgoing charts, both LTO3 and TS1120 perform with a much higher data rate when saving or restoring Large Database Files compared to User Mix. The TS1120 connected through 4 Gbit adapter #5761 achieves about a 30% to 50% higher rate than any other measured tape drive. With a User Mix, however, LTO3 connected via 4 Gbit adapter achieves about 25% to 30% higher data rate than the TS1120.

Note: Presently we have available measurements of LTO3 via 4 Gbit adapter only of save; measurements of restore are still to be completed.

4.4 Parallel and concurrent save and restore

In order to reduce the save window (the time required to save one or multiple objects to a tape) it is possible to use an i5/OS functionality to save a single object or library to multiple tape devices at the same time. When you save to multiple devices you can use one of the following two techniques:

Parallel save The ability to save or restore a *single object,* database library or IFS directory across *multiple tape devices* from the *same* i*5/OS job*. Parallel save provides the most significant improvement to customers with Large Database Files.

Concurrent save The ability to save and restore *different objects* from a single database library or IFS directory to *multiple tape devices,* or different database libraries or IFS directories to multiple tape devices at the same time *from different jobs*. Concurrent save provides significant improvements when saving typical customers' workloads.

For more information about different System i workloads, refer to 4.3, "Performance" on page 100.

Concurrent operations to multiple tape devices probably are the preferred solution for most customers. The customers must weigh the benefits of using parallel verses concurrent operations for multiple backup devices in their environment.

When planning for parallel save and restore, you might want to estimate the improvement from this as compared to traditional save and restore. Since performance of parallel and concurrent save depends very much on the particular workload, the most reliable way to estimate it is to test it by saving the customer's critical application.

However, some customers are not able to test parallel or concurrent save and restore of their production workload prior to implementing it. For such customers, you can do a rough estimation by using the performance measurements of typical workloads that were tested in System i development. The graphs in Figure 4-4 and Figure 4-5 show save and restore data rates for one LTO2 tape drive comparing to rates of parallel and concurrent save and restore to 2, 3 and 4 LTO2 tape drives.

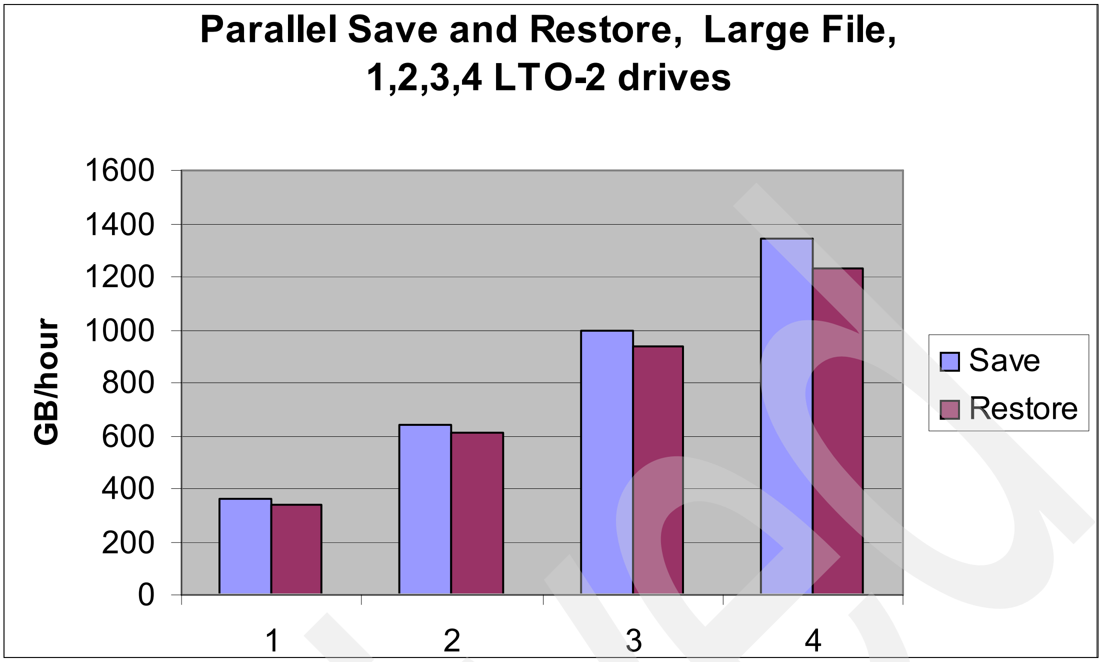


Figure 4-4 Parallel save and restore of Large Database Files

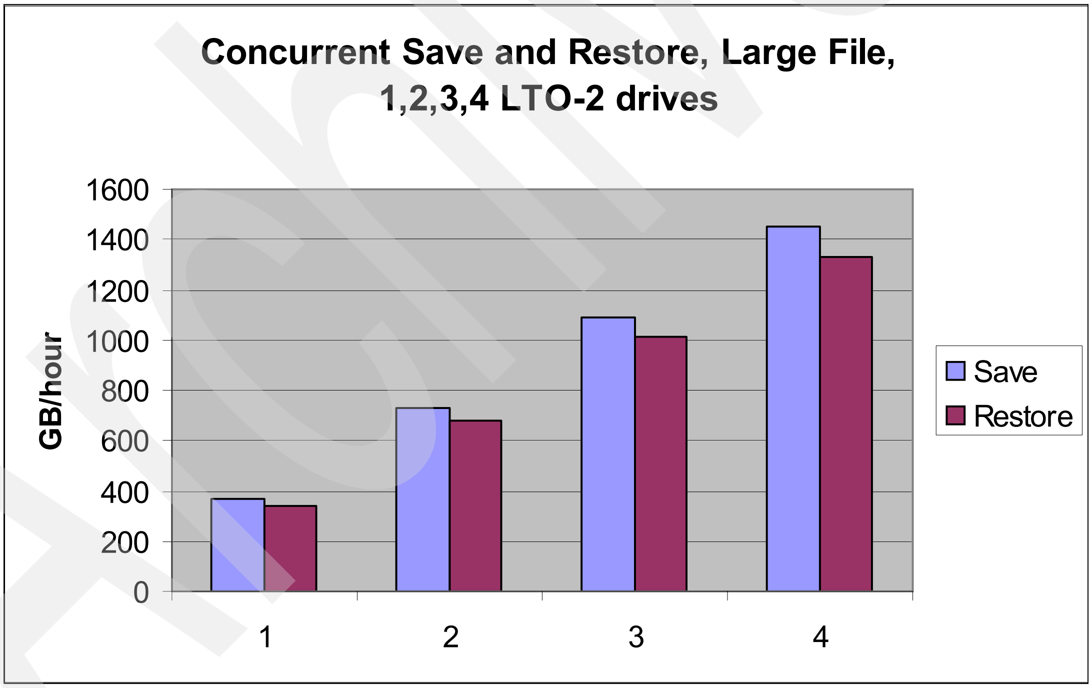


Figure 4-5 Concurrent save and restore of Large Database Files

More information about measurements of parallel save and restore can be found in the publication, *System i Performance capabilities Reference i5/OS Version 5 release 4,* available on the following Web site:

http://www-03.ibm.com/servers/eserver/iseries/perfmgmt/resource.html

When you plan to parallel or concurrent save and restore, it is essential to plan also for a tracking mechanism to, for recovery purposes, know what objects are on what data cartridges. Such function is provided by Backup Recovery and Media Services (BRMS). For more information about BRMS refer to Chapter 6., “Implementing tape with Backup Recovery and Media Services” on page 153.

4.5 Optimum block size and compression

When saving System i data, you can specify save options for improving performances, these options being Optimum block size, compression, and compaction, as described here:

USEOPTBLK Using optimum blocksize (save option USEOPTBLK) is designed to achieve better save performance, because you can specify the option USEOPTBLK with save operation. When using USEOPTBLK, the system sends larger blocks of data to tape devices that can take advantage of larger block sizes. With using larger blocks, less blocks are sent to the tape device for transferring the same amount of data, consequently less overhead in FC adapter and tape device is experienced. Different values can be specified for USEOPTBLK. When using this option with the value *YES, that is, USEOPTBLK(*YES), the usual results are significantly lower System i CPU utilization, and the backup device performs more efficiently.

DTACPR Data compression (save option DTACPR) is the ability to compress strings of identical characters and mark the beginning of the compressed string with a control byte. Strings of blanks from 2 to 63 bytes are compressed to a single byte. Strings of identical characters between 3 and 63 bytes are compressed to 2 bytes. If the backup device does not support data compaction, the system software can be used to compress the data. Different values can be specified for DTACPR. When using this option with the value *DEV, that is, DTACPR(*DEV), hardware compaction is performed if the tape device supports hardware compaction, otherwise no data compression is performed.

COMPACT Data compaction (save option COMPACT) is the same concept as software compression but available at the hardware level. Different values can be specified for COMPACT. When using value *DEV, that is, COMPACT(*DEV), device data compaction is performed if the tape device supports compaction.

We recommend that you use the following values for the listed options:

- USEOPTBLK(*YES)
- DTACPR(*DEV)
- COMPACT(*DEV)

With such usage, larger block sizes are used for transferring data to the tape device, and hardware compaction is used on the tape device if the device supports it.

4.6 Sharing a tape drive

Using SAN switches enables you to share one or more tape drives among multiple System i partitions. System i partitions can share a standalone Fibre Channel (FC) attached tape drive or an FC attached tape drive in a tape library. Each System i partition sees all tape drives that are connected for sharing.

Note: When connecting a tape drive to multiple System i partitions via switches, place System i adapters and the tape drive in a separate zone in the switch.

Sharing of a drive by different System i partitions is managed with a Reserve/Release function. The first partition to issue the reserve can use the drive until it issues the release. The other host receives a response that the drive is reserved elsewhere, until the drive is released by the first partition. When the drive is released, it can be reserved by the other host. For the System i server, the Reserve/Release function is a part of the device vary on or off, or the allocate/deallocate function of the library resource.

Figure 4-6 shows sharing of tape drives in a tape library between two System i partitions. Two tape drives are connected to one FC adapter in each System i partition. Each partition sees all 4 tape drives in the tape library.

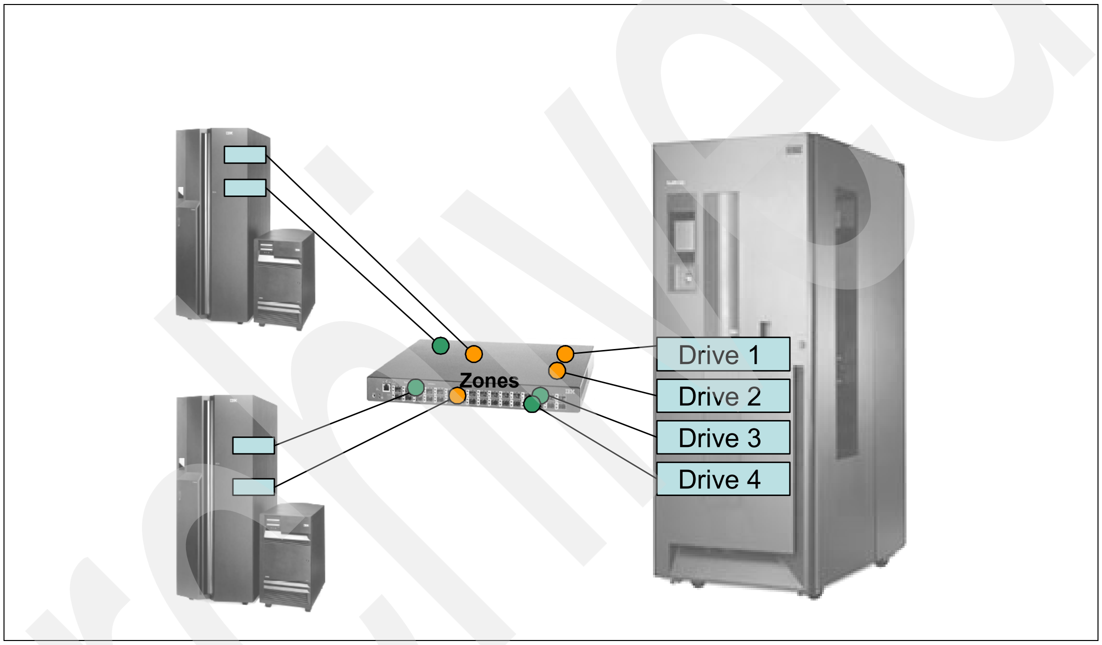


Figure 4-6 Sharing tape drives among System i partitions

A tape drive can be shared between a System i partition and another than System i server, as well. Also, in this case, sharing is done by reserve/release functionality.

5

Setup for IBM tape in i5/OS

In this chapter, we describe the basic setup steps required to implement a SCSI tape drive and a Fibre Channel Tape Library with i5/OS. We also explain how to share tape drives between multiple partitions. Last but not least, we explain how to use i5/OS commands to save and restore an i5/OS Database library.

5.1 Basic setup

In this section we describe the required actions to set up a tape drive or tape library for use with i5/OS. These actions include setup on the Tape device itself as well as setup in the System i partition and i5/OS.

We describe setup for the following configurations:

- Stand-alone SCSI tape drive connected to a System i partition
- Fibre Channel tape library connected to a System i partition

5.1.1 Stand-alone SCSI tape drive

In the following sections, we describe actions required to set up a SCSI attached tape drive for i5/OS.

Setting up the tape drive and connecting it to the System i partition

i5/OS recognizes the tape drive as soon as it is physically connected to the System i partition, as the hardware resource. A correct and properly attached resource is reported in i5/OS as *operational*. In case a tape drive is physically damaged or not correctly connected to the System i partition, the corresponding tape resource does not report it at all, or reports it as *failed*.

The tape resource must be described as a device in i5/OS in order to be able to perform save and restore operations. If the i5/OS system value *QAUTOCFG* is set to *On*, i5/OS automatically configures any new device as soon as it is attached to the system: i5/OS automatically creates the necessary device description for any device that is operational. However, if system value *QAUTOCFG* is set to *Off*, you have to create a device description for any new device attached to the system.

When automatic configuration is set to On by system value QAUTOCFG, i5/OS determines the names for new devices, based on the specification in system value QDEVNAMING. If system value QDEVNAMING is set to *NORMAL, the tape devices are automatically assigned names TAP01, TAP02, and so on. These device names can later be renamed to a name that is more helpful for users.

We recommend to check both:

- Hardware resource of tape device
- Device description of tape device

To check that a tape drive reports as an operational hardware resource, you can use i5/OS iSeries Navigator (i5/OS Graphical User Interface), or in i5/OS System Service Tools (SST) or Dedicated Service Tools (DST) — i5/OS environments to perform hardware managing and debugging activities.

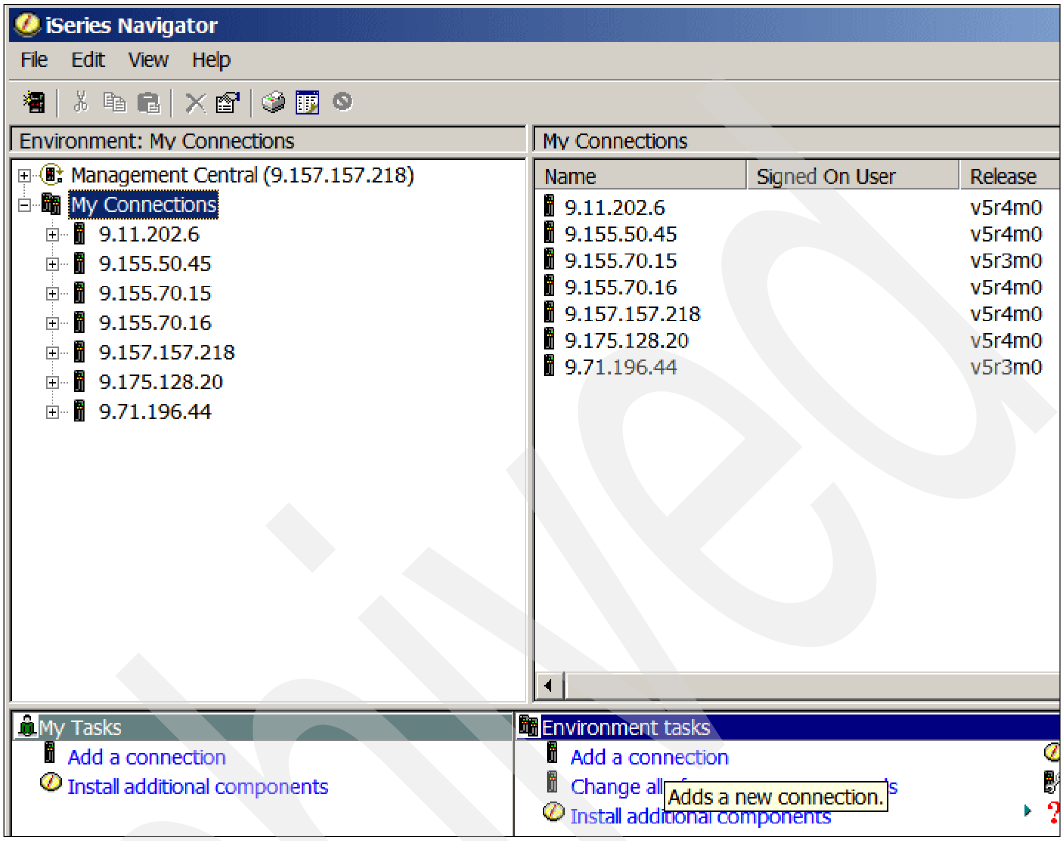
To see the description of a tape drive, you can use iSeries Navigator or the i5/OS green screen command line interface.

To check the status of a tape drive resource, and the device description in i5/OS via iSeries Navigator, perform the following steps:

1. Install part of the i5/OS licensed product *iSeries Access for Windows* on your PC. For instructions on how to do this, refer to System i Information Center at the Web site:

   http://publib.boulder.ibm.com/iseries/

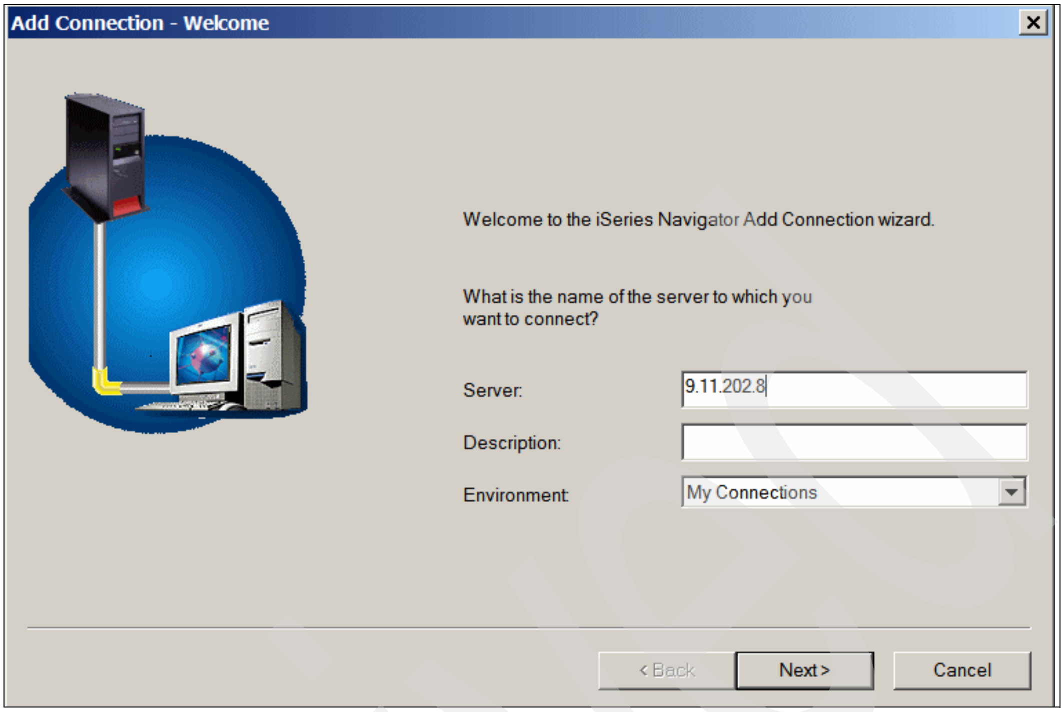
2. After iSeries Access for Windows is installed on your PC, click the iSeries Navigator icon. You are presented the Operations navigator window; part of it is shown in Figure 5-1. Go to Environment tasks and click **Add Connection**.



Name	Signed On User	Release
9.11.202.6		v5r4m0
9.155.50.45		v5r4m0
9.155.70.15		v5r3m0
9.155.70.16		v5r4m0
9.157.157.218		v5r4m0
9.175.128.20		v5r4m0
9.71.196.44		v5r3m0

Figure 5-1 Operations Navigator

3. By clicking **Add connection**, you bring up the Connection wizard, as shown in Figure 5-2. Insert the IP address or fully qualified host name of the System i partition you want to connect to and click **Next**.



Add Connection - Welcome

Welcome to the iSeries Navigator Add Connection wizard.

What is the name of the server to which you want to connect?

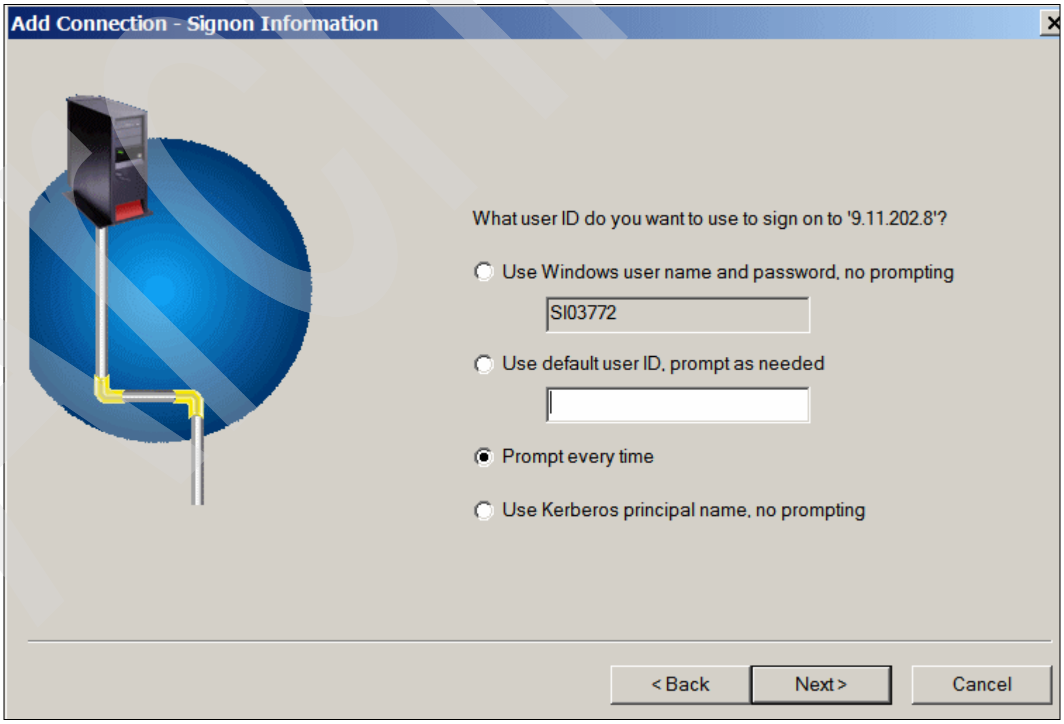
Server: 9.11.202.8

Description:

Environment: My Connections

Figure 5-2 iSeries Navigator - add connection

4. On the next wizard window, specify the System i User ID to connect, or instruct the iSeries Navigator to prompt for an ID every time it connects to the system. This is shown in Figure 5-3. Click **Next**.



Add Connection - Signon Information

What user ID do you want to use to sign on to '9.11.202.8'?

○ Use Windows user name and password, no prompting

SI03772

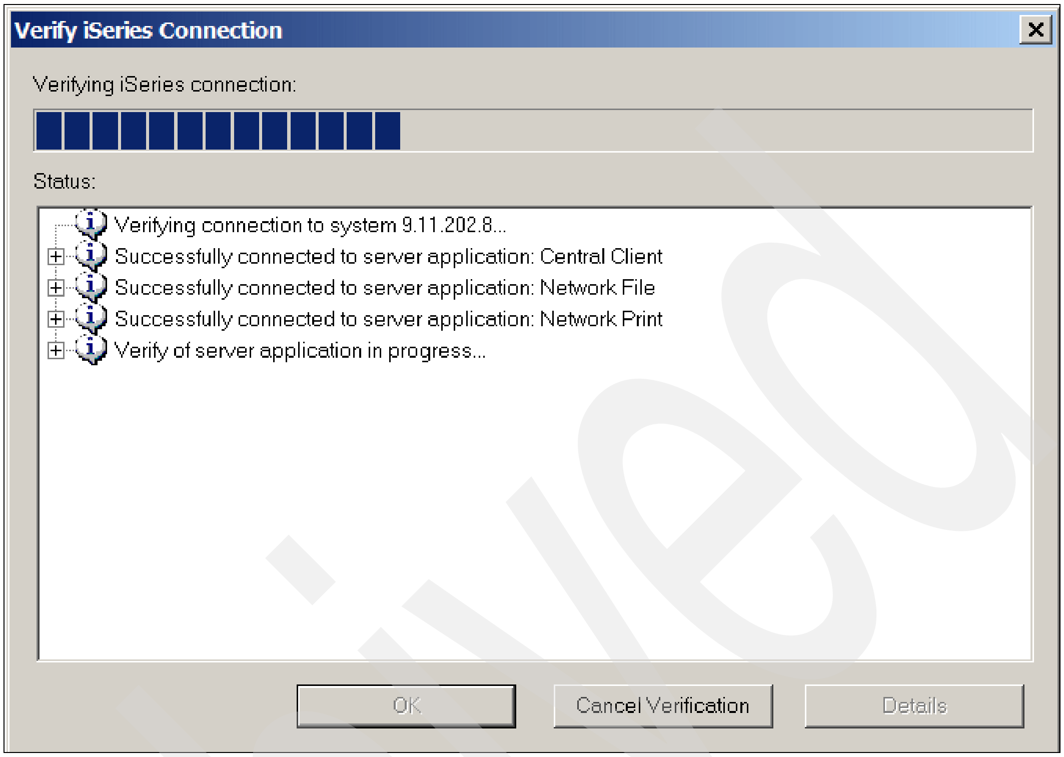
○ Use default user ID, prompt as needed

● Prompt every time

○ Use Kerberos principal name, no prompting

Figure 5-3 iSeries Navigator - Userid for connecting to System i partition in

5. On the window that appears next, click **Verify connection**. iSeries Navigator performs verification of the connection to the System i partition, as shown in Figure 5-4.



Verify iSeries Connection

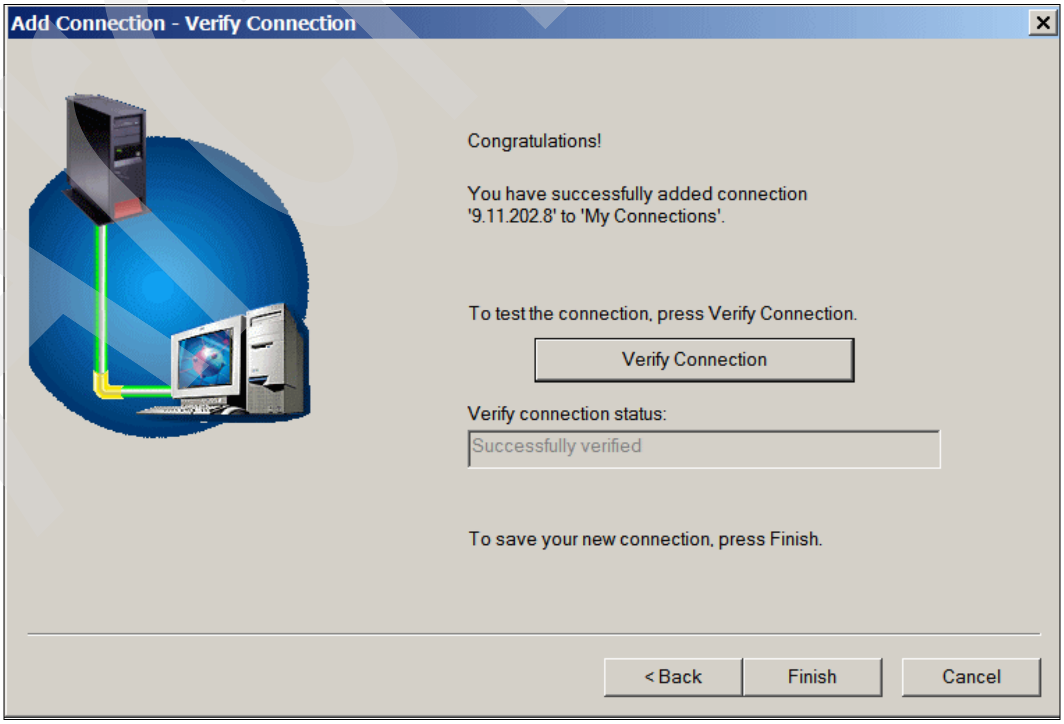
Verifying iSeries connection:

Status:

Verifying connection to system 9.11.202.8...
Successfully connected to server application: Central Client
Successfully connected to server application: Network File
Successfully connected to server application: Network Print
Verify of server application in progress...

Figure 5-4 iSeries Navigator - verifying Connection

6. After the connection is successfully verified, click **OK,** then click **Finish** on the next window, as can be seen in Figure 5-5.



Add Connection - Verify Connection

Congratulations!

You have successfully added connection '9.11.202.8' to 'My Connections'.

To test the connection, press Verify Connection.

Verify connection status:

Successfully verified

To save your new connection, press Finish.

Figure 5-5 iSeries Navigator - Finish adding connection

7. After the connection is successfully done, the IP address of the newly added System appears on the left part of the iSeries Navigator window.

   In the left panel of iSeries Navigator, expand the IP address of the System i partition where the tape drive is added. While expanding, the window asking for System i Userid and password pops up, you have to insert them. An expanded System i partition in iSeries Navigator is shown in Figure 5-6.

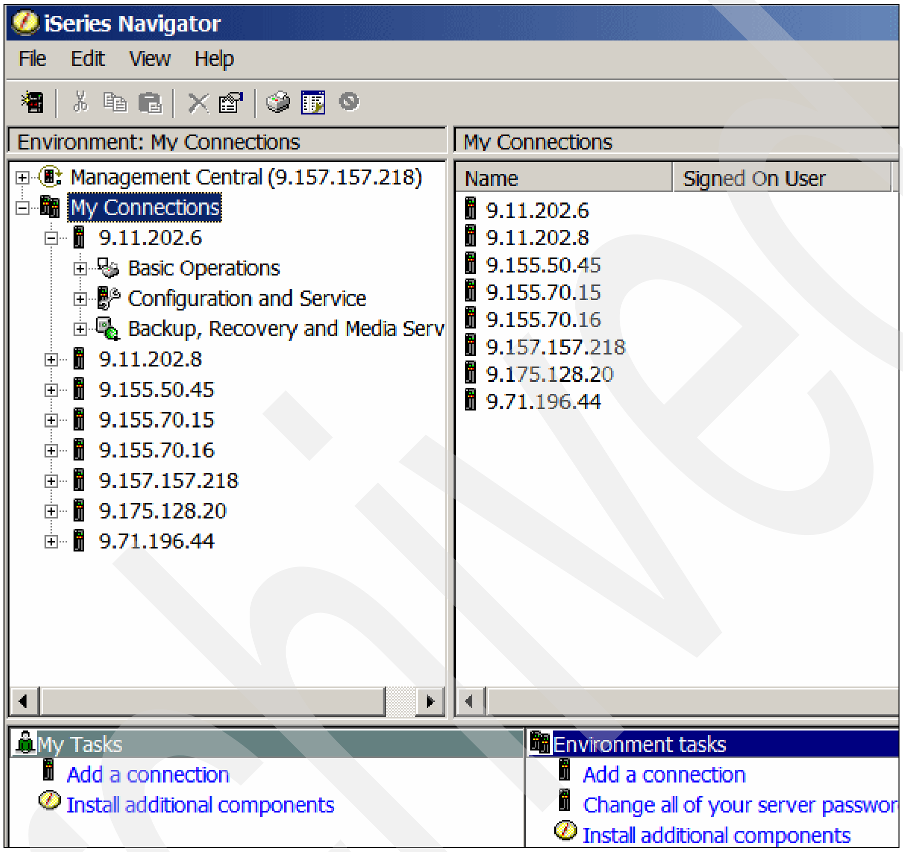
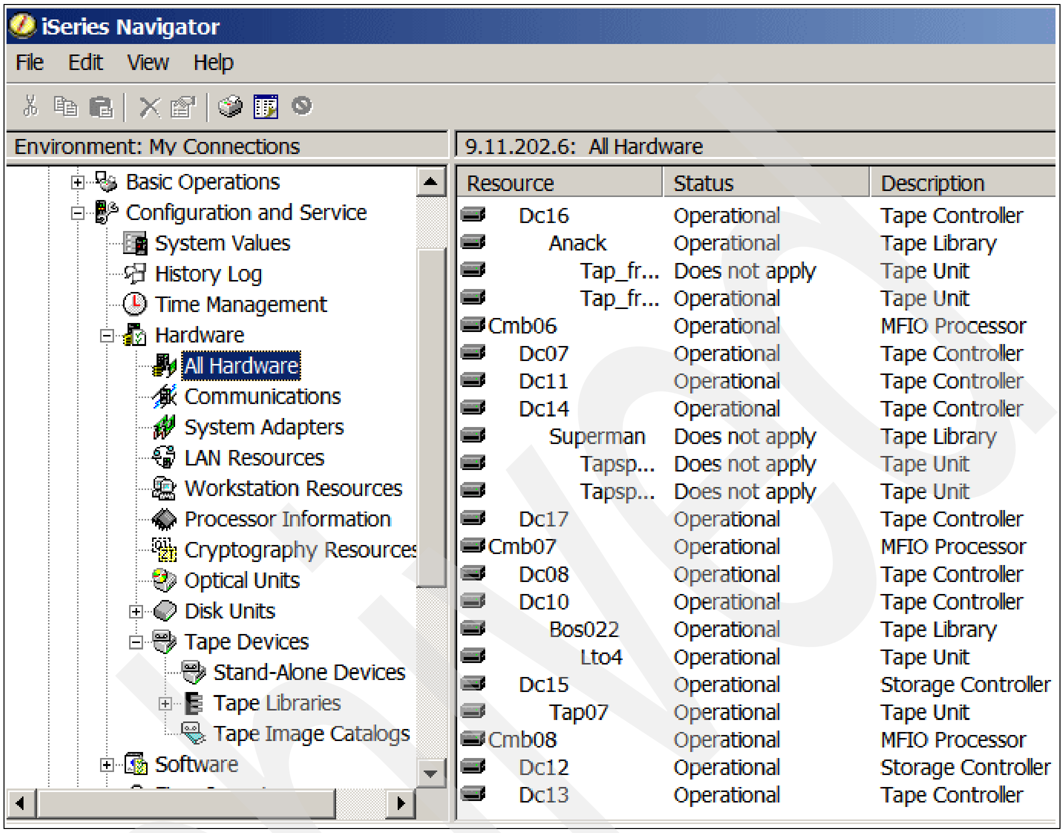


Figure 5-6 Iseries Navigator - expand System i

- On the iSeries Navigator left panel, expand *Configuration and Service*, expand *Hardware*, and click **All Hardware.** This displays a list of hardware resources that can be seen in the iSeries Navigator right panel, as shown in Figure 5-7.



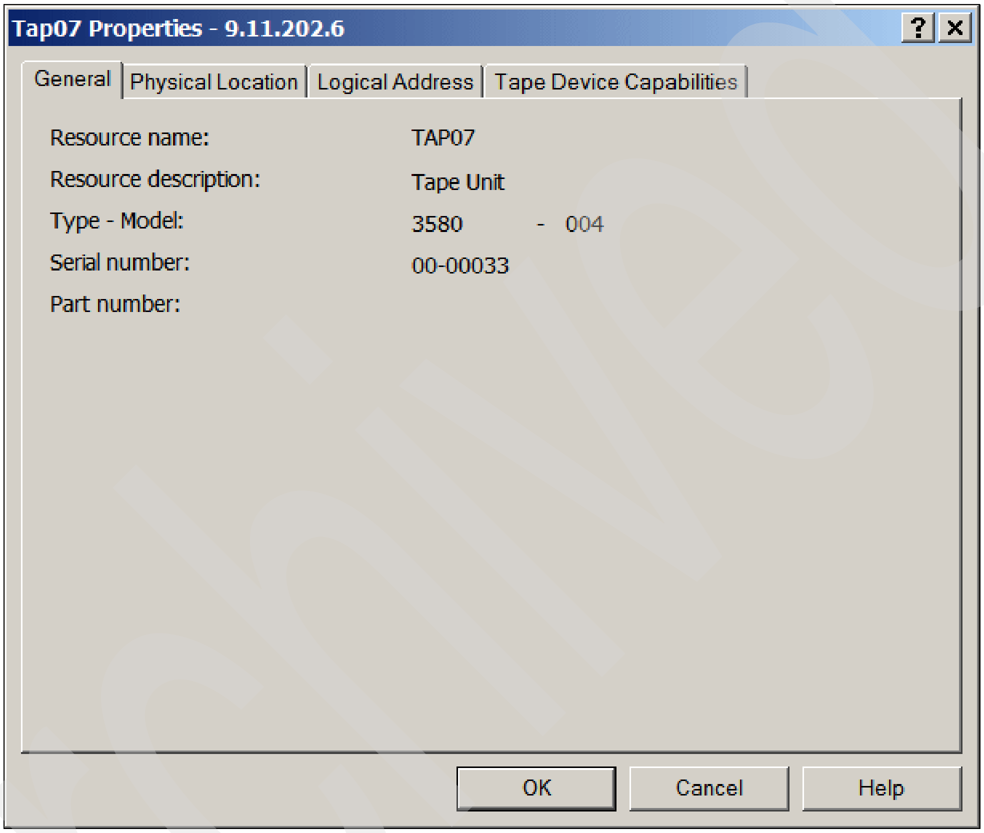
Resource	Status	Description
Dc16	Operational	Tape Controller
Anack	Operational	Tape Library
Tap_fr...	Does not apply	Tape Unit
Tap_fr...	Operational	Tape Unit
Cmb06	Operational	MFIO Processor
Dc07	Operational	Tape Controller
Dc11	Operational	Tape Controller
Dc14	Operational	Tape Controller
Superman	Does not apply	Tape Library
Tapsp...	Does not apply	Tape Unit
Tapsp...	Does not apply	Tape Unit
Dc17	Operational	Tape Controller
Cmb07	Operational	MFIO Processor
Dc08	Operational	Tape Controller
Dc10	Operational	Tape Controller
Bos022	Operational	Tape Library
Lto4	Operational	Tape Unit
Dc15	Operational	Storage Controller
Tap07	Operational	Tape Unit
Cmb08	Operational	MFIO Processor
Dc12	Operational	Storage Controller
Dc13	Operational	Tape Controller

Figure 5-7 iSeries Navigator - Hardware resources

8. In the list of hardware resources, observe the added tape device with resource name Tap07 attached to the Storage Controller resource name Dc15. The tape device reports as Operational.

   Initially, i5/OS assigns to the tape device resource a name TAP*xx* (*xx* stands for a number), but later you can change this name. Further in this section, you can find instructions on how to rename a tape resource in the SST environment.

9. On the iSeries navigator right panel, right-click the tape resource, then click **Properties**. This displays the *Tape Properties* panel as shown in Figure 5-8.



Resource name: TAP07

Resource description: Tape Unit

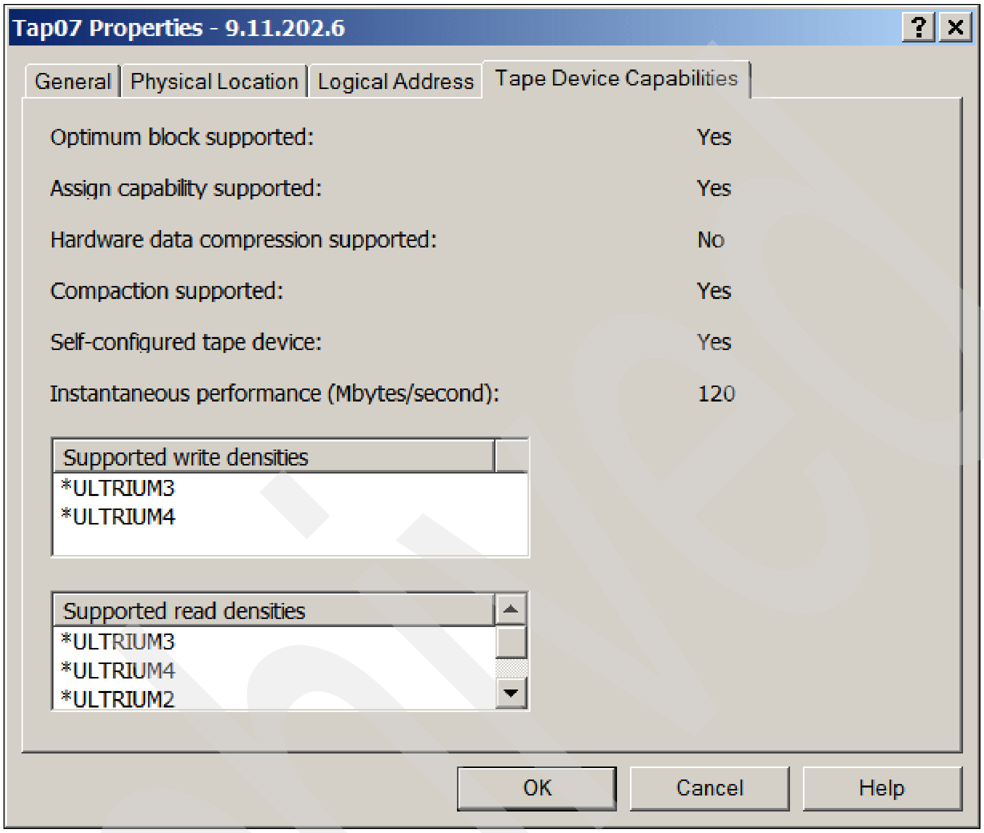
Type - Model: 3580 - 004

Serial number: 00-00033

Part number:

Figure 5-8 iSeries Navigator - Tape device properties

- On the *Tape device properties* panel, you can observe different properties of the tape device, by clicking the relevant tab. For example: the location of the tape device in the System i partition is shown in the tab *Physical Location*; available data cartridge densities for this drive are shown in the tab *Tape Device Capabilities*; as can be seen in Figure 5-9.



Optimum block supported:	Yes
Assign capability supported:	Yes
Hardware data compression supported:	No
Compaction supported:	Yes
Self-configured tape device:	Yes
Instantaneous performance (Mbytes/second):	120

Supported write densities
*ULTRIUM3
*ULTRIUM4

Supported read densities
*ULTRIUM3
*ULTRIUM4
*ULTRIUM2

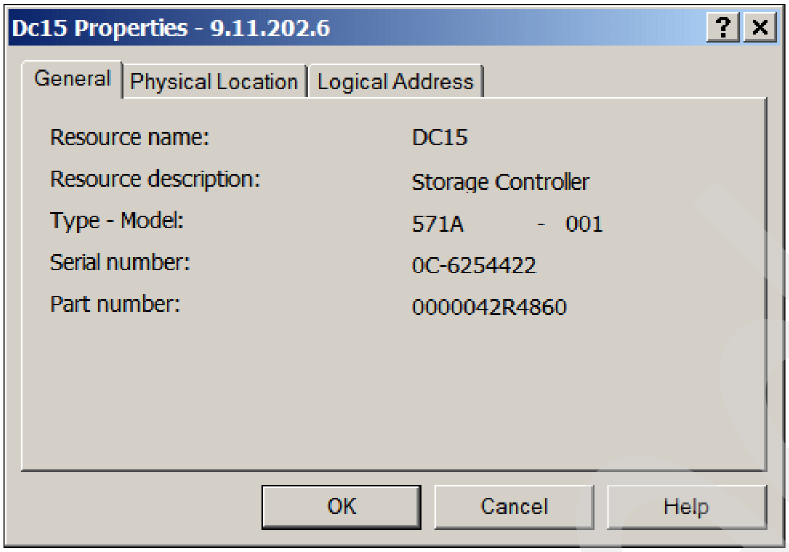
Figure 5-9 iSeries Navigator - data cartridge densities

10.On the right panel of iSeries Navigator, look for SCSI adapter (Storage controller) to which the tape device is attached. In our example the tape is attached to the SCSI adapter with resource name DS15, as can be seen in Figure 5-7.

Observe the Input Output Processor (IOP) to which the SCSI adapter is attached. In our example the SCSI adapter is attached to the Multi Function IOP (MFIOP) with resource name CMB07, as shown in Figure 5-7. For more information about IOP, refer to Chapter 3, “Overview of the IBM System i platform” on page 83.

> **Note:** If you do not know to which SCSI adapter and IOP the new tape device is attached, we recommend to browse through the listed IOPs and adapters to find the ones with attached tape devices.

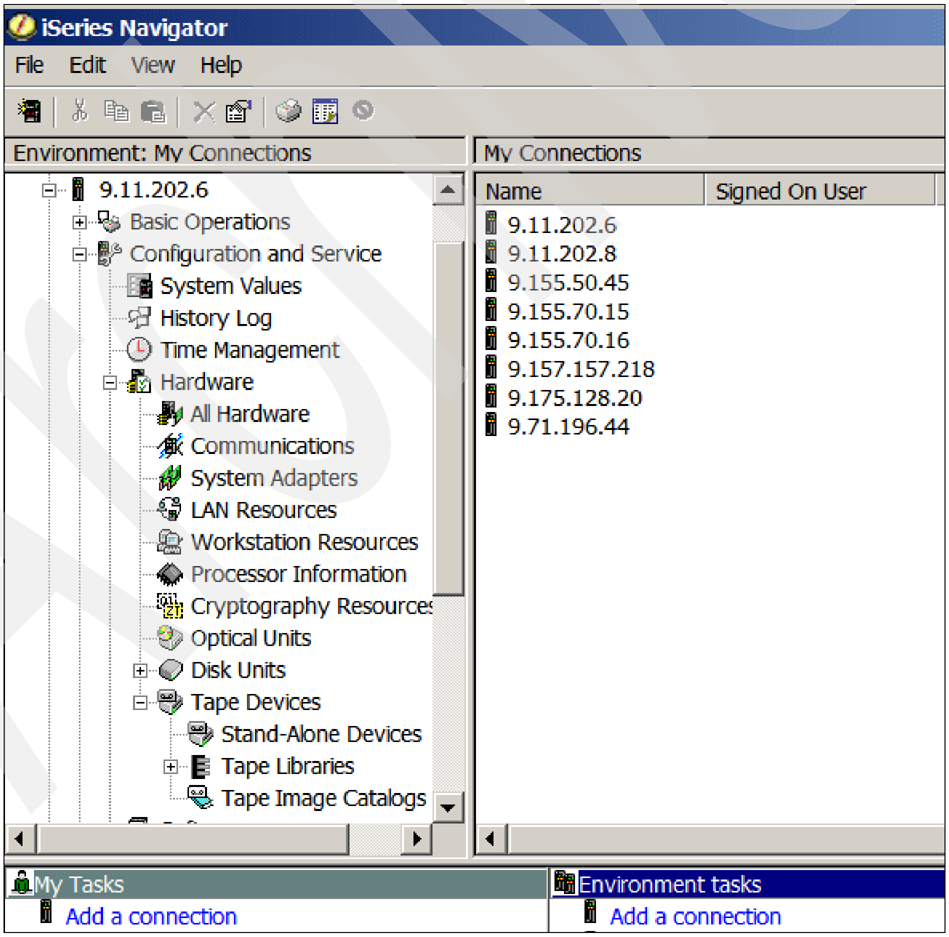
Right-click the Storage controller and click the **Properties** button that pops up. The window Resource Properties is displayed; it contains tabs with different properties of the SCSI adapter. For example, on the *General* tab you can see the serial number of the SCSI controller, as shown in Figure 5-10.



Resource name: DC15
Resource description: Storage Controller
Type - Model: 571A - 001
Serial number: 0C-6254422
Part number: 0000042R4860

Figure 5-10 iSeries Navigator - SCSI adapter

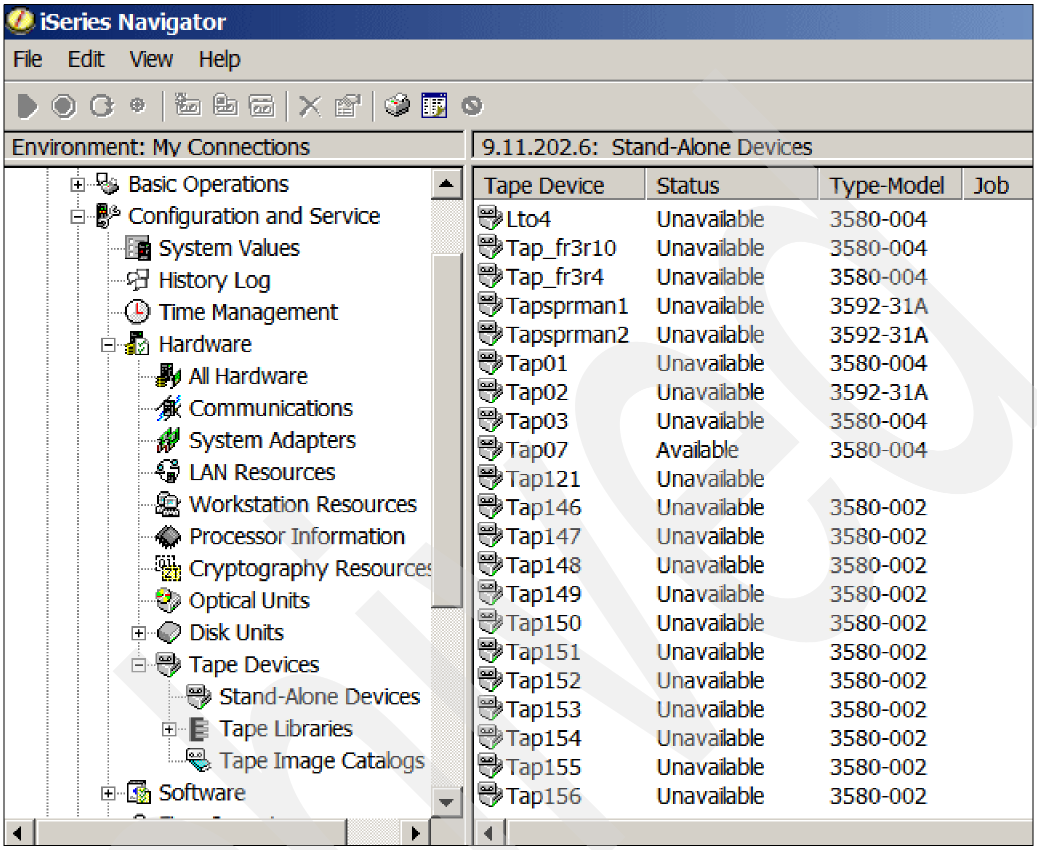
11.On the iSeries Navigator left panel, expand *Configuration and Service*, then expand *Hardware*, then expand *Tape Devices*, as shown in Figure 5-11.



Name	Signed On User
9.11.202.6	
9.11.202.8	
9.155.50.45	
9.155.70.15	
9.155.70.16	
9.157.157.218	
9.175.128.20	
9.71.196.44	

Figure 5-11 iSeries Navigator - expand Tape Devices

12. In iSeries navigator, in the expanded Tape Devices, click **Stand-Alone Devices**. This displays a list of stand-alone tape drives connected to the System i partition, the list is in the right part of the iSeries Navigator window. See Figure 5-12.



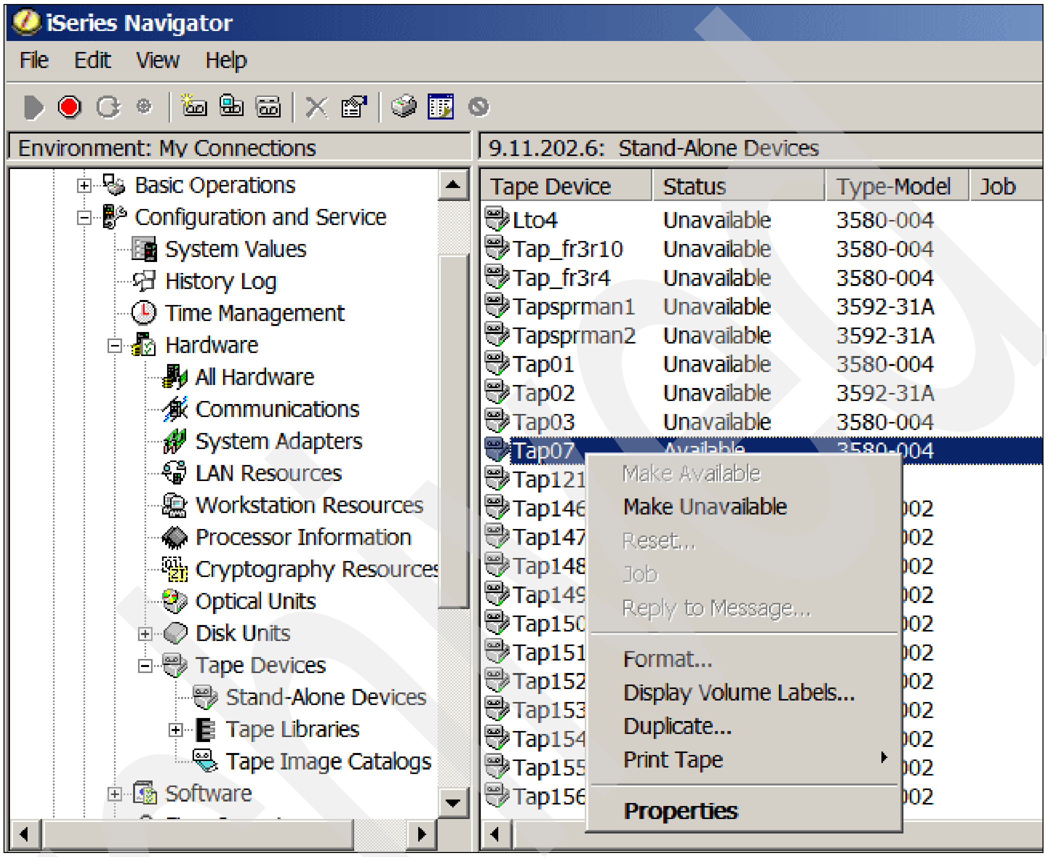
Tape Device	Status	Type-Model	Job
Lto4	Unavailable	3580-004	
Tap_fr3r10	Unavailable	3580-004	
Tap_fr3r4	Unavailable	3580-004	
Tapsprman1	Unavailable	3592-31A	
Tapsprman2	Unavailable	3592-31A	
Tap01	Unavailable	3580-004	
Tap02	Unavailable	3592-31A	
Tap03	Unavailable	3580-004	
Tap07	Available	3580-004	
Tap121	Unavailable		
Tap146	Unavailable	3580-002	
Tap147	Unavailable	3580-002	
Tap148	Unavailable	3580-002	
Tap149	Unavailable	3580-002	
Tap150	Unavailable	3580-002	
Tap151	Unavailable	3580-002	
Tap152	Unavailable	3580-002	
Tap153	Unavailable	3580-002	
Tap154	Unavailable	3580-002	
Tap155	Unavailable	3580-002	
Tap156	Unavailable	3580-002	

Figure 5-12 iSeries Navigator - Stand-alone tape drives

13. On the right panel, look for the drive which was added. With enabled autoconfiguration, i5/OS names the new *tape drive TAPxx*, where *xx* is the next available number to use. In our example, the added tape drive has the device description *TAP07*.

    Observe the status of tape device. In our example it is *Available*, which means that the device is varied-on or available to use.

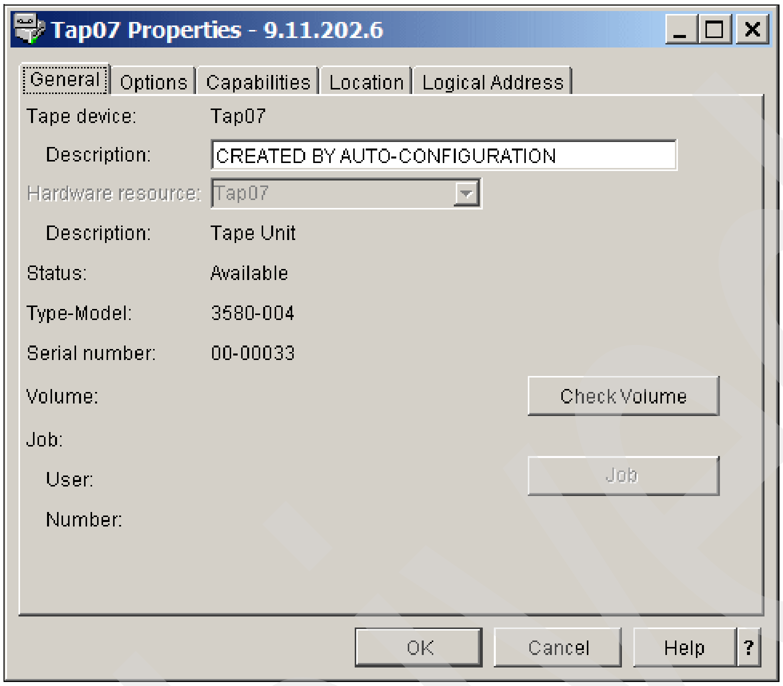
14. On the right panel of the iSeries Navigator window, right-click the newly added tape drive. This displays the pull-down menu from where you can perform actions such as these: make the tape drive available or unavailable (vary-on or vary-off the tape drive), format a data cartridge, or copy the data cartridge to another one in another tape drive. The pull-down menu can be seen in Figure 5-13.



Tape Device	Status	Type-Model	Job
Lto4	Unavailable	3580-004	
Tap_fr3r10	Unavailable	3580-004	
Tap_fr3r4	Unavailable	3580-004	
Tapsprman1	Unavailable	3592-31A	
Tapsprman2	Unavailable	3592-31A	
Tap01	Unavailable	3580-004	
Tap02	Unavailable	3592-31A	
Tap03	Unavailable	3580-004	
Tap07	Available	3580-004	
Tap121			
Tap146		02	
Tap147		02	
Tap148		02	
Tap149		02	
Tap150		02	
Tap151		02	
Tap152		02	
Tap153		02	
Tap154		02	
Tap155		02	
Tap156		02	

Figure 5-13 iSeries Navigator - Actions on the tape drive

- In the expanded pull-down, click **Properties**. This displays the *Tape Properties* panel, where you can observe properties of the tape drive. On the *General* tab, you can see the tape model, serial number, and status, as shown in Figure 5-14.



Tape device: Tap07

Description: CREATED BY AUTO-CONFIGURATION

Hardware resource: Tap07

Description: Tape Unit

Status: Available

Type-Model: 3580-004

Serial number: 00-00033

Volume:

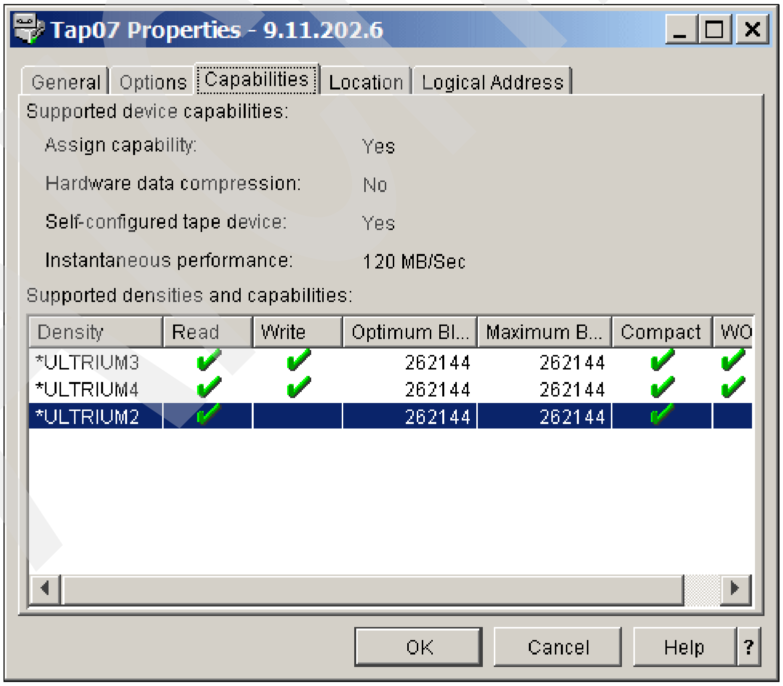
Job:

User:

Number:

Figure 5-14 iSeries Navigator - Tape drive properties

15.On the *Tape Properties* panel, click the tab **Capabilities** and observe the possible densities of data cartridges for this drive, as shown in Figure 5-15.



Supported device capabilities:

Assign capability: Yes

Hardware data compression: No

Self-configured tape device: Yes

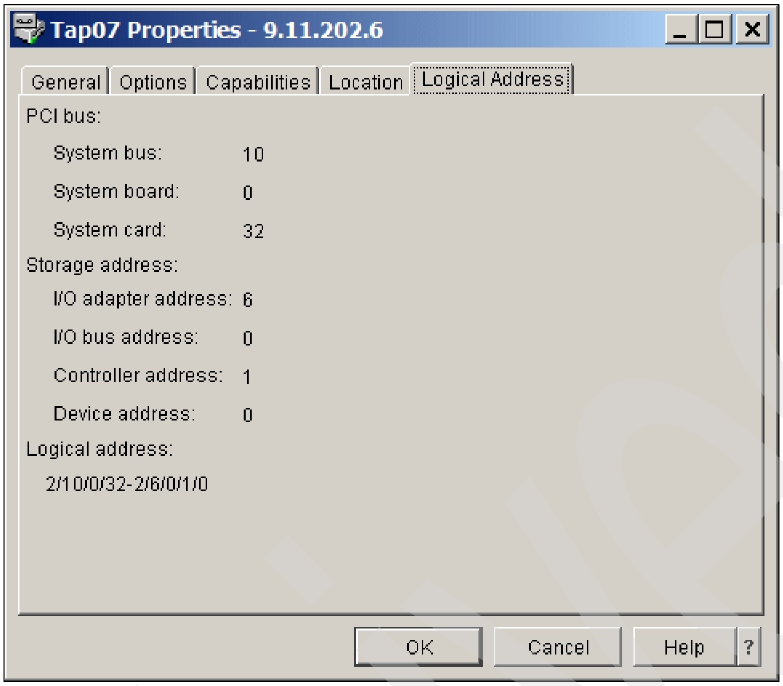
Instantaneous performance: 120 MB/Sec

Supported densities and capabilities:

Density	Read	Write	Optimum Bl...	Maximum B...	Compact	WO
*ULTRIUM3	✓	✓	262144	262144	✓	✓
*ULTRIUM4	✓	✓	262144	262144	✓	✓
*ULTRIUM2	✓		262144	262144	✓	

Figure 5-15 iSeries Navigator - Data cartridge densities

- On the *Tape Properties* panel, click the tab **Logical Address** and observe the placement of the SCSI adapter in the System i partition, as shown in Figure 5-16.



PCI bus:

System bus: 10

System board: 0

System card: 32

Storage address:

I/O adapter address: 6

I/O bus address: 0

Controller address: 1

Device address: 0

Logical address:

2/10/0/32-2/6/0/1/0

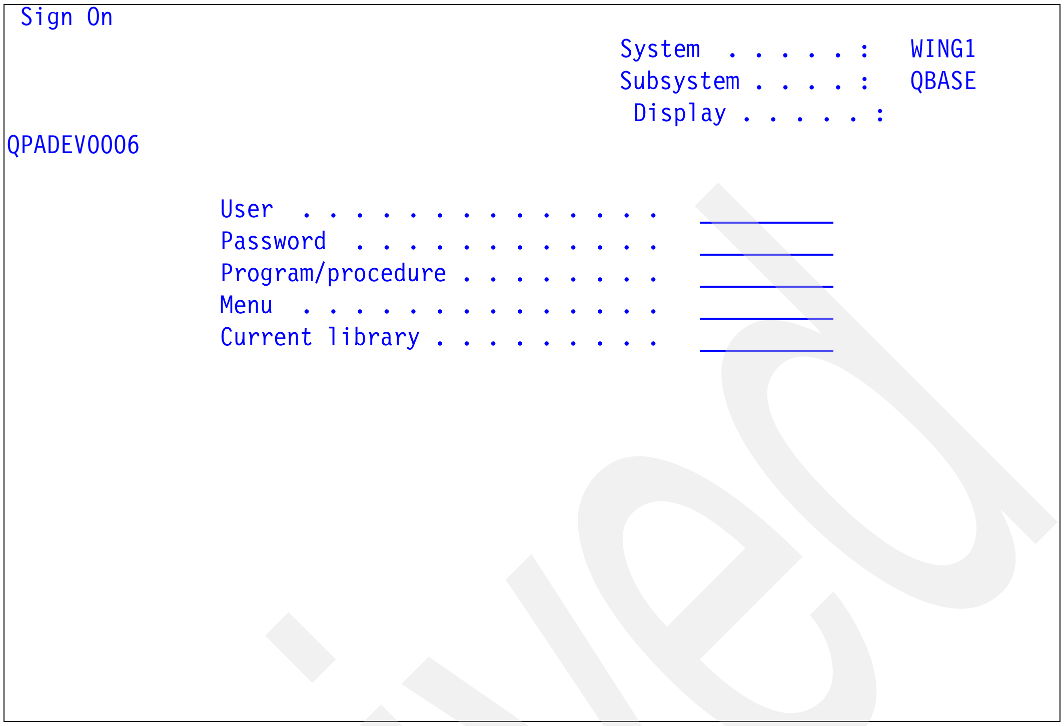
Figure 5-16 iSeries Navigator - Placement od SCSI adapter in System i partition

To observe tape resource and device description in the i5/OS green screen and SST, perform the following steps:

1. Connect to the System i partition via IP telnet, by using the IBM Personal communications tool. For more information about Personal communications, refer to the System i Information center at the following Web site:

   `http://publib.boulder.ibm.com/iseries/`

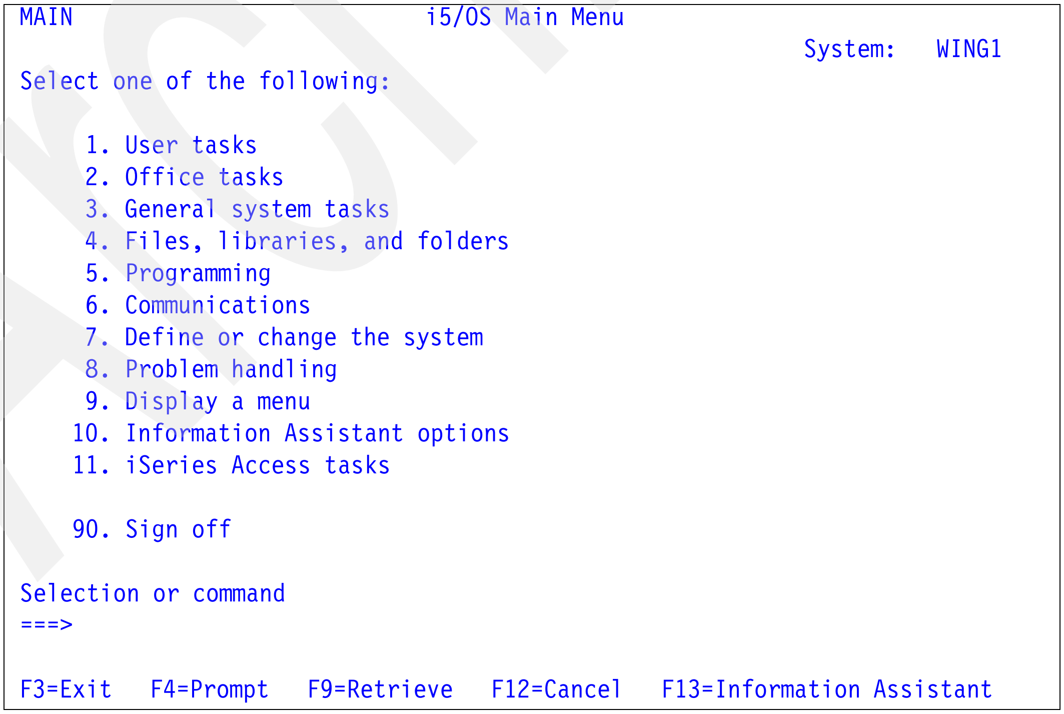
2. After you are connected, the i5/OS sign-on screen appears in the telnet window, as shown in Figure 5-17.



```
 Sign On
                                             System  . . . . . :   WING1
                                             Subsystem . . . . :   QBASE
                                              Display . . . . . :
QPADEV0006

                User  . . . . . . . . . . . . . .    __________
                Password  . . . . . . . . . . . .    __________
                Program/procedure . . . . . . . .    __________
                Menu  . . . . . . . . . . . . . .    __________
                Current library . . . . . . . . .    __________
```

Figure 5-17 I5/OS sign-on screen

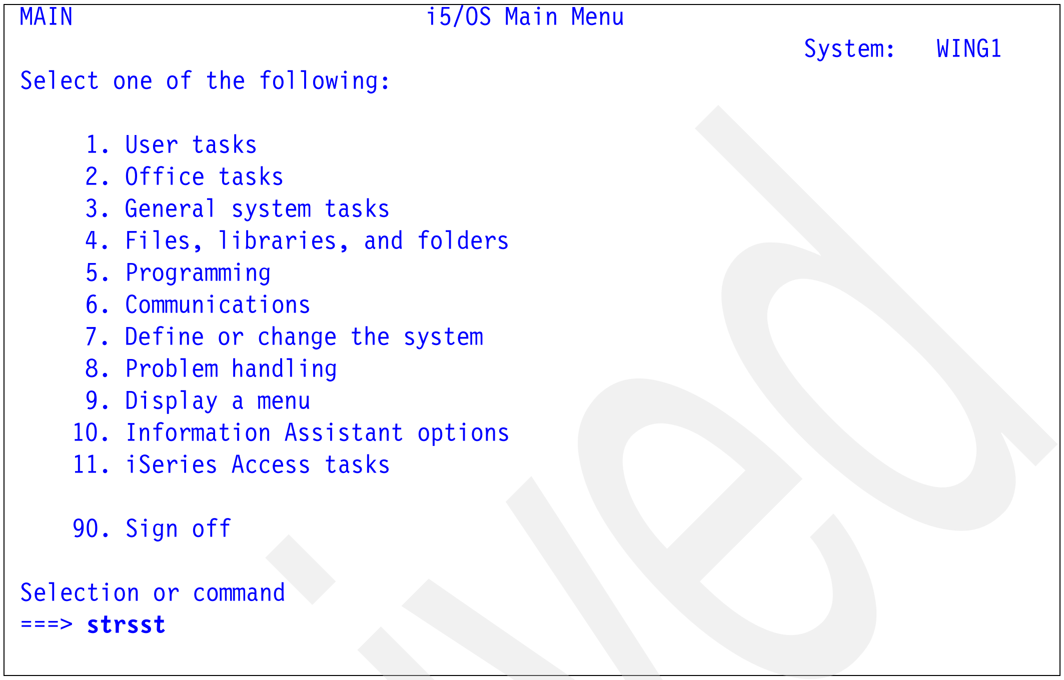
3. In the i5/OS sign-on screen, type in your i5/OS Userid and Password in the indicated fields, and press Enter. Next, you are presented the i5/OS green screen environment where you can use menu functions or type in i5/OS commands. This environment, with the i5/OS Main menu, is shown in Figure 5-18.



```
 MAIN                           i5/OS Main Menu
                                                        System:   WING1
 Select one of the following:

      1. User tasks
      2. Office tasks
      3. General system tasks
      4. Files, libraries, and folders
      5. Programming
      6. Communications
      7. Define or change the system
      8. Problem handling
      9. Display a menu
     10. Information Assistant options
     11. iSeries Access tasks

     90. Sign off

 Selection or command
 ===>

 F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel   F13=Information Assistant
```

Figure 5-18 i5/OS Main menu

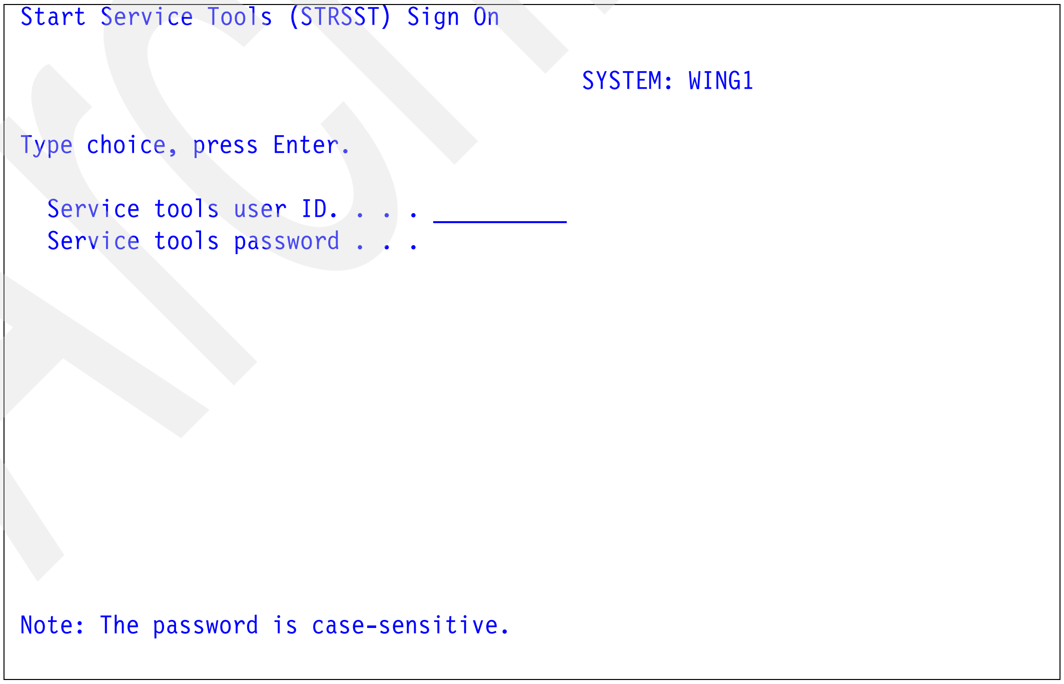
4. Start the SST environment by entering the command **STRSST** in the i5/OS Main menu, as can be seen in Figure 5-19. Press Enter.



```
MAIN                           i5/OS Main Menu
                                                             System:   WING1
Select one of the following:

     1. User tasks
     2. Office tasks
     3. General system tasks
     4. Files, libraries, and folders
     5. Programming
     6. Communications
     7. Define or change the system
     8. Problem handling
     9. Display a menu
    10. Information Assistant options
    11. iSeries Access tasks

    90. Sign off

Selection or command
===> strsst
```

Figure 5-19 Start SST

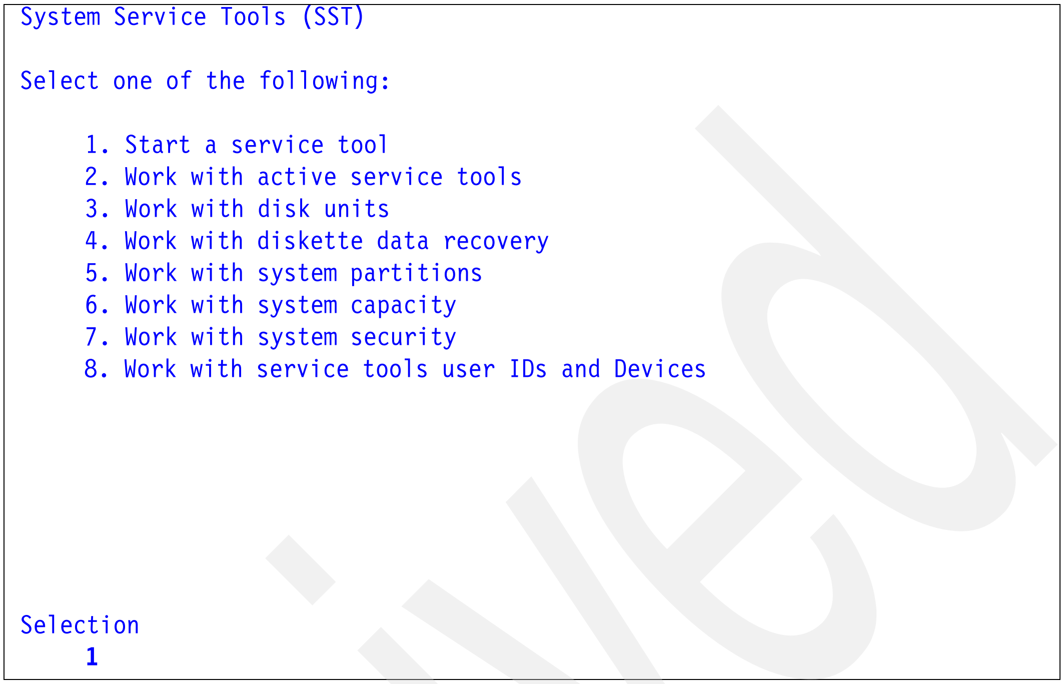
5. After you enter the command **STRSST**, you are presented with the SST sign-in screen, as can be seen in Figure 5-20. To enter SST, you require a special userid and password. Type those in the SST Sign On screen, then press Enter.



```
Start Service Tools (STRSST) Sign On

                                            SYSTEM: WING1

Type choice, press Enter.

  Service tools user ID. . . . __________
  Service tools password . . .










Note: The password is case-sensitive.
```

Figure 5-20 SST Sign On screen

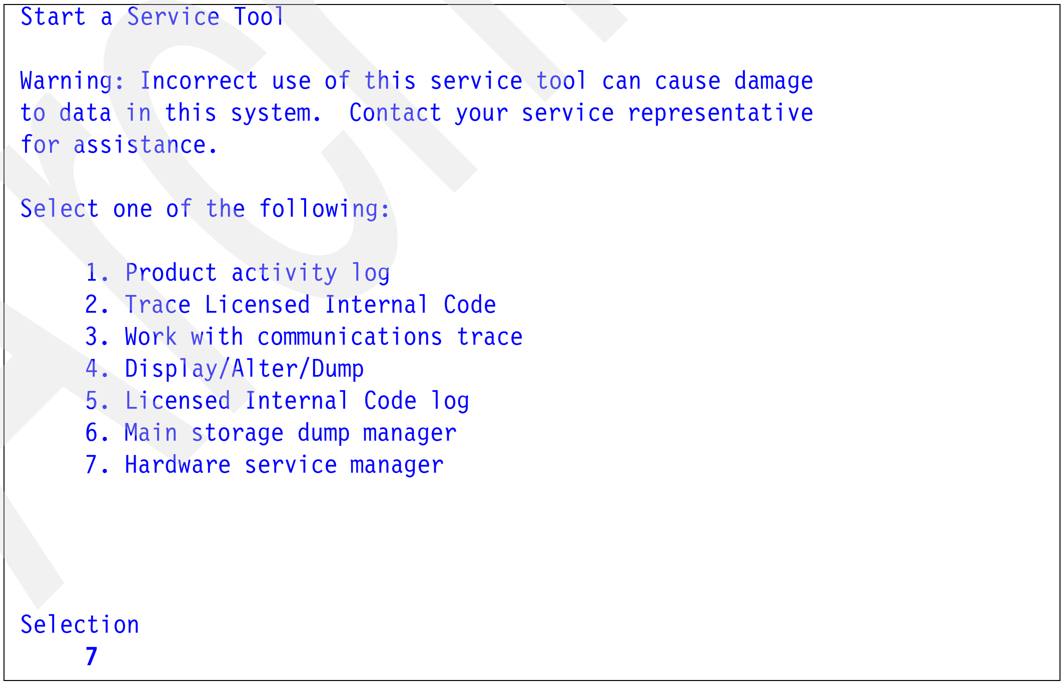
6. After signing on SST, you are presented the SST initial menu. Select option **1. Start a service tool**, as can be seen in Figure 5-21. Press Enter.



```
System Service Tools (SST)

Select one of the following:

     1. Start a service tool
     2. Work with active service tools
     3. Work with disk units
     4. Work with diskette data recovery
     5. Work with system partitions
     6. Work with system capacity
     7. Work with system security
     8. Work with service tools user IDs and Devices








Selection
     1
```

Figure 5-21 SST System Service Tools - initial menu

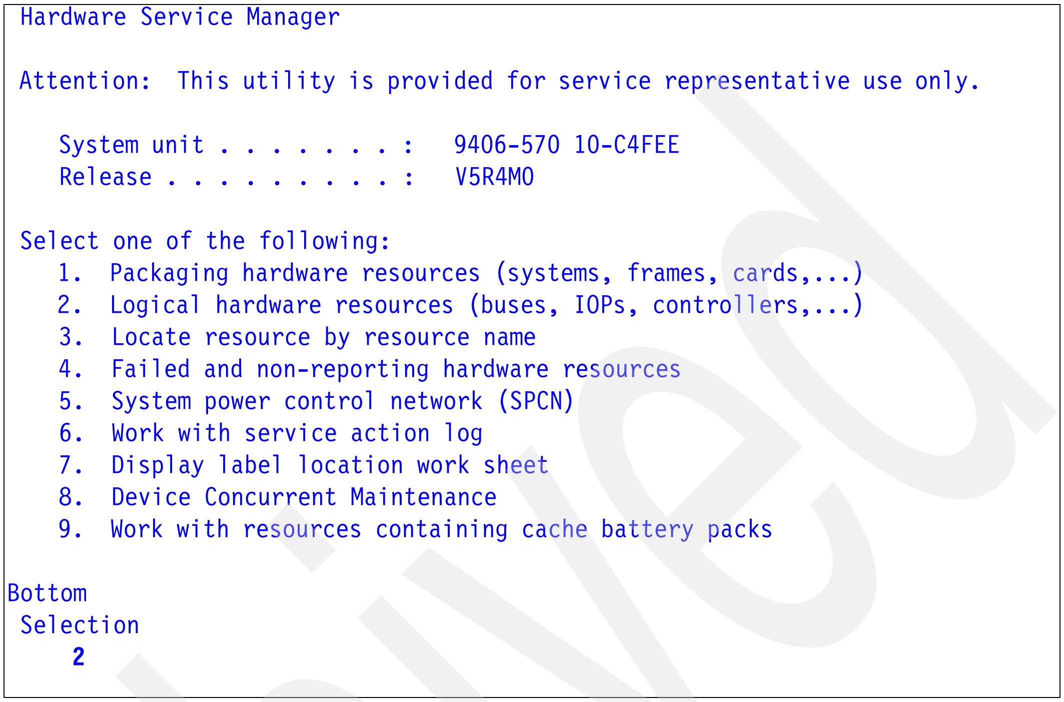
7. Next, the screen *Start a Service Tool* is shown. Select option **7. Hardware service manager**, as shown in Figure 5-22. Press Enter.



```
Start a Service Tool

Warning: Incorrect use of this service tool can cause damage
to data in this system.  Contact your service representative
for assistance.

Select one of the following:

     1. Product activity log
     2. Trace Licensed Internal Code
     3. Work with communications trace
     4. Display/Alter/Dump
     5. Licensed Internal Code log
     6. Main storage dump manager
     7. Hardware service manager




Selection
     7
```

Figure 5-22 SST Start a Service Tool

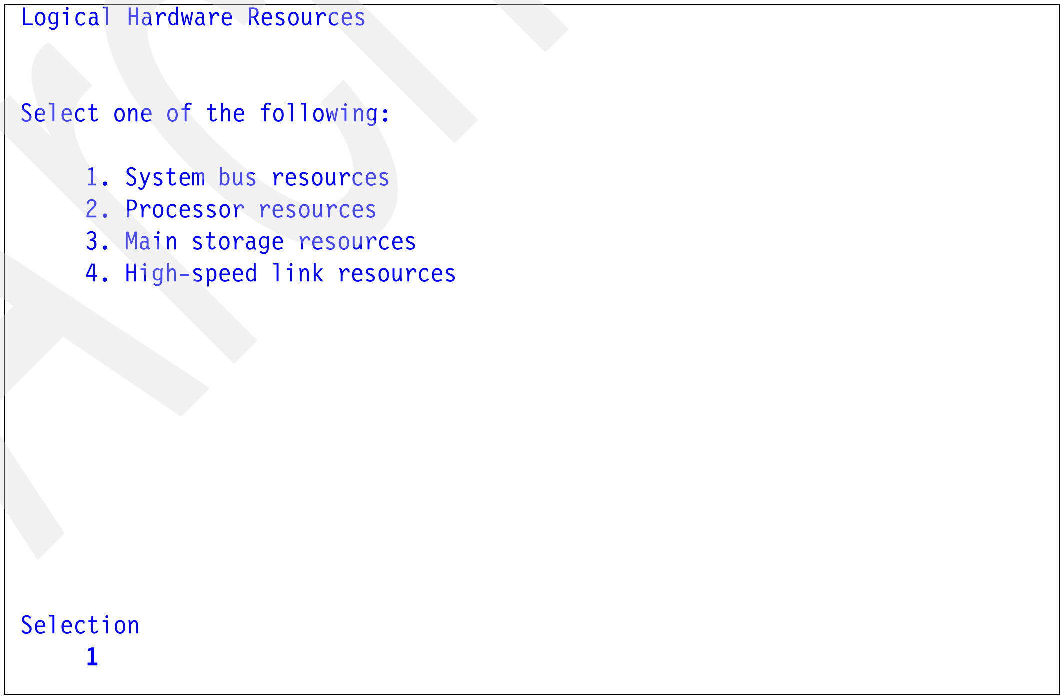
8. Next, you are presented the menu *Hardware Service Manager*. On the menu, select option **2. Logical hardware resources (buses, IOPs, controllers,...)**, as shown in Figure 5-23.



```
 Hardware Service Manager

 Attention:  This utility is provided for service representative use only.

    System unit . . . . . . . :   9406-570 10-C4FEE
    Release . . . . . . . . . :   V5R4M0

 Select one of the following:
    1.  Packaging hardware resources (systems, frames, cards,...)
    2.  Logical hardware resources (buses, IOPs, controllers,...)
    3.  Locate resource by resource name
    4.  Failed and non-reporting hardware resources
    5.  System power control network (SPCN)
    6.  Work with service action log
    7.  Display label location work sheet
    8.  Device Concurrent Maintenance
    9.  Work with resources containing cache battery packs

Bottom
 Selection
      2
```

Figure 5-23   SST Hardware Service Manager

9. Next you see the screen *Logical Hardware Resources*. *S*elect option **1. System bus resources,** as can be seen in Figure 5-24.

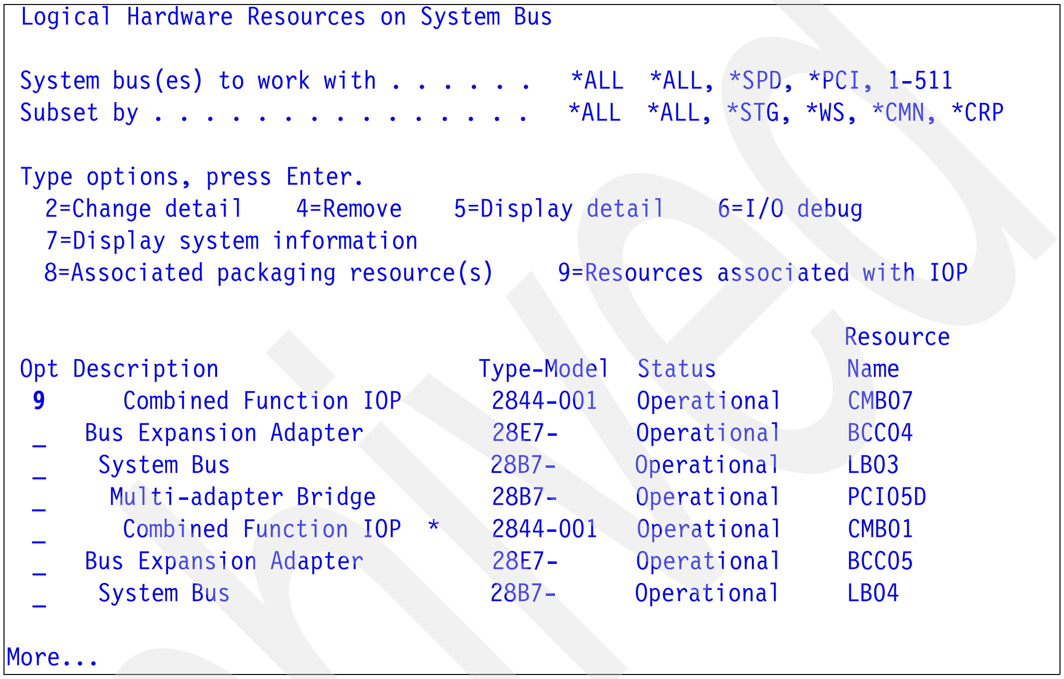


```
 Logical Hardware Resources


 Select one of the following:

      1. System bus resources
      2. Processor resources
      3. Main storage resources
      4. High-speed link resources









 Selection
      1
```

Figure 5-24   SST Logical Hardware Resources

10. Next, you see the screen *Logical Hardware Resources on System Bus.* On this screen, page down until you see the Input Out Processor (IOP) to which the SCSI adapters connecting the tape drive are attached. For more information about IOP, refer to Chapter 3, “Overview of the IBM System i platform” on page 83.

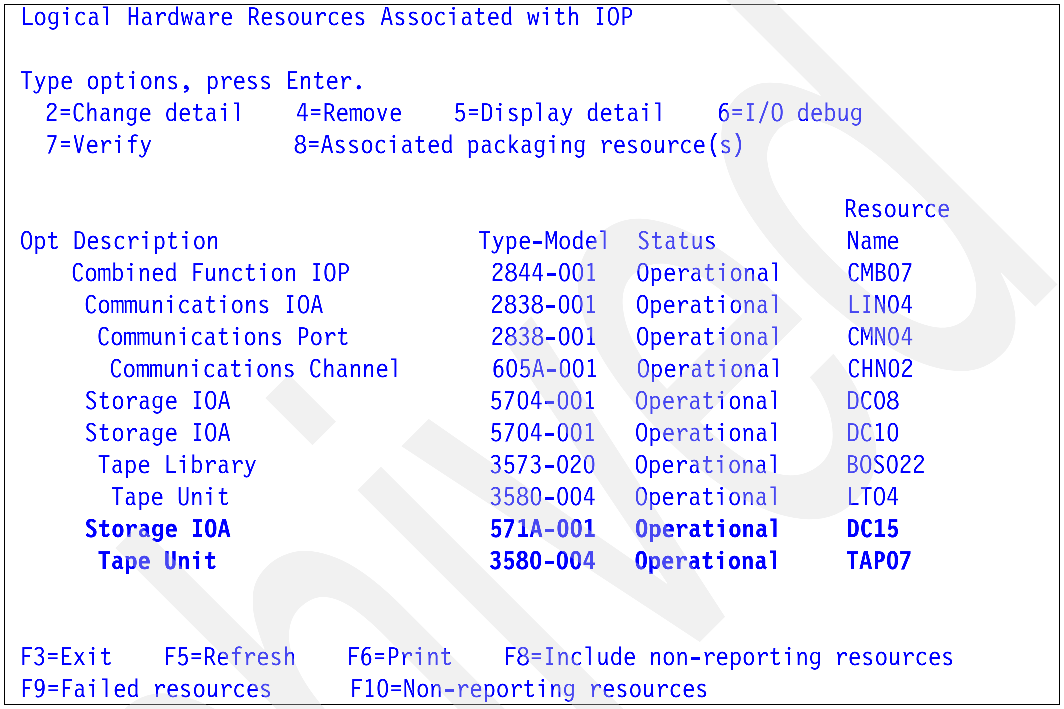
    Type **9** at the IOP to which the SCSI adapter with tape drive is attached, and press Enter, as shown in Figure 5-25. If you are not aware of which particular IOP is the relevant adapter, you might want to check every IOP and observe its associated resources until you find the SCSI adapter with a tape drive.



```
 Logical Hardware Resources on System Bus

 System bus(es) to work with . . . . . .   *ALL  *ALL, *SPD, *PCI, 1-511
 Subset by . . . . . . . . . . . . . . .   *ALL  *ALL, *STG, *WS, *CMN, *CRP

 Type options, press Enter.
   2=Change detail    4=Remove    5=Display detail    6=I/O debug
   7=Display system information
   8=Associated packaging resource(s)     9=Resources associated with IOP

                                                              Resource
 Opt Description                        Type-Model  Status          Name
  9      Combined Function IOP           2844-001   Operational     CMB07
  _    Bus Expansion Adapter             28E7-      Operational     BCC04
  _     System Bus                       28B7-      Operational     LB03
  _      Multi-adapter Bridge            28B7-      Operational     PCI05D
  _       Combined Function IOP  *       2844-001   Operational     CMB01
  _    Bus Expansion Adapter             28E7-      Operational     BCC05
  _     System Bus                       28B7-      Operational     LB04

More...
```

Figure 5-25   SST Logical HW Resources on System Bus

11. You are presented the screen *Logical Hardware Resources Associated with IOP*. Observe the SCSI adapter named *Storage Input Output Adapter (IOA)* and associated tape drive resource, make sure that it reports as *operational*. In our example, the TS2230 (reporting as 3580-004) is connected via SCSI adapter feature #5736, which reports in i5/OS as 571A, as can be observed in Figure 5-26. In our example, the *taoe* resource has the name TAP07 as initially assigned byi5/OS. You can change the resource name, as is described later in this section.



```
Logical Hardware Resources Associated with IOP

Type options, press Enter.
  2=Change detail    4=Remove    5=Display detail    6=I/O debug
  7=Verify           8=Associated packaging resource(s)

                                                                  Resource
Opt Description                        Type-Model  Status          Name
     Combined Function IOP              2844-001   Operational     CMB07
      Communications IOA                2838-001   Operational     LIN04
       Communications Port              2838-001   Operational     CMN04
        Communications Channel          605A-001   Operational     CHN02
      Storage IOA                       5704-001   Operational     DC08
      Storage IOA                       5704-001   Operational     DC10
       Tape Library                     3573-020   Operational     BOS022
        Tape Unit                       3580-004   Operational     LT04
      Storage IOA                       571A-001   Operational     DC15
       Tape Unit                        3580-004   Operational     TAP07


F3=Exit    F5=Refresh    F6=Print    F8=Include non-reporting resources
F9=Failed resources       F10=Non-reporting resources
```

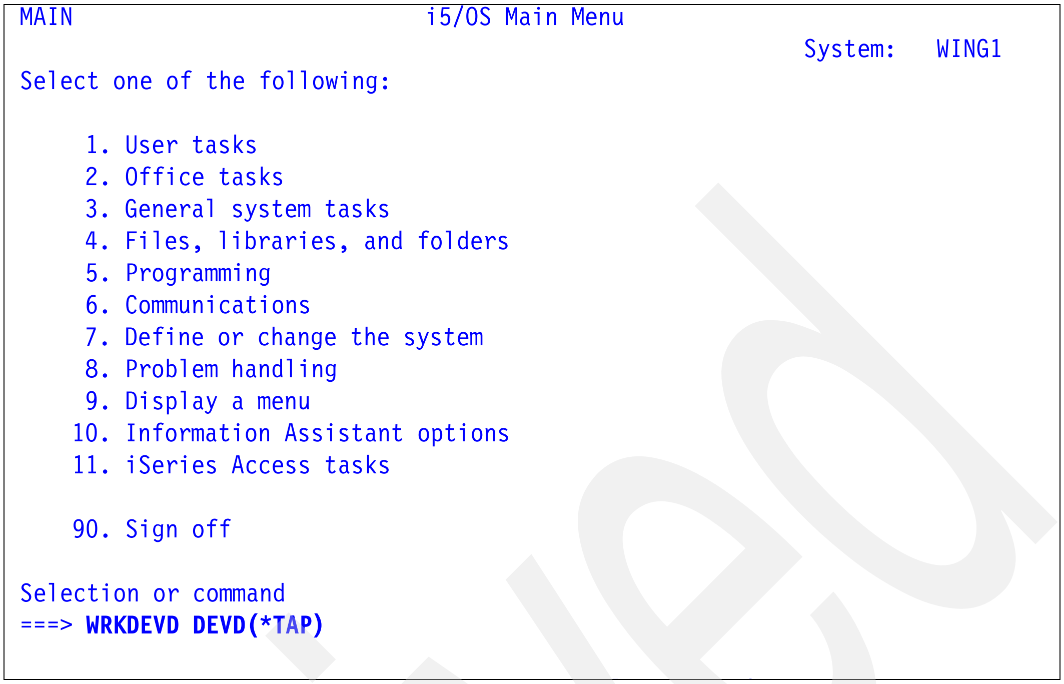
Figure 5-26 Operational SCSI adapter and tape drive

12. After you have checked the tape resource, keep pressing F12 (cancel) until the screen *Exit System Service Tools* is displayed. On this screen, press Enter, to exit SST.

