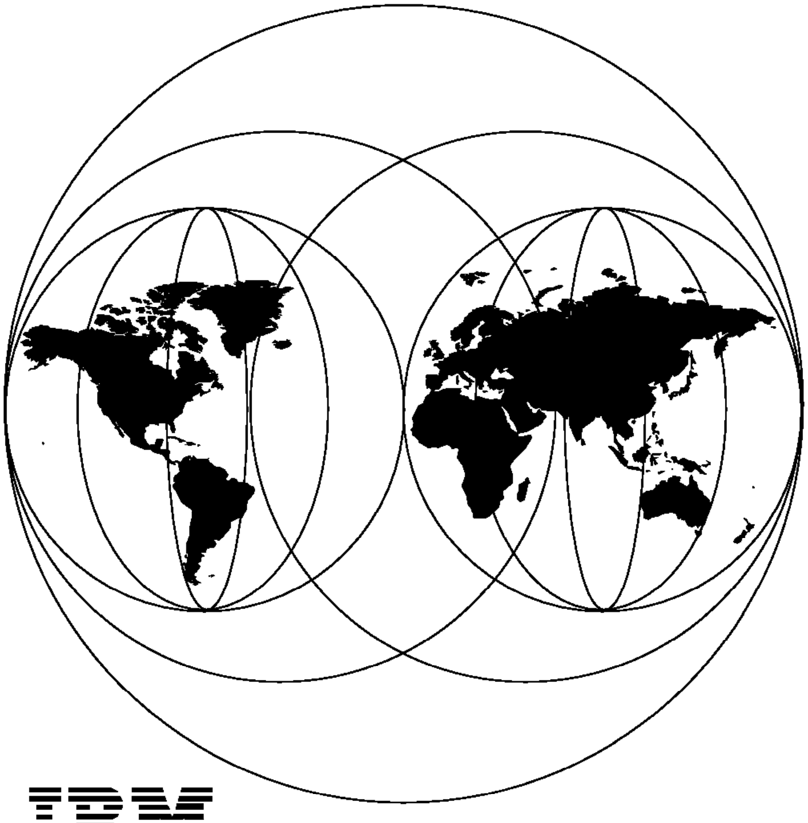
International Technical Support Organization

SG24-4631-00

Using ADSM Hierarchical Storage Management

April 1996



IBM
International Technical Support Organization
San Jose Center

International Technical Support Organization

SG24-4631-00

Using ADSM Hierarchical Storage Management

April 1996

Take Note!

Before using this information and the product it supports, be sure to read the general information under “Special Notices” on page xiii.

First Edition (April 1996)

This edition applies to ADSTAR Distributed Storage Manager for AIX Version 2 Release 1 5765-564 and ADSTAR Distributed Storage Manager for MVS Version 2 Release 1 5655-119.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

An ITSO Technical Bulletin Evaluation Form for reader′s feedback appears facing Chapter 1. If the form has been removed, comments may be addressed to:

IBM Corporation, International Technical Support Organization
Dept. 471 Building 80-E2
650 Harry Road
San Jose, California 95120-6099

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Abstract

ADSM Hierarchical Storage Management (HSM) enables AIX servers and workstations to migrate infrequently used data to an ADSM server. The migrated data can be transparently or explicitly recalled when it is needed. This document provides information about implementing HSM and recommendations for setting up and maintaining your environment.

(129 pages)

Contents

Figures

Tables

Special Notices

This publication is intended to help ADSM and AIX administrators and users responsible for implementing ADSM Hierarchical Storage Management (HSM). The information in this publication is not intended as the specification of any programming interfaces that are provided by ADSM. See the PUBLICATIONS section of the IBM Programming Announcement for ADSM for AIX and ADSM for MVS for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM′s product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM′s intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter 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 the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM (VENDOR) products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer′s ability to evaluate and integrate them into the customer′s operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

The following document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain 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.

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

ADSTAR	AIX
IBM	

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Windows is a trademark of Microsoft Corporation.

HP, Hewlett-Packard	Hewlett-Packard Company
SunOS, SPARCstation, Network File System, NFS	Sun Microsystems, Inc.
1-2-3, Lotus, Freelance, Freelance Graphics	Lotus Development Corporation

Other trademarks are trademarks of their respective companies.

Preface

ADSM Hierarchical Storage Management (HSM) enables AIX servers and workstations to migrate infrequently used data to an ADSM server. The migrated data can be transparently or explicitly recalled when it is needed. This document provides information about implementing HSM and recommendations for setting up and maintaining your environment.

This document is written for IBM, customer, and consultant personnel who are familiar with ADSM for backup and archive and want to understand how to use HSM for space management.

How This Document Is Organized

The document is organized as follows:

- Chapter 1, "HSM Overview"

  This chapter provides an overview of the ADSM HSM functions.

- Chapter 2, "HSM Setup Philosophies"

  There are many ways to implement HSM, given the number of parameters and options from which to choose. This chapter describes our recommendation for setting up an HSM environment that has the least impact on your end users. A methodology for monitoring HSM activity is also discussed.

- Chapter 3, "Implementing HSM"

  This chapter covers the main tasks necessary to implement HSM. Planning considerations are also covered.

- Chapter 4, "Care and Feeding of HSM"

  Once you have set up your HSM environment, you must provide for its continued care and feeding. Maintenance tasks for HSM control files, directories, and daemons are discussed as well as HSM and AIX interoperability.

- Chapter 5, "How to Use HSM"

  This chapter provides detailed examples of using HSM to selectively migrate and recall files and to view the results.

- Chapter 6, "Migrating NFS File Systems"

  When an HSM client is also an NFS server, it can be used to provide space management function to non-AIX platforms. This chapter describes how HSM works in an NFS environment, discusses NFS setup considerations and provides scenarios on how HSM and NFS work together.

- Chapter 7, "Recovery with ADSM and HSM"

  This chapter describes the steps required to recover files, an entire file system, and an entire AIX workstation that is HSM managed. It also provides a checklist of information needed to re-create a lost or destroyed file system.

- Appendix A, "Macros Used to Set Up Automation"

This appendix contains an ADSM macro that can be used to define schedules to perform reconcile, automatic migration, and resetting of age and size priority based on the recommendations in Chapter 2, "HSM Setup Philosophies"

- Appendix B, "Determining Average and Distribution of File Sizes"

  This appendix describes how to obtain information on average file size and distribution of files sizes on an HSM client.

- Appendix C, "Common UNIX Commands and Recall"

  This appendix contains two tables that describe some common UNIX commands that may not require a recall and that usually require a recall when the command is performed against a migrated file.

- Appendix D, "Fixfsm Script for Re-creating .SpaceMan Files"

  This appendix contains a shell script that can be used when some or all files in the .SpaceMan directory are lost. The script will re-create the missing files.

Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book. At the time of writing, HSM function was available on the ADSM Version 2 MVS and AIX servers and the AIX client.

- ADSM Publications
  - *ADSM Online Product Library CD-ROM*, SK2T-8714

    All of the ADSM publications are available in online readable format on the CD-ROM listed above. The ADSM library is also available on the following CD-ROMs:

    - *MVS Base Collection Kit*, SK2T-0710
    - *AIX Base Collection Kit*, SK2T-2066
    - *IBM SystemView for AIX*, SK2T-1451
  - *ADSM: General Information*, GH35-0131
  - *ADSM for AIX: Installing the Server and Administrative Client*, SH35-0136
  - *ADSM for MVS: Installing the Server and Administrative Client*, SH26-4043
  - *ADSM for AIX: Administrator's Guide*, SH35-0134
  - *ADSM for MVS: Administrator's Guide*, SH26-4039
  - *ADSM for AIX: Administrator's Reference*, SH35-0135
  - *ADSM for MVS: Administrator's Reference*, SH26-4040
  - *ADSM: Messages*, SH35-0133
  - *ADSM: Installing the Clients*, SH26-4049
  - *ADSM: Using the UNIX Hierarchical Storage Management (HSM) Clients*, SH26-4030
  - *ADSM Version 2: Using the UNIX Backup/Archive Clients*, SH26-4052
  - *ADSM: Client Reference Cards*, SX26-6013

  - *ADSM Version 2 Performance Evaluation Report*, available in the ADSM21PE PACKAGE on MKTTOOLS

- Related Publication

  - *AIX Version 3.2 and 4.1 Performance Monitoring and Tuning Guide*, SC23-2365

International Technical Support Organization Publications

- *ADSM Presentation Guide*, GG24-4146
- *ADSM Version 2 Presentation Guide*, SG24-4532
- *ADSM Implementation Examples*, GG24-4034
- *ADSM Advanced Implementation Examples*, GG24-4221
- *Getting Started with ADSM/2*, GG24-4321
- *Getting Started with ADSM/6000*, GG24-4421
- *Getting Started with the NetWare Client*, GG24-4242
- *Getting Started with the AIX/6000 Client*, GG24-4243
- *ADSM API Examples for OS/2 and Windows*, SG24-2588
- *Using ADSM to Back Up Databases*, SG24-4335
- *Using ADSM to Back Up Lotus Notes*, SG24-4534
- *ADSM for AIX: Advanced Topics*, SG24-4601
- *ADSM for MVS: Recovery and Disaster Recovery*, SG24-4537
- *ADSM for MVS: Using Tapes and Tape Libraries*, SG24-4538
- *AIX Storage Management*, GG24-4484
- *ADSM/VSE Implementation*, GG24-4266
- *Setting Up and Implementing ADSM/400*, GG24-4460
- *AIX Storage Management Products Comparison*, GG24-4495
- *ADSM/6000 on 9076 SP2*, GG24-4499
- Related Publication
  - *Using NFS in a Multivendor Environment*, GG24-4087
- Related ITSO Sold Bills of Form
  - *AIX Application Development and Database*, SBOF-6339
  - *AIX Operating System/Systems Management and High Availability*, SBOF-6338
  - *RISC System/6000 Hardware*, SBOF-6340
  - *Distributed Storage Management*, SBOF-6311

A complete list of International Technical Support Organization publications, known as redbooks, with a brief description of each, can be found in:

> *International Technical Support Organization Bibliography of Redbooks,* GG24-3070.

To get a catalog of ITSO redbooks, VNET users may type:

```
TOOLS SENDTO WTSCPOK TOOLS REDBOOKS GET REDBOOKS CATALOG
```

A listing of all redbooks, sorted by category, may also be found on MKTTOOLS as ITSOPUB LISTALLX. This package is updated monthly.

How to Order ITSO Redbooks

IBM employees in the USA may order ITSO books and CD-ROMs using PUBORDER. Customers in the USA may order by calling 1-800-879-2755 or by faxing 1-800-445-9269. Most major credit cards are accepted. Outside the USA, customers should contact their local IBM office. Guidance may be obtained by sending a PROFS note to BOOKSHOP at DKIBMVM1 or E-mail to bookshop@dk.ibm.com.

Customers may order hardcopy ITSO books individually or in customized sets, called SBOFs, which relate to specific functions of interest. IBM employees and customers may also order ITSO books in online format on CD-ROM collections, which contain redbooks on a variety of products.

ITSO Redbooks on the World Wide Web (WWW)

Internet users can find information about redbooks on the ITSO World Wide Web home page. To access the ITSO Web pages, point your Web browser (such as WebExplorer from the OS/2 3.0 Warp BonusPak) to the following:

```
http://www.redbooks.ibm.com/redbooks
```

IBM employees can access LIST3820s of redbooks as well. Point your web browser to the IBM Redbooks home page:

```
http://w3.itsc.pok.ibm.com/redbooks/redbooks.html
```

Acknowledgments

This project was designed and managed by:

Cybelle Beaulieu
International Technical Support Organization-San Jose Center

The authors of this document are:

Dave Canan
IBM North America

Roland Leins
IBM Germany

Joerg Pohlmann
IBM Canada

Ullfried Streu
IBM Storage Systems Division, Mainz

Cindy Sullivan
IBM Storage Systems Division, San Jose

Zhu Xiaowen
IBM China

This publication is the result of a residency conducted at the International Technical Support Organization- San Jose Center.

Thanks to the following people for the invaluable advice and guidance provided in the production of this document:

Lee Heslop
IBM Storage Systems Division, San Jose

Barry Herman
IBM Storage Systems Division, San Jose

Ed Quigley
IBM Storage Systems Division, San Jose

Kitty Stein
IBM Storage Systems Division, San Jose

Stefan Steiner
IBM Research Division, Almaden Research Center

Chapter 1. HSM Overview

ADSTAR Distributed Storage Manager (ADSM) provides a comprehensive storage management solution for workstations and file servers in a network environment. It includes backup, archive, and migration services. At the time of writing, HSM function was available on the ADSM Version 2 MVS and AIX servers and the AIX client.

1.1 Understanding Backup, Archive, and Migration

The ADSM *backup-archive client* provides these services:

Backup Provides data protection services

Backup makes successive copies of your files. You can restore the copies if the original files are accidentally deleted, corrupted, or lost because of a hardware failure.

Archive Provides data retention services

Archive makes essentially permanent copies of your files. You can keep the copies indefinitely. You can delete the original files from your local file systems and retrieve the archived copies when you need them.

The ADSM *hierarchical storage management client* provides this service:

Migration Provides space management services

Migration automatically moves infrequently used or large files to distributed storage devices through an ADSM server to free space on your local file systems. Stub files, which contain the information required to recall migrated files, are left on your local file systems so that the files appear to reside locally (for example, migrated files are listed by the UNIX **ls** command). Files are recalled to your local file systems automatically when they are accessed. No user intervention is necessary, although you can choose to migrate or recall selected files.

Although backup, archive, and migration provide similar services in some respects, each meets the specific needs of your data.