Tape device descriptions

To observe tape device descriptions in i5/OS, perform the following steps:

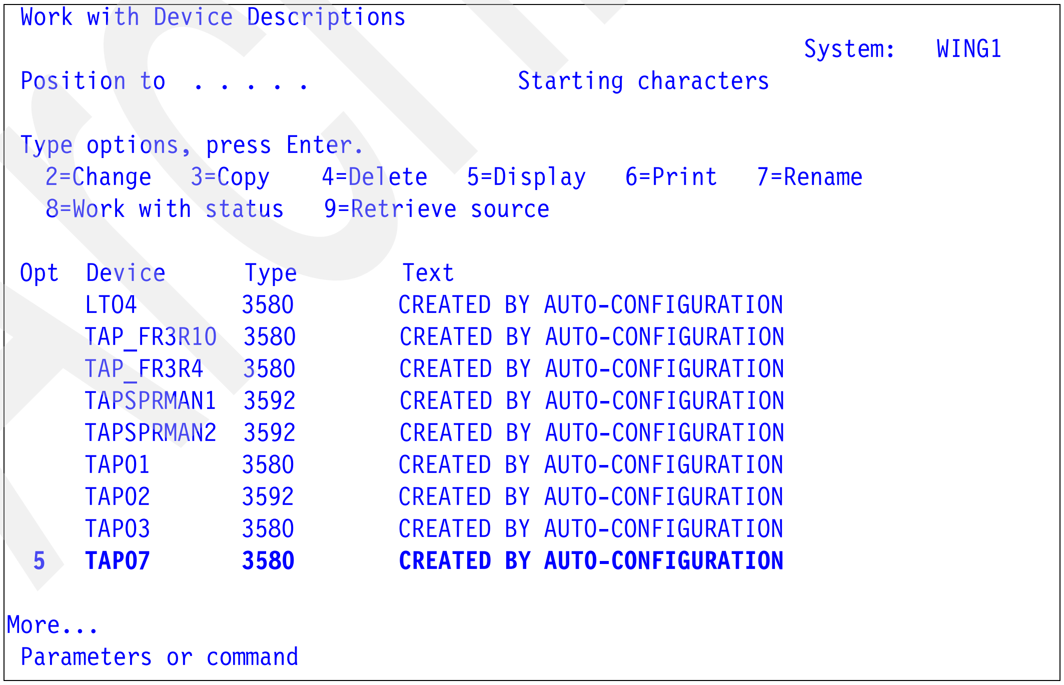
1. Use command **WRKDEVD DEVD(*TAP)** in the i5/OS green screen, as shown in Figure 5-27. Press Enter.



```
MAIN                              i5/OS Main Menu
                                                             System:   WING1
Select one of the following:

     1. User tasks
     2. Office tasks
     3. General system tasks
     4. Files, libraries, and folders
     5. Programming
     6. Communications
     7. Define or change the system
     8. Problem handling
     9. Display a menu
    10. Information Assistant options
    11. iSeries Access tasks

    90. Sign off

Selection or command
===> WRKDEVD DEVD(*TAP)
```

Figure 5-27 Work with device description

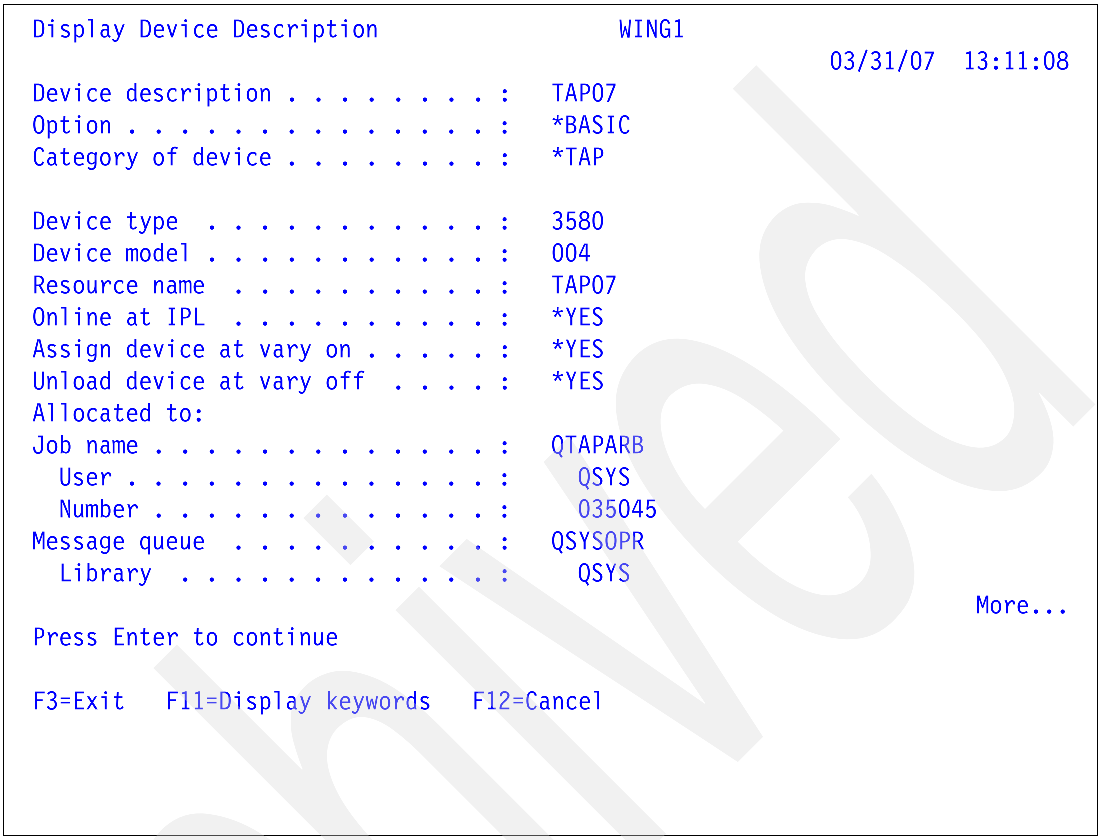
2. You are presented the screen with a list of tape devices described in i5/OS. In our example, the device description of the attached SCSI LTO4 tape drive is defined as TAP07. You can rename it as described later in this section. To observe details of the tape device description, specify option **5** at the relevant description, as shown in Figure 5-28. Press Enter.



```
Work with Device Descriptions
                                                             System:   WING1
Position to  . . . . .                Starting characters

Type options, press Enter.
  2=Change   3=Copy   4=Delete   5=Display   6=Print   7=Rename
  8=Work with status   9=Retrieve source

Opt  Device      Type        Text
     LTO4        3580        CREATED BY AUTO-CONFIGURATION
     TAP_FR3R10  3580        CREATED BY AUTO-CONFIGURATION
     TAP_FR3R4   3580        CREATED BY AUTO-CONFIGURATION
     TAPSPRMAN1  3592        CREATED BY AUTO-CONFIGURATION
     TAPSPRMAN2  3592        CREATED BY AUTO-CONFIGURATION
     TAP01       3580        CREATED BY AUTO-CONFIGURATION
     TAP02       3592        CREATED BY AUTO-CONFIGURATION
     TAP03       3580        CREATED BY AUTO-CONFIGURATION
 5   TAP07       3580        CREATED BY AUTO-CONFIGURATION

More...
 Parameters or command
```

Figure 5-28 Tape device descriptions

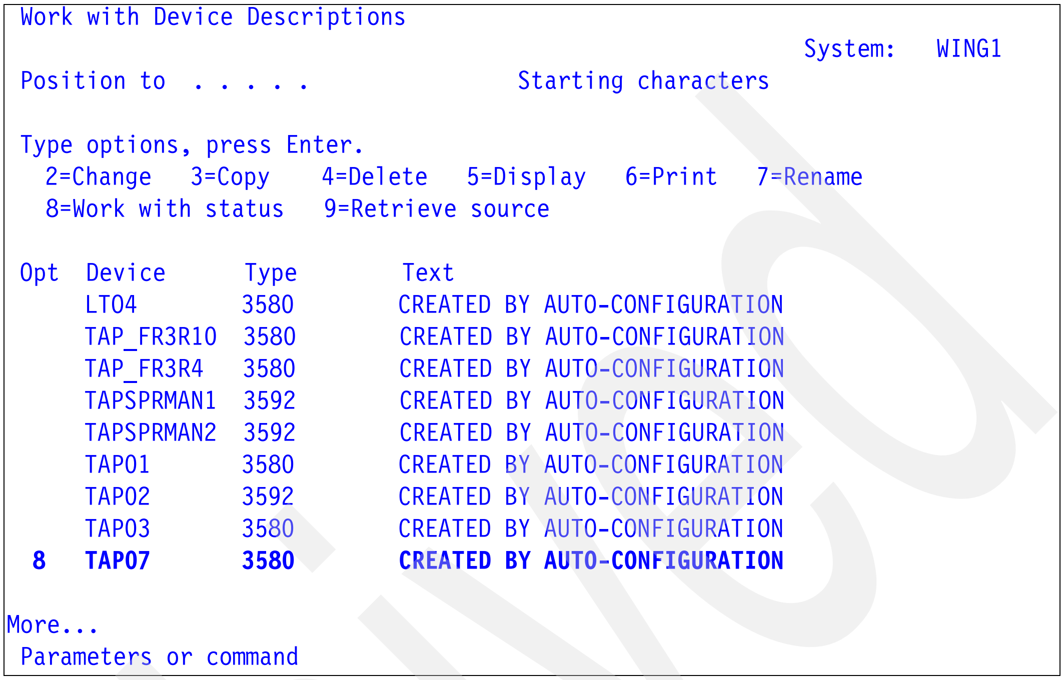
- The screen *Display Device Description*, containing specifications of the tape drive, is presented. You can observe type, model, resource name, and other specifications of the tape drive, as shown in Figure 5-29.



```
Display Device Description                       WING1
                                                                03/31/07  13:11:08

Device description . . . . . . . . :   TAP07
Option . . . . . . . . . . . . . . :   *BASIC
Category of device . . . . . . . . :   *TAP

Device type  . . . . . . . . . . . :   3580
Device model . . . . . . . . . . . :   004
Resource name  . . . . . . . . . . :   TAP07
Online at IPL  . . . . . . . . . . :   *YES
Assign device at vary on . . . . . :   *YES
Unload device at vary off  . . . . :   *YES
Allocated to:
Job name . . . . . . . . . . . . . :   QTAPARB
  User . . . . . . . . . . . . . . :     QSYS
  Number . . . . . . . . . . . . . :     035045
Message queue  . . . . . . . . . . :   QSYSOPR
  Library  . . . . . . . . . . . . :     QSYS
                                                                       More...

Press Enter to continue

F3=Exit   F11=Display keywords   F12=Cancel
```

Figure 5-29   Display Tape Device Description

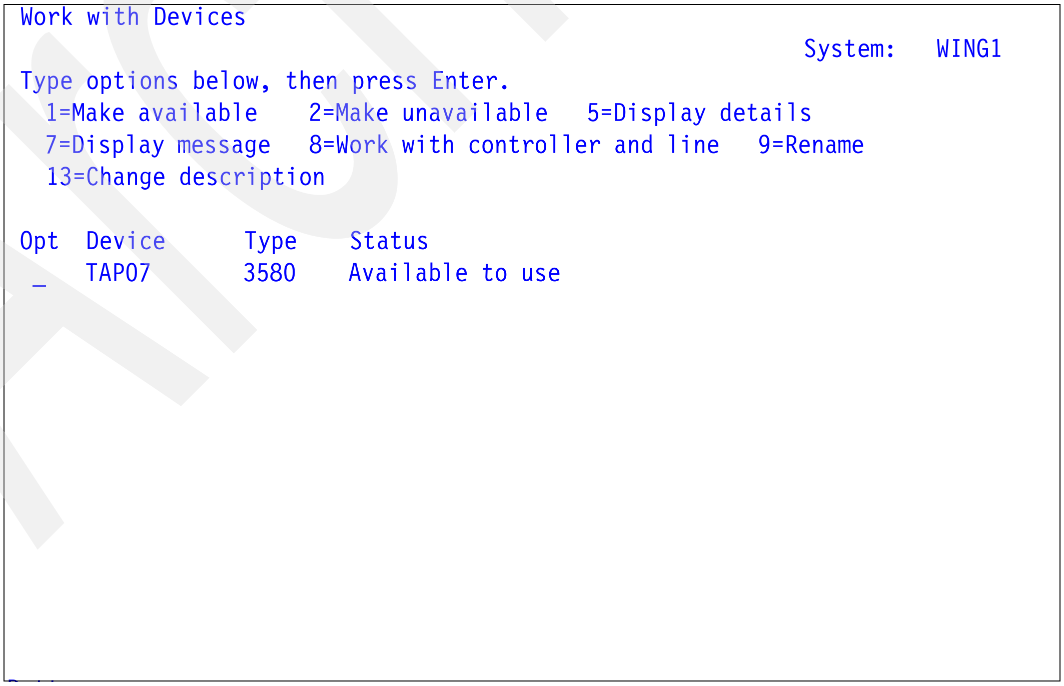
- On the screen *Display Device Description*, press **F12**. On the screen *Work with Device Descriptions*, specify **8 Work with Status** at the relevant tape device and press Enter, as shown in Figure 5-30.



```
 Work with Device Descriptions
                                                           System:   WING1
 Position to  . . . . .                Starting characters

 Type options, press Enter.
   2=Change    3=Copy    4=Delete    5=Display    6=Print    7=Rename
   8=Work with status    9=Retrieve source

 Opt  Device      Type        Text
      LTO4        3580        CREATED BY AUTO-CONFIGURATION
      TAP_FR3R10  3580        CREATED BY AUTO-CONFIGURATION
      TAP_FR3R4   3580        CREATED BY AUTO-CONFIGURATION
      TAPSPRMAN1  3592        CREATED BY AUTO-CONFIGURATION
      TAPSPRMAN2  3592        CREATED BY AUTO-CONFIGURATION
      TAP01       3580        CREATED BY AUTO-CONFIGURATION
      TAP02       3592        CREATED BY AUTO-CONFIGURATION
      TAP03       3580        CREATED BY AUTO-CONFIGURATION
  8   TAP07       3580        CREATED BY AUTO-CONFIGURATION

More...
 Parameters or command
```

Figure 5-30 Work with Device Description

- This displays the screen *Work with Devices*, as shown in Figure 5-31. Observe that the status of the tape drive is *Available to use* (varied-on). From this screen, you can make a tape drive available or unavailable by specifying relevant options.



```
 Work with Devices
                                                           System:   WING1
 Type options below, then press Enter.
   1=Make available    2=Make unavailable    5=Display details
   7=Display message   8=Work with controller and line    9=Rename
   13=Change description

 Opt  Device      Type    Status
  _   TAP07       3580    Available to use
```

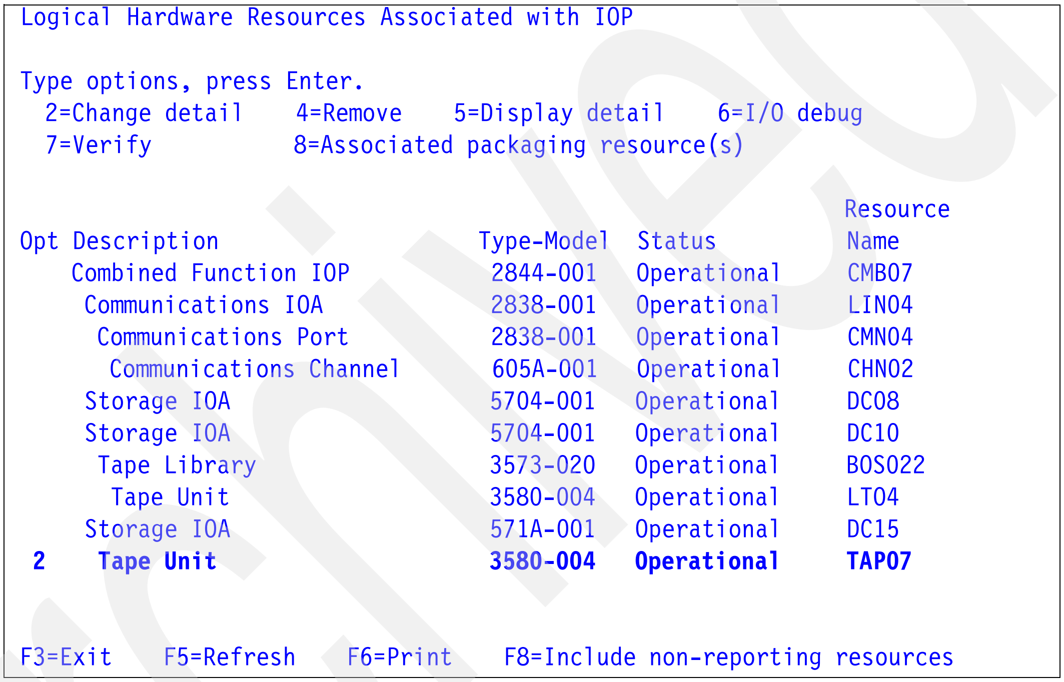
Figure 5-31 Work with Devices

Changing resource name and device description name in i5/OS

Especially in big installations with many tape drives and tape libraries, it can be convenient to rename tape resources and device descriptions so that you can quickly recognize them by name.

To rename a tape resource, perform the following steps:

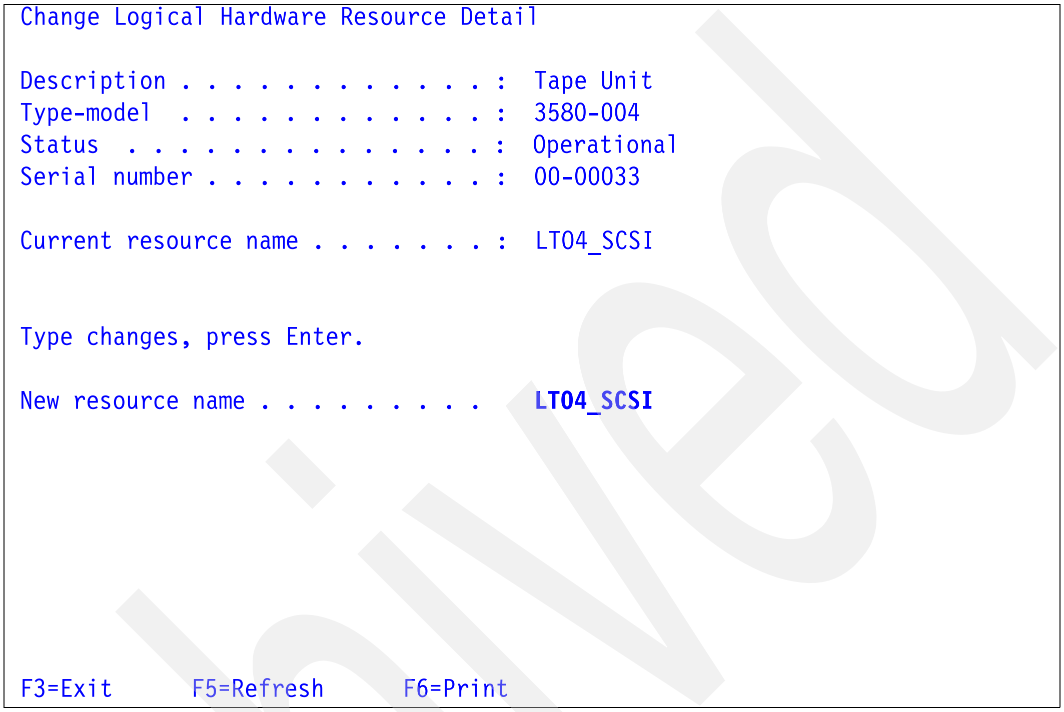
1. Make the tape unavailable by using a iSeries Navigator or green screen command, as explained in “Setting up the tape drive and connecting it to the System i partition”.
2. In i5/OS start SST and navigate to the screen *Logical Hardware Resources Associated with IOP*, as described in “Setting up the tape drive and connecting it to the System i partition”. Look for the tape resource you want to change the name, and specify option **2 Change detail at the tape resource**, as shown in Figure 5-32.



```
Logical Hardware Resources Associated with IOP

Type options, press Enter.
  2=Change detail    4=Remove    5=Display detail    6=I/O debug
  7=Verify           8=Associated packaging resource(s)

                                                              Resource
Opt Description                        Type-Model  Status         Name
    Combined Function IOP               2844-001   Operational    CMB07
     Communications IOA                 2838-001   Operational    LIN04
      Communications Port               2838-001   Operational    CMN04
       Communications Channel           605A-001   Operational    CHN02
     Storage IOA                        5704-001   Operational    DC08
     Storage IOA                        5704-001   Operational    DC10
      Tape Library                      3573-020   Operational    BOS022
       Tape Unit                        3580-004   Operational    LT04
     Storage IOA                        571A-001   Operational    DC15
 2    Tape Unit                         3580-004   Operational    TAP07


F3=Exit    F5=Refresh    F6=Print    F8=Include non-reporting resources
```

Figure 5-32 SST - Specify option Change detail

3. This displays the screen *Change Logical Hardware Resource Detail.* In this screen, change the name of tape resource and press Enter. At the bottom of the screen, you can see a confirmation message, *Change detail was successful*, as shown in Figure 5-33. Keep pressing F12 until you see the screen *Exit System Service Tools*. On this screen, press Enter to exit SST.



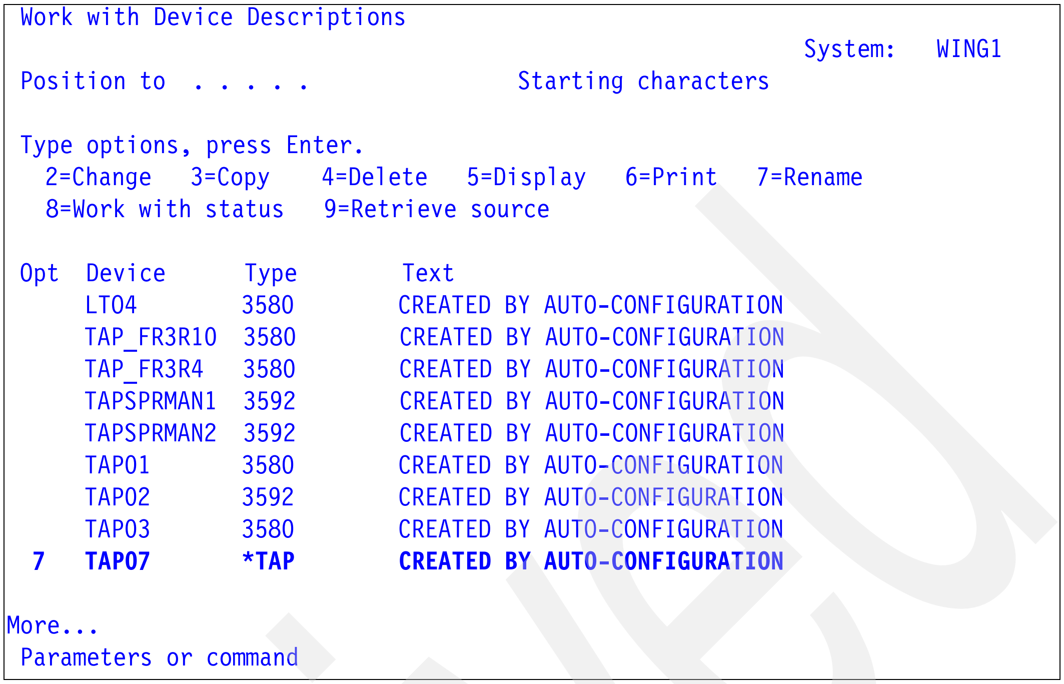
```
Change Logical Hardware Resource Detail

Description . . . . . . . . . . . . :  Tape Unit
Type-model  . . . . . . . . . . . . :  3580-004
Status  . . . . . . . . . . . . . . :  Operational
Serial number . . . . . . . . . . . :  00-00033

Current resource name . . . . . . . :  LTO4_SCSI


Type changes, press Enter.

New resource name . . . . . . . . .    LTO4_SCSI









F3=Exit      F5=Refresh      F6=Print
```

Figure 5-33 Changing tape resource name

To rename the tape device description, perform the following steps:

1. In the i5/OS green screen, type the command `WRKDEVD DEVD(*TAP)` as shown in Figure 5-27 on page 127. You are presented the screen *Work with Device Descriptions*. On this screen, look for the device description of the tape drive and specify option **7 Rename** at the tape description, as shown in Figure 5-34. Press Enter.

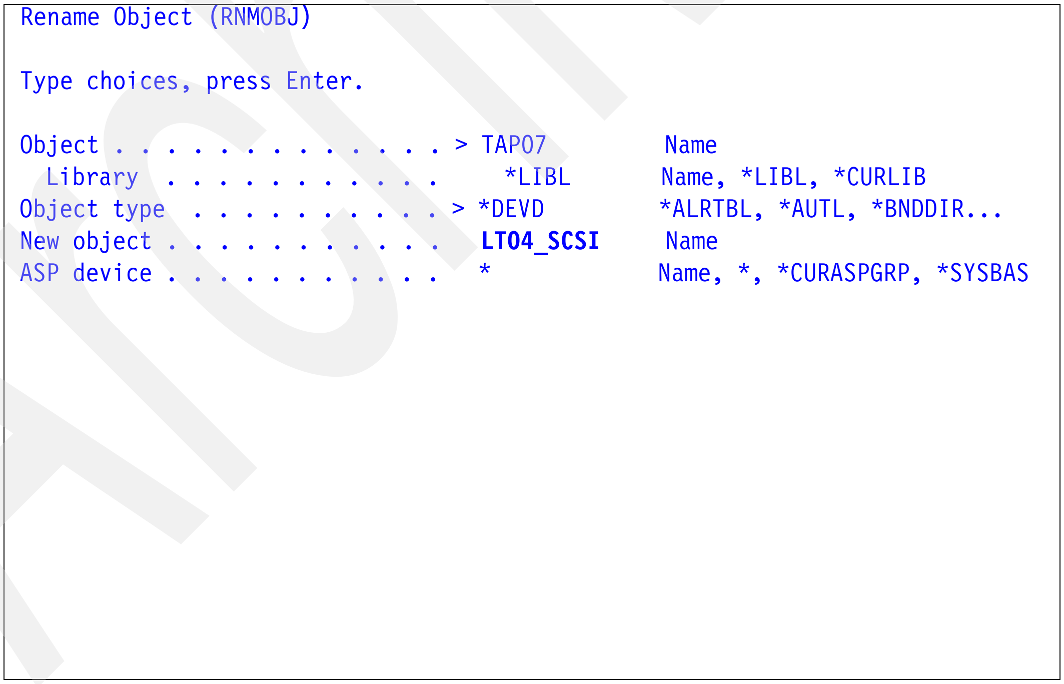
> **Note:** When you change the resource name, the device description automatically points to the changed resource name.



```
Work with Device Descriptions
                                                            System:   WING1
Position to  . . . . .                 Starting characters

Type options, press Enter.
  2=Change   3=Copy    4=Delete   5=Display   6=Print   7=Rename
  8=Work with status   9=Retrieve source

Opt  Device      Type        Text
     LTO4        3580        CREATED BY AUTO-CONFIGURATION
     TAP_FR3R10  3580        CREATED BY AUTO-CONFIGURATION
     TAP_FR3R4   3580        CREATED BY AUTO-CONFIGURATION
     TAPSPRMAN1  3592        CREATED BY AUTO-CONFIGURATION
     TAPSPRMAN2  3592        CREATED BY AUTO-CONFIGURATION
     TAP01       3580        CREATED BY AUTO-CONFIGURATION
     TAP02       3592        CREATED BY AUTO-CONFIGURATION
     TAP03       3580        CREATED BY AUTO-CONFIGURATION
 7   TAP07       *TAP        CREATED BY AUTO-CONFIGURATION

More...
 Parameters or command
```

Figure 5-34 Renaming tape device description

2. You are presented the screen *Rename Object*. Type the new name of the tape device description in the line *New Object*, as shown in Figure 5-35, and press Enter.



```
Rename Object (RNMOBJ)

Type choices, press Enter.

Object . . . . . . . . . . . . . > TAP07         Name
  Library  . . . . . . . . . . .     *LIBL       Name, *LIBL, *CURLIB
Object type  . . . . . . . . . . > *DEVD         *ALRTBL, *AUTL, *BNDDIR...
New object . . . . . . . . . . .   LTO4_SCSI     Name
ASP device . . . . . . . . . . .   *             Name, *, *CURASPGRP, *SYSBAS
```

Figure 5-35 Specifying new name for tape device description

Making a tape drive available for i5/OS

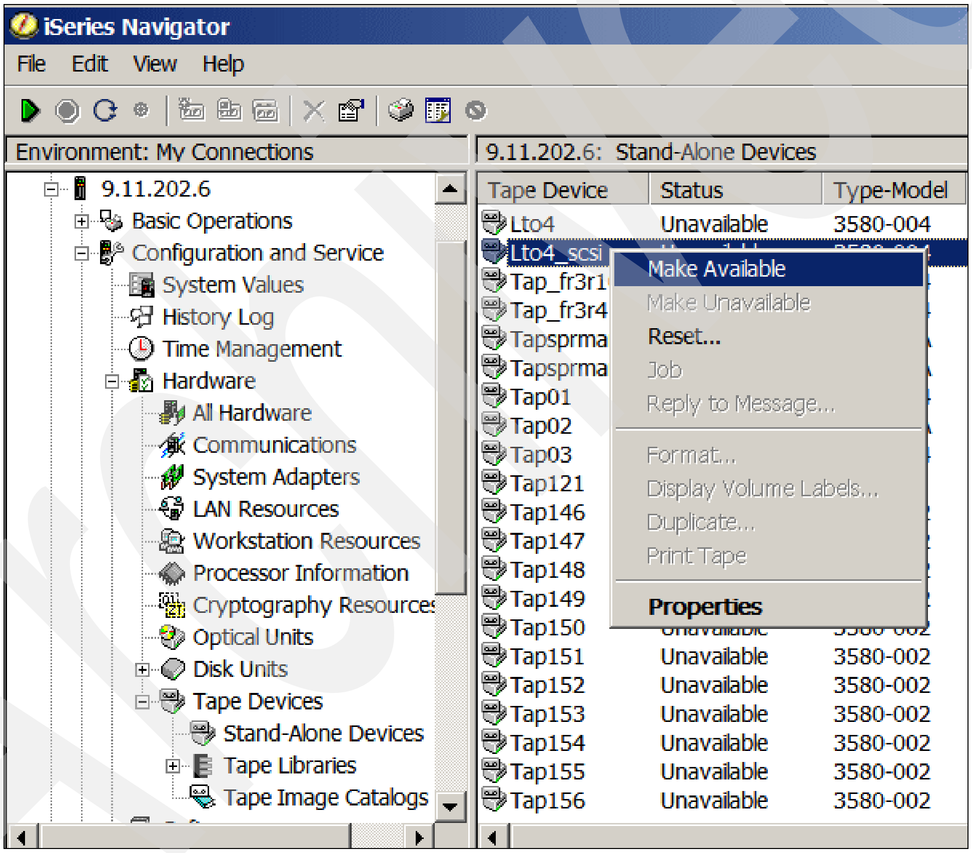
Before saving and restoring from a tape drive in i5/OS, make sure that the tape drive is available to use with i5/OS. For this, you can use the iSeries Navigator or the i5/OS green screen commands.

In the *iSeries Navigator*, perform the following steps to make a tape drive available:

1. Make a connection to the System i partition that contains the tape drive, if it is not yet made. Expand the System i IP address, expand *Configuration and Service*, expand *Hardware*, expand *Tape Devices*, and click **Stand-alone Devices**.

   These steps are described in “Setting up the tape drive and connecting it to the System i partition” on page 108.

2. On the right panel in iSeries Navigator are listed the tape devices. Check if the relevant tape device is listed as *Available*. If it is listed as *Unavailable*, right-click the tape device; this displays a pull-down menu. On the menu, click **Make Available,** as shown in Figure 5-36. This makes the tape drive available to use in i5/OS (varies-on a tape drive).



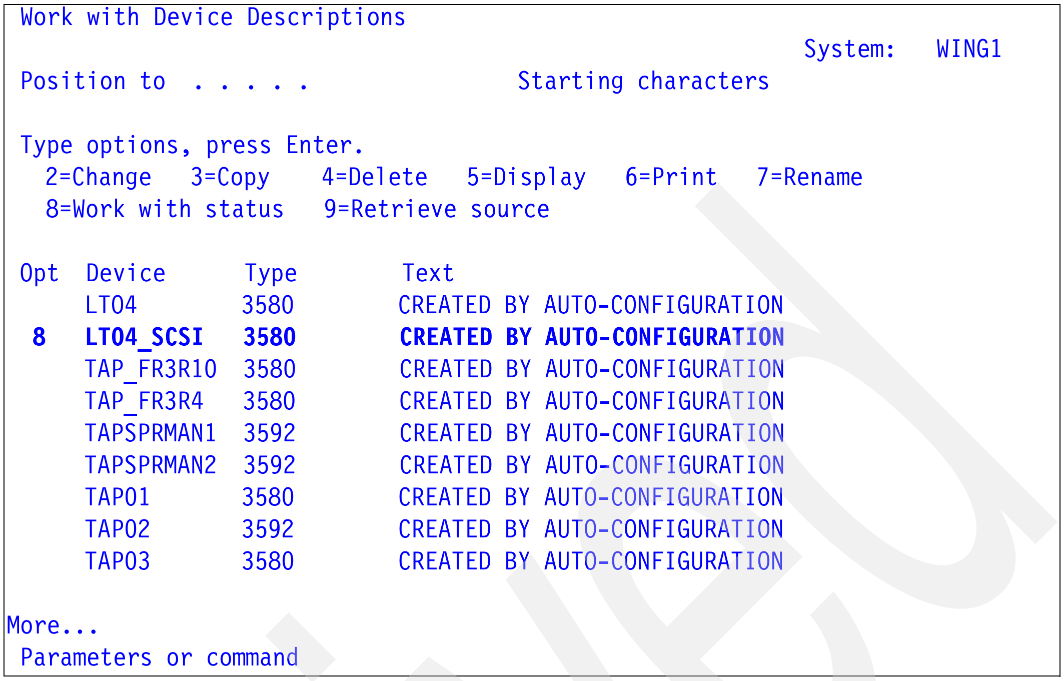
Tape Device	Status	Type-Model
Lto4	Unavailable	3580-004
Lto4_scsi		
Tap_fr3r1		
Tap_fr3r4		
Tapsprma		
Tapsprma		
Tap01		
Tap02		
Tap03		
Tap121		
Tap146		
Tap147		
Tap148		
Tap149		
Tap150		
Tap151	Unavailable	3580-002
Tap152	Unavailable	3580-002
Tap153	Unavailable	3580-002
Tap154	Unavailable	3580-002
Tap155	Unavailable	3580-002
Tap156	Unavailable	3580-002

Figure 5-36 iSeries navigator - Make tape drive available

On the i5/OS green screen, perform the following steps to make a tape drive available:

1. Sign in to the i5/OS green screen interface, and insert the command **`WRKDEVD DEVD(*TAP)`**, as described in “Setting up the tape drive and connecting it to the System i partition” on page 108.

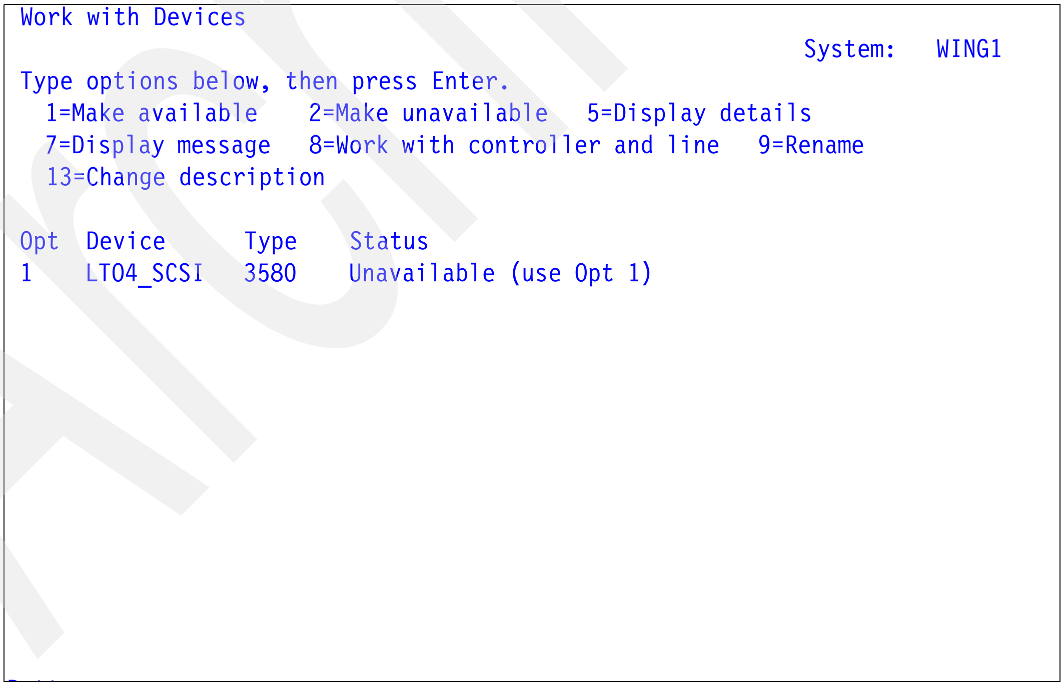
- In the display, *Work with Device Descriptions*, enter option **8 Work with status** at the relevant tape drive and press Enter. This is shown in Figure 5-37.



```
Work with Device Descriptions
                                                               System:   WING1
Position to  . . . . .                 Starting characters

Type options, press Enter.
  2=Change   3=Copy    4=Delete   5=Display   6=Print   7=Rename
  8=Work with status   9=Retrieve source

Opt  Device      Type        Text
     LTO4        3580        CREATED BY AUTO-CONFIGURATION
 8   LTO4_SCSI   3580        CREATED BY AUTO-CONFIGURATION
     TAP_FR3R10  3580        CREATED BY AUTO-CONFIGURATION
     TAP_FR3R4   3580        CREATED BY AUTO-CONFIGURATION
     TAPSPRMAN1  3592        CREATED BY AUTO-CONFIGURATION
     TAPSPRMAN2  3592        CREATED BY AUTO-CONFIGURATION
     TAP01       3580        CREATED BY AUTO-CONFIGURATION
     TAP02       3592        CREATED BY AUTO-CONFIGURATION
     TAP03       3580        CREATED BY AUTO-CONFIGURATION

More...
 Parameters or command
```

Figure 5-37 Work with tape drive status

2. This displays the screen *Work with Devices*. On this screen, check if the tape drive is available. If it is not, specify option **1 Make available** at the tape drive, as shown in Figure 5-38. Press Enter. This makes the tape drive available to use with i5/OS.



```
Work with Devices
                                                               System:   WING1
Type options below, then press Enter.
  1=Make available    2=Make unavailable   5=Display details
  7=Display message   8=Work with controller and line   9=Rename
  13=Change description

Opt  Device      Type     Status
1    LTO4_SCSI   3580     Unavailable (use Opt 1)
```

Figure 5-38 Make the tape drive available

5.1.2 Fibre Channel Tape Library

Next we describe the actions that you must do to set up a Fibre Channel Tape Library for i5/OS.

Setting up the tape library and connecting it to the System i partition

Similar to stand-alone tape drives, a tape library device and tape drives that belong to it are recognized by i5/OS as hardware resources as soon as they are physically connected to the System i partition. A correct and properly attached resource is reported in i5/OS as *operational*. Correct and properly attached resource reports in i5/OS as *operational*. In case the tape library or tape devices are physically damaged or not correctly connected to the System i partition, the corresponding tape resources do not report it at all, or report it as *failed*.

If the i5/OS System value *QAUTOCFG* is set to *On,* i5/OS automatically creates the necessary device description for the tape library device and for the tape drives belonging to it. However, if the system value *QAUTOCFG* is set to *Off,* you have to create a device description for any new device attached to the system.

After a tape library with tape drives is recognized and described by i5/OS, the correct status of devices is as follows:

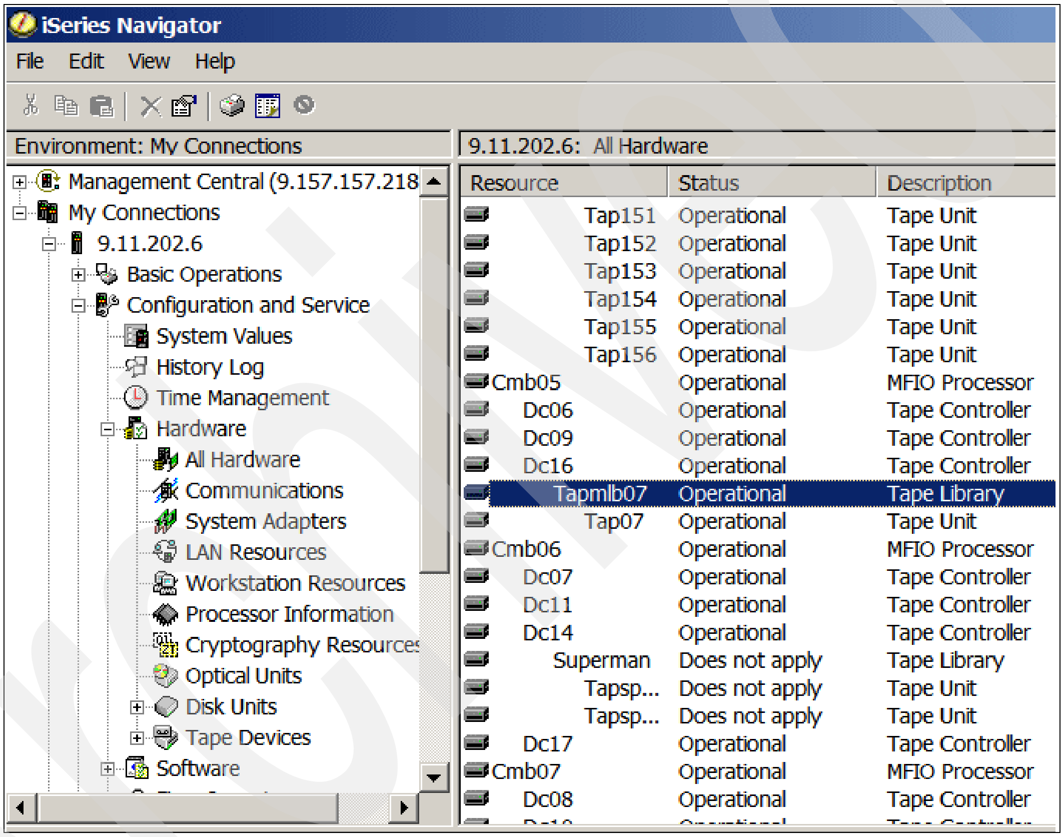
- Tape library device is available (varied-on).
- Tape drive devices belonging to the tape library are unavailable (varied off) and they are unprotected (shared). For more information about unprotected tape drives, refer to 5.2, “Sharing tape drives among multiple partitions” on page 142.

To check the hardware resources and i5/OS device descriptions of tape library and tape drives in the library, you can use iSeries Navigator, or i5/OS green screen commands.

In **iSeries Navigator**, perform the following steps to check the newly connected tape library:

1. In the iSeries Navigator, make a connection to the System i partition that contains the tape library, if it is not yet made.
2. In the iSeries navigator left panel, expand the IP address of the relevant System i partition, expand *Hardware*, and expand *All Hardware*. In the right panel, you see the available hardware resources. Look for the hardware resource of the connected tape library. Observe the tape device resources that belong to the tape library: they are listed under the library resource.

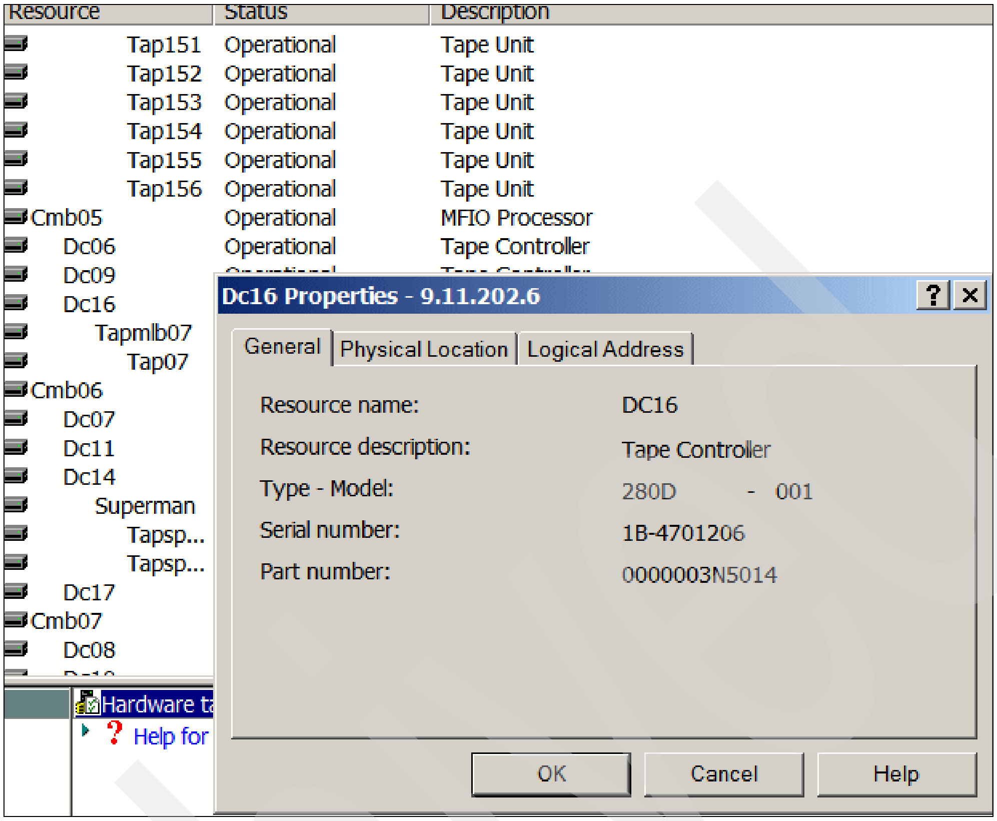
   Make sure that all resources are operational. In our example, tape library resource shows as Tapmlb07 and the corresponding tape resource shows as Tap07. This is shown in Figure 5-39.



Resource	Status	Description
Tap151	Operational	Tape Unit
Tap152	Operational	Tape Unit
Tap153	Operational	Tape Unit
Tap154	Operational	Tape Unit
Tap155	Operational	Tape Unit
Tap156	Operational	Tape Unit
Cmb05	Operational	MFIO Processor
Dc06	Operational	Tape Controller
Dc09	Operational	Tape Controller
Dc16	Operational	Tape Controller
Tapmlb07	Operational	Tape Library
Tap07	Operational	Tape Unit
Cmb06	Operational	MFIO Processor
Dc07	Operational	Tape Controller
Dc11	Operational	Tape Controller
Dc14	Operational	Tape Controller
Superman	Does not apply	Tape Library
Tapsp...	Does not apply	Tape Unit
Tapsp...	Does not apply	Tape Unit
Dc17	Operational	Tape Controller
Cmb07	Operational	MFIO Processor
Dc08	Operational	Tape Controller

Figure 5-39 iSeries Navigator - tape library resources

3. In the iSeries Navigator right panel, right-click the Tape Controller to which the tape library is connected, and click the button **Properties**. This displays the panel tape controller (FC adapter) properties, where you can observe its characteristics and location. In our example, the Tape Library is attached to the Fibre Channel Tape controller feature number #5761, which reports in i5/OS as type 280D. This is shown in Figure 5-40.



Resource	Status	Description
Tap151	Operational	Tape Unit
Tap152	Operational	Tape Unit
Tap153	Operational	Tape Unit
Tap154	Operational	Tape Unit
Tap155	Operational	Tape Unit
Tap156	Operational	Tape Unit
Cmb05	Operational	MFIO Processor
Dc06	Operational	Tape Controller
Dc09		
Dc16		
Tapmlb07		
Tap07		
Cmb06		
Dc07		
Dc11		
Dc14		
Superman		
Tapsp...		
Tapsp...		
Dc17		
Cmb07		
Dc08		

Dc16 Properties - 9.11.202.6

General | Physical Location | Logical Address

Resource name:	DC16
Resource description:	Tape Controller
Type - Model:	280D - 001
Serial number:	1B-4701206
Part number:	0000003N5014

Figure 5-40 iSeries Navigator FC Tape Controller with tape library

- In the iSeries Navigator left panel, expand *Tape Devices*, expand *Tape Libraries*, look for the newly connected tape library, and expand it. Right-click the tape library and select **Properties** from the pull-down menu that pops up, as shown in Figure 5-41.

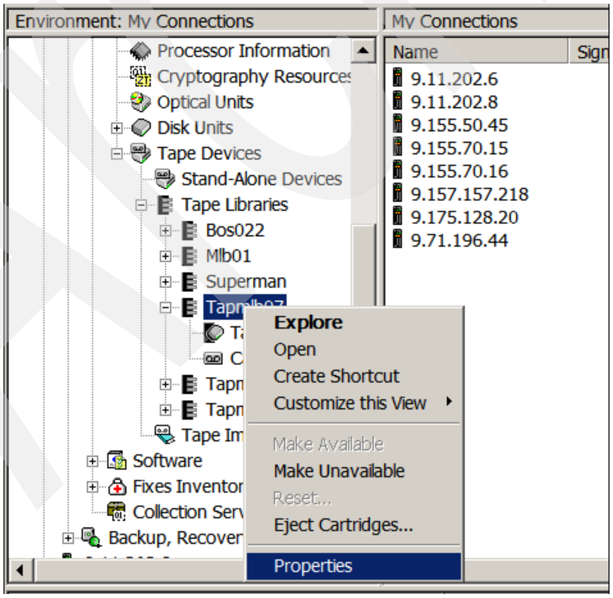
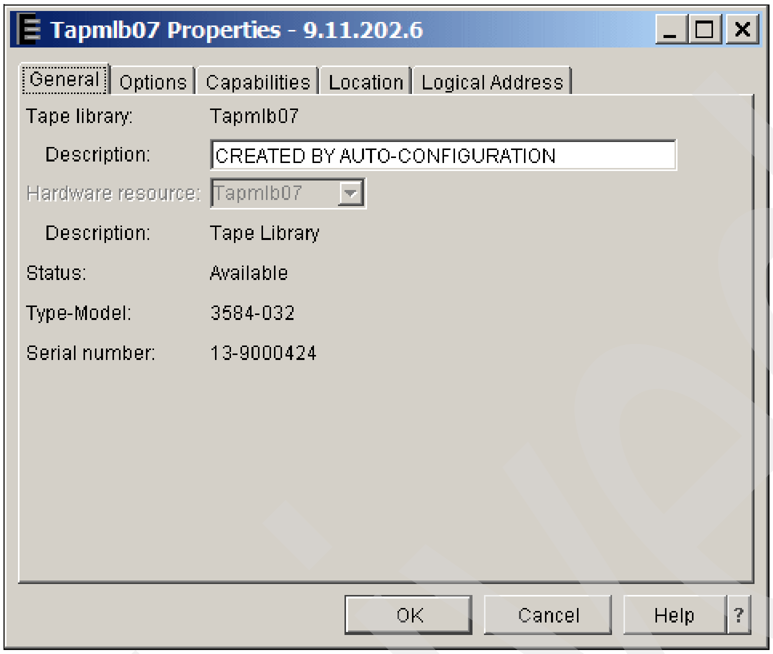


Figure 5-41 Series Navigator - bring up tape library properties

e. This displays the panel tape library properties in which you can observe characteristics and of the tape library device and location of attachment in System i partition. This is shown in Figure 5-42.



Tapmlb07 Properties - 9.11.202.6

Tape library: Tapmlb07

Description: CREATED BY AUTO-CONFIGURATION

Hardware resource: Tapmlb07

Description: Tape Library

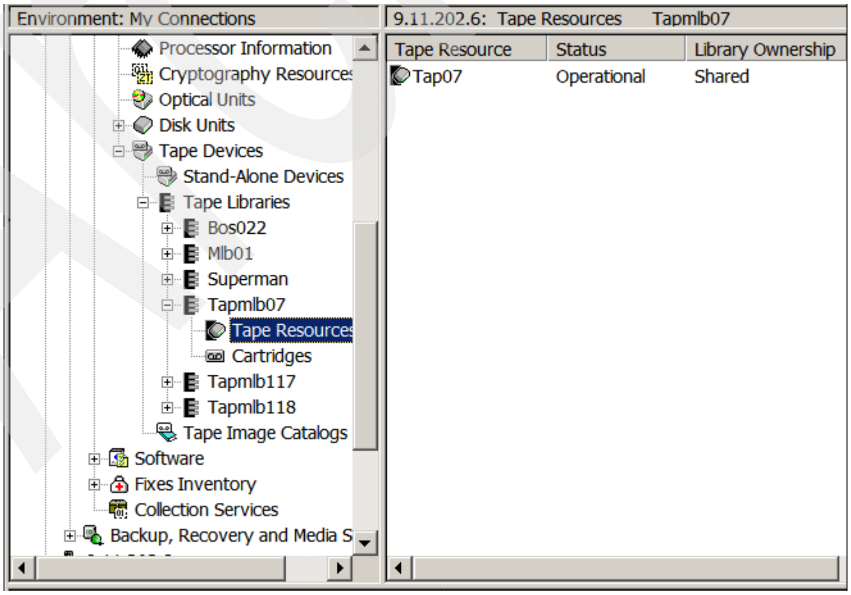
Status: Available

Type-Model: 3584-032

Serial number: 13-9000424

Figure 5-42 iSeries Navigator - tape library properties

4. In the left panel, click **Tape Resources** under the name of the tape library. This displays a list of tape drives in the tape library, which are shown in the right panel. Initially the library ownership for each tape drive is defined as *Shared (Unprotected)*. For more information about library ownership, refer to 5.2, “Sharing tape drives among multiple partitions” on page 142. In our example, one tape drive is listed; it is defined as Shared, as can be seen in Figure 5-43.

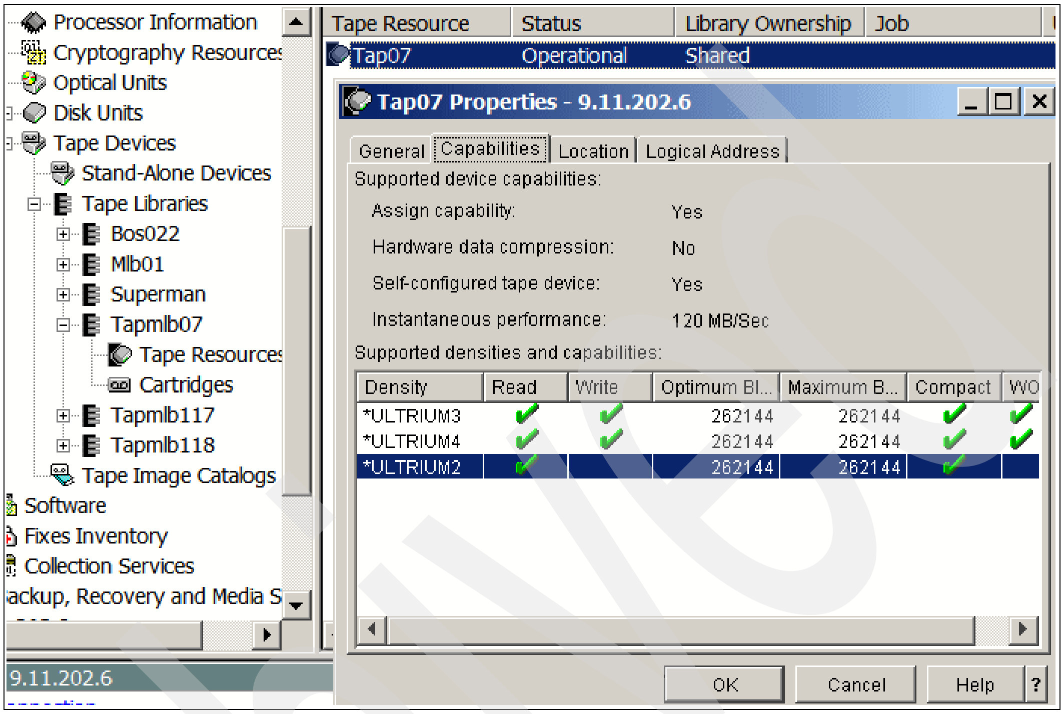


9.11.202.6: Tape Resources Tapmlb07

Tape Resource	Status	Library Ownership
Tap07	Operational	Shared

Figure 5-43 iSeries Navigator - Tape drives in the tape library

5. On the right panel, right-click the tape drive and select Properties from the pull-down menu that pops up. This displays the *Tape Properties* panel, on which you can observe characteristics of the tape drive and its placement in System i partition. This is shown in Figure 5-44.



Supported device capabilities:

Assign capability: Yes

Hardware data compression: No

Self-configured tape device: Yes

Instantaneous performance: 120 MB/Sec

Supported densities and capabilities:

Density	Read	Write	Optimum Bl...	Maximum B...	Compact	WO
*ULTRIUM3	✓	✓	262144	262144	✓	✓
*ULTRIUM4	✓	✓	262144	262144	✓	✓
*ULTRIUM2	✓		262144	262144	✓	

Figure 5-44 iSeries Navigator - properties of tape drive in the tape library

In the i5/OS command interface and SST, perform the following steps:

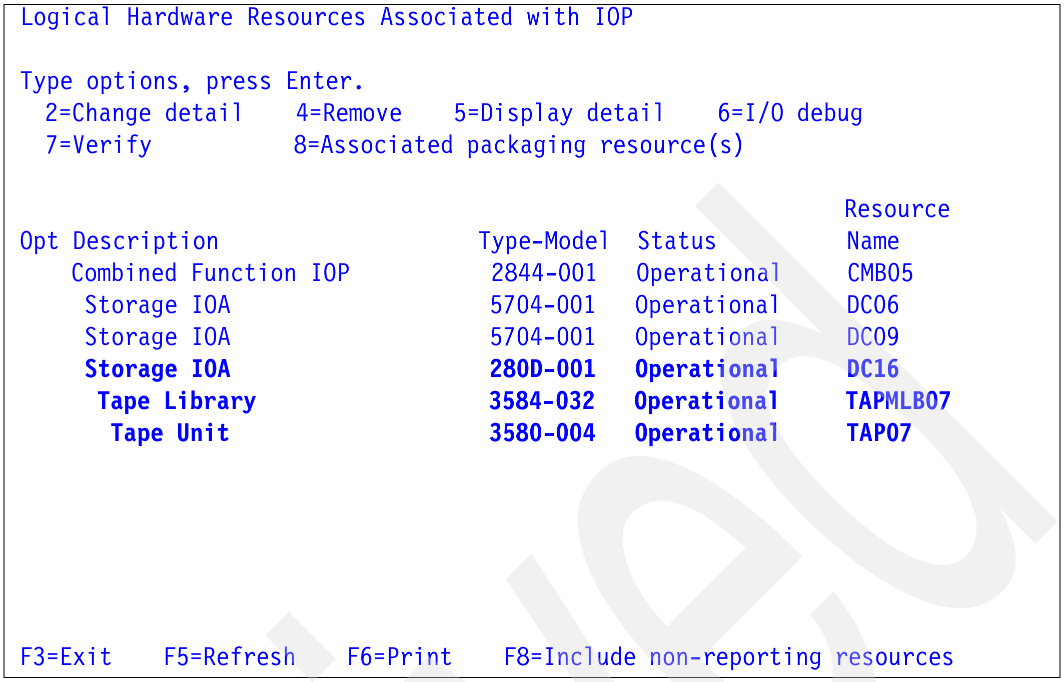
1. Connect to the System i partition via IP telnet, by using the IBM Personal communications tool. For more information about Personal communications, refer to System i Information center at the following Web site:

   `http://publib.boulder.ibm.com/iseries/`

2. After you are connected to i5/OS, start SST and navigate to the SST screen, *Logical Hardware Resources on System Bus*, as described in "Setting up the tape drive and connecting it to the System i partition" on page 108.

3. Specify option **9 Resources associated with IOP** at the IOP to which the tape library is connected. This displays the screen *Logical Hardware Resources Associated with IOP*, where you can observe the status of hardware resources for tape library and tape drives in the library, and check that resources report are operational. In our example, the tape library TAPLIB07 with tape drive TAP07 is connected via FC adapter feature #5761 (reporting as feature 280D). This is shown in Figure 5-45.

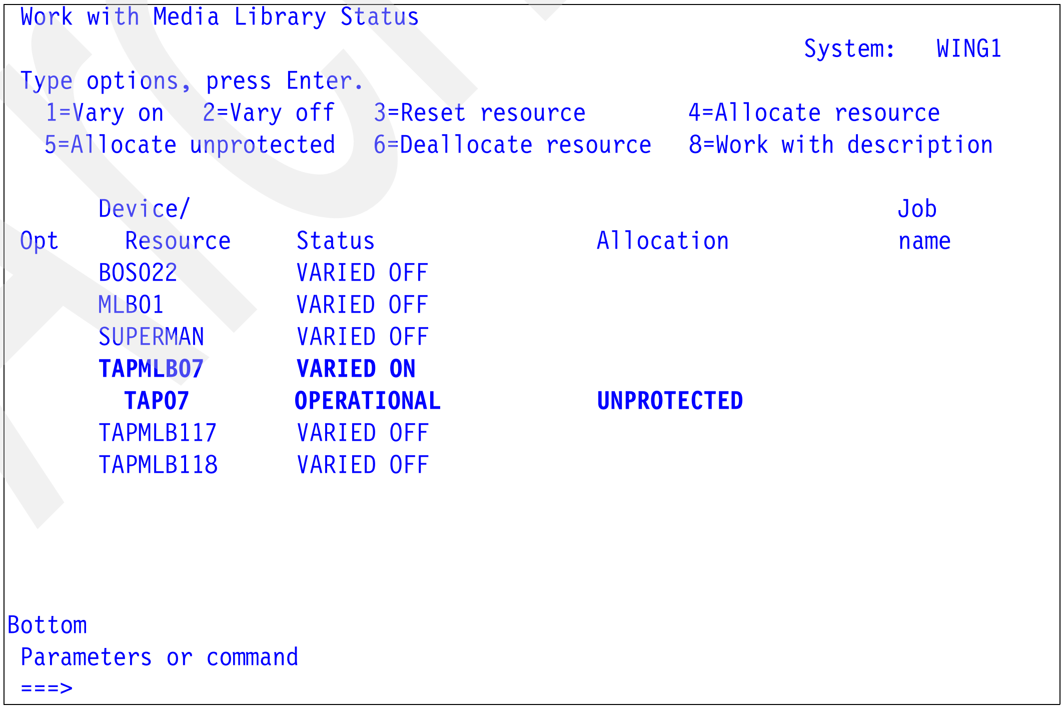
   Note: If you do not know to which IOP the library is connected, you have to look at the hardware resources of each IOP, or use iSeries Navigator to recognize to which IOP the library is attached.



```
Logical Hardware Resources Associated with IOP

Type options, press Enter.
  2=Change detail    4=Remove     5=Display detail    6=I/O debug
  7=Verify           8=Associated packaging resource(s)

                                                                   Resource
Opt Description                        Type-Model  Status           Name
    Combined Function IOP               2844-001   Operational      CMB05
     Storage IOA                        5704-001   Operational      DC06
     Storage IOA                        5704-001   Operational      DC09
     Storage IOA                        280D-001   Operational      DC16
      Tape Library                      3584-032   Operational      TAPMLB07
       Tape Unit                        3580-004   Operational      TAP07








F3=Exit    F5=Refresh    F6=Print    F8=Include non-reporting resources
```

Figure 5-45 SST - Hardware resources of tape library and tape drive

4. Exit from SST as described in “Setting up the tape drive and connecting it to the System i partition” on page 108. In the i5/OS green screen, enter the command **WRKMLBSTS**, this displays the screen *Work with Media Library Status*. Look for the newly connected tape library, and the tape drive that belongs to it. Check if the tape library is Available (varied-on) and the tape drive is Operational and Unprotected. TAPMLB07 is varied-on, and tape drive TAP07 is Unprotected (Figure 5-46). For more information about the status unprotected, refer to 5.2, “Sharing tape drives among multiple partitions” on page 142.



```
Work with Media Library Status
                                                          System:   WING1
Type options, press Enter.
  1=Vary on   2=Vary off   3=Reset resource       4=Allocate resource
  5=Allocate unprotected   6=Deallocate resource  8=Work with description

      Device/                                                     Job
Opt     Resource      Status                Allocation            name
      BOS022          VARIED OFF
      MLB01           VARIED OFF
      SUPERMAN        VARIED OFF
      TAPMLB07        VARIED ON
        TAP07         OPERATIONAL           UNPROTECTED
      TAPMLB117       VARIED OFF
      TAPMLB118       VARIED OFF




Bottom
 Parameters or command
 ===>
```

Figure 5-46 i5/OS - Work with Tape libraries

Changing resource name and device description in i5/OS

For instructions on how to change the resource name and device description of a tape library and the tape drive in the library, refer to “Changing resource name and device description in i5/OS”. The described procedure for a stand-alone tape drive applies also to a tape library.

Making a tape library available in i5/OS

For information how to make a tape library available, refer to “Making a tape drive available for i5/OS” on page 133. The described procedure for a stand-alone tape drive applies also to a tape library.

Tape pooling in i5/OS

When the tape drives in a tape library are connected via multiple System i FC adapters, i5/OS creates a device description TAPMLBxx for each System i adapter. The tape drives connected through a particular adapter are seen under the corresponding TAPMLBxx, this is because the library control path is enabled for each FC adapter connecting tape drives in the tape library.

To make all tape drives seen under the same tape library device, perform the following steps:

- Make both Tape libraries unavailable.
- Make one tape library available.

After this is done, all tape drives are seen under the device description of the available tape library.

Tape pooling in i5/OS is shown in Figure 5-47.

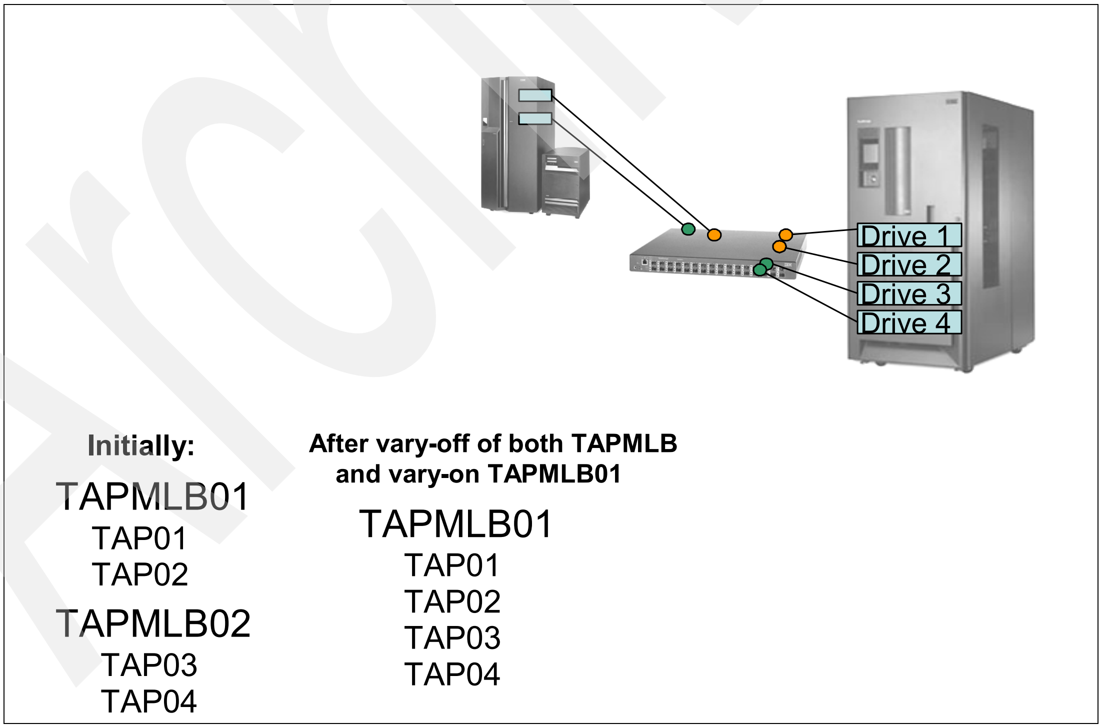


Figure 5-47 Tape pooling

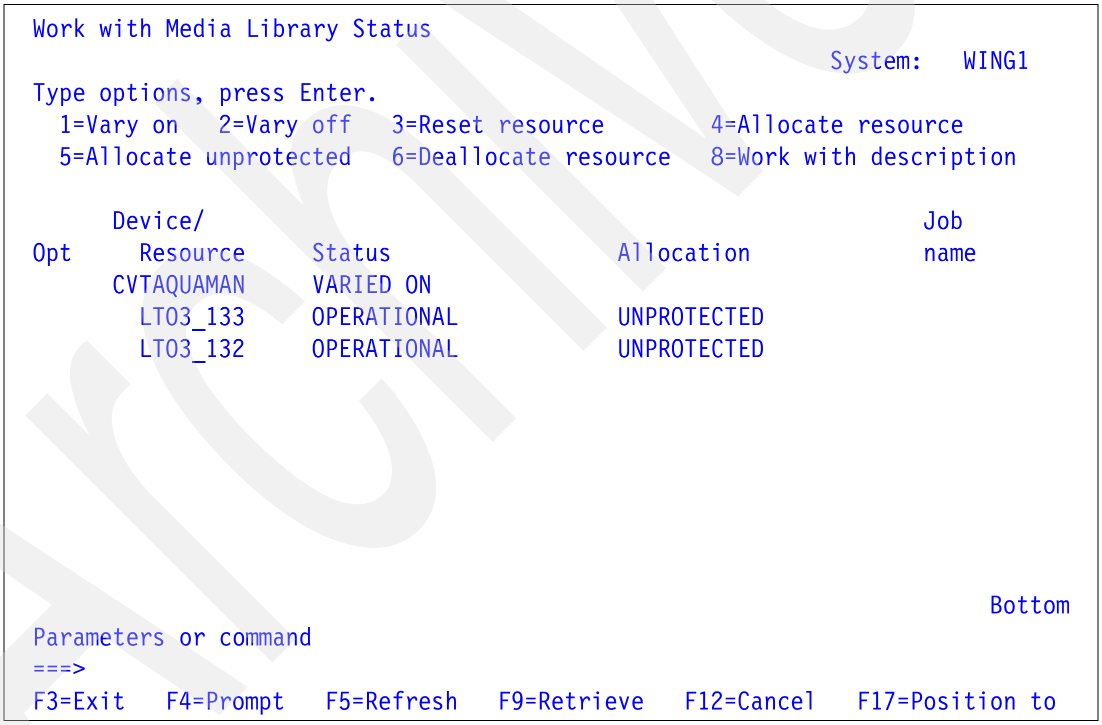
5.2 Sharing tape drives among multiple partitions

A stand-alone tape drive or a tape drive in a tape library can be shared among different System i partitions, or among System i partitions and servers other than System i. Tape sharing is achieved using the Reserve/Release functionality as described in“Shared drive assignment” on page 63.

When sharing a tape drive in a tape library among System i partitions, we recommend that you allocate the drive to a tape library as *Unprotected*. In this case the tape resource is available for use in the library device, and the resource has not been assigned or reserved to this system. The tape resource is available to the resource manager. Any attached system can share this tape resource.

As a request comes to the resource manager for a tape resource, an assign/reserve command is attempted to the device (this command is executed at the i5/OS Licensed Internal Code level and you cannot see it). If the system cannot obtain an assign/reserve, other available resources are used. If no other resources are available, the system waits for an available resource to successfully obtain an assign/reserve to the system. The wait is based on the MAXDEVTIME parameter in the device description.

Figure 5-48 shows tape library description with Protected tape drives in i5/OS.



```
Work with Media Library Status
                                                            System:   WING1
Type options, press Enter.
  1=Vary on   2=Vary off   3=Reset resource        4=Allocate resource
  5=Allocate unprotected   6=Deallocate resource   8=Work with description

      Device/                                                  Job
Opt     Resource     Status                 Allocation             name
      CVTAQUAMAN     VARIED ON
        LTO3_133     OPERATIONAL            UNPROTECTED
        LTO3_132     OPERATIONAL            UNPROTECTED






                                                                       Bottom
Parameters or command
===>
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve   F12=Cancel   F17=Position to
```

Figure 5-48 Tape drives allocated as Unprotected

5.3 Save and restore using basic i5/OS commands

Although customers are encouraged to use Backup Recovery and Media Services for their backup operations, some smaller installations might still use basic i5/OS commands for save and restore. In this section we describe save and restore of a database library to (from) a stand-alone tape drive, and save and restore of a database library to (from) a tape library.

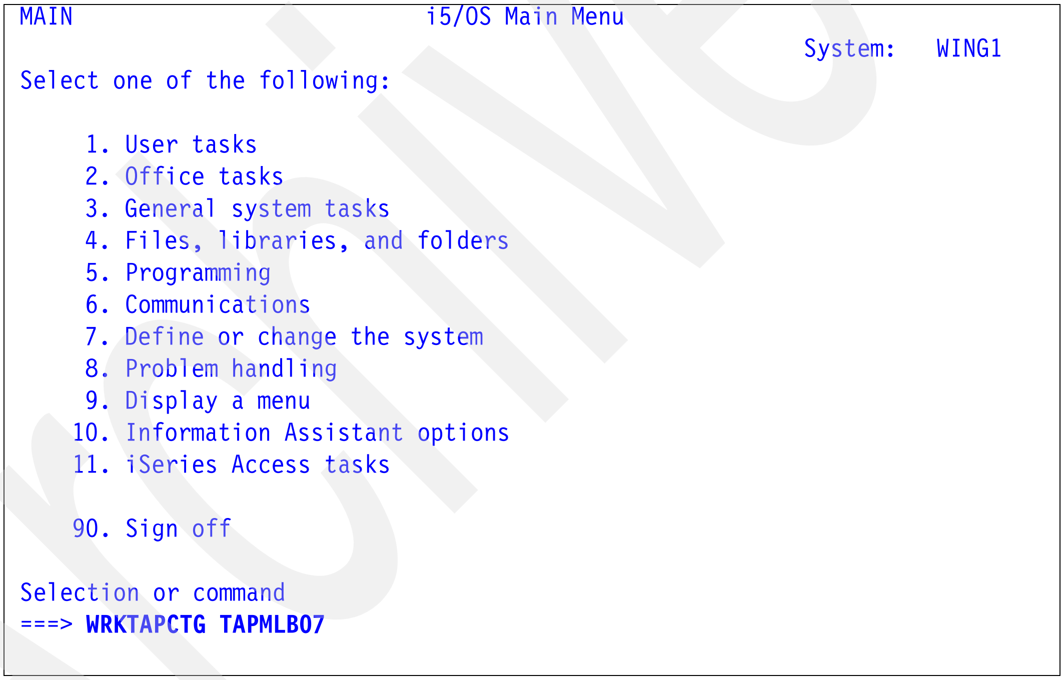
5.3.1 Saving a database library to a tape library

To save an i5/OS database library to a data cartridge in a tape library, perform the following steps:

1. Connect to the System i partition via IP telnet, by using the IBM Personal communications tool. For more information about Personal communications, refer to the System i Information center on the following Web site:

   `http://publib.boulder.ibm.com/iseries/`

2. In the i5/OS command interface, insert the command **WRKTAPCTG** followed by the name of the tape library, as shown in Figure 5-49.



```
MAIN                              i5/OS Main Menu
                                                              System:   WING1
Select one of the following:

     1. User tasks
     2. Office tasks
     3. General system tasks
     4. Files, libraries, and folders
     5. Programming
     6. Communications
     7. Define or change the system
     8. Problem handling
     9. Display a menu
    10. Information Assistant options
    11. iSeries Access tasks

    90. Sign off

Selection or command
===> WRKTAPCTG TAPMLB07
```

Figure 5-49 WRKTAPCTG

3. You are presented the screen *Work with Tape Cartridges* showing available data cartridges in this particular tape library.

   Following are some types of status for a cartridge in a tape library, as recognized by i5/OS:

   Inserted The cartridge has been inserted into the library.

   Available The cartridge ID is available for use.

   Mounted The cartridge is mounted in a tape device or in the queue ready to be loaded.

   Ejected The cartridge ID is in the *EJECT category or it was manually ejected from the library device.

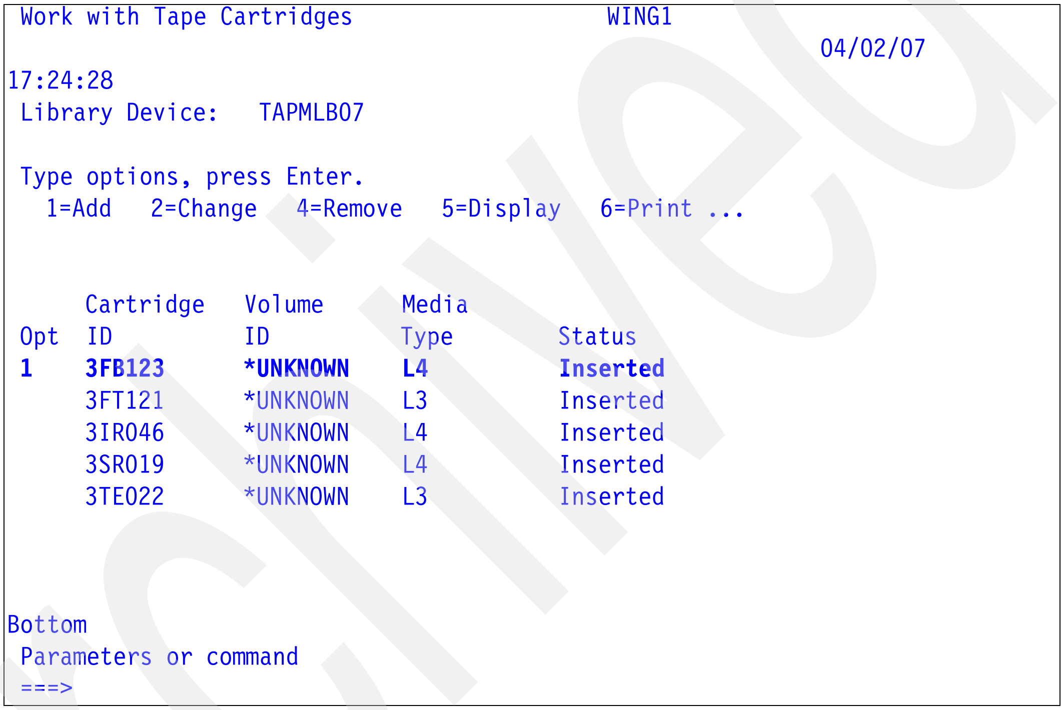
4. In our example, all data cartridges have status *Inserted*, as can be seen in Figure 5-50. Before using a data cartridge, the cartridge must be added to one of the categories in i5/OS. Following are some of the categories that are defined as default in i5/OS:

   ***NOSHARE** The cartridge in this category cannot be shared with other systems that are attached to the same device.

   ***SHARE400** The cartridge in this category can be shared with other System i partitions that are attached to the same device.

   ***IPL** The cartridge in this category can be used for an alternate initial program load (IPL) of a system.

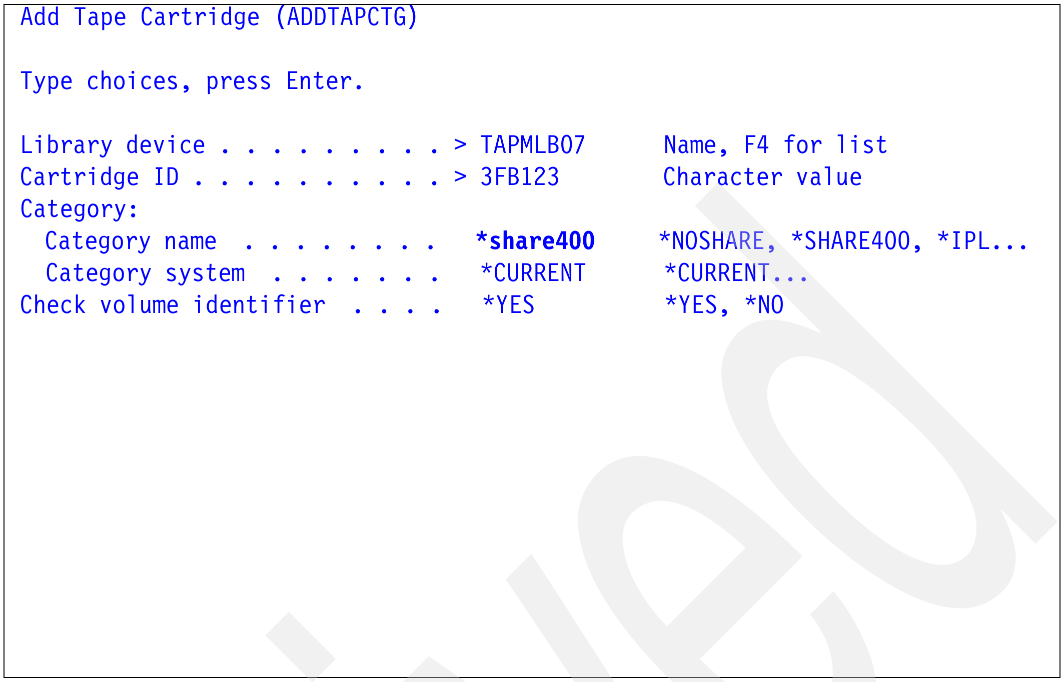
   Look for the data cartridge you want to use, and add it to a category, by specifying option **1 Add** at the cartridge, as shown in Figure 5-50, then press **F4**.



```
 Work with Tape Cartridges                       WING1
                                                                04/02/07
17:24:28
 Library Device:   TAPMLB07

 Type options, press Enter.
   1=Add   2=Change   4=Remove   5=Display   6=Print ...


      Cartridge   Volume      Media
 Opt  ID          ID          Type        Status
 1    3FB123      *UNKNOWN    L4          Inserted
      3FT121      *UNKNOWN    L3          Inserted
      3IR046      *UNKNOWN    L4          Inserted
      3SR019      *UNKNOWN    L4          Inserted
      3TE022      *UNKNOWN    L3          Inserted



Bottom
 Parameters or command
 ===>
```

Figure 5-50 Add data cartridge to a cartridge category

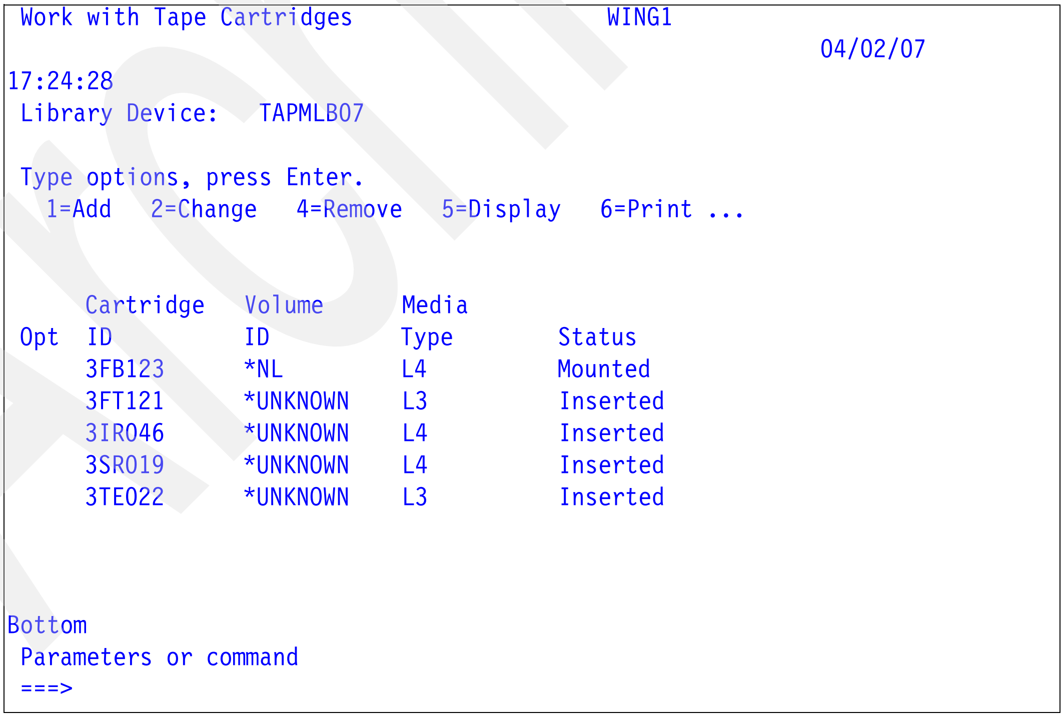
5. Using F4 only, many i5/OS commands result in prompting for required parameters. After pressing F4, you are presented the screen *Add Tape Cartridge (ADDTAPCTG)*, where you specify parameters for this command. You specify the category to which the cartridge must be added. In our example, we add it to category *SHARE400, as shown in Figure 5-51.



```
Add Tape Cartridge (ADDTAPCTG)

Type choices, press Enter.

Library device . . . . . . . . . > TAPMLB07      Name, F4 for list
Cartridge ID . . . . . . . . . . > 3FB123        Character value
Category:
  Category name  . . . . . . . .   *share400    *NOSHARE, *SHARE400, *IPL...
  Category system  . . . . . . .   *CURRENT      *CURRENT...
Check volume identifier  . . . .   *YES          *YES, *NO
```

Figure 5-51 Adding a data cartridge to category *SHARE400

6. Adding an inserted cartridge in a category results in mounting the cartridge to a tape drive. The message which is displayed after the cartridge is successfully added to a category indicates this. This is shown in Figure 5-52.



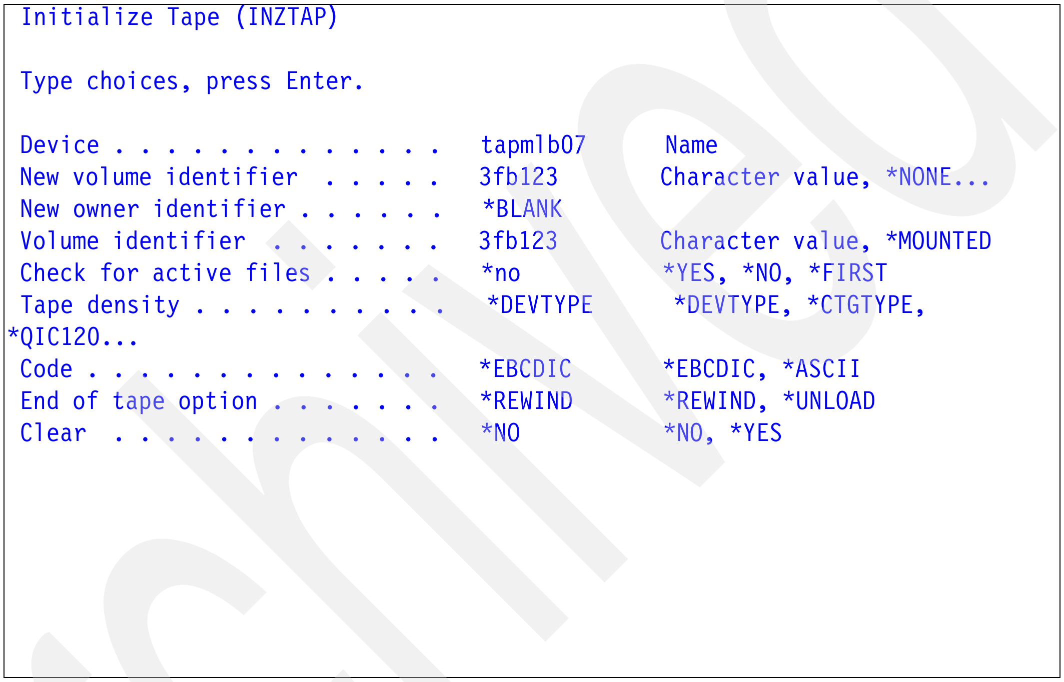
```
 Work with Tape Cartridges                     WING1
                                                                 04/02/07
17:24:28
 Library Device:    TAPMLB07

 Type options, press Enter.
   1=Add    2=Change    4=Remove    5=Display    6=Print ...


      Cartridge    Volume      Media
 Opt  ID           ID          Type        Status
      3FB123       *NL         L4          Mounted
      3FT121       *UNKNOWN    L3          Inserted
      3IR046       *UNKNOWN    L4          Inserted
      3SR019       *UNKNOWN    L4          Inserted
      3TE022       *UNKNOWN    L3          Inserted



Bottom
 Parameters or command
 ===>
```

Figure 5-52 Cartridge added to category and mounted

7. Next you might want to initialize the mounted data cartridge. To do this, enter the i5/OS command **INZTAP** and press F4 for a command prompt. You are presented the screen, *Initialize Tape*. In the screen, insert the following parameters:

   – Name of the tape library
   – New cartridge identifier
   – Current cartridge identifier
   – Density of the cartridge

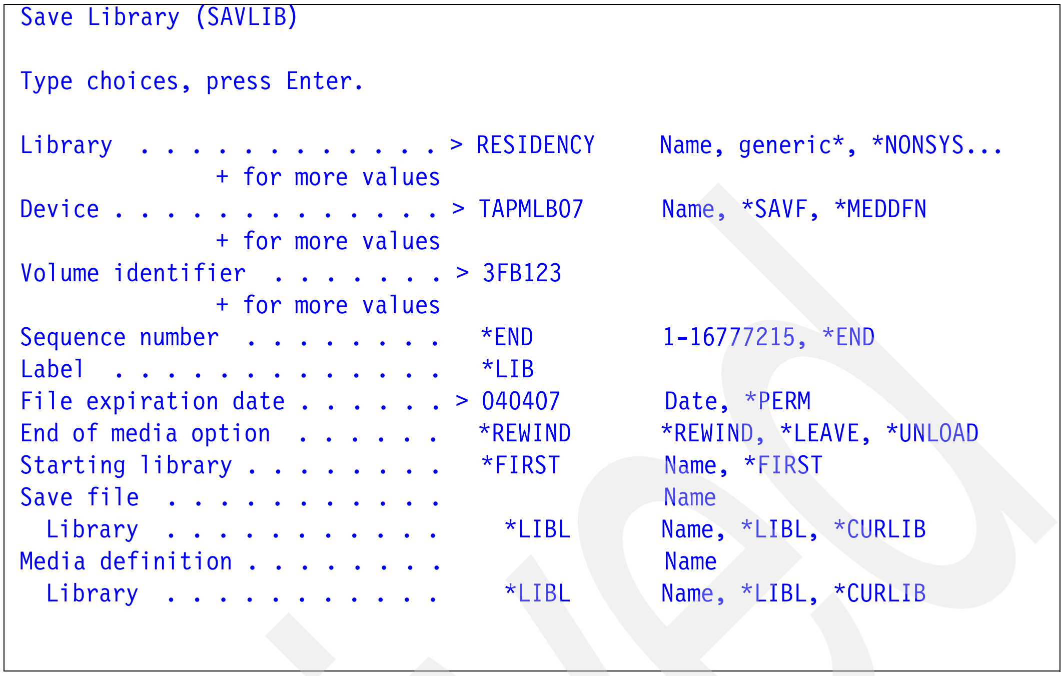
   In our example, we insert the current cartridge identifier also for the new identifier. We specify density as *DEVTYPE — The highest capacity density or format supported by the tape device is used. For faster initializing, we specify not to check for active files on the cartridge and not to delete previous files on the cartridge. This is shown in Figure 5-53.



```
 Initialize Tape (INZTAP)

 Type choices, press Enter.

 Device . . . . . . . . . . . . .   tapmlb07      Name
 New volume identifier  . . . . .   3fb123        Character value, *NONE...
 New owner identifier . . . . . .   *BLANK
 Volume identifier  . . . . . . .   3fb123        Character value, *MOUNTED
 Check for active files . . . . .   *no           *YES, *NO, *FIRST
 Tape density . . . . . . . . . .    *DEVTYPE      *DEVTYPE, *CTGTYPE,
*QIC120...
 Code . . . . . . . . . . . . . .   *EBCDIC       *EBCDIC, *ASCII
 End of tape option . . . . . . .   *REWIND       *REWIND, *UNLOAD
 Clear  . . . . . . . . . . . . .   *NO           *NO, *YES
```

Figure 5-53 Initializing a data cartridge

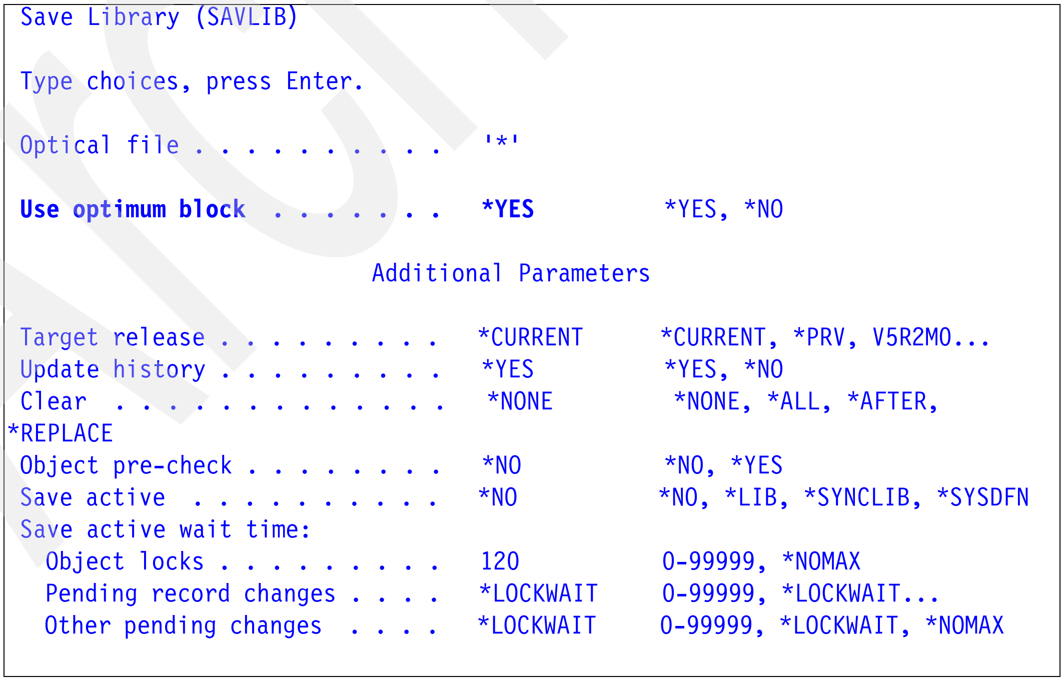
8. To save a database library to the data cartridge in the tape library, use the i5/OS command **SAVLIB**; press F4 for a command prompt. This displays the screen *Save Library (SAVLIB)* where you specify parameters. In our example, we save library **Residency** to the cartridge **3Fb123** in tape library **TAPMLB07**, as shown in Figure 5-54. Press Enter.



```
Save Library (SAVLIB)

Type choices, press Enter.

Library  . . . . . . . . . . . > RESIDENCY     Name, generic*, *NONSYS...
               + for more values
Device . . . . . . . . . . . . > TAPMLB07      Name, *SAVF, *MEDDFN
               + for more values
Volume identifier  . . . . . . > 3FB123
               + for more values
Sequence number  . . . . . . .   *END          1-16777215, *END
Label  . . . . . . . . . . . .   *LIB
File expiration date . . . . . > 040407        Date, *PERM
End of media option  . . . . .   *REWIND       *REWIND, *LEAVE, *UNLOAD
Starting library . . . . . . .   *FIRST        Name, *FIRST
Save file  . . . . . . . . . .                 Name
  Library  . . . . . . . . . .     *LIBL       Name, *LIBL, *CURLIB
Media definition . . . . . . .                 Name
  Library  . . . . . . . . . .     *LIBL       Name, *LIBL, *CURLIB
```

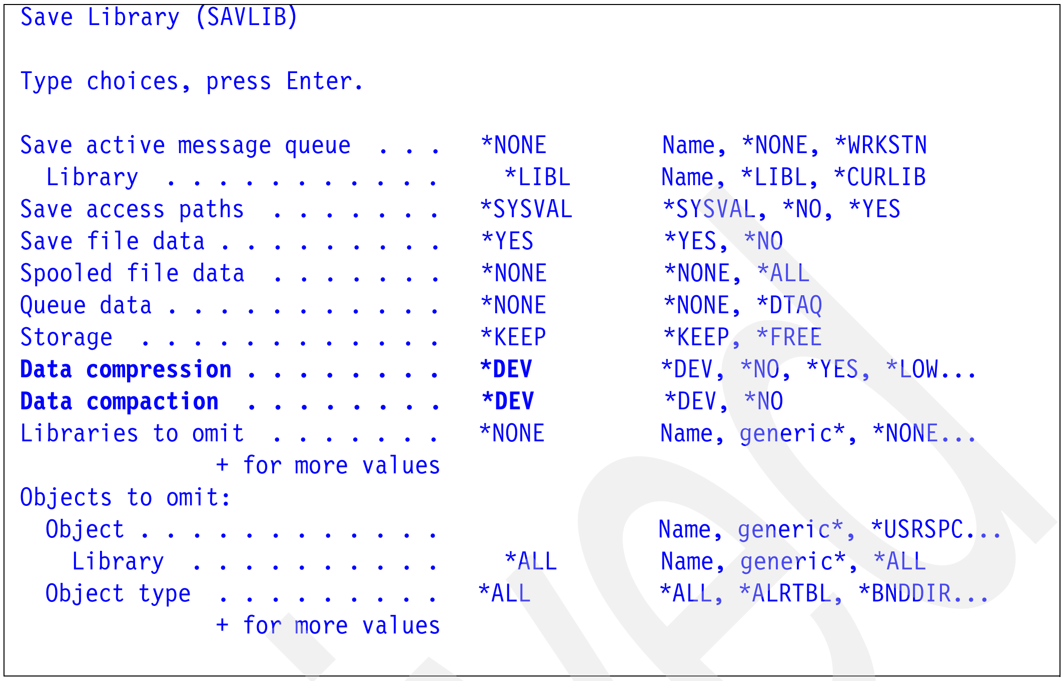
Figure 5-54   SAVLIB

9. On the screen *Save Library (SAVLIB)*, page down one page, and observe the parameter *Use optimum block *yes,* which is specified as default. List one more page down and observe the parameters *Data compression *DEV* and *Data compaction *DEV*, specified by default, as shown in Figure 5-55 and Figure 5-56. For more information about optimal block and data compression, refer to 4.5, "Optimum block size and compression" on page 105.



```
Save Library (SAVLIB)

Type choices, press Enter.

Optical file . . . . . . . . .   '*'

Use optimum block  . . . . . .   *YES          *YES, *NO

                           Additional Parameters

Target release . . . . . . . .   *CURRENT      *CURRENT, *PRV, V5R2M0...
Update history . . . . . . . .   *YES          *YES, *NO
Clear  . . . . . . . . . . . .    *NONE         *NONE, *ALL, *AFTER,
*REPLACE
Object pre-check . . . . . . .   *NO           *NO, *YES
Save active  . . . . . . . . .   *NO           *NO, *LIB, *SYNCLIB, *SYSDFN
Save active wait time:
  Object locks . . . . . . . .   120           0-99999, *NOMAX
  Pending record changes . . .   *LOCKWAIT     0-99999, *LOCKWAIT...
  Other pending changes  . . .   *LOCKWAIT     0-99999, *LOCKWAIT, *NOMAX
```

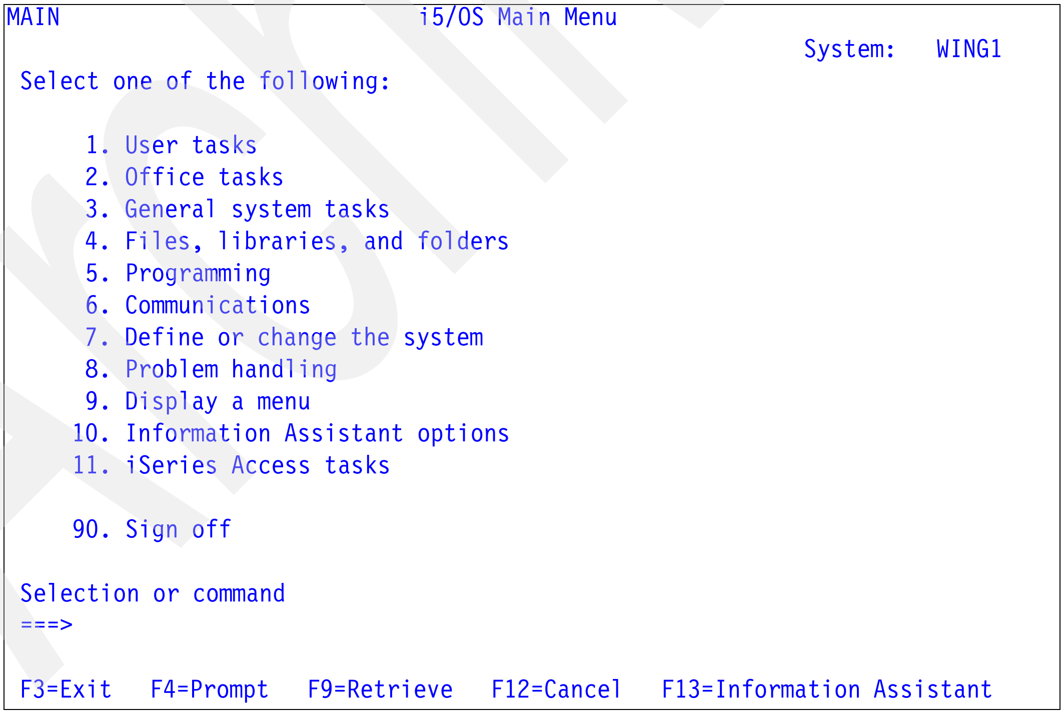
Figure 5-55   SAVLIB - use optimum block



```
Save Library (SAVLIB)

Type choices, press Enter.

Save active message queue  . . .   *NONE         Name, *NONE, *WRKSTN
  Library  . . . . . . . . . . .     *LIBL       Name, *LIBL, *CURLIB
Save access paths  . . . . . . .   *SYSVAL       *SYSVAL, *NO, *YES
Save file data . . . . . . . . .   *YES          *YES, *NO
Spooled file data  . . . . . . .   *NONE         *NONE, *ALL
Queue data . . . . . . . . . . .   *NONE         *NONE, *DTAQ
Storage  . . . . . . . . . . . .   *KEEP         *KEEP, *FREE
Data compression . . . . . . . .   *DEV          *DEV, *NO, *YES, *LOW...
Data compaction  . . . . . . . .   *DEV          *DEV, *NO
Libraries to omit  . . . . . . .   *NONE         Name, generic*, *NONE...
               + for more values
Objects to omit:
  Object . . . . . . . . . . . .                 Name, generic*, *USRSPC...
    Library  . . . . . . . . . .     *ALL        Name, generic*, *ALL
  Object type  . . . . . . . . .   *ALL          *ALL, *ALRTBL, *BNDDIR...
               + for more values
```

Figure 5-56 SAVLIB - data compression

10.After the database library is successfully saved, i5/OS message indicates the number of saved objects, as can be seen in Figure 5-57.



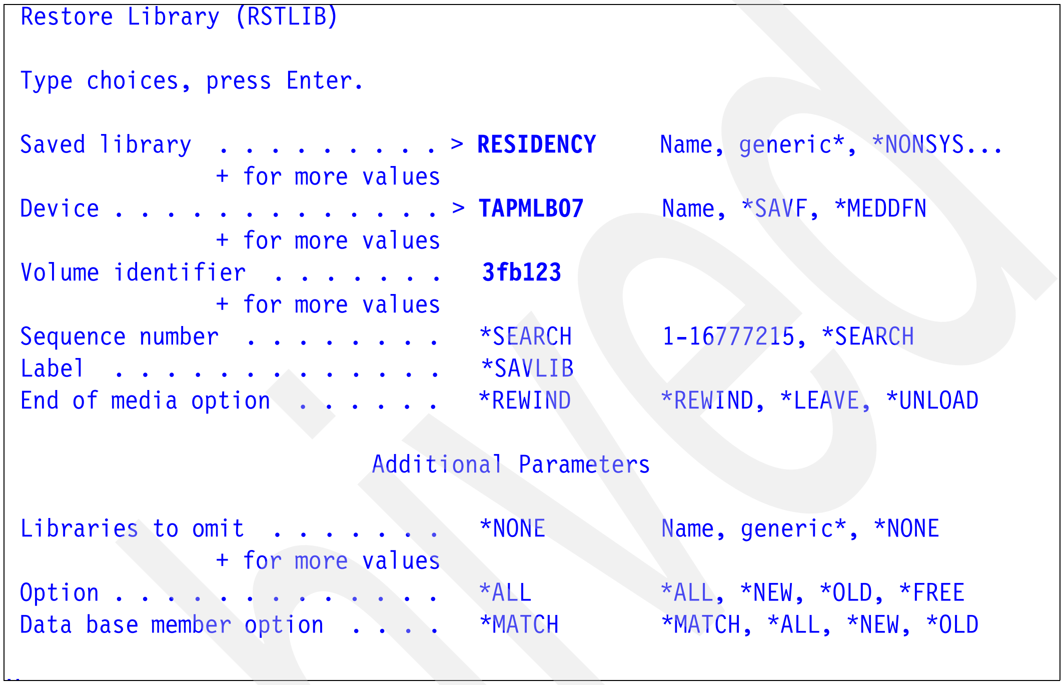
```
MAIN                           i5/OS Main Menu
                                                           System:   WING1
 Select one of the following:

      1. User tasks
      2. Office tasks
      3. General system tasks
      4. Files, libraries, and folders
      5. Programming
      6. Communications
      7. Define or change the system
      8. Problem handling
      9. Display a menu
     10. Information Assistant options
     11. iSeries Access tasks

     90. Sign off

 Selection or command
 ===>

 F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel   F13=Information Assistant
```

Figure 5-57 Successful save

5.3.2 Restoring a database library from a tape library

To restore a database library, perform the following steps:

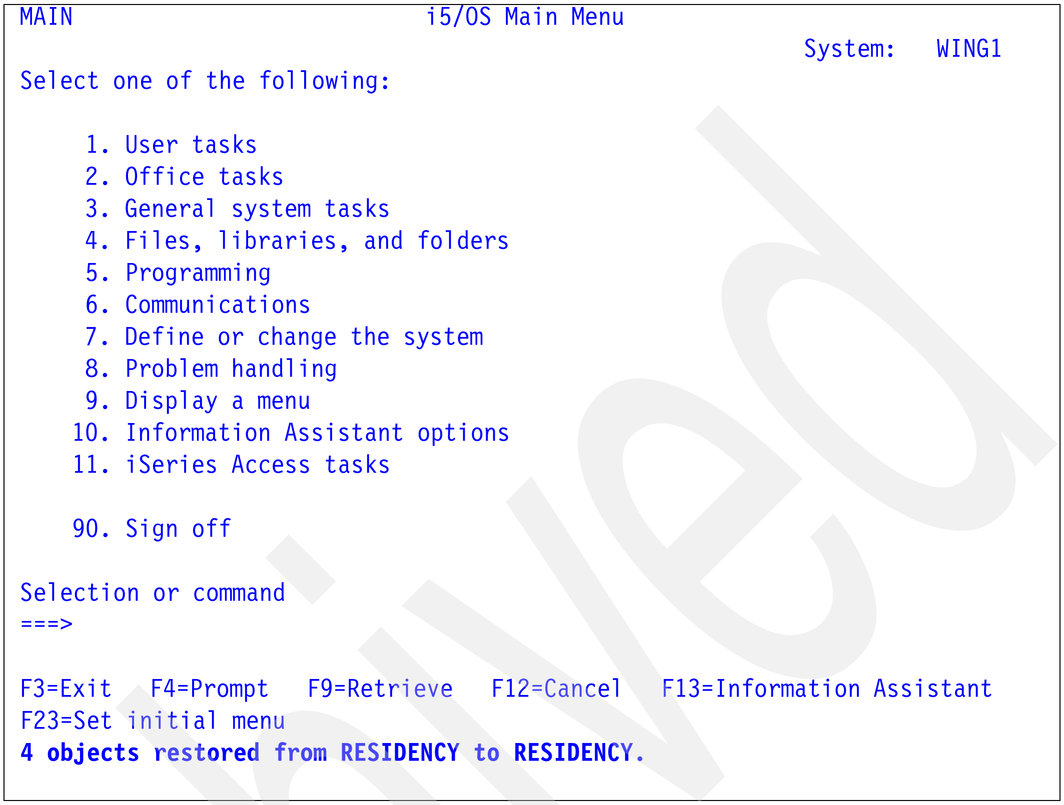
1. To restore a database library, issue the command **RSTLIB** and press F4 for a prompt. This displays the screen *Restore Library (RSTLIB)* where you specify the required parameters: database library being restored, tape library used for restore, and volume id of the data cartridge. This is shown in Figure 5-58. After specifying the parameters, press Enter.



```
Restore Library (RSTLIB)

Type choices, press Enter.

Saved library  . . . . . . . . . > RESIDENCY     Name, generic*, *NONSYS...
               + for more values
Device . . . . . . . . . . . . . > TAPMLB07      Name, *SAVF, *MEDDFN
               + for more values
Volume identifier  . . . . . . .   3fb123
               + for more values
Sequence number  . . . . . . . .   *SEARCH       1-16777215, *SEARCH
Label  . . . . . . . . . . . . .   *SAVLIB
End of media option  . . . . . .   *REWIND       *REWIND, *LEAVE, *UNLOAD

                          Additional Parameters

Libraries to omit  . . . . . . .   *NONE         Name, generic*, *NONE
               + for more values
Option . . . . . . . . . . . . .   *ALL          *ALL, *NEW, *OLD, *FREE
Data base member option  . . . .   *MATCH        *MATCH, *ALL, *NEW, *OLD
```

Figure 5-58 RSTLIB

2. After the database library is successfully restored, i5/OS issues a confirmation message with the number of restored objects, as shown in Figure 5-59.



```
MAIN                           i5/OS Main Menu
                                                             System:   WING1
Select one of the following:

     1. User tasks
     2. Office tasks
     3. General system tasks
     4. Files, libraries, and folders
     5. Programming
     6. Communications
     7. Define or change the system
     8. Problem handling
     9. Display a menu
    10. Information Assistant options
    11. iSeries Access tasks

    90. Sign off

Selection or command
===>

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel   F13=Information Assistant
F23=Set initial menu
4 objects restored from RESIDENCY to RESIDENCY.
```

Figure 5-59 Successful RSTLIB

Part 2

Tape libraries and backup software

In Part 2 we focus on System i tape implementation.

We cover the following topics:

- Implementation considerations with Backup Recovery and Media Services
- Tape encryption considerations and setup
- Implementation considerations for the IBM Virtualization Engine TS7520

6

Implementing tape with Backup Recovery and Media Services

This chapter describes the Backup Recovery and Media Services (BRMS) software for management and automation of backups and restores in i5/OS (formerly named OS/400).

We provide two examples of save and restore by using the BRMS Graphical User Interface. For more detailed information and examples, refer to *Backup Recovery and Media Services for OS/400 A Practical Approach,* SG24-4840.

6.1 Introduction to BRMS

With growing capacity and increasing requirements for managing information, System i customers require a tool to manage their saves and restores. Although some years ago, many System i shops could cover their backup requirements by simple i5/OS commands, nowadays they require software to manage their complex backups and take care of a growing amount of data cartridges.

Backup Recovery and Media Services (BRMS), a licensed product in i5/OS, meets these customers' requirements. It provides capability for fully automated backup, as well as comprehensive and efficient management of data cartridges. By using BRMS, the customers can recover their entire system, or single objects. With BRMS, it is also possible to share tape devices, use virtual tape drives, and use Tivoli Storage Manager for System i backups.

Advanced features of BRMS enable customers to archive data to various media, and dynamically retrieve data. The Network feature of BRMS provides management of multiple BRMS systems that share the inventory of media and backup policies.

The BRMS functions fall into six key areas, as follows:

- Managing your media:
  - Tracks the contents of your tapes as they are written
  - Prevents overwriting active tapes
  - Provides move reports showing which tapes should move to different locations each day
  - Provides lists of tapes that should be in each location at any given time, and so on.
- Automating your backups:
  - Sets up your backups in a standardized format that others can understand easily
  - Supports save-while-active, object-level saves, spooled file saves that maintain print attributes, saves to Tivoli Storage Manager, and so on

    For more information about the save-while-active function, refer to the System i Information center at the following Web site:

    `http://publib.boulder.ibm.com/iseries/`
  - Provides detailed reporting on activity and errors, and so on
- Simplifying your recoveries:
  - Shows you all the saves of a certain set of objects so you can choose which generation you want to restore
  - Provides interactive restores of those objects, complete with operator mount messages as appropriate
  - Simplifies full-system recoveries by providing reports showing ASP configuration, tapes required for recovery, and detailed steps for recovery; automates those steps once the BRMS product is back on the system
  - Provides an on-line progress report during a recovery.
- Hierarchical Storage Management (HSM):
  - Migrates objects among disk pool based on age, size, and usage criteria
  - Archives objects to tape based on age and usage criteria
  - Dynamically recalls *file objects, folders, and stream files when accessed by a user or application, and performs interactive recalls of other object types

- Tape library support:
  - Interfaces with automated tape libraries to select and mount/demount/eject volumes
- Networking feature:
  - Share Media Inventory
  - Share Policies
  - Media Managed across multiple systems
  - Allows recovery of objects from one BRMS network system to another system (the backup policies are described later in this chapter).

6.1.1 Functional components of BRMS

The architecture of BRMS is carefully and efficiently designed: it consists of different functional components or building blocks, of the following types:

Locations Define places where media and devices reside through their lifecycle

Policies Define how and when to perform actions

Control groups Define on which objects and how are actions done

These components refer to each other in a way that enables a user to design simple or complex backup strategies. A user can customize the components, and define multiple instances of some of them. By using a small group of these components, the user can quickly make a simple and straightforward save, and with a bigger group of related components, can design complex automated backups and restores.

For example:

- A user creates a policy defining when media expire, as well as a control group defining a database library to save. The control group refers to a created policy and leaves all the other referred components as default. So the user achieves a simple backup of a database library to media that can be retained as long as he defines.
- A user creates a few policies for different types of data cartridges, each of them having different expiration period, and defines policies for moving media to save locations. The user creates multiple control groups for saving different parts of the software, some control groups associated with one policy for media, and others associated with another policy for media. With careful combining of these components, the user can achieve clear and efficient complex backups.

Policies, location, control groups, and tasks are described in more detail next in this section.

> **Note:** In this chapter we use the term *media* to denote any removable storage medium available on the system; this includes data cartridges.

In this section, the components of which only one exists in BRMS are referred to in singular, such as backup policy and system policy. The components that can have multiple instances in BRMS are referred to in plural, such as media policies, locations, and control groups.

BRMS architecture consists of the following functional components:

- Storage locations
- Media devices
- Media library devices
- Media classes
- Move policies
- Media policies

- System policy
- Backup policy
- Recovery policy
- Archive policy
- Retrieve policy
- Backup control groups
- Archive control groups

Next we briefly describe these components.

Storage location

Storage location denotes a place where media are stored. The following two storage locations are provided as defaults with BRMS:

- **HOME*: The default on-site storage location
- *VAULT*: The default off-site storage location

These two locations might be enough for a smaller tape configuration, but in more complex environments, we recommend that you define additional storage locations. You could create a storage location for each tape library or stand-alone tape drive, and a storage location for scratch media. For example:

```
Define location L_TS2300 for tape devices and media in TS3200 tape library Define
location L_TS1120 for TS1120 tape drive and TS1120 media in TS3500 tape library.
```

When performing backup, BRMS looks for data cartridges in a storage location to which a particular backup policy refers through the media policy.

Media devices

Media devices denote a tape drive used by BRMS. At the time of installation, BRMS determines the tape drives and tape libraries in the system and creates media devices and media library devices with corresponding device information entries, such as device type, density, storage location for this device, allow sharing of the device, and so on. You can change these entries if you want.

Media library devices

Media library devices determine a tape library used by BRMS. At the time of installation or initializing, BRMS determines the tape drives and tape libraries in the system and creates media devices and media library devices with corresponding device information entries. You can change these entries, if you want.

Media classes

Media classes denote the type of media that are used for backup, archive, and recovery. Within each type of media there can be further distinction by format and capacity. At the time of installation or initializing, BRMS creates media classes to match the tape devices installed in the system. You can create additional media classes. For example, you might want to add a media class defining a different data cartridge that can be read by the same tape as media class created by BRMS. You can also add a media class for encrypted data cartridges.

Move policies

Move policies track the movement of a media from one storage location to another.

An example of a simple move policy is as follows: Media moves from its home location to the location where BRMS performs save, then to a safe location where it stays some days, and then to vault where is remains until expired.

After media expires, BRMS tracks its return to home location for future use. A default move policy *OFFSITE* is created when BRMS is installed. It tracks the media to the location *VAULT* where it remains until expired.

Media policies

Media policies are the key factor for implementing a backup strategy with BRMS. They define the type and length of media retention, and specify which media class and which move policy to use. The following media policies come as default with BRMS:

- The media policy *FULL* specifies a retention period of 35 days. This media policy can be used for full backups. Its move policy is **OFFSITE.*
- The media policy *INCR* specifies a retention period of 14 days. It can be used for incremental backups.
- The media policy *ARCHIVAL* is meant for saving an entire system. Its retention period is 1725 days (5 years).

You can create a media policy for every combination of retention, location, media class, or move policy that you plan to use.

Example of defining media policies

In this example, a TS3500 Tape Library containing LTO tape drives and TS1120 tape drives, and a TS3200 Tape Library with LTO tape drives, are connected to i5/OS with BRMS.

Every day, you incrementally save a database library to an LTO media in the TS3200 Tape Library. After one day, the media is moved to the save location, where it is kept for 3 days, then it expires. Once per week, you save the entire system to a TS1120 media, backup is full, it is kept for one week, then moved to the save location, where is stays for 3 weeks, and then it is moved to the offsite vault, where it is kept until expiration. The media expires after 5 weeks in the vault.

For this backup pattern, you can define the following two media policies:

- **Media policy A:** This specifies a media class of LTO media, a location of TS3200 Tape Library, type is incremental, expiration is 4 days, move policy from location of TS2300 Tape Library to save location after one day.
- **Media policy B:** This specifies a media class of TS1120 media, location of TS1120 tape drive and media, type is full, expiration is 9 weeks, move policy from TS1120 location to save location after 1 week, and from safe location to offsite vault after 3 weeks.

System policy

System policy determines which settings to use if a policy does not specify any particular setting. It provides default values for the following items: default media policy, tape device, and location of media.

For example: You create a media policy where you specify a media class as **SYSPCY*. In this case, the media class specified in the System policy is used for a newly created media policy.

Backup policy

Backup policy defines how to perform backups with BRMS. Here are some specifications provided by the backup policy:

- Type of backup (full or incremental)
- Days on which to perform backups
- Type of incremental backup (cumulative or non cumulative)

- Which media policy to use for the backup
- Whether to save specific System i objects (journals and access paths)
- Whether to append saved files to current media with active files, or to use a separate data cartage
- Usage of optimal blocksize for backup:

  For information about optimal blocksize with save and restore, refer to Chapter 4, “Planning for IBM tape in i5/OS” on page 95.

You can change default parameters in the backup policy to another value, as it suits you. The backup policy determines which parameters to use if the control group does not specify any particular parameter.

For example: You create a control group where you specify media policy for full backups as **BKUPCY*. In this case media classes are taken from the backup policy.

Recovery policy

Recovery policy defines how to implement recovery, for instance, which device to use for recovery, whether to perform parallel recovery, to restore contents to a library different than the saved library.

For more information about parallel save and restore, refer to Chapter 4, “Planning for IBM tape in i5/OS” on page 95.

Archive policy

Archive policy defines how to perform archives with BRMS. It specifies which devices to use for archiving, and criteria by which archiving is done: for instance, the threshold of System i disk pool, which triggers archiving of objects from this pool, minimal size of an object to become a candidate for archiving, and whether objects are included in an archive based on the object’s frequency of use.

Retrieve policy

Retrieve policy guides the retrieving of archived objects in BRMS. Retrieve policy specifies parameters for retrieving, such as the devices used for the retrieve operation, which level of i5/OS authorization is required for retrieve, and whether the confirmation is required to retrieve an object.

Backup control groups

Backup control groups define what is saved and when. Each control group can contain one or multiple i5/OS objects to be saved. It refers to a particular media policy and one or multiple backup devices. It also contains information about how to save parts of the System i database such as journals and access paths, whether to use optimal blocksize and compression, and so on. If you do not change the default attributes of the control group, they are taken from the backup policy.

For more information about journals and access paths, refer to Chapter 3, “Overview of the IBM System i platform” on page 83. For more information about optimal blocksize and compression, refer to Chapter 4, “Planning for IBM tape in i5/OS” on page 95.

Examples of backup control groups

Assuming the same environment and backup pattern as described in “Example of defining media policies” on page 157, you can define the following two backup policies:

- **Backup control group A:** This specifies to perform backup every day, backup type is incremental, use backup device that denotes TS2300 Tape Library, and use media policy A as defined in “Example of defining media policies” on page 157.
- **Backup control group B:** This specifies to perform backup once per week, backup type full, use tape backup device which denotes TS1120 Tape Drive, and use media policy B, as defined in “Example of defining media policies” on page 157.

6.1.2 Tasks performed in BRMS

Backup, restore, and archive operations in BRMS are accomplished by using BRMS tasks. Some of the most important of these tasks are:

- Enrolling and initializing media
- Backup by using BRMS control groups
- Using BRMS reports
- Restoring data by using BRMS

Next we briefly describe each of the listed task.

Enrolling and initializing media

Media must be known to BRMS before being used for backup operations. In order to make it known to BRMS, enroll the media by using the BRMS menu option or BRMS commands. For more information about commands used for enrolling media, refer to *Backup Recovery and Media Services for OS/400, A Practical Approach*, SG24-4840. We also discuss this in 6.2, “Saving and restoring a database library” on page 160.

If you are planning to append backup files to existing media, ensure that the necessary media is available on-site. When looking for media to append to, BRMS follows a set of rules by which it picks up a media that matches the best the requirements in the requesting media policy. For more information about how BRMS allies append rules for media, refer to *Backup Recovery and Media Services for OS/400, A Practical Approach*, SG24-4840.

Backup by using BRMS control groups

BRMS comes with three default control groups for backups:

- **Sysgrp*
- **Bkugrp*
- **System*

By using the control group **Sysgrp*, you save the system parts of i5/OS and licensed products. In order to save the system parts of i5/OS, the system must be in a restricted state — all jobs must be finished and subsystems must be ended. For more information about i5/OS subsystems, refer to the System i Information center on the following Web site:

http://publib.boulder.ibm.com/iseries/

Because it requires a restricted state backup with the control group, it must be done from the system console. Also, media used for such a save must be in the media class with the *Shared* parameter set to *No*, because the network media inventory cannot be updated when a system is in a restricted state.

The control group **Bkugrp* saves the non-system portion of the i5/OS system, such as database libraries, documents, and folders, as well as the Integrated File System (IFS). For more information about IFS, refer to Chapter 3, “Overview of the IBM System i platform” on page 83.

The control group **System* is meant for backup of the entire i5/OS system. For saving the entire system, i5/OS must be in a restricted state, and the backup must be done from the system console.

For saving database libraries, objects, and combinations of them, you have to define other control groups. In 6.2, “Saving and restoring a database library” on page 160, we describe how to define a Control Group (Backup policy in iSeries Navigator).

Using BRMS reports

Normally, you can display which objects are saved and where they are saved through the BRMS/400 displays. You can also use the BRMS/400 displays to assist in the restore.

However, in case of system failure, you have to restore data backed up by BRMS to another system or to a newly installed i5/OS in your system. For this, you use the *BRMS Recovery Analysis report*, which instructs you how to restore the entire system saved by BRMS to another System i partition, or newly installed i5/OS. Therefore you should maintain an up-to-date BRMS Recovery Analysis report and have it always available in printed format.

Restoring data by using BRMS

Part of the BRMS tasks includes restoring saved data and retrieving archived data. Restore of the entire system should be tested in advance to make sure that it works without problems in case the production System i fails.

6.2 Saving and restoring a database library

In this example, we back up an i5/OS database library to a data cartridge in a Tape library. For this, we use the BRMS Graphical User Interface (GUI) available in iSeries Navigator. Backup in our example consists of the following activities:

- Create a media pool and add a data cartridge to it
- Create a backup policy
- Run the backup policy — save the database library
- Restore the database library

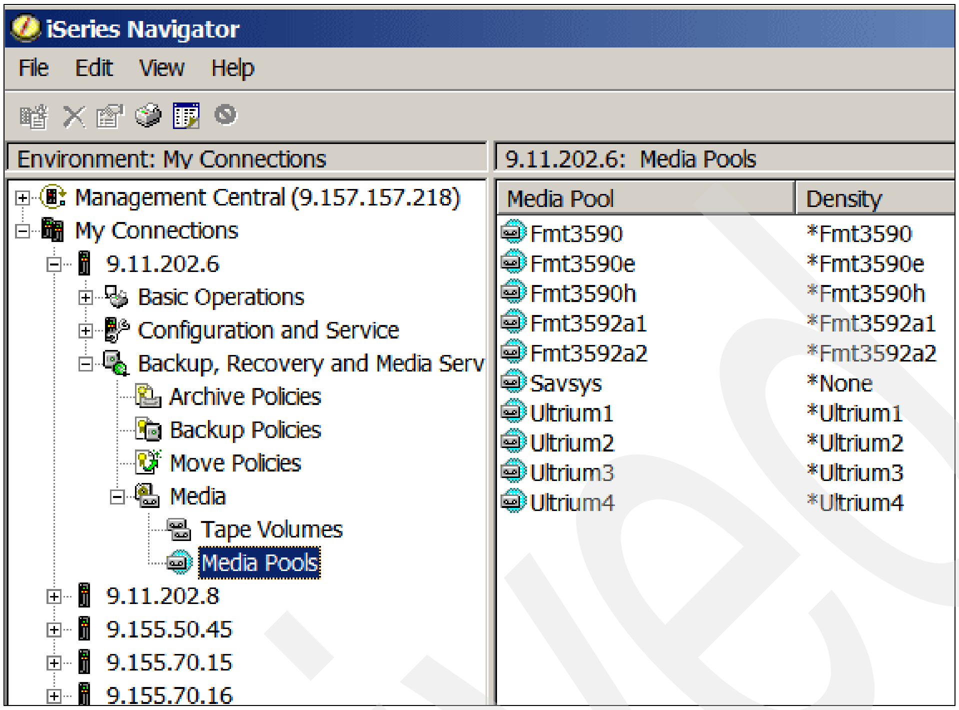
Next we describe the listed activities for backup and restore of the i5/OS library

Creating a media pool and adding a data cartridge to it

> **Note:** Media class is referred to as *media pool* in BRMS GUI.

Use the following steps to perform this activity:

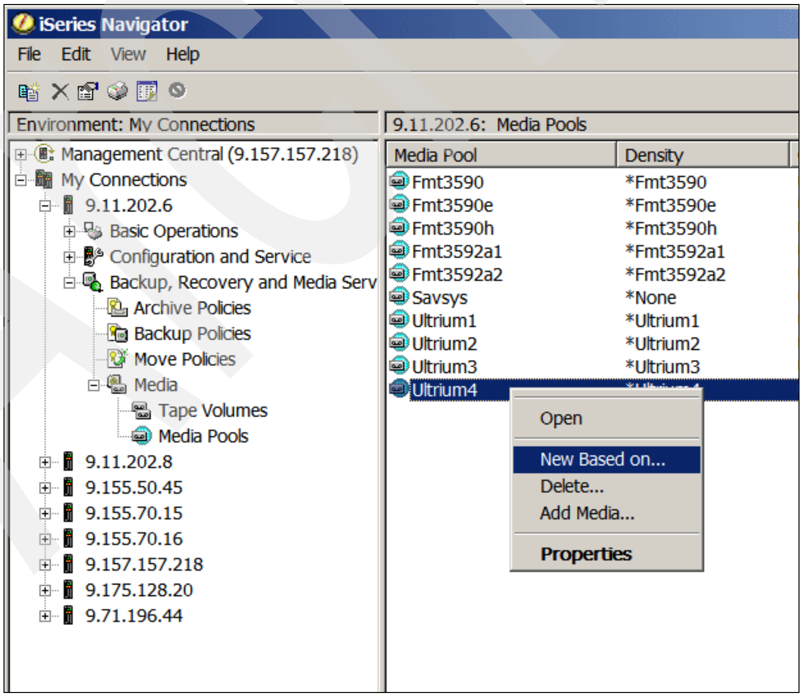
1. Install iSeries Navigator on your PC, launch it, and connect to the System i partition as described in 5.1, “Basic setup” on page 108.
2. In iSeries Navigator, expand the IP address or host name of the System i partition, expand *Backup Recovery and Media Services*, expand *Media*, and click **Media pools**. A list of media pools is displayed in the iSeries navigator right panel, as shown in Figure 6-1.



Media Pool	Density
Fmt3590	*Fmt3590
Fmt3590e	*Fmt3590e
Fmt3590h	*Fmt3590h
Fmt3592a1	*Fmt3592a1
Fmt3592a2	*Fmt3592a2
Savsys	*None
Ultrium1	*Ultrium1
Ultrium2	*Ultrium2
Ultrium3	*Ultrium3
Ultrium4	*Ultrium4

Figure 6-1 Media pools

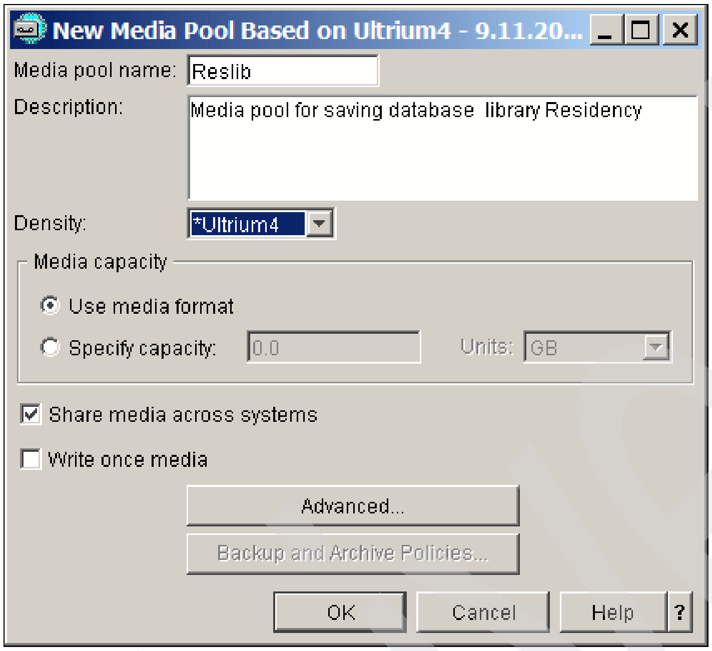
3. BRMS comes with default media pools such as Ultrium4, Ultrium3, and Fmt3582a1. To create a new media pool based on cartridge density and other properties of an existing media pool, right-click the media pool, and select **New Based on** from the pull-down menu, as shown in Figure 6-2.



Media Pool	Density
Fmt3590	*Fmt3590
Fmt3590e	*Fmt3590e
Fmt3590h	*Fmt3590h
Fmt3592a1	*Fmt3592a1
Fmt3592a2	*Fmt3592a2
Savsys	*None
Ultrium1	*Ultrium1
Ultrium2	*Ultrium2
Ultrium3	*Ultrium3
Ultrium4	*Ultrium4

Figure 6-2 Add new Media pool

4. This presents the wizard, *New Media Pool Based on...* In the wizard, specify the name, description, and cartridge density of the new media pool, as shown in Figure 6-3. Click **OK**.



New Media Pool Based on Ultrium4 - 9.11.20...

Media pool name: Reslib

Description: Media pool for saving database library Residency

Density: *Ultrium4

Media capacity

● Use media format

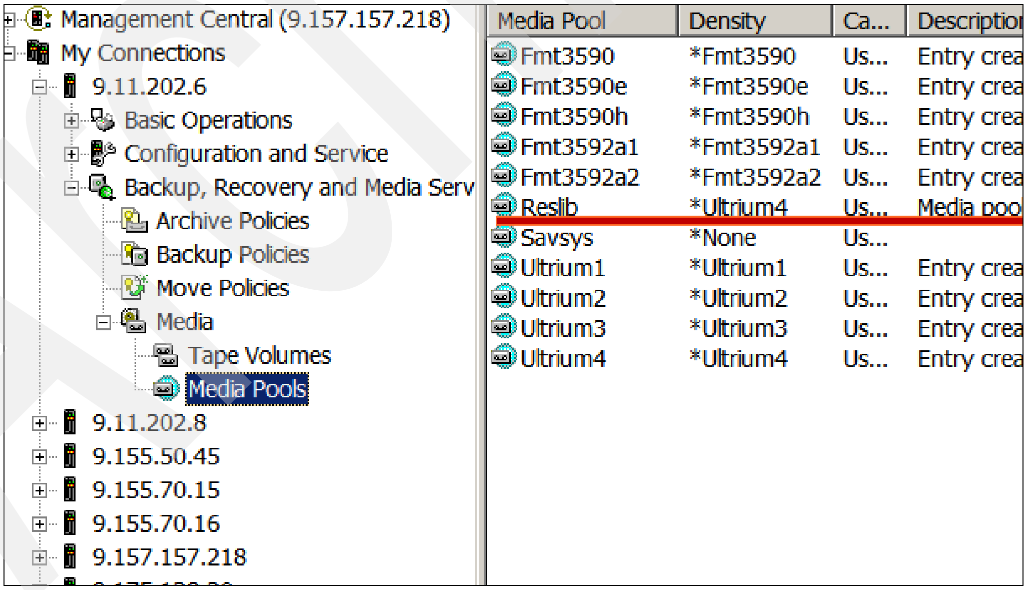
○ Specify capacity: 0.0 Units: GB

☑ Share media across systems

□ Write once media

Figure 6-3 New Media pool wizard

5. After refreshing the iSeries navigator view, a new media pool shows in the list, as can be seen in Figure 6-4.

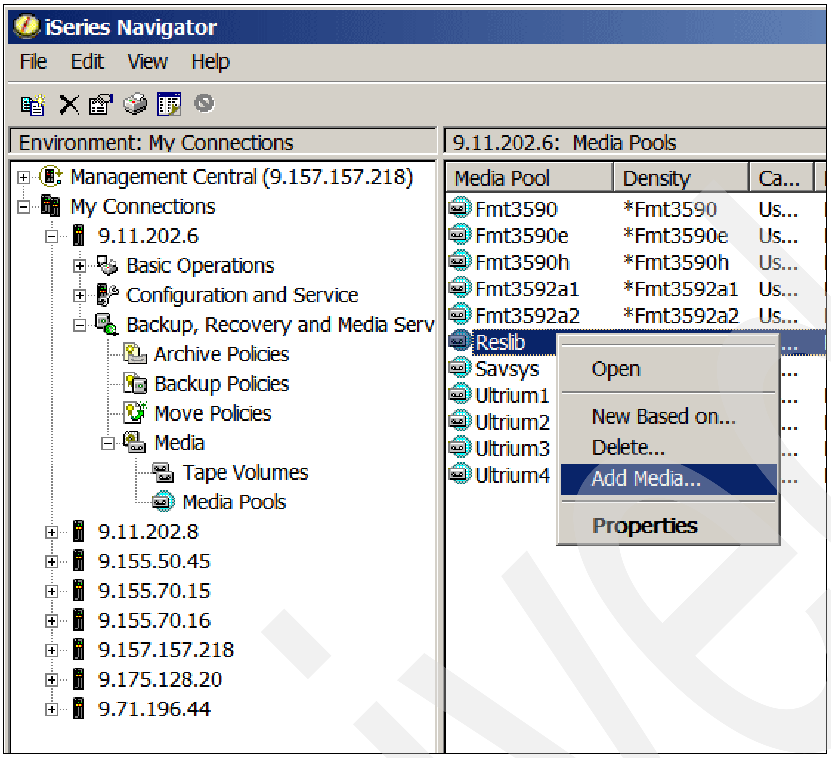


- Management Central (9.157.157.218)
- My Connections
  - 9.11.202.6
    - Basic Operations
    - Configuration and Service
    - Backup, Recovery and Media Serv
      - Archive Policies
      - Backup Policies
      - Move Policies
      - Media
        - Tape Volumes
        - Media Pools
  - 9.11.202.8
  - 9.155.50.45
  - 9.155.70.15
  - 9.155.70.16
  - 9.157.157.218

Media Pool	Density	Ca...	Descriptio
Fmt3590	*Fmt3590	Us...	Entry crea
Fmt3590e	*Fmt3590e	Us...	Entry crea
Fmt3590h	*Fmt3590h	Us...	Entry crea
Fmt3592a1	*Fmt3592a1	Us...	Entry crea
Fmt3592a2	*Fmt3592a2	Us...	Entry crea
Reslib	*Ultrium4	Us...	Media poo
Savsys	*None	Us...	
Ultrium1	*Ultrium1	Us...	Entry crea
Ultrium2	*Ultrium2	Us...	Entry crea
Ultrium3	*Ultrium3	Us...	Entry crea
Ultrium4	*Ultrium4	Us...	Entry crea

Figure 6-4 New media pool

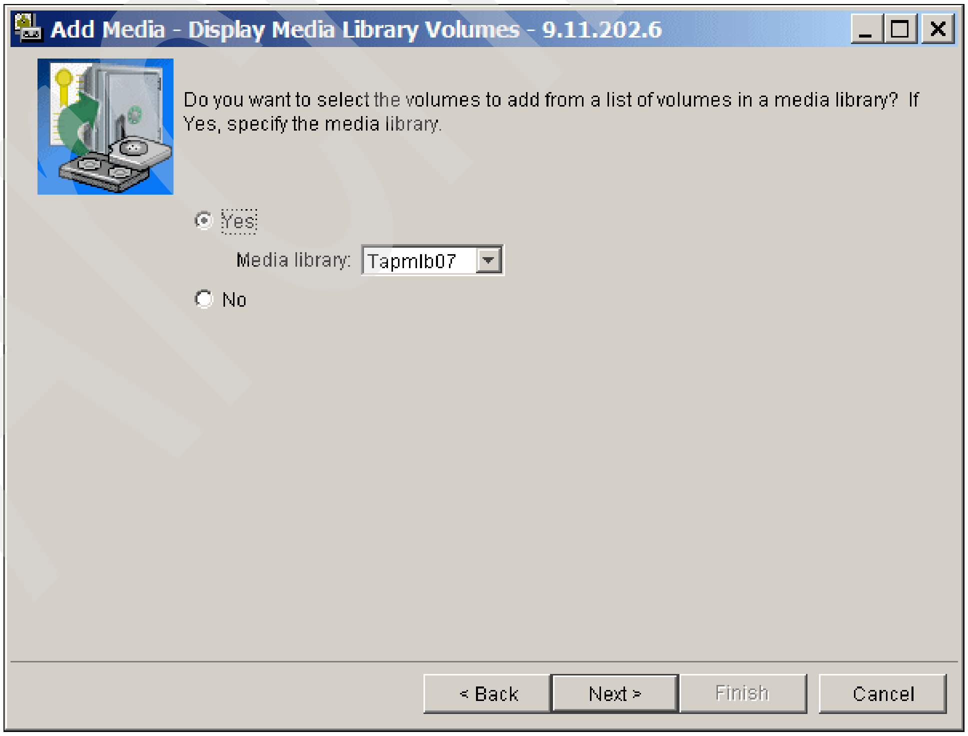
6. To add media to a created media pool, right-click it and select **Add Media** from the pull-down menu that pops up. This is shown in Figure 6-5.



Media Pool	Density	Ca...
Fmt3590	*Fmt3590	Us...
Fmt3590e	*Fmt3590e	Us...
Fmt3590h	*Fmt3590h	Us...
Fmt3592a1	*Fmt3592a1	Us...
Fmt3592a2	*Fmt3592a2	Us...
Reslib		...
Savsys		...
Ultrium1		...
Ultrium2		...
Ultrium3		...
Ultrium4		...

Figure 6-5 Add media

7. This presents the *Add Media* wizard. On the wizard click **Next**. On the next wizard window, select a tape library from which you want to add media, as in Figure 6-6. Click **Next**.



Do you want to select the volumes to add from a list of volumes in a media library? If Yes, specify the media library.

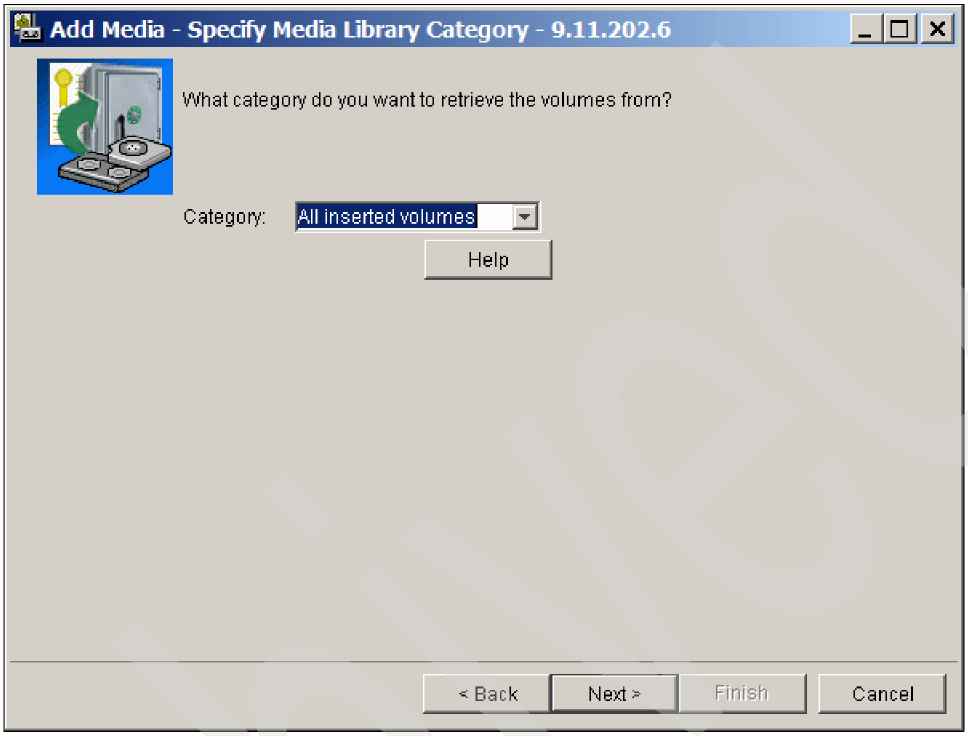
● Yes

Media library: Tapmlb07

○ No

Figure 6-6 Select Tape library to add media from

8. Next, you specify in the *Add Media* wizard from which category you want to add media. For information about categories, refer to 5.3, “Save and restore using basic i5/OS commands” on page 143. In our example we select all inserted cartridges, as shown in Figure 6-7. Click **Next**.

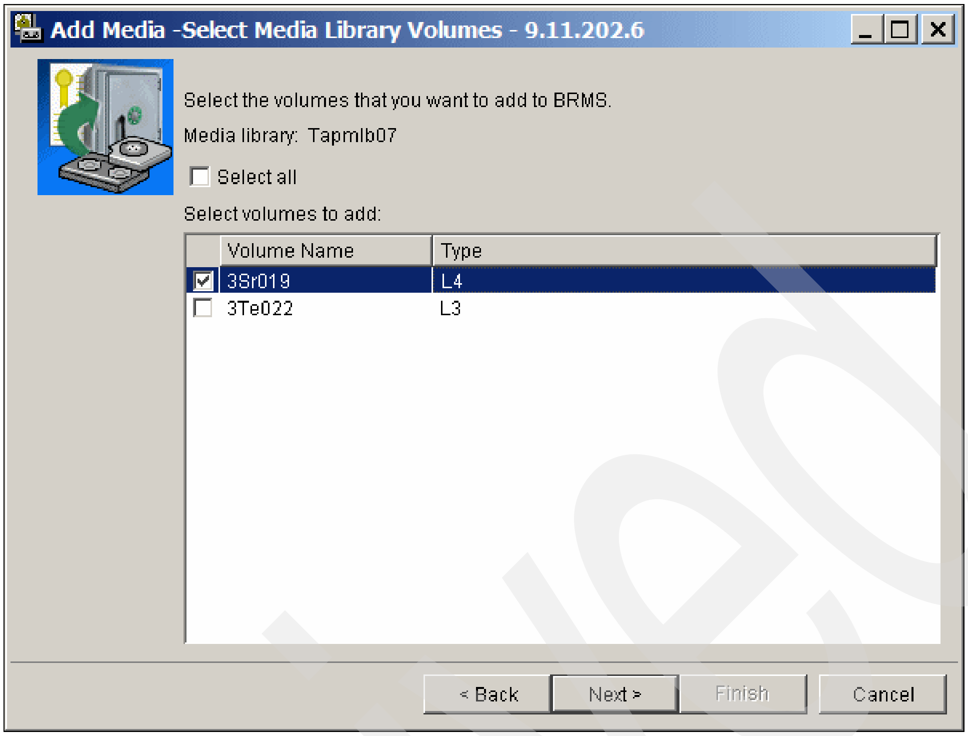


What category do you want to retrieve the volumes from?

Category: All inserted volumes

Figure 6-7 Add all inserted cartridges

9. Next you are prompted to select the cartridges to add to the media pool. In our example we select one cartridge, as shown in Figure 6-8. Click **Next**.



Select the volumes that you want to add to BRMS.

Media library: Tapmlb07

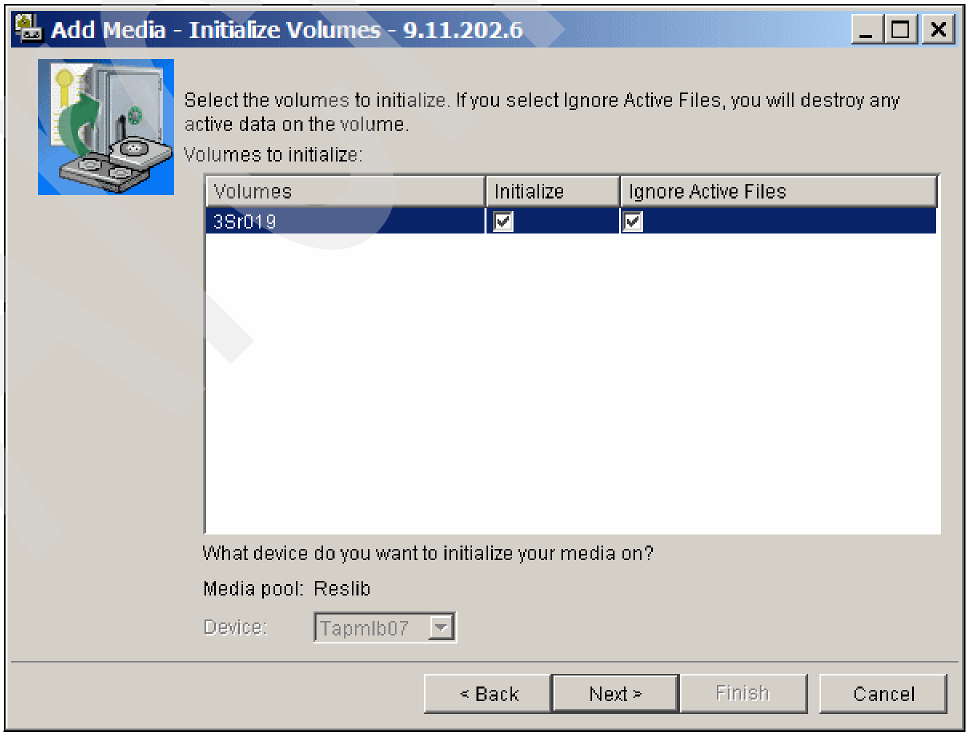
☐ Select all

Select volumes to add:

	Volume Name	Type
☑	3Sr019	L4
☐	3Te022	L3

Figure 6-8 Select media to add

10. Next, you have to specify if the added cartridge should be initialized. In our example we want it to be initialized, and active files on the cartridge should be ignored, as shown in Figure 6-9. Click **Next**. On next wizard window, click **Finish** to confirm anti-aliasing the data cartridge.



Select the volumes to initialize. If you select Ignore Active Files, you will destroy any active data on the volume.

Volumes to initialize:

Volumes	Initialize	Ignore Active Files
3Sr019	☑	☑

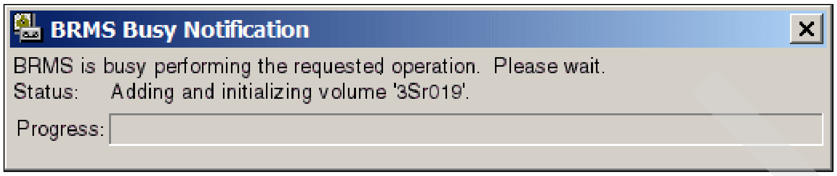
What device do you want to initialize your media on?

Media pool: Reslib

Device: Tapmlb07

Figure 6-9 Initialize media

A window with the progress of initializing is displayed while the cartridge is initialized, as shown in Figure 6-10. When the *BRMS Busy Notification* window finishes, the data cartridge is initialized and prepared in media pool Reslib.



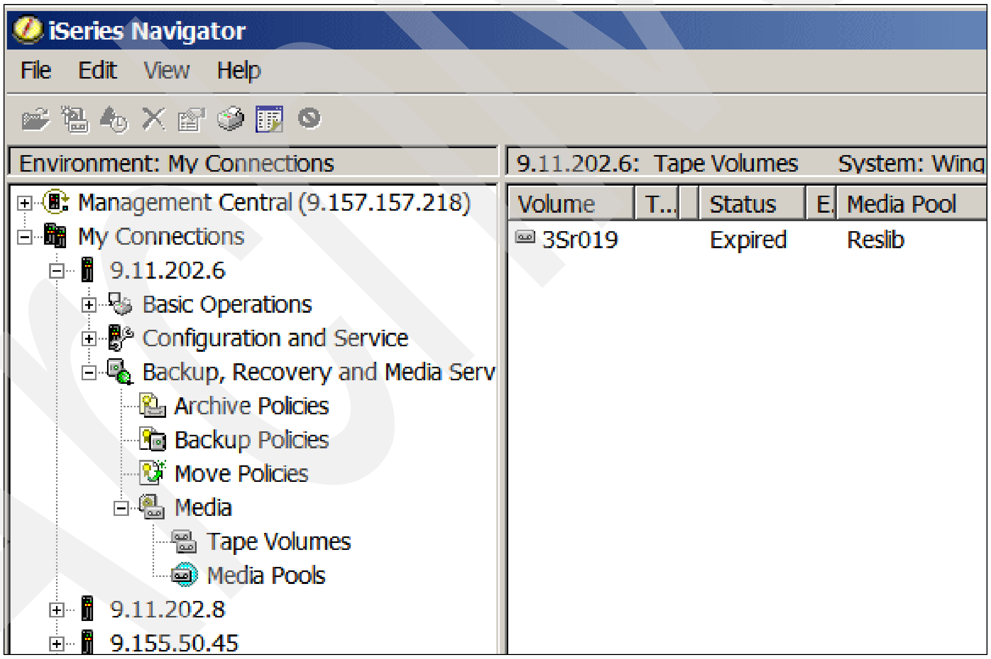
BRMS is busy performing the requested operation. Please wait.
Status: Adding and initializing volume '3Sr019'.
Progress:

Figure 6-10 Initializing Media

11. Still in expanded *Backup Recovery and Media Services*, and expanded *Media*, click **Tape Volumes**. This displays a list of data cartridges enrolled to BRMS, on the right iSeries Navigator panel.

> **Note:** Media can be enrolled to BRMS by using GUI or by BRMS menus in the i5/OS command interface. In the GUI, you enroll media to BRMS by adding them to a media pool.

In our example, only the cartridge 3Sr019, which we added to media pool Reslib, is enrolled to BRMS, as shown Figure 6-11.



9.11.202.6: Tape Volumes System: Winq

Volume	T...	Status	E.	Media Pool
3Sr019		Expired		Reslib

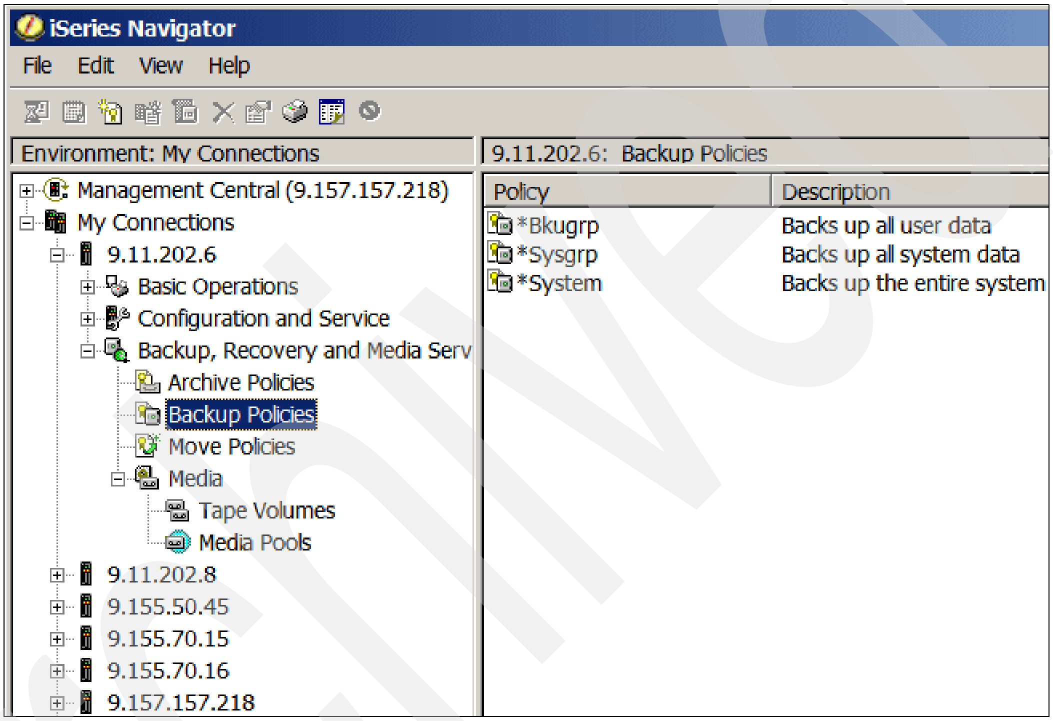
Figure 6-11 Enrolled media

Creating a backup policy

> **Note:** The BRMS control group is referred to as a backup policy in the BRMS GUI.

To create a backup policy and run save, perform the following steps:

1. Still in the iSeries Navigator, connect to System i partition if not yet connected, expand *Backup Recovery and Media Services*, and expand *Backup Policies*. In the right panel you see the list of default backup policies, as shown in Figure 6-12. For more information about default control groups (backup policies in GUI), refer to “Backup control groups” on page 158.



Policy	Description
*Bkugrp	Backs up all user data
*Sysgrp	Backs up all system data
*System	Backs up the entire system

Figure 6-12 Backup policies

2. To create a new backup policy, right-click **Backup Policies** in the left iSeries Navigator panel. Select **New Policy** from the pull-down menu that pops up, as shown in Figure 6-13.

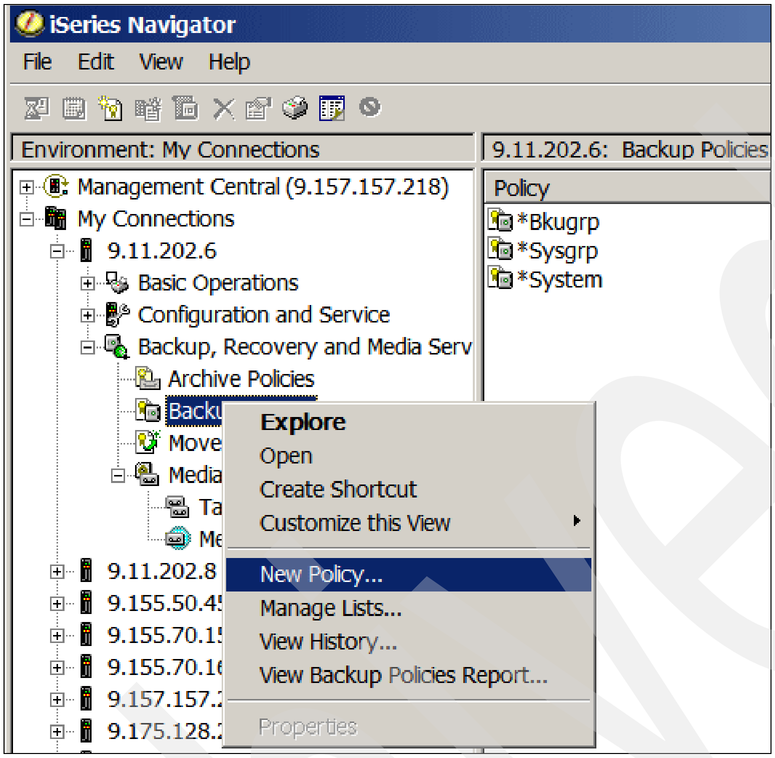
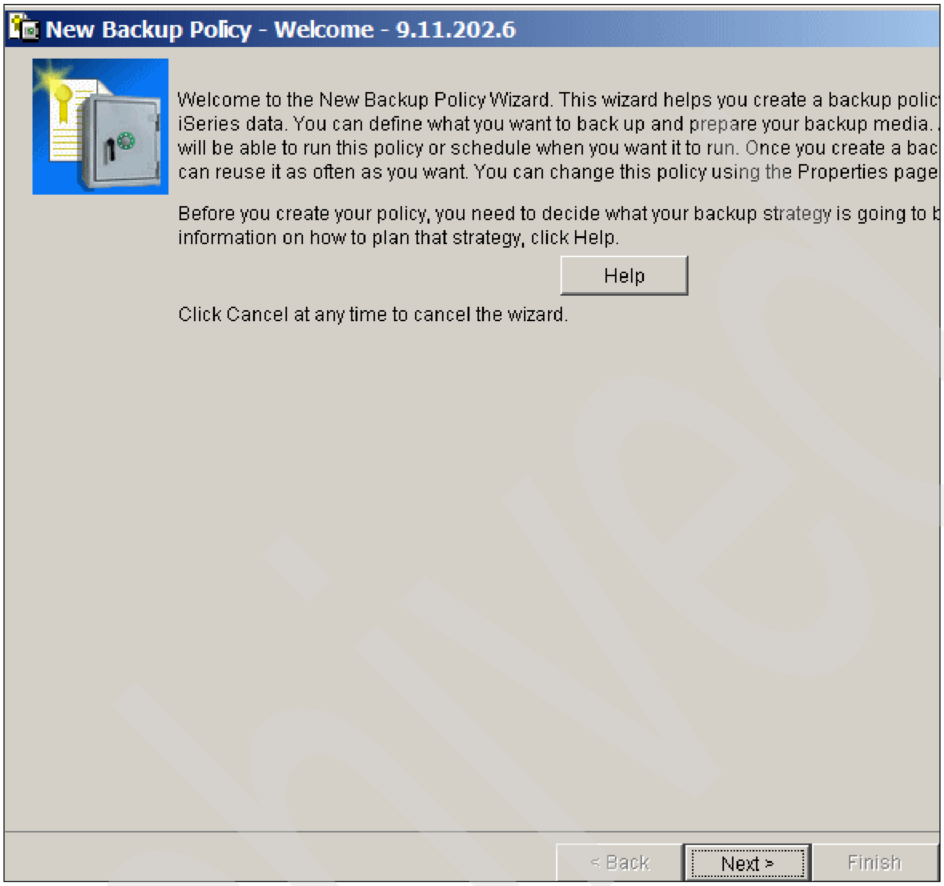


Figure 6-13 Create new backup policy

3. This presents a *New Backup Policy* wizard, as can be seen in Figure 6-14. On the first wizard welcome window, click **Next**.



New Backup Policy - Welcome - 9.11.202.6

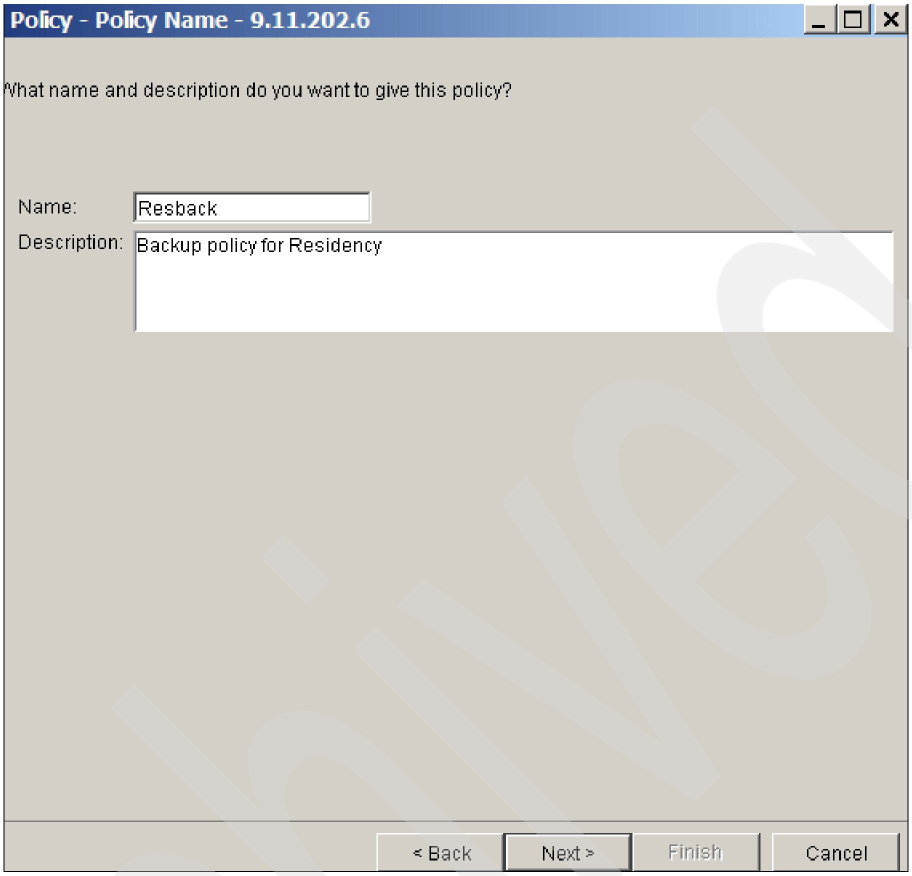
Welcome to the New Backup Policy Wizard. This wizard helps you create a backup polic iSeries data. You can define what you want to back up and prepare your backup media. will be able to run this policy or schedule when you want it to run. Once you create a bac can reuse it as often as you want. You can change this policy using the Properties page

Before you create your policy, you need to decide what your backup strategy is going to b information on how to plan that strategy, click Help.

Click Cancel at any time to cancel the wizard.

Figure 6-14 New Backup Policy wizard - welcome window

4. In the next wizard window, specify the name and description of the new backup policy. In our example, we name it Resback, as can be seen in Figure 6-15. Click **Next**.



Policy - Policy Name - 9.11.202.6

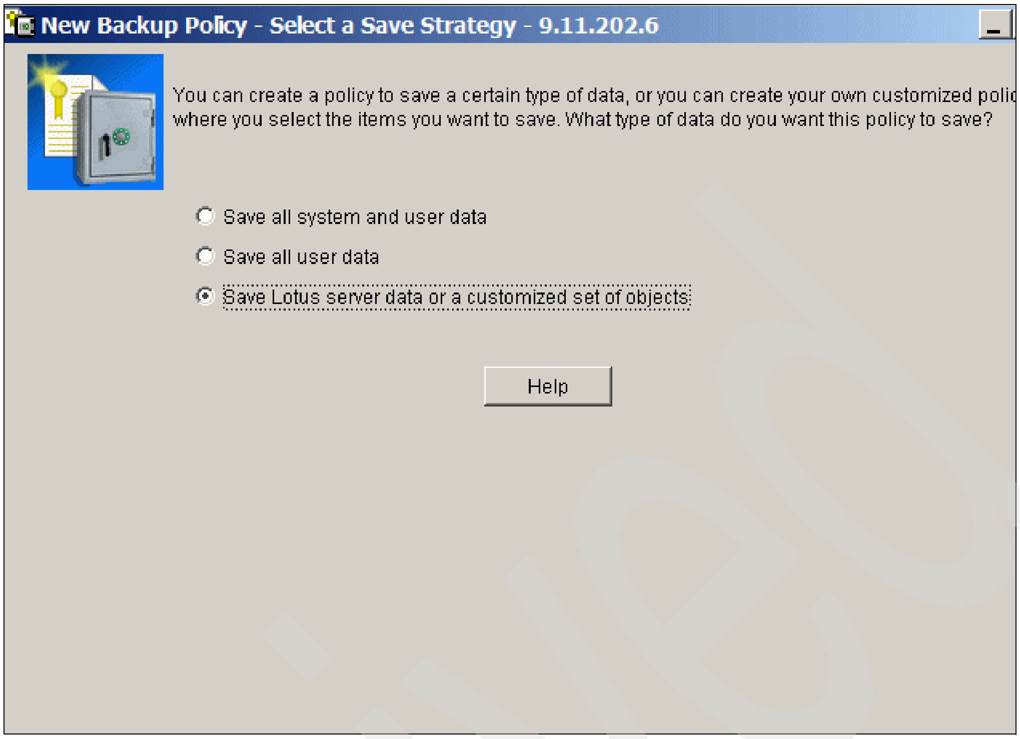
What name and description do you want to give this policy?

Name: Resback

Description: Backup policy for Residency

Figure 6-15 New Backup Policy wizard - Policy Name

5. In the next wizard window, specify which data you want to save by using this backup policy. In our example we plan to save one database library. For this, we have to use the option *customized set of objects*, so we select **Save Lotus server data or a customized set of objects**, as shown in Figure 6-16. Click **Next**.



New Backup Policy - Select a Save Strategy - 9.11.202.6

You can create a policy to save a certain type of data, or you can create your own customized polic
where you select the items you want to save. What type of data do you want this policy to save?

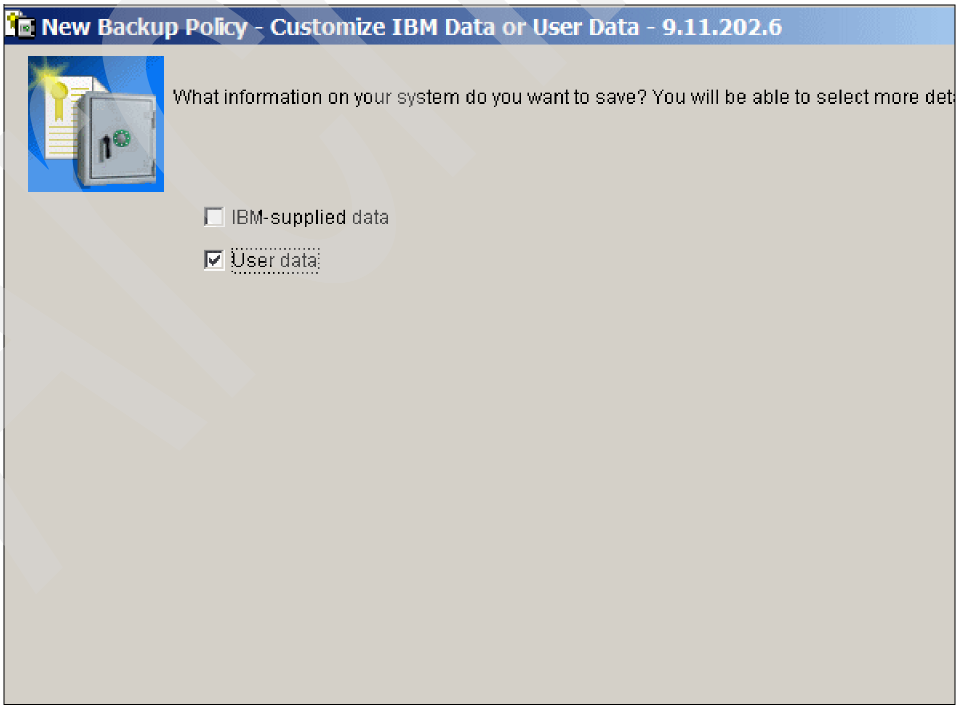
○ Save all system and user data

○ Save all user data

● Save Lotus server data or a customized set of objects

Figure 6-16 New Backup Policy wizard - Select a Save Strategy

6. In the next wizard window, specify which type of data is to be backed up by this backup policy. In our example we specify **User data** because we plan to back up the database library. This can be seen in Figure 6-17. After specifying the type of data, click **Next**.



New Backup Policy - Customize IBM Data or User Data - 9.11.202.6

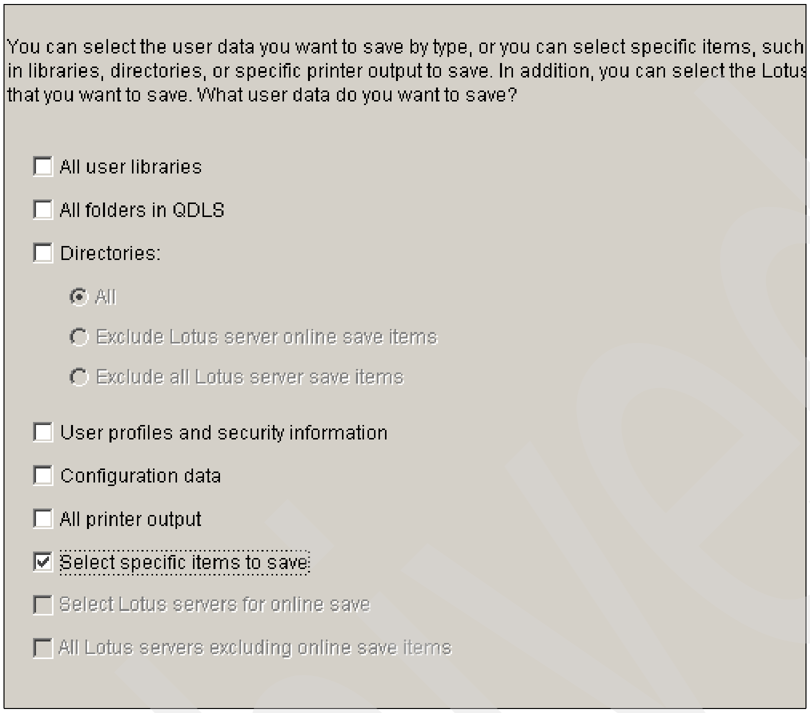
What information on your system do you want to save? You will be able to select more det

□ IBM-supplied data

☑ User data

Figure 6-17 New Backup policy wizard - select type of data

7. In the next wizard window, specify which kind of i5/OS objects this backup policy can save. In our example, we specify **Select specific items to save** because we want to save one i5/OS library. This is shown in Figure 6-18. After specifying objects to save, click **Next**.



You can select the user data you want to save by type, or you can select specific items, such in libraries, directories, or specific printer output to save. In addition, you can select the Lotus that you want to save. What user data do you want to save?

☐ All user libraries

☐ All folders in QDLS

☐ Directories:

● All

○ Exclude Lotus server online save items

○ Exclude all Lotus server save items

☐ User profiles and security information

☐ Configuration data

☐ All printer output

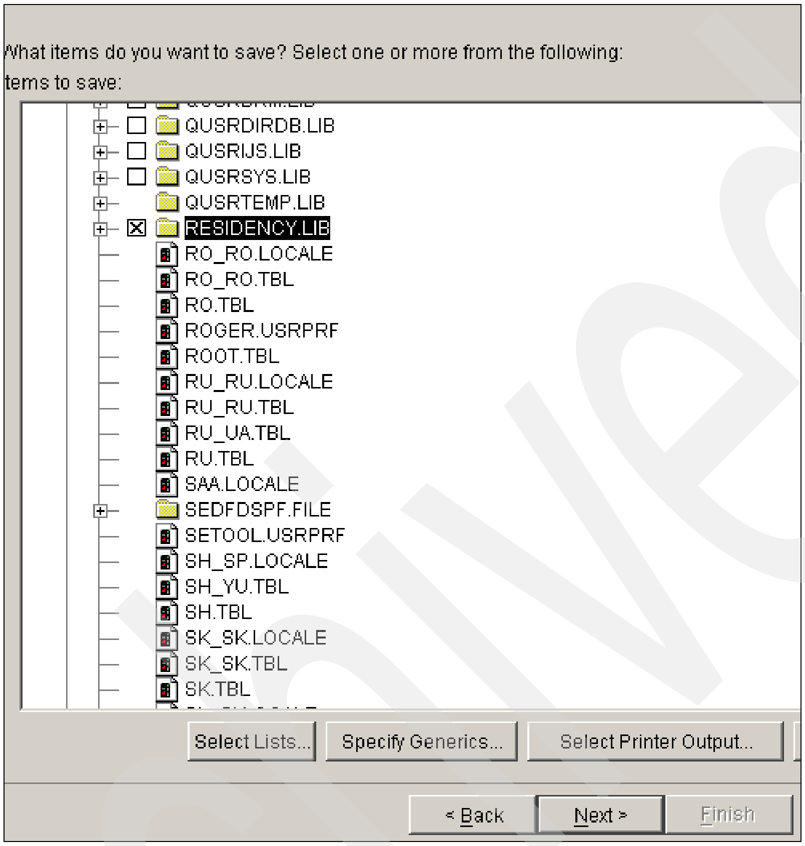
☑ Select specific items to save

☐ Select Lotus servers for online save

☐ All Lotus servers excluding online save items

Figure 6-18 New Backup policy wizard - select items to save

8. In the wizard window that pops up next, you are prompted to select which particular objects are to be saved with this backup policy. In our example we save the library Residency. Since all database libraries are objects in the system library *QSYS*, we first expand *QSYS.LIB*, then we look for the database library **Residency** and select it, as shown in Figure 6-19. After selecting the object to save, click **Next**.



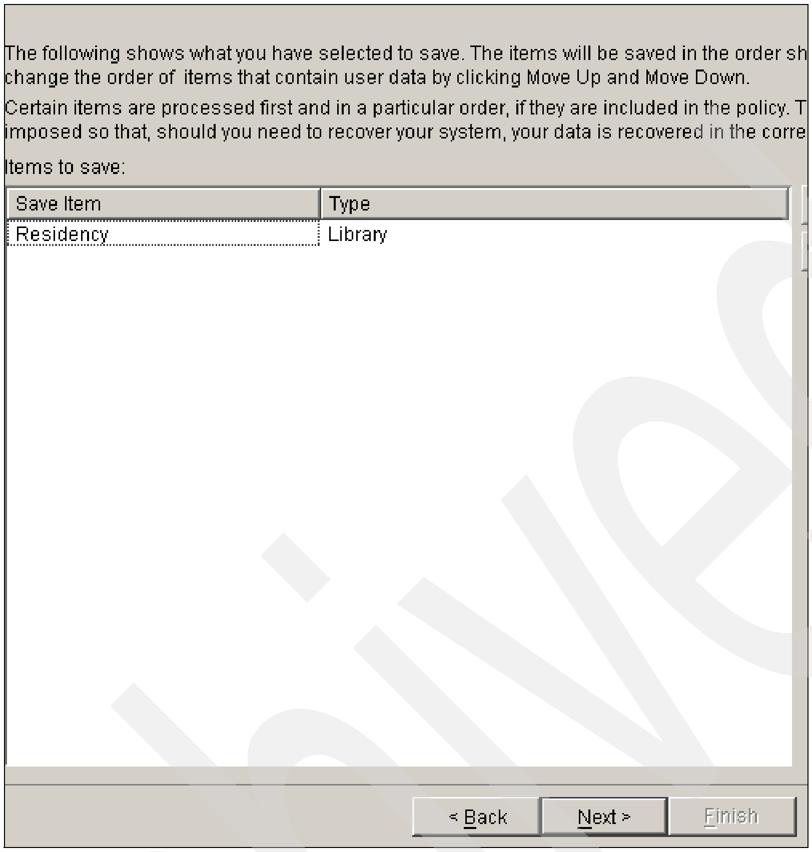
What items do you want to save? Select one or more from the following:

Items to save:

- ☐ QUSRDIRDB.LIB
- ☐ QUSRIJS.LIB
- ☐ QUSRSYS.LIB
- QUSRTEMP.LIB
- ☒ RESIDENCY.LIB
- RO_RO.LOCALE
- RO_RO.TBL
- RO.TBL
- ROGER.USRPRF
- ROOT.TBL
- RU_RU.LOCALE
- RU_RU.TBL
- RU_UA.TBL
- RU.TBL
- SAA.LOCALE
- SEDFDSPF.FILE
- SETOOL.USRPRF
- SH_SP.LOCALE
- SH_YU.TBL
- SH.TBL
- SK_SK.LOCALE
- SK_SK.TBL
- SK.TBL

Figure 6-19 New Backup policy wizard - specify object to save

9. Next, the wizard prompts you to change or confirm the order in which selected objects are saved. Click **Next** to confirm it, as shown in Figure 6-20.



The following shows what you have selected to save. The items will be saved in the order sh
change the order of items that contain user data by clicking Move Up and Move Down.

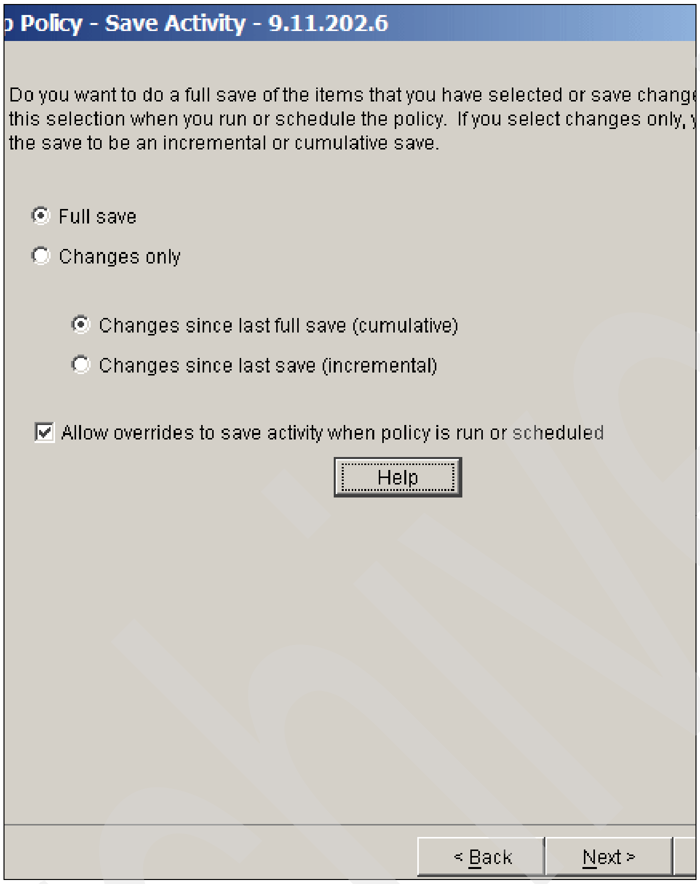
Certain items are processed first and in a particular order, if they are included in the policy. T
imposed so that, should you need to recover your system, your data is recovered in the corre

Items to save:

Save Item	Type
Residency	Library

Figure 6-20 New Backup policy wizard - change or confirm save order

10. Next, the *New Backup Policy* wizard prompts you to specify the type of backup. In our example, we take a full backup of the library Residency, so we select **Full** and we specify the option to override this selection every time the backup policy is run. This is shown in Figure 6-21. After selecting type of backup, click **Next**.



p Policy - Save Activity - 9.11.202.6

Do you want to do a full save of the items that you have selected or save change
this selection when you run or schedule the policy. If you select changes only, y
the save to be an incremental or cumulative save.

● Full save

○ Changes only

● Changes since last full save (cumulative)

○ Changes since last save (incremental)

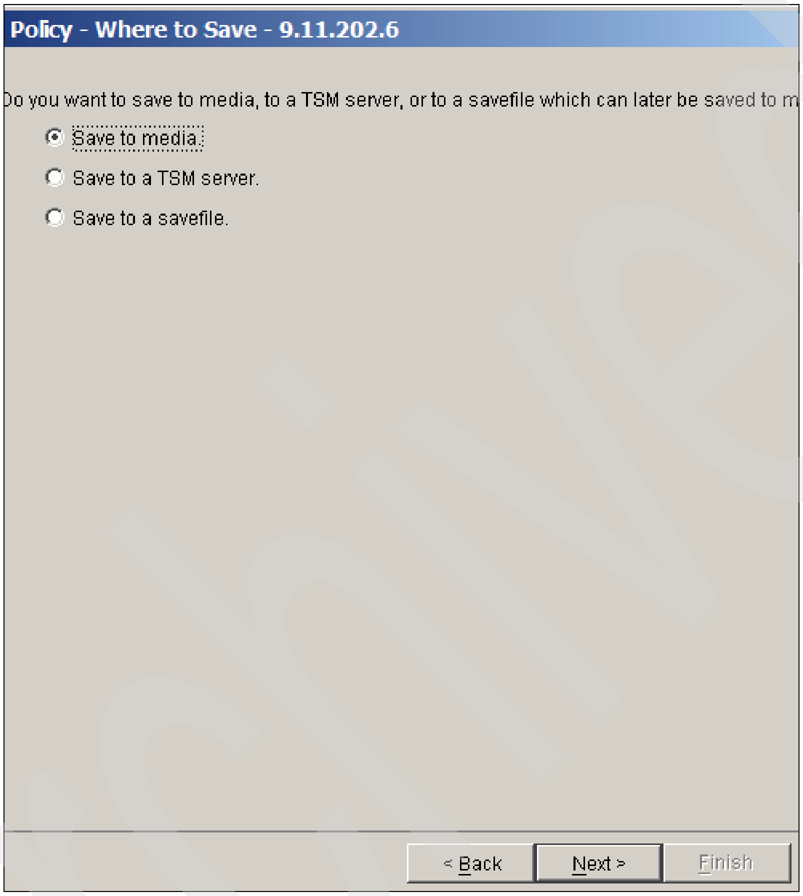
☑ Allow overrides to save activity when policy is run or scheduled

Figure 6-21 New Backup policy wizard - type of backup

11. Next you are prompted to specify where to save the newly created backup policy: to media, to the Tivoli Storage Manager server, or to i5/OS savefile. In this example we save to data cartridge, so we select **Media**, as shown in Figure 6-22. After selecting where to save, click **Next**.