The sections that follow compare the various services. For more detailed information about using backup and archive services, see *ADSM Version 2: Using the UNIX Backup-Archive Clients*.

1.1.1 Do You Want to Back Up or Archive Files?

When ADSM backs up or archives a file, it sends a copy of the file and its associated attributes to an ADSM server. However, backups and archives have different purposes.

Backups are used to protect against file damage or loss. A sequence of backup versions is kept for each file on your workstation (your ADSM administrator sets the number of versions), and older versions are deleted as newer versions are made.

Archives, however, are more permanent. An archived copy of a file is used to maintain the file in a particular state indefinitely (although your administrator also sets a limit on how long archives are kept). An archived copy is useful if you think you might have to go back to a particular version of a file or want to delete a file from your workstation and still be able to retrieve it. For example, you might have to save some spreadsheets for tax purposes but do not want to leave them on your workstation because you are not using them.

Use backups to protect against unforeseen damage to your files, and archives to maintain point-in-time copies of your files.

1.1.2 Do You Want to Archive or Migrate Files?

You can use both archive and migration to free space on your local file systems. However, there are instances where it is more efficient to use one service instead of the other. The sections that follow provide some examples.

1.1.2.1 Providing Continuous Space Management

For continuous space management, ADSM migrates and recalls files automatically as needed. A root user on your workstation can set options and space management settings to obtain optimal results. The options and settings determine which files are eligible for automatic migration, the order in which files are migrated, where the migrated files are stored, and how much free space is maintained on a local file system.

If you use ADSM to migrate files automatically, you save the time it would take to decide which files to archive and delete from your local file systems and to initiate archive operations yourself.

1.1.2.2 Working with Large Groups of Files

Because migrated files are designed to appear as though they reside locally, migration and recall are highly integrated with the operations of your operating system. Therefore, when files are migrated or recalled, ADSM must process them individually.

You can migrate and recall selected files. However, you should use that method of manually storing and accessing files only when you are working with a small number of files or for special situations where you want to recall one or more migrated files before you begin working with them.

For planned processes, such as storing a large group of files in ADSM storage and bringing the files back to a local file system all at once for processing, you should use archive and retrieve. For example, if you have a large number of files that are updated only once a week or once a month by a particular program, you can archive those files to save space on your local file system. Then, when you have to update the files, you can retrieve them all at one time. To simplify the process, your ADSM administrator can set up a schedule to retrieve all of the files at a particular time and then archive them after they are updated. You can assign a single description to a group of files and use that description to retrieve the files, making it easier to retrieve the entire group.

You can archive a file as many times as you want, creating multiple copies of the file. For example, you can archive a group of files containing accounting information at the end of each month. Migrate moves the copy of the file to ADSM storage so you only have one copy of any one file.

1.1.3 Do You Want to Migrate or Back Up Files?

Migration is not a replacement for backup. Migration only frees space on your local file systems. Unlike file backup, it does not protect against accidental file deletion, file corruption, or disk failure.

You should continue to back up all of your important files whether they reside on your local file system or are migrated to ADSM storage.

1.2 Understanding Hierarchical Storage Management

With ADSM hierarchical storage management, new files and the files you use most frequently remain on your local file systems, while those you use less often are automatically migrated to distributed storage devices through an ADSM server. You can also specify that files be prioritized for migration according to their size and/or the number of days since they were last accessed and their size.

By migrating eligible files to distributed storage devices, HSM frees space for new data on your local file systems and takes advantage of lower cost storage resources available in your network environment.

Files migrated to ADSM storage are easily accessible. When you access a migrated file, HSM automatically recalls it to your local file system. If you choose, HSM can recall a migrated file temporarily. If you do not modify the file, HSM automatically changes it back to a migrated file when you close it. You can also choose to have HSM read a migrated file from ADSM storage without storing it on your local file system.

HSM ensures the integrity of your data and provides the same level of security for migrated files as that provided by your operating system file systems. It works hand in hand with your operating system file system to provide advanced hierarchical storage management services, while maintaining optimal file system performance.

1.2.1 Migrating Files from a Local File System

To migrate a file, HSM sends a copy of the file to an ADSM server and replaces the original file with a stub file on the local file system. It does not change the access time (atime) or permissions for the file.

The ADSM server places the file in ADSM storage. ADSM storage consists of storage volumes on disk devices or devices that support removable media such as tape. Your ADSM administrator defines and groups the storage volumes into storage pools.

A *stub file* is a small file that contains the information required to locate and recall a migrated file. It also makes it appear as though the file still resides on your local file system. In addition, a stub file contains information that HSM can use to respond to specific UNIX commands, such as **ls**, without recalling the file.

HSM provides space management services for locally mounted file systems. HSM migrates only regular files. It does not migrate character special files, block special files, first-in-first-out (FIFO) special files (named pipe files), or directories.

HSM provides both automatic and selective migration.

1.2.1.1 Automatic Migration

To ensure that free space is available on your local file systems, HSM monitors space usage and automatically migrates files whenever necessary.

HSM migrates only those files that are eligible for automatic migration. Eligibility is based on the space management options and settings chosen by a root user on your workstation. The primary requirement for eligibility is the number of days since a file was last accessed. Other factors such as file size and whether or not the file has been backed up also influence the eligibility of a file to be migrated.

HSM provides two types of automatic migration:

Threshold migration Maintains a specific level of free space on a local file system.

HSM checks space usage on your local file systems at the intervals specified by a root user. The default interval is every 5 minutes. When space usage reaches the *high threshold* set for a file system, HSM automatically begins migrating eligible files to ADSM storage. When space usage drops to the *low threshold* set for a file system, HSM stops migrating files.

A root user can also start threshold migration for a file system before space usage reaches the high threshold. If space usage exceeds the low threshold set for the file system when a root user starts threshold migration manually, HSM migrates eligible files until space usage drops to the low threshold.

Demand migration Responds to an out-of-space condition on a local file system.

HSM checks for an out-of-space condition every 2 seconds. If a file system runs out of space, HSM automatically starts threshold migration. As files are migrated, space becomes available on the file system, and the process that caused the out-of-space condition can continue. The process does not have to wait until threshold migration is complete, and you do not receive an out-of-space error message.

The following are examples of how threshold migration and demand migration work:

- If a root user sets the high threshold for a file system to 90% and the low threshold to 70%:
  - HSM begins migrating files to ADSM storage whenever 10% or less free space is available on the file system. On a 100-MB file system, it would begin migrating files when 10 MB or less are available.
  - HSM stops migrating files when 30% or more free space is available on the file system. On a 100-MB file system, it would stop migrating files when at least 30 MB of free space are available.
- If you attempt to copy a very large file into one of your file systems, and there is not enough space available to hold the entire file, HSM automatically

begins migrating eligible files from the local file system to ADSM storage. As space becomes available, the process can continue copying the file to the file system.

1.2.1.2 Selective Migration

You can use *selective migration* to move specific files from a local file system to ADSM storage. For example, if you know you will not be using a particular group of files for an extended period of time, you can choose to migrate them to ADSM storage right away to free additional space on a local file system.

HSM migrates only those files that are eligible for selective migration. Eligibility is based on the space management options and settings chosen by a root user on your workstation. For example, a file must be at least the minimum size required for migration. However, unlike automatic migration, the number of days since a file was last accessed has no effect on whether the file is eligible for selective migration.

If you are a root user, you can selectively migrate all files on your workstation that are eligible for selective migration. If you are a user, you can selectively migrate any file you own that is eligible for selective migration.

1.2.2 Premigrating Files for a Local File System

To make migration faster, HSM prepares files for automatic migration, using a process called *premigration*. To premigrate a file, HSM copies the file to ADSM storage and leaves the original file intact on the local file system. An identical copy of the file resides both on the local file system and in ADSM storage.

The next time free space is needed on the file system, HSM can quickly change premigrated files to migrated files without having to spend time copying the files to ADSM storage. HSM verifies that the files have not changed since they were premigrated and replaces the copies of the files on the local file system with stub files.

HSM premigrates files each time it completes automatic migration if the file system contains additional files that are eligible for automatic migration, and the premigration percentage set for the file system has not been reached or exceeded.

The *premigration percentage* indicates the percentage of space on a file system that you want for premigrated files that are the next eligible candidates for migration. The default for the premigration percentage is the difference between the percentage set for the high threshold and the percentage set for the low threshold for the file system. However, a root user can adjust the premigration percentage at any time.

1.2.3 Recalling Migrated Files

To bring back a migrated file to your workstation or file server, HSM recalls the file from ADSM storage. Whenever HSM recalls a file to a local file system, it changes the atime for the file to the current time (unless the timestamp control mode is set to preserve the last access time recorded for the file); see 1.2.9, “Modifying the HSM-Related Behavior of Commands” on page 11.

HSM provides both transparent and selective recall.

1.2.3.1 Transparent Recall

To access a migrated file, you do not have to be aware that the file is migrated. You access it in the same way as you access a file that resides on a local file system. *Transparent recall* automatically brings back a migrated file to your local file system when the file is accessed.

When you access a migrated file, HSM automatically recalls it to its *originating file system* (the file system from which the file was migrated). A root user sets an option (the KERNELMESSAGES option) that determines whether HSM notifies you when a file is being recalled. However, whether a file resides on a local file system or has been migrated to ADSM storage is transparent to any process that accesses the file.

When HSM recalls a migrated file, it leaves a copy of the file in ADSM storage. Because an identical copy of the file resides both on the local file system and in ADSM storage, the file is in a premigrated state. The file remains premigrated until it once again becomes eligible for migration and is changed to a migrated state, or you modify the file. If you modify the file, it becomes a resident file.

1.2.3.2 Selective Recall

Although a migrated file appears to reside on your local file system, you can find out whether a file has been migrated by using the HSM graphical user interface (GUI) or HSM commands to display information about your files.

If you want to bring back specific migrated files to your local file system, you can use *selective recall.* For example, if you plan to use a group of files that you know have been migrated, you can request that HSM recall them to your local file system.

When you selectively recall a group of files, HSM recalls them in the most efficient, time-saving order according to where they are stored in ADSM storage. For example, if some of the files are stored on a disk storage device and some are stored on a tape storage device, HSM recalls all of the files on the disk storage device first and then recalls all of the files stored on the tape storage device.

If you are a root user, you can selectively recall any file migrated from your workstation. If you are a user, you can selectively recall any migrated file you have permission to access. When you selectively recall a file, HSM stores it on its originating file system.

1.2.4 File States

As files are migrated, premigrated, and recalled, different terms are used to describe the state of the file.

Resident A resident file resides on the local file system. For example, a newly created file is a resident file.

Migrated A migrated file is a file that has been copied from the local file system to ADSM storage and replaced with a stub file.

Premigrated A premigrated file is a file that has been copied from the local file system to ADSM storage but has *not* been replaced with a stub file. An identical copy of the file resides both on the local file system and in ADSM storage. A file can be in the premigrated state after premigration. If a file is recalled but not modified, it will also be in the premigrated state.

Figure 1 shows the file states.

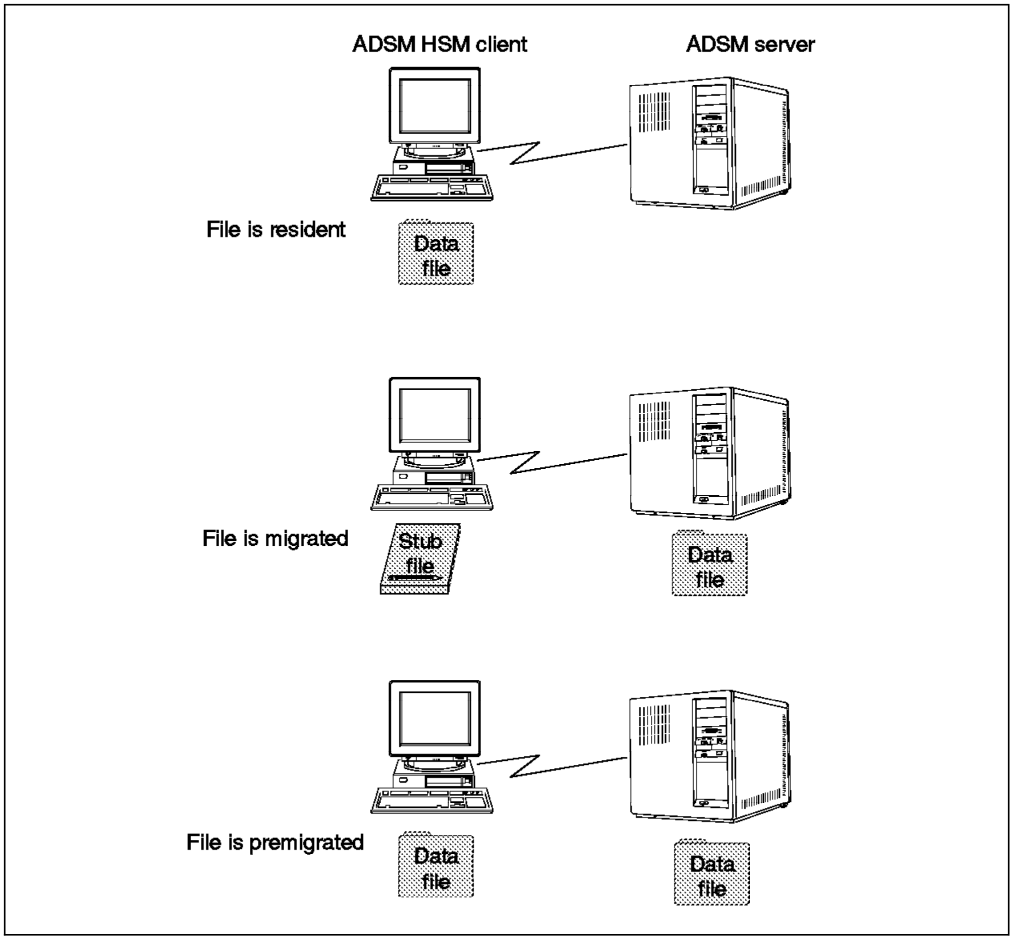


Figure 1. Resident, Migrated, and Premigrated Files

1.2.5 Using Advanced Transparent Recall

For special situations, you can choose to take advantage of HSM′s advanced transparent recall features. By changing the *recall mode* for a migrated file or a specific execution of a command, you can change how HSM recalls a migrated file.