12. For more information about the i5/OS savefile, refer to the System i Information Center at the following Web site:

    http://publib.boulder.ibm.com/iseries/



Do you want to save to media, to a TSM server, or to a savefile which can later be saved to m

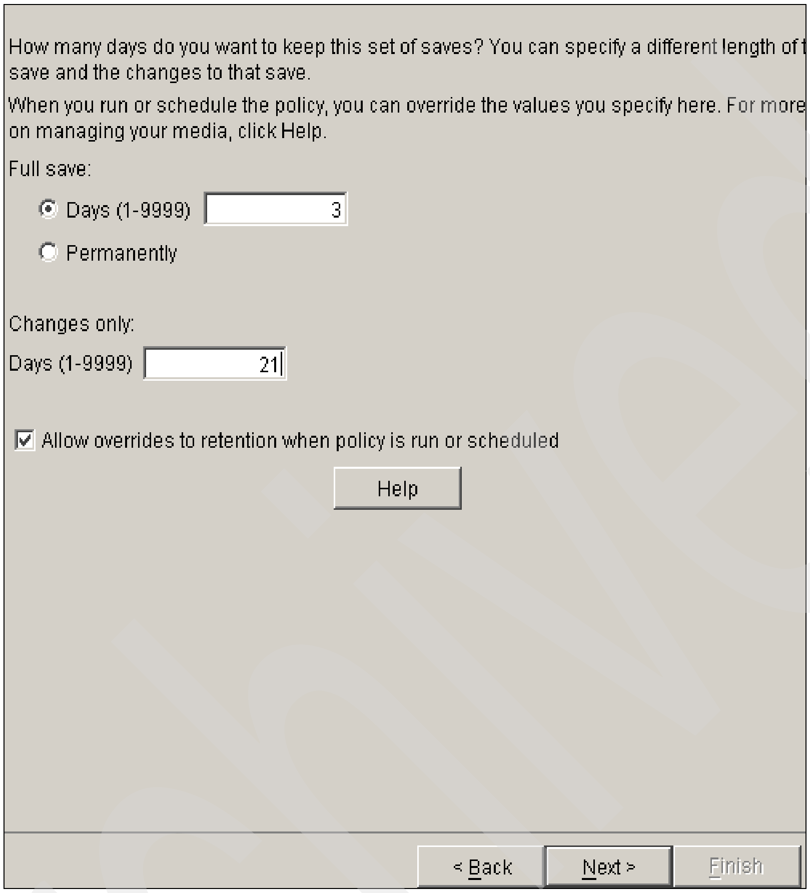
● Save to media.

○ Save to a TSM server.

○ Save to a savefile.

Figure 6-22 New Backup policy wizard - where to save

13. In the next wizard window, specify how many days the cartridge should last before expire. In our example, we save library Residency every day and we want to keep the cartridge for 3 days, so we specify 3 days to keep it, as shown in Figure 6-23. After specifying this, click **Next**.



How many days do you want to keep this set of saves? You can specify a different length of t save and the changes to that save.

When you run or schedule the policy, you can override the values you specify here. For more on managing your media, click Help.

Full save:

● Days (1-9999) 3

○ Permanently

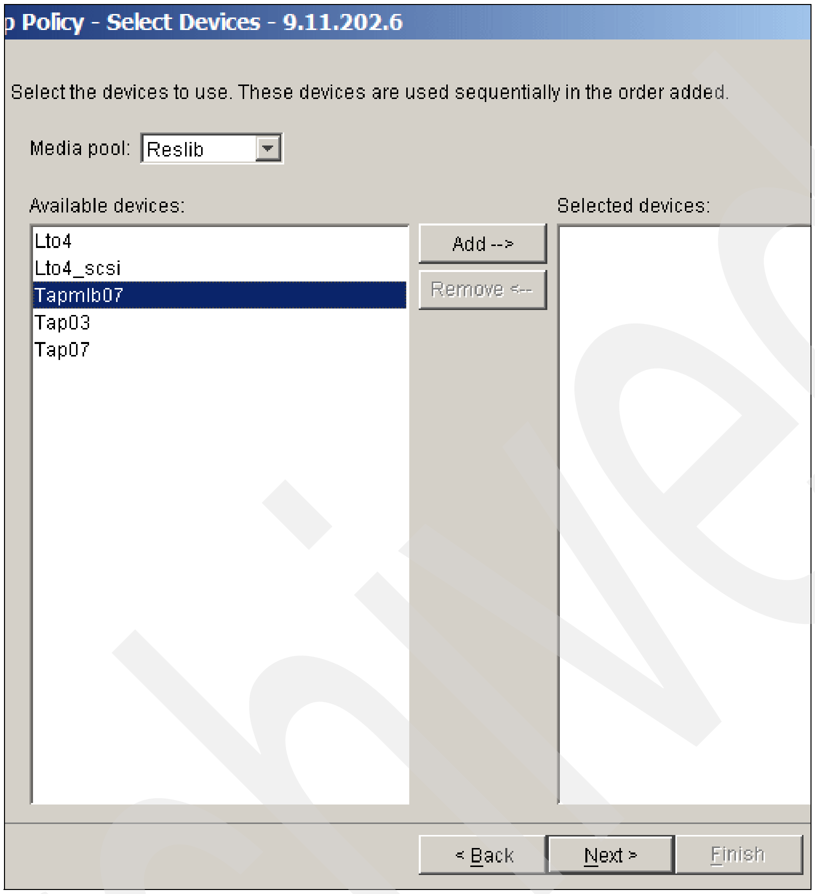
Changes only:

Days (1-9999) 21

☑ Allow overrides to retention when policy is run or scheduled

Figure 6-23 New Backup policy wizard - how many days to keep the media

14. In the next window, select the media pool from which the media are used for this backup policy, then select the device to use in the backup policy and click **Add**. In our example we use media pool Reslib and tape library device Tapmlb07, as shown in Figure 6-24.

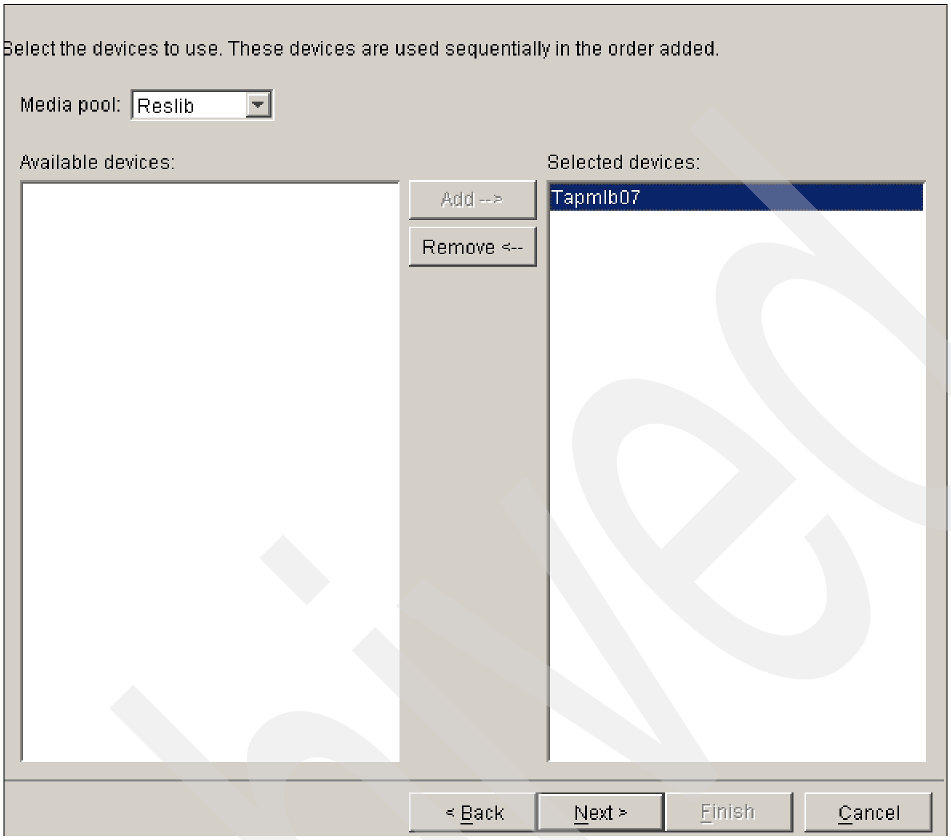


Select the devices to use. These devices are used sequentially in the order added.

Media pool: Reslib

Figure 6-24 New Backup policy wizard - which media and device to use

15. After clicking **Add**, the selected device appears in the right panel as shown in Figure 6-25. Click **Next**.



Select the devices to use. These devices are used sequentially in the order added.

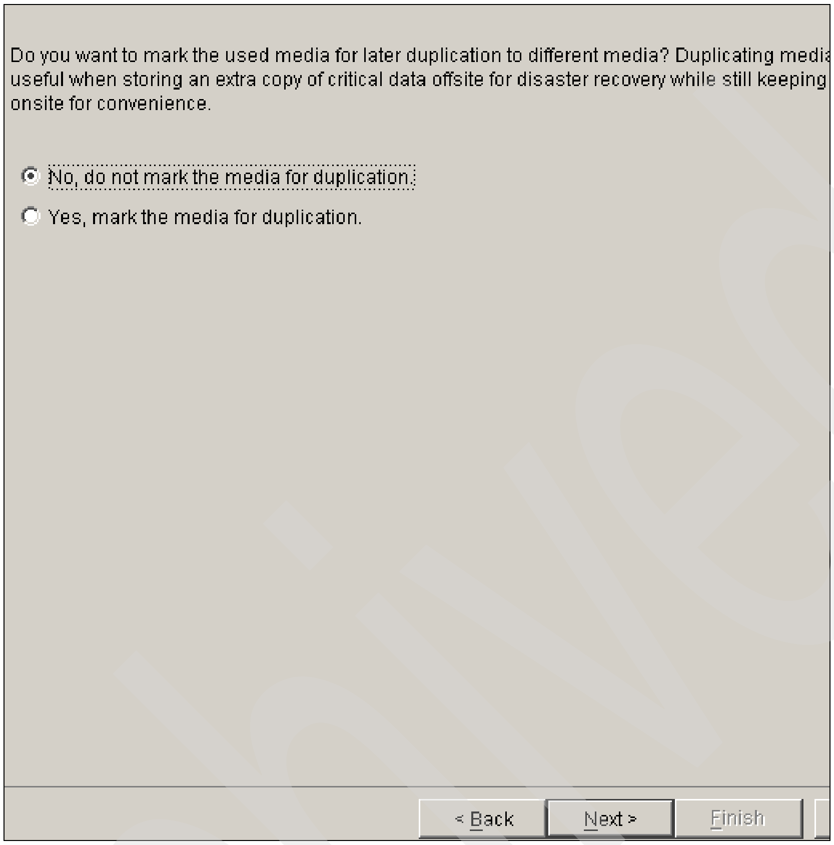
Media pool: Reslib

Available devices:

Selected devices: Tapmlb07

Figure 6-25 New Backup policy wizard - selected device

16. In the wizard window that pops up next, specify if you want the cartridges to be duplicated. In our example we do not want them to duplicate, so we select **No**, as can be seen in Figure 6-26. After making the selection, click **Next**.



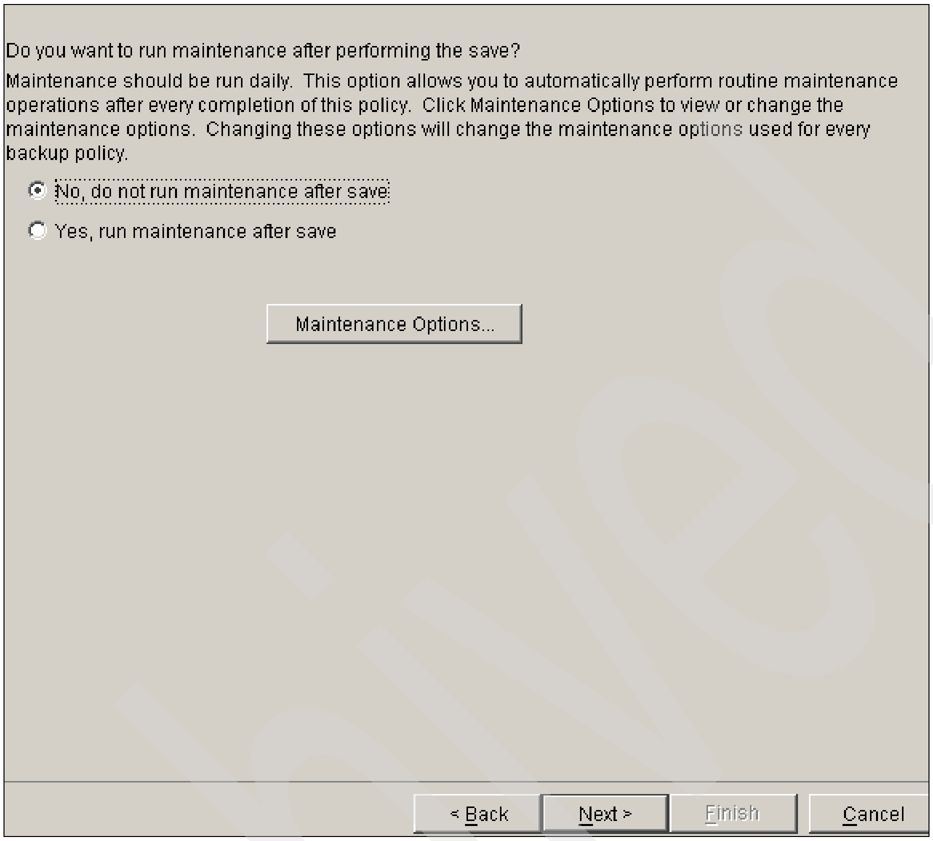
Do you want to mark the used media for later duplication to different media? Duplicating medi useful when storing an extra copy of critical data offsite for disaster recovery while still keeping onsite for convenience.

● No, do not mark the media for duplication.

○ Yes, mark the media for duplication.

Figure 6-26 New Backup policy wizard - duplicate media

17. Next, specify if you want to run BRMS maintenance after save; in out example we do not run it, as can be seen in Figure 6-27. After selecting, click **Next**.



Do you want to run maintenance after performing the save?

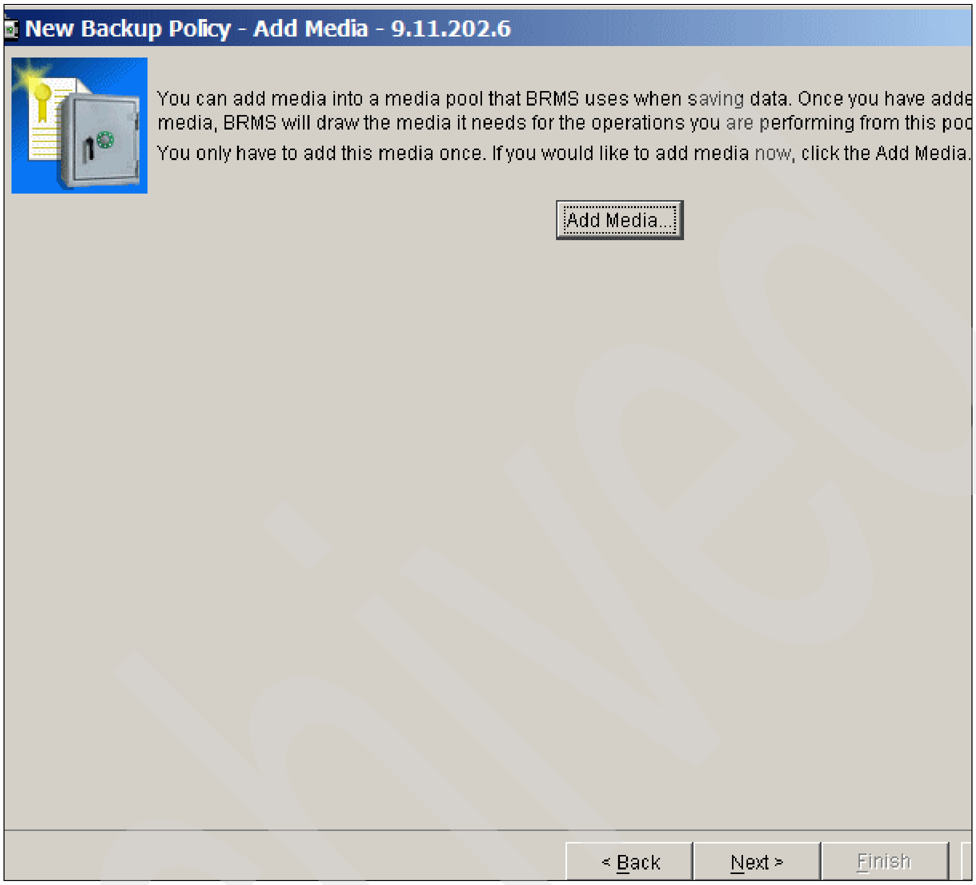
Maintenance should be run daily. This option allows you to automatically perform routine maintenance operations after every completion of this policy. Click Maintenance Options to view or change the maintenance options. Changing these options will change the maintenance options used for every backup policy.

● No, do not run maintenance after save

○ Yes, run maintenance after save

Figure 6-27 New Backup policy wizard - run maintenance

18. Next, specify if you want to add new media to the media pool used. In our example we do not add new media because we already added it before creating backup policy. So we only click **Next**. The wizard window for adding media is shown in Figure 6-28.

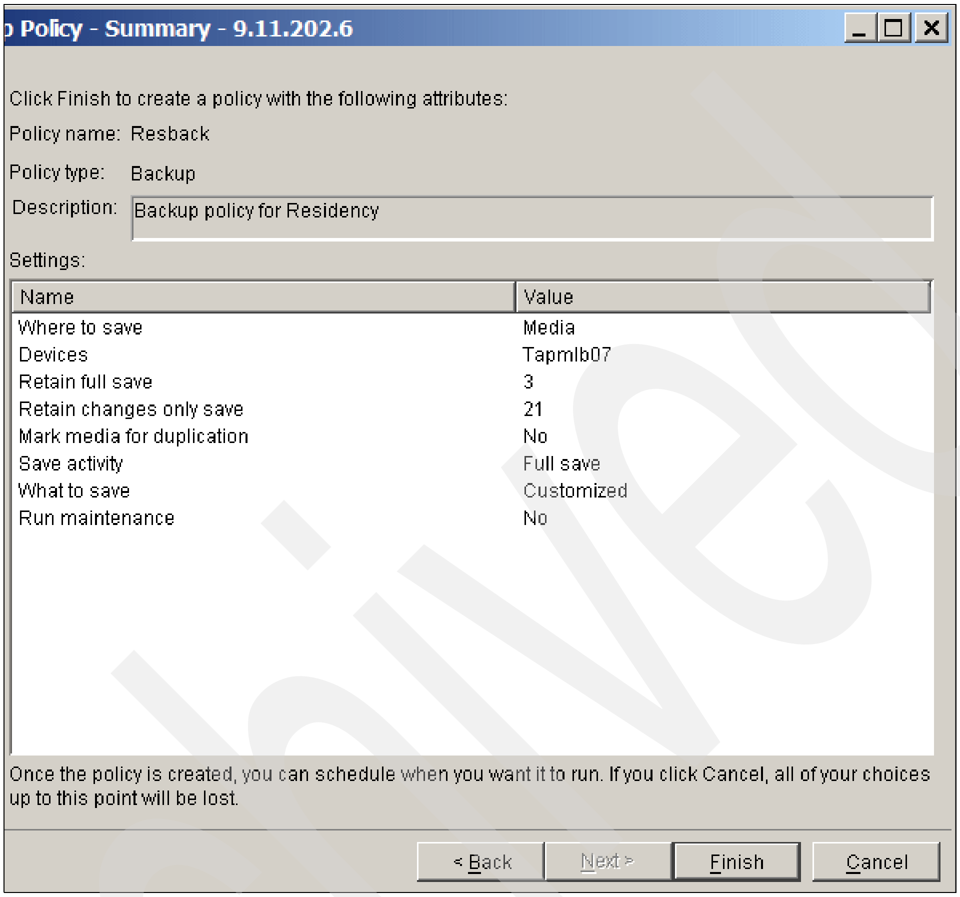


New Backup Policy - Add Media - 9.11.202.6

You can add media into a media pool that BRMS uses when saving data. Once you have adde
media, BRMS will draw the media it needs for the operations you are performing from this poo
You only have to add this media once. If you would like to add media now, click the Add Media.

Figure 6-28 New Backup policy wizard - add media

19. Next, you are presented a wizard window with features of the backup policy being created. After reviewing them, click **Finish** to create the backup policy. This is shown in Figure 6-29.



Click Finish to create a policy with the following attributes:

Policy name: Resback

Policy type: Backup

Description: Backup policy for Residency

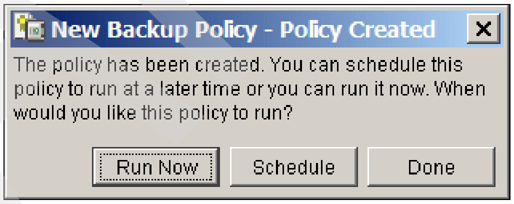
Settings:

Name	Value
Where to save	Media
Devices	Tapmlb07
Retain full save	3
Retain changes only save	21
Mark media for duplication	No
Save activity	Full save
What to save	Customized
Run maintenance	No

Once the policy is created, you can schedule when you want it to run. If you click Cancel, all of your choices up to this point will be lost.

Figure 6-29 New Backup policy wizard - policy summary

20. Next, you see a window showing the progress of creating the backup policy. After it is created, you see the window where you decide to run the backup with this policy, to schedule the backup, or just to save policy. This is shown in Figure 6-30. In our example we save the backup policy by clicking the button **Done**.



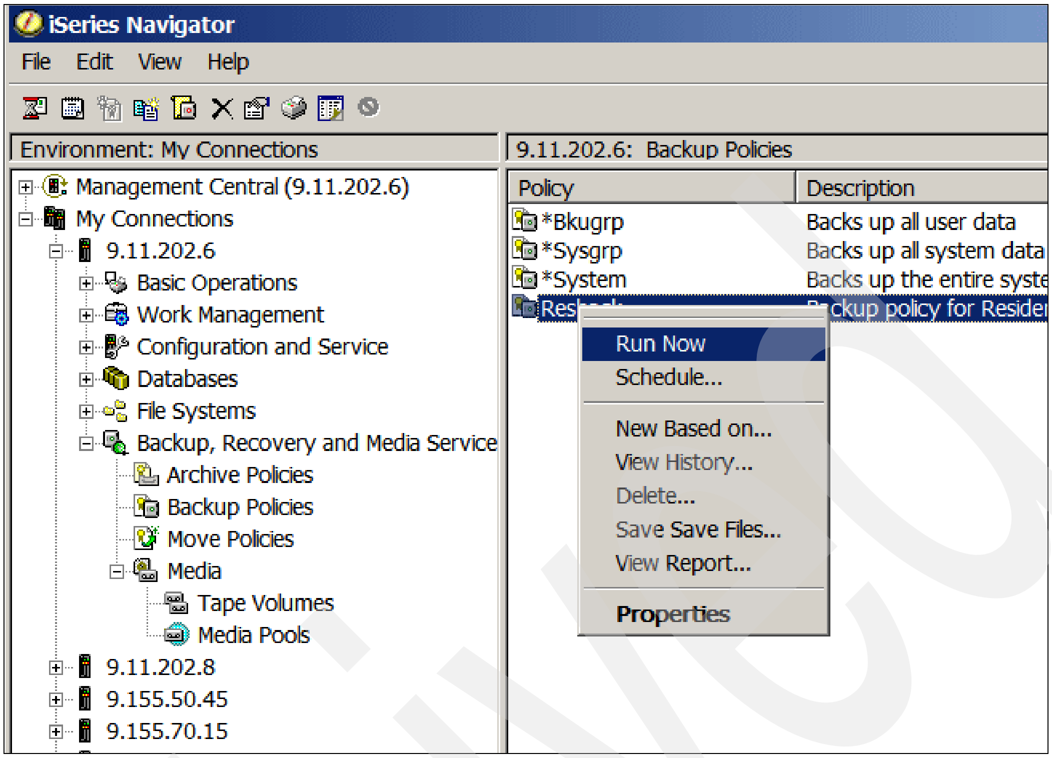
The policy has been created. You can schedule this policy to run at a later time or you can run it now. When would you like this policy to run?

Figure 6-30 New backup policy created

Running the backup policy

To run the created backup policy, perform the following steps:

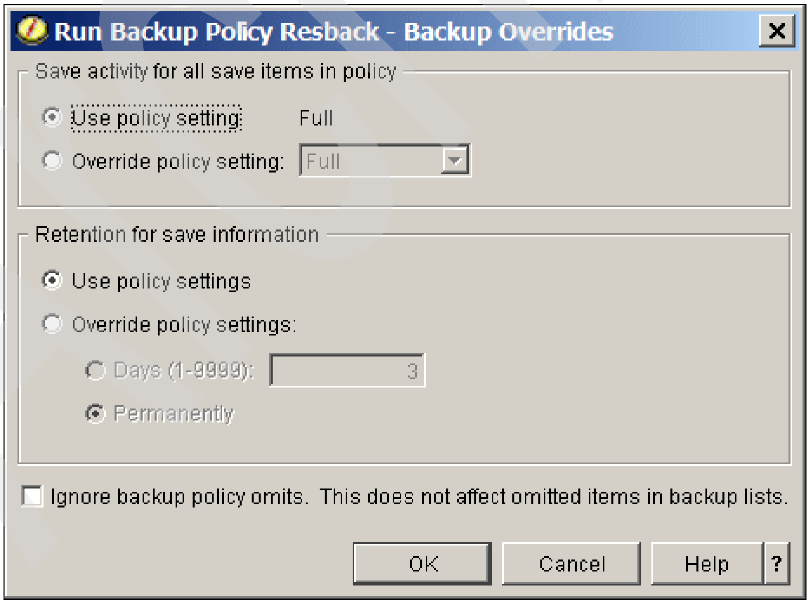
1. Still in iSeries Navigator, expand Backup Recovery and Media Services and click **Backup policies**. This displays a list of backup policies in the right panel of iSeries Navigator. Right-click the created policy and select **Run Now** from the pull-down menu. This is shown in Figure 6-31.



Policy	Description
*Bkugrp	Backs up all user data
*Sysgrp	Backs up all system data
*System	Backs up the entire syste
Res	ackup policy for Resider

Figure 6-31   Run backup policy

2. Next, you are presented a window where you can confirm or change the type of backup as specified in the backup policy. In our example we confirm what is defined in the backup policy, as shown in Figure 6-32. After using or overriding the policy settings, click **OK**.



Save activity for all save items in policy

● Use policy setting: Full

○ Override policy setting: Full

Retention for save information

● Use policy settings

○ Override policy settings:

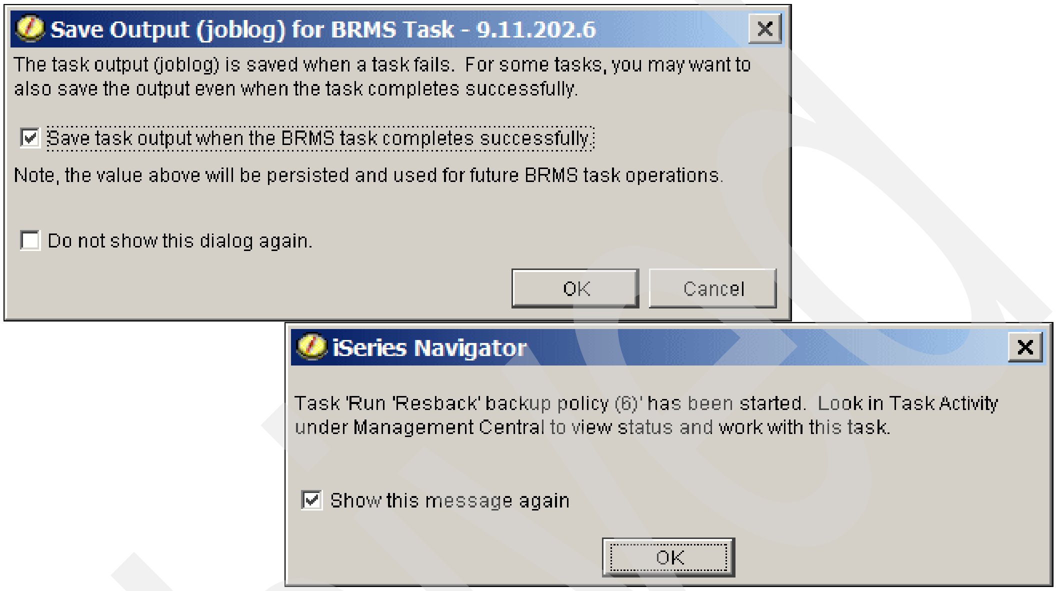
○ Days (1-9999): 3

● Permanently

□ Ignore backup policy omits. This does not affect omitted items in backup lists.

Figure 6-32   Run backup policy - use or override policy settings

3. Next you are presented a window where you select if you want to save the output of this BRMS task, even if the task is successful. In our example we specify to save output, as can be seen in Figure 6-33. Click **OK** after making the selection.
4. A window is displayed, informing you that the backup task has started. On this window, click **OK**. See Figure 6-33.


Save Output (joblog) for BRMS Task - 9.11.202.6

The task output (joblog) is saved when a task fails. For some tasks, you may want to also save the output even when the task completes successfully.

☑ Save task output when the BRMS task completes successfully.

Note, the value above will be persisted and used for future BRMS task operations.

□ Do not show this dialog again.

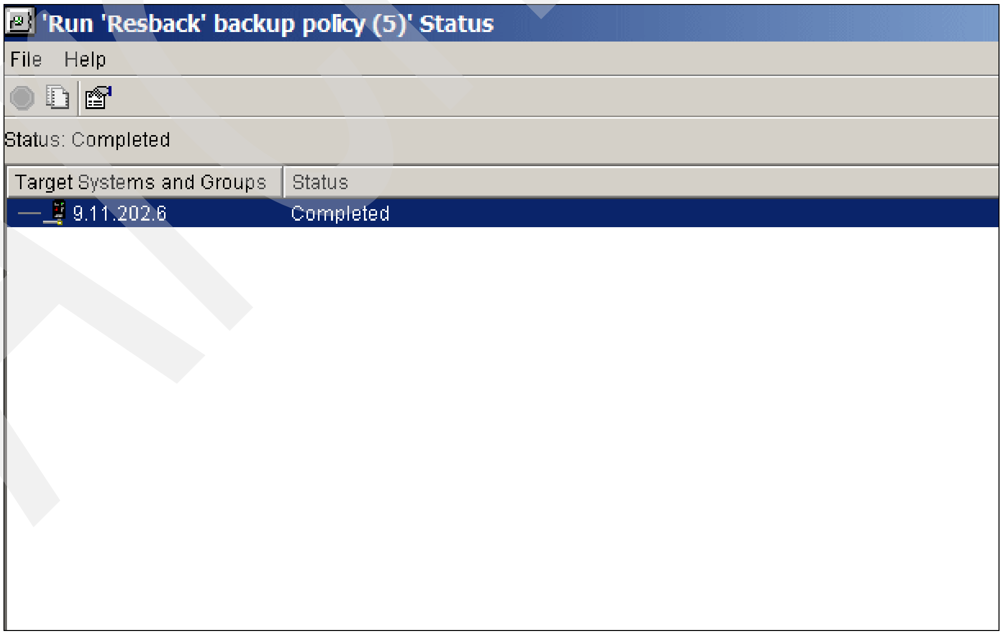
iSeries Navigator

Task 'Run 'Resback' backup policy (6)' has been started. Look in Task Activity under Management Central to view status and work with this task.

☑ Show this message again

Figure 6-33 Run backup policy - further messages

5. Next, you are presented the window showing the status of BRMS task for backup. After the task is successfully completed, the window shows completion, as can be seen in Figure 6-34.


'Run 'Resback' backup policy (5)' Status

Status: Completed

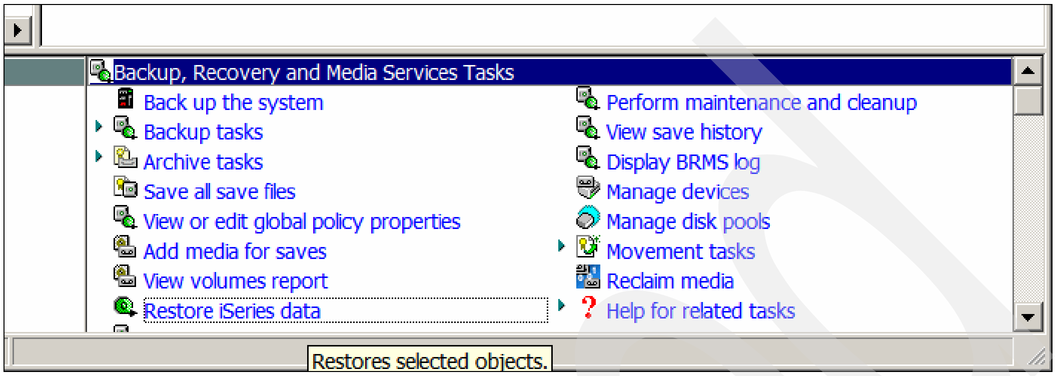
Target Systems and Groups	Status
9.11.202.6	Completed

Figure 6-34 Run backup policy completed

Restoring the database library

To restore the saved database library, perform the following steps:

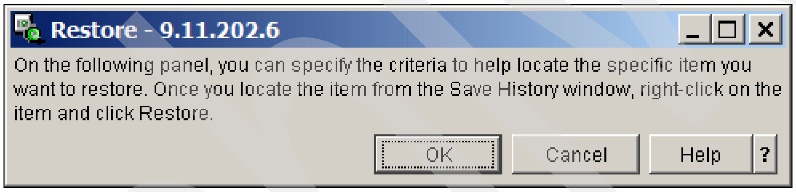
1. Still in iSeries Navigator, in the bottom right panel, click **Restore iSeries Data**. This is shown in Figure 6-35.



Restores selected objects.

Figure 6-35 Restore saved data i

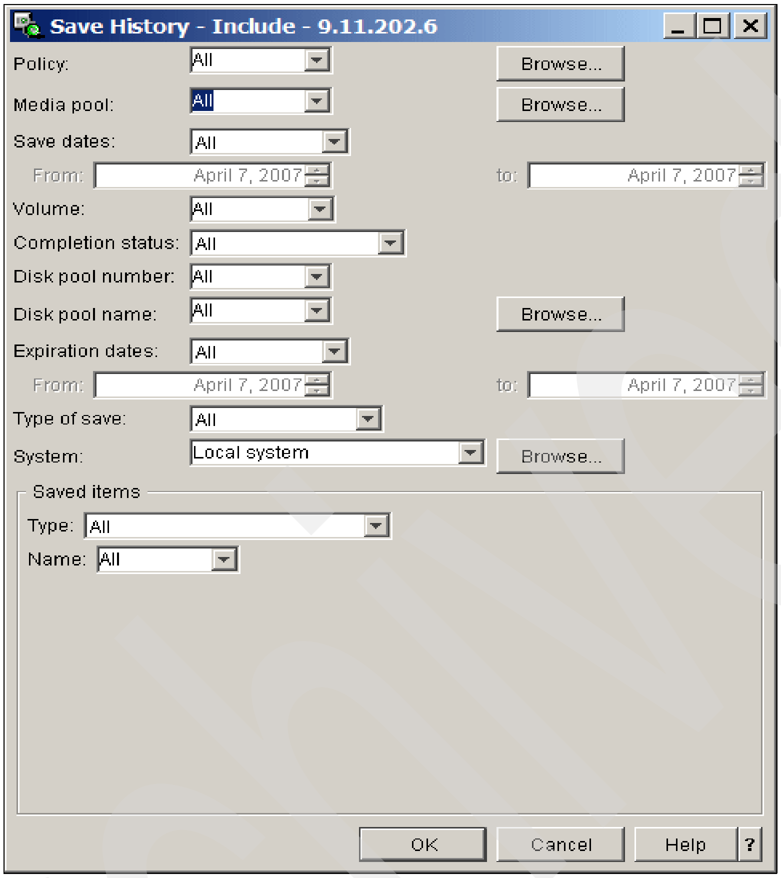
2. A window, which is displayed next, is informational: It tells you that you can insert criteria by which to choose the object to restore. This window is shown in Figure 6-36. On this window, click **OK**.



On the following panel, you can specify the criteria to help locate the specific item you want to restore. Once you locate the item from the Save History window, right-click on the item and click Restore.

Figure 6-36 Informational window

3. On the window that is displayed next, you have the possibility to limit the saves from which you choose the object to restore. You can limit them to a specific backup policy, media pool, or range of dates. In our example, we leave it as default: all backup policies, all media pools, all dates, and so on. This is shown in Figure 6-37.



Save History - Include - 9.11.202.6

Policy: All

Media pool: All

Save dates: All

From: April 7, 2007 to: April 7, 2007

Volume: All

Completion status: All

Disk pool number: All

Disk pool name: All

Expiration dates: All

From: April 7, 2007 to: April 7, 2007

Type of save: All

System: Local system

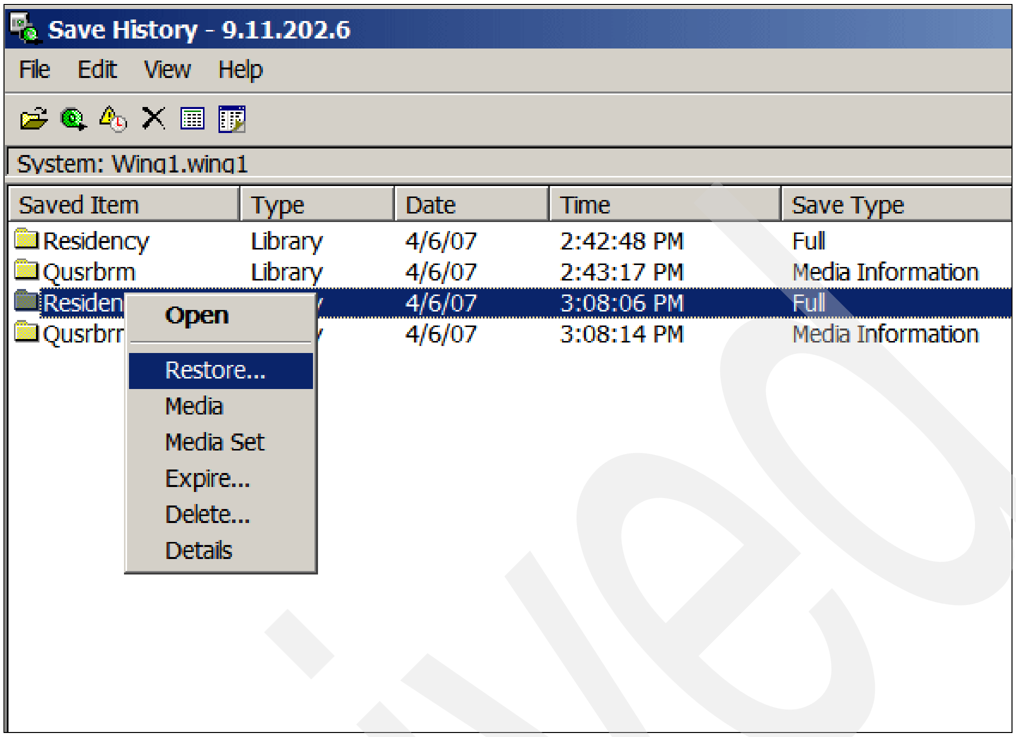
Saved items

Type: All

Name: All

Figure 6-37 Limit selection for restore

4. Next, BRMS shows you the saved objects within specifications you made. Right-click the object you want to restore, and select **Restore** from pull-down menu, as shown in Figure 6-38.

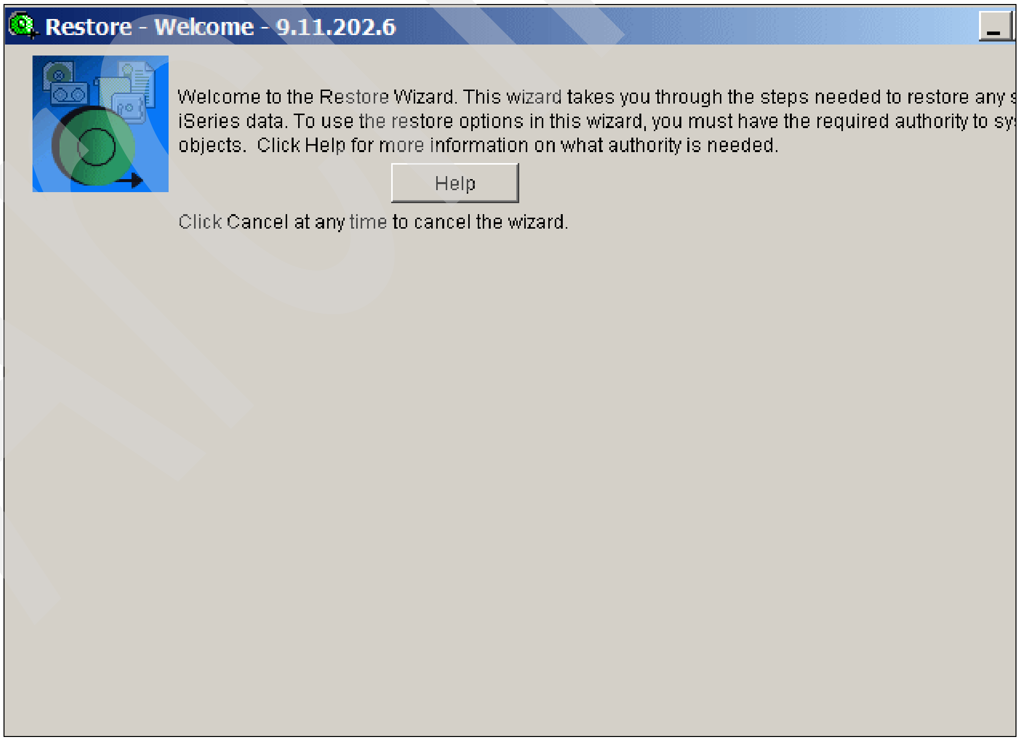


System: Wing1.wing1

Saved Item	Type	Date	Time	Save Type
Residency	Library	4/6/07	2:42:48 PM	Full
Qusrbrm	Library	4/6/07	2:43:17 PM	Media Information
Residen	y	4/6/07	3:08:06 PM	Full
Qusrbrr	y	4/6/07	3:08:14 PM	Media Information

Figure 6-38   Select object to restore

5. After selecting the item to restore, the *Restore* wizard starts. The initial wizard window is shown in Figure 6-39. On this window, click **Next**.



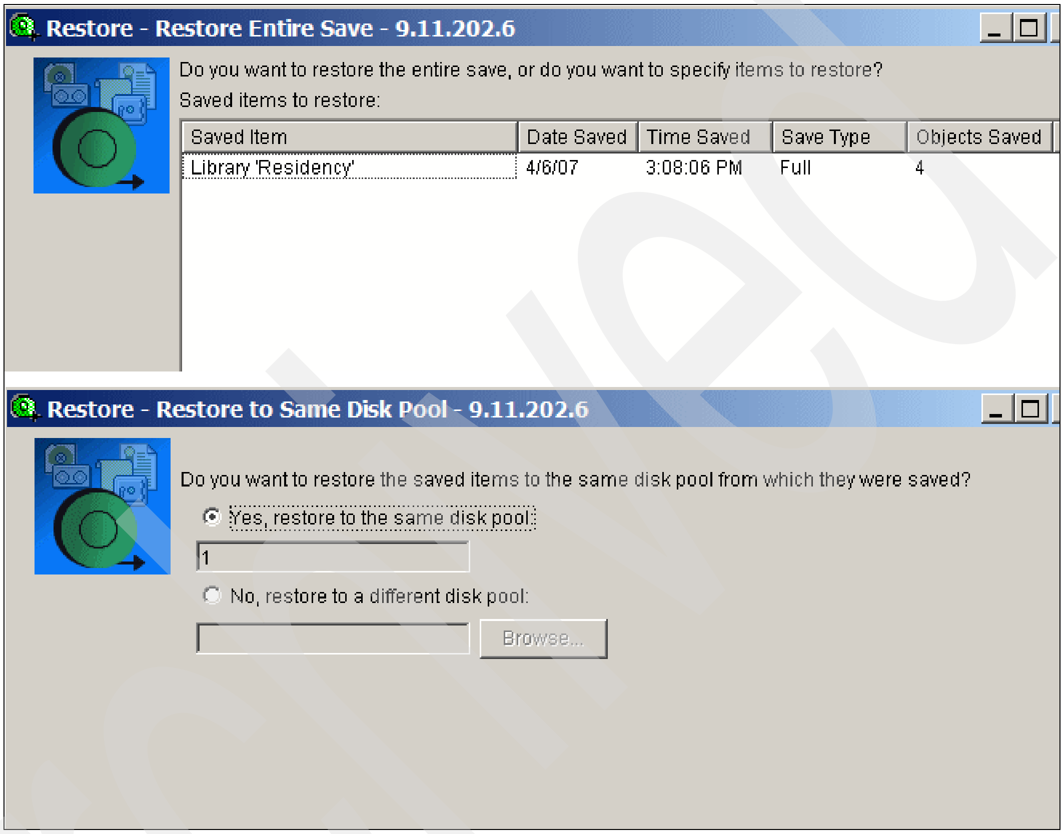
Welcome to the Restore Wizard. This wizard takes you through the steps needed to restore any s
iSeries data. To use the restore options in this wizard, you must have the required authority to sy
objects. Click Help for more information on what authority is needed.

Click Cancel at any time to cancel the wizard.

Figure 6-39   Restore Wizard Welcome window

- On next Wizard windows, you can select the following items:
  - Restore all items from the saved object, or restore just the selected ones.
  - Restore items to the same disk pool they were saved from, or another disk pool.
  - Restore items to the same location they were saved from, or another location.
  - Automatically or manually select the device from which to restore.

  After making your selection on each window, **click Next.** Parts of these windows are shown in Figure 6-40 and Figure 6-41.



Restore - Restore Entire Save - 9.11.202.6

Do you want to restore the entire save, or do you want to specify items to restore?

Saved items to restore:

Saved Item	Date Saved	Time Saved	Save Type	Objects Saved
Library 'Residency'	4/6/07	3:08:06 PM	Full	4

Restore - Restore to Same Disk Pool - 9.11.202.6

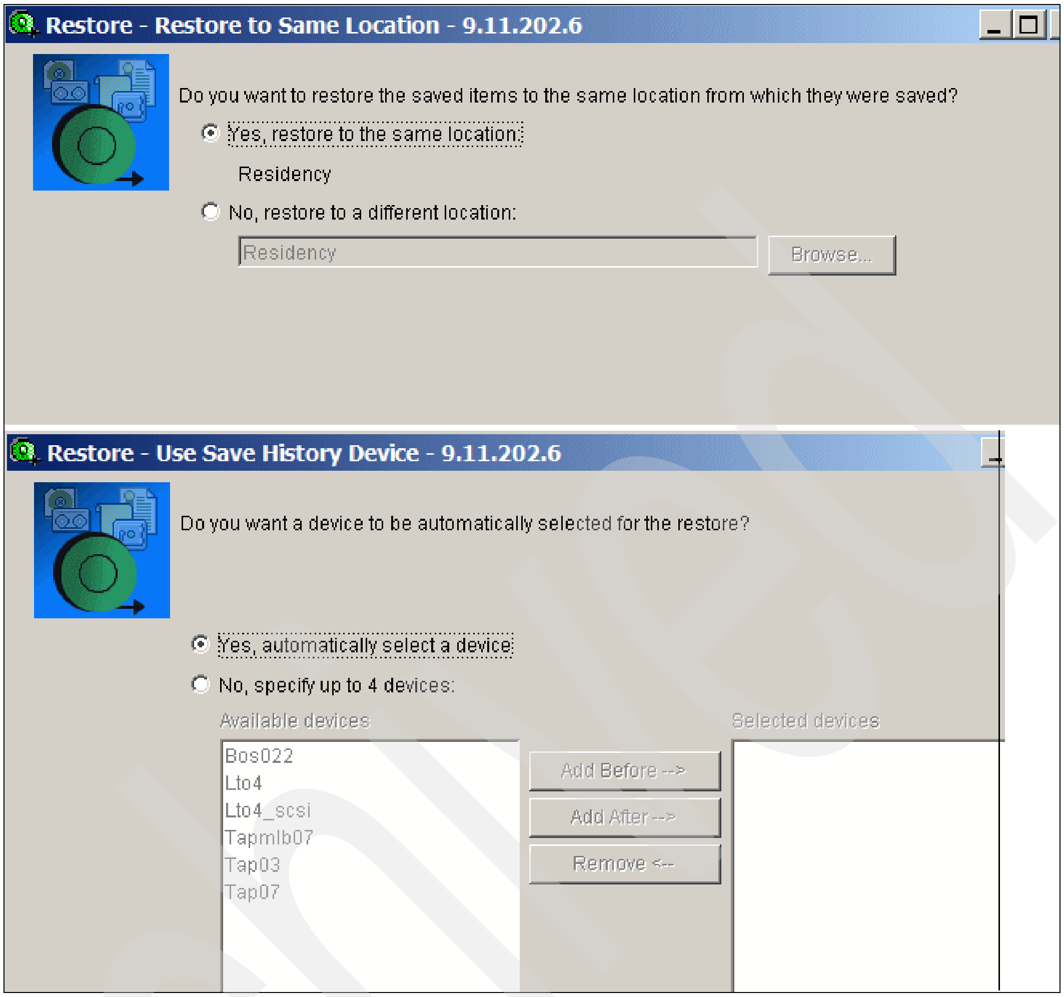
Do you want to restore the saved items to the same disk pool from which they were saved?

● Yes, restore to the same disk pool:

1

○ No, restore to a different disk pool:

Figure 6-40 Restore wizard -1



Restore - Restore to Same Location - 9.11.202.6

Do you want to restore the saved items to the same location from which they were saved?

● Yes, restore to the same location:

Residency

○ No, restore to a different location:

Residency

Restore - Use Save History Device - 9.11.202.6

Do you want a device to be automatically selected for the restore?

● Yes, automatically select a device

○ No, specify up to 4 devices:

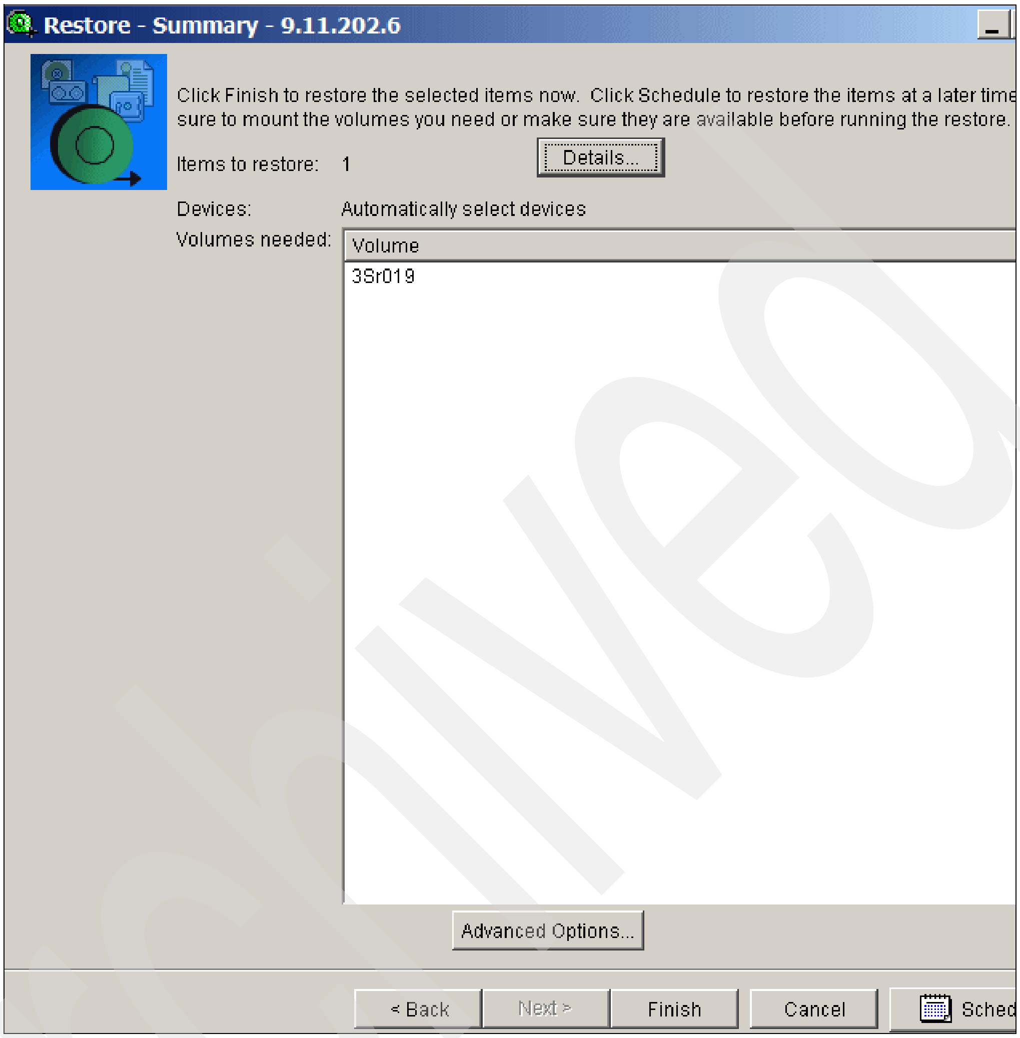
Available devices

Bos022
Lto4
Lto4_scsi
Tapmlb07
Tap03
Tap07

Selected devices

Figure 6-41 Restore wizard - 2

6. The next *Restore* wizard presents you a window where you can check if the data you want is specified to be restored. After checking, click **Finish**, as shown in Figure 6-42.



Restore - Summary - 9.11.202.6

Click Finish to restore the selected items now. Click Schedule to restore the items at a later time sure to mount the volumes you need or make sure they are available before running the restore.

Items to restore: 1

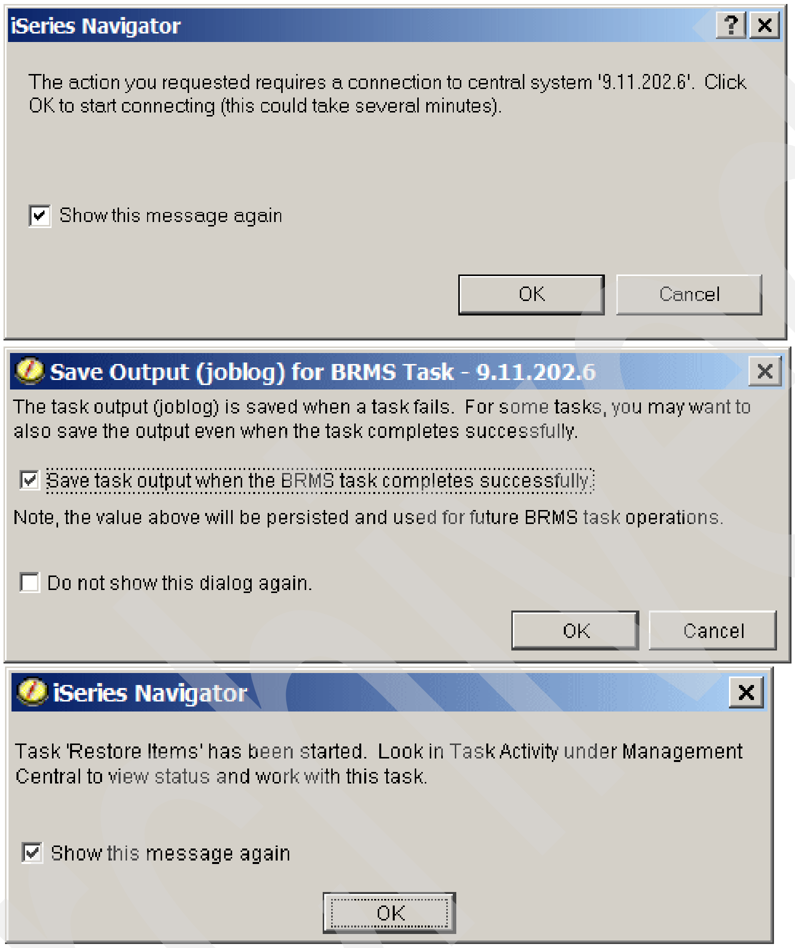
Devices: Automatically select devices

Volumes needed:

Volume
3Sr019

Figure 6-42 Check and confirm which data you want to restorer

7. Next, similar windows as with save (run backup policy) are shown, informing you about the connection to iSeries Management Central, asking you for a selection to save BRMS task output, and informing you about the possibility to look at status panel while the restore task is executed. These windows are shown in Figure 6-43. On each window, click **OK** after making your selections.



iSeries Navigator

The action you requested requires a connection to central system '9.11.202.6'. Click OK to start connecting (this could take several minutes).

☑ Show this message again

Save Output (joblog) for BRMS Task - 9.11.202.6

The task output (joblog) is saved when a task fails. For some tasks, you may want to also save the output even when the task completes successfully.

☑ Save task output when the BRMS task completes successfully.

Note, the value above will be persisted and used for future BRMS task operations.

☐ Do not show this dialog again.

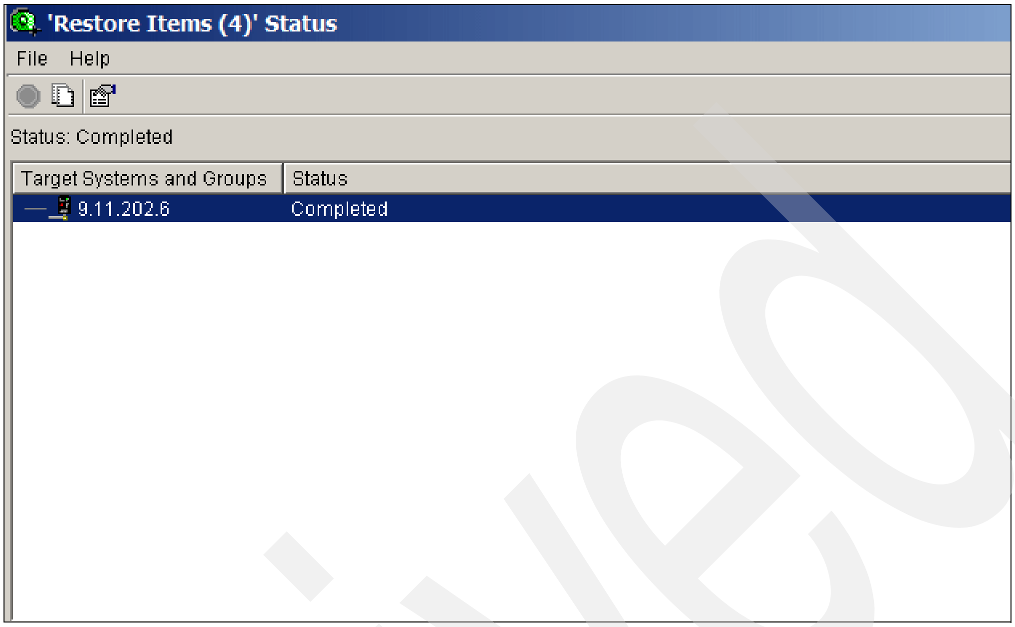
iSeries Navigator

Task 'Restore Items' has been started. Look in Task Activity under Management Central to view status and work with this task.

☑ Show this message again

Figure 6-43 Restore wizard - 3

8. When the restore is completed, the status window shows *Status Completed*, as can be seen in Figure 6-44.



Status: Completed

Target Systems and Groups	Status
9.11.202.6	Completed

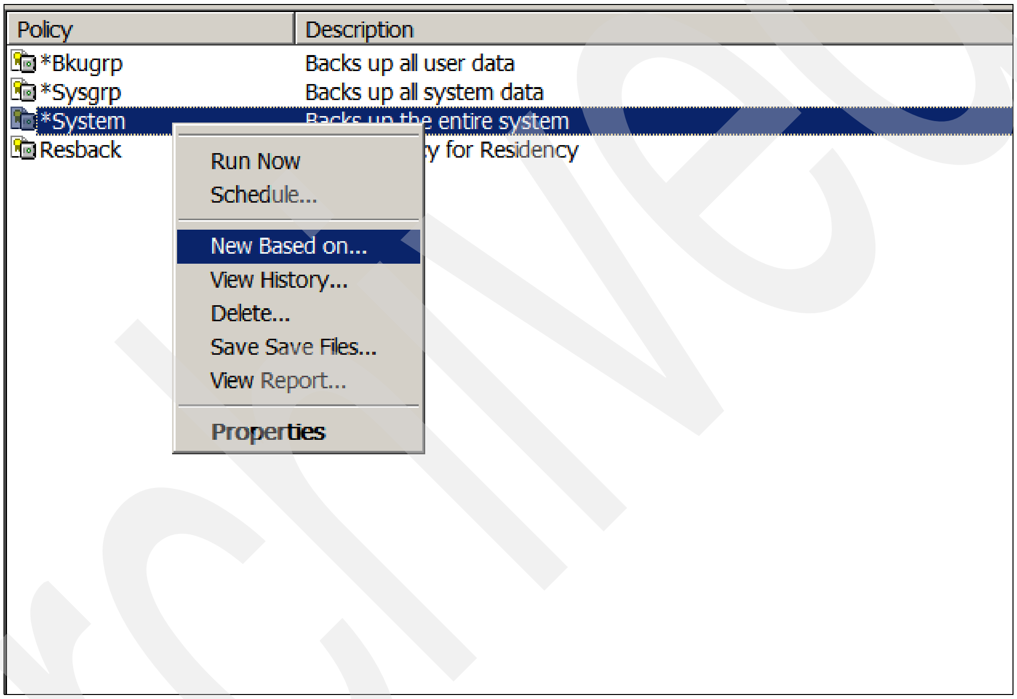
Figure 6-44 Restore complete

6.3 Saving the entire system

To schedule a save of the entire system with BRMS, use backup policy **System* or create another backup policy based on policy **System*. To create another backup policy for the entire system save, perform the following steps:

Start iSeries navigator if not yet started, and connect to System i, as is described in 5.1, “Basic setup” on page 108. Then perform these steps:

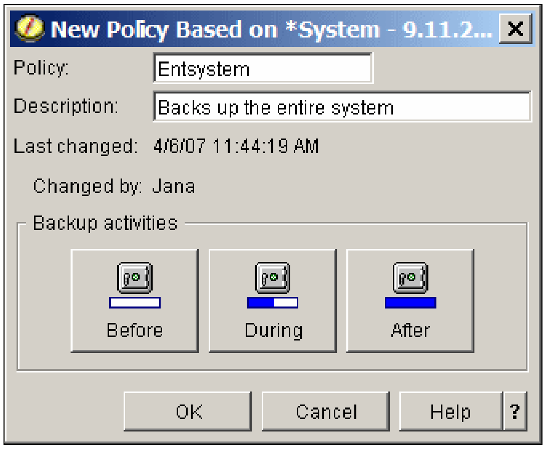
1. In iSeries navigator, expand the IP address of the System i partition with which you are working, expand *Backup Recovery and Media Services*, and click **Backup Policies**. This displays a list of existing backup policies in the right panel of iSeries Navigator. In the right panel, right-click the backup policy **System* and select **New based on** from the pull-down menu that pops up. This is shown in Figure 6-45.



Policy	Description
*Bkugrp	Backs up all user data
*Sysgrp	Backs up all system data
*System	Backs up the entire system
Resback	y for Residency

Figure 6-45 Create new backup policy for save entire system

2. This displays the window *New Policy Based on *System*. On this window, insert the name of new backup policy, as shown in Figure 6-46.



Policy: Entsystem

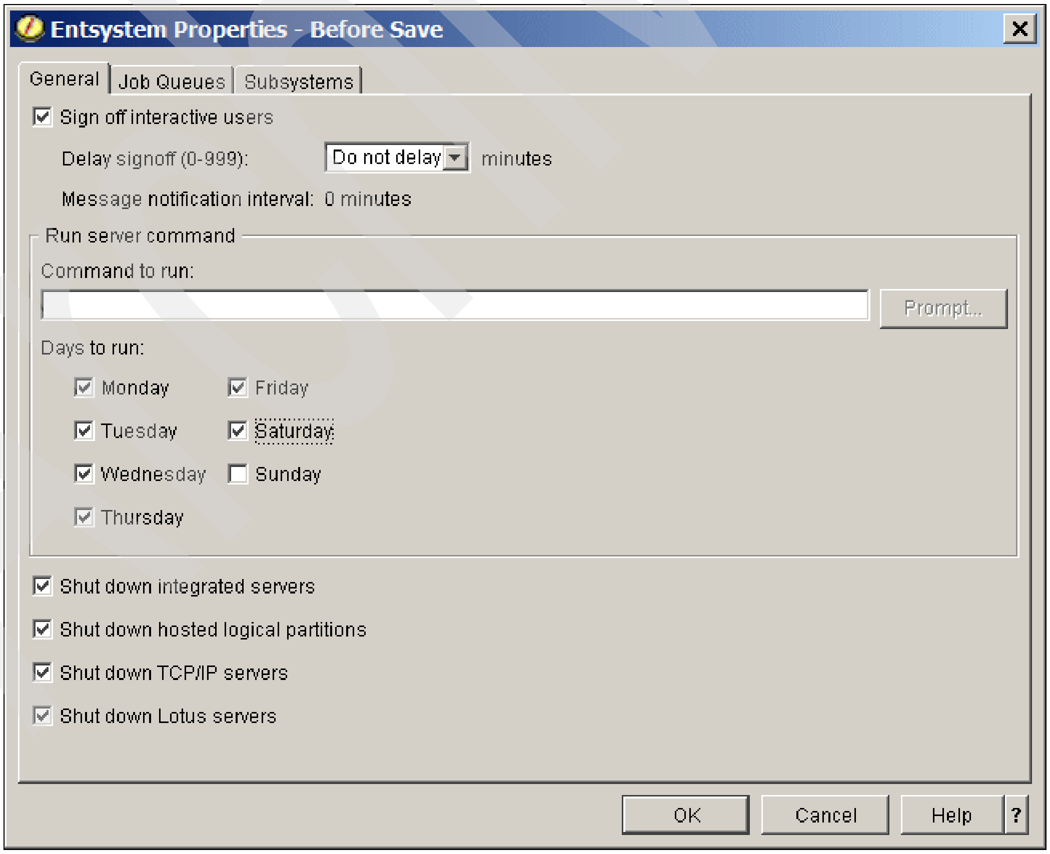
Description: Backs up the entire system

Last changed: 4/6/07 11:44:19 AM

Changed by: Jana

Figure 6-46 Specify name of new backup policy for entire system

3. Still in the window *New Policy Based on *System*, click the button **Before**. This displays the panel, *Backup Policy Properties - Before Save*, where you can adjust the default days on which the entire system is scheduled to save. In our example we want to take a backup of the entire system every day except Sunday, so we un-check the box at Sunday, as shown in Figure 6-47. After adjusting the schedule, click **OK**.



☑ Sign off interactive users

Delay signoff (0-999): Do not delay minutes

Message notification interval: 0 minutes

Command to run:

Days to run:

☑ Monday ☑ Friday

☑ Tuesday ☑ Saturday

☑ Wednesday ☐ Sunday

☑ Thursday

☑ Shut down integrated servers

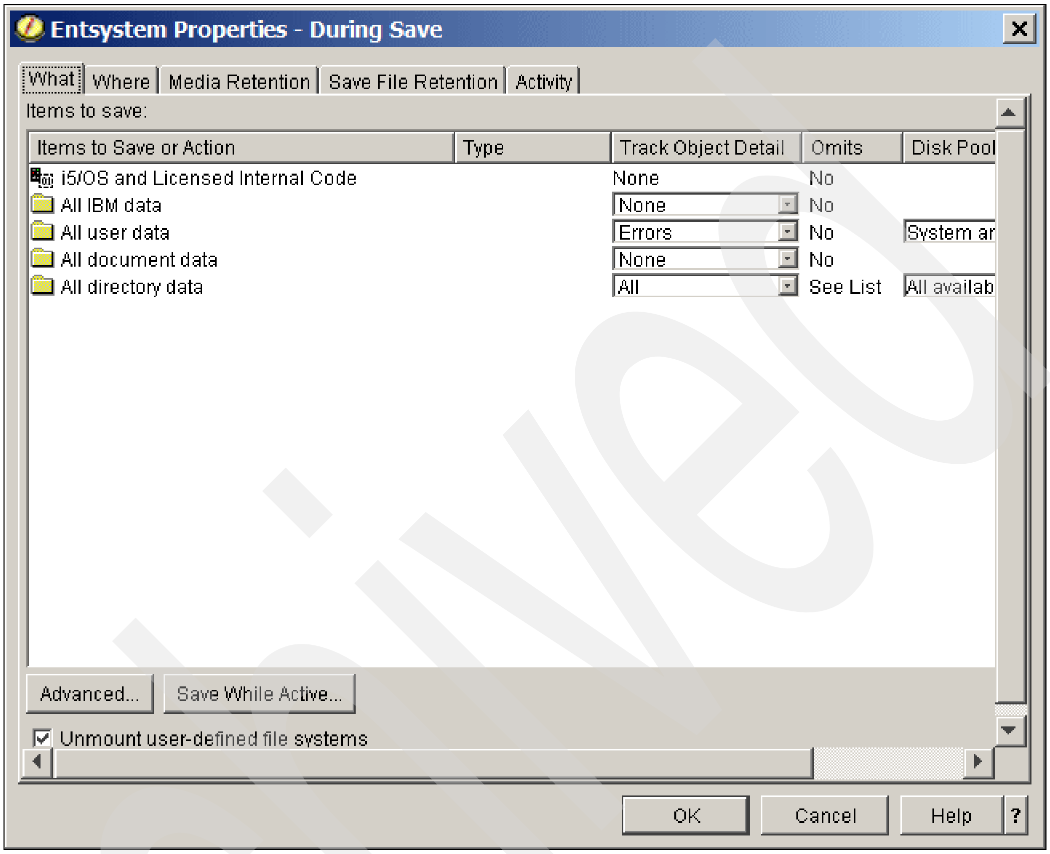
☑ Shut down hosted logical partitions

☑ Shut down TCP/IP servers

☑ Shut down Lotus servers

Figure 6-47 Adjust schedule for save entire system

4. In the window *New Policy Based on *System,* click the button **During**. This displays the panel *Backup policy properties - During save* where you can select which parts of the i5/OS are to be saved. In our example, we leave all parts listed by default to be saved, as shown in Figure 6-48. After making the selection, click **OK**.



Items to save:

Items to Save or Action	Type	Track Object Detail	Omits	Disk Pool
i5/OS and Licensed Internal Code		None	No	
All IBM data		None	No	
All user data		Errors	No	System ar
All document data		None	No	
All directory data		All	See List	All availab

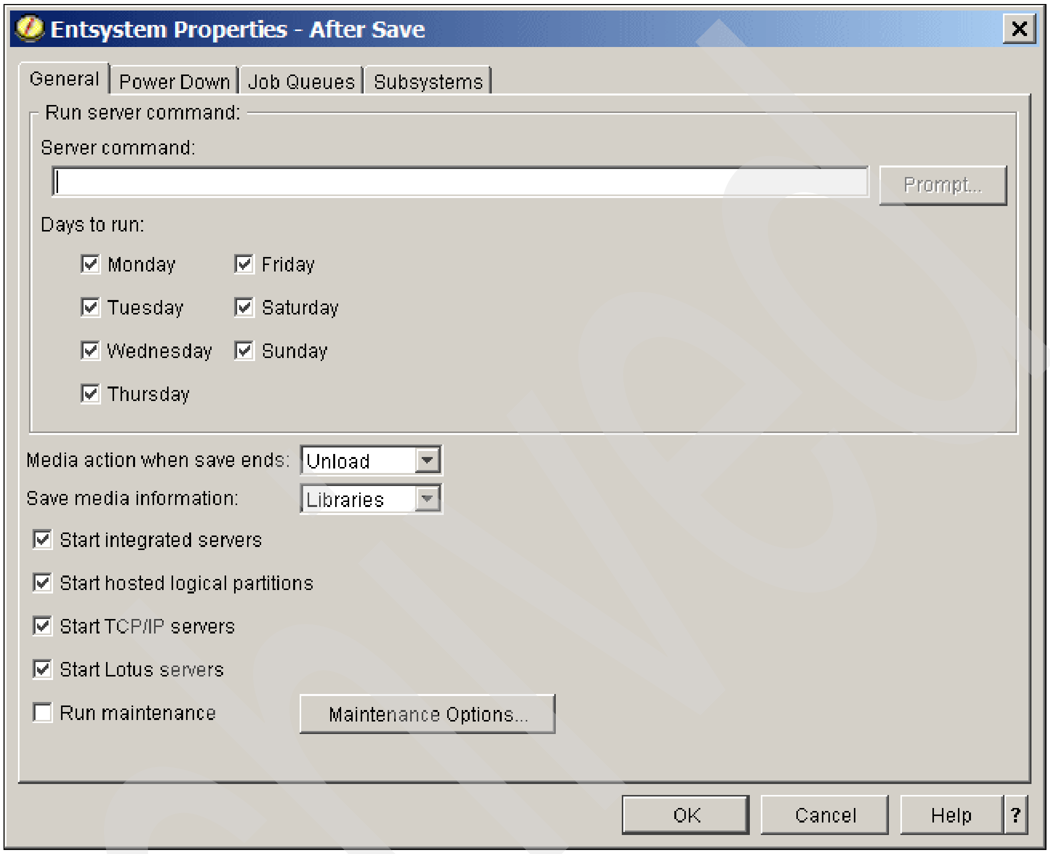
☑ Unmount user-defined file systems

Figure 6-48 Select parts of i5/OS to save

5. In the window *New Policy Based on *System,* click the button **After**. This displays the panel *Backup policy properties - After save*. Here you can specify how to handle media after save and which i5/OS functions to start after entire save is performed.

> **Note:** The save on the entire system requires that the system is in restricted state, so most of the i5/OS functions must be stopped during this time.

In our example we leave values as default, as shown in Figure 6-49. You can also click other tabs in the window *Backup policy properties - After save,* and specify say if it is required to power-down the system after save. After adjusting values, click **OK**. On the window *New Policy Based on *System,* click **OK** to save the created policy.



Run server command:

Server command:

Days to run:

☑ Monday ☑ Friday

☑ Tuesday ☑ Saturday

☑ Wednesday ☑ Sunday

☑ Thursday

Media action when save ends: Unload

Save media information: Libraries

☑ Start integrated servers

☑ Start hosted logical partitions

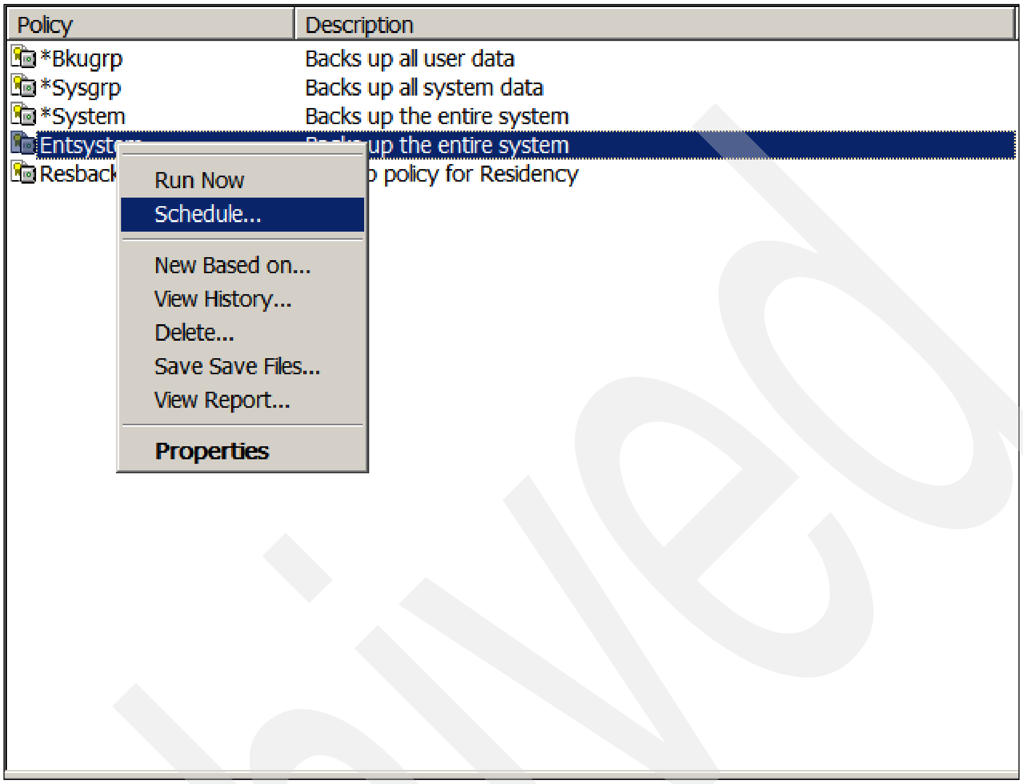
☑ Start TCP/IP servers

☑ Start Lotus servers

☐ Run maintenance

Figure 6-49 Specify what to do after save is performed

6. After the backup policy is created, you schedule it by right-clicking the newly created policy and selecting **Schedule** from the pull-down that pops up. This is shown in Figure 6-50.



Policy	Description
*Bkugrp	Backs up all user data
*Sysgrp	Backs up all system data
*System	Backs up the entire system
Entsyst	Backs up the entire system
Resback	p policy for Residency

Figure 6-50 Schedule save of entire system

7

Tape encryption with i5/OS

This chapter describes Library-Managed Tape Encryption with the IBM TS1120 Tape Drive (3592-E05) and the IBM Linear Tape-Open (LTO) Ultrium 4 Tape Drive for i5/OS environments.

We cover the following major topics:

- Reasons for using tape encryption and the different concepts between TS1120 and LTO4
- Planning for tape encryption with i5/OS and clarification of the software and hardware prerequisites together with considerations for disaster recovery and sharing tape cartridges with partners
- Detailed implementation procedures to provide guidance for installing the Encryption Key Manager on i5/OS
- Configuring Library-Managed Encryption for TS1120 and LTO4 drives

7.1 Tape encryption overview

Analog to data protection over network communication via Virtual Private Network (VPN) tunnels through the Internet or secure Web site communication via Secure Socket Layer (SSL) protocols, there is an increased demand for protection of tape data to close the gaps of previously unprotected tape data transit to a recovery site or business partner. A major contributor for companies seeking to protect their tape data is that many states have enacted laws that require notification of security breaches involving personal information.

While there have been tape data encryption solutions around for quite some time using *software data encryption* on the host or *external encryption devices*, these non-integrated encryption solutions have the drawbacks of requiring a significant administrative effort for each involved host system and either additional CPU cycles on the host or additional external hardware. Overall these are insular solutions with individual setups and configurations required for each host platform and therewith they put inherent burdens on interchanging encrypted tape cartridges among different systems or partners.

In contrast, tape data encryption done just like data compaction by the tape drive hardware itself provides an integrated and homogenous tape data encryption solution across host platforms.

IBM was first in the industry to offer a *tape drive hardware encryption* solution with the announcement of the IBM enterprise tape TS1120 encryption-capable model 3592-E05 in August 2006.

With the IBM LTO4 TS1040 tape drive announced in April 2007, hardware tape encryption is also available now for Fibre Channel or Serial Attached SCSI (SAS) LTO4 drives. Together with the free of charge *IBM Encryption Key Manager component for the Java Platform* (EKM) software that supports the generation and communication of encryption keys for the encryption enabled IBM tape drives, IBM offers a flexible integrated tape drive encryption solution across the enterprise for diverse operating system environments including z/OS, i5/OS, AIX, HP, Sun, Linux, and Windows.

Three different encryption management methods distinguished by the layer where the encryption policies and keys are managed (see Figure 7-1) are supported for the encryption enabled IBM tape drives: Application-Managed Encryption (AME), System-Managed Encryption (SME) or Library-Managed Encryption (LME).

Note: Library-Managed Encryption is currently the only tape hardware encryption method supported for an i5/OS environment.

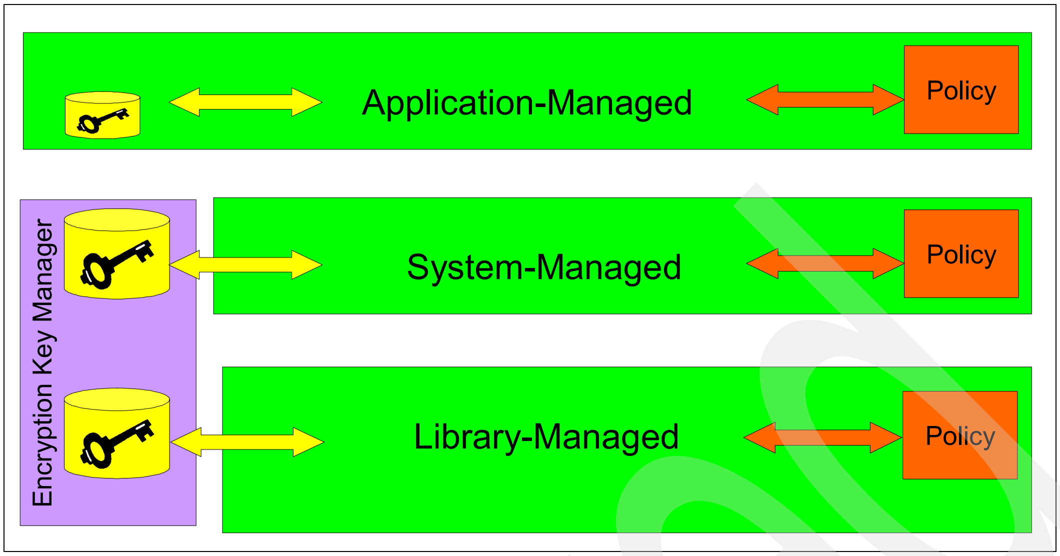


Figure 7-1 Layers for encryption policy and key management

For *Application-Managed Encryption* (AME), the backup application itself manages the policies specifying when encryption is to be used and the encryption keys that are passed through the data path between the application layer and the IBM encryption enabled tape drives. Currently, only IBM Tivoli Storage Manager supports AME with IBM TS1120 drives. For LTO4, as specified by the LTO consortium, ISV backup applications that are supposed to support AME must be compliant with the SCSI T10 SCS-3 standard using the SECURITY PROTOCOL IN/OUT commands to control the decryption and encryption processes.

With *System-Managed Encryption* (SME), which is transparent to any host applications, the encryption policies are either implemented via DFSMS™ in z/OS or for Open Systems on host-level granularity via the IBM tape device driver. Key management in SME is done using the Encryption Key Manager (EKM). SME and LME are transparent to one another meaning that tapes encrypted via LME can be decrypted via SME and vice-versa provided they have access to the same keystore.

Library-Managed Encryption (LME) is the method we focus on in this chapter because it is currently the only tape encryption method supported with i5/OS. Similar to SME it is also transparent to any host application. For this method the encryption enabled tape drives *must* reside within an IBM tape library because the library itself communicates via secure TCP/IP with the EKM server for key management to serve key requests from the drives.

For further information on implementing SME or SME, refer to *IBM System Storage TS1120 Tape Encryption: Planning, Implementation and Usage Guide*, SG24-7320 at:

http://www.redbooks.ibm.com/abstracts/sg247320.html?Open

The EKM is part of the IBM Java runtime environment and uses the IBM Java Security components for its cryptographic capabilities. It supports encryption-enabled IBM tape drives in generating, protecting, storing, and maintaining the encryption keys that are used to encrypt and decrypt data being written and read from tape media. EKM operates on i5/OS, z/OS, AIX, Linux, HP-UX, Sun Solaris and Windows. It is designed to be a shared resource that can be deployed in several locations within a customer enterprise serving numerous encryption-capable tape drives.

Figure 7-2 shows the three main components of the EKM with its configuration file, drive table, and keystore.

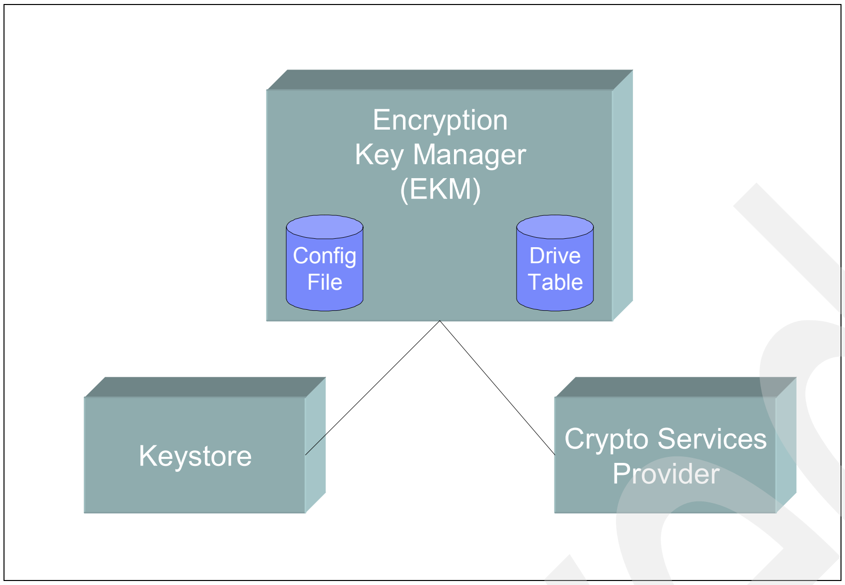


Figure 7-2 Encryption Key Manager components

The EKM *configuration file* allows the user to customize the EKM behavior, for example, with its TCP/IP listener port or with default key settings and holds various location settings for the keystore, drive table, and audit logs (refer to 7.4.2, "Configuring EKM for tape encryption" on page 229).

As the name suggests, the *key store* holds the keys and their digital certificates used for tape encryption, while the *drive table* contains the list of valid tape drives served by EKM.

For further information about the IBM Encryption Key Manager, refer to the *IBM Encryption Key Manager component for the Java platform: Introduction, Planning and User's Guide*, GA76-0418 at:

http://www-1.ibm.com/support/docview.wss?rs=1139&context=STCXRGL&dc=D400&uid=ssg1S4000504

The following two sections show the concepts of TS1120 tape encryption and LTO4 tape encryption, which differ significantly in how the data key used to encrypt and decrypt the data is protected.

7.1.1 Concepts of TS1120 tape encryption

Tape encryption for the IBM enterprise tape drive TS1120 model 3592-E05 is implemented by two classes of encryption algorithms. A *symmetric key algorithm* based on the Advanced Encryption Standard (AES) is employed by EKM to generate a 256-bit random *data key* (DK) utilizing the IBM Java Cryptographic Extension (JCE). This DK is used by the encryption enabled TS1120 Tape Drive for its encryption and decryption of user data. It is protected by a *key encryption key* (KEK), which is a public/private key pair based on a 1024-bit Rivest-Shamir-Adleman (RSA) *asymmetric encryption algorithm* used for encryption/decryption of the DK itself.

EKM determines the KEK it uses from its keystore for a specific DK encryption/decryption request from the associated *key label* or *key alias*, which is defined by one of the following encryption policies:

- A default label for all TS1120 drives in the drive table specified in the EKM configuration file
- A drive specific key label specified with the corresponding drive entry in the EKM drive table
- In the TS3500 or 3494 Tape Library, a cartridge VOLSER range specific key label specified in a *Barcode Encryption Policy* (BCE)

For further information on encryption policies, refer to 7.2.5, “3592 tape encryption policy considerations” on page 210.

Because the encrypted DK is not stored in the EKM keystore but externally in the 3592 tape cartridge memory (CM) and in several additional locations on the tape media, it is referred to as *externally encrypted data key* (EEDK). The two layered encryption method used with TS1120 is shown in Figure 7-3.

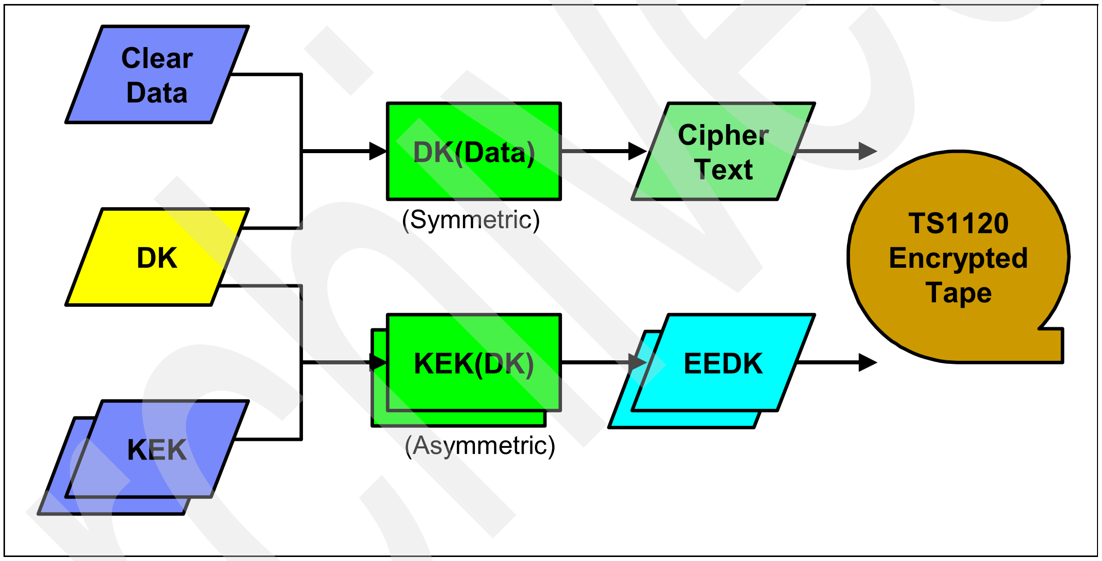


Figure 7-3 TS1120 two-layer encryption using symmetric and asymmetric encryption algorithms

Using a symmetric key for high-volume efficient data encryption/decryption by the drive hardware and a public/private key or asymmetric encryption algorithm for securing the data key provides excellent performance. IBM tests have shown outstanding results with enabled TS1120 tape drive encryption causing less than 1% performance degradation. For more details, see the White Paper, “TS1120/TS3500 Tape Encryption on System i” at:

http://www-03.ibm.com/support/techdocs/atsmastr.nsf/84279f6ed9ffde6f86256ccf00653ad3/fb77227fc78f069d862572500021bcf9?OpenDocument

In addition, this two-layer encryption design reduces key management to maintaining a minimum set of public/private KEKs in the keystore and allows *re-keying* of cartridges by replacing the EEDK without re-writing any user data on the tape (see "Re-keying encrypted 3592 cartridges" on page 255). IBM's implementation of TS1120 enterprise tape drive encryption accounts for two (different) key labels to be associated with a TS1120 tape cartridge that actually stores two EEDKs, EEDK1 and EEDK2, enabling easy exchange of tape cartridges with a partner in B2B relationship by using the partner's certificate as a second key label. For more details on exchanging encrypted tape cartridges with business partners, refer to 7.2.6, "Considerations for sharing tapes with partners" on page 211.

Library-Managed TS1120 Data Encryption process

For data encryption, the IBM tape library contacts EKM with the drive's request for a random symmetric data key (DK) to be generated for encryption of the user data written to the tape cartridge. After the verification that the drive is listed by its serial number in the drive table EKM looks for the associated key labels in its keystore and takes the public part of the asymmetric key encryption keys (KEKs) for encryption of the DK therewith creating the two externally encrypted data keys (EEDKs). EKM sends the DK itself to the drive in a secure manner. The drive uses the DK for its hardware encryption of the user data and stores the EEDKs in the cartridge memory and for redundancy on three other places on the tape media.

Library-Managed TS1120 Data Decryption process

For data decryption, the IBM tape library contacts EKM with the drive's request for decryption of the EEDK. After verification that the drive is listed by its serial number in the drive table EKM looks for the associated key label and gets the private part of the asymmetric key encryption key (KEK) from its keystore for decrypting the EEDK, that is, retrieving back the DK. EKM sends the DK in a secure manner to the drive for its hardware decryption of the encrypted user data.

Note: The TS1120 tape drive remembers the data key used for encryption/decryption of a tape cartridge as long as it is mounted so EKM is not repeatedly contacted and actually not required by the drive for the same mount session.

7.1.2 Concepts of LTO4 tape encryption

For LTO4 tape drive encryption, the same 256-bit AES symmetric key algorithm as for the TS1120 tape drive is used for the data key to encrypt and decrypt user data by the IBM LTO4 drive. However, in contrast to TS1120 tape encryption, for LTO4 there is no asymmetric encryption algorithm used for protecting the DK with a KEK. To achieve protection of the DK for LTO4 only using a single-layer symmetric encryption the DK cannot be randomly generated like for TS1120. Instead LTO4 utilizes *pre-generated data keys* created by the user in the EKM keystore (see "Symmetric Key Generation for LTO4 Encryption" on page 227) with the active symmetric key set to be used by EKM specified in the EKM configuration file as part of the setup before using LTO4 tape encryption.

EKM determines the actual DK to be used for a LTO4 drive encryption request by one of the following encryption policies:

- Selecting the DK in a round-robin manner from the active key set specified in the EKM configuration file (this encryption policy provides neither tape drive nor cartridge level granularity)
- Selecting a cartridge VOLSER range specific DK from a defined *Barcode Encryption Policy* (BCE), which is available with the IBM TS3500 library only since LTO tape drives are not supported in the 3494 Tape Library.

Figure 7-4 shows the single-layer LTO4 symmetric encryption process.S

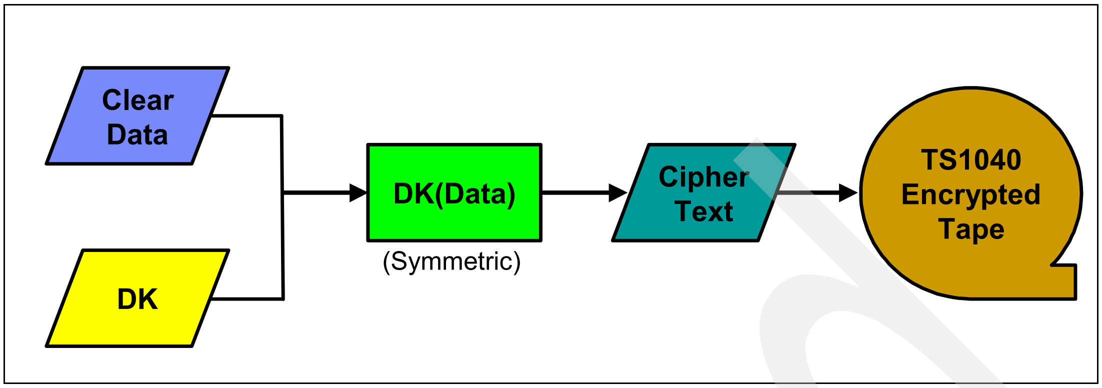


Figure 7-4 Single-layer LTO4 symmetric encryption process

The data key is passed to the drive in a secure manner. The drive uses the key to encrypt the data, but does not store the entire key on the cartridge. To be able to read back encrypted data, the LTO4 drive saves a 12-byte *key identifier* (key ID) provided by EKM in clear text, which maps to the associated DK in the keystore together with each encrypted data record on the tape. During read operations the drive sends a request for the DK for each encountered unique key ID through the library to EKM.

Similar to TS1120 the symmetric encryption/decryption algorithm is very efficient causing less than 1% performance degradation.

The single-layer LTO4 symmetric encryption method supports no re-keying of tape cartridges so if you want encryption by another DK, you have to take extra steps to specify another DK and perform a tape to tape copy of the LTO4 cartridge.

Library-Managed LTO4 Data Encryption process

For data encryption the IBM tape library contacts EKM with the drive's request for a data key (DK) to be provided for encryption of the user data written to the tape cartridge. Depending on the defined encryption policy mentioned above EKM selects the pre-generated data key itself from the active key set or in case of BCE via the optional key label passed on by the library. After verification that the drive is listed by its serial number in the drive table EKM passes the DK together with the key ID to the drive in a secure manner. The drive uses the DK for its hardware encryption of the user data with embedding the key ID in each data record.

Library-Managed LTO4 Data Decryption process

For data decryption the IBM tape library contacts EKM with the drive's request for providing the DK for the key ID it found during its started read operation. After verification that the drive is listed by its serial number in the drive table EKM retrieves the pre-generated DK from its keystore referenced by the key ID. EKM sends the DK wrapped with a session key in a secure manner to the drive for its hardware decryption of the encrypted user data.

Note: Like the TS1120 tape drive, the LTO4 tape drive also remembers the last data key used for encryption/decryption of a tape cartridge as long as it is mounted, so EKM is not repeatedly contacted and actually not required by the drive for the same mount session.

7.2 Planning for tape encryption with i5/OS

The following sections provide planning information about the hardware and software prerequisites for using tape encryption with i5/OS and the IBM TS1120 enterprise tape drive or the IBM TS1040 LTO4 tape drive. We discuss important considerations pertaining to the selection of the EKM keystore, the encryption policies, the EKM setup for disaster recovery, and sharing of tape cartridges with partners. Then we give you an overview of the implementation steps required for tape encryption with i5/OS, which are described in detail in 7.3, “Installing the Encryption Key Manager on i5/OS” on page 213 and 7.4, “Setup and usage of tape encryption with i5/OS” on page 217.

> **Note:** Within this book, we focus on Library-Managed Encryption (LME) with the Encryption Key Manager (EKM) running on i5/OS.
>
> There is no requirement to have EKM installed on i5/OS to use tape encryption for i5/OS because with LME, the EKM can be installed on any supported platform. However, we are convinced that, for System i environments, i5/OS with its high security and reliability is also the preferred choice for installation of the EKM and we have thus included customized information for planning and implementing tape encryption on i5/OS.

7.2.1 Hardware prerequisites

Currently the following IBM tape drives support hardware tape encryption:

- IBM TS1120 Tape Drive (3592-E05, encryption-capable) with FC9592. Earlier 3592-E05 models can be upgraded to be encryption-capable via the chargeable feature FC5592.
- IBM TS1040 LTO4 Fibre Channel or serial-attached SCSI (SAS) Tape Drive

To enable these encryption-capable IBM tape drives for LME, which is required for i5/OS, they must reside in one of the following supported IBM tape libraries:

- TS1120 (3592-E05) supported in:
  - IBM TS3400 library
  - TS3500 library frame models L23 or D23
  - IBM 3494 library frame models L22 or D22
- TS1040 LTO4 supported in:
  - IBM TS3100/TS3200 libraries (AAS orders only) Release 4 or later with Transparent LTO Encryption feature (FC5900)
  - IBM TS3310 library Release 4 or later with:
    - Transparent LTO Encryption feature (FC5900)
    - Encryption Configuration (FC9000)
  - IBM TS3500 library frame models L53 or D53 Release 7A’ or later with:
    - Transparent LTO Encryption feature (FC1604)
    - TS1040 Fibre Channel model 3588-F4A only

The TS1120 minimum drive firmware level to support Library-Managed Encryption is 1942, but it is highly recommended to have the latest PFE recommended level applied.

For the IBM TS3500, the *Advanced Library Management System* (ALMS), FC1690, is recommended to flexibly set encryption methods at a logical library level and to allow intermix of encryption-capable drives with non-encryption-capable drives within a logical library.

Without ALMS, all logical libraries of the same technology (either TS1120/3952 or LTO) must be set to the same encryption mode, which has the following implications:

- Encryption-capable drives added to a non-ALMS library with older non-encryption-capable drives cannot be encryption-enabled.
- Older, non-encryption-capable drives added to a non-ALMS encryption library are set to “restricted mode” not being available for use.

7.2.2 Software prerequisites

For using tape encryption with the EKM installed on i5/OS, the following software prerequisites have to be met:

- i5/OS V5R3 or later
- 5722-AC3: Crypto Access Provider 128-bit (V5R3 only)
- 5722-DG1: IBM HTTP Server for i5/OS (TS1120 tape encryption with IBMi5OSKeyStore only)
- 5722-SS1 option 34: Digital Certificate Manager (TS1120 tape encryption with IBMi5OSKeyStore only)

> **Note:** The i5/OS Digital Certificate Manager is used to administer an *IBMi5OSKeyStore* for TS1120 tape encryption and does not support symmetric keys required for LTO4 tape encryption.

- 5722-JV1 *BASE and option 7, “Java Developer Kit 1.5” (V5R3 only)
- 5722-JV1 *BASE and option 8 “J2SE™ 5.0 32 bit” (V5R4 only)
- Latest Java Group PTF (SF99269 for V5R3, SF99291 for V5R4)
- 5722-JV1 PTF SI26811 providing IBM Java 5.0 Service Release 4 containing the EKM Release 1 code (V5R4 only)
- 5722-SS1 PTF SI25094 providing the EKM default configuration file and strEKM script (V5R4 only)
- 5722-SS1 PTF SI26705 providing the IBM EKM Release 1 code, default configuration file and strEKM script (V5R3 only)
- 5722-BR1 PTF SI24934 providing a new media density FMT3592A2E for BRMS to help identify encrypted tape cartridges (V5R4 only)
- 5722-BR1 PTF SI24933 providing a new media density FMT3592A2E for BRMS to help identify encrypted tape cartridges (V5R3 only)

> **Note:** Library-Managed Encryption for LTO4 tape drives requires the EKM Release 2 code and IBM Java 5.0 Service Release 5, which adds support for handling symmetric data keys.

EKM Release 2 code (build 20070503) is planned to be released for i5/OS with IBM Java 5.0 Service Release 5, including the new IBM Java keytool required for the support of generating and storing symmetric keys, to be made available as a 5722-JV1 PTF for i5/OS.

For downloading a more recent version of the EKM code, refer to the IBM support Web site at:

http://www-1.ibm.com/support/docview.wss?rs=1139&context=STCXRGL&dc=D400&uid=ssg1S4000504

7.2.3 Disaster recovery considerations

The main reason to have more than one EKM server is that, if this single EKM server fails, there is no possibility to read from or write to encrypted tapes before having recovered the failed EKM server.

Note: For availability reasons, we recommend that you set up two redundant EKM servers on different host systems, ideally at different locations.

Another reason for setting up a secondary EKM server is that an EKM server, which was started in a batch job currently, cannot be dynamically reconfigured using the EKM admin console. Figure 7-5 shows a redundant setup with two EKM servers. If one EKM server fails, the IBM tape library that has been configured with two redundant EKM paths (EKM server TCP/IP addresses) automatically attempts to failover to the second EKM server for retrieving the data keys required for encryption and decryption of the tape cartridges. With two redundant EKM servers, it is required that their keystore, configuration file, and drive table are synchronized. You can define parameters in the EKM configuration to have this done automatically at regular intervals.

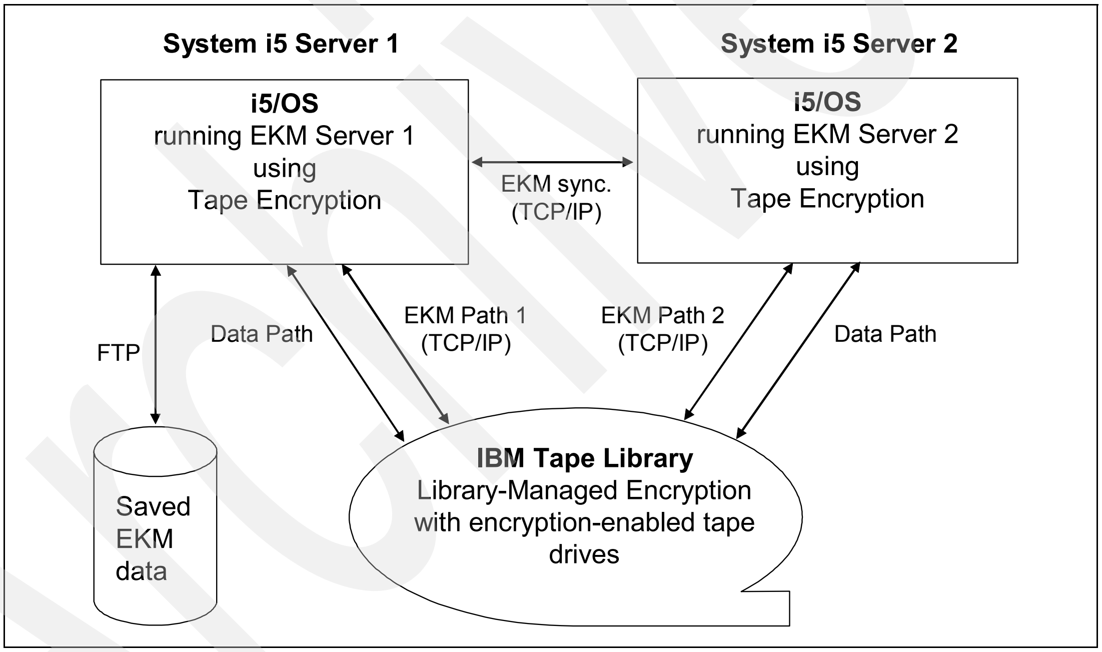


Figure 7-5 Redundant EKM server configuration using two different systems

For further details on setting up a secondary EKM server and synchronizing EKM servers, refer to "New installation of a secondary EKM server" on page 215.

Important: Taking regular *unencrypted* backups of the EKM keystore *.KDB file, drivetable, and configuration file *KeyManagerConfig.properties*, for example, via prior FTP transfer to another system, is crucial for restoring a working EKM server configuration after a disaster before being able to regain access to the encrypted tape data.

If EKM server availability and recovery time is not an issue, and if a single EKM server configuration is desired, install the EKM server on another LPAR or, even better, on another system than the one being taken system backups from with tape encryption. Otherwise, in case of a disaster, there is no possibility to quickly perform a system restore from the encrypted tapes without a lengthy and error prone configuration of a new EKM server from unencrypted saved EKM data.

For this reason, the distributed EKM server configuration shown in Figure 7-6 is the only *single* EKM server configuration supported by IBM System i development.

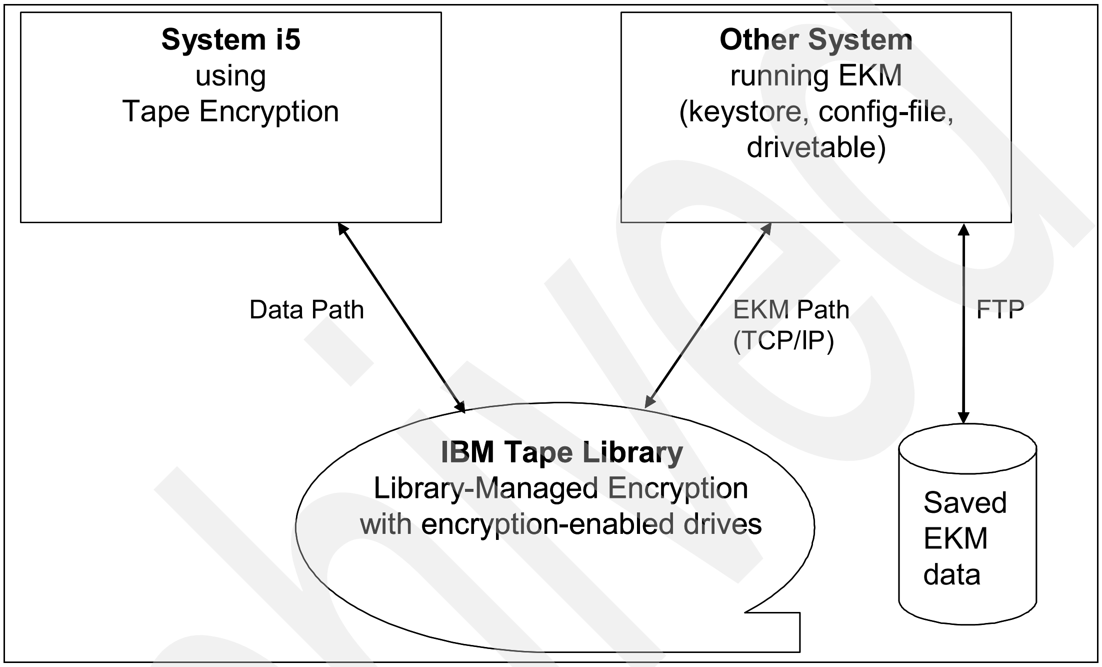


Figure 7-6 Single distributed EKM server configuration

7.2.4 EKM keystore considerations

For installing the EKM on i5/OS, there are two types of keystores supported. These are either an IBMi5OSKeyStore keystore managed through i5/OS Digital Certificate Manager, which is i5/OS specific and supports no storage of symmetric keys so that it can be used for 3592 tape encryption only, or a JCEKS keystore being supported on all platforms and supporting both LTO4 encryption with storage of symmetric keys and TS1120 tape encryption with storage of asymmetric keys.

We recommend using the IBMi5OSKeyStore only for TS1120 tape encryption environments where no LTO4 encryption is being used, and EKM, both a primary and optional secondary EKM server for high availability, is installed on i5/OS only.

In all other situations, a JCEKS keystore is either required when LTO4 encryption is being used, or is highly recommended when the EKM primary and secondary server reside on different platforms to ease synchronization of both EKM servers. For information about automatic synchronization between two EKM servers, refer to “New installation of a secondary EKM server” on page 215.

> **Note:** Each EKM server only supports *one* keystore, so a decision for using either an *IBMi5OSKeyStore* or *JCEKS* keystore is required.

Table 7-1shows a comparison between the supported features of a JCEKS and IBMi5OSKeyStore.

Table 7-1 Comparison between the IBMi5OSKeyStore and JCEKS keystore

Supported feature	IBMi5OSKeyStore	JCEKS
3592 (asymmetric keys)	Yes	Yes
LTO4 (symmetric keys)	no	Yes
Supported platforms	i5/OS only	All
Graphical User Interface	Yes	no

7.2.5 3592 tape encryption policy considerations

There are three different methods of defining encryption policies to determine which encryption keys from the EKM keystore referenced by key labels/aliases are used for 3592 tape encryption. These methods in ascending order of their priority being used by EKM are:

- Default global key aliases defined in the EKM configuration file
- Default drive key aliases defined in the EKM drivetable
- Barcode Encryption Policies defined in the TS3500 or IBM 3494 Tape Library

Default global key aliases are defined in the EKM configuration file via the parameters *drive.default.alias1* and *drive.default.alias2*, which can be set to the default key labels to be used for the EEDK1 and EEDK2. Defining default global key aliases is recommended when using the parameter setting *drive.acceptUnknownDrives = true* to make sure certificates for generating or decrypting the EEDK1 and EEDK2 are associated with new drives automatically added to the drivetable. For implementing default global key aliases, refer to “Customizing the EKM configuration file” on page 230.

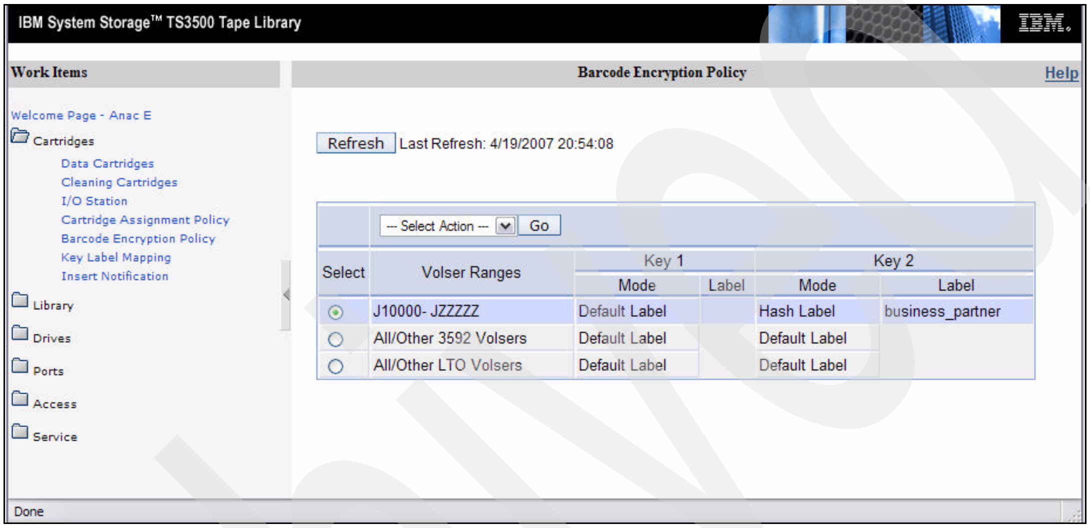
Default drive key aliases are used to associate certificates with 3592 drive serial numbers. They are defined by using the *rec1* and *rec2* parameters when manually creating or modifying an entry in the EKM drive table using the EKM admin console commands **adddrive** and **moddrive**. Defining default drive key aliases is useful if different (logical) tape libraries communicating to the same EKM server should use different encryption keys, for example, because only a subset of libraries is used for sharing tape cartridges with business partners. For reference information about the EKM admin console commands, refer to *IBM Encryption Key Manager component for the Java platform: Introduction, Planning, and User’s Guide*, GA76-0418.

Barcode Encryption Policies (BCE) are supported with the IBM System Storage TS3500 Tape Library and in the IBM TotalStorage 3494 Tape Library only. They are used to specify which VOLSER ranges are to be encrypted (and which not) and which certificates referred to by the specified key labels are to be used for the encryption process. A *key mode* specified for the two key labels determines the method by which EKM identifies the public/private keys to be used for generating/decrypting the EEDKs. Choices for key mode are either:

- *Default Label*, meaning that the key label, default drive key alias, or default global key alias, configured at the encryption key manager is used
- *Clear Label*, meaning that the key is referenced by the specified key label
- *Hash Label*, meaning that the key is referenced by a computed value from the public key that is referenced by the specified key label

Using a hash label is especially useful for sharing tapes with a business partner, because the certificate can be imported into the key store with another label than the one it was exported with, so that both partners do not have to agree on a common key label to be used. For further information about sharing tape cartridges, refer to “Considerations for sharing tapes with partners” on page 211.

Figure 7-7 shows an example from the IBM System Storage TS3500 Tape Library’s IBM UltraScalable Specialist **Cartridges** → **Barcode Encryption Policy** view with a user-defined BCE for the VOLSER range J10000-JZZZZZ using a hash label to refer to the public key certificate *business_partner* from the business partner.



Last Refresh: 4/19/2007 20:54:08

Select	Volser Ranges	Key 1		Key 2	
		Mode	Label	Mode	Label
●	J10000- JZZZZZ	Default Label		Hash Label	business_partner
○	All/Other 3592 Volsers	Default Label		Default Label	
○	All/Other LTO Volsers	Default Label		Default Label	

Figure 7-7 IBM UltraScalable Specialist: TS3500 Tape Library Barcode Encryption Policy screen

7.2.6 Considerations for sharing tapes with partners

Different approaches apply for sharing encrypted 3592 tape cartridges and encrypted LTO4 tape cartridges with partners, which we discuss in the following sections.

Sharing encrypted 3592 tape cartridges

To share encrypted 3592 cartridges with partners, for security reasons we do not recommend to provide them with the private part of the KEK for decryption. A *private key,* as the name suggests, is intended to be safely kept and should never be provided to others. Giving away the private key can be a security risk because anyone else getting access to your private key would be able to read your encrypted tape data.

> **Note:** The recommended way for sharing encrypted 3592 tapes with partners is to import your partner's certificate including only the *public key* but not the private key into your EKM keystore.

On i5/OS with DCM or on other platforms with the IBM Key Management tool as part of the IBM Java RTE, the digital certificate used for tape encryption can be exported into a file, which can then be imported into a partner’s EKM keystore. However, care has to be taken that not the full certificate that holds the public and corresponding private key is exported, but only the public key part of the certificate. In 7.4.4, “Importing and exporting of encryption keys” on page 242, we describe the detailed procedures to export and import private/public key certificates as PKCS12 binary files and public key only certificates as *Base64_encoded* text files.

Two sets of keys can be stored on a 3592 tape cartridge, so you can specify your partner's public key certificate as the second key label. Depending on your encryption policy, you specify it either in your EKM configuration file if using default key labels, in the drive table entries, or in your Barcode Encryption Policy defined on the TS3500 or 3494 library. In this way, you enable only your selected partner who owns the corresponding private key to read your 3592 cartridges newly written with encryption from beginning of tape (BOT).

Note: Existing encrypted 3592 tape cartridges continue to use their EEDK1 and EEDK2 originally stored with the first write on the cartridge even if the EKM encryption policy is changed.

To share already encrypted 3592 cartridges with existing data, they can be *re-keyed* via the IBM Tape Library Specialist Web GUI as described in "Re-keying encrypted 3592 cartridges" on page 255.

To export certificates for redundancy or disaster recovery from an i5/OS keystore to an EKM keystore on a platform other than i5/OS, consider that the i5/OS DCM exports certificates in the PKCS 12 version 3 file format. Therefore, the target keystore must support the same format, or the exported certificate file has to be converted, for example, by using the OpenSSL open-source utility.

Sharing encrypted LTO4 tape cartridges

The single-layer symmetric encryption algorithm used for LTO4 tape drive encryption limits the possibilities for sharing encrypted LTO4 cartridges.

You can always provide the partner the symmetric key certificate that was used for a specific encrypted LTO4 cartridge. The EKM audit metadata XML file specified in the EKM configuration file provides the information about which symmetric key was used for a specific cartridge volume serial number (see "Example of the EKM audit metadata XML file" on page 256).

However, sharing your symmetric data key implies the security risk that anyone else getting hold of it would be able to read your LTO4 cartridges that were encrypted with this same data key. It is possible to create a set of symmetric keys in the EKM keystore to be used across the pool of LTO4 cartridges. However, this rather serves for increased security than for sharing cartridges with partners, because there is no control over which key alias from this set is used for a specific LTO4 cartridge serial number.

With the IBM TS3500 Tape Library, a feasible work-around to prevent sharing your own symmetric data keys might be, to define a dedicated data key within a Barcode Encryption Policy for a LTO4 cartridge serial number range to be shared with the partner. Then you use a tool to send the symmetric key to your partner using asymmetric keys. The partner sends the certificate and public key to you, and you use the public key to encrypt the symmetric data key.

7.2.7 Implementation prerequisites

Before starting with the implementation steps described in detail in 7.3, "Installing the Encryption Key Manager on i5/OS" on page 213 and 7.4, "Setup and usage of tape encryption with i5/OS" on page 217, make sure that the following conditions are true:

- All hardware and software prerequisites described in 7.2.1, "Hardware prerequisites" on page 206 and 7.2.2, "Software prerequisites" on page 207 are met.

- You have elaborated the EKM backup and disaster recovery concept (see 7.2.3, “Disaster recovery considerations” on page 208).
- You have decided on the type of EKM keystore to be used (see 7.2.4, “EKM keystore considerations” on page 209).
- You have determined the encryption policies to be used (see 7.2.5, “3592 tape encryption policy considerations” on page 210), and the key/certificate requirements, especially for sharing cartridges (see 7.2.6, “Considerations for sharing tapes with partners” on page 211).

To implement tape encryption with i5/OS, the following steps are required:

- Install a primary or single EKM server on i5/OS.
- Create an EKM keystore and encryption keys.
- Configure EKM for 3592 or/and LTO4 tape encryption.
- Configure the IBM tape library for Library-Managed Encryption.
- Back up the EKM data (keystore, configuration, and drivetable files).
- Optionally install a secondary EKM server on another i5/OS system.

See the remainder of this chapter for a detailed description of the implementation steps.

7.3 Installing the Encryption Key Manager on i5/OS

Refer to the corresponding section to either newly install the EKM on i5/OS as a primary or secondary EKM server, or to upgrade an installed EKM release to a newer service release.

7.3.1 New installation of the Encryption Key Manager

Follow the steps in “New installation of a primary EKM server” next for a new installation of the EKM as a *primary* or *single* EKM server on an i5/OS server. Then refer to “New installation of a secondary EKM server” on page 215 for setting up a secondary EKM server on an i5/OS system.

New installation of a primary EKM server

Follow these steps:

1. Make sure to have all software prerequisites for either i5/OS V5R3 or V5R4 installed.
2. Install the unrestricted JCE policy files ‘‘local_policy.jar” and “US_export_policy.jar” version 1.4.2, which can be downloaded from the IBM Web site:

   `https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk`

   Install these to the following IFS directories:

   – For V5R,4 to:

     /QOpenSys/QIBM/ProdData/JavaVM/jdk50/32bit/jre/lib/security/

   – For V5R3, to:

     /QIBM/ProdData/Java400/jdk15/lib/security/

   > **Note:** Make to sure to replace the existing policy files with the unrestricted ones downloaded from above. The unrestricted JCE policy files version 1.4.2 are the same for Java version 1.4.2 and 1.5 and 5.0.

3. Edit the “java.security” file to include the following providers if they are not already included:

   - `security.provider.6=com.ibm.jsse2.IBMJSSEProvider2`
   - `security.provider.7=com.ibm.i5os.jsse.JSSEProvider`

   Note: The unique number to be used for adding the foregoing security providers depends on which ones are already specified in your “java.security” file.

   The “java.security” file is located in the following IFS directory:

   - For V5R4, in:

     /QOpenSys/QIBM/ProdData/JavaVM/jdk50/32bit/jre/lib/security/

   - For V5R3, in:

     /QIBM/ProdData/Java400/jdk15/lib/security/

4. Create an IFS directory for EKM holding the EKM keystore, configuration file, drivetable, and so on, with a subdirectory for the EKM auditlogs using the i5/OS commands:

   ```
   CRTDIR DIR('/EKM')
   ```

   ```
   CRTDIR DIR('/EKM/auditlogs')
   ```

5. Copy the default EKM configuration file to this created EKM directory to make sure it is not overwritten by an i5/OS Java software update by using the command:

   ```
   CPY OBJ('/QIBM/ProdData/OS400/Java400/ext/KeyManagerConfig.properties')
   TODIR('/EKM')
   ```

6. Proceed to “Creating an EKM keystore and certificate” on page 217 to create a keystore and corresponding certificates for EKM on i5/OS.
7. Complete the EKM configuration for 3592 tape encryption or/and LTO4 tape encryption described in “Configuring EKM for tape encryption” on page 229.
8. Set up the Encryption Key Manager address in the IBM TS3xxx or 3494 library and enable Library-Managed Encryption referring to “Configuring the IBM TS3500 Library for Library-Managed Encryption” on page 232.
9. After having completed the EKM configuration, submit the EKM server as a batch job by using the command:

   ```
   SBMJOB CMD(QSH CMD('strEKM -server -propfile /EKM/KeyManagerConfig.properties
   1> /EKM/stdout.log 2> /EKM/stderr.log')) JOB(EKMBCH) JOBQ(QSYS/QUSRNOMAX)
   ```

   The *strEKM* script on i5/OS in /usr/bin explicitly refers to the correct Java version for starting the EKM server, so there is no further specification required if multiple Java versions are installed on i5/OS.

   Note: We recommend that you add an autostart job entry for the subsystem that the EKM server should be running in, to guarantee that it is automatically started when the corresponding subsystem gets started, for example, after IPL. To accomplish this, create a job description for the EKM server job and add an autostart job entry to your subsystem by using this job description, as follows:

   ```
   CRTJOBD JOBD(library/EKMJOBD) JOBQ(QSYS/QUSRNOMAX) USER(userid)
   RQSDTA('STRQSH CMD(''strEKM -server -propfile
   /EKM/KeyManagerConfig.properties 1> /EKM/stdout.log 2> /EKM/stderr.log'')')
   ```

   ```
   ADDAJE SBSD(library/subsystem) JOB(EKMBCH) JOBD(library/EKMJOBD)
   ```

10. Back up the EKM keystore, EKM configuration file, drivetable, and auditlogs without using encrypted saves, for example, via prior transfer to a system not using tape encryption for backup.

New installation of a secondary EKM server

For optional installation and setup of a *secondary* EKM server on another i5/OS system, perform these steps:

1. Follow steps 1 to 4 of "New installation of a primary EKM server" on page 213 for the installation of the *secondary* EKM server.
2. When using solely LTO4 tape encryption, ensure a public/private key certificate exists in the EKM server's JCEKS keystore for SSL communication used for synchronization with the secondary EKM server. Refer to "Creating a JCEKS keystore and certificate" on page 227 for listing the certificates in a JCEKS keystore and creating a public/private key if required.
3. Copy the keystore file like `EKM.KDB` or `EKM.JCK`, the configuration file `KeyManagerConfig.properties` and the `drivetable` file from your primary EKM server IFS directory (for example, `/EKM`) to the same directory on your i5/OS system with the secondary EKM server, for example, via using the iSeries Navigator or FTP transfer.
4. On your i5/OS system used for the *secondary* EKM server, start the EKM server as a batch job, referring to step 9 in "New installation of a primary EKM server" on page 213.
5. Refer to "Setting up Encryption Key Manager addresses" on page 233 to set up the secondary EKM server IP address in the tape library.
6. On your i5/OS system used for the *primary* EKM server, end the EKM batch job (refer to step 1 in "Upgrading the Encryption Key Manager" on page 216), and start the EKM admin console from QShell by running the command:

   ```
   strEKM -propfile /EKM/KeyManagerConfig.properties
   ```

   > **Note:** *Currently* the EKM admin console knows nothing about the EKM server started as a batch job, so for any configuration changes to an EKM server started in a batch job, this batch job must be ended prior to the changes. Otherwise, the configuration changes would be lost when the batch job is ended and the EKM server writes its current configuration from memory to its file.

7. Use the following commands from the *primary* EKM server's admin console to set up automatic synchronization between the primary and secondary EKM server:

   ```
   modconfig -set -property sync.ipaddr -value 192.168.202.6:443
   modconfig -set -property sync.type -value all
   modconfig -set -property sync.timeinhours -value 24
   ```

   This example sets up automatic synchronization between the primary EKM server and the secondary EKM server, which has the IP address 192.168.202.6 using the EKM default SSL port 443 – as specified in the EKM configuration file `TransportListener.ssl.port` parameter. The specified `sync.type` parameter value of *`all`* means that the EKM configuration file, which is rewritten from the primary to the secondary server, *and* the EKM drivetable, which is merged by sending new updates from the primary to the secondary server, are synchronized. Synchronization is started every 24 hours as specified by the `sync.timeinhours` parameter value of "*24*".

   You can verify your changes in the EKM configuration by running the **`listconfig`** command.

For further information about synchronization of the EKM server, refer to *IBM Encryption Key Manager component for the Java platform: Introduction, Planning and User's Guide*, GA76-0418.

> **Note:** The EKM admin console **sync** command, for example, `sync -all -ipaddr 192.168.202.6:443` command can be used to manually synchronize or test the synchronization between the primary and secondary EKM server however it requires the primary EKM server to be started interactively.

8. Exit from the *primary* EKM admin console using the command **`exit`**.
9. Start the *primary* EKM server as a batch job again referring to step 9 above.

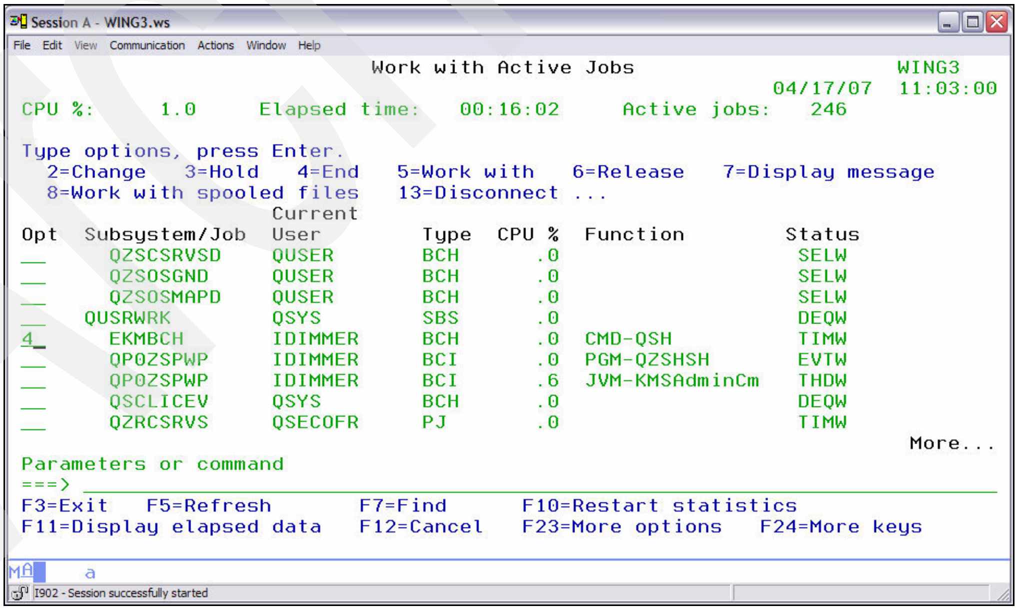
7.3.2 Upgrading the Encryption Key Manager

EKM Release 2 is the official IBM service path for EKM Release 1, so no new EKM Release 1 maintenance releases are made available. Use the following procedure to upgrade an existing EKM installation on i5/OS to a newer EKM service release:

1. Shut down the EKM server as follows:

   – If the EKM server was started as a batch job, use the i5/OS command **`WRKACTJOB`** to locate the EKM batch job, which usually runs in the `QUSRWRK` subsystem and end it either using the option **4** as shown in Figure 7-8 or using the **`ENDJOB JOB(EKMBCH)`** command.

   > **Note:** Do not use the ***IMMED** option for ending the EKM batch job immediately, because this prevents a proper shutdown of EKM without updating its configuration file, drive table, and XML metadata file.



```
                         Work with Active Jobs                     WING3
                                                          04/17/07  11:03:00
CPU %:      1.0     Elapsed time:    00:16:02     Active jobs:    246

Type options, press Enter.
  2=Change    3=Hold    4=End    5=Work with    6=Release    7=Display message
  8=Work with spooled files    13=Disconnect ...
                     Current
Opt  Subsystem/Job   User         Type  CPU %  Function         Status
___    QZSCSRVSD     QUSER        BCH      .0                     SELW
___    QZSOSGND      QUSER        BCH      .0                     SELW
___    QZSOSMAPD     QUSER        BCH      .0                     SELW
___  QUSRWRK         QSYS         SBS      .0                     DEQW
4_     EKMBCH        IDIMMER      BCH      .0  CMD-QSH            TIMW
___    QP0ZSPWP      IDIMMER      BCI      .0  PGM-QZSHSH         EVTW
___    QP0ZSPWP      IDIMMER      BCI      .6  JVM-KMSAdminCm     THDW
___    QSCLICEV      QSYS         BCH      .0                     DEQW
___    QZRCSRVS      QSECOFR      PJ       .0                     TIMW
                                                                       More...
Parameters or command
===> _________________________________________________________________________
F3=Exit   F5=Refresh       F7=Find      F10=Restart statistics
F11=Display elapsed data   F12=Cancel   F23=More options   F24=More keys

MA      a
I902 - Session successfully started
```

Figure 7-8 i5/OS WRKACTJOB screen showing the EKM batch job

   – If the EKM server was started interactively, run the command **`exit`** from the EKM admin console in i5/OS Qshell to stop the EKM server *and* exit from the EKM admin console.

2. Update the EKM code to the new release by replacing the following *IBMKeyManagementServer.jar* Java extension file with its newer version:

   – For i5/OS V5R4:

   ```
   /QOpenSys/QIBM/ProdData/JavaVM/jdk50/32bit/jre/lib/ext/IBMKeyManagementServe
   r.jar
   ```

   – For i5/OS V5R3:

   ```
   /QIBM/ProdData/OS400/Java400/ext/IBMKeyManagementServer.jar
   ```

   Note: Ensure that you *delete* or *overwrite* the old `IBMKeyManagementServer.jar` version. *Do not* rename the file from the old version, because Java would still find its class information from the old renamed file and the new EKM code would not be used.

3. If upgrading from EKM Release 1 to a newer release add the required `Audit.metadata.file.name` parameter to the EKM configuration file, referring to step 2 in “Customizing the EKM configuration file” on page 230.

4. If *newly* using LTO4 tape drive encryption after this EKM upgrade:

   a. Ensure that the required IBM Java 5.0 Service Release 5 is installed with the enhanced *keytool* for support of symmetric key management (refer to 7.2.2, “Software prerequisites” on page 207).

   b. Generate the required symmetric keys in a JCEKS type EKM keystore, referring to “Symmetric Key Generation for LTO4 Encryption” on page 227.

   c. Add the `symmetricKeySet` parameter to the EKM configuration file and make sure that the keystore file, its type, password and provider are adjusted if migrating from an IBMi5OSKeyStore to a JCEKS keystore for LTO4 tape encryption, referring to steps 8, 3, and 4 in “Customizing the EKM configuration file” on page 230.

5. Verify that the upgraded EKM server starts without errors by first starting/stopping it interactively from i5/OS Qshell using the following commands and check that the reported build level matches the new version:

   ```
   strEKM -propfile /EKM/KeyManagerConfig.properties
   startekm
   exit
   ```

6. Finally, start the newly upgraded EKM server as a batch job using the command:

   ```
   SBMJOB CMD(QSH CMD('strEKM -server -propfile /EKM/KeyManagerConfig.properties
   1> /EKM/stdout.log 2> /EKM/stderr.log')) JOB(EKMBCH) JOBQ(QSYS/QUSRNOMAX)
   ```

7.4 Setup and usage of tape encryption with i5/OS

In this chapter, we describe the EKM configuration and setup of Library-Managed Encryption in the IBM tape library for 3592 tape encryption or/and LTO4 tape encryption. We assume that the EKM has already been installed as described before.

7.4.1 Creating an EKM keystore and certificate

Refer to the planning sections in 7.2.4, “EKM keystore considerations” on page 209 for deciding on the type of the required keystore to be used for EKM on i5/OS before going to the corresponding sections below to create an EKM keystore.

To create an *IBMi5OSKeyStore*:

- Refer to “Creating an IBMi5OSKeyStore keystore and certificate” on page 218,

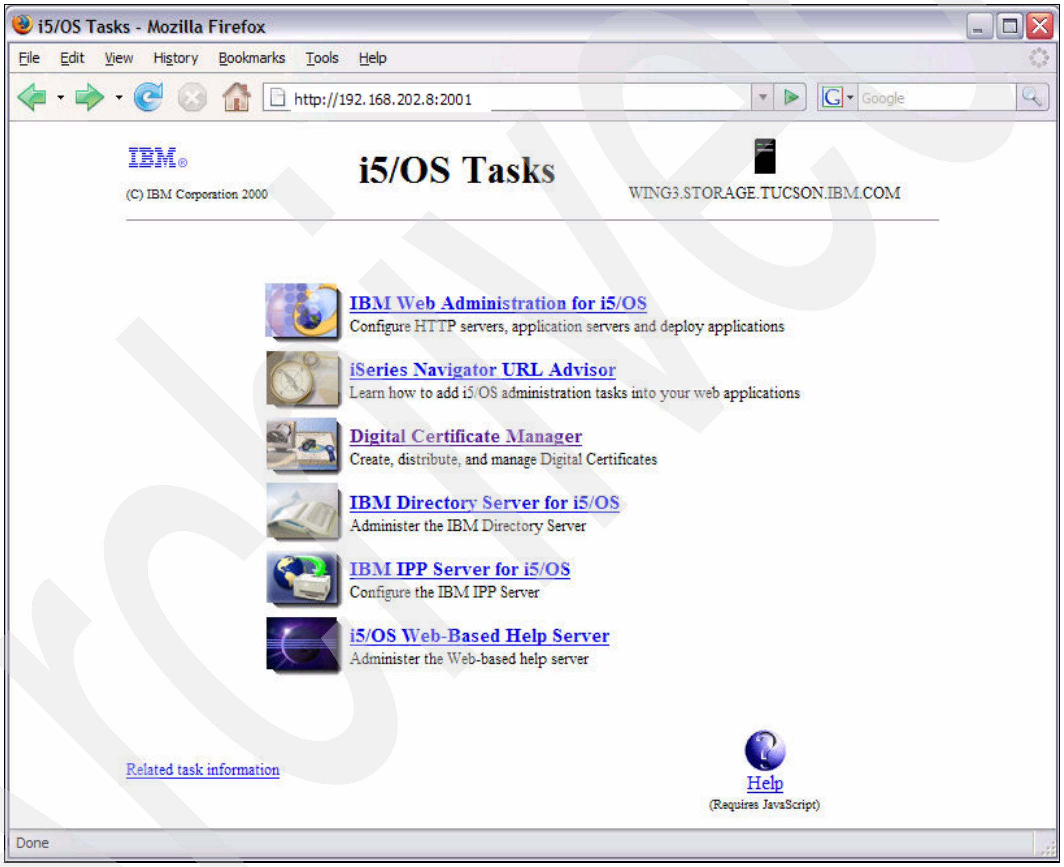
To create a *JCEKS* keystore:

- Refer to “Creating a JCEKS keystore and certificate” on page 227

Creating an IBMi5OSKeyStore keystore and certificate

Follow these steps:

1. Use a Web browser to connect to the i5/OS HTTP admin server at the URL `http://ipaddress:2001` and click on **Digital Certificate Manager** as shown in Figure 7-9 to access the i5/OS Digital Certificate Manager used for creating and managing an IBMi5OSKeyStore.


i5/OS Tasks - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.202.8:2001
Google
IBM
(C) IBM Corporation 2000
i5/OS Tasks
WING3.STORAGE.TUCSON.IBM.COM
Related task information
Help
(Requires JavaScript)
Done

IBM Web Administration for i5/OS
Configure HTTP servers, application servers and deploy applications

iSeries Navigator URL Advisor
Learn how to add i5/OS administration tasks into your web applications

Digital Certificate Manager
Create, distribute, and manage Digital Certificates

IBM Directory Server for i5/OS
Administer the IBM Directory Server

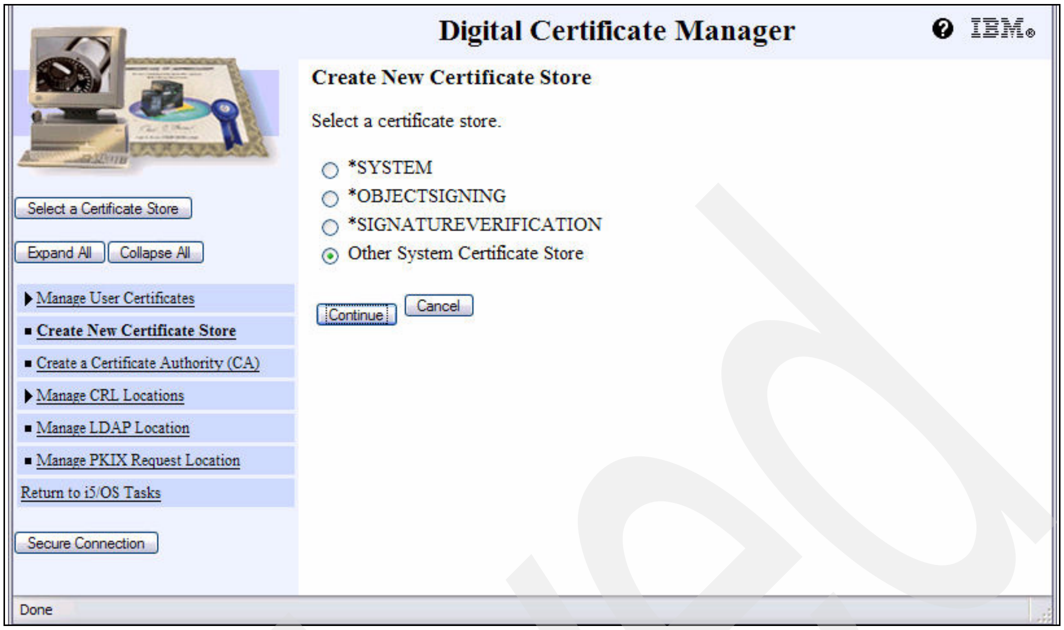
IBM IPP Server for i5/OS
Configure the IBM IPP Server

i5/OS Web-Based Help Server
Administer the Web-based help server

Figure 7-9 HTTP admin server i5/OS Tasks entry screen

> **Note:** When experiencing connection problems from the Web browser to the i5/OS HTTP admin server, use **`WRKACTJOB`** on i5/OS to check that the HTTP admin server QHTTPSVR/ADMIN is running, if not start it by entering the command **`STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)`**

2. Select **Create New Certificate Store** with choosing the option **Other System Certificate Store** as shown in Figure 7-10.


Digital Certificate Manager
IBM.
Select a Certificate Store
Expand All
Collapse All
Manage User Certificates
Create New Certificate Store
Create a Certificate Authority (CA)
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection
Done

Create New Certificate Store

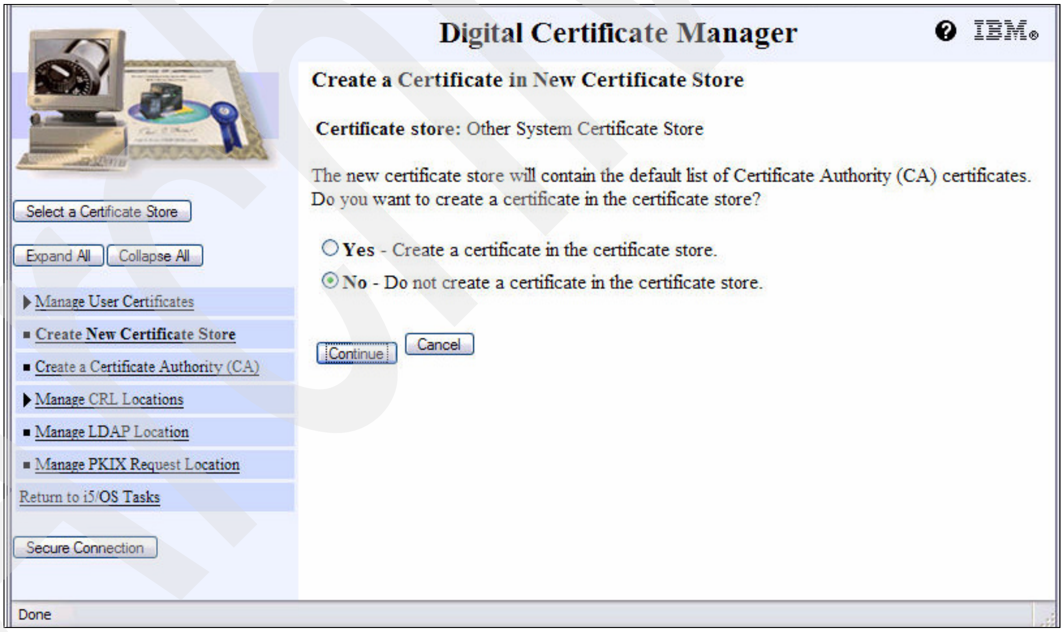
Select a certificate store.

○ *SYSTEM
○ *OBJECTSIGNING
○ *SIGNATUREVERIFICATION
● Other System Certificate Store

Continue | Cancel

Figure 7-10 DCM Create New Certificate Store screen

3. After clicking **Continue**, select the option **No - Do not create a certificate in the certificate store** as shown in Figure 7-11:


Digital Certificate Manager
IBM.
Select a Certificate Store
Expand All
Collapse All
Manage User Certificates
Create New Certificate Store
Create a Certificate Authority (CA)
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection
Done

Create a Certificate in New Certificate Store

Certificate store: Other System Certificate Store

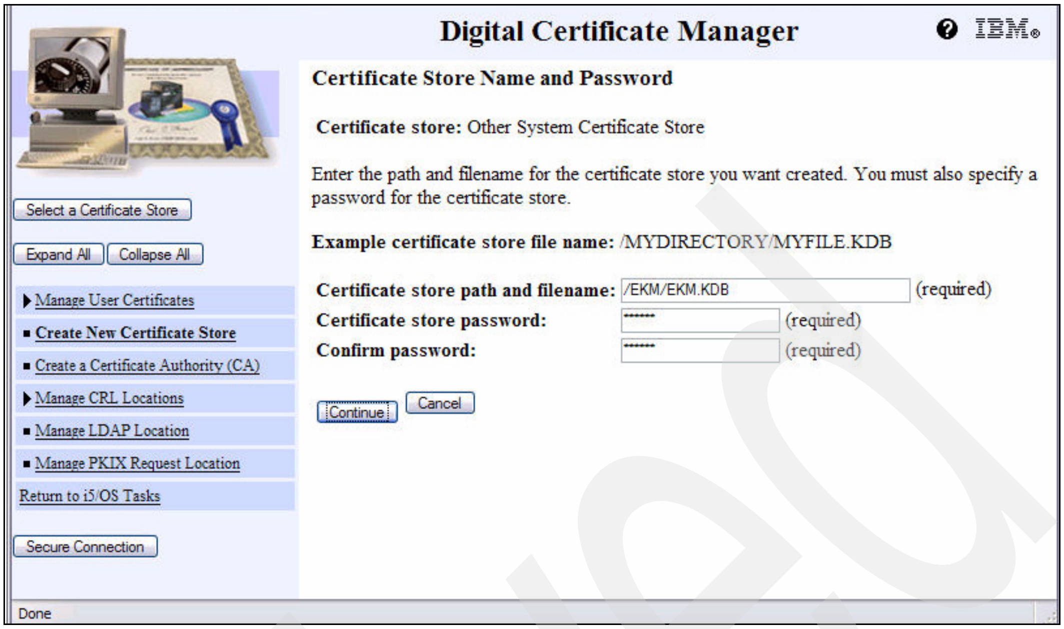
The new certificate store will contain the default list of Certificate Authority (CA) certificates. Do you want to create a certificate in the certificate store?

○ **Yes** - Create a certificate in the certificate store.
● **No** - Do not create a certificate in the certificate store.

Continue | Cancel

Figure 7-11 DCM Create a Certificate in New Certificate Store

4. After clicking **Continue**, enter the **Certificate store path and filename**, for example, `/EKM/EKM.KDB`, making sure to use the path for the IFS directory created for EKM before in 7.3.1, “New installation of the Encryption Key Manager” on page 213, step 4, and specify a **Certificate store password** – both are required later for configuring EKM – as shown in Figure 7-12.



Certificate Store Name and Password

Certificate store: Other System Certificate Store

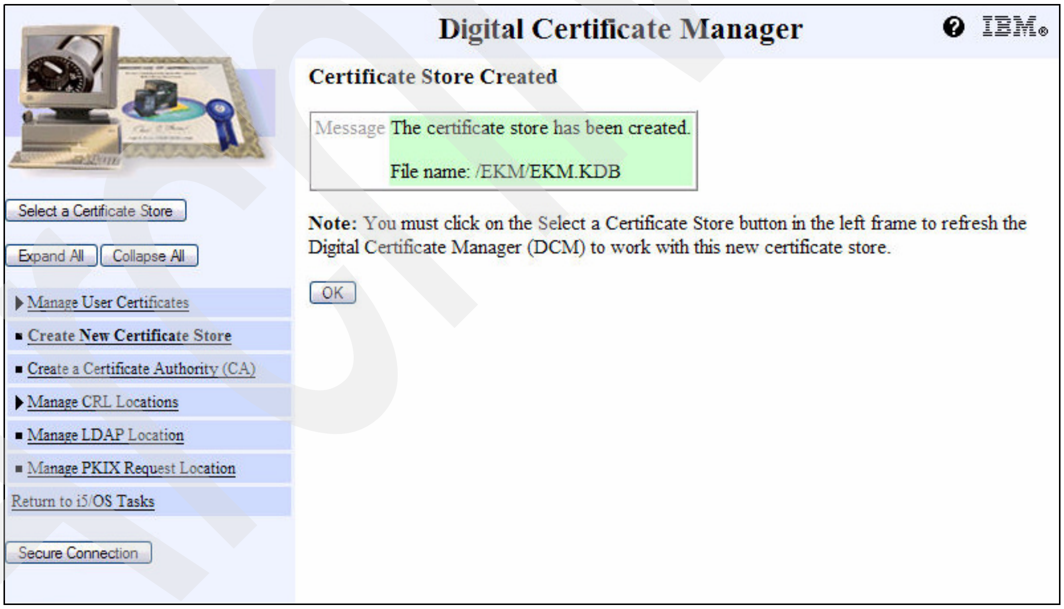
Enter the path and filename for the certificate store you want created. You must also specify a password for the certificate store.

Example certificate store file name: /MYDIRECTORY/MYFILE.KDB

Certificate store path and filename: /EKM/EKM.KDB (required)
Certificate store password: ******* (required)
Confirm password: ******* (required)

Figure 7-12 DCM Certificate Store Name and Password screen

5. After clicking **Continue**, the successful creation of the certificate store is indicated by the message, `The certificate store has been created`, as shown in Figure 7-13.


Digital Certificate Manager
IBM
Select a Certificate Store
Expand All
Collapse All
Manage User Certificates
Create New Certificate Store
Create a Certificate Authority (CA)
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection
OK

Certificate Store Created

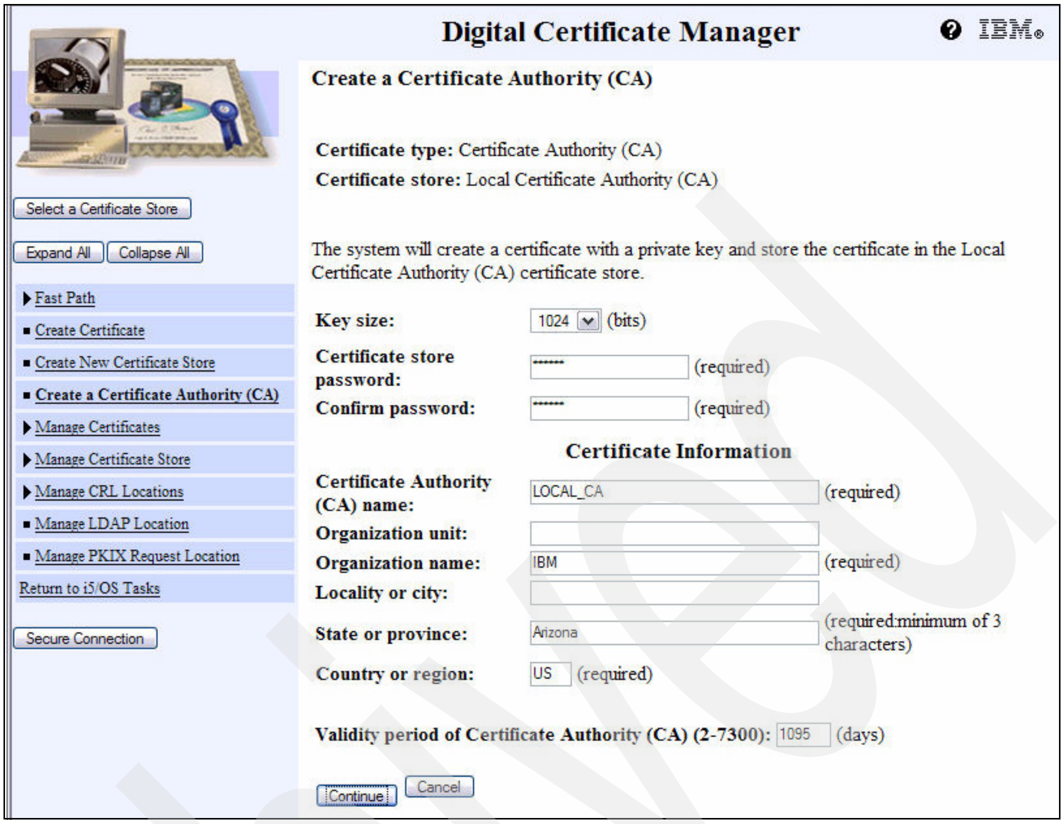
Message The certificate store has been created.

File name: /EKM/EKM.KDB

Note: You must click on the Select a Certificate Store button in the left frame to refresh the Digital Certificate Manager (DCM) to work with this new certificate store.

Figure 7-13 DCM Certificate Store Created screen

6. Select **Create a Certificate Authority (CA)**, choose a **Key size** of `1024` bits, fill in the required local CA certificate information as in the example shown in Figure 7-14, and click **Continue** to proceed.



Create a Certificate Authority (CA)

Certificate type: Certificate Authority (CA)
Certificate store: Local Certificate Authority (CA)

The system will create a certificate with a private key and store the certificate in the Local Certificate Authority (CA) certificate store.

Key size: 1024 (bits)
Certificate store password: ****** (required)
Confirm password: ****** (required)

Certificate Information

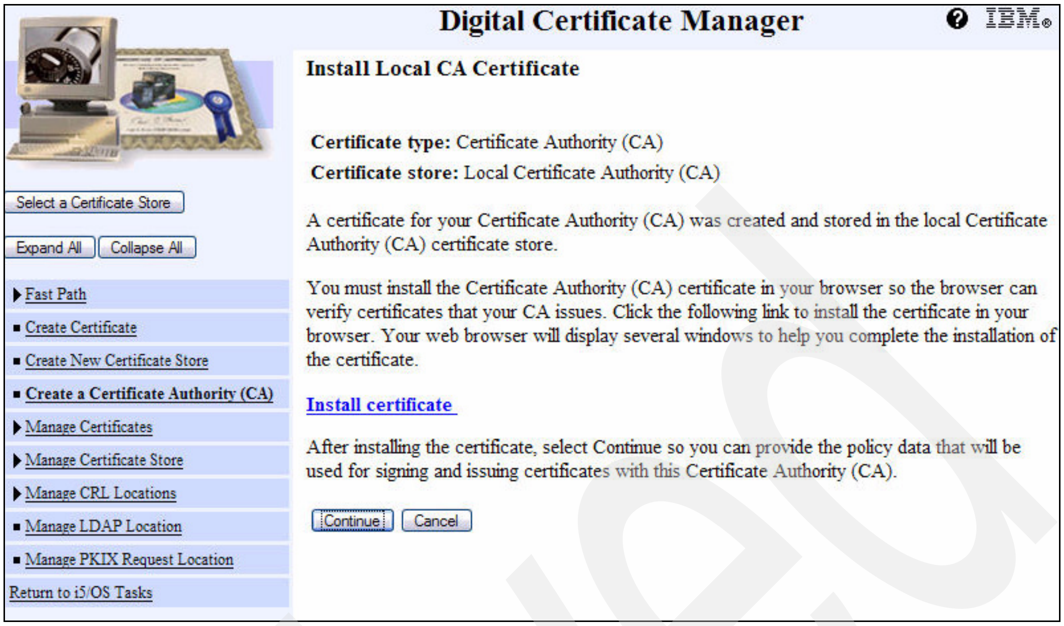
Certificate Authority (CA) name: LOCAL_CA (required)
Organization unit:
Organization name: IBM (required)
Locality or city:
State or province: Arizona (required:minimum of 3 characters)
Country or region: US (required)

Validity period of Certificate Authority (CA) (2-7300): 1095 (days)

Figure 7-14 DCM Create a Certificate Authority screen

Note: The *Create a Certificate Authority (CA)* menu option is only shown as long as no local CA has been created yet. If a local CA already exists, proceed directly to step 10.

7. Select **Continue** on the “Install Local CA Certificate” screen shown in Figure 7-15, which creates the local CA certificate – it is not necessary to install the local CA certificate in your browser, because the local CA is not meant to be used for SSL Web connections.



Install Local CA Certificate

Certificate type: Certificate Authority (CA)

Certificate store: Local Certificate Authority (CA)

A certificate for your Certificate Authority (CA) was created and stored in the local Certificate Authority (CA) certificate store.

You must install the Certificate Authority (CA) certificate in your browser so the browser can verify certificates that your CA issues. Click the following link to install the certificate in your browser. Your web browser will display several windows to help you complete the installation of the certificate.

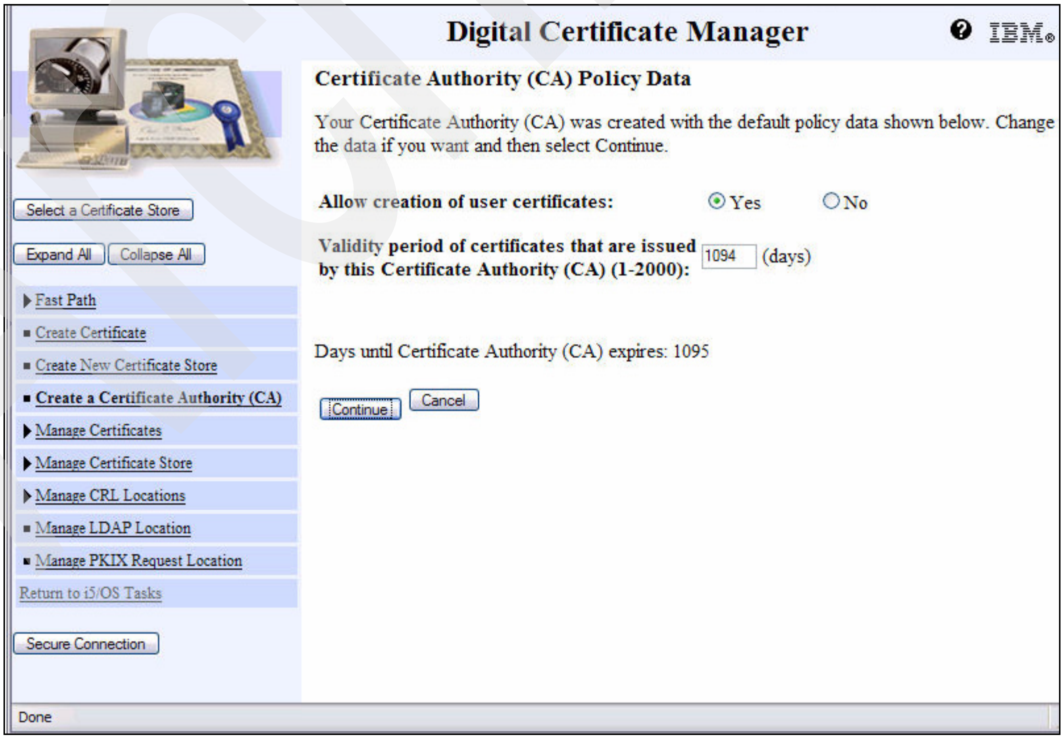
Install certificate

After installing the certificate, select Continue so you can provide the policy data that will be used for signing and issuing certificates with this Certificate Authority (CA).

Figure 7-15 Install Local CA Certificate

8. For the *Allow creation of user certificates* option, choose **Yes** and specify the validity period for the certificates issued by your local CA you want to use for tape encryption, which must be less than the validity of the CA certificate itself, as shown in Figure 7-16.

> **Note:** EKM does *not* care about the validity period or expiration of certificates. It also works with the keys from expired certificates as long as they remain in the keystore.



Certificate Authority (CA) Policy Data

Your Certificate Authority (CA) was created with the default policy data shown below. Change the data if you want and then select Continue.

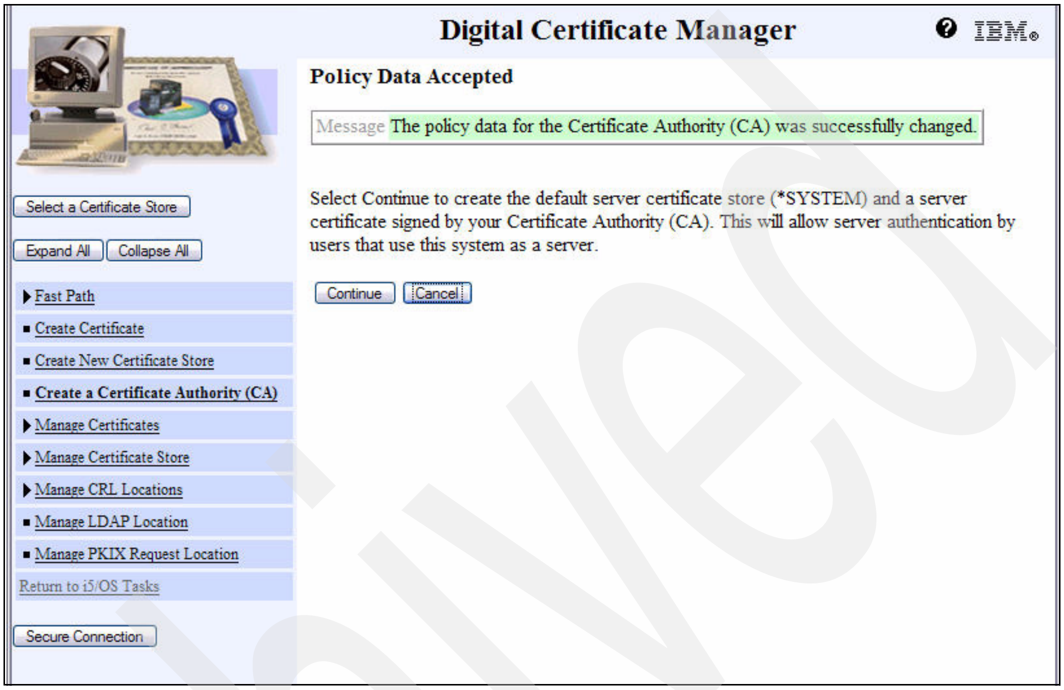
Allow creation of user certificates: ● Yes ○ No

Validity period of certificates that are issued by this Certificate Authority (CA) (1-2000): 1094 (days)

Days until Certificate Authority (CA) expires: 1095

Figure 7-16 Certificate Authority (CA) Policy Data screen

9. After clicking **Continue**, the successful modification of the local CA policy data is indicated by the message, `The policy data for the Certificate Authority (CA) was successfully changed`. Because the local CA certificate is used to issue self-signed certificates used for tape encryption, select **Cancel** to not create a server certificate store as shown in Figure 7-17.



Digital Certificate Manager

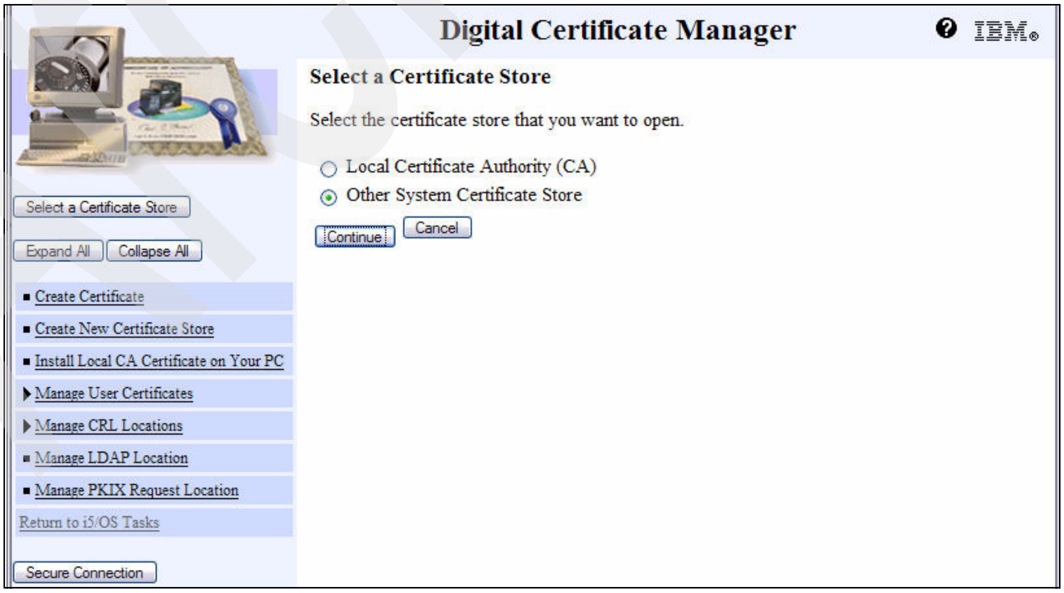
Policy Data Accepted

Message The policy data for the Certificate Authority (CA) was successfully changed.

Select Continue to create the default server certificate store (*SYSTEM) and a server certificate signed by your Certificate Authority (CA). This will allow server authentication by users that use this system as a server.

Figure 7-17 DCM Policy Data Accepted screen

10. After creation of the local CA keystore and certificate, select the EKM keystore created before in step 5 by using the **Select a Certificate Store** button, choosing the option **Other System Certificate Store**, as shown in Figure 7-18.



Digital Certificate Manager

Select a Certificate Store

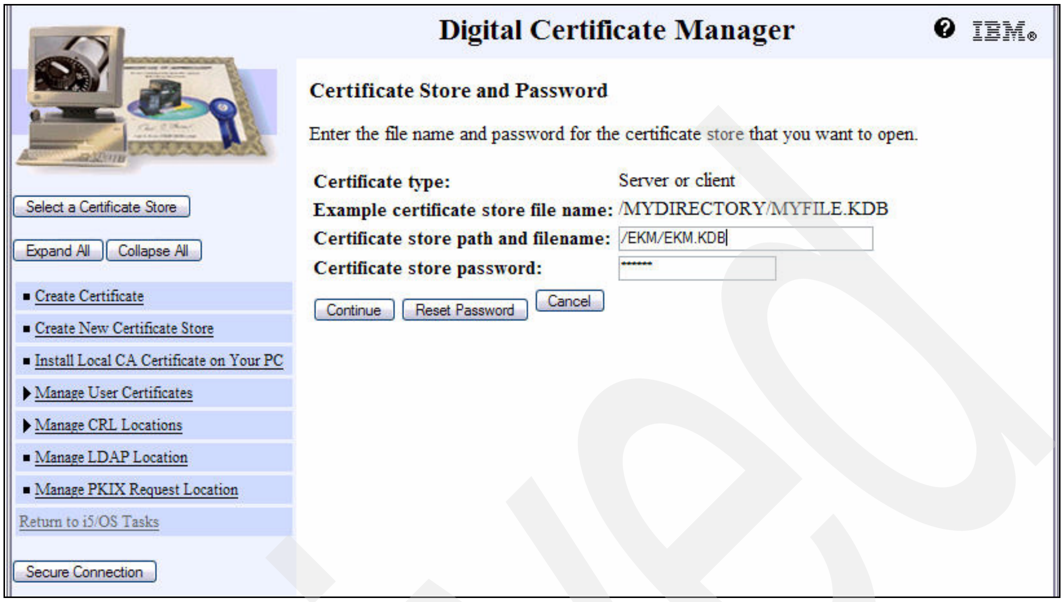
Select the certificate store that you want to open.

○ Local Certificate Authority (CA)

● Other System Certificate Store

Figure 7-18 DCM Select a Certificate Store screen

11. After clicking **Continue**, enter the **Certificate store path and filename** and **Certificate store password** of the previously created EKM keystore as shown in Figure 7-19.



Digital Certificate Manager

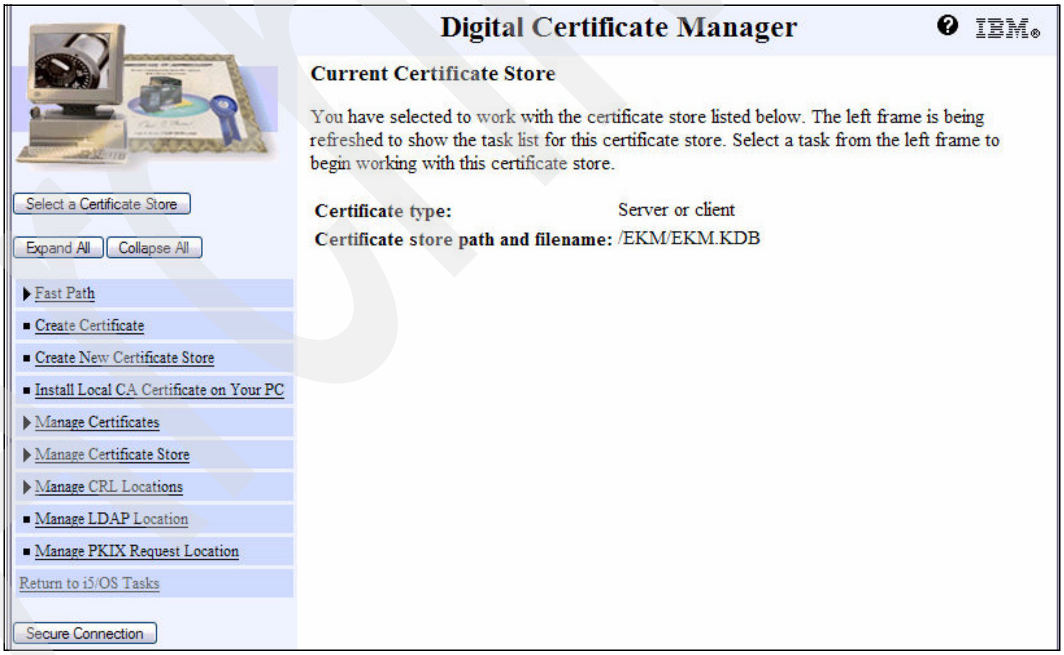
Certificate Store and Password

Enter the file name and password for the certificate store that you want to open.

Certificate type:	Server or client
Example certificate store file name:	/MYDIRECTORY/MYFILE.KDB
Certificate store path and filename:	/EKM/EKM.KDB
Certificate store password:	******

Figure 7-19 DCM Certificate Store and Password screen

12. After clicking **Continue**, successful selection of the certificate store is indicated as shown in Figure 7-20.



Digital Certificate Manager

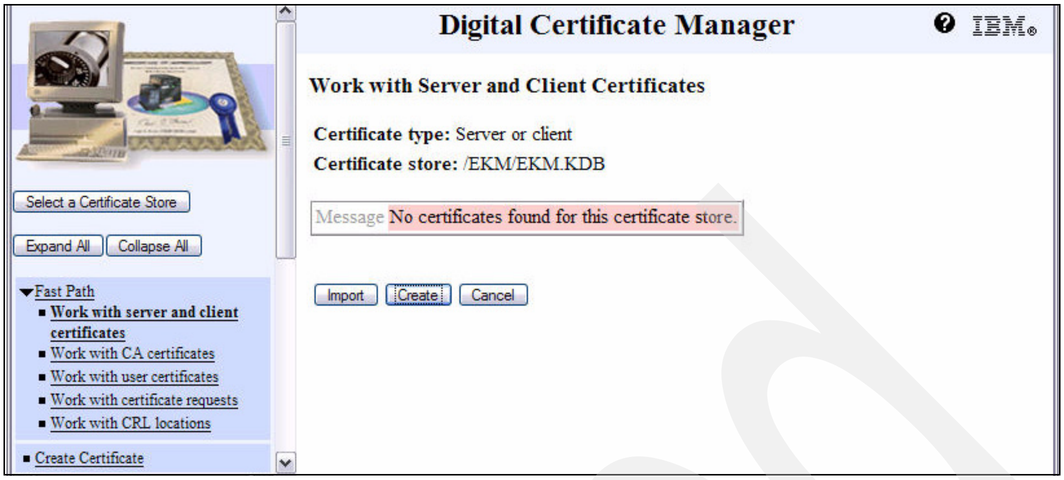
Current Certificate Store

You have selected to work with the certificate store listed below. The left frame is being refreshed to show the task list for this certificate store. Select a task from the left frame to begin working with this certificate store.

Certificate type:	Server or client
Certificate store path and filename:	/EKM/EKM.KDB

Figure 7-20 DCM Current Certificate Store screen

13. Select **Fast Path** → **Work with server and client certificates** and press the **Create** button shown in Figure 7-21.


Digital Certificate Manager
IBM.
Select a Certificate Store
Expand All
Collapse All
Fast Path
Work with server and client certificates
Work with CA certificates
Work with user certificates
Work with certificate requests
Work with CRL locations
Create Certificate
Import
Create
Cancel

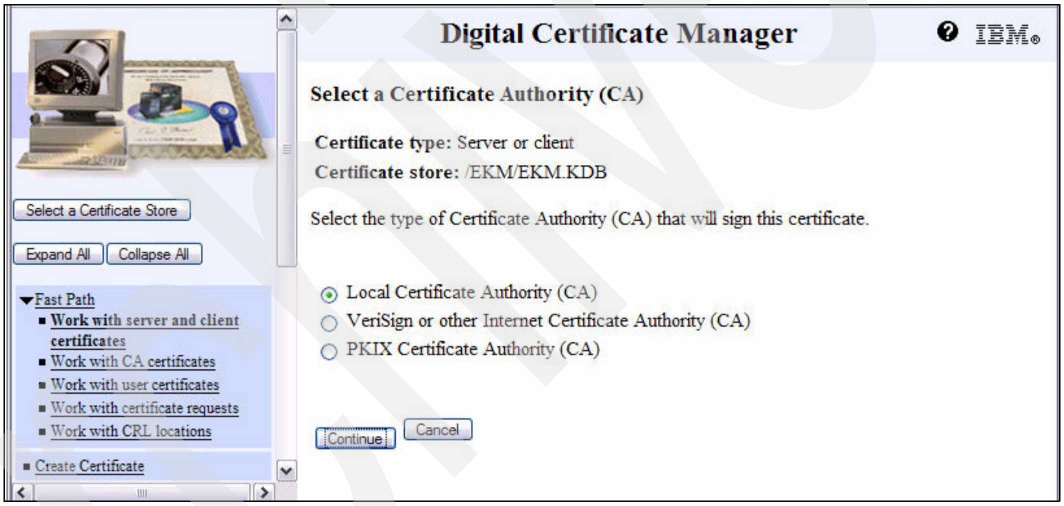
Work with Server and Client Certificates

Certificate type: Server or client
Certificate store: /EKM/EKM.KDB

Message No certificates found for this certificate store.

Figure 7-21 DCM Work with Server and Client Certificates

14.Select the option **Local Certificate Authority** for creation of a self-signed certificate to be used for tape encryption and click **Continue** as shown in Figure 7-22.


Digital Certificate Manager
IBM.
Select a Certificate Store
Expand All
Collapse All
Fast Path
Work with server and client certificates
Work with CA certificates
Work with user certificates
Work with certificate requests
Work with CRL locations
Create Certificate
Continue
Cancel

Select a Certificate Authority (CA)

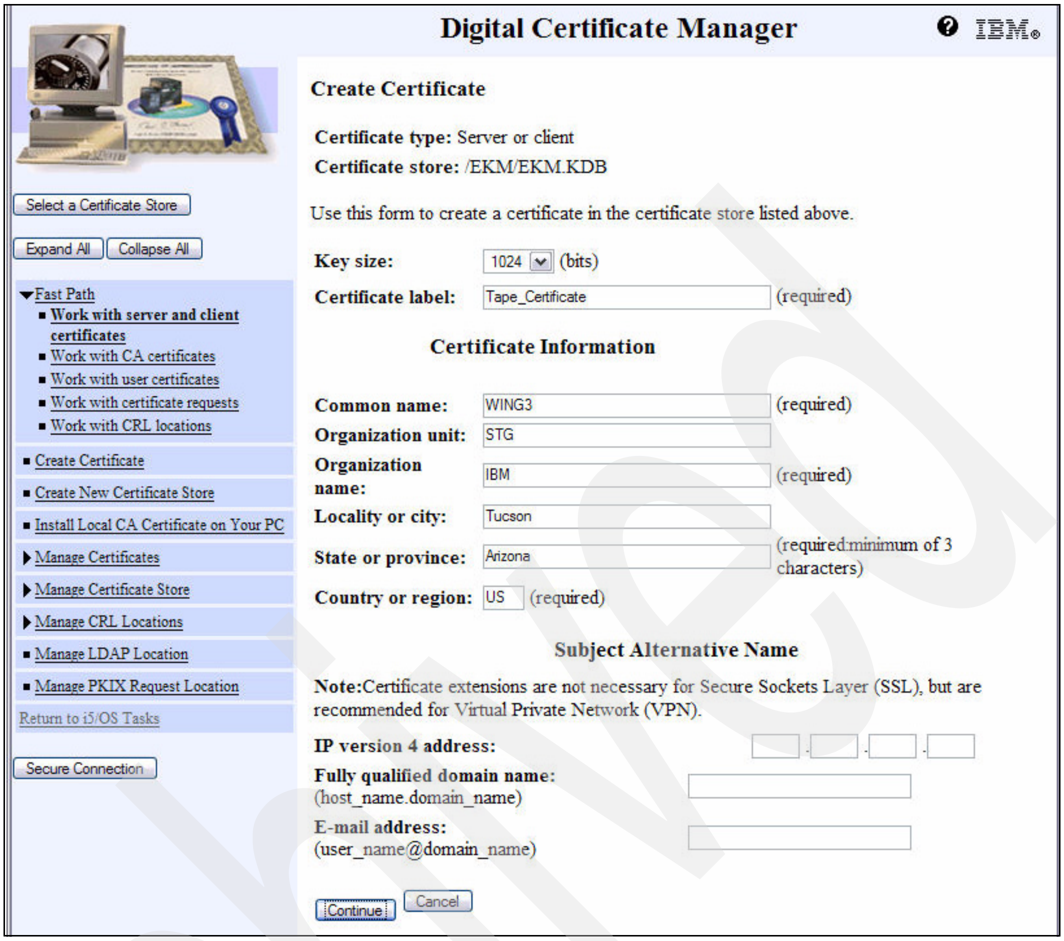
Certificate type: Server or client
Certificate store: /EKM/EKM.KDB

Select the type of Certificate Authority (CA) that will sign this certificate.

● Local Certificate Authority (CA)
○ VeriSign or other Internet Certificate Authority (CA)
○ PKIX Certificate Authority (CA)

Figure 7-22 DCM Select a Certificate Authority screen

15.Select for **Key size** `1024` bits, specify a **Certificate label**, which you should note down for later configuration of EKM, and complete the required **Certificate Information** fields with your identity information before pressing **Continue** to proceed as shown in Figure 7-23.


Digital Certificate Manager
IBM
Select a Certificate Store
Expand All
Collapse All
Fast Path
Work with server and client certificates
Work with CA certificates
Work with user certificates
Work with certificate requests
Work with CRL locations
Create Certificate
Create New Certificate Store
Install Local CA Certificate on Your PC
Manage Certificates
Manage Certificate Store
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection
Continue
Cancel

Create Certificate

Certificate type: Server or client
Certificate store: /EKM/EKM.KDB

Use this form to create a certificate in the certificate store listed above.

Key size: 1024 (bits)
Certificate label: Tape_Certificate (required)

Certificate Information

Common name: WING3 (required)
Organization unit: STG
Organization name: IBM (required)
Locality or city: Tucson
State or province: Arizona (required:minimum of 3 characters)
Country or region: US (required)

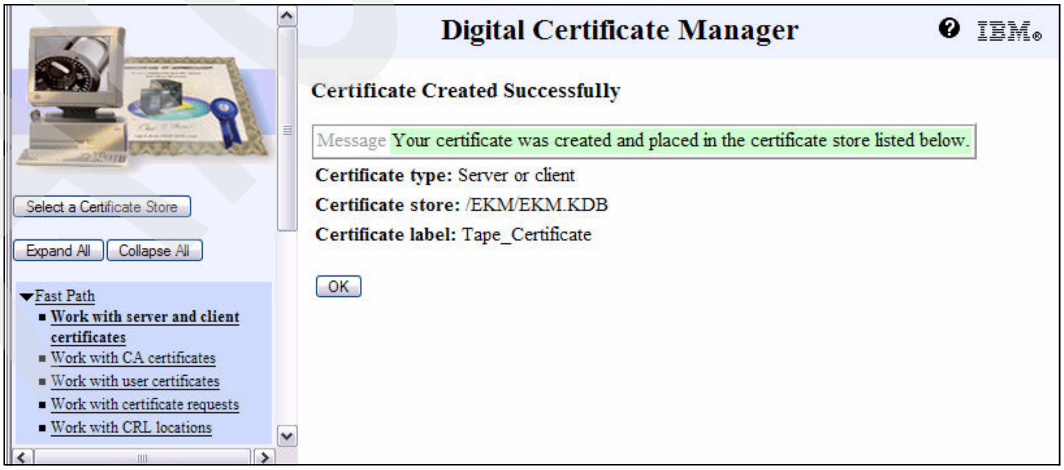
Subject Alternative Name

Note: Certificate extensions are not necessary for Secure Sockets Layer (SSL), but are recommended for Virtual Private Network (VPN).

IP version 4 address: . . .
Fully qualified domain name: (host_name.domain_name)
E-mail address: (user_name@domain_name)

Figure 7-23 DCM Create Certificate screen

16.Successful creation of your self-signed certificate in your EKM keystore is indicated by the message, `Your certificate was created and placed in the certificate store listed below`, as shown in Figure 7-24.


Digital Certificate Manager
IBM
Select a Certificate Store
Expand All
Collapse All
Fast Path
Work with server and client certificates
Work with CA certificates
Work with user certificates
Work with certificate requests
Work with CRL locations
OK

Certificate Created Successfully

Message Your certificate was created and placed in the certificate store listed below.

Certificate type: Server or client
Certificate store: /EKM/EKM.KDB
Certificate label: Tape_Certificate

Figure 7-24 DCM Certificate Created Successfully screen

17. Now an EKM keystore has been created, with a self-signed public/private key certificate to be used for 3592 tape encryption. To create a second certificate to be shared with a business partner as discussed in 7.2.6, “Considerations for sharing tapes with partners” on page 211, repeat steps 13 to 16 above, specifying a different certificate label. Return to 7.3.1, “New installation of the Encryption Key Manager” on page 213 and proceed with step 7 to continue with configuring EKM for tape encryption.

Creating a JCEKS keystore and certificate

To create a public/private key certificate for TS1120 tape encryption in a JCEKS keystore, refer to “Public/private key generation for 3592 tape encryption” on page 227. To create a symmetric key certificate for LTO4 tape encryption in a JCEKS keystore, refer to “Symmetric Key Generation for LTO4 Encryption” on page 227.

> **Note:** When using solely LTO4 tape encryption, we recommend to also create one public/private key as described in “Public/private key generation for 3592 tape encryption” on page 227 because it is required for SSL communication used for synchronization of two EKM servers – a missing public/private key does not cause the EKM server to fail, but can result in a Java exception `No available certificate corresponds to the SSL cipher suites that are enabled`.

The JCEKS keystore is automatically created with the corresponding key generation commands if it does not exist yet.

> **Note:** The *keypass* and *storepass* values used in the key generation procedures below must be the same since EKM allows to specify only one password in its KeyManagerConfig.properties configuration file, which is used for both the keystore and each associated key label.

Public/private key generation for 3592 tape encryption

Use the following command syntax from i5/OS Qshell to create a public/key certificate for 3592 tape encryption:

```
keytool -genkey -alias Tape_Certificate -dname "CN=WING3" -keystore /EKM/EKM.jck
-keyalg RSA -keysize 1024 -keypass password -storepass password -storetype JCEKS
```

This example creates a new self-signed *public/private key* certificate to be used for 3592 tape encryption generated from the RSA-1024 encryption key algorithm, labeled “Tape_Certificate” with the common name “WING3” in the JCEKS keystore “/EKM/EKM.jck”, both the keystore and certificate protected by the same specified “password” and valid for 90 days by default.

> **Note:** The validity period of a digital certificate is irrelevant, because certificate expiration does *not* matter for EKM.

Symmetric Key Generation for LTO4 Encryption

The *keytool* script in /usr/bin uses the default Java version configured on your i5/OS system. On i5/OS systems with multiple Java versions, that is, several 5722-JV1 options, installed this might not be the version required for any *symmetric* key management.

Check your current default Java version by running the command:

```
STRQSH CMD('java -version')
```

If your current default Java version is different than “J2SE 5.0 32 bit” for V5R4 and “Java 1.5” for V5R3 set the required version by defining an i5/OS job-level environment variable as shown below:

- For V5R4:

```
ADDENVVAR ENVVAR(JAVA_HOME) VALUE('/QOpenSys/QIBM/ProdData/JavaVM/jdk50/32bit')
LEVEL(*JOB)
```

- For V5R3:

```
STRQSH CMD('print “java.version=1.5” > /EKM/EKMjava.properties')
```

```
ADDENVVAR ENVVAR(QIBM_JAVA_PROPERTIES_FILE) VALUE('/EKM/EKMjava.properties')
```

> **Note:** The job-level environment variable, as defined, is only valid for the current interactive i5/OS user session. However, we do not recommend using a system-level environment variable for the default Java version, because it might result in incompatibilities with other programs such as the i5/OS HTTP admin server, which does not work with J2SE 5.0.

Use the following command in Qshell to generate symmetric key(s) for LTO4 tape encryption:

```
keytool -genseckey -alias LTO_Key -keypass password -keyalg AES -keysize 256
-keystore /EKM/EKM.jck -storepass password -storetype JCEKS
```

This example creates a new symmetric (or secret) key certificate to be used for LTO4 tape encryption generated from the AES-256 encryption key algorithm, labeled “LTO_Key” in the JCEKS keystore “/EKM/EKM.jck” and both the keystore and certificate are protected by the same specified “password”.

> **Note:** The *alias* is specified with up to 12 characters, but if you want increased security with using a set of symmetric LTO4 encryption keys across the pool of encrypted LTO4 cartridges to limit the work should a key get compromised, the keytool also allows creation of multiple symmetric keys in one step by using the *aliasrange* parameter instead.
>
> An alias range is specified with a three-character prefix followed by lower and upper limits of up to 16 hex digits, for example, like AES00-0F, which would create 16 symmetric key aliases at once.
>
> Refer to the online help accessible by the **keytool -ekmhelp** command for further information.

Viewing the newly created certificate in the EKM JCEKS keystore

List the contents of the keystore with the newly created certificate(s) using the command:

```
keytool -list -keystore /EKM/EKM.jck -storetype JCEKS -storepass password
```

Example 7-1 shows the listing for a sample JCEKS keystore with two public/private key certificates labeled “tape_certificate”, “tape_certificate2” and sixteen symmetric keys labeled aes0...0 to aes0...F.

Example 7-1 Sample JCEKS keystore

```
>  keytool -list -keystore /EKM/EKM.jck -storetype JCEKS -storepass TS1120
   Keystore type: JCEKS
   Keystore provider: IBMJCE
   Your keystore contains 18 entries
   aes000000000000000009, Apr 14, 2007, SecretKeyEntry,
   aes000000000000000008, Apr 14, 2007, SecretKeyEntry,
   aes000000000000000007, Apr 14, 2007, SecretKeyEntry,
   aes00000000000000000f, Apr 14, 2007, SecretKeyEntry,
   aes000000000000000006, Apr 14, 2007, SecretKeyEntry,
   aes00000000000000000e, Apr 14, 2007, SecretKeyEntry,
   aes000000000000000005, Apr 14, 2007, SecretKeyEntry,
   aes00000000000000000d, Apr 14, 2007, SecretKeyEntry,
   aes000000000000000004, Apr 14, 2007, SecretKeyEntry,
   aes00000000000000000c, Apr 14, 2007, SecretKeyEntry,
   aes000000000000000003, Apr 14, 2007, SecretKeyEntry,
   aes00000000000000000b, Apr 14, 2007, SecretKeyEntry,
   tape_certificate2, Apr 14, 2007, keyEntry, Certificate fingerprint (MD5):
   41:24:F7:87:7E:6F:C4:B6:DD:17:7E:76:5A:A3:C6:AB
   aes00000000000000000a, Apr 14, 2007, SecretKeyEntry,
   aes000000000000000002, Apr 14, 2007, SecretKeyEntry,
   aes000000000000000001, Apr 14, 2007, SecretKeyEntry,
   aes000000000000000000, Apr 14, 2007, SecretKeyEntry,
   tape_certificate, Apr 14, 2007, keyEntry, Certificate fingerprint (MD5):
   3F:6C:34:D1:2D:01:44:83:29:8F:4D:8A:2A:26:8C:F5
```

7.4.2 Configuring EKM for tape encryption

In this section, we describe the EKM configuration for TS1120 or LTO4 tape encryption or both, assuming steps 1 to 6 of 7.3.1, “New installation of the Encryption Key Manager” on page 213 have been completed.

Default EKM Configuration File

The default EKM configuration file “KeyManagerConfig.properties,” which still has to be customized for a specific environment, is shown in Example 7-2.