In addition to the *normal* recall mode (which causes HSM to recall a migrated file to disk on the local file system), HSM provides these recall modes:

Migrate-on-close
Recalls a migrated file to its originating file system only temporarily. The recalled file remains on your local file system only for as long as it is open. When you close the file, if it has not been modified, HSM replaces it with a stub file on the local file system, and it once again becomes a migrated file. HSM does not have to send a copy of the file to ADSM storage because the file has not been modified, and the copy that currently resides in ADSM storage is still valid.

Read-without-recall Reads a migrated file from ADSM storage without storing it on your local file system. HSM reads information from the migrated file sequentially and caches information read from the file in a memory buffer on your workstation.

HSM can use the migrate-on-close and read-without-recall modes only under certain conditions. In the sections that follow we provide more information about those conditions.

In addition, you should not use the migrate-on-close or read-without-recall modes for a file migrated from a file system that has been exported by an Network File System (NFS) server. Because NFS opens and closes a file many times when it is accessed by an NFS client, performance can be severely hampered.

Also note that selective recall overrides migrate-on-close and read-without-recall. You can selectively recall a migrated file to your local file system regardless of its recall mode.

1.2.5.1 Migrate-on-Close Mode

HSM can use the migrate-on-close mode to recall a file temporarily if:

- The recall mode set for a migrated file is migrate-on-close, and the file is accessed only by processes that do *not* modify the file.
- The recall mode set for a migrated file is normal, but *all* processes that access the file at one time use the migrate-on-close recall mode and do *not* modify the file.

If the recall mode set for a file is migrate-on-close, and the file is modified by any process, the file remains on your local file system. The file also remains on your local file system in the following situation: The recall mode set for the file is normal, and the file is accessed by processes that use the migrate-on-close mode, but at least one process accesses the file at the same time through normal recall mode or accesses and modifies it.

1.2.5.2 Read-without-Recall Mode

HSM can use the read-without-recall mode to read a migrated file without storing it on your local file system only when:

- The recall mode set for a file is read-without-recall, and *all* processes that access the file at one time do *not* modify the file and do *not* use memory mapping.
- The recall mode set for a file is read-without-recall, and, if the file is a binary executable file, the process does not execute it.

If a process that accesses the file writes to the file, modifies the file, or uses memory mapping, HSM recalls the file to its originating file system. In addition, if the file is a binary executable file, and it is executed, HSM recalls it to its originating file system. (If you want a file to be returned to a migrated state after it is executed, you can set the recall mode for a process that executes it to migrate-on-close.)

Attention

When the recall mode set for a file is read-without-recall, multiple processes can access the file at one time, and a process can seek backward in the file. However, the read-without-recall mode is intended for single-access, sequential reads of nonexecutable files. Accessing the file with multiple processes at one time or seeking backward in the file can significantly affect the performance of each process that is accessing the file.

1.2.6 Reconciling Your File Systems

To keep your local file systems synchronized with the ADSM server you use for space management services, HSM uses *reconciliation*. Reconciliation also keeps the migration candidates list for each of your file systems up to date.

HSM automatically reconciles your file systems at intervals set by a root user on your workstation. For example, the default interval is every 24 hours. A root user can also run reconciliation at any time.

1.2.6.1 Synchronizing Your Client and Server

When you access (causing a recall) and modify a migrated or premigrated file or erase a migrated or premigrated file from a local file system, an outdated copy of the file still exists in ADSM storage.

During reconciliation, ADSM marks any outdated copies of migrated or premigrated files for expiration. The copies expire and are removed from the server after the expiration period specified by a root user has elapsed.

When synchronizing a file system, HSM also updates other space-management information, for example, counters for the number of files migrated.

1.2.6.2 Building a New Migration Candidates List

A *migration candidates list* is a prioritized list of all files in a file system that are eligible for automatic migration at the time the list is built. HSM uses that list to determine which files to migrate and the order in which to migrate them during threshold and demand migration.

HSM builds a new migration candidates list each time reconciliation is run. If the migration candidates list for a file system does not exist or is empty when automatic migration is needed, HSM runs reconciliation to attempt to build a list at that time. In addition, a root user can build a new migration candidates list at any time.

To be eligible for automatic migration, a file must:

- Reside in a file system to which space management has been added
- Meet all management class requirements for eligibility
- Be at least the minimum size required for migration

In addition, a file must not be excluded from space management services.

HSM prioritizes files for migration according to the number of days since they were last accessed, their size, and the age and size factors set for the file system by a root user on your workstation. The *age factor* determines how much weight is given to the number of days since a file was last accessed, and the *size factor* determines how much weight is given to a file′s size.

1.2.7 Setting Space Management Options

A root user sets space management options for your workstation that determine:

- How often HSM checks space usage on your file systems
- The ADSM server to which your files are migrated and premigrated
- How often HSM automatically reconciles your file systems
- How many days must elapse since a migrated or premigrated file was deleted or modified on the local file system before the copy in ADSM storage expires and is removed

A root user sets those options, along with other space management and ADSM options, in your *client system options file*.

In addition, a root user can set options to:

- Exclude specific files from space management services
- Assign specific management classes to files

1.2.7.1 Excluding Files from Space Management

Some files, such as system files and files created by and used for HSM processing, should not be migrated from a local file system. HSM automatically excludes those files from space management.

You may also have some additional files that you want to keep on your local file systems at all times. A root user can set options to exclude specific files or groups of files from all space management services in your *include-exclude options file*.

1.2.7.2 Assigning Management Classes to Files

The *management class* assigned to a file determines:

- Whether HSM can migrate the file automatically and by user request, by user request only, or neither
- The number of days that must elapse since the file was last accessed before it is eligible for automatic migration
- Whether a current backup version of the file (created by using the ADSM backup-archive client) must exist on your migration server before the file is eligible for migration
- Where the file is stored when it is first migrated

ADSM provides a *default management class* that you can use for some or all of your files. A root user can also assign different management classes to specific files by setting options in your include-exclude options file.

Your ADSM administrator defines the management classes from which a root user can choose. For example, your administrator can define a management class that allows a file to be migrated to ADSM storage automatically if it has not been accessed for at least 30 days, and a current backup version of the file exists on your migration server. Or, your administrator can define a management class that allows you to selectively migrate a file regardless of whether a current backup version of the file exists on your migration server.

1.2.8 Choosing Space Management Settings

A root user must also add space management to each file system for which you want space management services. When adding space management to a file system, the root user chooses *space management settings* that determine:

- The high and low thresholds for the file system

  The high and low thresholds determine when HSM automatically starts and stops threshold migration.

- The size of the stub files left on the file system when files are migrated

  The *stub file size* determines how many leading bytes of data from a migrated file HSM can store in a stub file. If only that data is accessed and not modified, HSM does not have to recall the file from ADSM storage.

  The stub file size also determines the minimum size a file must be before it is eligible for migration. To be eligible for migration, a file′s size must be greater than both the stub file size plus 1 byte and the block size defined for the file system.

- The order in which eligible files are automatically migrated from the file system

  A root user can choose settings that determine whether HSM prioritizes files for automatic migration according to the number of days since they were last accessed (age factor), their size (size factor), or a combination of both.

- The total number of megabytes of data that can be migrated and premigrated from the file system to ADSM storage

  This number is called a *quota*. The default is the same number of megabytes allocated for the file system itself. For example, if 200 MB are allocated to a file system, ADSM can migrate and premigrate files from the file system until the total number of megabytes migrated and premigrated equals 200.

  A root user can increase or decrease the quota to accommodate the growth of a file system or to adhere to any restrictions placed on space usage by your ADSM administrator.

1.2.9 Modifying the HSM-Related Behavior of Commands

Most commands, such as those provided by your operating system, can access migrated files, cause the atime for a file to be updated, and cause a migrated file to be recalled. In addition, if a command causes a local file system to run out of space during processing, HSM intercepts the out-of-space condition and begins automatic migration.

HSM enables you to modify those behaviors for a specific execution of a command or series of commands by changing the *execution modes* that are in effect. For example, if you want to prevent a command, such as the **grep** command, from accessing migrated files, you can change the *data access control mode* before issuing that command.

To prevent a command, such as a utility that creates backup versions of files, from updating access times, a root user can change the *timestamp control mode*.

If you want to prevent HSM from intercepting an out-of-space condition caused by a command, you can change the *out-of-space protection mode* before issuing the command. If, as previously discussed, you want HSM to change a recalled file back to a migrated file if it has not been modified, you can change the *recall mode* for a command to migrate-on-close.

Note: When you back up or archive a file by using the ADSM backup-archive client, the access time for a file remains unchanged. A root user does not have to change the timestamp control mode.

1.2.10 Scheduling Space Management Services

ADSM provides *central scheduling* that allows your ADSM administrator to schedule ADSM services. For example, if you are using the ADSM backup-archive client on your workstation, your administrator can schedule regular incremental backups of your files.

Although HSM automatically performs most space management services according to options and settings selected by a root user on your workstation, your administrator can choose to schedule space management services, such as threshold migration or reconciliation, to occur at specific times.

Before ADSM can perform scheduled services, a root user on your workstation must set scheduling options in your client system options file (if the defaults for those options are not appropriate) and start a client scheduler on your workstation.

In addition, a root user can set up a **cron** job to run space management services at specific times. For example, a root user can set the RECONCILEINTERVAL option in the client system options file to 0 so that HSM does not automatically reconcile file systems at specific intervals. Then, the root user can use a **cron** job to run reconciliation at a specific time each day.

1.2.11 Backing Up and Restoring Migrated Files

You can back up and restore migrated files by using the ADSM backup-archive client in the same way you use it to back up and restore files that reside on your local file system.

In addition, if stub files are accidentally deleted from a local file system or you lose an entire local file system, you can re-create the stub files for migrated files.

1.2.12 Archiving and Retrieving Copies of Migrated Files

You can archive and retrieve copies of migrated files by using the ADSM backup-archive client in the same way you use it to archive and retrieve copies of files that reside on a local file system.

Chapter 2. HSM Setup Philosophies

HSM is a new technology in today′s client/server environment. When designing your environment, keep in mind that migrated data is *active* data that must be treated differently from backup data. ADSM server availability becomes more critical now that it is storing active data. It is also important to ensure that the ADSM server database and storage pools are backed up on a regular basis with a copy stored offsite for disaster recovery purposes. You may also want to provide a larger disk pool for migrated data than for backup data so that recently migrated files can be quickly recalled without having to wait for a tape mount.

One of the key factors in making HSM successful in your environment is to make HSM *invisible to your users.* To do this, you should structure your setup so that the HSM activities (migrate, transparent recall) have a minimum impact on your users. Transparent recall should be as quick as possible, and threshold as well as out-of-space demand migration should be avoided during normal working hours. IBM′s experience in storage management has shown that, in a typical interactive user community, the recommendations made in this chapter provide a well-managed (and well-liked) system.

2.1 Management Class Settings

The first step in minimizing the impact of HSM on your users is to ensure that the files that are migrated are not likely to be recalled.

We recommend setting the management class controls according to the application or typical user access pattern for your system. For example, migrating files after *15 days* of nonusage will ensure that files used by applications and people within two weeks are kept on the local file system.

2.2 Using Quotas

One concern that you may have is the amount of storage required for the migrated data. ADSM provides the ability to define a quota to set limits on how much data an HSM client can migrate to an ADSM server. The default value is the number of megabytes used by the local file system. For example, a 500 MB file system can migrate 500 MB of data.

Whether or not you use quotas depends on your environment. If you are using a chargeback system for ADSM services, you may not need quotas. If you are in a research or university environment, however, or require strict control over the use of ADSM server storage resources, you may want to set quotas.

There are a few points to keep in mind when deciding to use quotas. If you use quotas, remember that the default value is dynamic; that is, if you increase a 500 MB file system to 800 MB, HSM automatically adjusts that file system′s quota to 800 MB. In addition, *when a file system′s quota has been reached, migration from that file system is disabled*. You could have a situation where a file that is larger than the file system can hold has to be recalled. HSM tries to migrate data in such situations, and, if the quota has been exceeded, data cannot be migrated to satisfy the recall request.

If you decide to use quotas, use the HSM client periodically to determine how much data has been migrated and how close the client is to reaching its quota. Use the **Space Manager** button from the HSM GUI, or the **dsmdf** command to see the amount of migrated data and the **dsmmigfs q** command to compare that amount with the quota.

2.3 Nightly Migration and Reconciliation

Threshold migration is an event-driven process that starts when the high threshold is exceeded. Because it is event driven, migration may occur during a busy time of day.

To minimize the impact of migration on your users, you should migrate most of the data during less busy times for the network and HSM clients. To cause most migrations to occur during off-peak times, you can “manually” start threshold migration with a client command schedule that executes the **dsmautomig** command.

As your space-managed file system matures, more data is in a migrated state. As more files are migrated, reconciliation can increase the load on the network. Also, how you use the **dsmmigundelete** command depends on whether or not reconcile has run. (For details on **dsmmigundelete** refer to Chapter 7, “Recovery with ADSM and HSM” on page 87.) Therefore, we recommend scheduling reconcile to occur during off-peak hours.