Example 7-2 Default EKM configuration file

```
# Note that the file is sorted by property name.  EKM shutdown automatically
# reorders the values in the properties file.
Audit.event.outcome = success,failure
Audit.event.types = all
Audit.eventQueue.max = 0
# Need to change the following directory value or create the directories
Audit.handler.file.directory = /EKM/auditlogs
Audit.handler.file.name = ekm_audit.log
Audit.handler.file.size = 10000
# Need to change the following 2 pathnames to the correct pathnames for
# the keystores being used on your system
Admin.ssl.keystore.name = /EKM/EKM.kdb
Admin.ssl.truststore.name = /EKM/EKM.kdb
# Need to change the following pathname value or create the directories
config.drivetable.file.url = FILE:///EKM/drives/drivetable
# Need to change the following pathname to the correct pathname for
# the keystore being used on your system
config.keystore.file = /EKM/EKM.kdb
config.keystore.provider = IBMi5OSJSSEProvider
config.keystore.type = IBMi5OSKeyStore
debug = all
debug.output = simple_file
# Need to change the following pathname value or create the directory
debug.output.file = /EKM/debug.log
# Change this to 'false' if you do not want new tape drives automatically
# added to the EKM drive table
drive.acceptUnknownDrives = true
fips = Off
TransportListener.ssl.ciphersuites = JSSE_ALL
TransportListener.ssl.clientauthentication = 0
# Need to change the following pathname to the correct pathname for
# the keystore being used on your system
TransportListener.ssl.keystore.name = /EKM/EKM.kdb
TransportListener.ssl.keystore.type = IBMi5OSKeyStore
# Need to specify the ssl port being used on your system
TransportListener.ssl.port = 443
TransportListener.ssl.protocols = TLSv1
# Need to change the following pathname to the correct pathname for
# the keystore being used on your system
TransportListener.ssl.truststore.name = /EKM/EKM.kdb
TransportListener.ssl.truststore.type = IBMi5OSKeyStore
# Need to specify the tcp/ip port being used on your system
TransportListener.tcp.port = 3801
# Need to specify the passwords for the keystores being used
Admin.ssl.keystore.password = kspwd
Admin.ssl.truststore.password = kspwd
config.keystore.password = kspwd
TransportListener.ssl.keystore.password = kspwd
TransportListener.ssl.truststore.password = kspwd
```

Customizing the EKM configuration file

Use the following i5/OS command to edit the EKM configuration file and customize it for your environment:

```
EDTF STMF('/EKM/KeyManagerConfig.properties')
```

Change the following configuration parameters according to your environment:

1. Adjust the **Audit.handler.file.directory** parameter value to match your audit log directory created in 7.3.1, “New installation of the Encryption Key Manager” on page 213, step 4, which must exist.

   Example: `Audit.handler.file.directory = /EKM/auditlogs`

2. Add the **Audit.metadata.file.name** parameter newly supported with EKM Release 2 for tracking of key usage requests for volume serial numbers in an XML metadata file, which is an abbreviated version of the EKM audit log and especially useful for LTO4 encryption (see “Example of the EKM audit metadata XML file” on page 256).

   Example: `Audit.metadata.file.name = /EKM/auditlogs/metadata.xml`

   The audit metadata XML file can be queried for specific volume serial numbers or key aliases via the *EKMDataParser* Java tool using the following syntax:

```
EKMDataParser [-filename metadatafile] [-volser volser] [-keyalias keyalias]
```

> **Note:** New XML metadata entries are generated with each key usage request. By default 100 entries are cached in memory before they are written to the XML metadata file. The optional *Audit.metadata.file.cachecount* parameter can be used to set the value of maximum cached entries however for performance reasons it is not recommended to turn off caching via setting this parameter to "0".

3. Modify the values for the following parameters to match your *name, type and provider of the EKM keystore* created in 7.4.1, "Creating an EKM keystore and certificate" on page 217 if it differs from the default name `/EKM/EKM.kdb`, type `IBMi5OSKeyStore` and provider `IBMi5OSJSSEProvider` – for example, for a JCEKS keystore the name might be `/EKM/EKM.jck`, type `JCEKS` and provider `IBMJCE`:

```
Admin.ssl.keystore.name
Admin.ssl.truststore.name
config.keystore.file
config.keystore.provider
config.keystore.type
TransportListener.ssl.keystore.name
TransportListener.ssl.keystore.type
TransportListener.ssl.truststore.name
TransportListener.ssl.truststore.type
```

> **Note:** The truststore and keystore are used for optional EKM to EKM server synchronization using SSL communication, not for communication between EKM and the tape library.

4. Modify the values for the following parameters to match your *password* for the keystore defined in chapter 7.4.1:

```
Admin.ssl.keystore.password
Admin.ssl.truststore.password
config.keystore.password
TransportListener.ssl.keystore.password
TransportListener.ssl.truststore.password
```

5. Modify the **config.drivetable.file.url** parameter value to reflect your preferred location of the EKM drivetable used to validate drives by their serial numbers for usage with EKM.

   Example: `config.drivetable.file.url = FILE:///EKM/drivetable`

6. Modify the **debug.output.file** parameter value to indicate the file used for output of EKM debug information.

   Example (default value): `debug.output.file = /EKM/debug.log`

7. The parameter **drive.acceptUnknownDrives** is set to "`true`" in the sample EKM configuration file so that any new tape drive that contacts EKM through the IBM tape library is automatically added with its serial number to the EKM drivetable containing the list of valid drives for usage with EKM. If instead you prefer to control which drives are valid for usage with EKM this parameter can be set to its default value of "`false`" so that new drives must be manually added to the drivetable using the **`adddrive`** command from the EKM admin console.

When the default parameter value of “`true`” is used with *3592* tape encryption, then also two default key aliases *must* be set for the drives via adding the **drive.default.alias1** and **drive.default.alias2** parameters to make sure an EEDK1 and EEDK2 can be generated for the new drive.

Example:

```
drive.default.alias1 = Tape_Certificate
drive.default.alias2 = Tape_Certificate2
```

> **Note:** If for 3592 tape encryption only one public/key certificate is used because sharing tapes with a business partner is currently no issue still make sure that if default aliases are used *both* alias1 and alias2 are defined even if they are both set to the same key label – otherwise the IBM library EKM configuration test might fail.
> The *default key aliases* could still be overruled by explicit key aliases specified via the “rec1” and “rec2” parameters for a drive in the drivetable or by the IBM TS3500 Tape Library Barcode Encryption Policy.

8. For *LTO4 encryption*, add the parameter **symmetricKeySet** specifying all symmetric keys to be used for LTO4 tape encryption – single key aliases and alias ranges can both be specified at once delimited by commas.

   Example: `symmetricKeySet = AES00-0F`

9. Save the changed EKM configuration file “KeyManagerConfig.properties”.

For further information about the EKM configuration file parameters and EKM admin console command line interface refer to the *IBM Encryption Key Manager Component for the Java platform: Introduction, Planning and User’s Guide*, GA76-0418, available at

`http://www-1.ibm.com/support/docview.wss?rs=1139&context=STCXRGL&dc=D400&uid=ssg1S4000504`

7.4.3 Configuring the IBM TS3500 Library for Library-Managed Encryption

Using the example of an IBM TS3500 tape library, we describe in this section the procedures for setting up the Encryption Key Manager (EKM) addresses in the tape library and enabling it for Library-Managed Encryption.

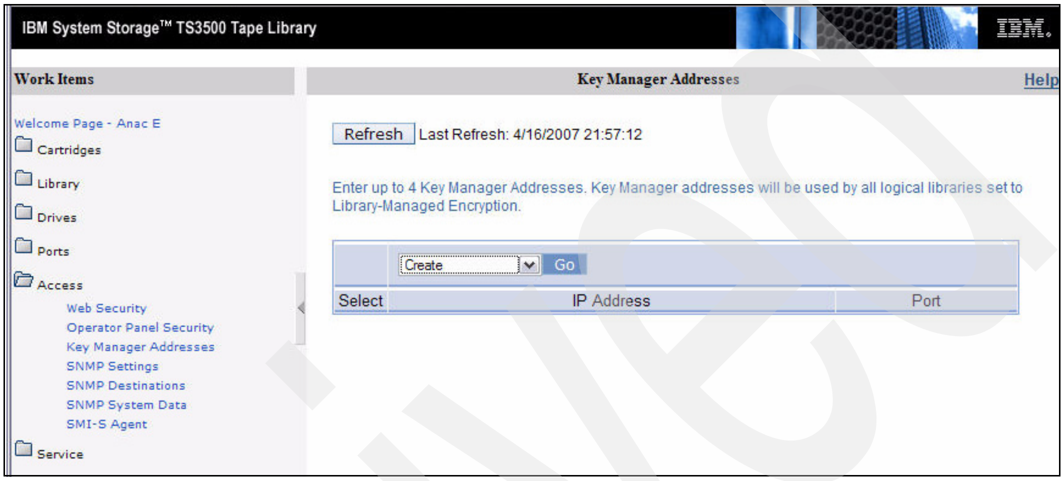
For information about configuring encryption on the IBM TS3100, TS3200, TS3310, TS3400, and 3493 tape libraries, refer to the corresponding operator guides:

- *IBM System Storage TS3100 Tape Library and TS3200 Tape Library: Setup, Operator and Service Guide*, GA32-0545
- *IBM System Storage TS3310 Tape Library Setup and Operator Guide*, GA32-0477
- *IBM System Storage TS3400 Tape Library Planning and Operator Guide*, GC27-2107
- *IBM TotalStorage Enterprise Automated Tape Library Operator Guide*, GA32-0449

Setting up Encryption Key Manager addresses

Follow the procedure below to set up the EKM server TCP/IP addresses used by the IBM TS3500 tape library for communication with the EKM servers:

1. Use a Web browser entering the IBM TS3500 tape library IP address to connect to the IBM TS3500 Tape Library Specialist, the Web user interface of the TS3500 Tape Library.
2. Select the **Access** → **Key Manager Addresses** menu and choose **Create** from the drop-down menu as shown in Figure 7-25.



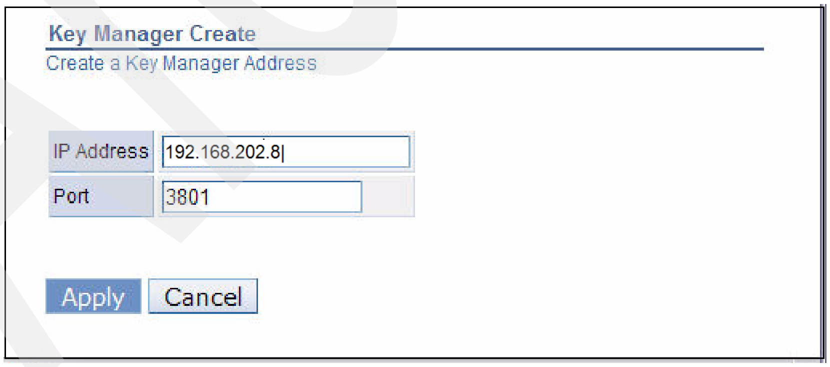
Last Refresh: 4/16/2007 21:57:12

Enter up to 4 Key Manager Addresses. Key Manager addresses will be used by all logical libraries set to Library-Managed Encryption.

Figure 7-25 IBM TS3500 Tape Library - Key Manager Addresses window

3. After clicking **Go,** in the newly opened "Create Key Manager Address" window, enter the IP address of the i5 server where EKM has been installed as shown in Figure 7-26.

> **Note:** If another TCP/IP port than the default port 3801 should be used, for example, because it is already used for other TCP/IP services, or if multiple EKM servers should be installed on the same host system, remember to change the parameter *TransportListener.tcp.port* in your corresponding EKM configuration file */EKM/KeyManagerConfig.properties* as well.



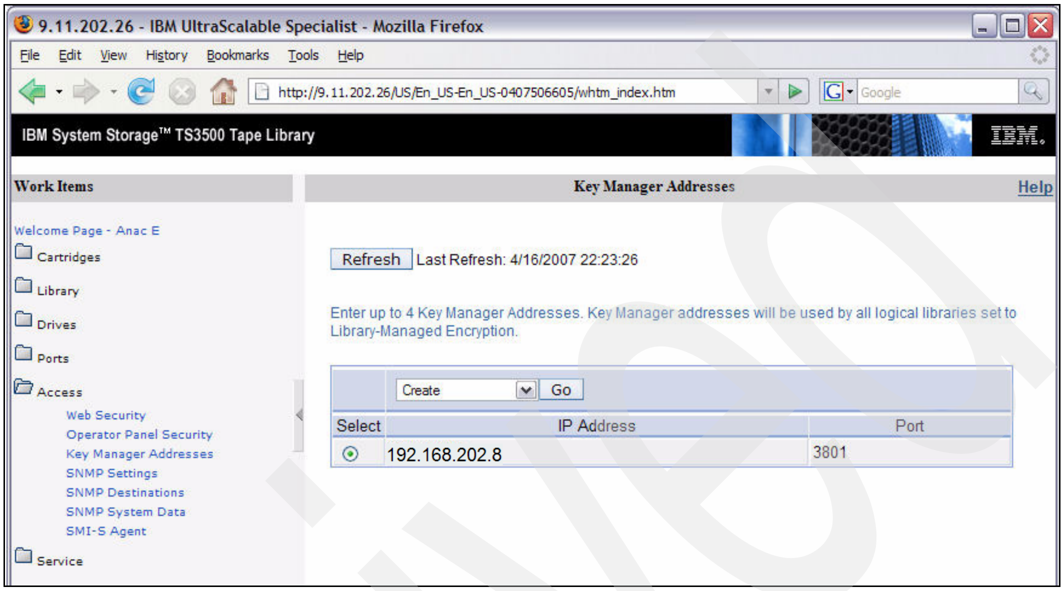
IP Address: 192.168.202.8

Port: 3801

Figure 7-26 IBM TS3500 Tape Library - Create Key Manager Address window

4. After clicking **Apply** to proceed, **close** the newly opened window with the message, `The Key Manager Address Change is complete.`

5. The ITS3500 Tape Library Specialist shows the newly created EKM address in the *Key Manager Addresses* window as shown in Figure 7-27.



Last Refresh: 4/16/2007 22:23:26

Enter up to 4 Key Manager Addresses. Key Manager addresses will be used by all logical libraries set to Library-Managed Encryption.

Select	IP Address	Port
●	192.168.202.8	3801

Figure 7-27 IBM TS3500 Tape Library - Key Manager Addresses window

6. Repeat steps 2 to 5 for any further secondary EKM servers being used.

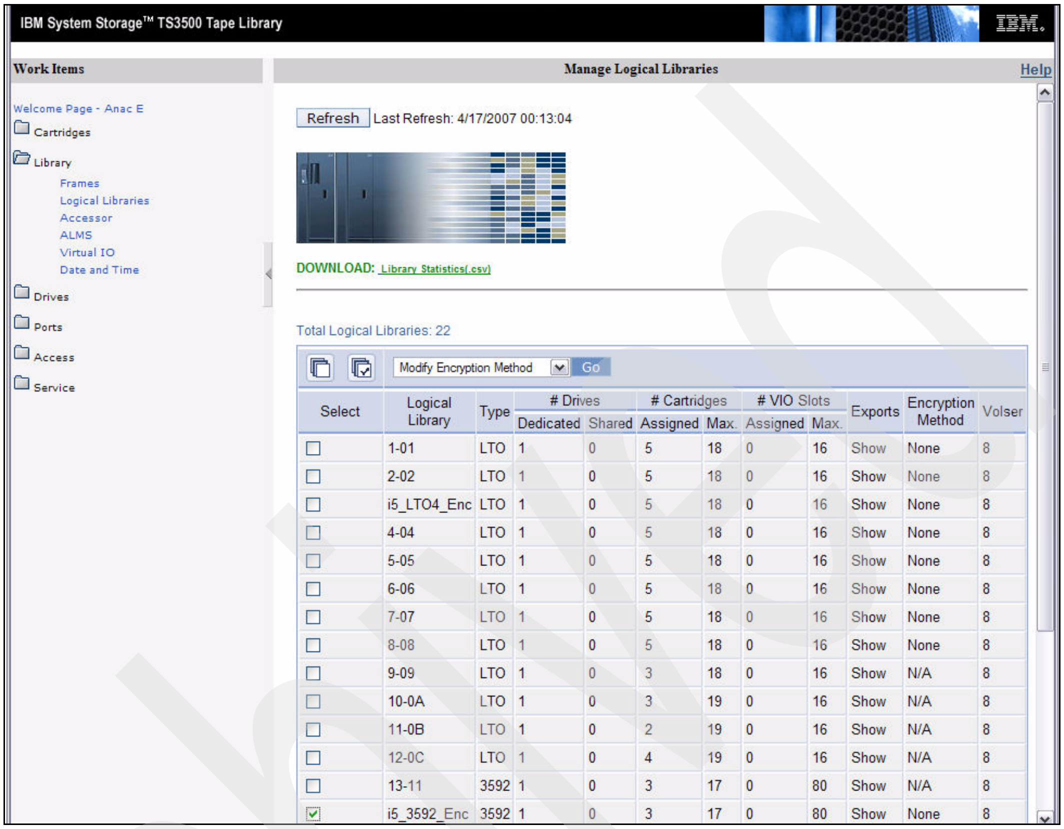
> **Note:** Up to four EKM server addresses can be configured in the IBM TS3500 tape library for automatic EKM server failover. The library attempts to talk to the first configured EKM server. If this fails, it proceeds, trying to talk to the next one in the list. At the end of the list, it starts over again, trying the first one.

Enabling Library-Managed Encryption

Follow this procedure to configure logical libraries in the IBM TS3500 Tape Library for Library-Managed Encryption:

1. Use a Web browser entering the IBM TS3500 tape library IP address to connect to the TS3500 Tape Library Specialist.

2. Select **Library** → **Logical Libraries**, select the logical libraries from the list with the same media type (either 3592 or LTO4) for which Library-Managed Encryption should be enabled. Choose the option **Modify Encryption Method** as shown in Figure 7-28.



Last Refresh: 4/17/2007 00:13:04

Total Logical Libraries: 22

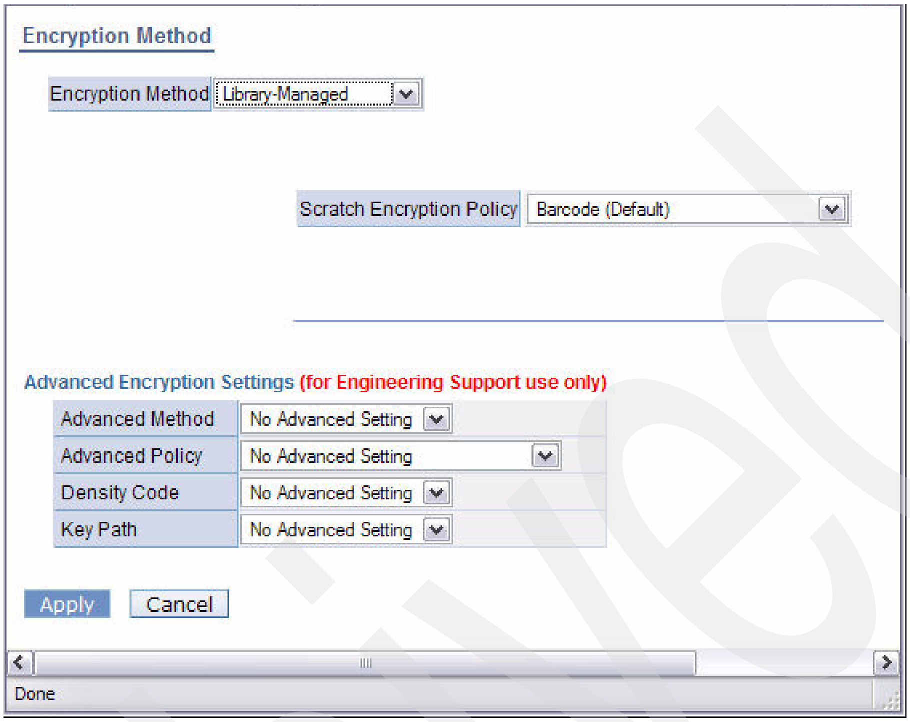
Modify Encryption Method

Select	Logical Library	Type	# Drives		# Cartridges		# VIO Slots		Exports	Encryption Method	Volser
			Dedicated	Shared	Assigned	Max.	Assigned	Max.			
□	1-01	LTO	1	0	5	18	0	16	Show	None	8
□	2-02	LTO	1	0	5	18	0	16	Show	None	8
□	i5_LTO4_Enc	LTO	1	0	5	18	0	16	Show	None	8
□	4-04	LTO	1	0	5	18	0	16	Show	None	8
□	5-05	LTO	1	0	5	18	0	16	Show	None	8
□	6-06	LTO	1	0	5	18	0	16	Show	None	8
□	7-07	LTO	1	0	5	18	0	16	Show	None	8
□	8-08	LTO	1	0	5	18	0	16	Show	None	8
□	9-09	LTO	1	0	3	18	0	16	Show	N/A	8
□	10-0A	LTO	1	0	3	19	0	16	Show	N/A	8
□	11-0B	LTO	1	0	2	19	0	16	Show	N/A	8
□	12-0C	LTO	1	0	4	19	0	16	Show	N/A	8
□	13-11	3592	1	0	3	17	0	80	Show	N/A	8
☑	i5_3592_Enc	3592	1	0	3	17	0	80	Show	None	8

Figure 7-28 IBM Tape Library Specialist - Manage Logical Libraries screen

> **Notes:** Logical libraries in the list that show an *Encryption Method* of “N/A” have no encryption-capable drives and cannot be enabled for encryption.

3. After clicking **Go,** select the option **Library-Managed** for Encryption Method and leave the other settings at their default values as shown in Figure 7-29.



Encryption Method

Encryption Method: Library-Managed

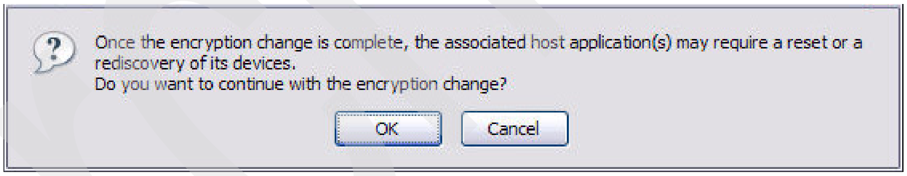
Scratch Encryption Policy: Barcode (Default)

Advanced Encryption Settings (for Engineering Support use only)

Advanced Method	No Advanced Setting
Advanced Policy	No Advanced Setting
Density Code	No Advanced Setting
Key Path	No Advanced Setting

Figure 7-29 IBM UltraScalable Specialist - Encryption Method screen

4. After clicking **Apply,** select **OK** for the following confirmation window shown in Figure 7-30.

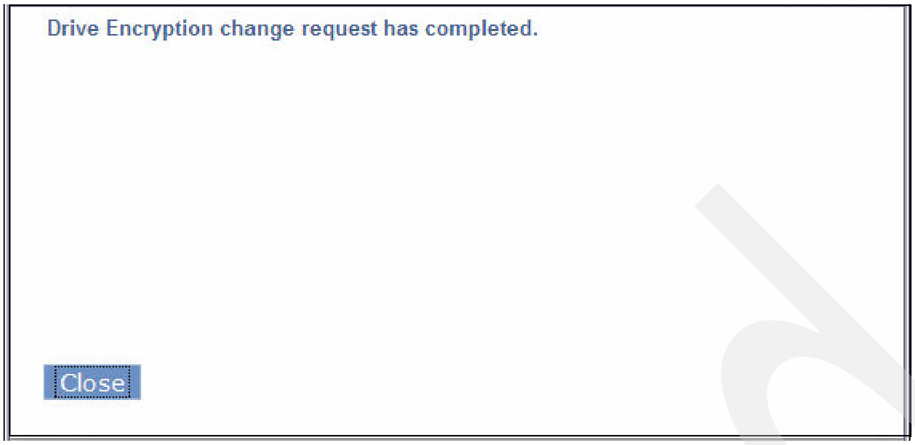


Once the encryption change is complete, the associated host application(s) may require a reset or a rediscovery of its devices.
Do you want to continue with the encryption change?

Figure 7-30 IBM UltraScalable Specialist - Encryption Method change confirmation window

Note: i5/OS supports no dynamic device reconfiguration, so that an IOP reset is required to recognize the changedencryption setting, which we account for later as the last step of this procedure.

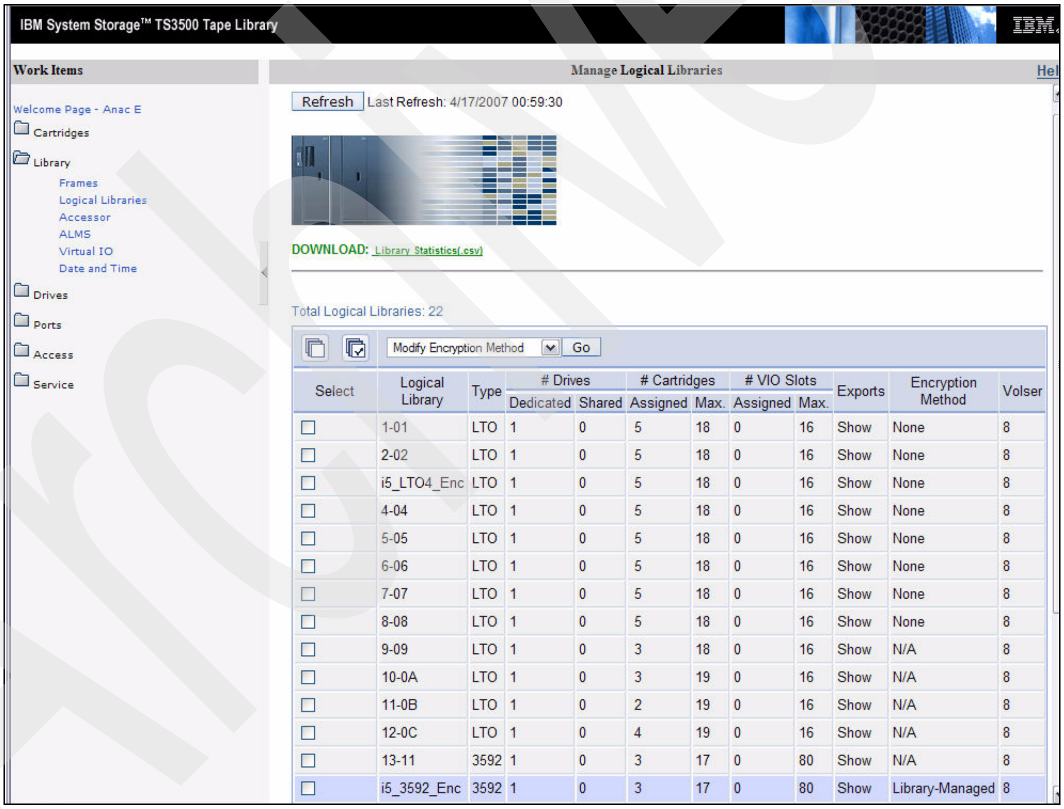
5. A new progress window about modification of the encryption method is opened. Await its completion as indicated by the message, `Drive Encryption change request has completed`, and select **Close** for closing the "Success window" shown in Figure 7-31.



Drive Encryption change request has completed.

Figure 7-31 IBM UltraScalable Specialist - Success window

6. The automatically refreshed “Manage Logical Libraries” screen shows the enabled *Library-Managed Encryption* method for the changed logical library (Figure 7-32).



Last Refresh: 4/17/2007 00:59:30

DOWNLOAD: Library Statistics(.csv)

Total Logical Libraries: 22

Select	Logical Library	Type	# Drives		# Cartridges		# VIO Slots		Exports	Encryption Method	Volser
			Dedicated	Shared	Assigned	Max.	Assigned	Max.			
□	1-01	LTO	1	0	5	18	0	16	Show	None	8
□	2-02	LTO	1	0	5	18	0	16	Show	None	8
□	i5_LTO4_Enc	LTO	1	0	5	18	0	16	Show	None	8
□	4-04	LTO	1	0	5	18	0	16	Show	None	8
□	5-05	LTO	1	0	5	18	0	16	Show	None	8
□	6-06	LTO	1	0	5	18	0	16	Show	None	8
□	7-07	LTO	1	0	5	18	0	16	Show	None	8
□	8-08	LTO	1	0	5	18	0	16	Show	None	8
□	9-09	LTO	1	0	3	18	0	16	Show	N/A	8
□	10-0A	LTO	1	0	3	19	0	16	Show	N/A	8
□	11-0B	LTO	1	0	2	19	0	16	Show	N/A	8
□	12-0C	LTO	1	0	4	19	0	16	Show	N/A	8
□	13-11	3592	1	0	3	17	0	80	Show	N/A	8
□	i5_3592_Enc	3592	1	0	3	17	0	80	Show	Library-Managed	8

Figure 7-32 IBM UltraScalable Specialist - Manage Logical Libraries screen

Repeat the foregoing steps 2 to 6 to enable Library-Managed Encryption for other logical libraries if required.

Use the following procedure on i5/OS to make it recognize the configuration change after enabling encryption with added two new media densities FMT3592A1E and FMT3592A2E for encrypted 3592 cartridges:

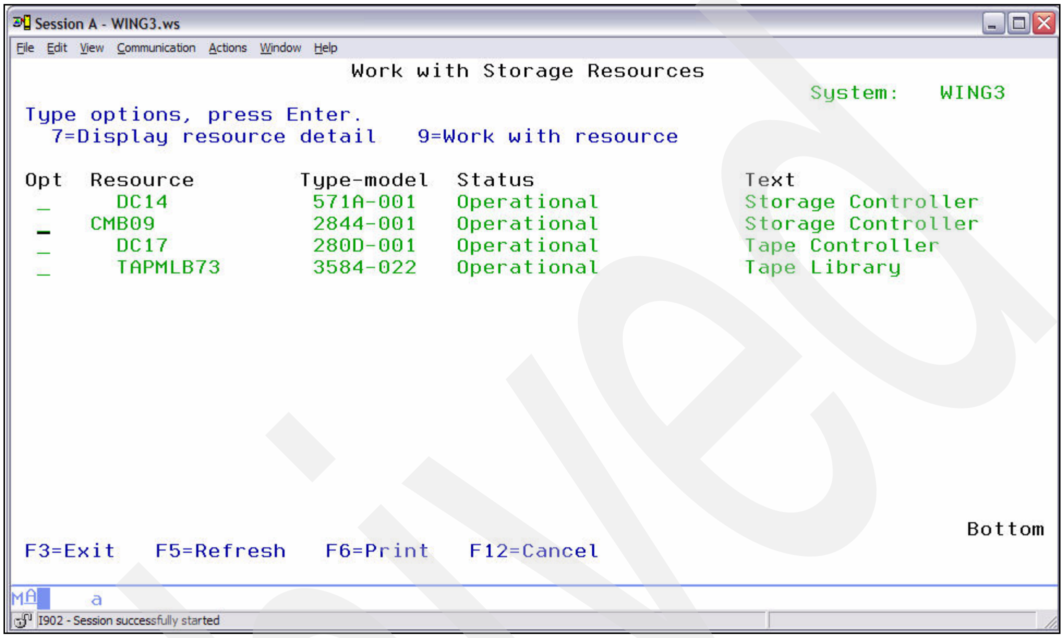
1. Vary off the corresponding tape library device by running the command:

   VRYCFG CFGOBJ(*TAPMLB73*) CFGTYPE(*DEV) STATUS(*OFF)

2. Find out the *IOP resource name* of the attached newly encryption-enabled tape drive from the output of the following command:

   WRKHDWRSC *STG

   Figure 7-33 shows an example with the TAPMLB73 library being attached via the #2844 IOP with the resource name CMB09.



```
Session A - WING3.ws
File  Edit  View  Communication  Actions  Window  Help
                         Work with Storage Resources
                                                             System:   WING3
 Type options, press Enter.
   7=Display resource detail    9=Work with resource

 Opt  Resource         Type-model  Status                Text
  _     DC14            571A-001    Operational           Storage Controller
  _   CMB09             2844-001    Operational           Storage Controller
  _     DC17            280D-001    Operational           Tape Controller
  _     TAPMLB73        3584-022    Operational           Tape Library

                                                                        Bottom
 F3=Exit   F5=Refresh   F6=Print   F12=Cancel
MA     a
I902 - Session successfully started
```

Figure 7-33 i5/OS Work with Storage Resources screen

3. Access System Service Tools to reset and re-IPL the IOP associated with the attached encryption-enabled tape drive as follows:

   STRSST

   Log in to SST with your SST password and userID and select the following menu options:

   a. **1. Start a service tool** from the “System Service Tools (SST)” screen

   b. **7. Hardware service manager** from the “Start a Service Tool” screen

   c. **3. Locate resource by resource name** from the “Hardware Service Manager” screen

      In the “Locate Resource By Resource Name” screen enter your IOP resource name from step b above (in the given example it would be CMB09)

      i. Select the option **6=I/O debug** for the IOP in the “Logical Hardware Resources” screen

      ii. Select **3. Reset I/O processor** in the “Select IOP Debug Function” screen and confirm the action by pressing ENTER.

      iii. After receiving the completion message “Reset of IOP was successful.” select **4. IPL I/O processor** from the “Select IOP Debug Function” screen and confirm the action by pressing ENTER.

      iv. After receiving the completion message “Re-IPL of IOP was successful.” press F3 three times and ENTER to exit SST.

4. Vary on the corresponding tape library device again by running the command:

   VRYCFG CFGOBJ(*TAPMLB73***) CFGTYPE(*DEV) STATUS(*ON)**

Testing the EKM IBM TS3500 Library-Managed Encryption setup

After having completed the preceding steps of “Setting up Encryption Key Manager addresses” on page 233 and “Enabling Library-Managed Encryption” on page 234 use the following procedure to test the IBM TS3500 library communication with the configured EKM server address(es):

1. Start the EKM admin consoles for all configured EKM server addresses:

   – For EKM servers installed on i5/OS, run the following command from i5/OS Qshell:

     strEKM -propfile /*EKM***/KeyManagerConfig.properties**

     > **Note:** Always use the strEKM start script on i5/OS for starting the EKM admin console, which helps to ensure that the correct Java version is being used for EKM.

   – For EKM server(s) installed on other Java platforms run the following Java command:

     java com.ibm.keymanager.KMSAdminCmd *KeyManagerConfig_full_file_path_name*

   Example 7-3 shows the EKM admin command prompt # displayed after starting the EKM admin console. The output from the *listdrives* EKM command shows that there are no drives yet listed in the EKM drivetable.

   Example 7-3 EKM admin command prompt

   ```
   > strEKM -propfile /EKM/KeyManagerConfig.properties
   Apr 16, 2007 4:33:21 PM Thread[main,5,main] com.ibm.keymanger.config.ConfigImpl get
   FINER: ENTRY
   Apr 16, 2007 4:33:21 PM Thread[main,5,main] com.ibm.keymanger.config.ConfigImpl get ALL:
   debug.output = simple_file
   Apr 16, 2007 4:33:21 PM Thread[main,5,main] com.ibm.keymanger.config.ConfigImpl get
   FINER: RETURN
   #
   > listdrives
   Drive entries: 0
   #
   ```

2. If using the EKM configuration file *KeyManagerConfig.properties* parameter setting “`drive.acceptUnknownDrivesBefore = false`” to not automatically add new drives, each tape drive to be used for encryption must be manually added to the EKM drive table using the EKM **adddrive** command before they can be used with the EKM server as follows:

   adddrive -drivename *drivename* **-rec1** *alias1* **-rec2** *alias2*

   Example:

   ```
   adddrive -drivename 000123456789 -rec1 Tape_Certificate -rec2 Tape_Certificate2
   ```

   > **Note:** The *drivename* parameter value has to be specified as a 12-digit drive serial number (with leading zeroes). The *rec1* and *rec2* parameters apply for 3592 tape encryption only and allow to use an encryption policy with specified default key aliases to be used for a selected drive serial number.
   >
   > The drivetable can dynamically be changed without restarting the EKM server -- however *currently* only if the EKM server was started interactively from the EKM admin console.

3. Start the EKM server for all configured EKM server addresses by running the command **startekm** from the EKM admin console.

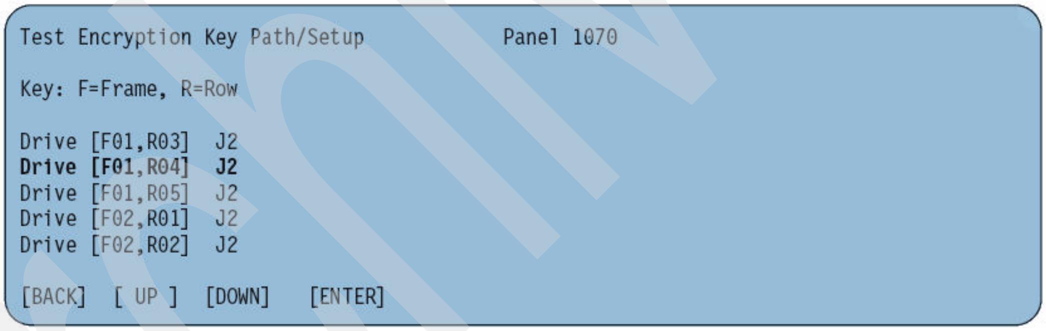
   Example 7-4 shows the output from the *startEKM* command.

   Example 7-4 startEKM output

```
> startekm
Loaded drive key store successfully
No symmetric keys in symmetricKeySet, LTO drives can not be supported.
Starting the Encryption Key Manager 2.0-20070328
Processing Arguments
Processing
Server is started
#
```

> **Note:** The message, `No symmetric keys in symmetricKeySet, LTO drives can not be supported`, is posted by EKM only to inform that it found no *symmetricKeySet* parameter in its configuration file and thus cannot support LTO4 encryption.

4. Test the encryption setup by using the IBM TS3500 tape library operator panel function **MENU** → **Service** → **Tests/Tools** → **Diagnostics** → **Test Encryption Key Path/Setup** → **ENTER** and use **DOWN** or **UP** to select the drive from the list of encryption enabled-drives as shown in Figure 7-34.



```
Test Encryption Key Path/Setup          Panel 1070

Key: F=Frame, R=Row

Drive [F01,R03]  J2
Drive [F01,R04]  J2
Drive [F01,R05]  J2
Drive [F02,R01]  J2
Drive [F02,R02]  J2

[BACK]  [ UP ]  [DOWN]   [ENTER]
```

Figure 7-34 IBM TS3500 operator panel Test Encryption Key Path/Setup select screen

5. After pressing ENTER, the library performs the following tests for the encryption setup:

   – *Ethernet*

     The library performs a ping to the EKM IP address(es) where the selected drive is registered. It can ping up to four host server IP addresses. If successful, the screen displays `Passed`, which means that the target host system can be reached by the library over the network. If unsuccessful, the screen displays `Failed`. If at least one ping test passes, the testing continues with the *EKM Path* and *EKM Configuration* tests otherwise it stops and `ENTER` is displayed.

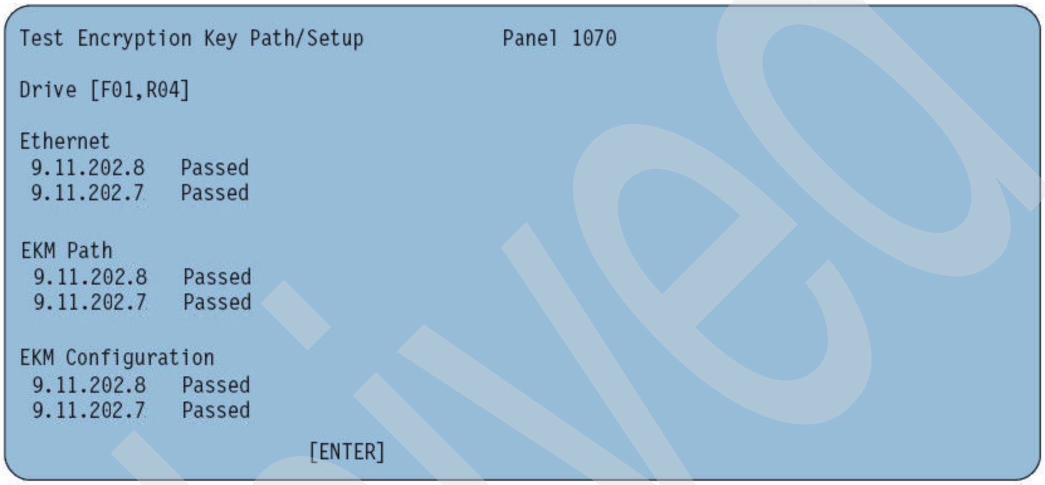
   – *EKM Path*

     The EKM Path test tries to establish communication to an encryption key manager. It ensures that the communication path between the drive and the EKM including the library's proxy server is working. If successful, the screen displays `Passed`; if unsuccessful, it displays `Failed` and the following *EKM Configuration* test does not run and `ENTER` is displayed.

– *EKM Configuration*

The EKM Configuration test is a diagnostic that establishes a link to a encryption key manager and requests a default key, which ensures that the drive has been correctly installed and is able to service key requests.

Note: The library's three encryption diagnostics, that is, ping, EKM path, and EKM configuration test, *all* have to pass successfully as shown in Figure 7-35 as a prerequisite of being able to use tape encryption for the selected drive.



```
Test Encryption Key Path/Setup          Panel 1070

Drive [F01,R04]

Ethernet
 9.11.202.8   Passed
 9.11.202.7   Passed

EKM Path
 9.11.202.8   Passed
 9.11.202.7   Passed

EKM Configuration
 9.11.202.8   Passed
 9.11.202.7   Passed
                        [ENTER]
```

Figure 7-35 IBM TS3500 operator panel Test Encryption Key Path/Setup result screen

6. Ensure that all above three diagnostic tests are passed successfully and repeat steps 4 to 5 above for each encryption-enabled drive.

   A *failed Ethernet test* normally points to a network problem of the library not reaching the host server where the EKM is installed, which might be further isolated by trying to ping the EKM host server and library from another server in the network.

   For a *failed EKM Path test* the first steps in failure isolation should be to verify if the EKM server was started and is running properly using the EKM admin console **`status`** command and to check that the IP port settings for the EKM servers defined in the library match with those in the EKM configuration file and cause no port conflicts on the host.

   A *failed EKM configuration test* typically points to a problem with the configured key alias or/and keystore. For further guidance to isolate and resolve the problem refer to *IBM System Storage TS3500 Tape Library Operator Guide*, GA32-0560, "Chapter 6. Problem Determination". Contact your IBM support representative for further assistance if required.

   Note: When using the `drive.acceptUnknownDrives = true` EKM configuration file parameter setting new drives are automatically added to the EKM drivetable after their successful completion of above *EKM Path* diagnostic tests – even if the subsequent EKM configuration test fails.

7. End the interactive EKM server session(s) again by entering the command **exit** from each EKM admin console. Return to "New installation of the Encryption Key Manager" on page 213 and proceed with step 9 to start the EKM server(s) as a batch job.

7.4.4 Importing and exporting of encryption keys

In the following sections, we describe the procedures to import or export a digital certificate used for tape encryption from an EKM keystore, which depend on whether public/private keys, symmetric keys, or public key only certificates are considered.

For importing/exporting public/private key certificates and symmetric keys, for example, for transfer to another EKM server on a different host platform, refer to “Procedures for public/private key certificates and symmetric keys”.

For importing/exporting a public key only certificate to provide it to a business partner for exchanging encrypted 3592 tape cartridges, refer to “Procedure for exporting/importing public key only certificates”.

Procedures for public/private key certificates and symmetric keys

The procedures for import or export of either a public/private key certificate used for TS1120 tape encryption or a symmetric key used for LTO4 tape encryption depend on the type of keystore being used:

- For *IBMi5OSKeyStore* keystores use the i5/OS Digital Certificate Manager (DCM) **Manage Certificates** → **Export certificate** or **Import certificate** menu option choosing **Server or client certificate** to export your public/private key certificate used for 3592 tape encryption.

  Further information about DCM is available at:

  iSeries Information Center Version 5 Release 4 in section **Systems management** → **Security** → **Digital Certificate Manager** at:

  `http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp`

- For *JCEKS* keystores, use the IBM Java keytool command as follows:

  – For *exporting a public/private key* certificate:

  `keytool -export -alias` *keylabel* **`-file`** *filename* **`-keystore`** *keystore* **`-storepass`** *password* **`-storetype JCEKS -keypass`** *password* **`-pkcs12`**

  – For *importing a public/private key* certificate:

  `keytool -import -alias` *keylabel* **`-file`** *filename* **`-keystore`** *keystore* **`-storepass`** *password* **`-storetype JCEKS -keypass`** *password* **`-pkcs12`**

  – For *exporting a symmetric key* wrapped by a public key:

  `keytool -exportseckey -alias` *keylabel* **`-keyalias`** *publickey* **`-keystore`** *keystore* **`-storepass`** *password* **`-storetype JCEKS -exportfile`** *filename*

  – For *importing a symmetric key* wrapped by a public key:

  `keytool -importseckey -alias` *keylabel* **`-keyalias`** *publickey* **`-keystore`** *keystore* **`-storepass`** *password* **`-storetype JCEKS -importfile`** *filename*

  Further information about the IBM Java keytool is available at:

  – IBM Java Keytool online help by entering **`keytool -help`** and **`keytool -ekmhelp`**

  – IBM Java Keytool Users Guide, available online at:

  `http://www-128.ibm.com/developerworks/java/jdk/security/50/secguides/keytoolDocs/KeyToolUserGuide-150.html`

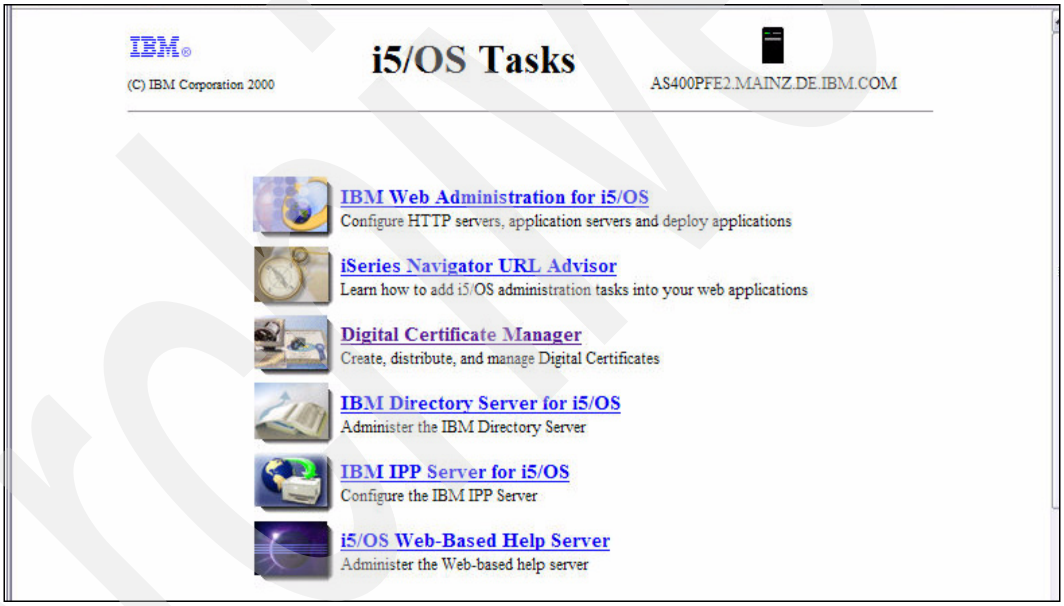
Procedure for exporting/importing public key only certificates

The following procedures to export/import a public key only certificate apply only in the context of providing/receiving a public key certificate to/from a business partner for sharing encrypted 3592 tape cartridges as described in 7.2.6, “Considerations for sharing tapes with partners” on page 211 and depend on the type of keystore being used.

Exporting a public key only from an i5OS keystore

For *IBMi5OSKeyStore* “*Other System Certificate Store” type EKM keystores the i5/OS Digital Certificate Manager (DCM) provides no option to directly export only the public key of a digital certificate used for 3592 tape encryption. However using the work-around described below via creating an **OBJECTSIGNING certificate store* first and exporting the EKM keystore certificate used for tape encryption into the *OBJECTSIGNING certificate store the public key only can be exported from the *OBJECTSIGNING certificate store as a *signature verification certificate* without the private key:

1. Connect to the HTTP admin server from the i5/OS system with the EKM keystore via entering the URL `http://`*`ipaddress`*`:2001` in a Web browser.
2. Access the i5/OS Digital Certificate Manager via selecting **Digital Certificate Manager** from the “i5/OS Tasks” HTTP admin server entry screen shown in Figure 7-36.



IBM®
(C) IBM Corporation 2000

i5/OS Tasks

AS400PFE2.MAINZ.DE.IBM.COM

IBM Web Administration for i5/OS
Configure HTTP servers, application servers and deploy applications

iSeries Navigator URL Advisor
Learn how to add i5/OS administration tasks into your web applications

Digital Certificate Manager
Create, distribute, and manage Digital Certificates

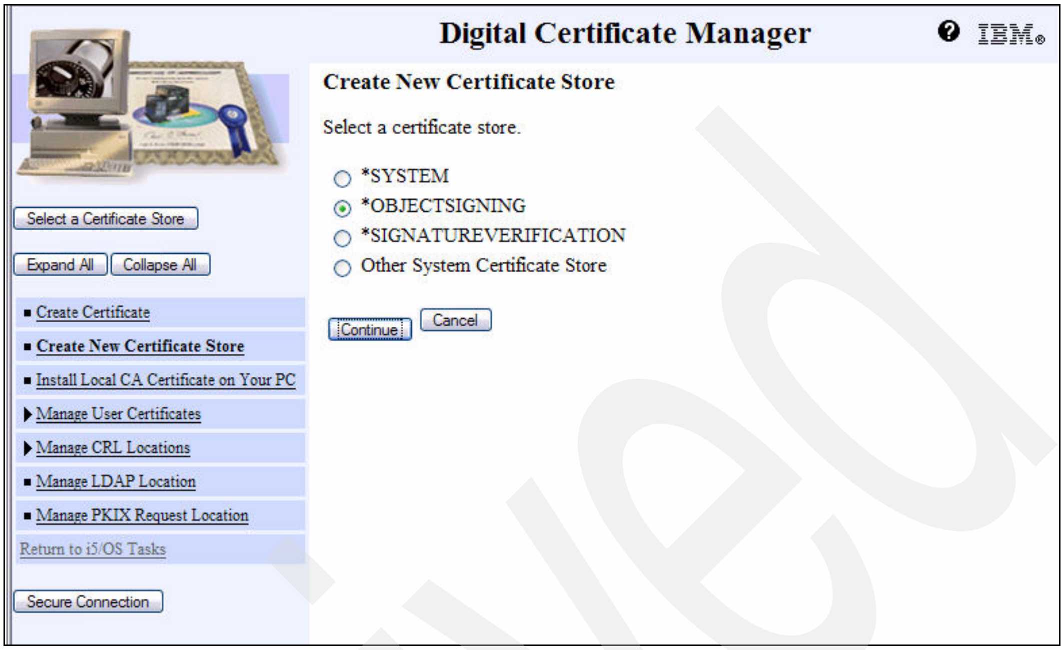
IBM Directory Server for i5/OS
Administer the IBM Directory Server

IBM IPP Server for i5/OS
Configure the IBM IPP Server

i5/OS Web-Based Help Server
Administer the Web-based help server

Figure 7-36 HTTP Admin Server “i5/OS Tasks” entry screen

3. Select to create an ***OBJECTSIGNING** certificate store from the **Create New Certificate Store** menu option shown in Figure 7-37.



Digital Certificate Manager
IBM
Select a Certificate Store
Expand All
Collapse All
▪ Create Certificate
▪ Create New Certificate Store
▪ Install Local CA Certificate on Your PC
▶ Manage User Certificates
▶ Manage CRL Locations
▪ Manage LDAP Location
▪ Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection
Continue
Cancel

Create New Certificate Store

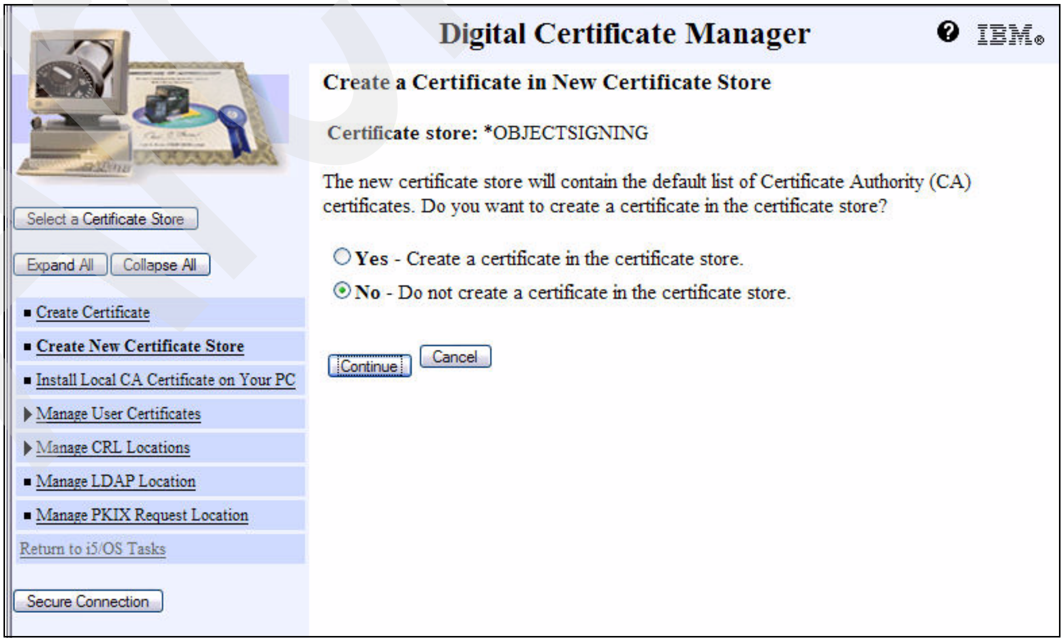
Select a certificate store.

○ *SYSTEM
● *OBJECTSIGNING
○ *SIGNATUREVERIFICATION
○ Other System Certificate Store

Figure 7-37 DCM Create New Certificate Store screen

> **Note:** If the *OBJECTSIGNING option is not shown in the DCM “Create New Certificate Store” screen then directly proceed to step 7 as an *OBJECTSIGNING certificate store already exists.

4. After clicking **Continue**, choose the option **No** to create no certificate in the new certificate store as shown in Figure 7-38.



Digital Certificate Manager
IBM
Select a Certificate Store
Expand All
Collapse All
▪ Create Certificate
▪ Create New Certificate Store
▪ Install Local CA Certificate on Your PC
▶ Manage User Certificates
▶ Manage CRL Locations
▪ Manage LDAP Location
▪ Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection
Continue
Cancel

Create a Certificate in New Certificate Store

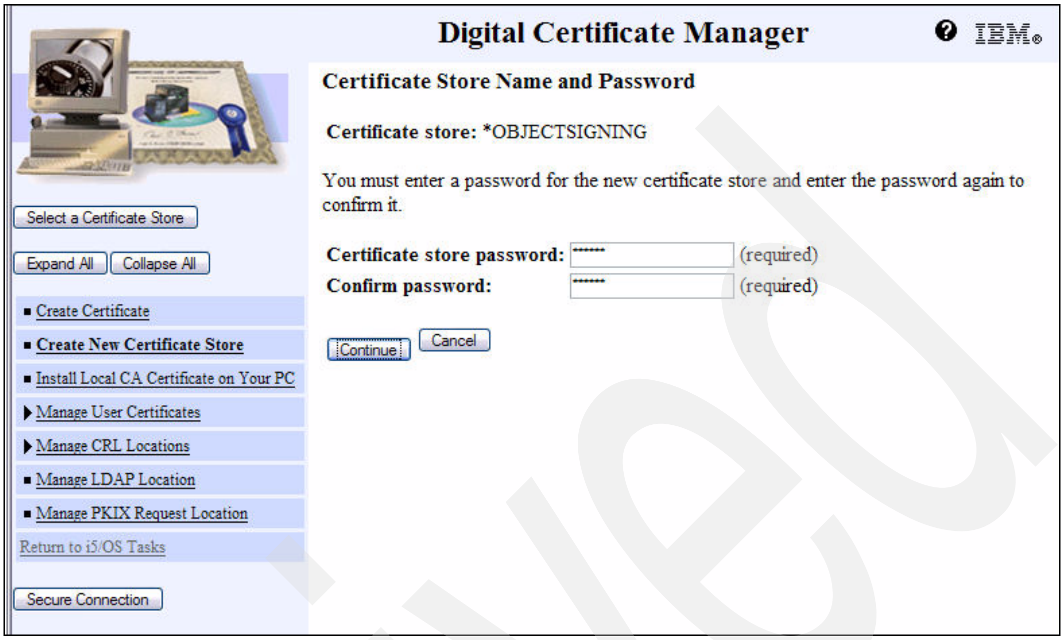
Certificate store: *OBJECTSIGNING

The new certificate store will contain the default list of Certificate Authority (CA) certificates. Do you want to create a certificate in the certificate store?

○ **Yes** - Create a certificate in the certificate store.
● **No** - Do not create a certificate in the certificate store.

Figure 7-38 DCM Create a Certificate in New Certificate Store screen

5. After clicking **Continue**, specify a password for the new *OBJECTSIGNING certificate store as shown Figure 7-39.



Certificate Store Name and Password

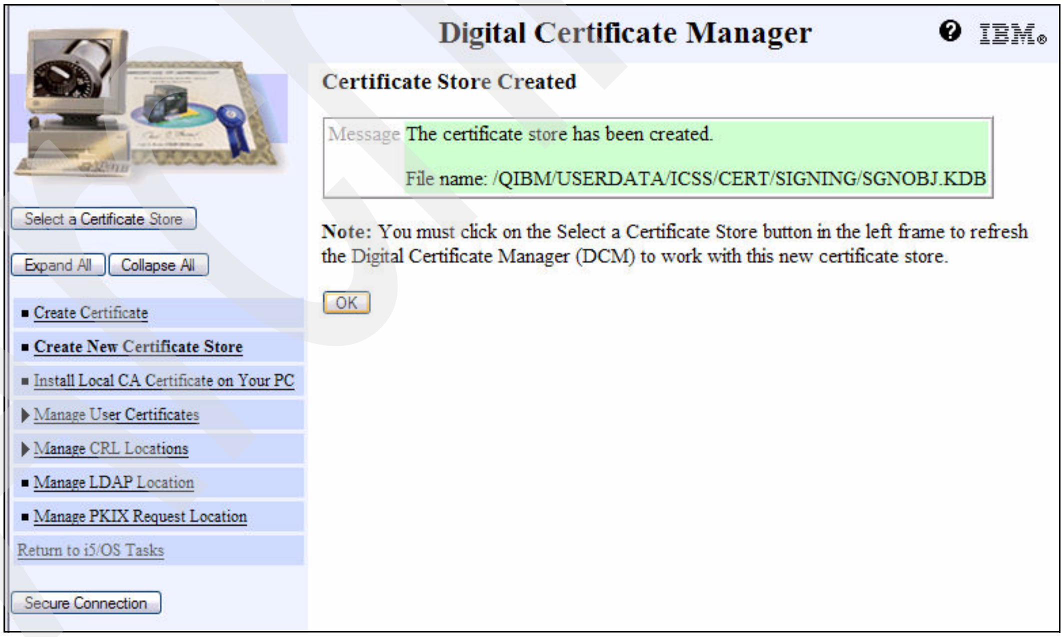
Certificate store: *OBJECTSIGNING

You must enter a password for the new certificate store and enter the password again to confirm it.

Certificate store password: ******* (required)
Confirm password: ******* (required)

Figure 7-39 DCM Certificate Store Name and Password screen

6. After clicking **Continue**, the following confirmation message in Figure 7-40 shows the successful creation of the new *OBJECTSIGNING certificate store.


Digital Certificate Manager
IBM
Select a Certificate Store
Expand All
Collapse All
Create Certificate
Create New Certificate Store
Install Local CA Certificate on Your PC
Manage User Certificates
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection
OK

Certificate Store Created

Message The certificate store has been created.

File name: /QIBM/USERDATA/ICSS/CERT/SIGNING/SGNOBJ.KDB

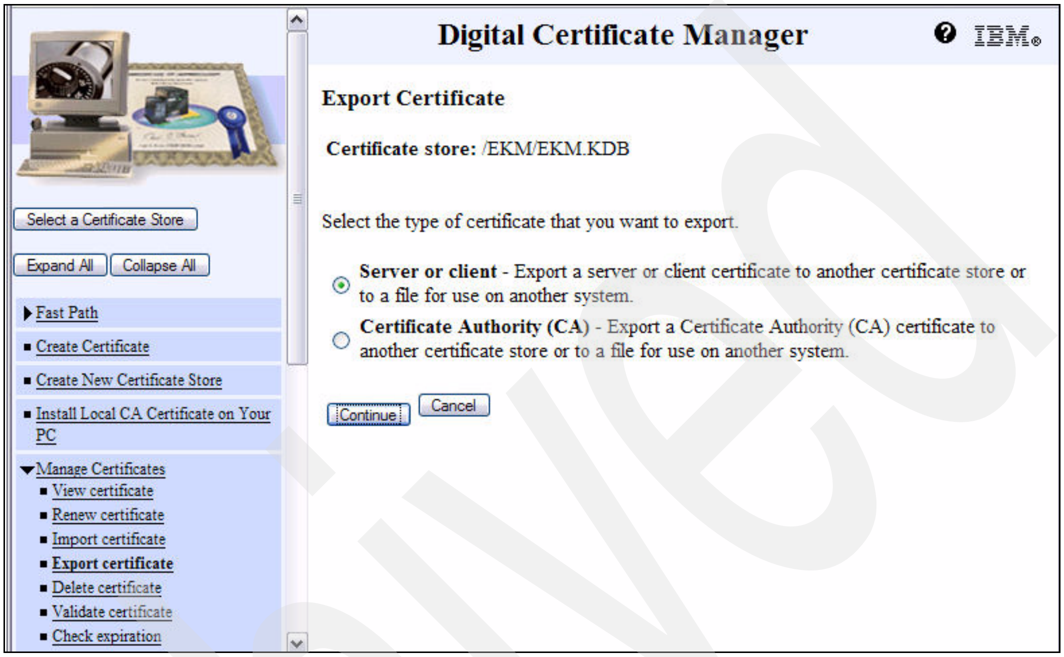
Note: You must click on the Select a Certificate Store button in the left frame to refresh the Digital Certificate Manager (DCM) to work with this new certificate store.

Figure 7-40 DCM Certificate Store Created screen

7. After having created the *OBJECTSIGNING certificate store, select the EKM keystore via **Select a Certificate Store** → **Other System Certificate Store** that contains the certificate to be exported first into the *OBJECTSIGNING certificate store as described next. Finally, the public key only is exported into a file to be provided to the business

partner who can use it as a second key label for encryption of 3592 tape cartridges to be shared with you having the private key required to decrypt them.

8. Export the EKM keystore certificate into the *OBJECTSIGNING certificate store via selecting **Manage Certificates** → **Export certificate** choosing the option **Server or client** as shown in Figure 7-41.



Export Certificate

Certificate store: /EKM/EKM.KDB

Select the type of certificate that you want to export.

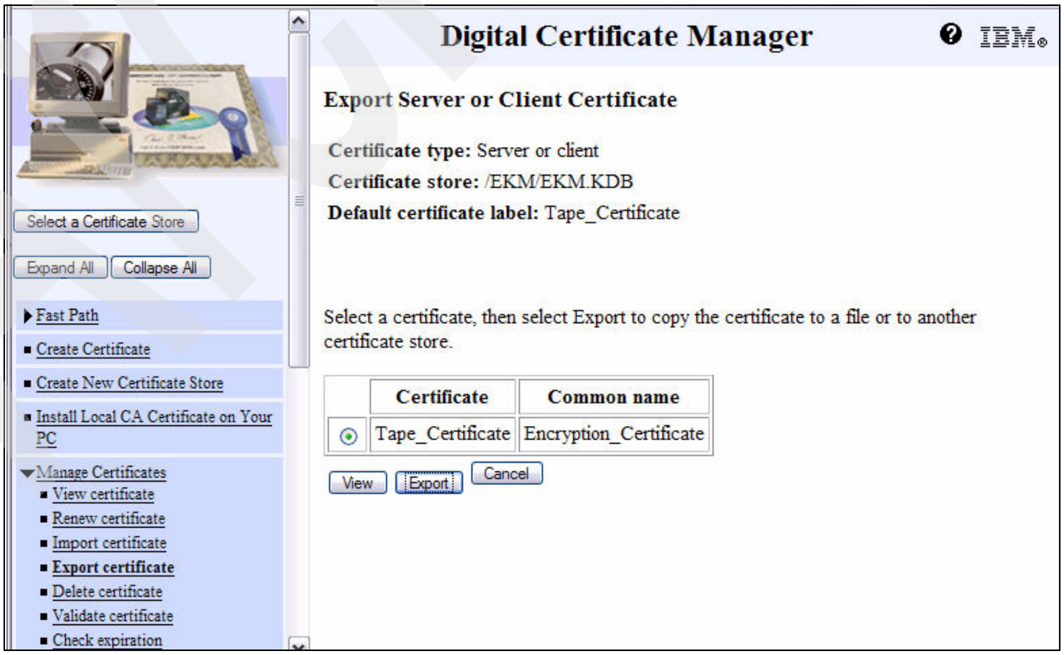
● **Server or client** - Export a server or client certificate to another certificate store or to a file for use on another system.

○ **Certificate Authority (CA)** - Export a Certificate Authority (CA) certificate to another certificate store or to a file for use on another system.

Continue Cancel

Figure 7-41 DCM Export Certificate screen

9. After clicking **Continue**, select the certificate used for 3592 tape encryption for which the public key should finally be exported for providing it to the business partner as shown in Figure 7-42.



Export Server or Client Certificate

Certificate type: Server or client
Certificate store: /EKM/EKM.KDB
Default certificate label: Tape_Certificate

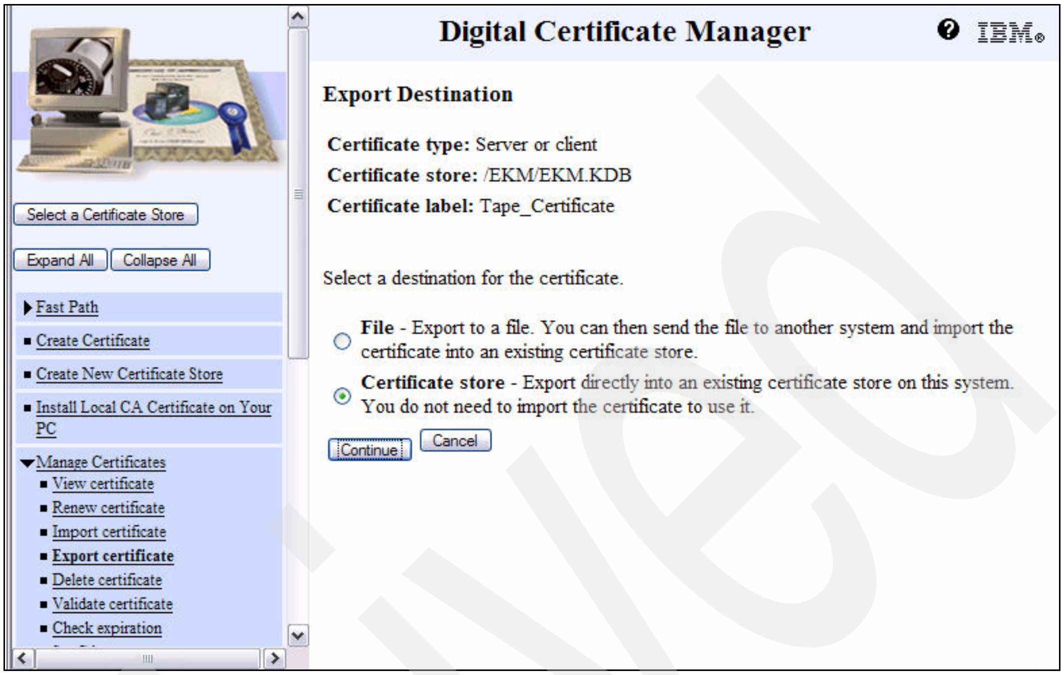
Select a certificate, then select Export to copy the certificate to a file or to another certificate store.

	Certificate	Common name
●	Tape_Certificate	Encryption_Certificate

View Export Cancel

Figure 7-42 DCM Export Server or Client Certificate

10. After clicking **Export**, select the option **Certificate Store** for the export destination to export the certificate into the previously created *OBJECTSIGNING certificate store as shown in Figure 7-43.



Export Destination

Certificate type: Server or client
Certificate store: /EKM/EKM.KDB
Certificate label: Tape_Certificate

Select a destination for the certificate.

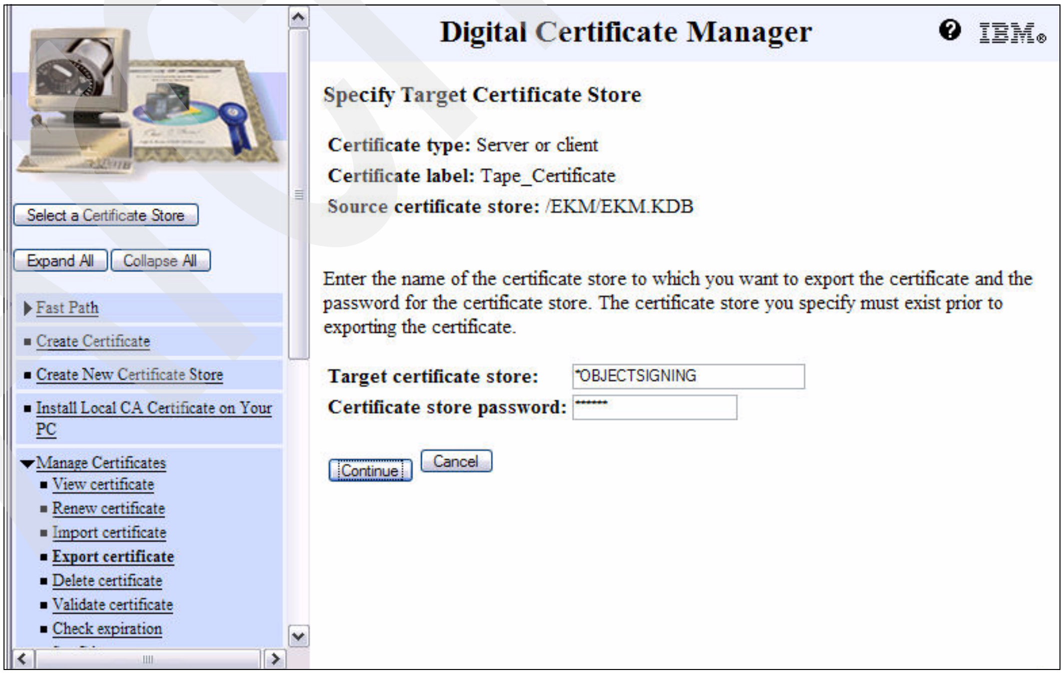
○ **File** - Export to a file. You can then send the file to another system and import the certificate into an existing certificate store.

● **Certificate store** - Export directly into an existing certificate store on this system. You do not need to import the certificate to use it.

Continue Cancel

Figure 7-43 DCM Export Destination screen

11. After clicking **Continue**, specify the target certificate store by entering **`*OBJECTSIGNING`** and your password as shown in Figure 7-44. DMC automatically replaces *OBJECTSIGNING by its full IFS file path name.



Specify Target Certificate Store

Certificate type: Server or client
Certificate label: Tape_Certificate
Source certificate store: /EKM/EKM.KDB

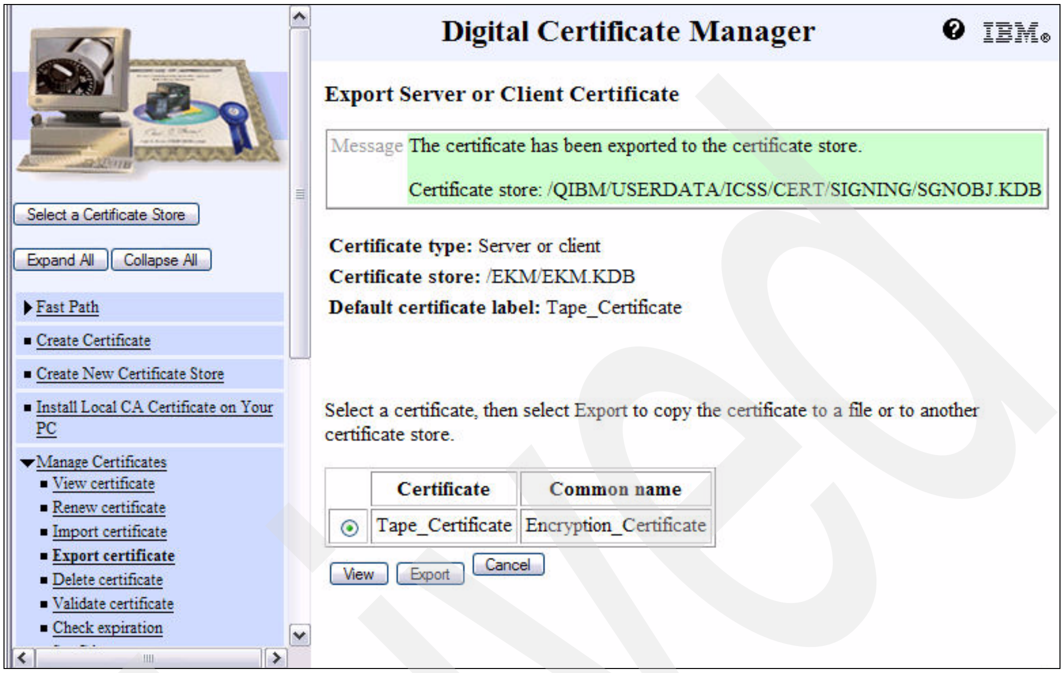
Enter the name of the certificate store to which you want to export the certificate and the password for the certificate store. The certificate store you specify must exist prior to exporting the certificate.

Target certificate store: *OBJECTSIGNING
Certificate store password: *******

Continue Cancel

Figure 7-44 DCM Specify Target Certificate Store screen

12. After clicking **Continue**, the message “The certificate has been exported to the certificate store” shown in Figure 7-45 confirms successful completion of the public/private key certificate into the *OBJECTSIGNING certificate store.



Digital Certificate Manager

Export Server or Client Certificate

Message The certificate has been exported to the certificate store.

Certificate store: /QIBM/USERDATA/ICSS/CERT/SIGNING/SGNOBJ.KDB

Certificate type: Server or client
Certificate store: /EKM/EKM.KDB
Default certificate label: Tape_Certificate

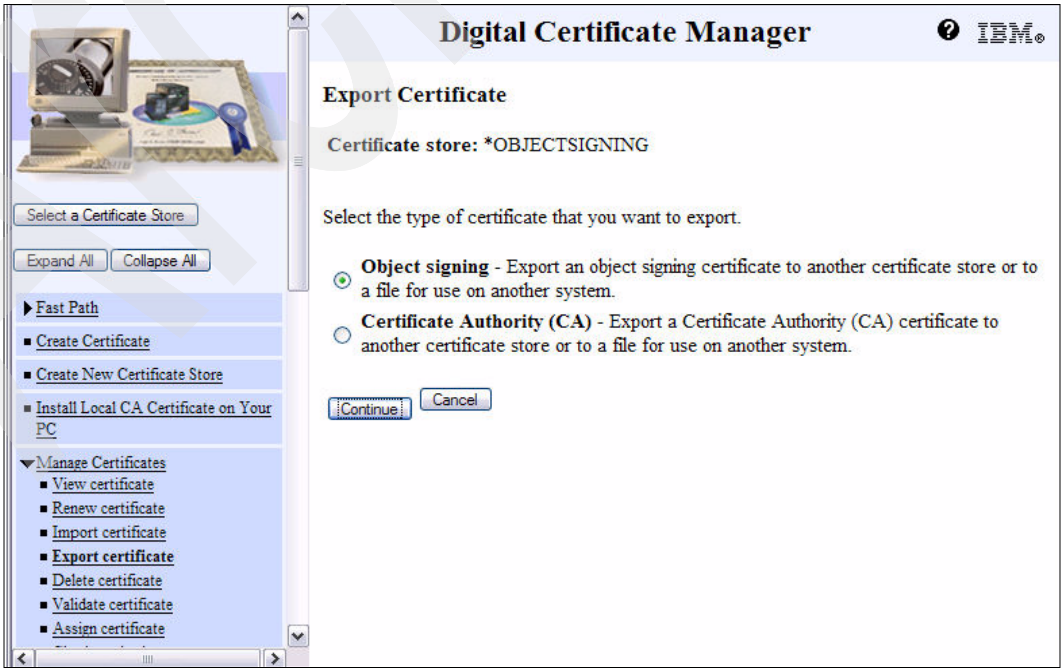
Select a certificate, then select Export to copy the certificate to a file or to another certificate store.

	Certificate	Common name
●	Tape_Certificate	Encryption_Certificate

Figure 7-45 DCM Export Server or Client Certificate screen

13. For the remaining tasks, switch to the *OBJECTSIGNING certificate store again via selecting **Select a Certificate Store** → ***OBJECTSIGNING**, clicking **Continue**, entering your password, and clicking **Continue**.

14. Export the public key only certificate via selecting **Manage Certificates** → **Export certificate** choosing the option **Object signing** as shown in Figure 7-46:



Digital Certificate Manager

Export Certificate

Certificate store: *OBJECTSIGNING

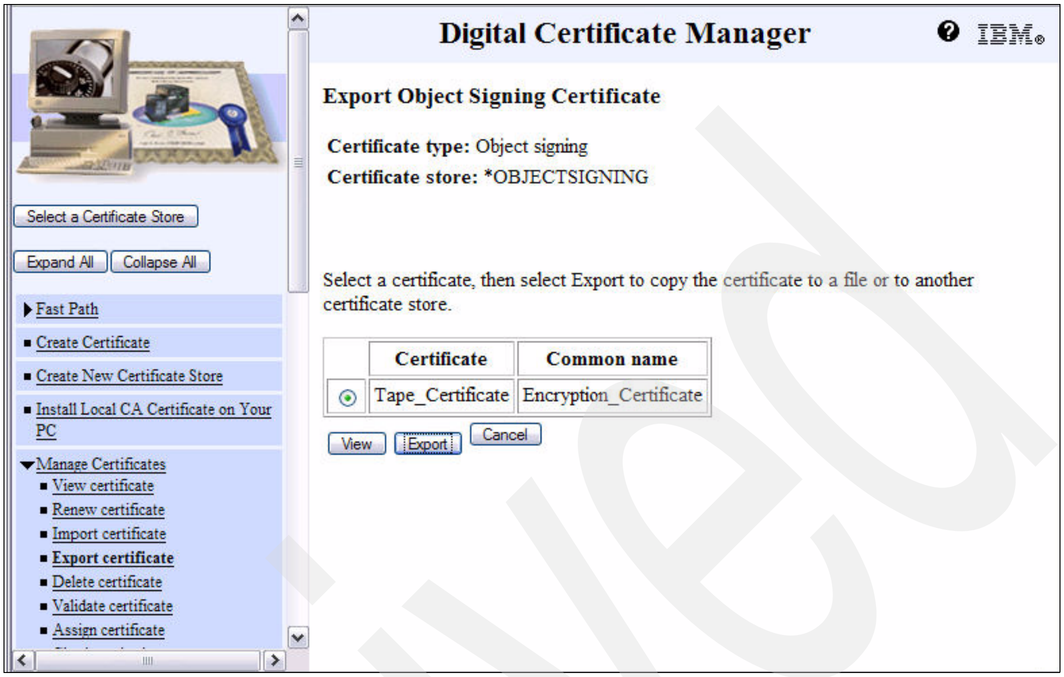
Select the type of certificate that you want to export.

● **Object signing** - Export an object signing certificate to another certificate store or to a file for use on another system.

○ **Certificate Authority (CA)** - Export a Certificate Authority (CA) certificate to another certificate store or to a file for use on another system.

Figure 7-46 DCM Export Certificate screen

15. After clicking **Continue**, select your certificate used for 3592 tape encryption for which the public key should be exported as shown in Figure 7-47.



Digital Certificate Manager

Export Object Signing Certificate

Certificate type: Object signing
Certificate store: *OBJECTSIGNING

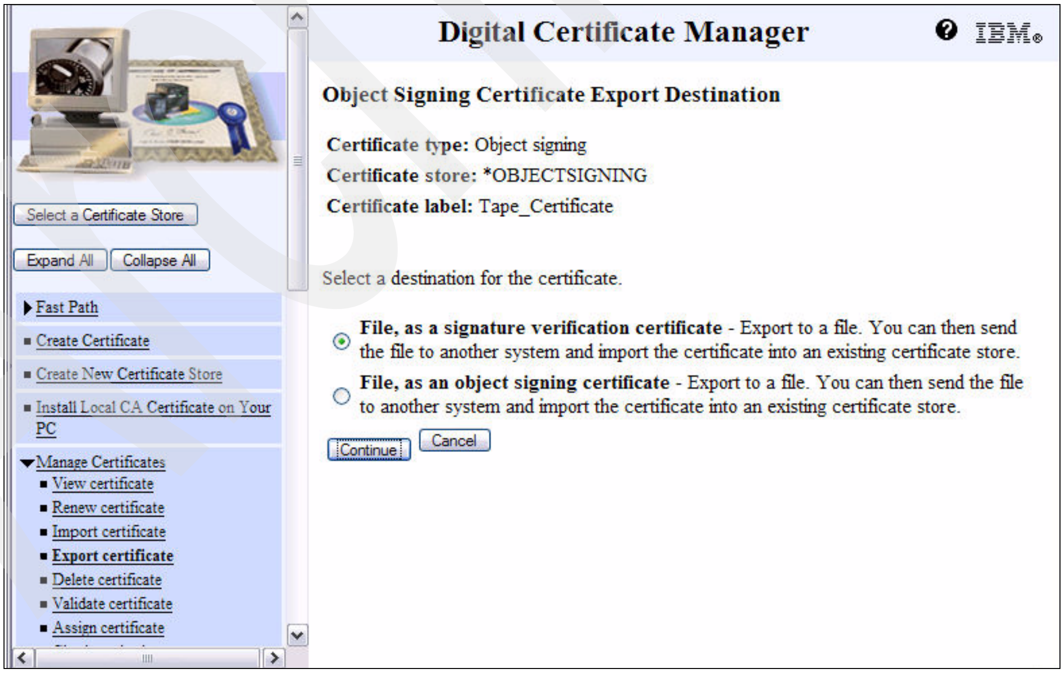
Select a certificate, then select Export to copy the certificate to a file or to another certificate store.

	Certificate	Common name
●	Tape_Certificate	Encryption_Certificate

View | Export | Cancel

Figure 7-47   DCM Export Object Signing Certificate screen

16. After clicking **Export**, select the option **File, as a signature verification certificate** for exporting the public key only as shown in Figure 7-48.



Digital Certificate Manager

Object Signing Certificate Export Destination

Certificate type: Object signing
Certificate store: *OBJECTSIGNING
Certificate label: Tape_Certificate

Select a destination for the certificate.

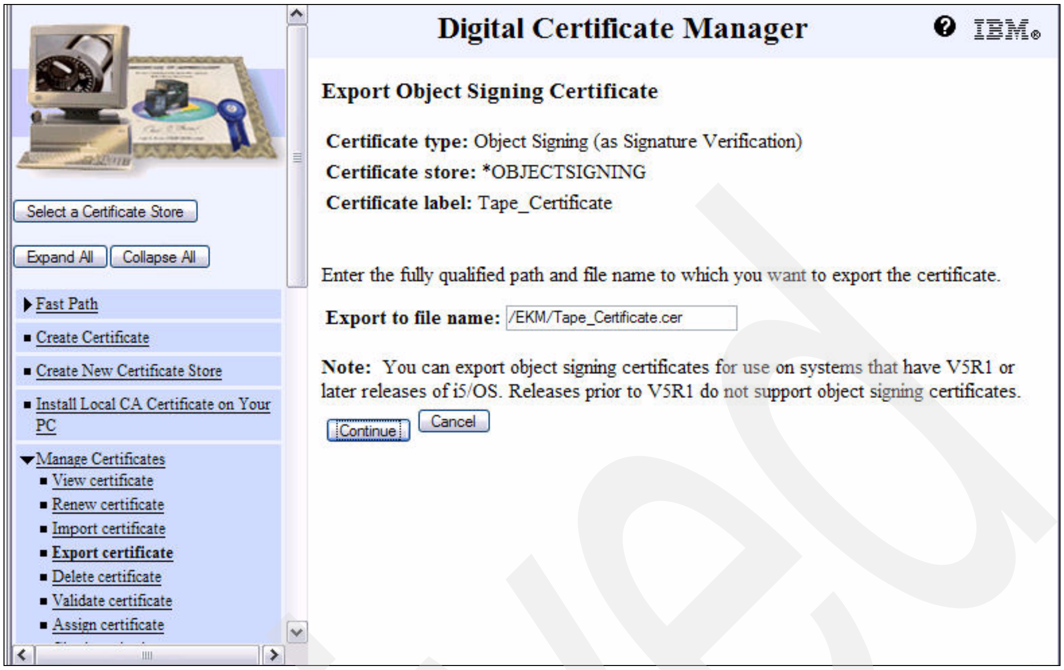
● **File, as a signature verification certificate** - Export to a file. You can then send the file to another system and import the certificate into an existing certificate store.

○ **File, as an object signing certificate** - Export to a file. You can then send the file to another system and import the certificate into an existing certificate store.

Continue | Cancel

Figure 7-48   DCM Object Signing Certificate Export Destination screen

17. After clicking **Continue**, specify the file name for exporting the certificate as shown in Figure 7-49.



Digital Certificate Manager

Export Object Signing Certificate

Certificate type: Object Signing (as Signature Verification)
Certificate store: *OBJECTSIGNING
Certificate label: Tape_Certificate

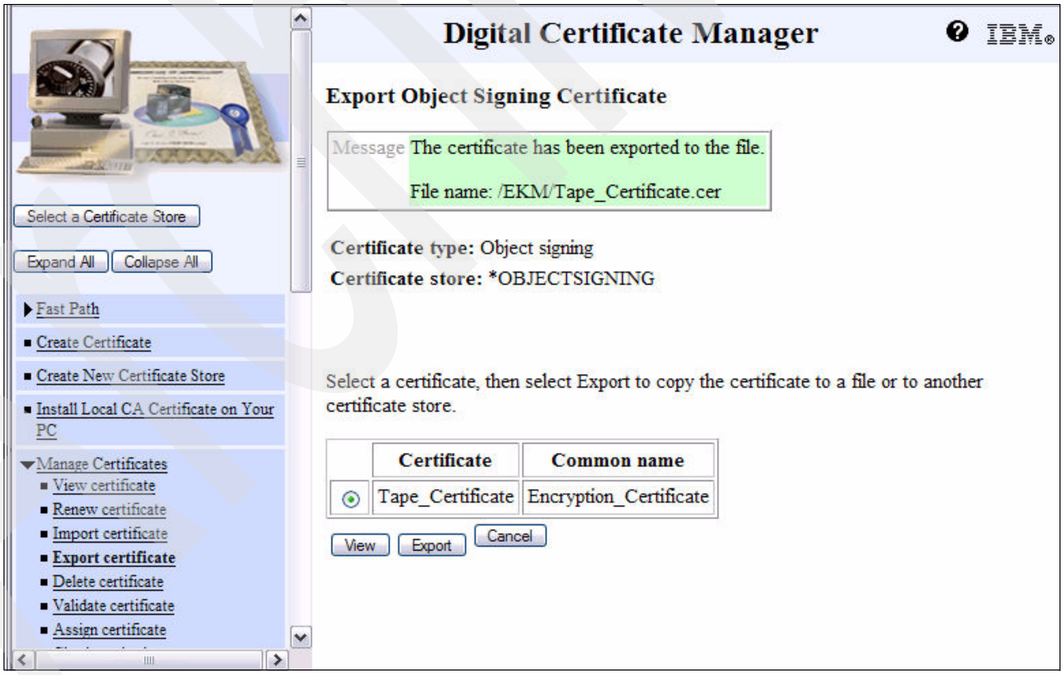
Enter the fully qualified path and file name to which you want to export the certificate.

Export to file name: /EKM/Tape_Certificate.cer

Note: You can export object signing certificates for use on systems that have V5R1 or later releases of i5/OS. Releases prior to V5R1 do not support object signing certificates.

Figure 7-49 DCM Export Object Signing Certificate screen

18.After clicking **Continue**, a successful export of the public key certificate is indicated by the message, `The certificate has been exported to the file`, as shown in Figure 7-50.



Digital Certificate Manager

Export Object Signing Certificate

Message The certificate has been exported to the file.
File name: /EKM/Tape_Certificate.cer

Certificate type: Object signing
Certificate store: *OBJECTSIGNING

Select a certificate, then select Export to copy the certificate to a file or to another certificate store.

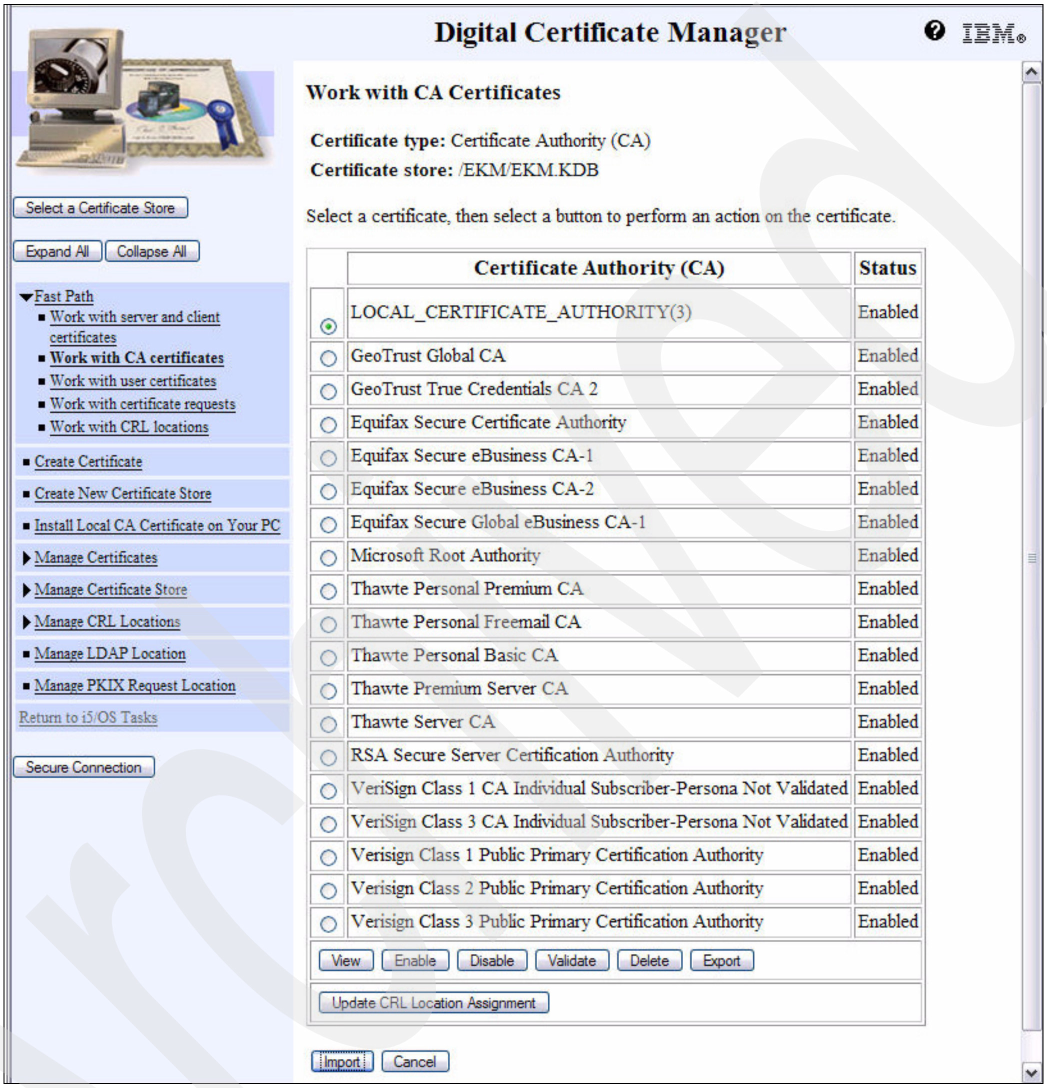
	Certificate	Common name
●	Tape_Certificate	Encryption_Certificate

Figure 7-50 DCM Export Object Signing Certificate confirmation screen

Note: For importing this exported public key certificate on another system, use FTP ASCII mode to transfer the file in the same way as the certificate has been exported in the *Base64_encoded* text format. For example, copying the file via iSeries Navigator to a PC would invalidate the certificate.

Importing a public key only to an IBMi5OSKeyStore

For importing a public key only certificate received in a *Base64_encoded* text file from a business partner to an *IBMi5OSKeyStore*, use the i5/OS *Digital Certificate Manager's* **Fast Path** → **Work with CA Certificates** → **Import** function shown in Figure 7-51 to import it into your EKM keystore.


Digital Certificate Manager
IBM
Select a Certificate Store
Expand All
Collapse All
Fast Path
Work with server and client certificates
Work with CA certificates
Work with user certificates
Work with certificate requests
Work with CRL locations
Create Certificate
Create New Certificate Store
Install Local CA Certificate on Your PC
Manage Certificates
Manage Certificate Store
Manage CRL Locations
Manage LDAP Location
Manage PKIX Request Location
Return to i5/OS Tasks
Secure Connection
View
Enable
Disable
Validate
Delete
Export
Update CRL Location Assignment
Import
Cancel

Work with CA Certificates

Certificate type: Certificate Authority (CA)
Certificate store: /EKM/EKM.KDB

Select a certificate, then select a button to perform an action on the certificate.

	Certificate Authority (CA)	Status
●	LOCAL_CERTIFICATE_AUTHORITY(3)	Enabled
○	GeoTrust Global CA	Enabled
○	GeoTrust True Credentials CA 2	Enabled
○	Equifax Secure Certificate Authority	Enabled
○	Equifax Secure eBusiness CA-1	Enabled
○	Equifax Secure eBusiness CA-2	Enabled
○	Equifax Secure Global eBusiness CA-1	Enabled
○	Microsoft Root Authority	Enabled
○	Thawte Personal Premium CA	Enabled
○	Thawte Personal Freemail CA	Enabled
○	Thawte Personal Basic CA	Enabled
○	Thawte Premium Server CA	Enabled
○	Thawte Server CA	Enabled
○	RSA Secure Server Certification Authority	Enabled
○	VeriSign Class 1 CA Individual Subscriber-Persona Not Validated	Enabled
○	VeriSign Class 3 CA Individual Subscriber-Persona Not Validated	Enabled
○	Verisign Class 1 Public Primary Certification Authority	Enabled
○	Verisign Class 2 Public Primary Certification Authority	Enabled
○	Verisign Class 3 Public Primary Certification Authority	Enabled

Figure 7-51 DCM Work with CA Certificates screen

Exporting/importing a public key only from a JCEKS keystore

For *Java Cryptography Extension Keystores* (*JCEKS)*, use the IBM Java *keytool* command to export a public key only certificate as follows:

- For *exporting a public key only* certificate:

  keytool -export -alias *keylabel* **-file** *filename* **-keystore** *keystore* **-storepass** *password* **-storetype JCEKS**

- For *importing a public key only* certificate:

  keytool -import -alias *keylabel* **-file** *filename* **-keystore** *keystore* **-storepass** *password* **-storetype JCEKS**

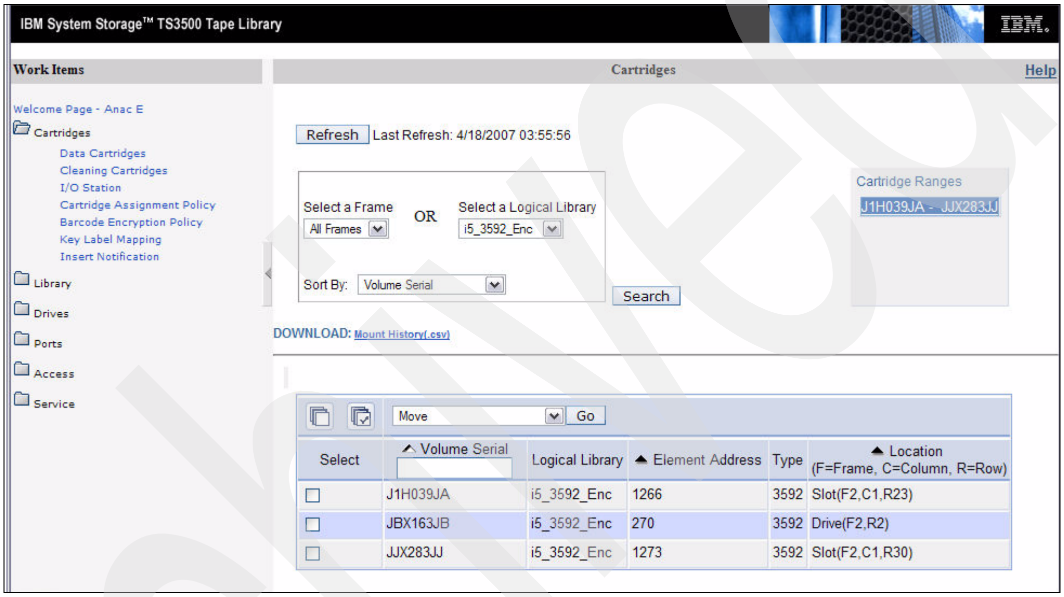
7.4.5 Working with encrypted tape cartridges

This section shows some basic examples of working with encrypted tape cartridges, such as viewing their encryption status or re-keying 3592 tape cartridges.

Viewing tape cartridge encryption status

This example shows how to view the tape cartridge encryption status using the IBM UltraScalable Specialist GUI on an IBM TS3500 Tape Library.

- Selecting the menu **Cartridges** → **Data Cartridges** using the option to select a logical library shows its assigned data cartridges as shown for a 3592 drive logical library in Figure 7-52 and LTO4 drive logical library in Figure 7-53.



Last Refresh: 4/18/2007 03:55:56

Select a Frame: All Frames

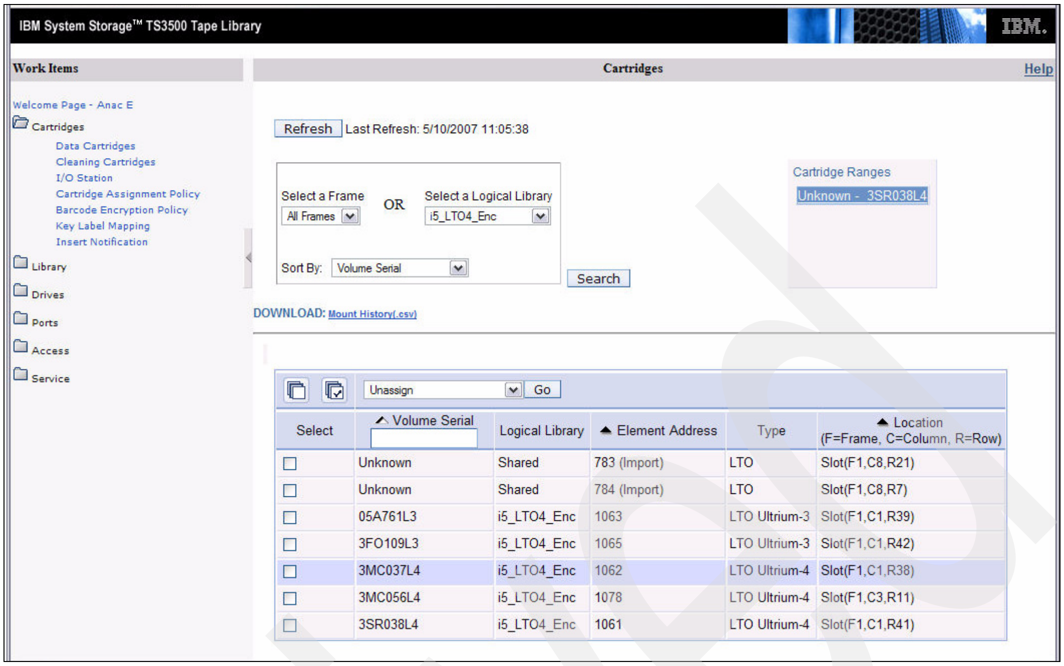
Select a Logical Library: i5_3592_Enc

Sort By: Volume Serial

Cartridge Ranges: J1H039JA - JJX283JJ

Select	Volume Serial	Logical Library	Element Address	Type	Location (F=Frame, C=Column, R=Row)
□	J1H039JA	i5_3592_Enc	1266	3592	Slot(F2,C1,R23)
□	JBX163JB	i5_3592_Enc	270	3592	Drive(F2,R2)
□	JJX283JJ	i5_3592_Enc	1273	3592	Slot(F2,C1,R30)

Figure 7-52 IBM Ultra™ Scalable Specialist - 3592 Logical Library Cartridges screen



Last Refresh: 5/10/2007 11:05:38

Select a Frame: All Frames OR Select a Logical Library: i5_LTO4_Enc

Sort By: Volume Serial

Cartridge Ranges: Unknown - 3SR038L4

DOWNLOAD: Mount History(.csv)

Unassign

Select	Volume Serial	Logical Library	Element Address	Type	Location (F=Frame, C=Column, R=Row)
□	Unknown	Shared	783 (Import)	LTO	Slot(F1,C8,R21)
□	Unknown	Shared	784 (Import)	LTO	Slot(F1,C8,R7)
□	05A761L3	i5_LTO4_Enc	1063	LTO Ultrium-3	Slot(F1,C1,R39)
□	3FO109L3	i5_LTO4_Enc	1065	LTO Ultrium-3	Slot(F1,C1,R42)
□	3MC037L4	i5_LTO4_Enc	1062	LTO Ultrium-4	Slot(F1,C1,R38)
□	3MC056L4	i5_LTO4_Enc	1078	LTO Ultrium-4	Slot(F1,C3,R11)
□	3SR038L4	i5_LTO4_Enc	1061	LTO Ultrium-4	Slot(F1,C1,R41)

Figure 7-53 IBM UltraScalable Specialist - LTO4 Logical Library Cartridges Screen

> **Note:** The “Encryption” column in the cartridges screen for an encryption-enabled logical library is not shown before the first data cartridge has been written to and unloaded from the drive.

- Adding tape cartridges from the *INSERT category to the *SHARED category to make them available for usage with the TAPMLB73 3592 logical library and TAPMLB71 LTO4 logical library and initializing a 3592 and LTO4 data cartridges using the new media density FMT3592A2E for 3592 encryption as follows:

  ADDTAPCTG DEV(*TAPMLB73***) CTG(***J1H039 JEX163 JJX283***)**

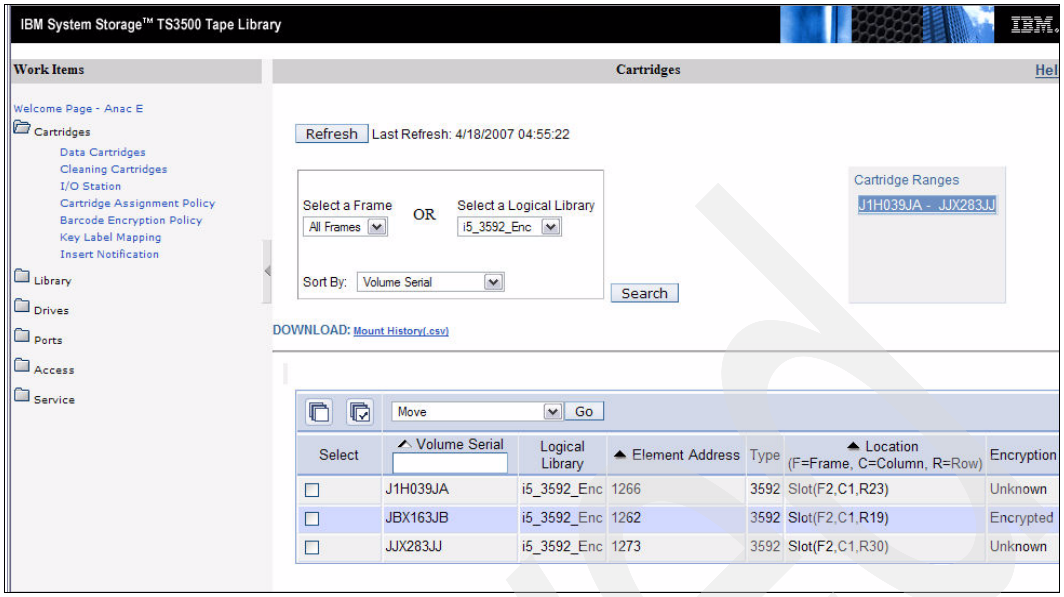
  ADDTAPCTG DEV(*TAPMLB71***) CTG(***3MC037 3MC055 3SR038***)**

  INZTAP DEV(*TAPMLB73***) NEWVOL(***JBX163***) VOL(***JBX163***) CHECK(*NO) DENSITY(FMT3592A2E)**

  INZTAP DEV(*TAPMLB71***) NEWVOL(***3MC037***) VOL(***3MC037***) CHECK(*NO)**

> **Note:** Though there are two new media densities FMT3592A1E and FMT3592A2E available on i5/OS for encryption-enabled 3592 tape drives only the format FMT3592A2E is supported. FMT3592A1E was originally intended for usage with the 3592-J1A emulation mode of the 3595-E05 drive but IBM made the decision to not support encryption in the emulation mode.

- Unloading the initialized cartridges from the drives using the IBM UltraScalable Specialist Cartridges **Move** option from the IBM UltraScalable Specialist “Cartridges” screen the *initialized* cartridges now have the encryption status *Encrypted* as shown for the 3592 cartridge VOLSER JBX163 in Figure 7-54 and for the LTO4 cartridge VOLSER 3MC037 in Figure 7-55.



Last Refresh: 4/18/2007 04:55:22

Select a Frame: All Frames OR Select a Logical Library: i5_3592_Enc

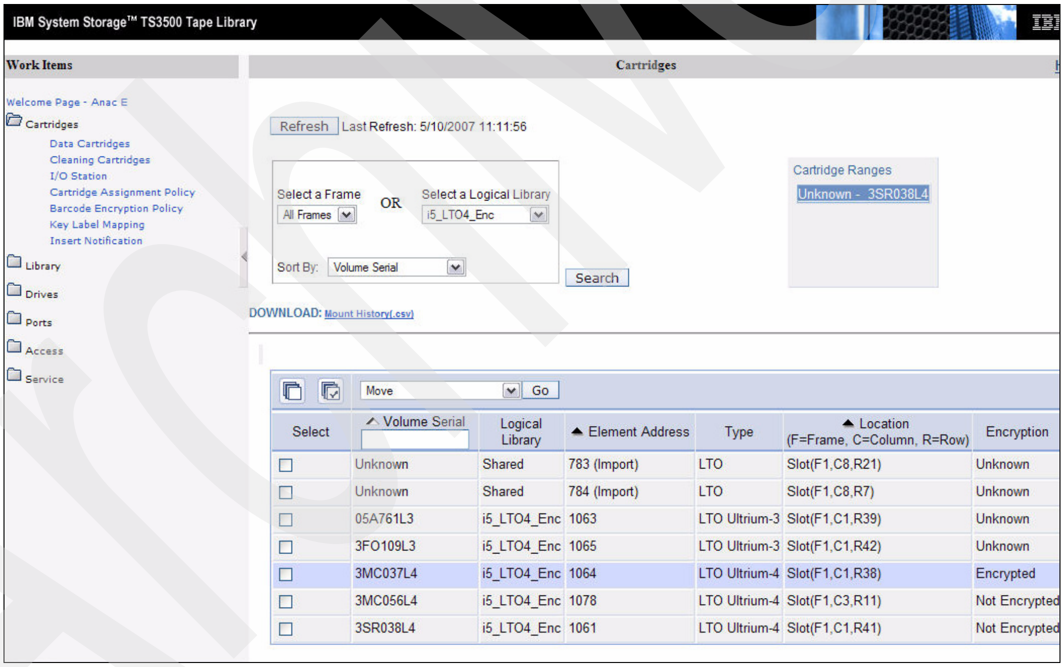
Sort By: Volume Serial

Cartridge Ranges: J1H039JA - JJX283JJ

DOWNLOAD: Mount History(.csv)

Select	Volume Serial	Logical Library	Element Address	Type	Location (F=Frame, C=Column, R=Row)	Encryption
□	J1H039JA	i5_3592_Enc	1266	3592	Slot(F2,C1,R23)	Unknown
□	JBX163JB	i5_3592_Enc	1262	3592	Slot(F2,C1,R19)	Encrypted
□	JJX283JJ	i5_3592_Enc	1273	3592	Slot(F2,C1,R30)	Unknown

Figure 7-54 IBM UltraScalable Specialist - 3592 Cartridges Screen with Encryption Information



Last Refresh: 5/10/2007 11:11:56

Select a Frame: All Frames OR Select a Logical Library: i5_LTO4_Enc

Sort By: Volume Serial

Cartridge Ranges: Unknown - 3SR038L4

DOWNLOAD: Mount History(.csv)

Select	Volume Serial	Logical Library	Element Address	Type	Location (F=Frame, C=Column, R=Row)	Encryption
□	Unknown	Shared	783 (Import)	LTO	Slot(F1,C8,R21)	Unknown
□	Unknown	Shared	784 (Import)	LTO	Slot(F1,C8,R7)	Unknown
□	05A761L3	i5_LTO4_Enc	1063	LTO Ultrium-3	Slot(F1,C1,R39)	Unknown
□	3FO109L3	i5_LTO4_Enc	1065	LTO Ultrium-3	Slot(F1,C1,R42)	Unknown
□	3MC037L4	i5_LTO4_Enc	1064	LTO Ultrium-4	Slot(F1,C1,R38)	Encrypted
□	3MC056L4	i5_LTO4_Enc	1078	LTO Ultrium-4	Slot(F1,C3,R11)	Not Encrypted
□	3SR038L4	i5_LTO4_Enc	1061	LTO Ultrium-4	Slot(F1,C1,R41)	Not Encrypted

Figure 7-55 IBM TS3500 Specialist - LTO4 Cartridges Screen with Encryption Information

Note: The cartridge encryption status displayed in the “Encryption” column is updated only when the cartridge is unloaded from a drive. The status *Unknown* is displayed for cartridges in an encryption-enabled logical library as long as they have not been loaded/unloaded from a drive.

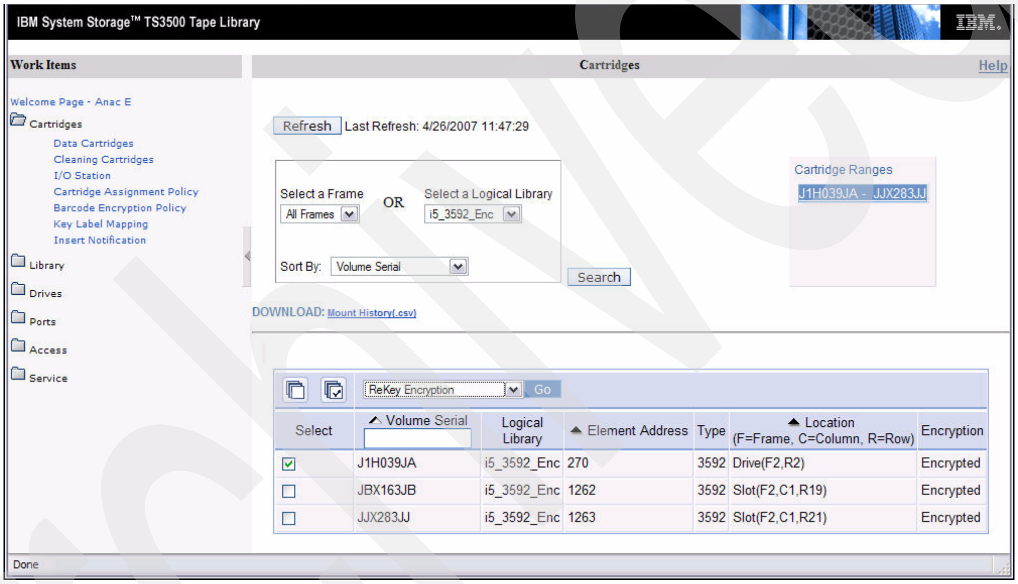
Re-keying encrypted 3592 cartridges

This example shows using the IBM TS3500 Tape Library Specialist Web interface for re-keying encrypted 3592 tape cartridges that you can use, for example, after having imported a public key certificate from a business partner for sharing already encrypted tape cartridges. Use the Enterprise Tape Library Specialist for re-keying of cartridges residing in a 3494 Tape Library.

> **Note:** The cartridge must have been mounted into the drive prior to the sequence described next.

For the TS3500, follow these steps:

1. Encrypted 3592 tape cartridges loaded into a Library-managed Encryption-enabled drive are *re-keyed* via the IBM Tape Library Specialist Web GUI **Manage Cartridges** → **Data Cartridges** menu option **Rekey Encryption** shown in Figure 7-56.



Last Refresh: 4/26/2007 11:47:29

Select a Frame: All Frames OR Select a Logical Library: i5_3592_Enc

Sort By: Volume Serial

Cartridge Ranges: J1H039JA - JJX283JJ

DOWNLOAD: Mount History(.csv)

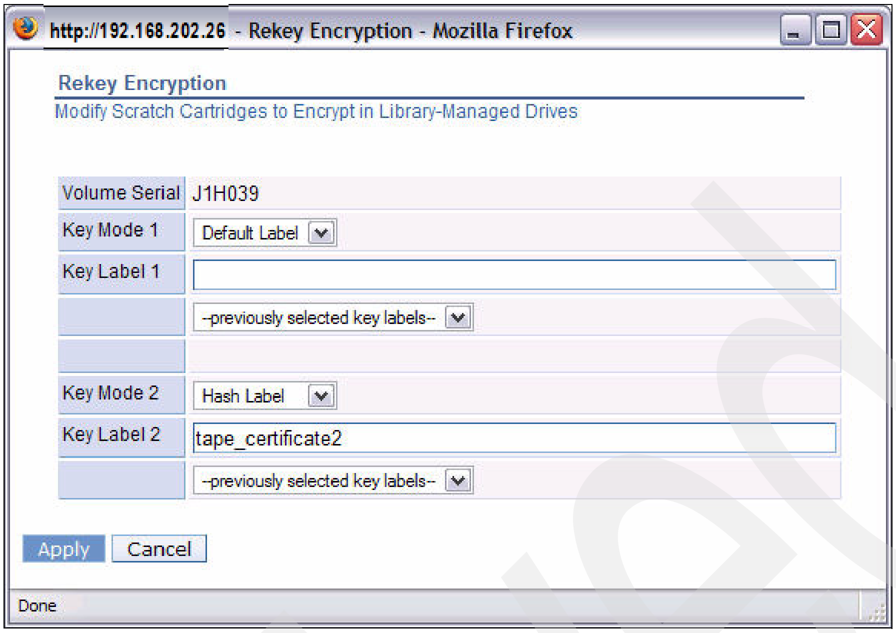
ReKey Encryption

Select	Volume Serial	Logical Library	Element Address	Type	Location (F=Frame, C=Column, R=Row)	Encryption
☑	J1H039JA	i5_3592_Enc	270	3592	Drive(F2,R2)	Encrypted
☐	JBX163JB	i5_3592_Enc	1262	3592	Slot(F2,C1,R19)	Encrypted
☐	JJX283JJ	i5_3592_Enc	1263	3592	Slot(F2,C1,R21)	Encrypted

Figure 7-56 IBM TS3500 Specialist - Cartridges screen with selected ReKey Encryption option

2. After clicking **Go**, new key settings can be specified for the *Key Mode* and *Key Label* for each of the two key labels used to refer to EEDK1 and EEDK2 shown in Figure 7-57. In the example, a *hash label* key mode was chosen for a new EEDK2 so that a hash computed value of the public key part of the specified "tape_certificate2" key label, for example, which refers to the imported public key certificate from the business partner, is stored within the EEDK2 instead of the clear label itself.

> **Note:** Using a *hash label* is recommended for sharing tape cartridges with business partners because it eliminates the requirement of using the same key label as the business partner.



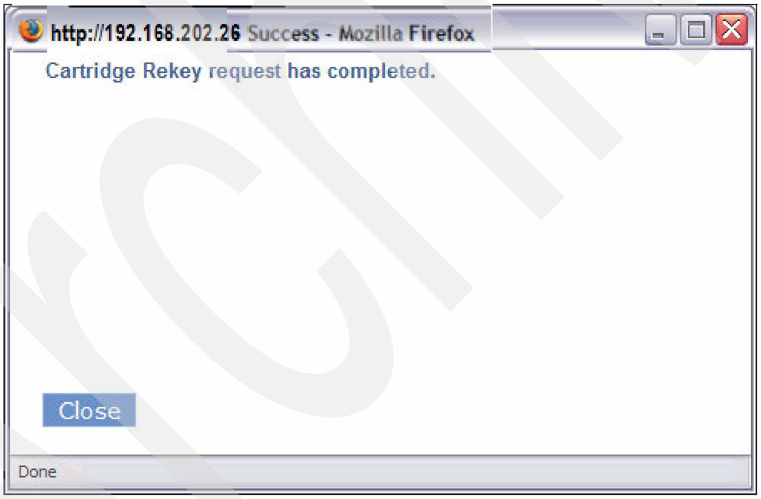
Rekey Encryption

Modify Scratch Cartridges to Encrypt in Library-Managed Drives

Volume Serial	J1H039
Key Mode 1	Default Label
Key Label 1	
	--previously selected key labels--
Key Mode 2	Hash Label
Key Label 2	tape_certificate2
	--previously selected key labels--

Figure 7-57 IBM UltraScalable Specialist - Rekey Encryption window

3. Successful completion of the 3592 cartridge re-keying request is indicated by the message, `Cartridge Rekey request has completed`, as shown in Figure 7-58.

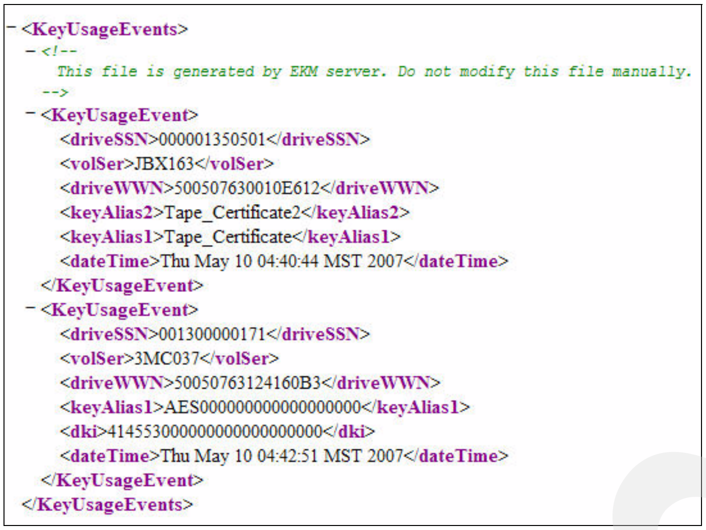


Cartridge Rekey request has completed.

Figure 7-58 IBM UltraScalable Specialist - Rekey Encryption Success window

Example of the EKM audit metadata XML file

With EKM Release 2, an audit metadata XML log file has been introduced for logging key usage events for 3592 and LTO4 cartridge serial numbers. Refer to “Customizing the EKM configuration file” on page 230, item 2, for information about the new *EKMDataParser* Java tool, which can be used for querying this file for a particular VOLSER or key alias. Figure 7-59 shows an example of the audit metadata XML file with key usage events logged for 3592 cartridge VOLSER `JBX163` and LTO4 cartridge VOLSER `3MC037`:



```
- <KeyUsageEvents>
  - <!--
      This file is generated by EKM server. Do not modify this file manually.
    -->
  - <KeyUsageEvent>
      <driveSSN>000001350501</driveSSN>
      <volSer>JBX163</volSer>
      <driveWWN>500507630010E612</driveWWN>
      <keyAlias2>Tape_Certificate2</keyAlias2>
      <keyAlias1>Tape_Certificate</keyAlias1>
      <dateTime>Thu May 10 04:40:44 MST 2007</dateTime>
    </KeyUsageEvent>
  - <KeyUsageEvent>
      <driveSSN>001300000171</driveSSN>
      <volSer>3MC037</volSer>
      <driveWWN>50050763124160B3</driveWWN>
      <keyAlias1>AES000000000000000000</keyAlias1>
      <dki>414553000000000000</dki>
      <dateTime>Thu May 10 04:42:51 MST 2007</dateTime>
    </KeyUsageEvent>
  </KeyUsageEvents>
```

Figure 7-59 Example of EKM audit metadata XML file

7.4.6 Troubleshooting,

When encountering problems with EKM check the EKM standard outputs, on the EKM admin console or in the files `/EKM/stdout.log` and `/EKM/stderr.log` if EKM was started as a batch job, and the EKM audit log file, which is typically `/EKM/auditlogs/ekm_audit.log`.

For failure isolation, refer to the "Problem Determination" chapter in *IBM Encryption Key Manager component for the Java platform: Introduction, Planning and User's Guide*, GA76-0418 (EKM IPUG) at:

http://www-1.ibm.com/support/docview.wss?rs=1139&context=STCXRGL&dc=D400&uid=ssg1S4000504

For debugging *EKM error messages* that are displayed on the admin console or logged in the standard error outfile when starting EKM or issuing EKM admin commands, refer specifically to "Debugging EKM Server problems" and "Messages" of the problem determination chapter from the EKM IPUG.

EKM runtime errors show up as error code = Exyz in the EKM audit log. For debugging EKM runtime errors, refer to "EKM-Reported Errors" of the problem determination chapter from the EKM IPUG.

Usually the following data should be collected if further assistance is required from IBM support:

- Audit log (typically `/EKM/auditlogs/ekm_audit.log`)
- EKM configuration file (typically `/EKM/KeyManagerConfig.properties`)
- Standard output files if EKM was running as a batch job (typically `/EKM/stdout.log` and `/EKM/stderr.log`)
- Debug log if debugging was enabled (typically `/EKM/debug.log`)

8

IBM TS7520 implementation with i5/OS

In this chapter we discuss implementation and usage of the TS7520 Virtualization Engine with i5/OS. We describe planning for the TS7520 Virtualization Engine with i5/OS, setup, and connection of a virtual tape library to i5/OS, and we also provide two examples of implementing virtual tape libraries with i5/OS.

For detailed information about the TS7520 Virtualization Engine, refer to the *IBM Virtualization Engine TS7520: Planning, Implementation, and Usage Guide*, SG24-7520.

8.1 Planning and sizing the TS7500 for i5/OS

Good planning for backup and recovery processes that *fit your business* are critical if you require a system up and running most of the time. As the time for running in production mode within a 24-hour day and within a 7-day week increases, this planning becomes even more critical.

Reading this section cannot make you an expert in overall backup and recovery planning. However, we do review many basic planning considerations that lead into planning for effective use of the TS7500 in your overall backup and recovery planning process.

8.1.1 How a virtual tape library fits in with i5/OS backup and recovery strategy

In this section we give you a *short list* of things that you must consider, so we can discuss them in the context of using the IBM Virtualization Engine TS7520 within your strategy. In other words, the use of a *virtual tape device* should expedite the actual saving and restoring of objects necessary for recovery, but you have to ensure that the processes you develop include the *right objects*, saving at the *right time*, and testing your recovery processes before the actual requirement for a *business recovery*.

We recommend that you consider the following steps when developing a backup and recovery strategy for a System i environment running i5/OS in at least one partition:

- Determine what to save and how often to save it.
- Determine your save window. This is the amount of time:
  - Objects being saved can be unavailable for use.
  - The entire system can be unavailable for i5/OS *save system* functions.

  Note that i5/OS has *save while active* functions for many objects. However, further coverage of those capabilities are beyond the scope of this book. For more discussion of all save and restore considerations while running applications under i5/OS, refer to the iSeries Information Center Systems management - Availability and Systems Management - Backup and Recovery topics. Recommended documents located there include:

  - IBM Systems - iSeries Systems management: *Plan a backup and recovery strategy* PDF
  - IBM Systems - iSeries: *Backup and Recovery Version 5 Revision 4*, SC41-5304-08, PDF
- Consider recovery time and choose availability options.
- Test developed backup and recovery strategy.

After determining what to save and how often to save, the customer probably decides on an approach similar to this:

- Daily save the libraries and objects that regularly change, such as application libraries, user profiles, configuration objects, and so on
- Save the entire system every week

Typically, the objects that regularly change have to be restored more frequently and in a shorter period of time, compared to objects that do not change frequently. A virtual tape library can provide faster save and restore than a physical tape library in some cases. Therefore, it might be a good idea to save the frequently changing objects regularly to a virtual tape library and save the entire system objects to a physical tape drive.

Note that i5/OS supports parallel and concurrent save operations to properly set up virtual tape library configurations as it does for physical tape environments and V5R4 i5/OS virtual tape image catalog support.

Some customers who require a relatively short save window and do not want to invest in fast tape drives, might want to perform both daily and weekly saves to the virtual tape library, and duplicate weekly saves to physical tapes, or duplicate both daily and weekly saves to physical tapes.

Depending on a properly estimated or actual experience with recovery time periods, you have to decide how long a time period to keep virtual tapes. This requires sizing the required disk space in TS7500 accordingly.

Customers with many systems or partitions might want to use virtual tape libraries to enable save of all systems in the same general save window time period, each of them to a different virtual tape library.

All backup and recovery approaches require careful management of tapes, especially in the virtual tape library environment because both virtual and physical tapes are used. This is especially valid for customers with many systems, each of them using virtual tape library and physical tape library.

For examples that can help determine your processes, see 8.3, “Usage examples” on page 290.

8.1.2 Planning for copying virtual tapes to physical tapes

The data on virtual tapes in TS7500 can be exported to tapes in a physical tape library attached to the TS7500, to provide long-term archiving of data. For this, the virtual tape has to be ejected by Backup Recovery and Media Services or BRMS (or backup software on non-i5/OS partitions), which moves it to a virtual vault in IBM Virtualization Engine TS7520. When the virtual tape is in the virtual vault, we can export it to physical tape by using commands from the IBM TapeSystem Virtualization Engine for Tape Console. Alternatively, we can set up to automatically export to a physical tape as soon as the virtual tape is in the virtual vault. For more information about this, refer to the *IBM Virtualization Engine TS7520: Planning, Implementation, and Usage Guide*, SG24-7520.

From an i5/OS viewpoint, we recommend that you connect a physical tape library to the i5/OS partition and duplicate virtual tape data to real physical media on the attached tape device. You do this using the BRMS DUPMEDBRM command or the i5/OS Duplicate Tape (DUPTAP) command.

Presently, i5/OS does not formally support reading tape media data produced by the TS7500 writing directly to a physically attached tape device.

8.1.3 Planning for failover

A customer can decide for a *high availability configuration* of TS7500, which includes two Virtualization Engines CV6, two Cache Controller SV6s, and optionally Cache Module SX6s. With this configuration, the customer can set up failover, which reduces downtime that can occur should the Virtualization Engine fail. In the failover setup, two Virtualization Engines CV6 are configured to monitor each other. If one Virtualization Engine fails, the other takes over its identity.

For more information about how to set up failover, refer to the *IBM Virtualization Engine TS7520: Planning, Implementation, and Usage Guide*, SG24-7520.

Exactly how this feature provides high availability to a certain host server depends on the backup management software on the server. With some backup management software, the failover is transparent, but with others, failover requires restarting the backup job in i5/OS. Given the scope of a "getting started" manual, failover scenarios are not covered in this book.

The TS7520 is built with *redundant pathing* from each Virtualization Engine CV6 to each SV6.

Base configuration of TS75010 contains one Virtualization Engine CV6 and two Cache Controller SV6s. In case a path from Virtualization Engine to each controller fails, or a Cache Controller fails, Virtualization Engine still has access to disk storage within TS7520.

The same is true for high availability configuration of TS7520 where each Virtualization Engine connects to each Cache Controller with redundant paths.

8.1.4 Planning for the TS7520 Virtualization Engine with System i

Next we describe the possibilities in functionality and throughput that a TS7500 can offer. They are important for planning the number and configuration of virtual tape libraries used by i5/OS.

In principle, each virtual tape library can attach to multiple host adapters, and it can attach to each host adapter via multiple ports in the TS7520. We decide which host FC adapters - Input Output Processors (IOAs) can access a virtual tape library when we assign storage area network (SAN) clients to virtual tape library using the Virtualization Engine console. We decide which ports in TS7520 each host adapter can see, by zoning SAN switches, and by selecting target FC ports when we create a SAN client in the Virtualization Engine console. For more information about how to do this, refer to the *IBM Virtualization Engine TS7520: Planning, Implementation, and Usage Guide*, SG24-7520.

In a System i environment, we attach a virtual tape library to many host servers only if we plan to share the library among them. We do not attach some tape drives from a virtual tape library to one i5/OS and some drives to another i5/OS, as is possible with other host servers. This is because only one control path is possible in a virtual tape library and each i5/OS must have a control path defined.

We do not expect many customers to share a virtual tape library among multiple i5/OS partitions. Rather, they would define a virtual tape library for each i5/OS and, if necessary, move virtual tape drives from one to another virtual tape library by using the Virtualization Engine console.

Because each IOA in i5/OS establishes only one path to a virtual tape library, it makes sense to zone switches or select target FC ports so that each IOA sees a virtual tape library through only one FC port in TS7500.

Regarding this, we recommend that you assign one or more virtual tape libraries to one IOA in i5/OS, each containing one or two tape drives. For planning the number of tape drives in a virtual tape library, consider also parallel and concurrent save described in later in this section.

You might also want to assign each virtual tape library to one IOA, multiple assignment using the same port in TS7500. These possibilities are shown in Figure 8-1.

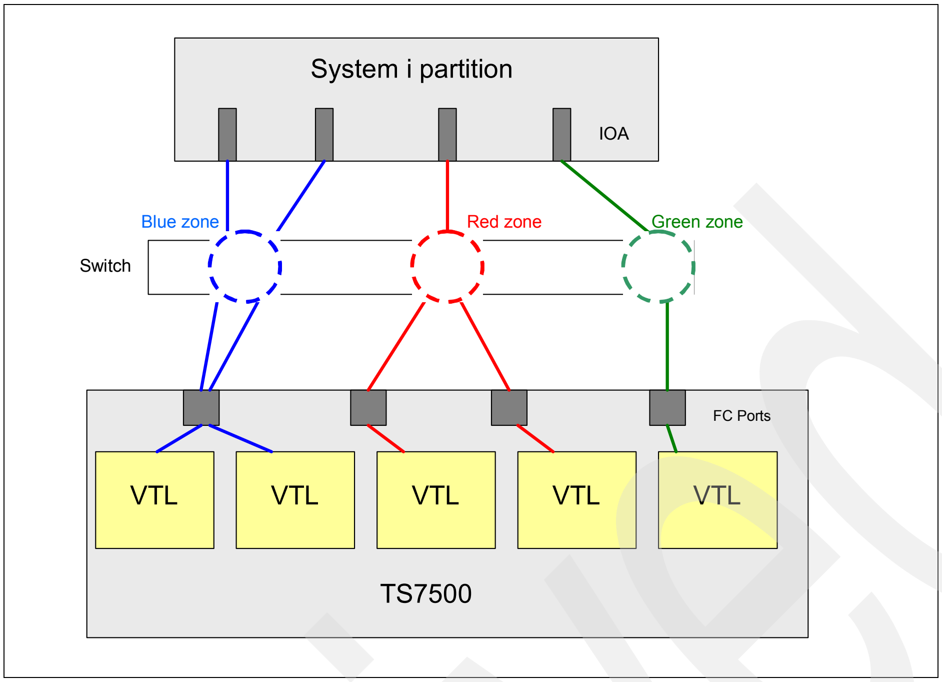


Figure 8-1 Connecting virtual tape libraries to System i partitions

8.1.5 Parallel and concurrent save

Parallel save and restore is the ability to save or restore a single object or library in i5/OS to multiple backup devices from the same job. This includes saving only *changed objects*. This technique can drastically reduce the time required to save an object, it is especially efficient with saving large files.

When you use this function, it is essential to have a tracking mechanism to, for recovery purposes, know what objects are on what tape volumes. In the context of this book, Backup and Recovery Media Services is the strategic product for i5/OS that we assume is used in this book.

Parallel save can be done to multiple virtual tape drives from different virtual tape libraries, or it can be done to multiple virtual tape drives within the same virtual tape library. With parallel save to virtual tape drives from different virtual tape libraries, you might experience better save performances than with saving to multiple virtual drives within the same virtual tape library, providing that each virtual tape library is connected to separate FC adapters via separate port in TS7500. However, when using virtual tape drives from different virtual tape libraries, consider that you must do restore from tapes in different media location.

You can also decide to parallel save to virtual tape drives within the same virtual tape library. This save might not perform as quickly as saving to different virtual tape libraries, but it provides easier management of tapes for restore.

Concurrent save and restore is the ability to save or restore different libraries or directories to multiple backup devices at the same time from different jobs. Concurrent save and restore also means saving or restoring different objects from a single library or directory to multiple backup devices at the same time from different jobs. You can consider doing concurrent saves to virtual tape drives from different virtual tape libraries. It might be enough to plan one tape drive in each virtual tape library to be used for concurrent saves.

8.1.6 Sizing the disk capacity in IBM Virtualization Engine TS7520

When sizing the required disk space in SV6 and SX6, it is important to keep in mind that a virtual tape does not have fixed capacity. When created, a tape has capacity of 5 GB by default, unless you specify different capacity when you create it. When data is saved to the tape, its capacity increases as required. This is different to physical tapes which have fixed capacity.

Therefore, with virtual tapes you just size the amount of disk space required, regardless of how many tapes must be defined. This is the opposite to sizing physical tapes where you size the number of tapes required.

To properly size the required disk space, you have to estimate how long you intend to keep any backed up data within the IBM Virtualization Engine TS7520. This depends on your company's backup policies, and the critical nature of the data and the frequency at which it would have to be restored to the system.

When determining how long saved data should stay in the IBM Virtualization Engine TS7520 before exporting to physical tape or deleting it, you should consider at least the following issues:

- Usually, some data used by a critical application must be restored faster than others. Typically, this data would be kept on virtual tapes, and other less critical data or less frequently required data can be exported to physical tapes on slower physical tape drives.

  Often the data that has to be restored quickly expires (becomes obsolete information) in a few days and is replaced by a more recent version of that data. Then the obsoleted data can simply be erased from the TS7520 disks.

- Each company has agreements about how quickly specific backup data has to be restored. Typically, this is included in agreements often called *service-level agreements*. For example:

  – Backup of Domino mail which is kept for less than 2 weeks must be restored in 1 hour.
  – Mail which is kept for longer than 2 weeks can be restored in 3 hours.

We recommend sizing disk space within IBM Virtualization Engine TS7520 for each i5/OS partition separately. The following formulas can help you to estimate how much disk space is required for a specific i5/OS partition:

- If full backup is done every day:

  Formula: (daily amount of backup data) x (number of days the backup is kept) = disk capacity required for current backup environment

  Example: A customer saves daily 500 GB of data, and he keeps the saved data for 14 days. Disk capacity required for current backup environment is as follows:

  500 GB x 14 = 7000 GB = 7 TB

- If incremental backup is done every day, and full backup is done every week:

  Formula: (weekly amount of backup data) x (number of weeks the backup is kept) +

  (daily amount of backup data) x 10 = disk capacity required for current backup environment

  > **Note:** In this case, we recommend keeping the daily incremental backup data for at least one week (7 days), in order to apply to the last full backup. To be on the safe side, we suggest keeping these incremental saves for 10 days rather than 7 days, just in case some problem occurs with the "next full backup."

Example: A customer saves weekly 1.4 TB as full backup, and he saves daily 200 GB of incremental backup. He keeps the saved data for 3 weeks (more than 10 days). Disk capacity required for current backup environment is as follows:

1.4 TB x 3 + 200 GB x 10 = 6.2 TB

8.2 Implementing the TS7520 with i5/OS

This section provides a general overview of the setup steps and considerations for the IBM Virtualization Engine TS7520 and its connections to an IBM System i partition running i5/OS.

8.2.1 Physical setup for IBM Virtualization Engine TS7520

For detailed information about how to perform the physical setup of the IBM Virtualization Engine TS7520, refer to the *IBM Virtualization Engine TS7520: Planning, Implementation, and Usage Guide*, SG24-7520.

8.2.2 Installing IBM Virtualization Engine TS7500 Console

A TS7500 Management Console is used for configuration, management, and service support of the IBM Virtualization Engine TS7500. This console is required by the TS7500 and is either supplied by the customer or optionally ordered from IBM.

For configuration, management, and service support of the IBM VirtualizationEngine TS7500, IBM provides a graphical user interface (GUI), which is called the *IBM TotalStorage 7500 V2 R1 Virtualization Engine for Tape Console* (TS7500 VE for Tape Console). The SSR can provide you with an installation package that contains the TS7520 VE for Tape Console on a CD.

For information how to install IBM Virtualization Engine TS7500 management console and VE for Tape Console, refer to the *IBM Virtualization Engine TS7520: Planning, Implementation, and Usage Guide*, SG24-7520.

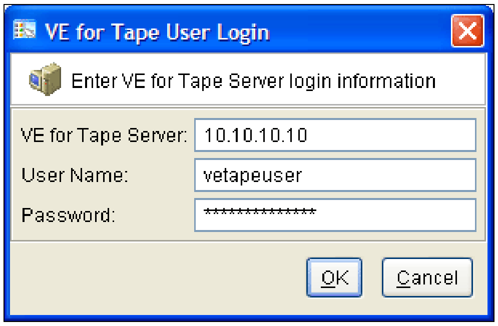
8.2.3 Connecting to IBM Virtualization Engine TS7500

To connect to your TS7500 Virtualization Engine by using VE console installed on your PC, perform the following steps:

1. Launch the VE for Tape Console installed on your PC. Right-click the TS7500 Virtualization Engine Servers object and select **Add**.This brings up the window *VE for Tape User Login.*
2. In the login window, insert IP address for the system to which you are connecting, insert userid and password, click **OK**.

> **Note:** The default user ID and password are as follows:
>
> - Default user name: vetapeuser
> - Default password: veuserpassword

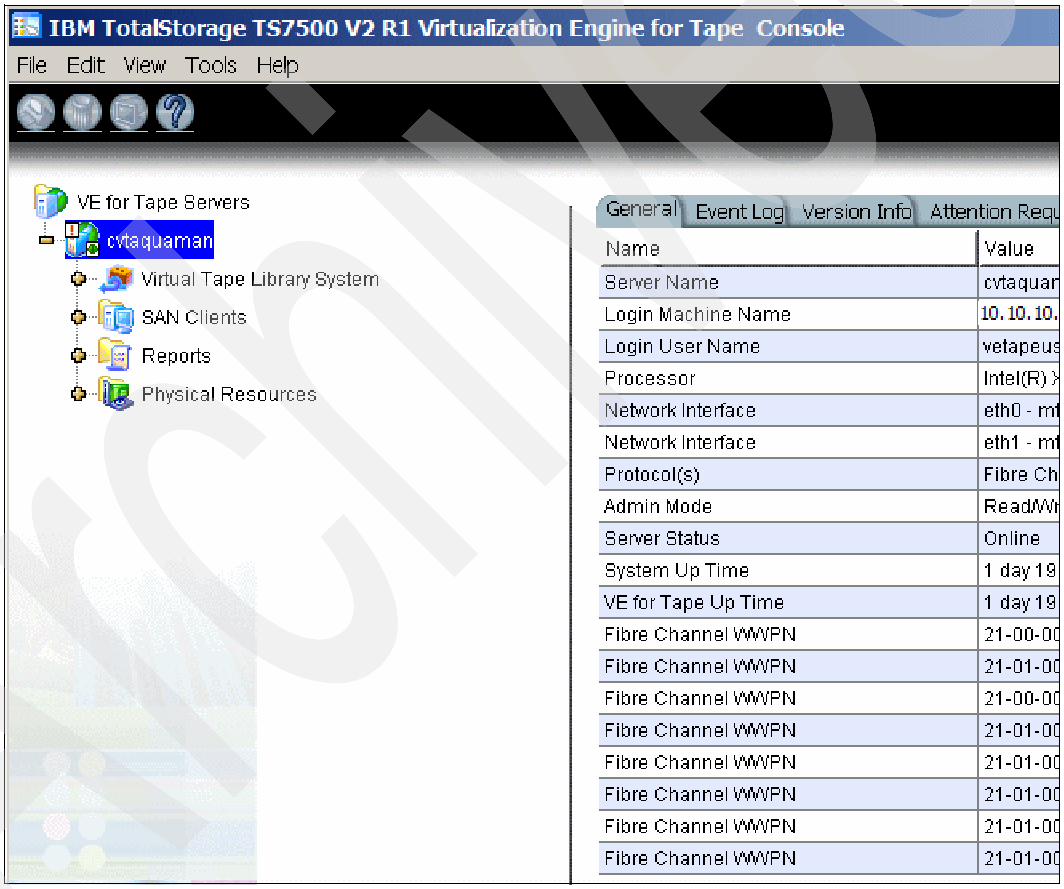
Login to Virtualization Engine TS7500 as shown in Figure 8-2.



VE for Tape Server: 10.10.10.10
User Name: vetapeuser
Password: ***************

Figure 8-2 Login to TS7500

3. If the connection is successful, you can see the server on Virtualization Engine for Tape Console. A part of GUI window is shown in Figure 8-3.



Name	Value
Server Name	cvtaquar
Login Machine Name	10.10.10.
Login User Name	vetapeus
Processor	Intel(R) X
Network Interface	eth0 - mt
Network Interface	eth1 - mt
Protocol(s)	Fibre Ch
Admin Mode	Read/Wr
Server Status	Online
System Up Time	1 day 19
VE for Tape Up Time	1 day 19
Fibre Channel WWPN	21-00-00
Fibre Channel WWPN	21-01-00
Fibre Channel WWPN	21-00-00
Fibre Channel WWPN	21-01-00
Fibre Channel WWPN	21-01-00
Fibre Channel WWPN	21-01-00
Fibre Channel WWPN	21-01-00
Fibre Channel WWPN	21-01-00

Figure 8-3 VE for Tape console window

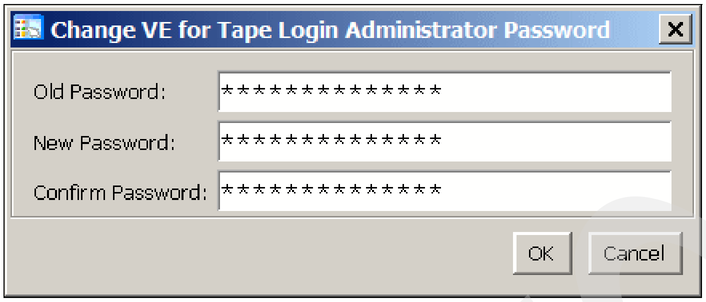
8.2.4 Setting network information and host name

We assume that network information and host name are already set up when you connect to the IBM Virtualization Engine TS7520 by VE for Tape Console. For information about how to set up Network information and host name, refer to the *IBM Virtualization Engine TS7520: Planning, Implementation, and Usage Guide*, SG24-7520.

8.2.5 Changing the default password

Next you should change the default password. If the password remains as a default, anybody can connect to IBM Virtualization Engine TS7500:

1. Right-click your TS7500 server and select **Change Password**.
2. In the window that opens, type the original password (`VEUSERPASSWORD`), type the new password, and then type the new password again to confirm it, as is shown in Figure 8-4.



Change VE for Tape Login Administrator Password

Old Password: **************

New Password: **************

Confirm Password: **************

Figure 8-4 TS7500 - Change default password

8.2.6 Setup a virtual tape library

The TS7520 VE for Tape Server lists supported tape libraries using the Product ID returned by a SCSI inquiry. Table 8-1 cross references the IBM Tape libraries with their SCSI Product Id.

Table 8-1 Library - Product Id cross reference

IBM Library	Product ID
IBM TotalStorage 3584 with TS1120, 3592 drives	03584L22
IBM TotalStorage 3584 with LTO drives	03584L32
IBM TS3500 with TS1120, 3592 drives	03584L22
IBM TS3500 with LTO drives	03584L32
IBM TS3100 with LTO drives	3573-TL or TS3100
IBM 3573 with LTO drives	3573-TL
IBM TS3200 with LTO drives	3573-TL or TS3200
IBM TS7510 Virtualization Engine with LTO, TS1120 or 3592 drives[1]	TS7510
IBM TS7520 Virtualization Engine with LTO, TS1120 or 3592 drives[1]	TS7520
IBM Total Storage 3576 with LTO Drives	3576-MTL
IBM TS3310 with LTO Drives	3576-MTL
IBM TotalStorage 3582 with LTO drives	ULT3582-TL
IBM TotalStorage 3583 with LTO drives	ULT3583-TL

In the IBM Virtualization Engine TS7520 you have the possibility to create the following virtual tape libraries, tape drives, and cartridges:

- 3584 Model L22 for 3592 J1A and E05 drives and 3584 L32 for LTO2 and LTO3 drives
- TS3310 (3576 Models L5B and E9U)
- TS3200 (3573 Model L4U) and TS3100 (3573 Model L2U) for LTO 3 drives
- 3583 (Models L18, L36, and L72) – with LTO3 drives

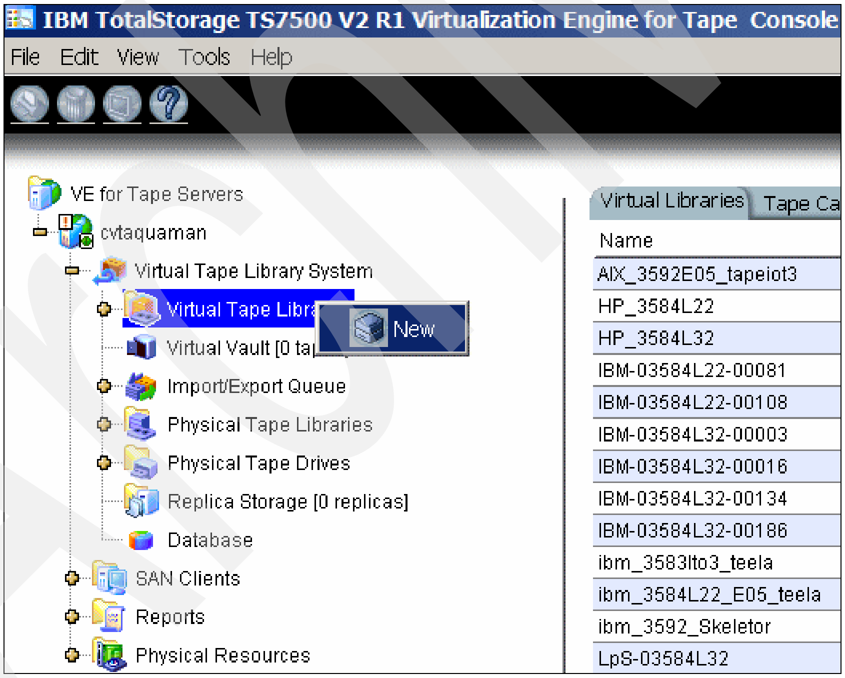
8.2.7 Creating libraries, tape drives and cartridges

IBM Virtualization Engine TS7520 comes with pre-configured virtual libraries. You can use the default libraries, if they are suitable for your usage, or you can change or delete the default libraries, and you can create additional new libraries. Keep in mind the following rules:

- Up to 128 virtual libraries are supported by one single node
- Up to 1024 virtual drives are supported by one single node
- Up to 64,000 virtual tape cartridges are supported by one single node
- One virtual library can contain same type of drives only; no mixed configuration is supported. LTO2 and LTO3, therefore, cannot exist in one virtual library.

To create a virtual tape library, follow these steps:

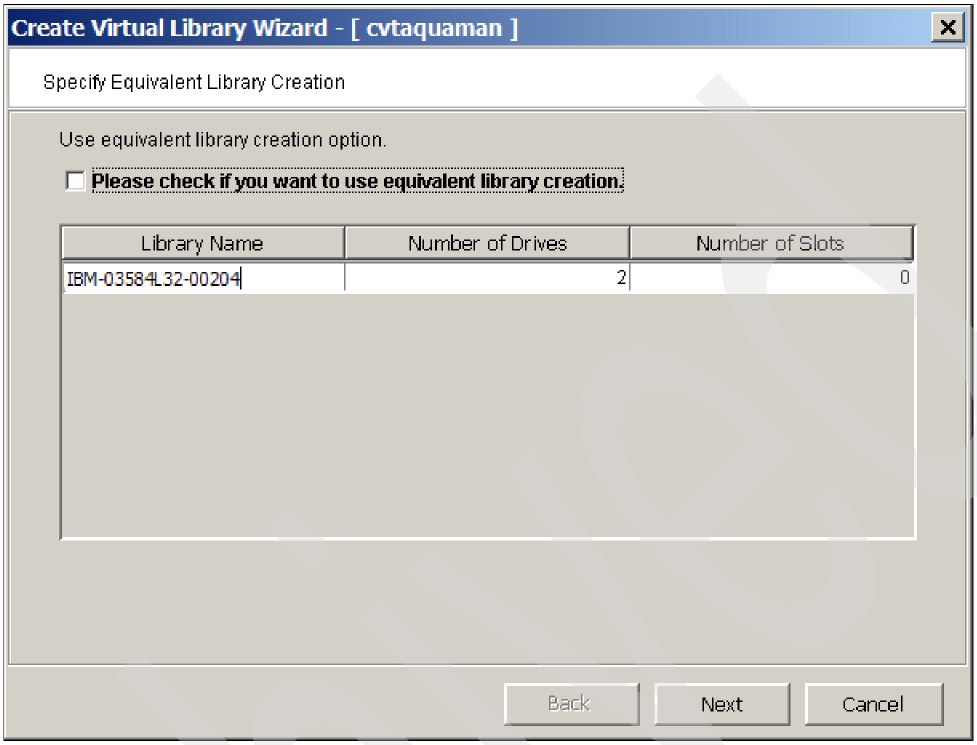
1. As shown in Figure 8-5, right-click the **Virtual Tape Library System** icon and select **New**. This starts the Creating Virtual Tape Library Wizard.



Name
AIX_3592E05_tapeiot3
HP_3584L22
HP_3584L32
IBM-03584L22-00081
IBM-03584L22-00108
IBM-03584L32-00003
IBM-03584L32-00016
IBM-03584L32-00134
IBM-03584L32-00186
ibm_3583lto3_teela
ibm_3584L22_E05_teela
ibm_3592_Skeletor
LpS-03584L32

Figure 8-5 Create new virtual tape library

2. In the first wizard window you can specify to create a virtual library based on existing default library, as can be seen in Figure 8-6. In our example we do not use the default library as a base, so we do not select this choice.



Create Virtual Library Wizard - [cvtaquaman]
Specify Equivalent Library Creation

Use equivalent library creation option.

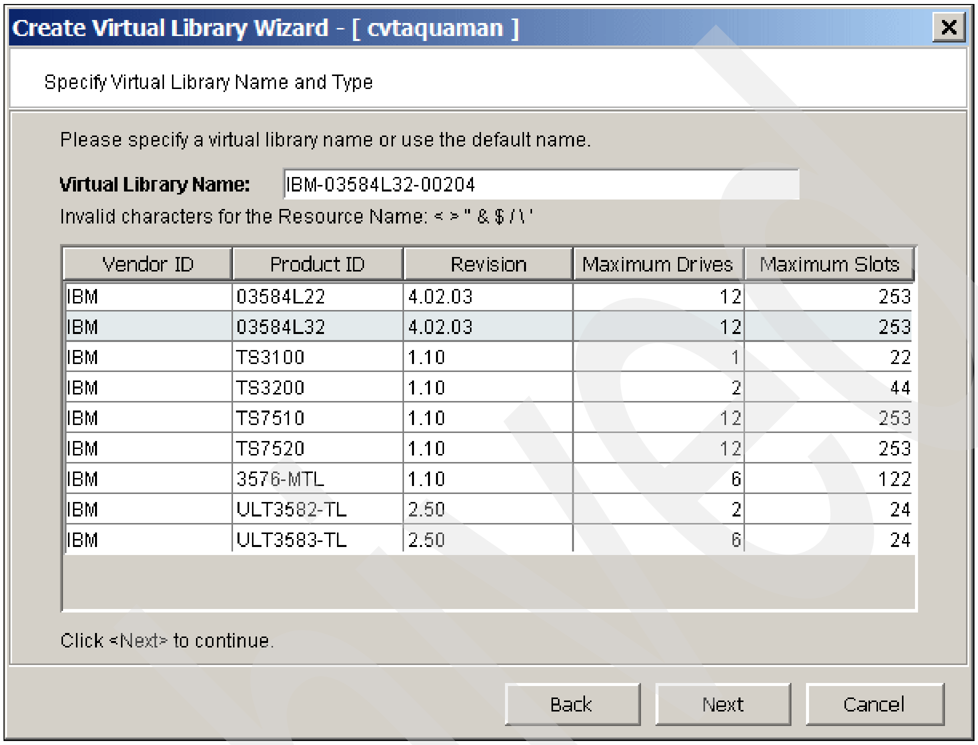
☐ Please check if you want to use equivalent library creation.

Library Name	Number of Drives	Number of Slots
IBM-03584L32-00204	2	0

Figure 8-6 Choice for using default virtual tape library

3. In the *Specify Virtual Library Name and Type* panel (Figure 8-7), select the library type, and type a name for the new virtual library.

   In this example, for the library type, we select **IBM 3584-L32** and for Virtual Library Name, we leave it as created by default: `IBM-03584L32-00204`. Then click **Next**.



Create Virtual Library Wizard - [cvtaquaman]

Specify Virtual Library Name and Type

Please specify a virtual library name or use the default name.

Virtual Library Name: IBM-03584L32-00204

Invalid characters for the Resource Name: < > " & $ / \ '

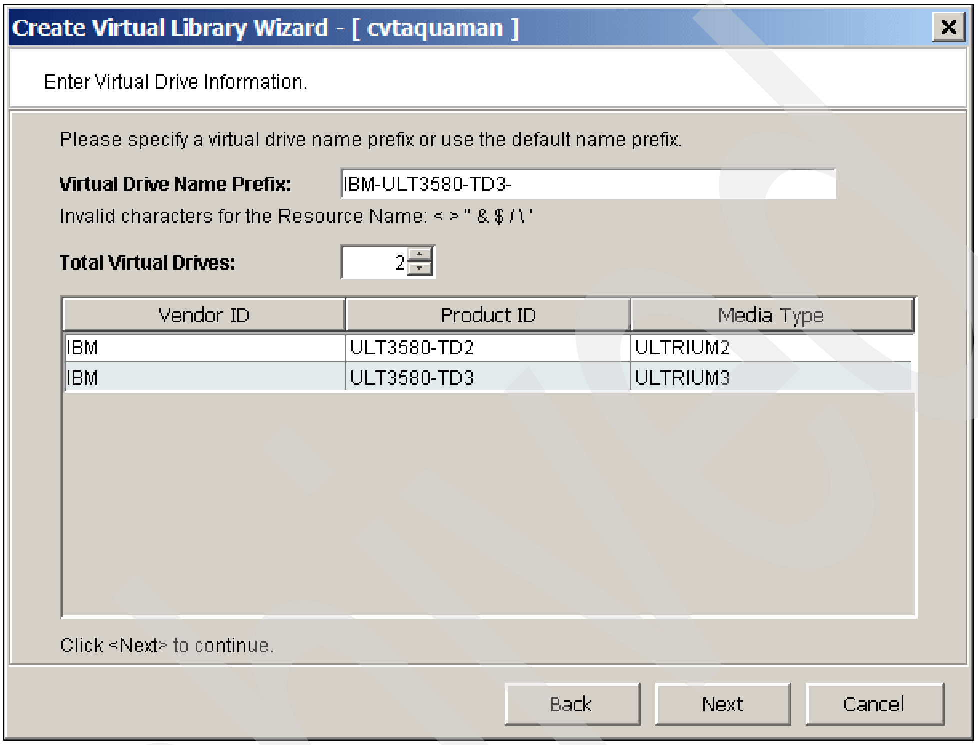
Vendor ID	Product ID	Revision	Maximum Drives	Maximum Slots
IBM	03584L22	4.02.03	12	253
IBM	03584L32	4.02.03	12	253
IBM	TS3100	1.10	1	22
IBM	TS3200	1.10	2	44
IBM	TS7510	1.10	12	253
IBM	TS7520	1.10	12	253
IBM	3576-MTL	1.10	6	122
IBM	ULT3582-TL	2.50	2	24
IBM	ULT3583-TL	2.50	6	24

Click <Next> to continue.

Figure 8-7 TS7500 - Select type of virtual library

4. Define the virtual tape drive. As shown in the *Enter Virtual Drive Information* panel (Figure 8-8), you can choose either **LTO Ultrium Generation 2**, **LTO Ultrium Generation 3**, or **3592-J1A** as the tape drive.

   In the example, after selecting **ULTRIUM 3** and specifying Virtual Drive Name Prefix, we click **Next**.



Create Virtual Library Wizard - [cvtaquaman]

Enter Virtual Drive Information.

Please specify a virtual drive name prefix or use the default name prefix.

Virtual Drive Name Prefix: IBM-ULT3580-TD3-

Invalid characters for the Resource Name: < > " & $ / \ '

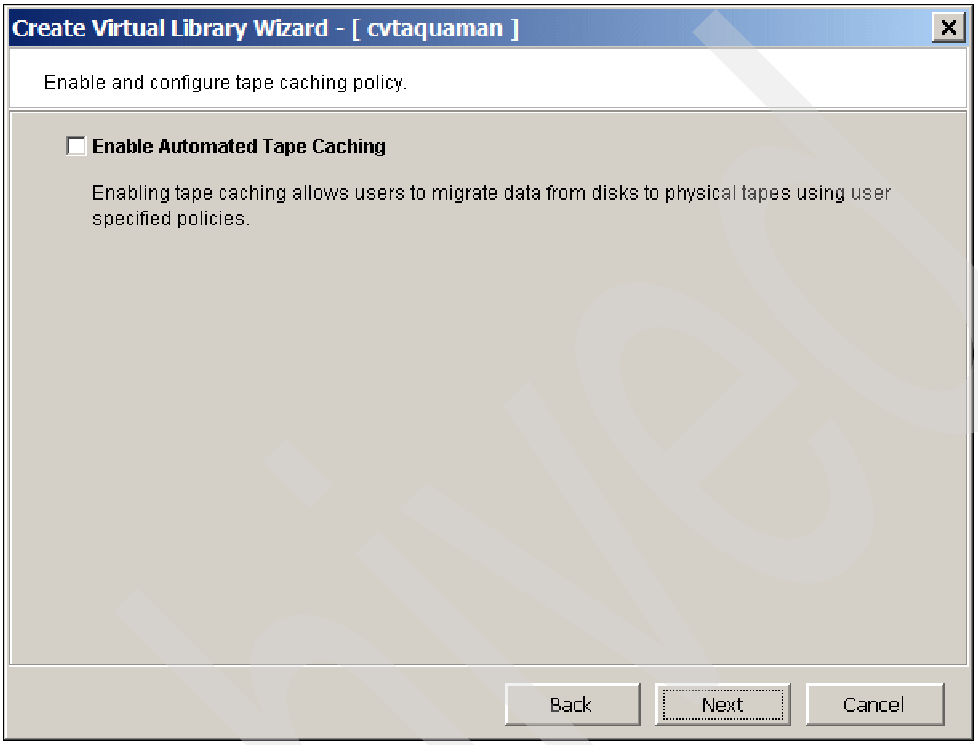
Total Virtual Drives: 2

Vendor ID	Product ID	Media Type
IBM	ULT3580-TD2	ULTRIUM2
IBM	ULT3580-TD3	ULTRIUM3

Click <Next> to continue.

Figure 8-8 TS7500 - Specify virtual tape drives

5. In the panels *Enable and Configure Tape Caching Policy* (Figure 8-9) and *Enter Virtual Library Information* (Figure 8-10), we can select Auto Archive / Replication. You can select this option if the TS7500 should automatically move or copy virtual volumes to physical tape or to another TS7500, whenever a virtual tape volume is moved to the virtual input/output station (I/O station).

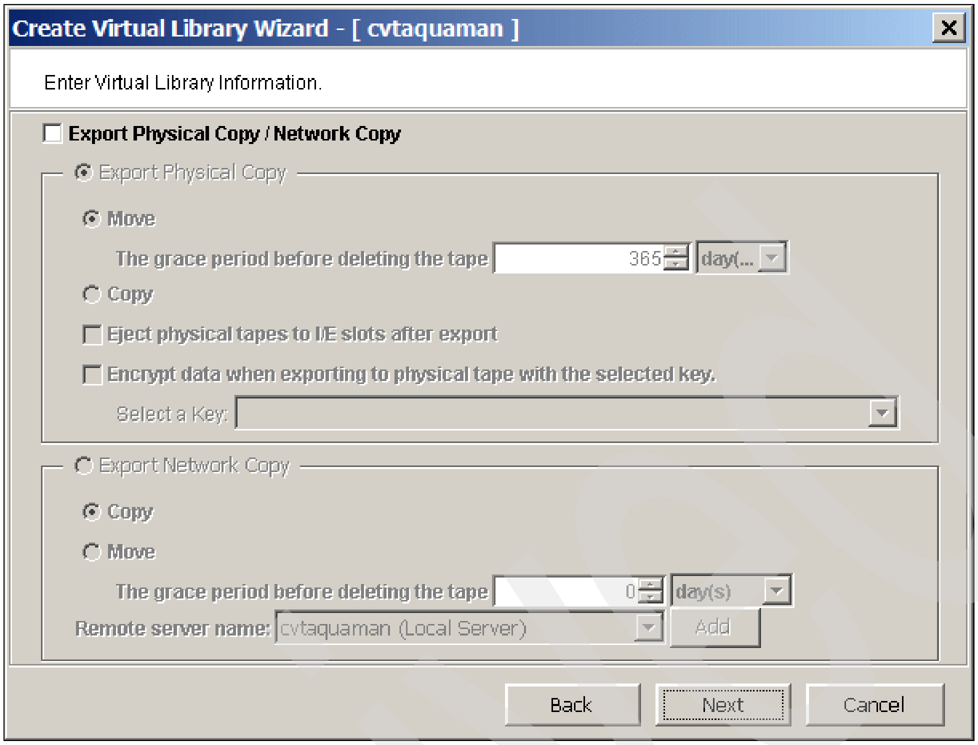

Create Virtual Library Wizard - [cvtaquaman]
Enable and configure tape caching policy.
Back
Next
Cancel

☐ Enable Automated Tape Caching

Enabling tape caching allows users to migrate data from disks to physical tapes using user specified policies.

Figure 8-9 TS7500 - Enable Automatic Tape Caching

Note that the Auto Archive functions are for use by non-System i platforms. If this virtual tape library is assigned to only i5/OS, you should not select Auto Archive. If another Virtualization Engine TS7500 is available for replication, you can select the Auto Replication function (Figure 8-10).



Create Virtual Library Wizard - [cvtaquaman]

Enter Virtual Library Information.

☐ Export Physical Copy / Network Copy

● Export Physical Copy

● Move

The grace period before deleting the tape 365 day(...

○ Copy

☐ Eject physical tapes to I/E slots after export

☐ Encrypt data when exporting to physical tape with the selected key.

Select a Key:

○ Export Network Copy

● Copy

○ Move

The grace period before deleting the tape 0 day(s)

Remote server name: cvtaquaman (Local Server)

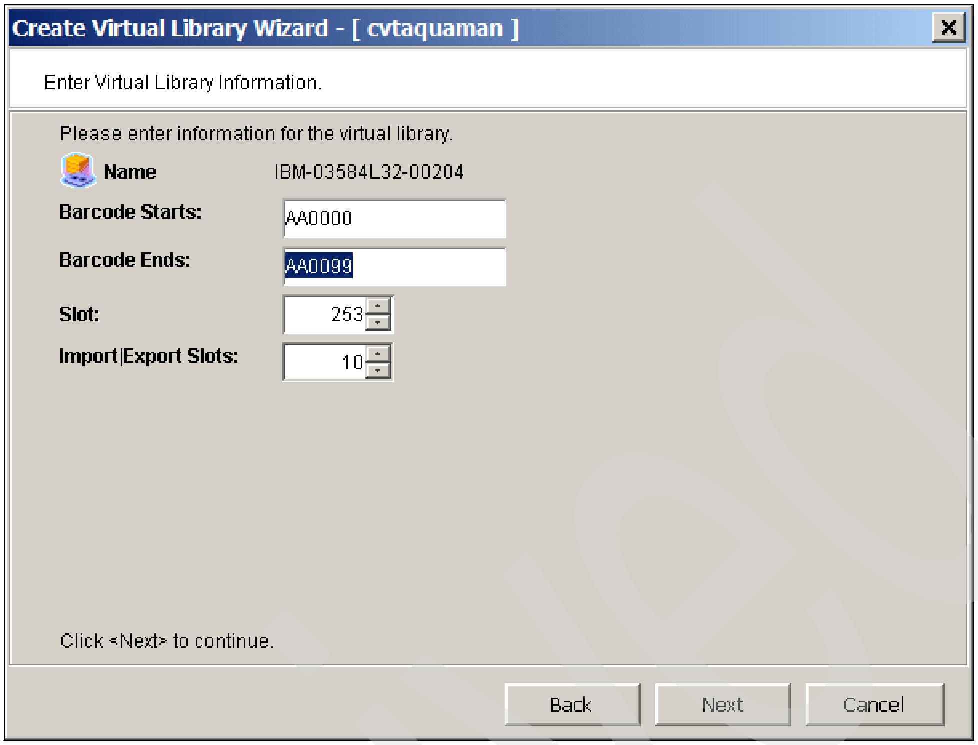
Figure 8-10 TS7500 - Export to physical tape

6. In the next panel (Figure 8-11), specify a volume range. This defines only the barcode range for the virtual volumes, but does not create the virtual volumes.

   In our example, we select a different barcode range than our physical tape library has in use. As you can see in, we choose the volume range `AA0000` to `AA0099`.

   Also in this panel, you can select the size of the virtual library slots and the size of the Import/Export Slots. We want to create an virtual library with **253** slots to allow for a possible growth in the next few years. You can use the Export to physical tape check box to limit the maximum size of a virtual tape in order to match a physical cartridge. We leave the I/O station at the default of **10** slots.

   Click **Next**.



Create Virtual Library Wizard - [cvtaquaman]

Enter Virtual Library Information.

Please enter information for the virtual library.

Name IBM-03584L32-00204

Barcode Starts: AA0000

Barcode Ends: AA0099

Slot: 253

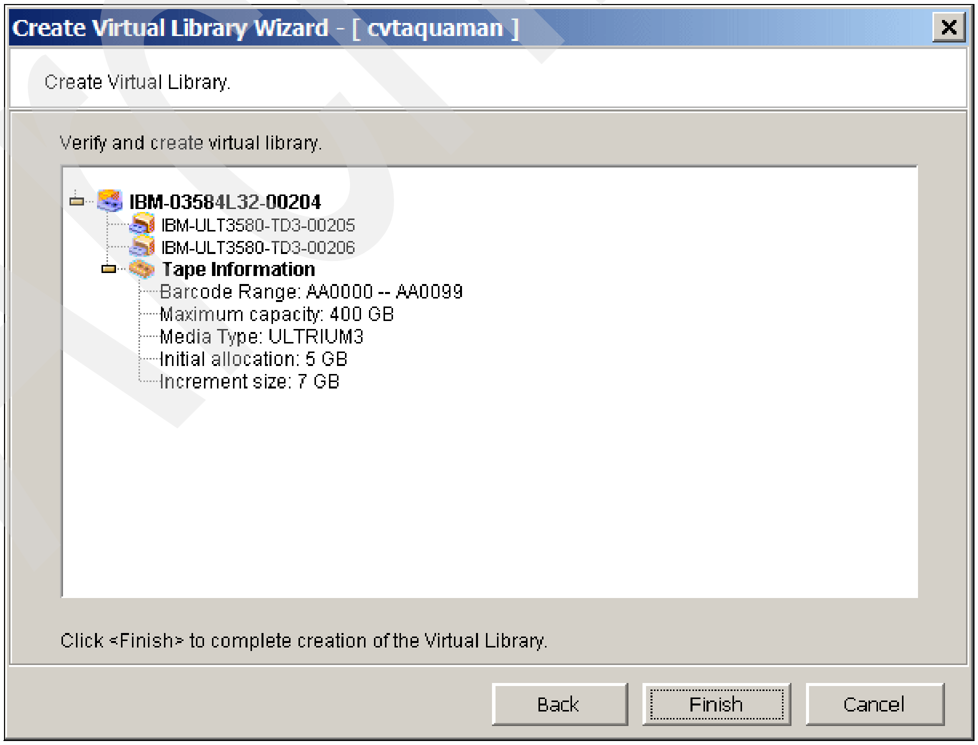
Import|Export Slots: 10

Click <Next> to continue.

Figure 8-11 Specify barcode range for virtual cartridges

7. In the *Create Virtual Library* panel (Figure 8-12), verify the details and click **Finish** if it is correct. Then the virtual library is created and creation status is shown (Figure 8-13).

   Click **Finish**.



Create Virtual Library Wizard - [cvtaquaman]

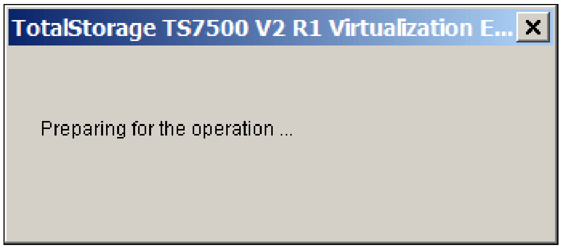
Create Virtual Library.

Verify and create virtual library.

```
IBM-03584L32-00204
    IBM-ULT3580-TD3-00205
    IBM-ULT3580-TD3-00206
    Tape Information
        Barcode Range: AA0000 -- AA0099
        Maximum capacity: 400 GB
        Media Type: ULTRIUM3
        Initial allocation: 5 GB
        Increment size: 7 GB
```

Click <Finish> to complete creation of the Virtual Library.

Figure 8-12 TS7500 - virtual tape library is created

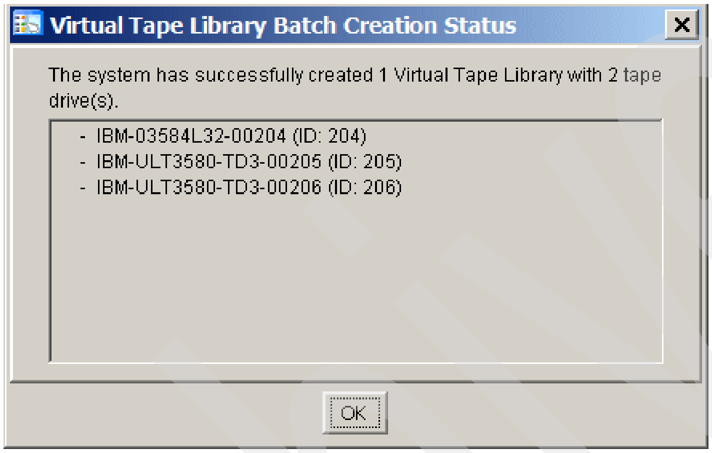


TotalStorage TS7500 V2 R1 Virtualization E...

Preparing for the operation ...

Figure 8-13 TS7500 - virtual tape library creation in progress

8. The Virtual Tape Library Creation Status window opens as shown in Figure 8-14. Click **OK**.



Virtual Tape Library Batch Creation Status

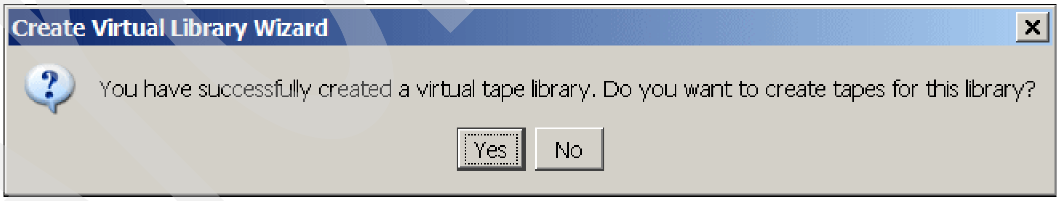
The system has successfully created 1 Virtual Tape Library with 2 tape drive(s).

- IBM-03584L32-00204 (ID: 204)
- IBM-ULT3580-TD3-00205 (ID: 205)
- IBM-ULT3580-TD3-00206 (ID: 206)

Figure 8-14 TS7500 - virtual tape library creation status

9. After you create the virtual library, you are asked to create tapes for the virtual tape library just created, as shown in Figure 8-15. Then you can create virtual volumes.

   Click **Yes**.



Create Virtual Library Wizard

You have successfully created a virtual tape library. Do you want to create tapes for this library?

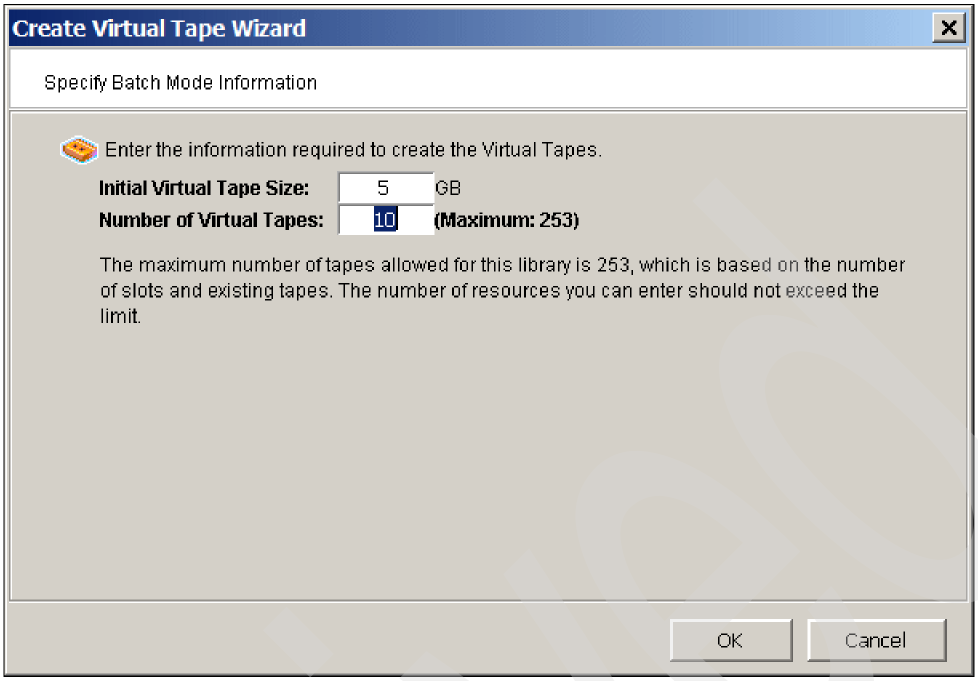
Figure 8-15 TS7500 - Specify to create tapes

The Create Virtual Tape Wizard starts.

10. In the *Create Virtual Tape Wizard, Specify Batch Mode Information* panel (Figure 8-16), you can choose the initial virtual tape size. The default size for all media types is 5 GB. This means that at least 5 GB of space is required for all virtual tape volumes. You can change this value, but it is not necessary, because while writing to a virtual volume, the volume expands its size in increments defined by the increment size. The increment size is 5 GB for LTO2 and 3592 and 7 GB for LTO3. In this example, we keep the default initial size.

    Click **OK**.

    The TS7500 creates 10 virtual tapes with barcode labels that match the physical barcode labels and have an initial size of 5 GB.



Create Virtual Tape Wizard

Specify Batch Mode Information

Enter the information required to create the Virtual Tapes.

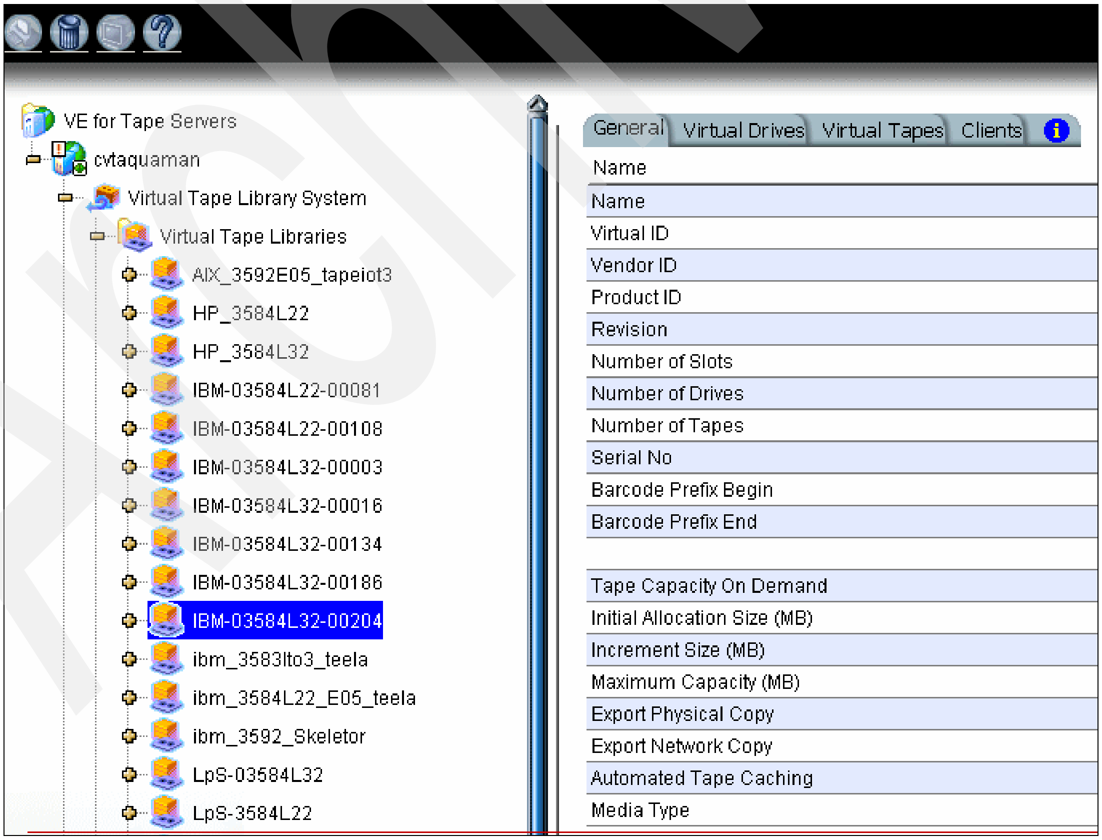
Initial Virtual Tape Size: 5 GB

Number of Virtual Tapes: 10 **(Maximum: 253)**

The maximum number of tapes allowed for this library is 253, which is based on the number of slots and existing tapes. The number of resources you can enter should not exceed the limit.

Figure 8-16 TS7500 - Create Virtual tapes

Figure 8-17 shows an overview of the newly created library.



- VE for Tape Servers
  - cvtaquaman
    - Virtual Tape Library System
      - Virtual Tape Libraries
        - AIX_3592E05_tapeiot3
        - HP_3584L22
        - HP_3584L32
        - IBM-03584L22-00081
        - IBM-03584L22-00108
        - IBM-03584L32-00003
        - IBM-03584L32-00016
        - IBM-03584L32-00134
        - IBM-03584L32-00186
        - IBM-03584L32-00204
        - ibm_3583lto3_teela
        - ibm_3584L22_E05_teela
        - ibm_3592_Skeletor
        - LpS-03584L32
        - LpS-3584L22

Name

Name
Virtual ID
Vendor ID
Product ID
Revision
Number of Slots
Number of Drives
Number of Tapes
Serial No
Barcode Prefix Begin
Barcode Prefix End

Tape Capacity On Demand
Initial Allocation Size (MB)
Increment Size (MB)
Maximum Capacity (MB)
Export Physical Copy
Export Network Copy
Automated Tape Caching
Media Type

Figure 8-17 Created virtual tape library

We have now created a virtual library. Other than the libraries that are already created by default, this newly created library is not yet assigned to any host. Therefore, to make this library usable by any host, we must add SAN Clients to IBM Virtualization Engine TS7520. So we must assign a host to the library. These actions are explained further in this section.

8.2.8 Adding an FC adapter in i5/OS as a SAN client of the TS7500

In the physical world, you assign tape drives and tape libraries to a host by creating appropriate SAN zones. With SAN zones, you can separate hosts from connecting to every tape drive. With the tape virtualization of the IBM Virtualization Engine TS7520, you can have several tape drives and several tape libraries on one single Fibre Channel port. Therefore, SAN zoning, which is based on Fibre Channel ports, might not be sufficient for separating hosts. For that reason, the IBM Virtualization Engine TS7520 allows you to create access rules on a host basis.

For security purposes, you can assign a specific virtual library and its virtual tape drives definition to specific clients. For general usage, you can use the Everyone_CF client. This everyone client is a generic client that you can assign to all or some of your virtual library-device definitions.

You can select how the client sees the virtual devices in any of the following ways:

- **One to one:** This limits visibility to a single pair of WWPNs. A WWPN is a worldwide port name that is uniquely assigned to each Fibre Channel (FC) adapter port. The WWPN consists of exactly 16 hexadecimal characters (0 - 9 and A - F). In the following section, you see setup windows that use the WWPN.
- **One to all:** You have to select the client's Fibre Channel initiator WWPN.
- **All to one:** You have to select the server's Fibre Channel target WWPN.
- **All to all:** You create multiple path data paths. If ports are ever added to the client or server, they are automatically included in your WWPN mapping.

The following section shows an example of a one to one SAN client setup. Before you assign a tape library to an i5/OS partition, you must add this partition as a SAN client to the IBM Virtualization Engine TS7520. The term SAN client refers to a client host connecting to the IBM Virtualization Engine TS7520, such as our i5/OS partition.

To add a SAN client, perform the following steps on the Virtualization Engine for Tape Console:

1. Right-click the **SAN Client** icon and select **Add**, as shown in Figure 8-18.

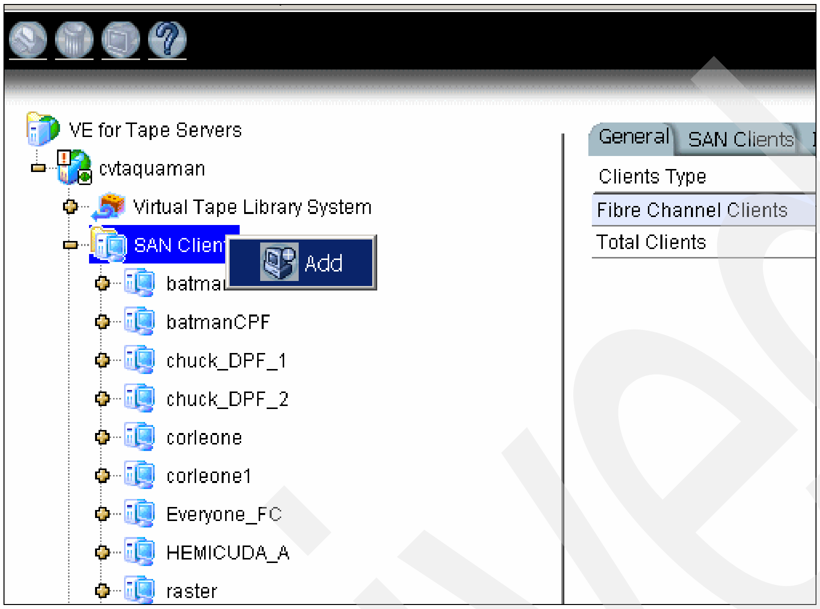
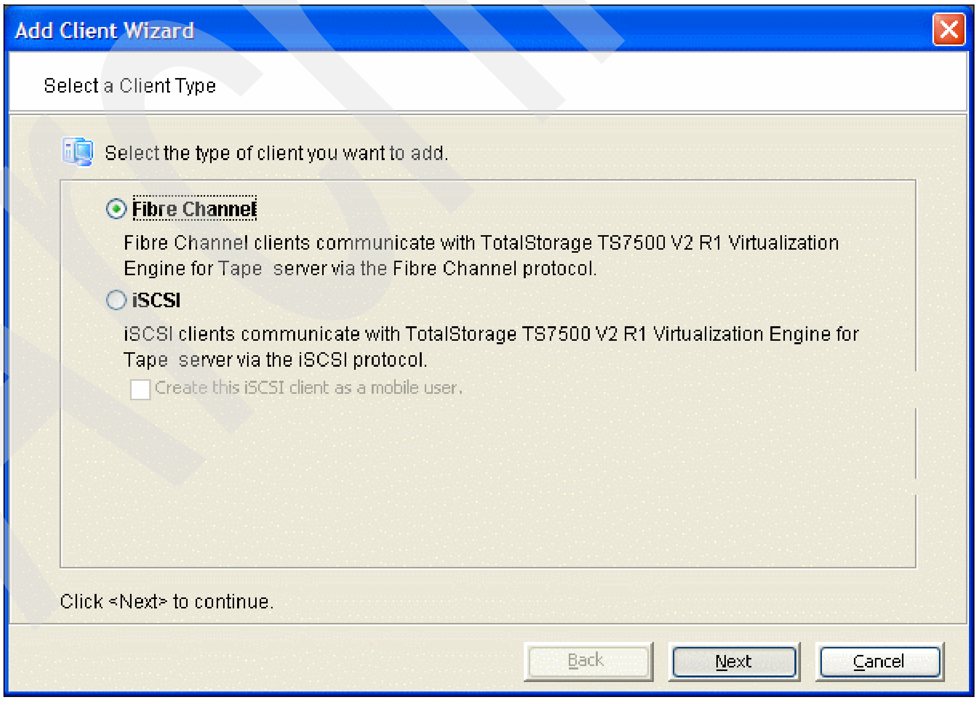


Figure 8-18 TS7500 - Add SAN client

2. In the window shown in Figure 8-19, select the access method to be used by the SAN client. We chose **Fibre Channel**. Click **Next**.



Select a Client Type

Select the type of client you want to add.

● **Fibre Channel**

Fibre Channel clients communicate with TotalStorage TS7500 V2 R1 Virtualization Engine for Tape server via the Fibre Channel protocol.

○ **iSCSI**

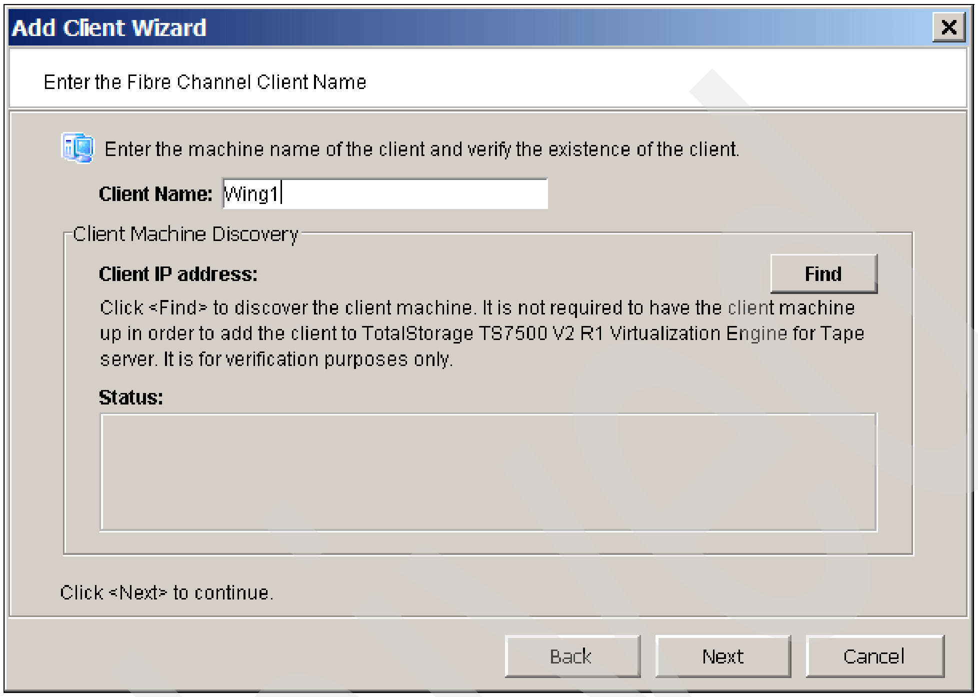
iSCSI clients communicate with TotalStorage TS7500 V2 R1 Virtualization Engine for Tape server via the iSCSI protocol.