You must also set the RECONCILEINTERVAL option to 0 in the client system options file so that automatic reconcile runs only during the scheduled time.

2.4 Priority of Size and Age Factors

Optimizing the perceived performance of migration and recall also helps minimize the impact of HSM activities on your users. The *ADSM Version 2 Performance Evaluation Report* provides some performance information on migrate and recall. On the basis of the numbers in that report, you may think that it is better to migrate larger files because you will achieve higher throughput. Remember, however, that threshold migration occurs in the background, and end users are not aware of the elapsed time. The speed with which a transparent recall is satisfied is much more important. When it comes to performance of a recall, visible elapsed time is more important than throughput.

The *ADSM Version 2 Performance Evaluation Report* presents a test case involving a single LAN-connected HSM client migrating to an ADSM server. A 5 KB file achieved a throughput rate of 5 KB/sec. A 100 KB file achieved a 100 KB/sec throughput rate, and a 10 MB file achieved a 1210 KB/sec throughput rate. The 5 KB and 100 KB files took 1 sec to be recalled, a time period barely noticeable by a user. The 10 MB file, while achieving higher throughput, took 8 sec before the user could access the entire file. That time period would be noticeable to a person using an application.

Therefore, in choosing settings that determine the order in which HSM automatically migrates eligible files, we recommend the following: When performing nightly or off-peak migration, set the age factor and size factor to equal weight (1:1). This will give priority to older files, which are least likely to be recalled. Thus the performance of the most frequently accessed files is optimized because those files remain resident. During the day or at peak times, you can set the age factor to 0 and the size factor to 1 so that, in the rare instance where the high threshold is exceeded during the day, space is cleared off the local file system more quickly. For further discussion on age factor and size factor, refer to 3.3.2.2, “Age and Size Factors” on page 34.

Before performing the nightly migration, you can automatically reset the size and age priorities with a client command schedule that issues **dsmmigfs update** to set the size factor to 1 and the age factor to 0 and then reset the age factor to 1 at the beginning of the day. An example of a macro defining these schedules is provided in Appendix A, “Macros Used to Set Up Automation” on page 105.

After changing the age factor or size factor you must also run **dsmreconcile -candidatelist** to build a new migration candidates list.

2.5 High and Low Thresholds

Each file system that is HSM managed has a high and low threshold. Generally, it is best to start with the default values of 90% for the high threshold and 80% for the low threshold. We are not recommending that you micro-manage your HSM environment by examining every file system to an extreme degree. However, here are some things to consider about threshold settings.

Thresholds are percentages and not absolute values. For example, a 500 MB file system has a 90% high threshold of 450 MB and an 80% low threshold of 400 MB. A 1500 MB file system has a 90% high threshold of 1350 MB and an 80% low threshold of 1200 MB.

The high threshold triggers automatic migration. If you are using nightly migrations, the high threshold becomes a safety net for avoiding out-of-space conditions. Even though HSM intercepts and reacts to an out-of-space condition, the process that causes the file system to fill up has to wait until enough space has been cleared to satisfy the request. When using nightly migrations, you may be able to set the high threshold a little higher than 90%, especially for larger file systems. For example, a 500 MB file system has 50 MB free when it is 90% full, but a 1500 MB file system has 150 MB free when it is 90% full. If you set the high threshold for the 1500 MB file system to 95%, that still leaves a minimum of 75 MB of free space.

The low threshold is the point at which HSM stops migrating files. Assuming you are performing nightly threshold migration, you should make the low threshold low enough to allow enough space for one day′s worth of data. As with the high threshold, larger file systems can handle a higher low threshold than smaller file systems.

The premigration percentage defines the percentage below the low threshold where HSM should premigrate files. For example, if a file system has a 90% high threshold, an 80% low threshold, and a 10% premigration percentage, HSM will premigrate down to 70%. In the event of an out-of-space condition, ADSM will immediately replace premigrated files with stub files, freeing up storage space without having to wait for the time it takes to copy the data to the ADSM server. The default premigration percentage is the difference between the high and low threshold. You may want to consider increasing the premigration percentage for smaller file systems.

2.6 Monitoring HSM Activity

HSM enables you to defer the cost of adding physical storage to your local file systems by migrating less active data and making room for new files to be created. When HSM is initially added to a file system, a large number of files are likely to be migrated because nothing has been migrated before. As time progresses, the pattern of data growth and data migration should settle down so that threshold migration clears off enough space at night to accommodate new data created during the day. There may be cases where the thresholds you have defined have to be increased or decreased to allow for data growth on the file system.

At some point, your local file system may not be able to accept new files without having to migrate recently referenced files. When recently migrated files are constantly being recalled, thrashing occurs. If you cannot provide the desired level of free space without thrashing, you may have to consider adding additional physical storage to your local file system.

If you follow the philosophy described in this chapter, no automatic migration (threshold or demand) and very few recalls should occur during the day. The best indication of how well things are running is the telephone. If users are not complaining, you must be doing your job right. However, to ensure the general health of the thresholds you have set, and to get an idea of when a system is running out of space, you can monitor the recall and automatic migration activity.

At the time this book was written, logging information on when migrate and recall occur was not available. However, by using the ADSM accounting records, we could make some educated guesses and get a general feel for the HSM activity.

The ADSM accounting records have fields that indicate the number of objects and amount of data backed up, restored, archived, or retrieved. (For a description of the accounting record, refer to the *Administrator's Guide* for the appropriate ADSM server platform.) When ADSM creates a record that is HSM-related, all of the backup-archive fields are 0. These records could be for migrate, recall, reconcile, or another HSM command (such as **dsmdf**). We can use the average file size and standard deviation of file sizes to determine which of these HSM transactions are migrates and recalls. (See Appendix B, "Determining Average and Distribution of File Sizes" on page 107 for information on calculating the average file size.) This method is based on the following assumptions:

- All accounting records for backup, archive, restore, and retrieve have been eliminated.
- HSM is performing automatic migration on a nightly basis.
- During the day, the age factor is set to 0 and the size factor is set to 1 so that files are prioritized for migration only by size.
- Most recalls are for a single file, so the amount of data transferred is approximately the size of the file being recalled.
- Most automatic migrations migrate many files, so the amount of data transferred will be much larger than the average file size for that system.

If the number of kilobytes transferred during the session is within one standard deviation of the average file size, the session is probably a recall. If the number of kilobytes transferred during the session is more than one standard deviation plus the average file size, the session is probably automatic (threshold or demand) migration.

Note: If you are using compression, divide your file sizes in half before calculating the average file size and standard deviation to compensate for the compression.

If your goal is to minimize the impact of HSM on your users (as described in 2.3, “Nightly Migration and Reconciliation” on page 14), use the guidelines below to determine whether further investigation of HSM processing is required.

Resist the temptation to reduce the number of days before a file can be migrated. If you make this value too low, you run the risk of affecting the service provided to your users. If you annoy your users by migrating files too soon, they may end up recalling all of their files on a daily basis.

2.6.1 More Than a Few Recalls from Tape per Day

If an HSM client is experiencing more than a few recalls per day from a migrated file that is in a tape storage pool, the HSM client deserves a closer look. A recall from disk is faster than a recall from tape, so we are not concerned about recalls from disk.

The ADSM administrator can check the activity log for tape mount requests issued for space management storage pools that use tape. If a user is complaining, or if you see more than a few recalls during the day, use the accounting records to determine which client is causing the recalls.

The exact number of recalls that are acceptable will vary according to how large the file system is and whether or not all recalls are caused by one or many users. We recommend using five recalls per day as a starting point. If you have extremely large file systems (for example, 2 TB), you can allow more recalls. If you are seeing more than five recalls during the day, you can attribute the excessive number to one of the following reasons:

1. The file system is too small.

   In other words, data is growing on this system so fast that you are migrating data that is still in regular use. At this point, you have to weigh the cost of buying additional storage against decreased recall performance.

2. The number of days before a file can migrate is set too low.

   Based on the use pattern of the files on this system, the files are being used on a periodic basis that is higher than the number of days set in the management class. Try setting the number of days in the management class to a higher value.

3. A user does not like his or her files being migrated and is thus causing a recall by selectively recalling files.

   If a user is selectively recalling his or her migrated files, there is not much you as an ADSM administrator can do. If the user is recalling files for valid reasons, you need not take any action.

2.6.2 Automatic Migration during the Day

Since you are performing nightly automatic migration to clear off space, you should not expect to see very much migration activity. A migrate during daytime hours could be due to one of the following reasons:

1. The user is using selective migrate. This is not very likely, unless the user is migrating a very large file or a group of files.

2. The file system is too small.

   HSM cannot keep up with the growth of data on the system. In this case, even though HSM is migrating data on a nightly basis, the file system is filling up during the day and causing automatic migration.

   One symptom of a file system that is too small is a small migration candidates list. The following are methods to determine the size of the migration candidates list:

   - Use the output from the **dsmreconcile** command to determine the number of new candidates

   - Use the HSM GUI to view the migration candidates list.

   If the number of files eligible for migration is small, you may have no choice but to increase the amount of physical storage available on this system.

   Another symptom of a file system that is too small is when automatic migration cannot reach the low threshold. To determine whether automatic migration is not reaching the low threshold use one of the following methods shortly after scheduled automatic migration occurs:

   - Use the HSM GUI to view the amount of free space available and the low threshold of the file system.

   - Use the **dsmmigfs query** command to determine the low thresholds and the **df** command to see the percentage of space used.

   If the amount of free space is less than the low threshold, it is time either to add more space to the file system or upgrade your system with more physical storage. You could decrease the number of days before a file is eligible for migration in the management class, but be careful not to make the number of days too low. If you set the number of days to a value that is too low, the files you migrate each night will be recalled the next day.

3. The low threshold for this system is too high.

   Checking to see whether the low threshold is set too high is a little more labor intensive. You must use either the pie charts in the HSM GUI or the **dsmdf** command to check the number of premigrated files. Check the number of premigrated files on the system in the morning (after the nightly threshold migration completes) and again later in the day. If the system starts the day with a high number of premigrated files but is down to very few later in the day, perhaps your low threshold is too high.

Chapter 3. Implementing HSM

In this chapter we cover the main tasks required to implement HSM in your environment. We describe which tasks the ADSM administrator and which tasks the root user has to perform. We explain how to get HSM up and running and adapt it to your special requirements. We also provide practical tips and recommendations for the best configuration.

HSM provides a GUI for most setup and maintenance tasks. However, if you prefer to type commands or have a task that can be performed only through a command, you can use the HSM command line interface. In this chapter we use the GUI, except when it does not provide the required function. For a list of command-line-only and GUI-only functions see 5.1.1, “Command Line Only Functions” on page 63 and 5.1.2, “GUI Only Functions” on page 63.

This chapter covers the following tasks:

- Planning considerations
- Setting up the ADSM server for HSM
- Setting up the HSM client
- Setting up advanced features

3.1 Planning Considerations

Before you start to set up HSM you will want to think about the following fundamental configuration decisions:

- Using the same ADSM server or different ADSM servers for backup, archive, and migration
- Using the same storage pool or different storage pools for backup, archive, and migration
- Planning for storage pool size and structure
- Choosing file systems for space management
- Using client compression for migrated data

Below we discuss the advantages and disadvantages of these options and provide some tips for the best setup in your own environment.

3.1.1 Same or Different ADSM Servers for Backup, Archive, and Migration

The first fundamental decision you have to make is whether you want to migrate and back up your data to the same ADSM server or to different ADSM servers. We strongly recommend that you use the same ADSM server for backup and migration for the reasons discussed in this section.

The advantage of using different ADSM servers is that you have a clear separation of tasks on different machines. You also have more security because there is no single point of failure, and, in a high performance environment, you will have the full power of one server for each task.

The use of different servers for backup, archive, and migration has many disadvantages. First of all, the software cost of running two ADSM servers on different machines is twice as much. You also have to administer two servers: you have to register all clients twice, set up all policies twice, and keep both servers synchronized. In addition, you must have the storage hardware (such as tape libraries) on each server.

A more important disadvantage of using different servers is that you lose the integration between HSM and backup. If you back up and migrate your files to the same ADSM server, HSM can verify that a current backup version of a file exists before it migrates the file. If you back up your files to one server and migrate files to another, a root user must choose a management class for your files that does not include the requirement for a current backup version. Otherwise, the files cannot be migrated. HSM checks for backup versions only on the server to which you migrate your files.

If a file is assigned a management class that does not include the requirement for an existing backup version, you can still back up the file before or after it is migrated.

If you back up a file to the same ADSM server to which it was migrated, ADSM copies the file from the migration destination to the backup destination. It does not recall the file to your local file system (see Figure 2). As you can see, this minimizes the load on the network because the file is copied within the server.