□ Create this iSCSI client as a mobile user.

Click <Next> to continue.

Figure 8-19 Adding SAN clients - select client access method

3. In the *Enter the Fibre Channel Client Name* panel (Figure 8-20), type the client name. Client name indicates the name of initiator IOA (i5/OS partition Fibre Channel adapter). You can specify the name as you want. Then click **Next**.



Add Client Wizard

Enter the Fibre Channel Client Name

Enter the machine name of the client and verify the existence of the client.

Client Name: Wing1

Client Machine Discovery

Client IP address:

Click <Find> to discover the client machine. It is not required to have the client machine up in order to add the client to TotalStorage TS7500 V2 R1 Virtualization Engine for Tape server. It is for verification purposes only.

Status:

Click <Next> to continue.

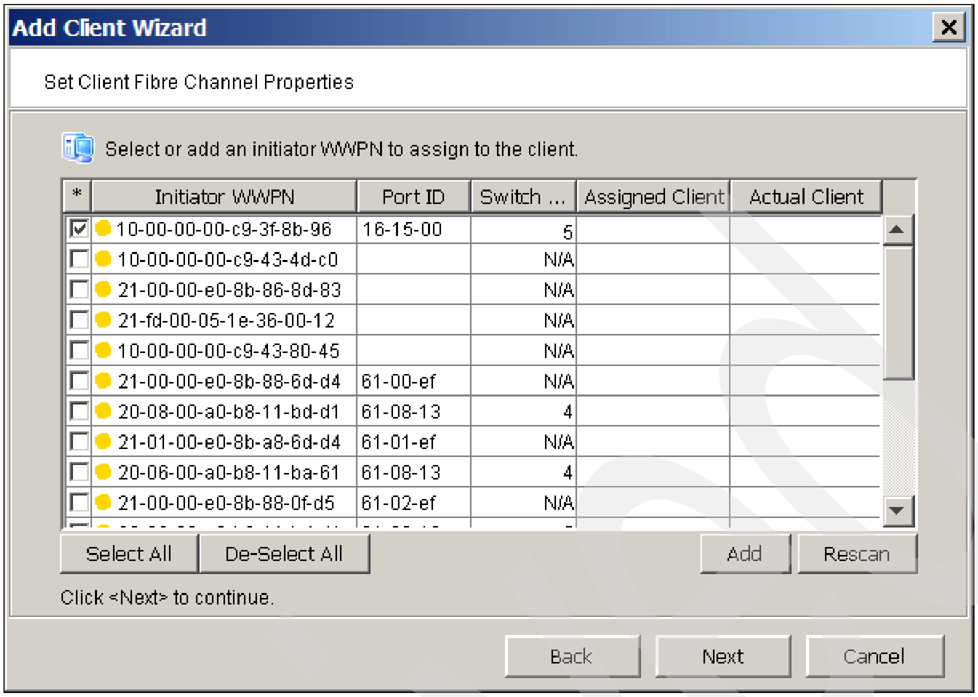
Figure 8-20 TS7500 - Specify SAN client name

4. In the *Set Client Fibre Channel Properties* panel (Figure 8-21), select the WWPN of the client, and the WWPN of the Fibre Channel host bus adapter (HBA) that you want to add. The WWPN of the Fibre Channel HBA is printed on the card. You can also look for WWPN in i5/OS System Service Tools (SST).

   For more information about i5/OS SST, refer to System i Information center on the following Web site:

   `http://publib.boulder.ibm.com/iseries/`

   If your client has several Fibre Channel HBAs and you want to connect to the TS7500 over several Fibre Channel links, you must select the corresponding WWPNs of those Fibre Channel HBAs. Then click **Next**.



Select or add an initiator WWPN to assign to the client.

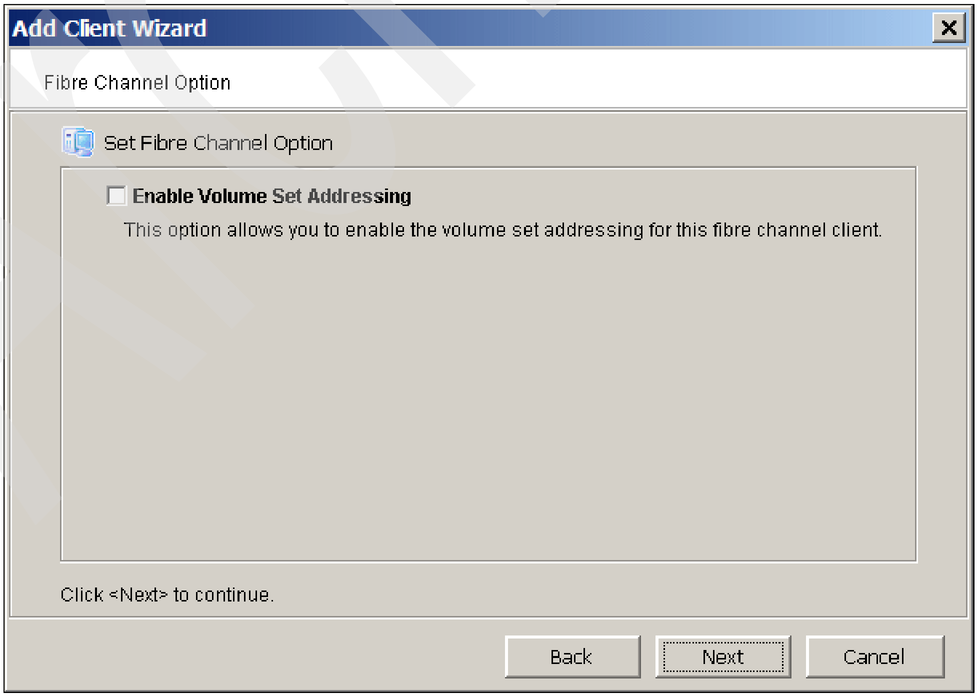
*	Initiator WWPN	Port ID	Switch ...	Assigned Client	Actual Client
☑	● 10-00-00-00-c9-3f-8b-96	16-15-00	5		
☐	● 10-00-00-00-c9-43-4d-c0		N/A		
☐	● 21-00-00-e0-8b-86-8d-83		N/A		
☐	● 21-fd-00-05-1e-36-00-12		N/A		
☐	● 10-00-00-00-c9-43-80-45		N/A		
☐	● 21-00-00-e0-8b-88-6d-d4	61-00-ef	N/A		
☐	● 20-08-00-a0-b8-11-bd-d1	61-08-13	4		
☐	● 21-01-00-e0-8b-a8-6d-d4	61-01-ef	N/A		
☐	● 20-06-00-a0-b8-11-ba-61	61-08-13	4		
☐	● 21-00-00-e0-8b-88-0f-d5	61-02-ef	N/A		

Click <Next> to continue.

Figure 8-21 TS7500 - Specify WWPN of adapter in i5/OS

5. In the *Fibre Channel Option* panel (Figure 8-22), determine whether you want to use Volume Set Addressing (VSA) for this adapter. This might be required for particular Fibre Channel storage depending upon the storage system's requirements. For example, storage that is connected to an HP-UX host with an HP Fibre Channel adapter requires VSA addressing.

   You should *not* select Enable Volume Set Addressing for an i5/O partition connection.



Set Fibre Channel Option

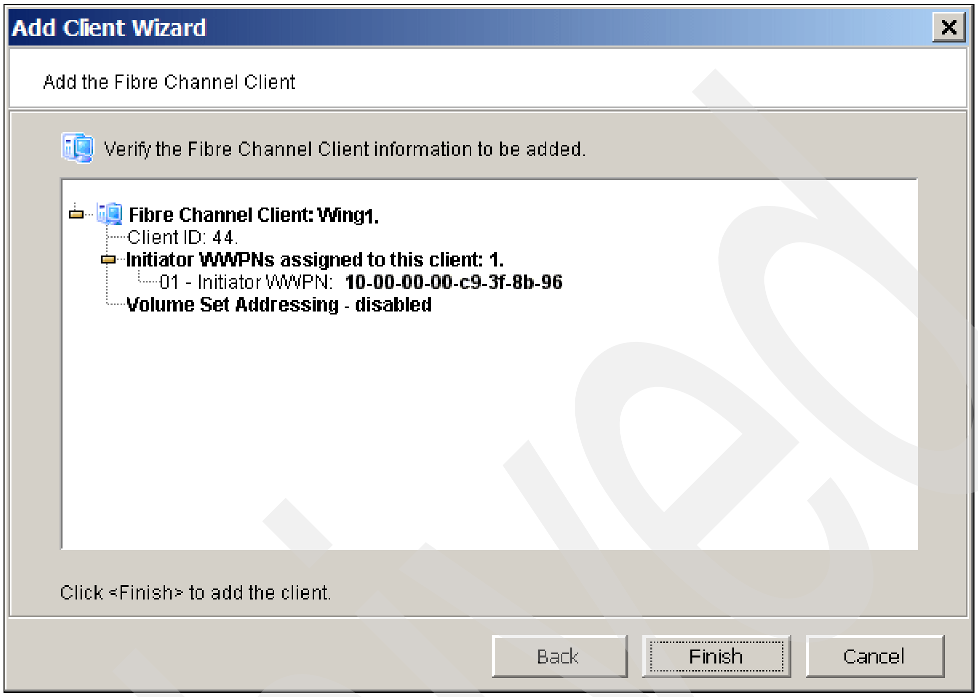
☐ **Enable Volume Set Addressing**

This option allows you to enable the volume set addressing for this fibre channel client.

Click <Next> to continue.

Figure 8-22 TS7500 - Volume set addressing

6. The *Add the Fibre Channel Client* panel (Figure 8-23) shows a summary of your selections. If the information is correct, click **Finish**, and your SAN client is added. If the information is not correct, click the **Back** button to make any necessary corrections.



Verify the Fibre Channel Client information to be added.

Fibre Channel Client: Wing1.
Client ID: 44.
Initiator WWPNs assigned to this client: 1.
01 - Initiator WWPN: **10-00-00-00-c9-3f-8b-96**
Volume Set Addressing - disabled

Click <Finish> to add the client.

Figure 8-23 TS7500 - Check created SAN client

8.2.9 Assigning a host to a library and drives

Up to this point, we have created the library with drives and tape cartridges. All libraries that you create must be assigned to the host to enable its access to those libraries.

In addition to the assignment of a host to a virtual library and virtual drives, you can select which Fibre Channel target port from the IBM Virtualization Engine TS7520 to use. With this option, you can balance the workload to different Fibre Channel HBAs (target ports) by assigning a number of drives to one Fibre Channel HBA and other drives to other Fibre Channel HBAs on the IBM Virtualization Engine TS7520.

To assign a host to the library, follow these steps:

1. Right-click the **host** icon and select **Assign**, as shown in Figure 8-24.

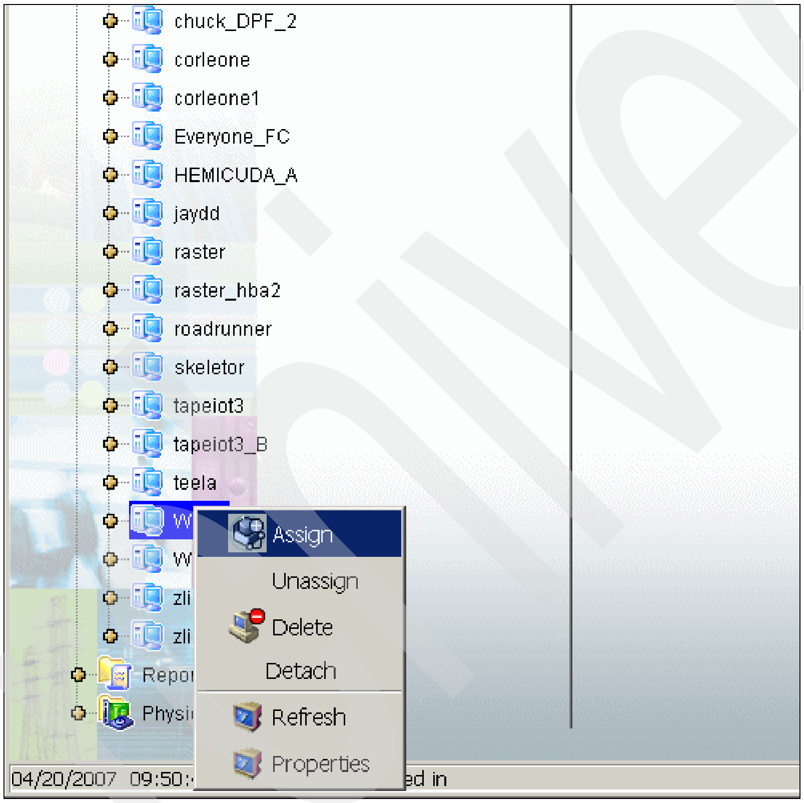


Figure 8-24 TS7500 - Assign virtual tape library to a SAN client

2. In the *Select Tape Libraries or Drives* panel (Figure 8-25), you can select different access modes to assign libraries and drives. The access types are:

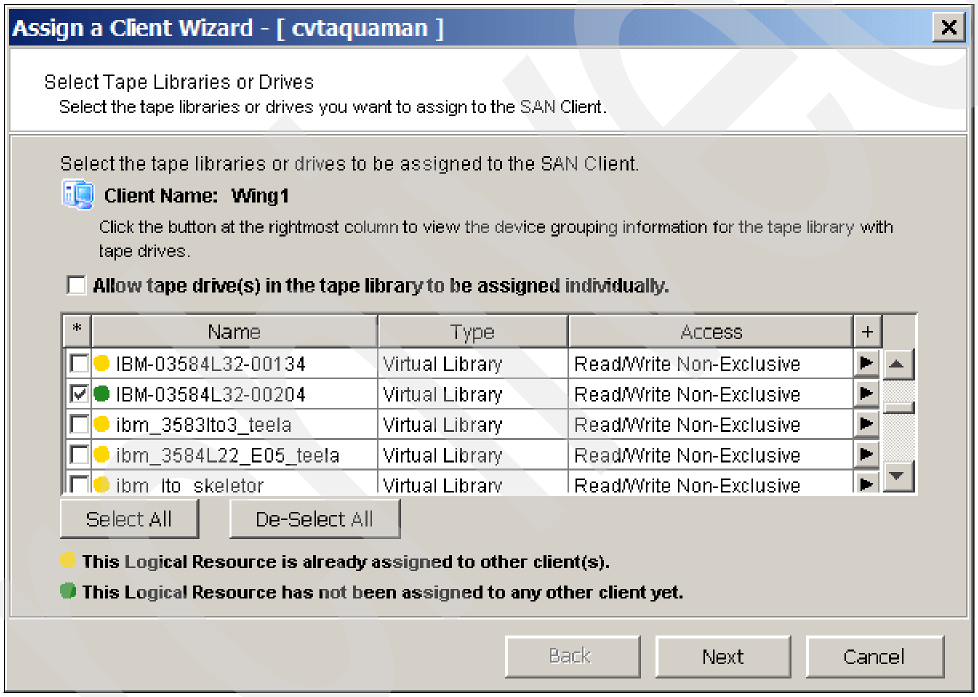
   – *Read/Write access* indicates that only one client can access the library or drive. If another host tries to access the library or the drive, this access is denied.

   – *Read/Write Non-Exclusive* access indicates that several clients can access the drive or library. Use this mode if the library or the drives are to be shared.

   You can assign the complete library with drives over a Fibre Channel target port. Alternatively, you can assign the drives individually by selecting the **Allow drive(s) in the library to be assigned individually** check box.

   For example, you can select **Allow drive(s) in the library to be assigned individually** as well as the library and the first three drives. The other three tape drives are assigned over a different Fibre Channel port.

   Click **Next**.



Assign a Client Wizard - [cvtaquaman]

Select Tape Libraries or Drives

Select the tape libraries or drives you want to assign to the SAN Client.

Select the tape libraries or drives to be assigned to the SAN Client.

Client Name: Wing1

Click the button at the rightmost column to view the device grouping information for the tape library with tape drives.

☐ Allow tape drive(s) in the tape library to be assigned individually.

*	Name	Type	Access	+
☐	● IBM-03584L32-00134	Virtual Library	Read/Write Non-Exclusive	▶
☑	● IBM-03584L32-00204	Virtual Library	Read/Write Non-Exclusive	▶
☐	● ibm_3583lto3_teela	Virtual Library	Read/Write Non-Exclusive	▶
☐	● ibm_3584L22_E05_teela	Virtual Library	Read/Write Non-Exclusive	▶
☐	● ibm_lto_skeletor	Virtual Library	Read/Write Non-Exclusive	▶

● This Logical Resource is already assigned to other client(s).

● This Logical Resource has not been assigned to any other client yet.

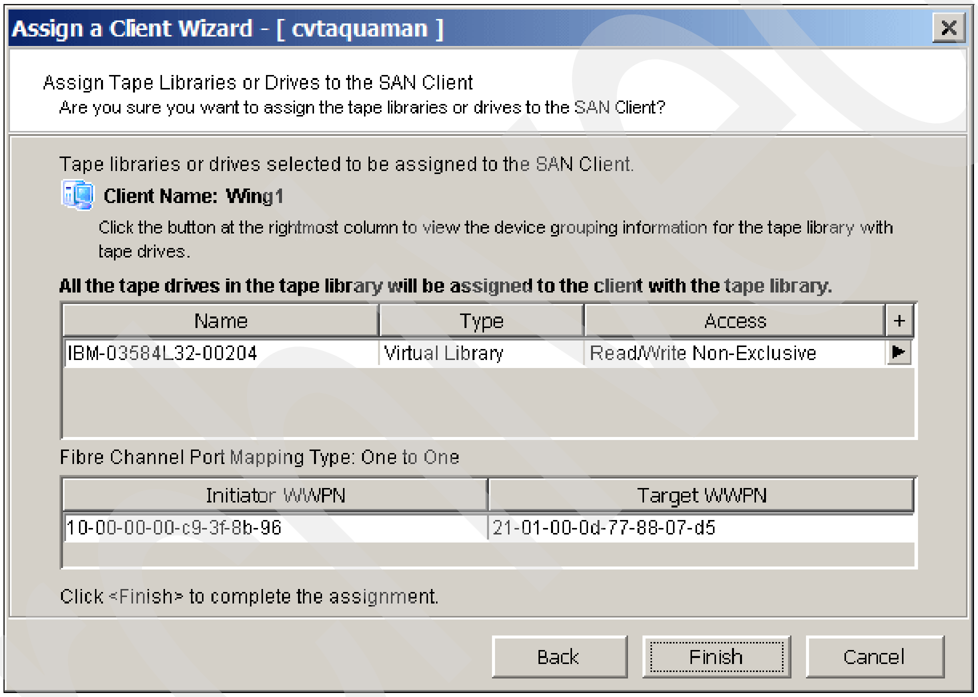
Figure 8-25 TS7500 - Select virtual tape library to assign

3. In the *Select a Fibre Channel Target* panel, select the Fibre Channel HBA to use for the connection to the host. This selection is available only if several paths from the host to the TS7500 exist. This means that several zones must be created, because only one initiator and only one target should be in one zone.

   If your i5/OS partition has several Fibre Channel HBAs for connecting to the TS7500, you must select each Fibre Channel HBA WWPN connecting to the correct Fibre Channel adapter on i5/OS partition. After selecting the WWPN, click **Next**.

   In our example only one path from the host to TS7500 is available, so this panel is not shown.

4. In the *Assign Tape Libraries or Drives to the SAN Client* panel (Figure 8-26), verify your selection before you make this assignment. If everything appears to be correct, click **Finish**. To make changes, click the **Back** button.



Assign a Client Wizard - [cvtaquaman]

Assign Tape Libraries or Drives to the SAN Client

Are you sure you want to assign the tape libraries or drives to the SAN Client?

Tape libraries or drives selected to be assigned to the SAN Client.

Client Name: Wing1

Click the button at the rightmost column to view the device grouping information for the tape library with tape drives.

All the tape drives in the tape library will be assigned to the client with the tape library.

Name	Type	Access	+
IBM-03584L32-00204	Virtual Library	Read/Write Non-Exclusive	▶

Fibre Channel Port Mapping Type: One to One

Initiator WWPN	Target WWPN
10-00-00-00-c9-3f-8b-96	21-01-00-0d-77-88-07-d5

Click <Finish> to complete the assignment.

Figure 8-26 TS7500 - Check the WWPNs to assign virtual tape library

We have now assigned the virtual tape library IBM-03584L32-00204 to host Wing1 (the name assigned to the Fibre Channel adapter owned by our i5/OS partition), as shown in Figure 8-27.

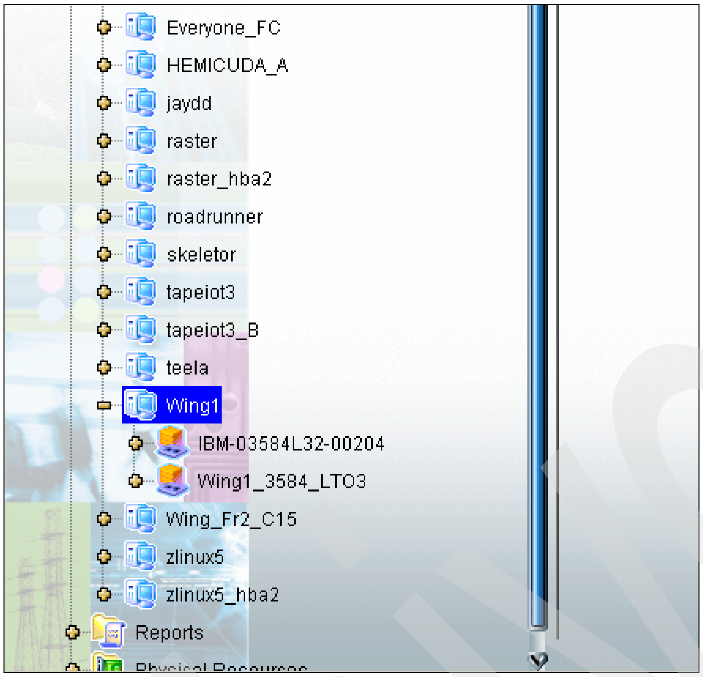


Figure 8-27   TS7500 - Assigned virtual tape library

8.2.10 Recognizing a virtual tape library in 5/OS partition

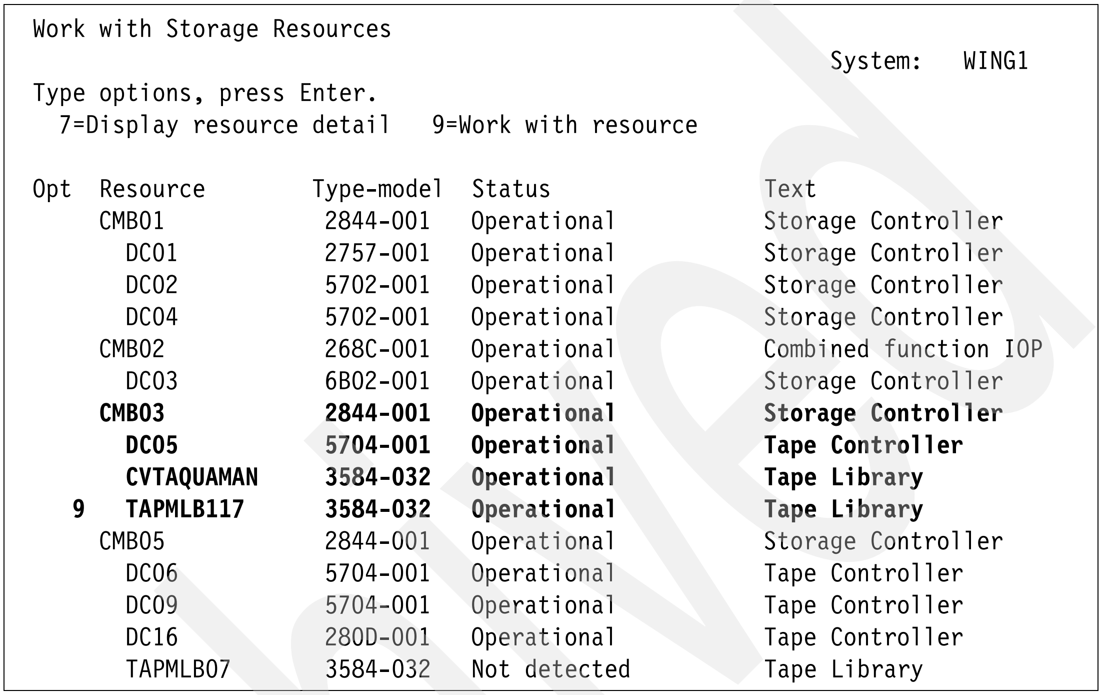
If the assignment of the virtual tape library (IBM Virtualization Engine TS7520) to the i5/OS partition is done correctly, i5/OS uses a virtual tape library as though it is a physical tape library. The following section explains how the i5/OS partition can recognize and use the virtual tape library of an IBM Virtualization Engine TS7520.

Using i5/OS commands

If the virtual tape library is recognized, you can verify it using the Work with Storage Resources (WRKHDWRSC TYPE(*STG)) command. See Figure 8-28; the example shows that CVTAQUAMAN and TAPMLB117 belong to one 5704 Fibre Channel Tape Controller Adapter.

> **Important:** If WRKHDWRSC TYPE(*STG) does not show any TAPMLB devices, check if System Value QAUTOCFG is **1**=On.
>
> You might encounter a situation where you have to perform an *IOP-reset* to get i5/OS to recognize a new tape library. Contact IBM Support and to get the directions to perform IOP-reset if you require help do this.

You have to determine which virtual tape library on IBM Virtualization Engine TS7520 is TAPMLB117. The Work with Storage Resources screen (Figure 8-28) does not show exactly which virtual tape is TAPMLB117. The tape drive serial number shows which TAPxx device is the tape drive on the TS7520 Virtualization Engine. Select TAPMLBxx (04 in our example) with **9=Work with resource**. Press Enter.

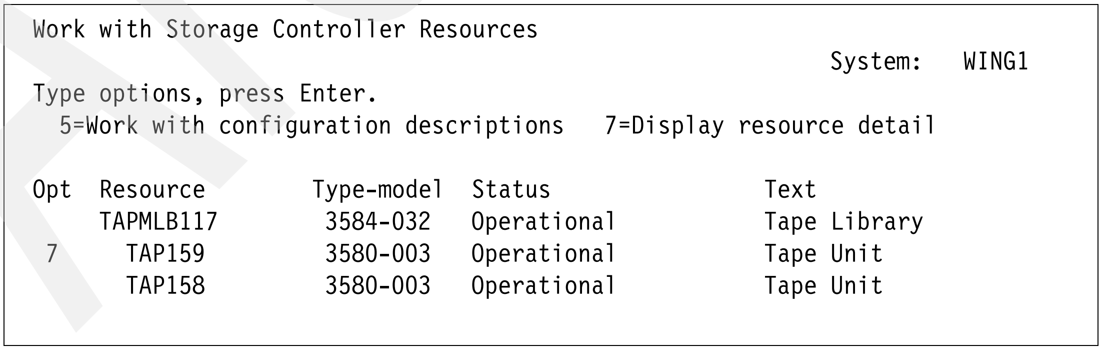


```
Work with Storage Resources
                                                            System:   WING1
Type options, press Enter.
  7=Display resource detail   9=Work with resource

Opt  Resource        Type-model  Status               Text
     CMB01            2844-001   Operational          Storage Controller
       DC01           2757-001   Operational          Storage Controller
       DC02           5702-001   Operational          Storage Controller
       DC04           5702-001   Operational          Storage Controller
     CMB02            268C-001   Operational          Combined function IOP
       DC03           6B02-001   Operational          Storage Controller
     CMB03            2844-001   Operational          Storage Controller
       DC05           5704-001   Operational          Tape Controller
       CVTAQUAMAN     3584-032   Operational          Tape Library
   9   TAPMLB117      3584-032   Operational          Tape Library
     CMB05            2844-001   Operational          Storage Controller
       DC06           5704-001   Operational          Tape Controller
       DC09           5704-001   Operational          Tape Controller
       DC16           280D-001   Operational          Tape Controller
       TAPMLB07       3584-032   Not detected         Tape Library
```

Figure 8-28 Virtual tape libraries as hardware resources

In Figure 8-28, you see which TAPMLBnn tape libraries are associated with the Fibre Channel Tape Controller (DC05 5704, in our example). The associated IOP is shown as CMB03.

In Figure 8-29, you see the TAPnn devices associated with a tape library, TAPMLBnn. Enter **7=Display resource detail** next to the TAPnn device (tape unit) and press Enter. This shows the tape unit resource details shown in Figure 8-30.

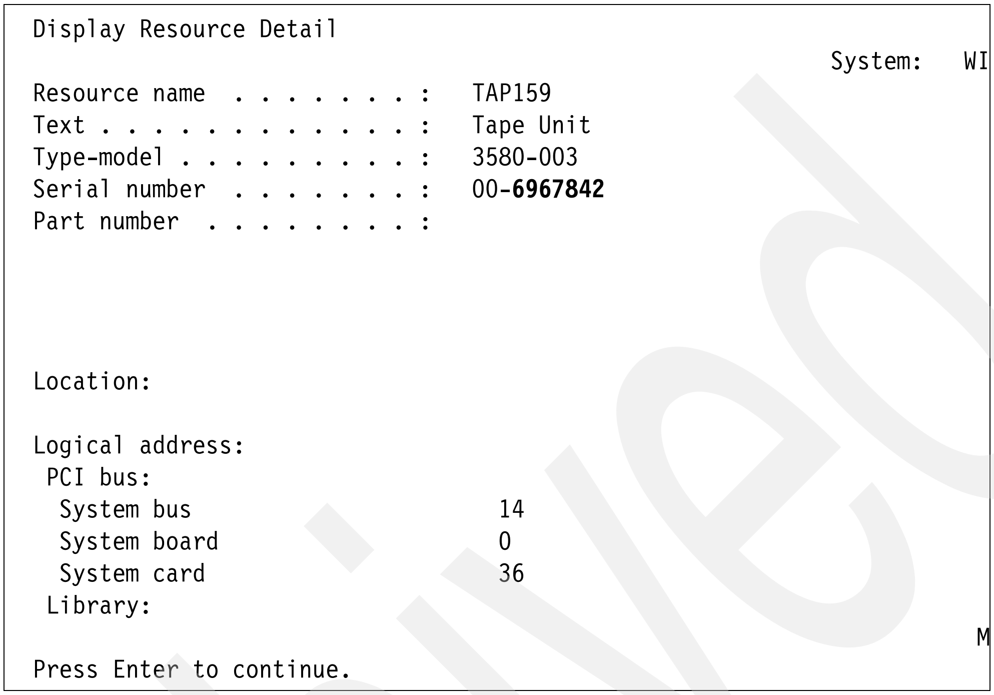


```
Work with Storage Controller Resources
                                                            System:   WING1
Type options, press Enter.
  5=Work with configuration descriptions   7=Display resource detail

Opt  Resource        Type-model  Status               Text
     TAPMLB117        3584-032   Operational          Tape Library
 7     TAP159         3580-003   Operational          Tape Unit
       TAP158         3580-003   Operational          Tape Unit
```

Figure 8-29 Virtual tape drives in HW resources

The Display Resource Detail screen (Figure 8-30) shows the serial number of TAP device. This example shows 00-6967842 of the serial number on i5/OS. You want to correlate this serial number to a corresponding value shown using the Virtualization Engine for Tape Console interface.

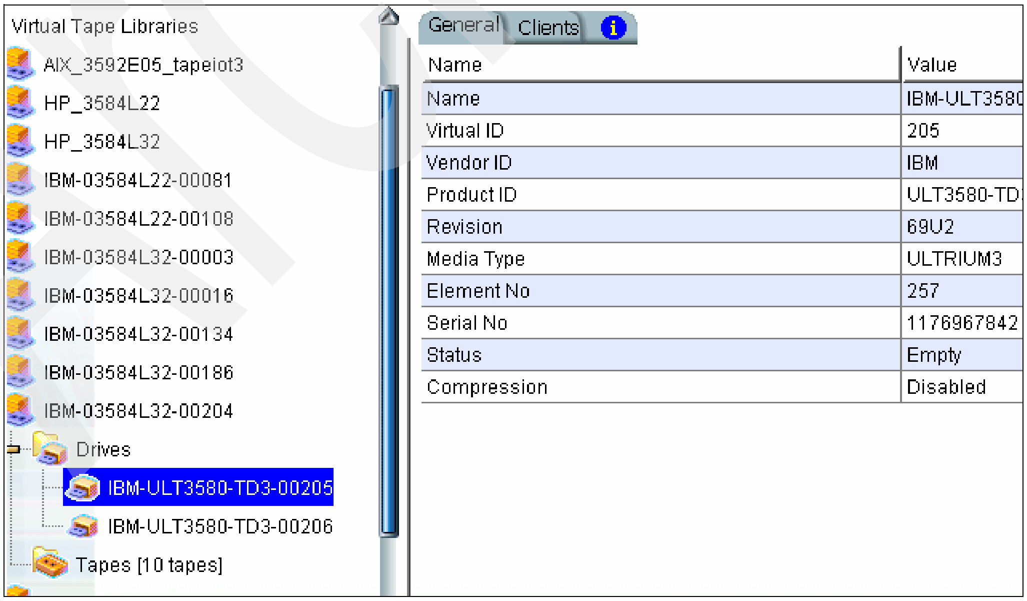
We have to write down the last seven digits (6967842 in our example). You can confirm the association between the TAPnn device and virtual tape drive on IBM Virtualization Engine TS7520 by following the text after Figure 8-30.



```
Display Resource Detail
                                                            System:   WI

Resource name . . . . . . . :   TAP159
Text . . . . . . . . . . . . :   Tape Unit
Type-model . . . . . . . . . :   3580-003
Serial number  . . . . . . . :   00-6967842
Part number  . . . . . . . . :




Location:

Logical address:
 PCI bus:
  System bus                      14
  System board                    0
  System card                     36
 Library:
                                                                      M
Press Enter to continue.
```

Figure 8-30 Tape resource details

Check the tape drives using Virtualization Engine for Tape Console. Select **Virtual Tape Library System** → **Virtual** Tape Libraries → **your tape library** → **Drives** → ***your drive***. The General tab in the right panel in Figure 8-31 shows the Serial No field for this virtual tape drive. Compare the last seven digits of this field with the last seven digits of the Serial number field from the Display Resource Detail 5250 screen.



Name	Value
Name	IBM-ULT358(
Virtual ID	205
Vendor ID	IBM
Product ID	ULT3580-TD:
Revision	69U2
Media Type	ULTRIUM3
Element No	257
Serial No	1176967842
Status	Empty
Compression	Disabled

Figure 8-31 TS7500 serial number of virtual tape drive

Important: You might have to verify the i5/OS virtual library and tape name with the serial number more than once. If, for example, you have verified the virtual tape library and tape device names on the i5/OS partition, then, in your TS7500 environment, cables are moved among a set of Fibre Channel (FC) adapters. This could cause additional i5/OS virtual tape library and virtual tape device descriptions to be created. You should work with only one set of i5/OS virtual tape library and virtual tape device descriptions.

Using iSeries Navigator

You can also use iSeries Navigator to recognize the virtual tape library and perform operations to it. If the virtual tape library is recognized, you can verify it using an iSeries Navigator interface rather than an i5/OS command-level interface.

See Figure 8-32. The example shows TAPMLB02, TAPMLB03, and TAPMLB04. Open your Server on iSeries Navigator and select **Configuration and Service** → **Hardware** → **Tape Devices** → **Tape Libraries**. Then iSeries Navigator shows the tape libraries on i5/OS partition.

Important: If iSeries Navigator does not show any TAPMLB devices, open **Configuration and Service** → **System Values** and double-click **Devices**. Confirm the check on **Local Controllers and Devices** in the Automatic configuration tab.

Sometimes you might have to perform IOP-reset to recognize the new tape library. Contact IBM Support and get the directions to perform IOP-reset.

You must recognize which virtual tape library on IBM Virtualization Engine TS7520 is TAPMLB04. The iSeries Navigator window does not directly show which virtual tape library on IBM Virtualization Engine TS7520 is the TAPMLBnn library. The tape drive serial number shown on i5/OS for TAPxx must be used to correlate this tape drive to one defined on the IBM Virtualization Engine TS7520. Right-click **TAPxx** and select **Properties,** as shown in Figure 8-32.

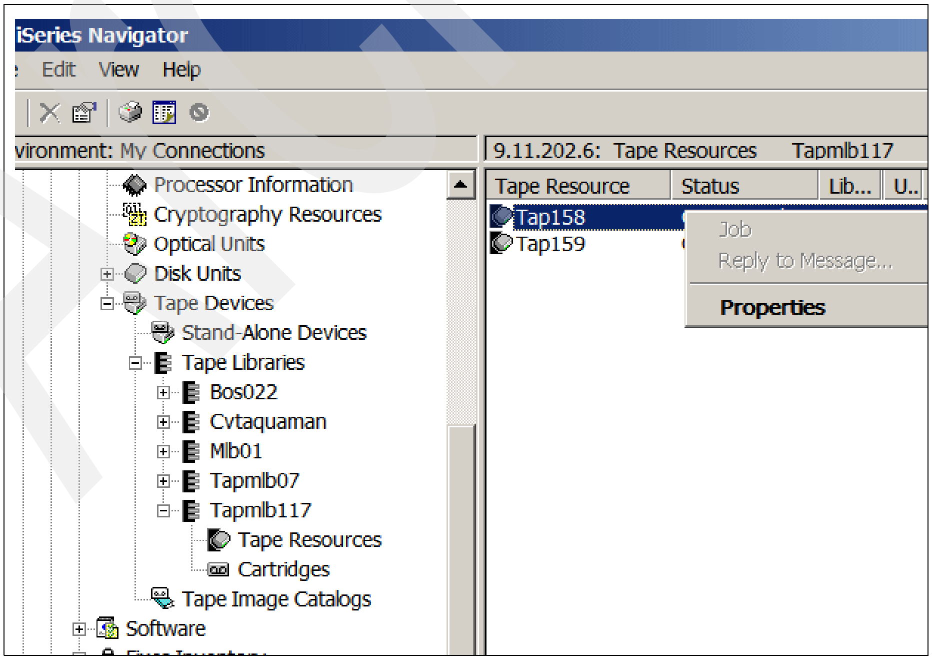
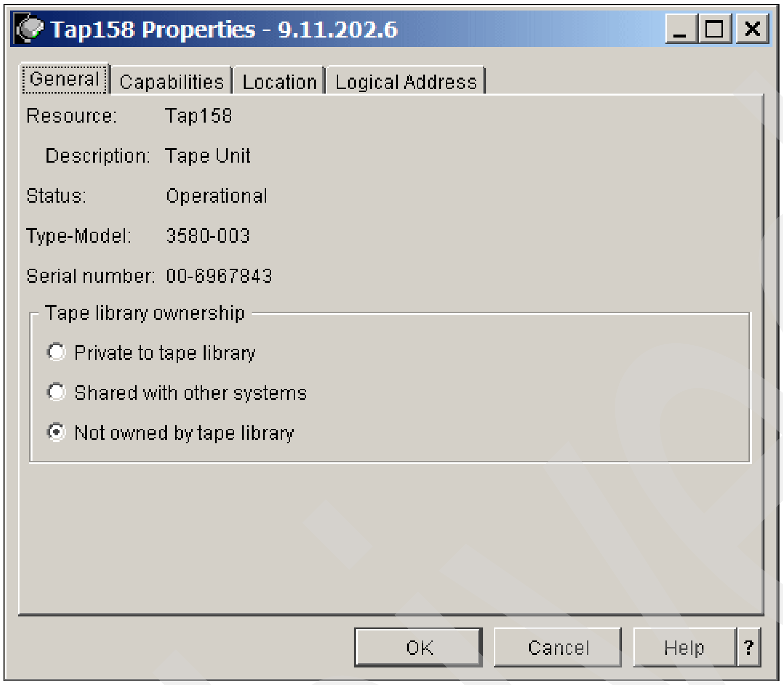


Figure 8-32 Virtual tape libraries in iSeries Navigator

See Figure 8-33. The properties of the tape device show its serial number. Use the last seven digits shown (6317110 in our example) to correlate with the corresponding serial number shown using the Virtualization Engine for Tape Console interface.



Tap158 Properties - 9.11.202.6

Resource: Tap158

Description: Tape Unit

Status: Operational

Type-Model: 3580-003

Serial number: 00-6967843

Tape library ownership

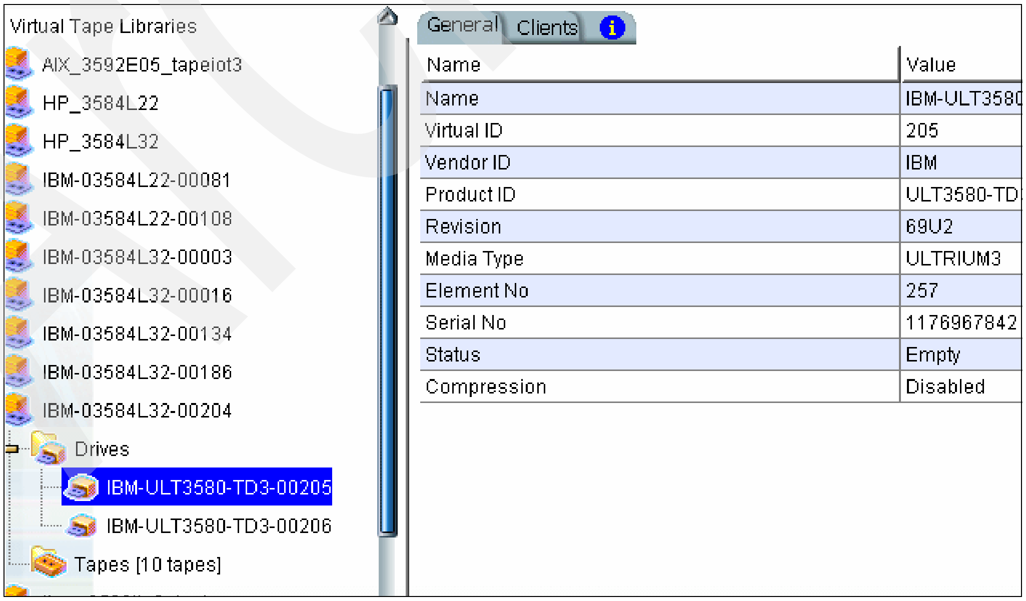
○ Private to tape library

○ Shared with other systems

● Not owned by tape library

Figure 8-33 Virtual tape drive details

From the Virtualization Engine for Tape Console, select **Virtual Tape Library System** → **Virtual** Tape Libraries → ***your tape library*** → **Drives** → ***your drive***. The General tab in the right window shows the Serial No field for this tape drive; see Figure 8-34. Compare the last seven digits of this window's serial number with the one shown in the iSeries Navigator window.



Virtual Tape Libraries
- AIX_3592E05_tapeiot3
- HP_3584L22
- HP_3584L32
- IBM-03584L22-00081
- IBM-03584L22-00108
- IBM-03584L32-00003
- IBM-03584L32-00016
- IBM-03584L32-00134
- IBM-03584L32-00186
- IBM-03584L32-00204
  - Drives
    - IBM-ULT3580-TD3-00205
    - IBM-ULT3580-TD3-00206
  - Tapes [10 tapes]

Name	Value
Name	IBM-ULT3580
Virtual ID	205
Vendor ID	IBM
Product ID	ULT3580-TD:
Revision	69U2
Media Type	ULTRIUM3
Element No	257
Serial No	1176967842
Status	Empty
Compression	Disabled

Figure 8-34 TS7500 Virtual tape drive details

Note: You use virtual tape library with i5/OS and BRMS the same way as physical tape library. For more information about usage refer to Chapter 5, “Setup for IBM tape in i5/OS” on page 107 and Chapter 6., “Implementing tape with Backup Recovery and Media Services” on page 153.

8.3 Usage examples

In this section, we describe four customer cases of using the IBM Virtualization Engine TS7520 with i5/OS partitions. We believe that these examples show typical customer scenarios where use of the IBM Virtualization Engine TS7520 is a logical choice. Use these examples to help you plan for using this product as part of your specific backup and recovery processes.

8.3.1 Four i5/OS partitions saving the entire system in different time periods

The customer has four i5/OS partitions, each of them saving different amounts of data on different days in the week. This is their backup schedule:

- System A backs up 0.7 TB of data daily from Monday to Thursday, and on Sunday. From Monday to Thursday, backups are incremental, the estimates are 0.2 TB on Monday and Tuesday, and 0.3 TB on Wednesday and Thursday. On Sunday, full backup is taken.
- System B performs full backup of 1.3 TB of data, on Saturday and Sunday.
- System C backs up 1.2 TB of data incrementally from Monday to Wednesday, 0.2 TB each day, and full backup is taken on Thursday.
- System D backs up1.5 TB of data, on Friday, Saturday, and Sunday. Full backup is taken on each of these three days.

All backups start at the same time in a day.

Table 8-2 shows these backup activities.

Table 8-2 Backup activities for Example 1

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
System A	0.2 TB	0.2 TB	0.3 TB	0.3 TB			0.7 TB
System B						1.3 TB	1.3 TB
System C	0.2 TB	0.2 TB	0.2 TB	1.2 TB			
System D					1.5 TB	1.5TB	1.5 TB
Total size	0.4 TB	0.4 TB	0.5TB	1.5 TB	1.5 TB	2.8 TB	3.5 TB

As we can see in Table 8-2, a maximum of 3.5 TB of data is being saved at the same time.

After sizing is performed, you have information about how many tape drives are to be used in each partition and how many are to be used in total at the same time. You also have information for how many IOAs in a partition to plan, and how many ports in CV5 to plan. Then decide to use all available ports in CV5 to connect to all IOA in four partitions, or zone ports so that one or more partitions use the same port in CV5.

For information how to set up and use BRMS examples, refer to Chapter 6, “Implementing tape with Backup Recovery and Media Services” on page 153.

8.3.2 Two partitions saving data with replication to remote site once a week

The customer has an i5/OS partition running Domino and another partition running WebSphere. Disaster recovery solution for both partitions is provided by IBM Virtualization Engine TS7520. IBM Virtualization Engine TS7520's replication function enables the recovery of partitions on remote site.

On the production site, full backup of user data in libraries QUSRSYS and application libraries are performed every day. The customer transported the replicated tape to a safe place and restore to a remote site on Sunday before. They plan to replicate the tapes to recovery site over TCP/IP.

i5/OS partition A saves 300 GB of user data; partition B saves 200 GB of use data.

We plan two virtual tape libraries, each of them used by one i5/OS partition. We plan the disk space in IBM Virtualization Engine TS7520 based on the time period of how long to keep each backup, as described in "Sizing the disk capacity in IBM Virtualization Engine TS7520" on page 264.

We consider that replication to the remote IBM Virtualization Engine TS7520 is the correct solution for the customer's requirements to copy backups taken on Sunday to the remote site. For more information about replication, refer to the *IBM Virtualization Engine TS7520: Planning, Implementation, and Usage Guide*, SG24-7520.

We decided to set up replication so that the replication process is triggered when the virtual tapes for Sunday's backups reach a certain size. After replication is set up, updates made to primary tape are copied to target tape on the remote site. In our case, the primary tape is rewritten with new full backup every Sunday, therefore the entire backup is replicated to remote each time.

On production IBM Virtualization Engine TS7520, the customer requires 0.3 TB for Domino partition and 0.2 TB for WebSphere Application Server partition every day of a week. Also it required 5 generations data on Sunday for one month. Table 8-3 shows the requirement space for the production IBM Virtualization Engine TS7520.

Table 8-3 Production site: Disk space for IBM Virtualization Engine TS7520

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Total
Domino partition	0.3TB	0.3TB	0.3TB	0.3TB	0.3TB	0.3TB	1.5TB	3.3TB
WebSphere Application Server partition	0.2TB	0.2TB	0.2TB	0.2TB	0.2TB	0.2TB	1.0TB	2.2TB

On the remote IBM Virtualization Engine TS7520, we size the disk space to accommodate copies of tapes for full backups taken on Sundays. We keep five generations of saved Sunday data just as we did on the primary production site.

Table 8-4 shows the disk space estimate for saved Sunday data on the backup TS7500.

Table 8-4 Backup site: Disk space for IBM Virtualization Engine TS7520

	Monday	**Tuesday**	**Wednesday**	**Thursday**	**Friday**	**Saturday**	**Sunday**	**Total**
Domino Partition							1.5TB	1.5TB
WebSphere Application Server partition							1.0TB	1.0TB

We must also consider the bandwidth of the IP connection between the production and remote sites. The connection should provide enough bandwidth for regular replication of Sunday's backups. If the data for two partitions on Sunday replicates in 3 hours, then the following bandwidth is required.

(300,000 MB + 200,000 MB) x 8 bit / 3 hours / 3600 seconds = 370 Mbps

370 Mbps speed is required for replication. Of course, 1Gbps Ethernet infrastructure is essential.

Part 3

Appendixes

A

Virtual tape in i5/OS

In this appendix, we introduce virtual tape in i5/OS. First we explain the virtual tape concept and describe how to position it. Next, we compare virtual tape with physical tape and discuss the benefits of using virtual tape.

Finally, we describe the physical devices that are supported, and how virtual tape actually works.

What virtual tape is

The virtual tape concept is a simulated tape environment within i5/OS. It consists of the following:

- Virtual tape drives (up to 35)
- Virtual tapes (256 maximum per image catalog)
- One or more image catalogs holding the virtual tapes. These are called *image catalog entries*.

This virtual environment behaves exactly as though there were real tape drives with real physical tape volumes. The virtual tape volumes are structured exactly like real tapes, with headers, tape marks, trailer labels, and so on.

You use virtual tapes exactly as you would real tapes. Commands such as DSPTAP, CHKTAP, and so on behave in the same manner as they would in real tapes. As a user you should not notice any difference. You can even flip their write protect switch.

Notice the emphasis on the word “exact”. This is because virtual tapes are *exactly* like real tapes, with only a minor difference: since they are virtual, you should copy the virtual tapes to real tape volumes and store them safely. Apart from this, no other difference exists.

Positioning the virtual tape

This section discusses the positioning of virtual tape and compares it with other virtual media services and physical tape.

Other virtual media services

The following virtual media services are available:

- Virtual optical:

  This is available in i5/OS V5R2, i5/OS V5R4, and subsequent releases. With this function, you can load optical images and use them for installation of software and PTFs.
- Virtual Tape Server (VTS):

  This is currently *not* available in i5/OS. This function, which is actually a tape server on which clients can back up their details, is available on some other platforms (for example, the IBM z/OS platform).
- Virtual tape:

  This is available in i5/OS V5R4 and subsequent releases, and can be used to back up and restore data from a virtual tape device.

Supported applications and operating systems

The virtual tape function in i5/OS provides the same functionality as a physical tape. There are, however, a few exceptions with regard to specific functions. These are discussed in Chapter 4, “Planning for IBM tape in i5/OS” on page 95.

Virtual tape in i5/OS acts as a Random Access Cartridge Loader (RACL), which is still a tape device and not a media library. All the save commands in i5/OS can use the virtual tape function.

The following applications and integrated operating systems are supported:

- Backup Recovery and Media Services (BRMS):

  BRMS V5R4 fully supports virtual tape. Chapter 4, “Planning for IBM tape in i5/OS” on page 95 provides more information about BRMS and virtual tape.

- Linux on integrated IBM eServer™ xSeries server:

  For more information about Linux and virtual tape, refer to the IBM eServer iSeries Information Center, which is available on the Web at:

  `http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp`

  In the Contents frame on the left panel, select **iSeries Information Center Version 5 Release 4**, expand **Integrated operating environments**, and select **Linux** → **Linux on an integrated xSeries solution**.

- Windows on an integrated IBM eServer xSeries server:

  Only the xSeries servers connected through the new V5R4 iSCSI support can use virtual tape. There is no support for xSeries servers connected via HSL.

- System i5 guest operating system support:

  Linux in a guest partition on i5 using virtual I/O (hosted). Currently, there is no support for AIX.

Benefits of virtual tape

Using virtual tape offers the following benefits:

- Physical tape devices do not have to be attached during backup or restore.

  This can be due to one or more of the following reasons:

  - The tape device or media library is shared between systems or partitions.
  - The tape device or media library is being used by another process or job at that time.
  - The tape device or media library is unavailable or is unstable due to a hardware defect.

  Of course, the virtual media still has to be *duplicated* to physical media, but the backup can go on.

- Virtual tape can be used to reduce backup time by running concurrent backups in situations where there are insufficient physical tape devices available to perform this task.

- You can FTP the image to other partitions or systems and add it as an entry to the image catalog. There can be multiple reasons why you want the virtual tape image on another system or partition, including these:

  - In the system on which you are running a backup or restore, there is no hardware to support the media you use for backup. In such a situation, you can back up to virtual tape and then transfer the image to a partition or system to which a physical tape device is attached.

  - You want to restore data from an image on another system and you do not use a switchable iASP to store the virtual tape images on. The image can be used in either switchable iASP or user ASP.

    For user ASP and non-switchable iASP, the only benefit is that the user ASP or iASP are on other DASDs. For switchable iASP, the image can be used for backup and restore on multiple systems, without requiring the image to be transferred to another system. You can simply switch the iASP.

- It can reduce the save time, depending on the configuration and workload.

- There are no media errors with virtual tape.

  A permanent media error causes a backup to fail, which implies that there is no complete backup.

- The concept of failed saves when using Save-While-Active (SWA) is no longer present.

  When performing a backup to physical tape, there is always a chance of a media error and with SWA checkpoint processing, there is no possibility of restarting the backup since the applications or batch jobs are already running. With virtual tape, this is no longer a concern.

- It can reduce recovery time, especially in the case of applications in which it is common practice to restore files frequently. For example, for restoring mail files in Domino, you can restore the files directly from the virtual volumes.
- It allows having a local copy of data and an offsite duplicated copy of the data. Local copies can be retained on the system for a period of time for recall of the data.
- It has the ability to save more than one library, while a user without BRMS can only save one library per save file.

Supported physical devices

Virtual tape on i5/OS supports every physical tape device that is supported on i5/OS. However, there are four different densities you can choose for virtual tape, and the density should be compatible with the physical device.

For virtual tape, density is used to control the optimum block size that the volume can use. Following are the four densities available for virtual tape:

- *VRT32K

  This does not use an optimum block size and is compatible with all physical devices.

- *VRT64K

  This uses an optimum block size of 64 KB and is compatible with 3490F model 18 track media, VXA, 8 mm devices, 35xx devices, and newer type QIC devices.

- *VRT240K

  This uses an optimum block size of 240 KB and is compatible with VXA, 8 mm devices, 35xx devices, and newer type QIC devices.

- *VRT256K

  This uses an optimum block size of 256 KB and is compatible with 35xx devices and newer type QIC devices.

For maximum performance, use the largest compatible block size. The density can only be changed with the INZTAP command.

> **Note:** A backup performed on a volume with a density that is not compatible with the physical device cannot be duplicated.

More details about virtual tape

This section provides more information about how virtual tape actually works.

Virtual tape device

A virtual tape device acts as a real tape device. It uses the same technology used by virtual optical devices, such as an image catalog and image catalog entries. The following specifications apply to virtual tape:

- Every system with V5R4 or a subsequent release installed has an IOP type 268C with a storage controller (IOA) type 6B02. These are the virtual IOPs and IOAs to which the virtual devices are to be attached.
- The virtual tape device resources have a type 63B0 and are automatically created when a virtual tape device description is created specifying `*VRT` as the hardware resource.
- You can create as many virtual tape device descriptions as you want, but the maximum number of virtual tape resources is 35. Therefore, there can be up to 35 virtual tape devices being varied on at same time.
- Virtual tape resources (type 63B0) have a status of NOT DETECTED in WRKHDWRSC or DSPHDWRSC after the next IPL, when no device description is attached. It is not necessary to delete this hardware resource.

Image catalog

Virtual tape uses the same technology as virtual optical on i5/OS. It also uses an image catalog with image catalog entries. The properties of the image catalog for virtual tape are:

- An image catalog is an object of type *IMGCLG and resides in QUSRSYS.
- When creating the image catalog, a directory in the Integrated File System (IFS) must be specified, in which the virtual volumes are to be stored.
- An image catalog must be loaded. Specify a virtual tape device before using it. The virtual tape device should be varied on.
- One image catalog can hold up to 256 virtual volumes.
- Different density types within one image catalog are allowed.

Image catalog entries

Image catalog entries in an image catalog represent the virtual tape volumes.

The following specifications apply:

- An image catalog entry is actually a streamfile in IFS residing in the directory specified for the image catalog. This streamfile has a special attribute to prevent the following:
  - Save with storage free
  - Scan processing (virus checking)
  - Journaling
- The maximum size of one image catalog entry (virtual volume) is 1000,000,000,000 bytes (1TB).
- It can be stored in iASPs or user ASPs.
- Virtual volumes can be write protected.

B

BRMS and Tivoli Storage Manager

IBM Tivoli Storage Manager and BRMS together provide a solid backup strategy. Many of the key capabilities and interfaces available with each product include these:

- User interface:
  - BRMS has a set of i5/OS BRMS commands to configure, save, restore, schedule, and otherwise manage automated running of BRMS functions. The *BRMS iSeries Navigator client* (installed as a plug-in to iSeries Navigator) offers a Windows operating system-based GUI to its functions.
  - IBM Tivoli Storage Manager offers a browser-based graphical Web administrative client interface to management functions and supports command-level statements. The command-level UNIX-like interface is available on the browser-based interface.
- Policies to manage save and restore activities:

  Both products provide similar capabilities in the following areas. Note that the defaults and implementation details may be different for each product.

  - Directory level or individual object (file)-level save and restore functions. i5/OS provides the QSYS.lib file system for library-level saves and restores.
  - Scheduled save and restore functions. BRMS uses i5/OS job scheduler as a default scheduling facility.
  - Expiration, retention, and multiple version management.
  - Full or “changed only” (incremental) saves. Defaults may be different within each product.
  - Rules to migrate saved data from disk (internal storage) to external media.
- Saves to internal storage as well as external tape device media:
  - BRMS supports saves to i5/OS save files, tape device media, or, an IBM Tivoli Storage Manager server, using the IBM Tivoli Storage Manager APIs.
  - IBM Tivoli Storage Manager, using both server and client products, supports saves to disk pools (internal storage pools), tape (pools) device media, or optical (pools) device media. The internal storage is sometimes referred to as *caching to disk*.

  - Both products support movement of saved data from this internal storage repository to external device media.
  - Depending on which product you are using, there are various levels of automated movement of internal data to external media and automatic loading of offline data previously managed by the product.
- Use and manage tape devices in tape library servers:
  - Both products support the use and media management of tape devices within a tape library server, for example:
    - Automatically mounting the required tape media
    - Allocating specific tape devices exclusively or as sharable.
  - Based upon user-specified parameter values, both products support the capability of spreading or not spreading saved data onto multiple media. For example, you may have over one terabyte of data to save. The fastest possible save can occur only if some of the objects are saved in parallel, but this can require more physical media. In some environments, you may consider this additional exposure to a tape media error. In those cases, you determine to save to fewer tape devices.
  - Both products support reclaiming tape media volumes when data on them has expired. Where you may have a mixture of expired and unexpired data on the same tape media, IBM Tivoli Storage Manager can consolidate sets of unexpired data onto a lesser number of media, potentially freeing up more media for reuse.
- Use database constructs to contain the full backup recovery and associated recovery log information:

  Both products use a database, rather than a flat file indexed catalog, to contain and access the important recovery information. BRMS contains its database in the i5/OS library QUSRBRM, while IBM Tivoli Storage Manager has a specific set of database and recovery log volumes. For either product, you must backup this information to ensure a successful disaster recovery.
- Disaster recovery facilities:

  Both products provide disaster recovery capabilities.
  - BRMS tracks on- and off-site data. Recovery reports are produced and maintained as part of the backup process. These provide step-by-step instructions for recovery. We show report examples in this book, but do not cover disaster recovery in any detail.
  - The IBM Tivoli Storage Manager's Disaster Recovery Manager (DRM) option, not covered in this book, includes tracking your on-site and off-site tapes. It also identifies which tapes to take off site. You can audit and refresh daily the automatically generated disaster recovery plan. This means your disaster recovery plan is as current as last night's backup. And, The IBM Tivoli Storage Manager V3.7 Disaster Recovery module includes electronic vaulting of the disaster recovery data to another IBM Tivoli Storage Manager server.
- Central management:

  Both products provide a level of centralized management where you either configure multiple IBM Tivoli Storage Manager servers or install the BRMS Network Management feature.
  - BRMS functions can be used under iSeries Management Central interfaces.
  - The IBM Tivoli Storage Manager central management support is part of the base product. You can use the Tivoli Enterprise Console® (TEC) and Tivoli Business System Manager to provide additional automation and business impact analysis.

- Backup and archive client functions:
  - There is a family of IBM Tivoli Storage Manager backup and archive clients for various platforms (operating systems), but none for the iSeries i5/OS. These Tivoli backup and archive clients have many functions. These include the ability to schedule the saving and restoring of data exchanged with any IBM Tivoli Storage Manager server product.
  - Using the Tivoli Storage Manager APIs for BRMS, you can configure your iSeries server to run BRMS as an iSeries BRMS Application Client to perform save and restore functions to any IBM Tivoli Storage Manager server product.

See Chapter 6., “Implementing tape with Backup Recovery and Media Services” on page 153for more information.

IBM Tivoli Storage Manager and the iSeries server

From an iSeries standpoint, IBM Tivoli Storage Manager can be viewed as:

- A server running on a System i that uses i5/OS Portable Application Solutions Environment (PASE) or in an AIX or Linux on POWER Partition on System i
- A server on a different platform to which the iSeries server saves backup data

Software support

In this section, we summarize software levels for Tivoli Storage Manager and a System i server:

- Tivoli Storage Manager V5.2 Server is the latest version available under i5/OS V5R3 PASE, but is no longer supported from Tivoli. End of support was April 30, 2007; see:

  `http://www-306.ibm.com/software/sysmgmt/products/support/lifecycle/index.html`

- Tivoli Storage Manager V5.2 was also supported for i5/OS V5R4 PASE with PTF SI25023 (APAR SE26657). See:

  `http://www-1.ibm.com/support/docview.wss?rs=663&context=SSGSG7&q1=V5R4&uid=swg21243734&loc=en_US&cs=utf-8&lang=en`

- Tivoli Storage Manager V5.3, V5.4, V5.5 are available for i5 under AIX or Linux on POWER.
- Any i5/OS V5R4 system can be a Backup Archive Client to a TSM server using BRMS and APIs (program number 5733-197).
- This client is called the “BRMS application client to Tivoli Storage Manager”. For more information, see:

  `http://www-03.ibm.com/servers/eserver/iseries/service/brms/adsmclnt.html`

- The latest version of the API is V5.5; see:

  `ftp://ftp.software.ibm.com/storage/tivoli-storage-management/maintenance/client/v5r5/OS400/v550/`

- Tivoli Storage Manager server devices can now be IBM Data Retention DR450 and DR550 servers. Saving to the retention protected servers prevents BRMS history from being deleted until the objects expire on the TSM servers. Refer to the following link for more details:

  `http://www-03.ibm.com/servers/eserver/iseries/service/brms/v5r4news.html`

IBM Tivoli Storage Manager as a client

This is a common setup where the iSeries is a client only. IBM Tivoli Storage Manager is a multiplatform set of server and client products, but there is no client IBM Tivoli Storage Manager product for the iSeries server. It is not equivalent to an IBM Tivoli Storage Manager backup and archive client product. However, you can use the iSeries BRMS Application Client setup to deliver its saved user data to any IBM Tivoli Storage Manager server in the network. The BRMS Application Client setup can request its saved data when it is needed.

All of this is possible to any IBM Tivoli Storage Manager server product, including the IBM Tivoli Storage Manager for OS/400 PASE server.

IBM Tivoli Storage Manager on iSeries (OS/400 PASE environment) as a server

Running IBM Tivoli Storage Manager under iSeries OS/400 PASE (based on AIX 5.2L) as an IBM Tivoli Storage Manager server is used when your iSeries is the primary business system. In this same environment, you can backup other servers and users in your network to this iSeries server. You can use all the IBM Tivoli Storage Manager client platform products and the iSeries BRMS Application Client to exchange saved data with the iSeries IBM Tivoli Storage Manager server.

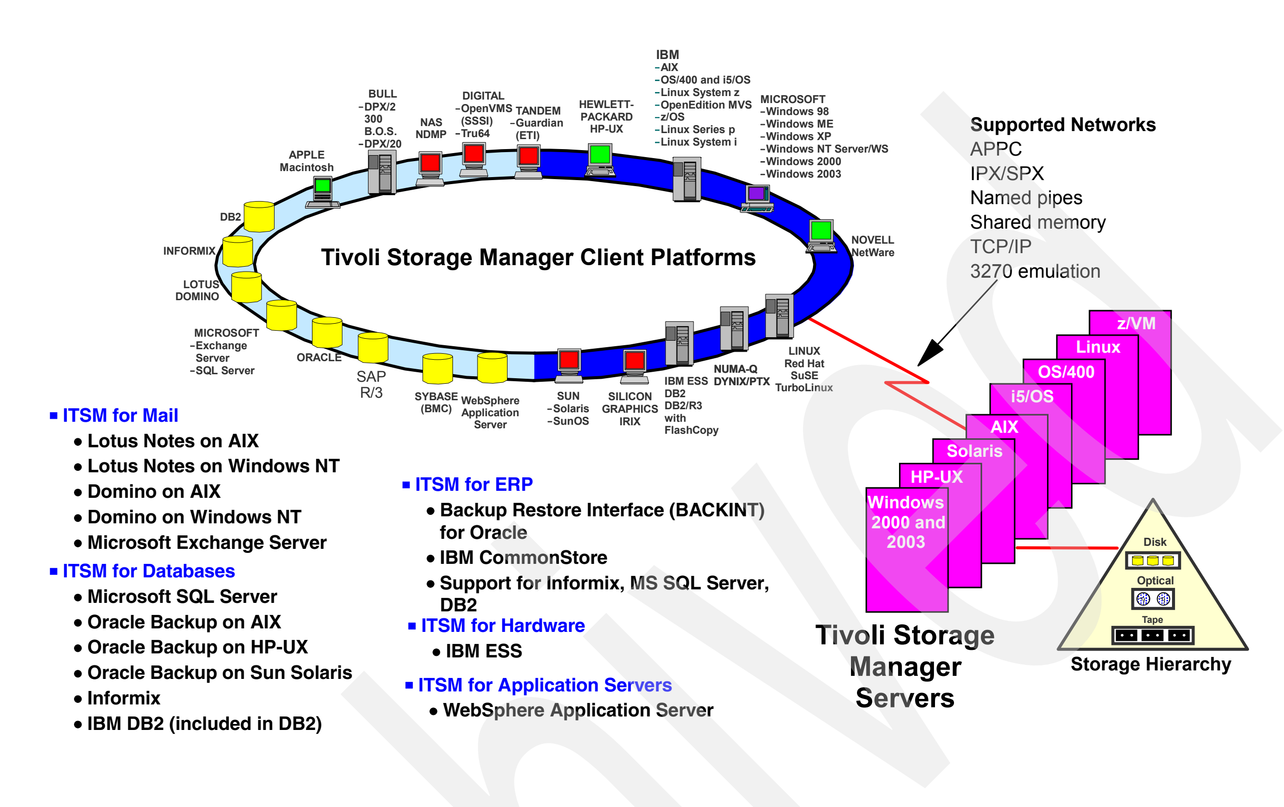
Running the IBM Tivoli Storage Manager server on the iSeries also means that you have tape and disk resources available in your iSeries server. When you use both BRMS and IBM Tivoli Storage Manager with these tape devices, you *must* plan and configure appropriately your tape management procedures.

You might have enough tape drive resources to let IBM Tivoli Storage Manager and BRMS run in parallel with separate devices or your requirement to share the same tape devices. You can schedule each product's use of a shared device so that, when one product is finished using the device, it is available for use.

You can use BRMS as an IBM Tivoli Storage Manager tape manager, which allows BRMS to handle IBM Tivoli Storage Manager's tape inventory. When you use BRMS and IBM Tivoli Storage Manager on the same system, we recommend that you have BRMS perform all tape management. To do this, you must have defined the IBM Tivoli Storage Manager tape volumes in BRMS, although BRMS does not need to actually read or write to any of those tapes.

BRMS does the mounting, demounting, and expiring of volumes on request from IBM Tivoli Storage Manager.

Figure B-1 shows the set of IBM Tivoli Storage Manager server and client products through December 2003.


Tivoli Storage Manager Client Platforms
APPLE Macintosh
BULL -DPX/2 300 B.O.S. -DPX/20
NAS NDMP
DIGITAL -OpenVMS (SSSI) -Tru64
TANDEM -Guardian (ETI)
HEWLETT-PACKARD HP-UX
IBM -AIX -OS/400 and i5/OS -Linux System z -OpenEdition MVS -z/OS -Linux Series p -Linux System i
MICROSOFT -Windows 98 -Windows ME -Windows XP -Windows NT Server/WS -Windows 2000 -Windows 2003
NOVELL NetWare
LINUX Red Hat SuSE TurboLinux
NUMA-Q DYNIX/PTX
IBM ESS DB2 DB2/R3 with FlashCopy
SILICON GRAPHICS IRIX
SUN -Solaris -SunOS
WebSphere Application Server
SYBASE (BMC)
SAP R/3
ORACLE
MICROSOFT -Exchange Server -SQL Server
LOTUS DOMINO
INFORMIX
DB2
Supported Networks
APPC
IPX/SPX
Named pipes
Shared memory
TCP/IP
3270 emulation
z/VM
Linux
OS/400
i5/OS
AIX
Solaris
HP-UX
Windows 2000 and 2003
Tivoli Storage Manager Servers
Disk
Optical
Tape
Storage Hierarchy

- ITSM for Mail
  - Lotus Notes on AIX
  - Lotus Notes on Windows NT
  - Domino on AIX
  - Domino on Windows NT
  - Microsoft Exchange Server
- ITSM for Databases
  - Microsoft SQL Server
  - Oracle Backup on AIX
  - Oracle Backup on HP-UX
  - Oracle Backup on Sun Solaris
  - Informix
  - IBM DB2 (included in DB2)
- ITSM for ERP
  - Backup Restore Interface (BACKINT) for Oracle
  - IBM CommonStore
  - Support for Informix, MS SQL Server, DB2
- ITSM for Hardware
  - IBM ESS
- ITSM for Application Servers
  - WebSphere Application Server

Figure B-1 Summary of IBM Tivoli Storage Manager server and client products

For the latest on IBM Tivoli Storage Manager products, see:

http://www-3.ibm.com/software/tivoli/products/storage-mgr/platforms.html

System backup strategies to IBM Tivoli Storage Manager

Unlike native i5/OS commands, BRMS can save and restore to or from a Tivoli Storage Manager server. You do this by using the BRMS Application Client, which is provided in the standard feature of BRMS LPP. The Tivoli Storage Manager APIs LPP (5733-197) are also necessary on the iSeries server. BRMS uses the IBM Tivoli Storage Manager server as it would use any other type of storage device. There are some advantages and restrictions when saving iSeries data to the IBM Tivoli Storage Manager server.

Advantages

The advantages of using BRMS to save to an IBM Tivoli Storage Manager server are:

- You can use BRMS policies to save non-system objects across a network for storage on any server in the IBM Tivoli Storage Manager family.
- You can reduce the amount of media that is required at the off-site location, increasing the level of backup automation.
- You can reduce the amount of time that is spent managing media.
- You can minimize device purchases on the off-site system.

Restrictions

When saving to an IBM Tivoli Storage Manager server, consider the following restrictions:

- Save-while-active *SYNCLIB is not supported when saving libraries to an IBM Tivoli Storage Manager server.
- You cannot save iSeries system data to an IBM Tivoli Storage Manager server.
  - The iSeries and BRMS architecture only allows save of system data to local media so that you are protected if you need to recover your system. Only after i5/OS is restored, communication with an IBM Tivoli Storage Manager server can be established for restoration of the user data that is stored on the server.
  - Any user data that you can save to a save file, you can also save to an IBM Tivoli Storage Manager server, except user data that is required to restore i5/OS to a functional level. This includes security data, configuration data, IBM-supplied libraries, licensed program products, IBM-supplied libraries that are considered user data such as QGPL, QUSRSYS, QUSRBRM, and BRMS media information.
- You cannot schedule operations from an IBM Tivoli Storage Manager server. However, you can schedule your BRMS operations at the client using the native i5/OS job scheduler or Advanced Job Scheduler LPP.
- BRMS uses its own media policies to manage the retention and expiration of data that is stored on the IBM Tivoli Storage Manager server. IBM Tivoli Storage Manager policies are not used for this purpose.
- You can only use BRMS to restore data saved to an IBM Tivoli Storage Manager server.

Restore considerations

When using BRMS to perform saves, there are some restore considerations:

- If you are performing a full system restore, make sure that the media is owned by the system to which you are doing the restore. If it is not, you must follow the guidance in Informational APAR II12462:

  http://www-912.ibm.com/n_dir/nas4apar.nsf/$$Search?openform
- If you saved iSeries data to an IBM Tivoli Storage Manager server, you can only restore that data from the IBM Tivoli Storage Manager server using BRMS.
- A save to an IBM Tivoli Storage Manager server only contains user data. Therefore, a full system recovery is not possible from an IBM Tivoli Storage Manager server.

C

Firmware upgrades

In this appendix we describe how to upgrade firmware on a stand-alone tape drive connected to System i, by using System i means. We describe two possible ways to do this:

- Upgrade firmware by using System i functions
- Upgrade firmware by using IBM the *IBM Tape Diagnostic Tool (IDTD)* on System i.

Upgrade firmware by using System i functions

Since OS/400 V5R1, it is possible to make a firmware update to an SCSI or FC drive from OS/400 or I5/OS. This function is supported on OS/400 and i5/OS levels from V5R1 on. Three PTFs are required for each release:

- V5R2: SI15200, SI15183, and MF33986
- V5R3: SI15201, SI15182, and MF33989
- V5R4: No particular PTFs are required.

Those PTFs are updating the device microcode (QTAUPDDV) API. The IOP 6501 is not supported and attached tape drives cannot be updated with this method.

Place firmware on System i IFS

The following steps explain how to install the firmware on the tape drive:

1. Download the latest firmware from the Web and select the drive you want to update:

   `http://www-03.ibm.com/servers/storage/tape/lto/`

   `ftp://index.storsys.ibm.com/`

2. Save this firmware to your local PC disk. This should be a Windows zip file.
3. Unzip the firmware. The result should be a XXXXXX.ro file.
4. Transfer the firmware image from your PC to the System i Integrated File System (IFS).

   Note: For more information about IFS, refer to the System i Information Center at the following Web site:

   `http://publib.boulder.ibm.com/iseries/`

The preferred method is FTPing the file into binary mode to the System i host. Follow these steps to FTP the file to your System i host:

1. Open a DOS command prompt window on your PC.
2. CD (change directory) to the directory/location of the *XXXXX.ro* file on your PC.

   For example: **`c:\cd temp\downloads`**

3. FTP *YYYYYY* (*YYYYYY*=System i name or IP address)

   Enter user name and password when prompted.

   For example: **`c:\temp\download> FTP System name`**

4. PWD (Present Working Directory) to see, on the i5/OS, in which directory you are.

   For example: **`ftp>pwd`**

   ```
   QGPL is the current library.
   ```

5. If QGPL shown as your current directory, specify command `quote site namefmt 1`, to make IFS available in FTP.
6. CD to the directory or location on the i5/OS where you want to put the .ro file.

   For example: **`ftp>cd /usr/exDir`**

7. Type **`bin`** to transfer the firmware in binary.

   For example: **`ftp>bin`**

8. Type **`put`** to transfer the .ro file.

   For example: **`ftp>put 5BG4L2S.ro`**

9. Type **`exit`** to exit.

   For example: **`ftp>exit`**

Using the QTAUPDDV API to install firmware on a tape drive

Before using the QTAUPDDV API, make sure that the drive you want to update is varied on as a stand-alone device and that there is not a cartridge loaded. Follow these steps:

1. Type the following command from the System i or iSeries prompt:

   WRKCFGSTS *DEV *TAP*

   This will show you all tape devices. Make a note which tape device you want to update, for example, `TAP03`.

2. Type the following command from the System i or iSeries prompt:

   CALL QTAUPDDV (TAP03 '/DIR/5BG4L2S.ro')

   Be sure to include the spaces.

3. What you can expect:

   The screen of the System i partition will be frozen for about four minutes. During the code load, the tape drive LED flashes. Once the download is complete, the tape drive reboots in order to load the new firmware. The System i or iSeries window comes back when the download is complete.

When this method does not work, check the following possibilities:

- Verify that the tape drive is varied on as a stand-alone device.
- Check if you transferred the firmware in binary to the iSeries (using the BIN option).
- Ensure that there is no cartridge in the tape drive.
- Verify that you are using the proper firmware image, which matches the tape drive type.
- Check this Web site for any known issues for your tape drive:

  `http://www-1.ibm.com/support/docview.wss?rs=543&context=STCVQ6R&dc=DB500&q1=ssg1*&uid=ssg1S1002478&loc=en_US&cs=utf-8&lang=en`

Upgrade firmware by using IBM Tape Diagnostic Tool

In this section we describe a method of updating the firmware of a tape drive by using the *IBM Tape Diagnostic Tool (ITDT)*. This tool provides practical way to upgrade firmware on standalone tape drives, it also offers efficient diagnostic possibilities.

The procedure to install firmware by ITDT works on both software levels V5R3 and V5R4. On V5R4, PTF SI25023 has to be installed.

> **Note:** Updating the drive firmware and a drive dump is supported. Updating the library firmware is not supported.

The latest information about ITDT is available on the following Web site:

`http://www-1.ibm.com/support/docview.wss?rs=0&uid=ssg1S1002706`

Before making an upgrade by ITDT, check the following items:

- The drive must be stand-alone, otherwise the drive is not seen by the scan.
- Use the i5/OS command `WRKMLBSTS` to deallocate the drive if allocated to a Tape library.

> **Notes:**
>
> - ITDT-SE on i5/OS requires QShell, so Qshell Interpreter (5722-SS1 Option 30) must be installed on i5/OS.
> - ITDT-SE can only be used by user with QSECOFR authorization.

To install ITDT-SE, perform the following steps:

1. Unzip itdtinst<version>i5/OS.zip (Note: The zipped save file has more than 15 MB).
2. Create a savefile ITDTI5OS on the i5/OS, by using command `CRTSAVF FILE(QGPL/ITDTI5OS)`
3. FTP the savefile on PC to the created savefile on i5/OS binary mode. To do this, perform the following steps:
   - Open a DOS command prompt window on your PC.
   - CD (change directory) to the directory/location of the XXXXX.ro file on your PC.

     For example: **`c:\cd temp\downloads`**
   - FTP *YYYYYY* (*YYYYYY*=System i name or IP address)

     Enter user name and password when prompted.

   ```
   For example: c:\temp\download> FTP System name
   ```

   - PWD (Present Working Directory) to see, on the i5/OS, in which directory you are.

   ```
   For example: ftp>pwd
   QGPL is the current library.
   ```

   - Check that QGPL shown as your current directory, if not use command `CD QGPL` to make it current directory.
   - Type **`bin`** to transfer the firmware in binary.

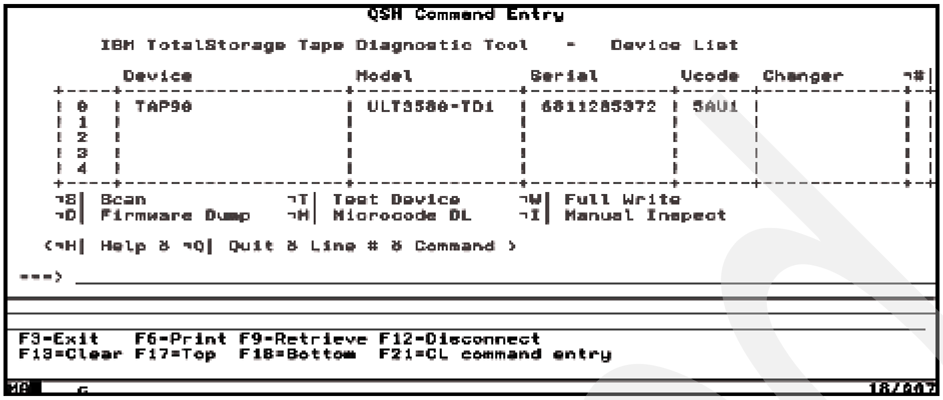
     For example: **`ftp>bin`**
   - Type **`put`** to transfer the savefile to i5/OS.

     For example: **`ftp>put itdti5os.file`**
4. Restore ITDT library by using command `RSTLIB SAVLIB(ITDT) DEV(*SAVF) SAVF(QGPL/ITDTI5OS)`

   Four objects should be restored.
5. Call the install program by using command `CALL ITDT/INSTALL`.
6. Launch the System i QShell environment by using command QSH.
7. Enable QShell support for multi-threaded programs by using command export `QIBM_MULTI_THREADED=Y` (the command is case sensitive).
8. Change to the directory home/itdt.

9. Start ITDT.

   After the scan, the output in i5/OS looks like the screen in Figure C-1.

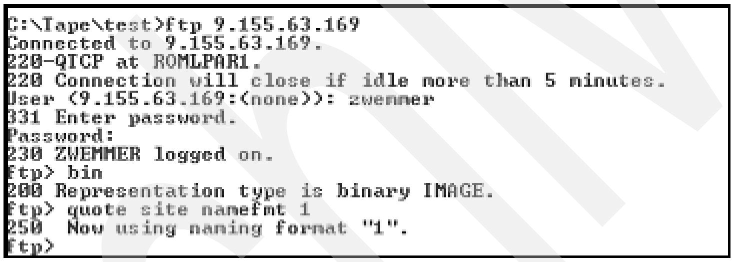


```
                              QSH Command Entry

     IBM TotalStorage Tape Diagnostic Tool   -   Device List

       Device                 Model          Serial        Ucode  Changer      ¬#|
   +----+----------------------+---------------+--------------+------+-------------+-+
   | 0  | TAP90                | ULT3580-TD1   | 6811285372   | 5AU1 |             | |
   | 1  |                      |               |              |      |             | |
   | 2  |                      |               |              |      |             | |
   | 3  |                      |               |              |      |             | |
   | 4  |                      |               |              |      |             | |
   +----+----------------------+---------------+--------------+------+-------------+-+
   ¬S| Scan                ¬T| Test Device      ¬W| Full Write
   ¬D| Firmware Dump       ¬M| Microcode DL     ¬I| Manual Inspect

  <¬H| Help & ¬Q| Quit & Line # & Command >

 ===> ____________________________________________________________________________


 F3=Exit    F6=Print F9=Retrieve F12=Disconnect
 F13=Clear F17=Top   F18=Bottom  F21=CL command entry
MB     c                                                                    18/007
```

Figure C-1   Qshell screen after scan

10. Download the drive firmware to your PC from one of the known IBM Web sites and FTP it in binary mode to the following directory in i5/OS IFS: /home/itdt/input

11. Use FTP as described in point 3, but use the FTP command **`QUITE SITE NAMEFMT 1`** to make FTP point to IFS. This is shown in Figure C-2.



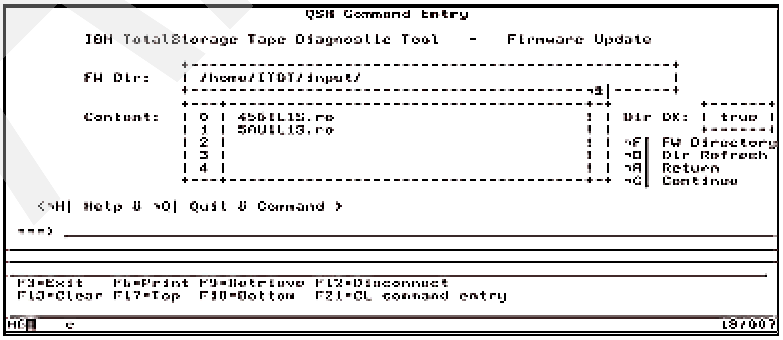
```
C:\Tape\test>ftp 9.155.63.169
Connected to 9.155.63.169.
220-QTCP at ROMLPAR1.
220 Connection will close if idle more than 5 minutes.
User (9.155.63.169:(none)): zwemmer
331 Enter password.
Password:
230 ZWEMMER logged on.
ftp> bin
200 Representation type is binary IMAGE.
ftp> quote site namefmt 1
250  Now using naming format "1".
ftp>
```

Figure C-2   FTP file with firmware

Update the drive firmware by performing the following steps:

1. Select the device you want to update by entering its number (in our example it is **`0`**) and press Enter.

2. Type **`M`** and press Enter to display the firmware update screen: This firmware resides in the IFS directory /home/itdt/input as shown in Figure C-3.

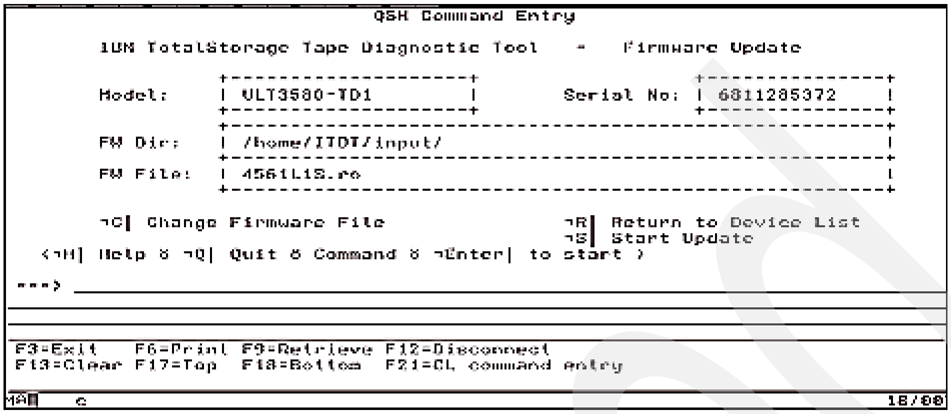


```
                              QSH Command Entry

     IBM TotalStorage Tape Diagnostic Tool   -   Firmware Update

                    +----------------------------------------------+
     FW Dir:        | /home/ITDT/input/                            |
                    +-----------------------------------¬S|-------+
                    +---+--------------------------------+-+        +-------+
     Content:       | 0 | 45BIL15.ro                     | |  Dir OK: | true |
                    | 1 | 5AU1L13.ro                     | |          +-------+
                    | 2 |                                | |  ¬F| FW Directory
                    | 3 |                                | |  ¬D| Dir Refresh
                    | 4 |                                | |  ¬R| Return
                    +---+--------------------------------+-+  ¬C| Continue

  <¬H| Help & ¬Q| Quit & Command >

 ===> ____________________________________________________________________________


 F3=Exit    F6=Print F9=Retrieve F12=Disconnect
 F13=Clear F17=Top   F18=Bottom  F21=CL command entry
MB     c                                                                    19/007
```

Figure C-3   Firmware Update screen

3. Select the firmware (by entering the number) you want to use for your update and then C for continue.

4. The output you get is similar to the screen shown in Figure C-4.



```
                               QSH Command Entry

        IBM TotalStorage Tape Diagnostic Tool    -    Firmware Update

                  +---------------------+                  +----------------+
        Model:    | ULT3580-TD1         |       Serial No: | 6811285372     |
                  +---------------------+                  +----------------+
                  +-------------------------------------------------------------+
        FW Dir:   | /home/ITDT/input/                                           |
                  +-------------------------------------------------------------+
        FW File:  | 4561L1S.ro                                                  |
                  +-------------------------------------------------------------+

        ¬C| Change Firmware File                   ¬R| Return to Device List
                                                   ¬S| Start Update
   <¬H| Help & ¬Q| Quit & Command & ¬Enter| to start >
 ===> ____________________________________________________________________________


 F3=Exit    F6=Print  F9=Retrieve F12=Disconnect
 F13=Clear F17=Top   F18=Bottom  F21=CL command entry

MA      c                                                                  18/007
```

Figure C-4   Output of selecting firmware and continue

5. With an S you can start the firmware update.

6. To get dumps of the drive, follow the description in the link:

   http://www-1.ibm.com/support/docview.wss?rs=0&uid=ssg1S1002706

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

For information about ordering these publications, see “How to get IBM Redbooks” on page 314. Note that some of the documents referenced here may be available in softcopy only.

- *IBM Tape Library Guide for Open Systems,* SG24-5946
- *Designing an IBM Storage Area Network,* SG24-5758
- *iSeries in Storage Area Networks: A Guide to Implementing FC Disk and Tape with iSeries*, SG24-6220
- *Logical Partitions on System i5: A Guide to Planning and Configuring LPAR with HMC on System i*”, SG24-8000
- *IBM System i5 Handbook: IBM i5/OS Version 5 Release 4*, SG24-7486
- *IBM System i5, eServer i5 and iSeries System Builder: IBM i5/OS Version 5 Release 4*, SG24-2155
- *Introduction to Storage Area Networks,* SG24-5470
- *Backup Recovery and Media Services for OS/400 A Practical Approach,* SG24-4840
- *IBM System Storage Tape Encryption Solutions: Planning, Implementation and Usage Guide*, SG24-7320
- *The IBM Virtualization Engine TS7510: Getting started with i5/OS and Backup Recovery and Media Services, SG24-7510*
- *IBM Virtualization Engine TS7520: Planning, Implementation, and Usage Guide*, SG24-7520

Other resources

- *IBM System Storage TS3100 Tape Library and TS3200 Tape Library Installation Quick Reference*, GA32-0548
- *IBM System Storage TS3310 Tape Library Setup and Operator Guide,* GA32-0477
- *IBM System Storage TS3400 Tape Library Planning and Operator Guide*, GC27-2107
- *IBM Encryption Key Manager Component for the Java platform: Introduction, Planning and User’s Guide*, GA76-0418

Online resources

These Web sites are also relevant as further information sources:

- Linear Tape-Open Home Page:

  http://www.lto.org
- IBM LTO home page:

  http://www.ibm.com/storage/lto
- Compatibility matrix:

  http://www-03.ibm.com/servers/storage/tape/compatibility
- Java Home Page:

  http://java.com/en/
- IBM Tape Library Publications:

  http://www-1.ibm.com/servers/storage/tape/resource-library.html#publications
- *IBM TotalStorage UltraScalable Tape Library TS3500 Tape Library Advanced Library Management System Technology White Paper:*

  http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101038
- System i Single-Level Storage Architecture:

  http://www-03.ibm.com/servers/enable/site/porting/iseries/overview/overview.html
- System i5 Server Consolidation:

  http://www-03.ibm.com/systems/i/os
- *IBM Hardware Systems Information Center* section “Partitioning the server”:

  http://www.redbooks.ibm.com/redbooks/pdfs/sg248000.pdf
- *System i Performance capabilities Reference i5/OS Version 5 release 4:*

  http://www-03.ibm.com/servers/eserver/iseries/perfmgmt/resource.html
- System i Information Center:

  http://publib.boulder.ibm.com/iseries/
- TS1120/TS3500 Tape Encryption on System i:

  http://www-03.ibm.com/support/techdocs/atsmastr.nsf/84279f6ed9ffde6f86256ccf00653ad3/fb77227fc78f069d862572500021bcf9?OpenDocument
- JCE Policy files:

  https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk
- IBM Java Keytool Users Guide:

  http://www-128.ibm.com/developerworks/java/jdk/security/50/secguides/keytoolDocs/KeyToolUserGuide-150.html

How to get IBM Redbooks

You can search for, view, or download Redbooks, IBM Redpapers, Technotes, draft publications and Additional materials, as well as order hardcopy Redbooks, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

Implementing IBM Tape in i5/OS

(0.5” spine)
0.475”<->0.873”
250 <-> 459 pages

Implementing IBM Tape in i5/OS

Learn about IBM Tape Solutions

Use BRMS to manage Tape Libraries

Protect your data with Tape Encryption

This IBM Redbooks publication follows *The IBM System Storage Tape Libraries Guide for Open Systems*, SG24-5946, and can help you plan, install, and configure IBM Ultrium LTO tape drives, as well as the TS1120 Tape Drive and libraries in i5/OS environments. The book focuses on the setup and customization of these drives and libraries.

The first part of the book gives an overview of the System i family of servers and describes how to attach and configure the drives and libraries. It also covers basic installation and administration. We describe the sharing and partitioning of libraries and explain the concept and usage of the Advanced Library Management System (ALMS).

In the second part of the book, we document how to use these products with Backup Recovery and Media Services (BRMS), how to implement Tape Encryption, and how to use the IBM TS7520 Virtualization Engine with i5/OS.

This book can help IBM personnel, Business Partners, and customers to better understand and implement the IBM Ultrium LTO product line, and also the TS1120 Tape Drive attached to System i servers. We assume that the reader is familiar with tape drives and libraries and has a basic understanding of System i servers and i5/OS.

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

SG24-7440-00 ISBN 0738488569