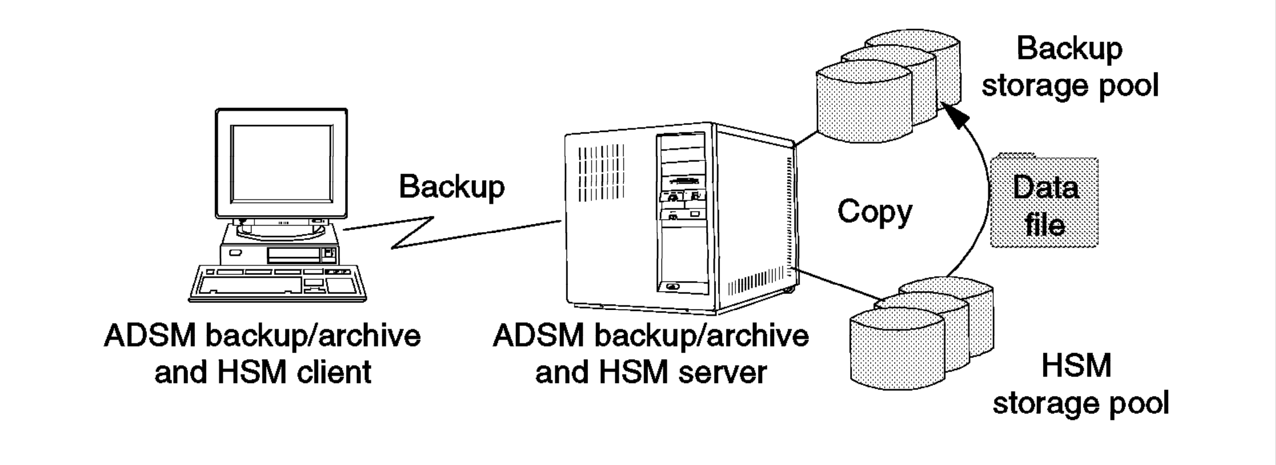


Figure 2. Backup and Migration to the Same ADSM Server

If you back up a file to an ADSM server that is different from the one to which the file was migrated, ADSM backup accesses the file by using the migrate-on-close recall mode if the recall mode set for the file is set to normal or migrate-on-close. The file resides on your local file system only until ADSM finishes sending a backup version of the file to the backup destination. If the recall mode set for the file is read-without-recall, ADSM backup uses that mode (see Figure 3 on page 21).

Note: If you back up a premigrated file to either the same server to which it was migrated or a different server, ADSM sends a copy of the file from your local file system to ADSM storage.

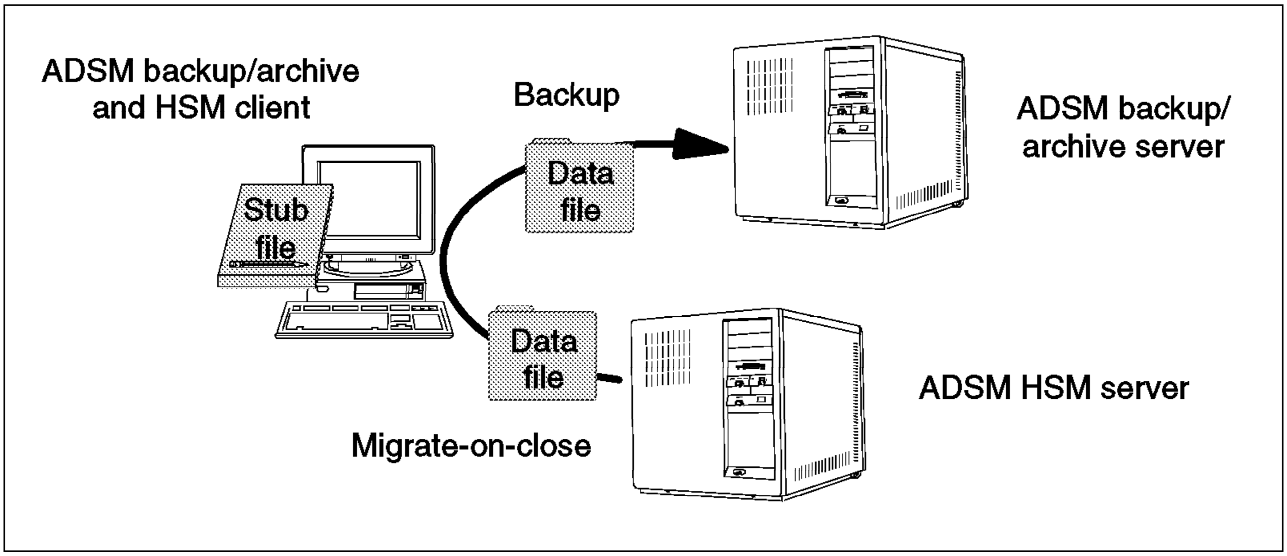


Figure 3. Backup and Migration to Different ADSM Servers

The manner in which stub files are restored differs according to whether you are backing up to the same server to which you are migrating or a different server. If you back up and migrate to the same server, you have the option in the ADSM backup-archive restore command to tell ADSM to re-create a stub file if the file was in a migrated state the last time a backup was performed.

If you back up and migrate to different servers and have to restore a file system, you must use the **dsmmigundelete** command to re-create the stub files and then use **dsmc restore** with the **noreplace** option to restore the resident files. The **dsmmigundelete** command only restores the stub files for an entire file system. You cannot use the command to restore a single file. The steps for recovering HSM-managed file systems are covered in Chapter 7, "Recovery with ADSM and HSM" on page 87.

3.1.2 Same or Different Storage Pools for Backup, Archive, and Migration

If you are using the same ADSM server for backup, archive, and migrate, you can either put all of the migration, backup, and archive data together in one storage pool or separate them in different storage pools.

Although combining migration and backup data in the same storage pool is easier to set up and enables maximum reuse of the storage pool space, we recommend that you create separate storage pools for backup and migration, for several reasons. First you have a clear separation of the data on the ADSM server. Thus it is much easier to handle maintenance tasks. In addition, locating the backup and migration data on different physical volumes ensures that if a media failure occurs, only one copy of the data will be lost. Separating the backup and migration data provides better performance for concurrent access to the migrated data. Finally, separate storage pools provide more flexibility in deciding which storage pools to back up. Backing up storage pools that contain migrated data is more important than backing up storage pools that contain backup data.

3.1.3 Planning for Storage Pool Size and Structure

Another step in planning for HSM is to estimate the required storage pool size and structure for the migrated data. Keep in mind that the performance requirements for migrated data may be stricter than those for backup copies.

We recommend that you migrate to a disk storage pool first. This will provide better performance for recalls that are performed on files that were recently migrated. Performance for migration, especially when more than one migration is running concurrently, is also better when migrating to a disk storage pool.

There are two important considerations when it comes to tape storage pools containing migrated data. First, make sure that you are using separate tape drives for backup and migrated data; otherwise, a transparent recall could potentially wait a long time for the drive to be available. Second, if your storage pools are structured so that the data merges as it moves from storage pool to storage pool, be careful not to combine migration and backup data at a lower level.

The size of the pool depends on the distribution of size and age of the files in the file system that you want to manage with HSM. For example, if you have a lot of small and frequently changed files in your file system, fewer files will be eligible for migration, thus reducing the ADSM storage required to contain them. If you have large files that are not frequently accessed, you will need much more storage space, because more data will be migrated to ADSM server storage. The distribution of file sizes is described in Appendix B, “Determining Average and Distribution of File Sizes” on page 107.

Quotas limit the amount of data a client can migrate to an ADSM server.

Experience from ADSM backup-archive customers has shown that the very best way to determine your storage pool requirements is to begin with a few clients and then measure the actual space that data occupies. Whether or not you are using compression also affects how much storage pool space is required.

3.1.4 Choosing File Systems for Space Management

In general, we recommend that you add space management to file systems where data usage is low, data is not essential for system operation, and access to data is not time critical. The classical /home file system is a file system that best meets these criteria.

HSM does not allow you to add space management to the root (/) and the /tmp file systems. Adding space management to the root file system does not make sense because it contains files that are frequently accessed, essential for the whole system operation, and used for system startup. Also, the files usually are not very large. Adding space management to the /tmp file system makes no sense because it contains files that are temporary.

Other file systems are not well suited for migration. We recommend that you not add space management to the /usr and /var file systems. The /usr file system contains parts of the operating system and most applications. The performance of your whole system will be affected if frequently used applications have to be recalled before you can use them. The /var file system contains files that are frequently changed.

3.1.5 Using Client Compression for Migrated Data

You have the option of compressing your migration data on the client side before it is sent to the ADSM server. The ADSM administrator can specify whether or not to use compression or can allow the compression option to be specified in the client user options file (dsm.opt). Your decision to turn compression on or off will apply to all data sent to the server, whether it is backup, archive, or migrated data.

Compression reduces the amount of space needed in storage pools and decreases the load on the network. In an environment where the network throughput is one of the most critical performance factors, compression on the client gives you a performance advantage.

In some cases, however, compression increases the time it takes to send data to the server, especially when the processor performance of your client machine is poor. Also, if your data does not compress well, migration time will increase. Every time the client notices that a compressed file is larger than the original file, it stops compressing and sends the file again, this time uncompressed, from the client. This is an additional transaction with all of the associated transaction overhead. Finally, many storage devices such as tape provide hardware compression, which is much faster than software compression.

We recommend that you not use client compression for migrated data in an environment where you have sufficient bandwidth, such as Fiber Distributed Data Interface (FDDI). If the network is the performance-critical part of your configuration and does not have high bandwidth, consider using compression.

Another determining factor is whether your data compresses well. To find out whether compression on the client side will give you performance advantages in your environment, migrate some production data with and without compression and compare the operation time. To determine whether the data does not compress well, run the operation with FORMAT=DETAILED and then check the client log. You will receive a message indicating whether compression was canceled.

3.2 Setting Up the ADSM Server for HSM

In this section we describe how to set up the ADSM server for HSM. We use a single server and separate storage pools for backup and migration.

We assume that the ADSM server and HSM client are installed. For information on installing the ADSM server, refer to *Installing the Server and Administrative Client* for the appropriate server platform. For information on installing the HSM client, refer to *ADSM: Installing the Clients*. The basis for all of our work is the default configuration provided by the installation process.

After installation, by default the ADSM server has three storage pools (ARCHIVEPOOL, BACKUPPOOL and SPACEMGPOOL) and a STANDARD policy set with a management class and copy groups. Starting with this setup, the ADSM administrator must perform the following tasks:

- Set up the space management storage pool
- Enable migration in a management class
- Register the license for HSM

- Register the HSM client

3.2.1 Set Up the Space Management Storage Pool

By default the SPACEMGPOOL storage pool was created at installation time, but it is still empty; that is, volumes have not been defined to it.

The first thing to do is to define some disk volumes to the SPACEMGPOOL storage pool. Depending on the ADSM server platform you are using, you may have to format some disk space or simply set aside a logical volume for ADSM to use. Then you define the volume to your storage pool using either the administrative GUI or the **def volume** command.

In your own environment you will probably have to define more than one disk volume in your storage pool. The size and structure of your storage pool depend on the amount of data to be migrated, the requirements for performance, and last but not least, your available storage hardware. For the amount of space required, use the same rules you used for your backup storage pools.

The main difference between planning for backup and planning for migration is that migrated data is active data, and the access should be transparent for the end user. Thus you should focus on the recall performance of the storage pools you will use for migration. For example, be sure that you do not migrate time-critical data on sequential access storage devices such as tape libraries.

Use the storage pool backup feature available with the ADSM V2 server to protect data against loss by a server or media failure. This is especially true for migrated data, which users consider to be active data. If you keep the storage pool backups on site, a transparent recall request can still be satisfied before the administrator has to restore the damaged volume.

3.2.2 Enable Migration in a Management Class

With HSM you can enable migration in any management class by setting additional options when you define a management class.

In our example, we modify the default management class provided in the STANDARD policy domain, using the administrative GUI (see Figure 4 on page 25).

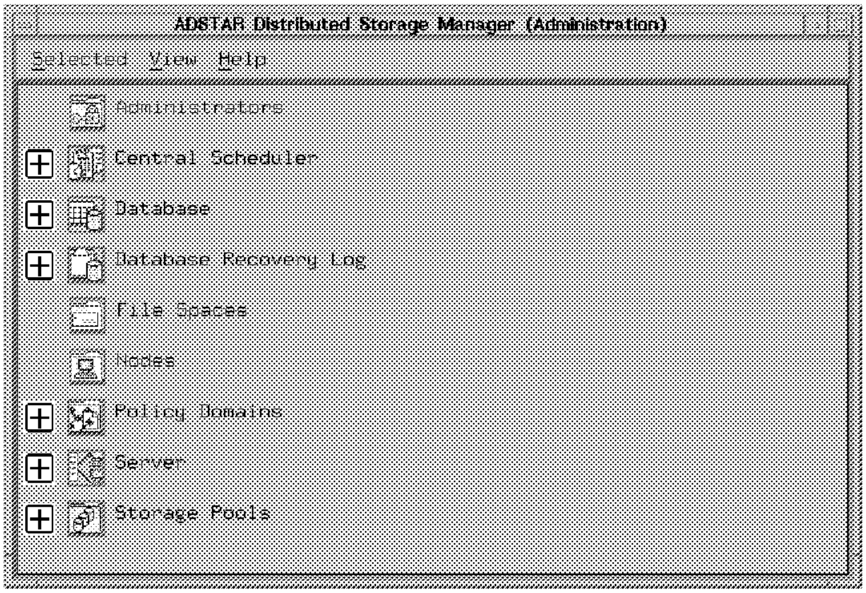
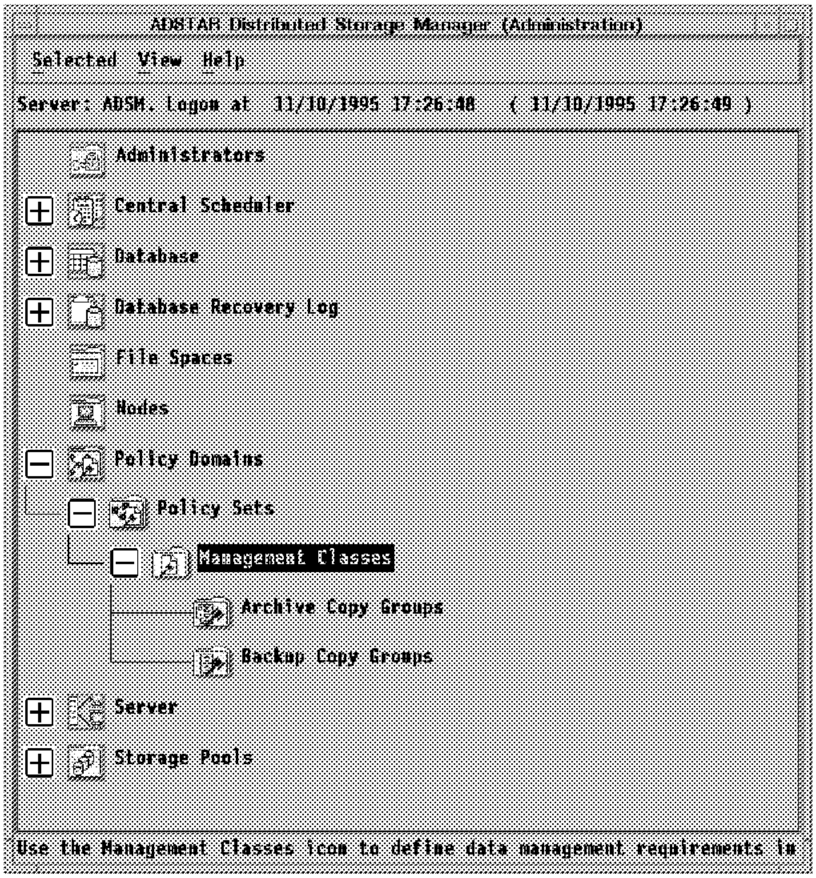


Figure 4. Administrative GUI

Click on the **plus sign (+)** button next to the **Policy Domains** icon to open the icon tree shown in Figure 5.

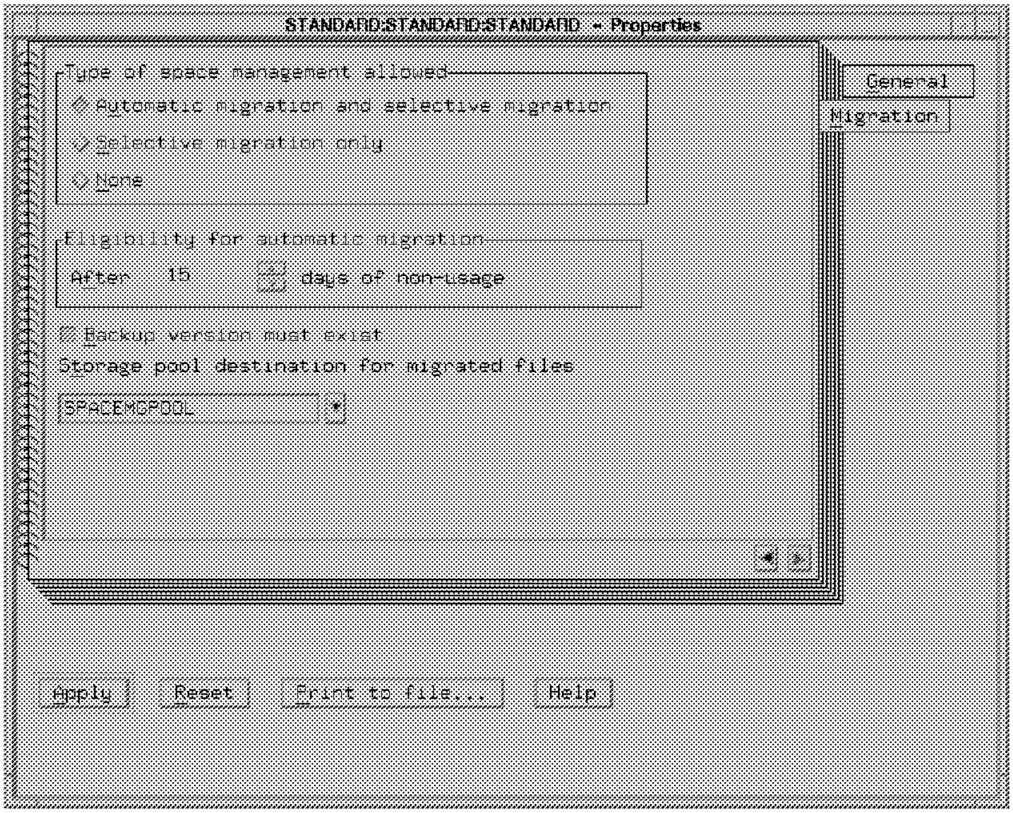


Server: ADSM. Logon at 11/10/1995 17:26:48 (11/10/1995 17:26:49)

Use the Management Classes icon to define data management requirements in

Figure 5. Management Classes

Click on the icon next to **Management Classes** to get to a window that displays all management classes defined in your system. Select the management class that you want to enable for migration. Click on **Selected** and on the pull-down menu item **Open as Properties**. The **Properties** window will appear as shown in Figure 6 on page 26.



STANDARD:STANDARD:STANDARD - Properties

Type of space management allowed

● Automatic migration and selective migration

○ Selective migration only

○ None

Eligibility for automatic migration

After 15 days of non-usage

☒ Backup version must exist

Storage pool destination for migrated files

SPACEMGPOOL

Figure 6. Management Class Properties to Enable Migration

In the **Properties** window you can decide how HSM should work for this management class. In the **Type of space management allowed** selection box you can select **Automatic and selective migration**, **Selective migration only**, or **None**. Then you can decide how long a file has to stay on the HSM-managed file system before it can be migrated.

The **Backup version must exist** option enables you to decide whether the file must have been backed up before it can be migrated through HSM. We strongly recommend that you choose this option to protect your data. When you migrate a file, the only copy of that file resides in the ADSM server. Backing up the file first ensures that a copy of the file is available to restore if recalling the migrated file fails.

Note: You cannot use the **Backup version must exist** option if you are backing up and migrating data to different ADSM servers. You can specify the option in the management class but ADSM does not allow any data to be migrated subsequently because the migration server does not have a backup copy.

The last option you can specify is the storage pool where the migrated files should go. Here you can select from all of the defined storage pools in your environment. We recommend that you use a separate storage pool for the migrated files, but it is possible to use the same storage pool that you use for backup or archive files.

3.2.3 Register the License for HSM

HSM is a separately licensed feature of ADSM. Therefore you have to register a separate license key for HSM by issuing a command at the administrator command line interface. Here is a sample command for an AIX ADSM server:

```
register license 3774ab302cb4a6720ba00
```

The above command would not work in your environment because you need a real license key.

Here is a sample command for an MVS ADSM server:

```
register license spacemgmt
```

3.2.4 Register the HSM Client

The last step is to register the HSM client (if you have not already registered the client as a backup-archive client). You can register the client through the administrative GUI or issue the following command at the administrator command line interface:

```
register node bering s3xjb5 domain=standard
```

If you have set the client registration to open, you do not have to register the client explicitly. The first time the client contacts the server, the user is asked for a password, and the client is registered. We do not recommend setting the registration to open because ADSM administrators would not be able to control which clients use ADSM services.

3.3 Setting Up the HSM Client

Typically the HSM client is installed with the other client code. In this section, we assume that the HSM client has already been installed and proceed with the basic setup for the HSM client. We cover the following tasks:

- Setting up basic parameters in the options files
- Adding HSM to your file systems

These tasks are to be performed by system administrators (root users) of the client systems or an ADSM administrator who has been given root authority on the machine that HSM manages.

3.3.1.1 Setting Up Basic Parameters in the Options Files

After you have installed the client code, you have to set up the client system options file, dsm.sys, and the client user options file, dsm.opt. If you want to separate the include-exclude options from dsm.sys, you can create a separate include-exclude options file and point to it with the INCLEXCL option in dsm.sys. *ADSM: Installing the Clients* provides complete documentation on all of the options that can be used in dsm.sys and dsm.opt. Here, we touch on some of the specific options for HSM.

The client system options file and the optional include-exclude file are systemwide options files that are created by the root user of the workstation. A default client user options file also exists at a central place in the system, but one difference between dsm.sys and dsm.opt is that all users can create their own options file. Users can use the DSM_CONFIG AIX environment variable to point to their own options file instead of the default file.

The dsm.sys and dsm.opt files have the same meaning for HSM as they have when used with the backup-archive client. The client system options file must contain at least the required communication option for each server that the client node will contact. It can also contain options for authorizing the ADSM user, backup-archive processing, schedule processing, and all of the options that affect HSM functionality.

The client user options file generally contains options for messages and prompt formats. Some of these options can be overridden when the user starts the ADSM client.

Client System Options File: With HSM your use of some options are limited. Remember, you are managing active data, so the data is moved from the workstation to an ADSM server. This is in contrast to backup; you can back up data to multiple servers because the original data remains on the workstation.

When pointing to an ADSM server, you can use one of three options: MIGRATESERVER, DEFAULTSERVER, and SERVERNAME. MIGRATESERVER and DEFAULTSERVER are specified in the client system options file. SERVERNAME is specified in the client user options file and applies only to backup-archive services. If you do not specify a MIGRATESERVER, the DEFAULTSERVER will be used. If you do not specify DEFAULTSERVER, the first server stanza specified in dsm.sys will be used.

When migrating data, you must be careful about changing the ADSM server to which you point. For example, if HSM migrates a file to, say, server severn, and somehow the server name is switched to u03aix, when the ADSM client attempts to access a file, HSM will not be able to find the file.

PASSWORDACCESS must be set to GENERATE to enable files to be migrated and recalled transparently. If the file is to be recalled transparently, you do not want to have to prompt the user for a password. The process that is performing the recall (the dsmrecalld daemon) runs independently of any user process. So the password request has to be transferred to the process that accesses the recalled data. If another server process accesses the data (for example, an NFS or database server), the password request has to be transferred to the client of that server (for example, the NFS or database client). This will be impossible or, at the very least, complicated.

Because PASSWORDACCESS must be set to GENERATE, the HSM client does not support the NODENAME option. Thus the HSM client must be registered with the hostname of the real client machine.

Figure 7 on page 29 shows our startup client system options file. Some simple settings are enough initially. We specified the server communications options only.

```
**************************************************************************
*   ADSTAR Distributed Storage Manager                                   *
*                                                                        *
*   Client System Options file (dsm.sys)                                 *
**************************************************************************

DEFAULTServer           u03aix

SErvername              u03aix
  COMMmethod            TCPip
  TCPPort               1500
  TCPServeraddress      9.113.88.172
  PASSWORDACCESS        GENERATE
  INCLEXCL              /usr/lpp/adsm/bin/inclexcl.opt
```

Figure 7. Client System Options File (dsm.sys)

On the INCLEXCL line we specified a separate file, which contains all of our include and exclude statements. In 3.4.2, “Include-Exclude Lists” on page 39, we explain how to use those statements.

Client User Options File: For HSM, it is important to set TAPEPROMPT to NO. If you do not specify NO, you have the same problem as discussed above for PASSWORDACCESS. Figure 8 shows our client user options file.

```
**************************************************************************
*   ADSTAR Distributed Storage Manager                                   *
*                                                                        *
*   Client User Options file (dsm.opt)                                   *
**************************************************************************

SErvername      u03aix

REPLACE          ON
TAPEPROMPT       NO
MAKESPARSE       NO
```

Figure 8. Client User Options File (dsm.opt)

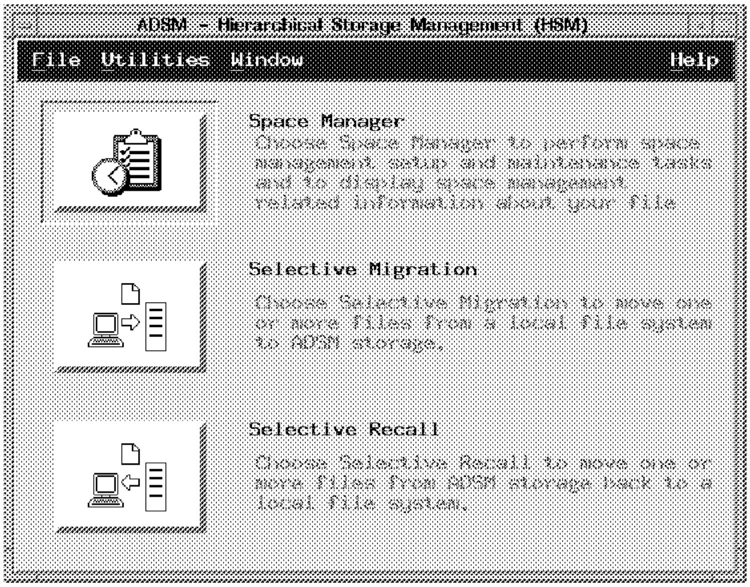
3.3.1.2 Adding HSM to Your File Systems

During the process of adding HSM to a file system, the file system is mounted and a file system migrator (FSM) is mounted over it. The FSM is a kernel extension that intercepts all file system operations and provides any space management support that is required. If space management support is not required, the operation is passed through to the journaled file system (JFS) and performed there.

The mount can be performed either manually or automatically. In this section we describe an automatic mount. For manual mounts please consult *ADSTAR Distributed Storage Manager: Using the UNIX Hierarchical Storage Management (HSM) Clients*.

The AIX operating system mounts file systems automatically at all reboots if there are entries in the /etc/filesystems file. If you add space management to a file system, HSM automatically adds the required entries in that file.

For this task start the HSM GUI with the dsmhsm command. The HSM client contacts the server for the first time. If you have chosen open registration and you are performing this command for the first time, you are asked for the client password. In our case, we explicitly registered the client, so a message window informs us that the client is trying to connect to the server. If the setup is correct, the **ADSM-Hierarchical Storage Management (HSM)** window shown in Figure 9 will open.



Space Manager
Choose Space Manager to perform space management setup and maintenance tasks and to display space management related information about your file

Selective Migration
Choose Selective Migration to move one or more files from a local file system to ADSM storage.

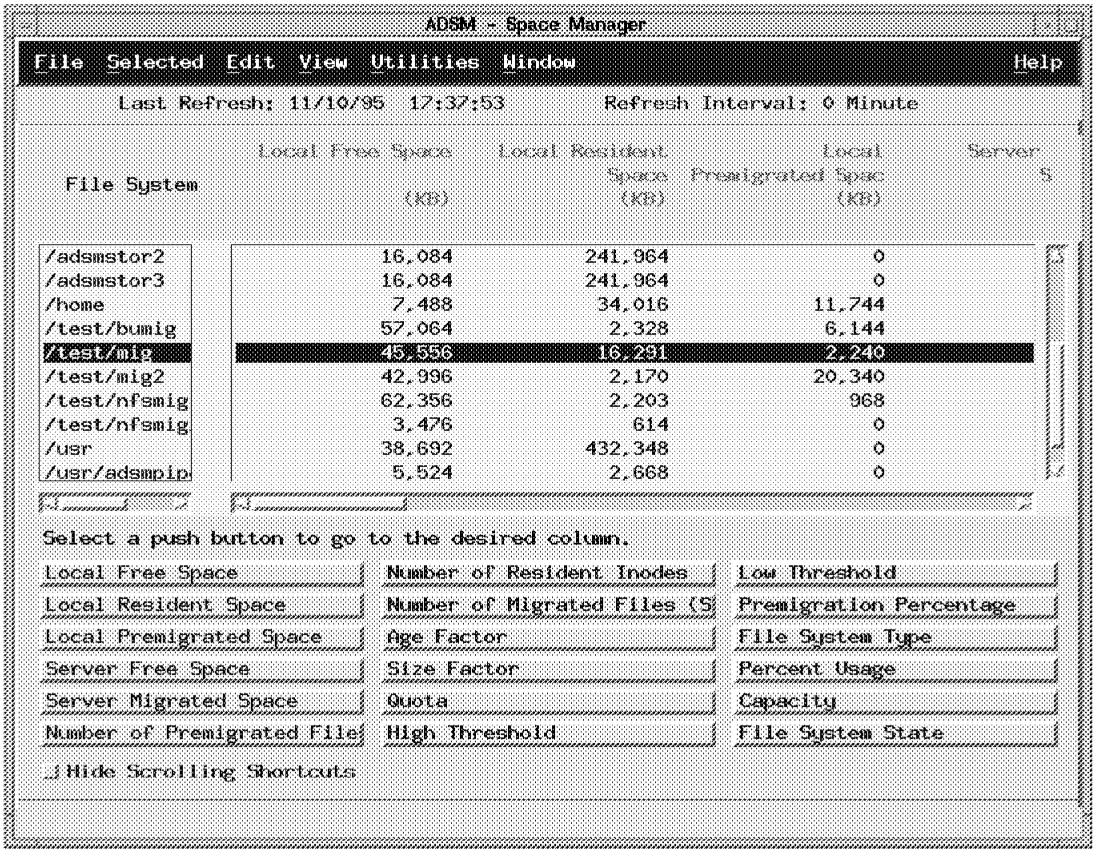
Selective Recall
Choose Selective Recall to move one or more files from ADSM storage back to a local file system.

Figure 9. HSM Graphical User Interface

If this window does not appear or an error message is displayed, please check the following items:

- Can you reach the ADSM server machine? (If you use TCP/IP, try a ping.)
- Is the ADSM server up?
- Are the dsm.sys communication options correct?
- Did you specify the right server in dsm.sys?

Now click on the **Space Manager** button to get to the **ADSM - Space Manager** window (Figure 10 on page 31).



Last Refresh: 11/10/95 17:37:53   Refresh Interval: 0 Minute

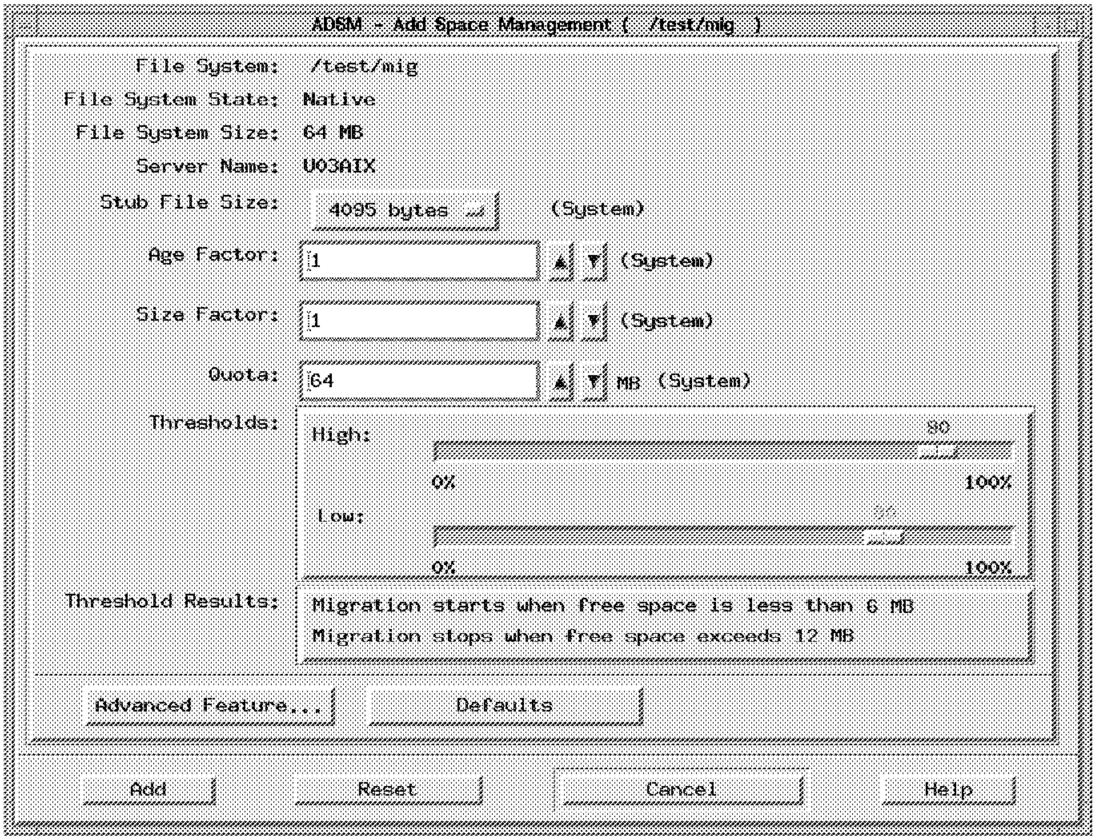
File System	Local Free Space (KB)	Local Resident Space (KB)	Local Premigrated Spac (KB)	Server S
/adsmstor2	16,084	241,964	0	
/adsmstor3	16,084	241,964	0	
/home	7,488	34,016	11,744	
/test/bumig	57,064	2,328	6,144	
/test/mig	45,556	16,291	2,240	
/test/mig2	42,996	2,170	20,340	
/test/nfsmig	62,356	2,203	968	
/test/nfsmig	3,476	614	0	
/usr	38,692	432,348	0	
/usr/adsmpip	5,524	2,668	0	

Select a push button to go to the desired column.

Figure 10. HSM Space Manager Window

In this window you see all existing file systems and HSM-related information, such as **Local Premigrated Space**. You can scroll to the right to view additional information, such as **Server Migrated Space**, **Number of Migrated Files**, and **Size Factor**, or you can use the buttons on the bottom of the window to scroll directly to a column.

To add HSM to one of the displayed file systems, you have to highlight the file system and click on **Selected** in the action bar. In the **Selected** pull-down menu click on **Add Space Management** to open the **Add Space Management** window (Figure 11 on page 32).



ADSM - Add Space Management (/test/mig)

File System: /test/mig
File System State: Native
File System Size: 64 MB
Server Name: U03AIX
Stub File Size: 4095 bytes (System)
Age Factor: 1 (System)
Size Factor: 1 (System)
Quota: 64 MB (System)
Thresholds:
High: 90
Low: 80
Threshold Results:
Migration starts when free space is less than 6 MB
Migration stops when free space exceeds 12 MB

Figure 11. The ADSM-Add Space Management Window

In the **ADSM - Add Space Management** window you can set up the space management policies for the file system. Initially, you can choose the default settings. If necessary you can tailor the settings to your real requirements. To confirm the default settings click on **Add**. You will get an information window informing you of the successful add, and the status of the file system will change to **Active**.

Repeat the above procedure for all file systems for which you to want add space management. Then you will be able to migrate and recall files in those file systems.

In Chapter 5, “How to Use HSM” on page 63 we explain in detail how to perform selective migrate and recall.

3.3.2 Tailoring HSM Parameters for File Systems

After you have added HSM to your file systems, you may have to change some HSM-related parameters to adapt the HSM functions to your own requirements. Values you can change are:

- Stub File Size - the size of the remaining stub files after migration
- Age and Size Factors - the values that influence the file sequence in the migration candidates list
- Thresholds - which control automated threshold migration
- Quota - the total number of megabytes that can be migrated or premigrated from the file system to an ADSM server

To tailor the HSM parameters, start from the **ADSM - Space Manager** window (Figure 10 on page 31). Select the file system whose parameters you want to change, and click on **Selected**. In the **Selected** pull-down menu click on **Update Space Management**. The **ADSM-Update Space Management** window will open similar to that shown in Figure 11 on page 32. In this window you can update all HSM-related parameters. When you have finished, click on the **Update** button to apply the changes.

If you do not change the parameters, the defaults for the following three parameters will be calculated according to your system′s configuration and other HSM parameters:

Stub File Size Is equal to the file system block size minus 1. In AIX 3.2.5 the block size is 4 KB, so the default stub file size is equal to 4095 bytes.

Premigration Percentage
Is the difference between the high and the low threshold, in percent, of file system space that should stay in a premigrated state. If you later change the values for high or low threshold, the premigration percentage will be recalculated.

Quota Is equal to the file system size, which is actually managed with HSM. If you enlarge the file system size after adding space management, the quota will be automatically increased.

Sometimes it is a good idea to set the values back to the default so that the parameters can change dynamically. There are two ways to do this: You can click on **Defaults** in the **ADSM - Update Space Management** window (this action changes all parameter values back to the default values), or you can edit the /etc/adsm/SpaceMan/config/dsmmigfstab file (see Figure 19 on page 50; the minus signs indicate defaults). **Be careful when directly editing this file. You might change a value for a parameter that does not have a dynamic value.**

3.3.2.1 Stub File Size

The stub file size is the size of the remaining place holder file that is created after the original file is migrated to the ADSM server. It contains all information necessary to locate and recall the original file from the ADSM server and for HSM to respond to some basic AIX commands such as **ls** and **find**. For this information the stub file size must be at least 511 bytes.

With HSM you can increase the stub file size beyond 511 bytes, and the remaining space will be used to store the first bytes of the original file. This is called *leader data*. If the file is accessed as read only and only the first bytes are read, the file is not recalled.

Valid values for the stub file size are sizes that are powers of 2 minus 1 byte (for example 511, 1023, 4095, ... up to 32767 bytes). The minimum value is 511 bytes. The default is 4095 bytes.

To correctly set the stub file size, consider these factors: The default file system block size under AIX is 4096 bytes. If you set the stub file size to a value lower than 4095 bytes, the operating system will use a 4 KB block to store this file, and you will waste storage. If you choose a larger value, you should consider the average file size in your file system. A file will be migrated only if the file size is greater than the stub file size plus 1 byte or greater than the block size of the file system.

We recommend a minimum stub file size that is equal to the file system block size minus 1. If you have a large stub file size and a small average file size, a lot of files will not be migrated. We recommend a larger stub file size only in cases where you have large files and will frequently access only the leader data.

3.3.2.2 Age and Size Factors

For automated migration it is important to have rules for selecting files that will be migrated first. HSM uses the following simple formula to calculate a score value:

score_value = (size_factor * size) + (age_factor * age)

The size_factor and age_factor are weight factors that you can set up for each file system. The size is the real file size in blocks rounded up to 1 KB, and the age is the time since the file was last accessed rounded up to full days. Files with the largest score value will be migrated first.

With the score value in mind, you can set up many different scenarios. Notice, however, that a size difference of 1 KB is not as much as a time difference of 1 day, so setting the weight factors to 1:1 will not create an equal balance between size and age. For example, if you have two files, file A is 1 MB and file B is 1 KB, file A has an age of 1 day, but file B has to have an age of 1024 days or nearly three years in order for the score value to be equal.

This discussion assumes that the files are eligible for migration. Remember, you can set up in your management class definition a time frame for how long a file has to stay on the local disk before it is eligible for migration. You can also require that a backup copy exist before a file can be migrated. These management class controls prevent a file from being migrated no matter what its score value is.

For further discussion and recommendations on setting score values, refer to 2.4, “Priority of Size and Age Factors” on page 14.

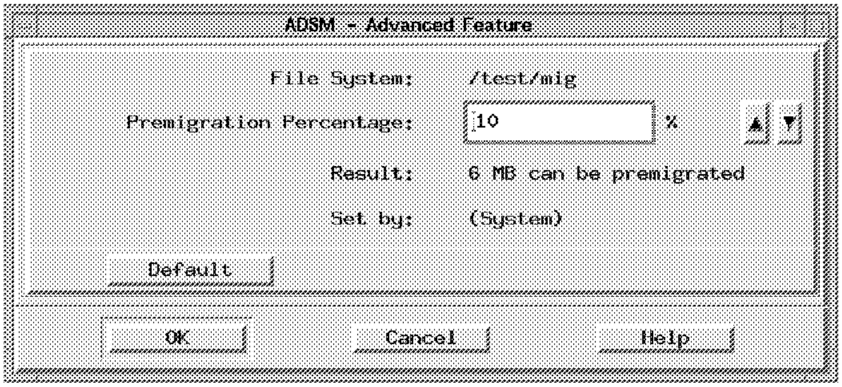
3.3.2.3 Thresholds

With the threshold parameters you control the point when automated threshold migration starts and stops. There are three thresholds. The high threshold defines the point at which threshold migration should be started. At defined intervals, the HSM monitor daemon compares the space usage of a file system with the high threshold. If the high threshold is exceeded, threshold migration begins.

The second threshold is the low threshold. Threshold migration will stop once the amount of space used in the file system is below the low threshold.

The third threshold that HSM uses is based on the value of the *premigration percentage*. The default for the premigration percentage is the difference between the high and the low threshold. The premigration percentage is subtracted from the low threshold to obtain the “premigration threshold.” After the low threshold is reached, ADSM copies data to the ADSM server and leaves the original file intact on the local file system in a premigrated state. The premigration threshold is the point at which premigration stops. Thus ADSM can quickly clear off space when migration next begins. HSM can migrate a premigrated file simply by replacing that file with a stub file without having to first copy the file to ADSM storage.

To change the premigration percentage, click on the **Advanced Feature...** button on the **ADSM - Update Space Management** window (similar to Figure 11 on page 32). On the **ADSM - Advanced Feature** window (Figure 12) you can change this value as you like. Click on **OK** to save the changes.


ADSM - Advanced Feature

File System: /test/mig

Premigration Percentage: 10 %

Result: 6 MB can be premigrated

Set by: (System)

Figure 12. ADSM Advanced Features Window

For further discussion and recommendations on setting threshold values, refer to 2.5, “High and Low Thresholds” on page 15.

3.3.2.4 Quota

With the quota parameter you can control how much ADSM server storage is used for migrated files. The root user must consult the ADSM administrator to determine the best value for the parameter. The value depends on the expected growth of the file system as well as available storage space on the ADSM server. Remember that when the quota is reached, no more files can migrate. Thus if your file system is full and you have to recall a file, the recall will not be successful because ADSM cannot migrate any files from the local file system to make room for the file that has to be recalled.

For further discussion and recommendations on using quotas, refer to 2.2, “Using Quotas” on page 13.

3.3.3 Setting up Automated Space Management

HSM can perform all migration and recall tasks automatically and transparently for the user. In this section we show how you can set up the automatic function and change the behavior of the automated tasks to match your requirements.

3.3.3.1 Overview

The most important part of space management automation is the space monitor daemon, dsmmonitord. This daemon monitors space usage on all file systems for which space management is active. It also starts these processes:

- Threshold migration
- Reconciliation
- Demand migration

The daemon is started automatically when the first HSM-managed file system is mounted. If for any reason the space monitor daemon stops running, the root user can start it by issuing the **dsmmonitord** command.

On a regular basis the dsmmonitord performs threshold migration and reconciliation. The frequency with which these processes occur depends on the values set for the CHECKTHRESHOLDS and RECONCILEINTERVAL options in the dsm.sys file. The dsmmonitord “wakes up” at frequent intervals (every 2 seconds), checks for any out-of-space conditions, and then checks whether the intervals set for threshold migration or reconciliation have elapsed.

If the time interval for threshold migration has been reached, dsmmonitord checks space usage on all file systems for which space management is active. If one file system′s space usage equals or exceeds the high threshold, dsmmonitord invokes dsmautomig to perform threshold migration. The maximum number of parallel automatic threshold migration processes depends on the setting of MAXTHRESHOLDPROC in the dsm.sys file.

If the time interval set for reconciliation has elapsed, the dsmmonitord invokes the dsmreconcile process to reconcile all file systems for which space management is active. The reconciliation process then:

1. Verifies that there is a stub file for each migrated file. If not, it marks the migrated copy of the file for expiration, and, after the expiration interval the file is deleted from ADSM storage.
2. Verifies that there is a migrated file in ADSM storage for each stub file. If not, the name is recorded in the orphan.stubs file in the .SpaceMan directory of the file system.
3. Verifies that premigrated files are still valid. If a premigrated file is modified or deleted, the copy in ADSM storage is marked for expiration.
4. Checks for which files have expired and removes them from ADSM server storage.
5. Updates some status information and builds a new migration candidates list.

The maximum number of parallel automatic reconciliation processes depends on the setting of MAXRECONCILEPROC in the dsm.sys file.

When it wakes up, the dsmmonitord also checks for an out-of-space condition, that is, the need for a demand migration. If it finds an out-of-space condition, it checks whether dsmautomig is running for the affected file system. If it is not, the dsmmonitord invokes dsmautomig regardless of whether the maximum number of migration processes specified by the MAXTHRESHOLDPROC option has been reached.

The dsmmonitord also checks whether /etc/adsm/SpaceMan/config/dsmmigfstab has been changed. If the file has been changed, it reads the file contents again.

Another daemon, the ADSM master recall daemon (dsmrecalld), is responsible for transparent and automated recall. It creates a slave recall daemon (also called dsmrecalld) for every file that has to be recalled. The number of recall daemons that can run in parallel is determined by dsm.sys options MINRECALLDAEMONS and MAXRECALLDAEMONS.

The slave recall daemons are started automatically by the master recall daemon if a process has requested access to a migrated file. If the KERNELMESSAGE option in the dsm.sys file is set to YES and the recall daemon can recall the file, the kernel sends the following message to the stdout stream (usually, this message is sent to the window where you started the process that accessed the migrated file):

```
ANS9283K Attempting to access remote file.
```

Then the recall daemon copies the file from ADSM storage and informs the kernel that the file has been recalled.

If the file cannot be recalled, the kernel sends the following message to the stderr stream:

```
ANS9285K Cannot complete remote file access.
```

3.3.3.2 Setting Up the Daemons and the Environment

Automation is set up as soon as you install the HSM client code. At that point the /etc/rc.adsmhsm script is created. This script is the startup script for integrating space management into the AIX operating system. In addition, the following entry is added to the /etc/inittab file:

entry to /etc/inittab file

```
adsmsmext:2:once:/etc/rc.adsmhsm # ADSM SpaceMan
```

This entry causes the /etc/rc.adsmhsm script to be executed once at all system restarts. For more information on what this script does, refer to page 49.

3.3.3.3 Automation-Related Parameters

Several HSM parameters influence the automation processes. The root user of the client system can set these in the client system options file (dsm.sys). The parameters are valid for the whole system, and end users cannot override them with command line options. If you want to change these parameters, you must first bring down the dsmmonitord daemon. Once you have changed the parameters, you have to restart the daemon. See 4.5, “Maintaining the Space Management Daemons” on page 60.

Figure 13 on page 38 shows a sample dsm.sys file with the space management parameters we describe below. The actual values you use for the parameters depend on your own requirements.

```
************************************************************************
*   ADSTAR Distributed Storage Manager                                 *
*                                                                      *
*   Client System Options file (dsm.sys)                               *
************************************************************************

DEFAULTServer           u03aix
MIGRATEServer           u03aix
CHEckthresholds         2
RECOncileinterval       0
MAXRECOncileproc        5
MAXThresholdproc        5
MIGFILEEXPiration       7
MINRECAlldaemons        5
MAXRecalldaemons        15
KERNelmessages          Yes


SErvername              u03aix
  COMMmethod            TCPip
  TCPPort               1500
  TCPServeraddress      9.113.88.172
  PASSWORDACCESS        GENERATE
  INCLEXCL              /usr/lpp/adsm/bin/inclexcl.opt
```

Figure 13. Sample dsm.sys File with Space Management Options

CHECKTHRESHOLDS
Specifies the time interval, in minutes, during which the space monitor daemon checks space usage on local file systems.

RECONCILEINTERVAL
Specifies the time interval, in hours, during which the space monitor daemon initiates the reconciliation process.

MIGFILEEXPIRATION
Specifies the number of days to retain copies of migrated and premigrated files in ADSM storage after they have been modified or erased from the local file system.

MAXRECONCILEPROC
Specifies the maximum number of automatic reconciliation processes ADSM can run at one time for a client node.

MAXTHRESHOLDPROC
Specifies the maximum number of automatic threshold migration processes ADSM can run at one time for a client node.

MINRECALLDAEMONS and MAXRECALLDAEMONS
Specify the minimum number of recall daemons that have to be retained and the maximum number that can be run at one time.

ERRORPROG Specifies the server to which ADSM sends a message if a severe error occurs during space management processing.

Further descriptions and default values for these parameters are provided in *ADSM: Installing the Clients*. The valid ranges of values for these parameters are provided in *ADSM: Using the UNIX Hierarchical Storage Management (HSM) Clients*.

3.4 Setting Up Advanced Features

In this section we cover the special options that you can use to tailor your environment.

3.4.1 Kernel Recall Messages

With the HSM client you can use kernel recall messages to inform users that they are recalling a remote file. We recommend this option if most file accesses that would cause a recall are interactive, for example, editing. If most file accesses are not interactive, for example, an NFS or database, kernel recall messages are not useful.

Add the KERNELMESSAGES parameter to your dsm.sys file. The possible values are YES or NO; the default is YES. When you change the value, the change will not take effect until the HSM kernel extension is loaded. This typically occurs at each system reboot, initiated by the /etc/rc.adsmhsm script.

3.4.2 Include-Exclude Lists

The include-exclude options have been enhanced in HSM to enable administrators to specify which data should be migrated, which backed up, and which ADSM should not manage. Especially for space management, not all data is well suited to be managed by (see 3.1, “Planning Considerations” on page 19).

The following include-exclude options are provided for creating your own include-exclude lists:

INCLUDE Includes a file for both space management and backup services. When you exclude a group of files, you can use an INCLUDE option to include a subset of those files.

EXCLUDE Excludes a file from both space management and backup services. Any file you exclude with this option is not considered for migration or backup.

EXCLUDE.SPACEMGMT
Excludes a file from space management services only. Any file you exclude with this option is not considered for migration.

EXCLUDE.BACKUP Excludes a file from backup services only. Any file you exclude with this option is not considered for backup. Note that you cannot exclude a file from being archived. Also, be careful what you exclude from backup if your management class requires that a file be backed up before it is migrated.

You can also use this option to:

- Assign a specific management class to a file or a group of files

- Assign a management class to all files to which you do not assign a specific management class

A common use of the include-exclude options is to create a separate include/exclude options file and point to it with the INCLEXCL client system option as shown in Figure 13 on page 38. When the backup-archive client or the space management client is looking for candidates for backup or migration, it inspects the file from bottom up and compares all files with the entries in the include-exclude options file. The client uses the first matching entry to determine whether the file is included or excluded and which management class will be used for its service. If there is no matching entry in the include-exclude file, the file is assumed to be included and managed with the default management class.

We provide two examples to demonstrate how to use the include-exclude options in connection with space management and backup of typical systems.

Example 1: This example covers the simplest case of managing a workstation with ADSM for backup and space management. The workstation configuration has five file systems: / (root), /tmp, /var, /usr, and /home. For backup service you can include all file systems, except the /tmp file system. The /tmp/ file system contains temporary data only, which is erased from time to time and can be easily re-created.

In 3.1, “Planning Considerations” on page 19 we show that in this case only the /home file system is suitable for space management. From a disaster recovery point of view (see Chapter 7, “Recovery with ADSM and HSM” on page 87), it is also a good idea to exclude from backup the .SpaceMan directory of each file system managed by HSM and the central space management data in the /etc/adsm/SpaceMan directory. Only the /etc/adsm/SpaceMan/config/dsmmigfstab should be backed up to prevent a restore from bringing back old space management control data. In this example we use the default management class. With these considerations in mind we create the include-exclude file shown in Figure 14.

```
************************************************************************
* ADSTAR Distributed Storage Manager                                   *
*                                                                      *
* Include-Exclude Options file for UNIX clients  (inclexcl.opt)        *
************************************************************************

EXCLUDE.SPACEMGMT ″/usr/.../*″
EXCLUDE.SPACEMGMT ″/var/.../*″
                                * exclude /usr and /var from
                                * space management
EXCLUDE.BACKUP    ″/etc/adsm/SpaceMan/.../*″
INCLUDE.BACKUP    ″/etc/adsm/SpaceMan/config/dsmmigfstab″
EXCLUDE.BACKUP    ″/home/.SpaceMan/.../*″
                                * exclude space management related
                                * data from backup except the
                                * dsmmigfstab
EXCLUDE           ″/tmp/.../*″
                                * /tmp is excluded from backup
                                *   and from space management
```

Figure 14. Sample inclexcl.opt File

With the exclude statements we exclude the above-described directories and file systems from backup. The first two exclude options exclude the /usr and the /var from space management. Remember, / and /tmp are excluded by default from ADSM, so there is no need to exclude them with an explicit exclude option.

The next two exclude options exclude the space management directories from backup. The last option excludes the /tmp file system from both backup and space management.

Example 2: This example uses the same entries from example 1. In addition there is a /project file system with different requirements for backup and migration. The /project file system has the following directories:

../development Contains fast growing data, which should be backed up and migrated to fast media

../definitions Contains frequently accessed data that is not growing but is really important. It should be backed up, but there is no need for space management

../data Contains a large amount of data, which could be reproduced. There i s no need for backup, but there is a need for large virtual file systems (space management to tape).

For the data in the /project/data directory, we established a management class, TAPEMIG, which has a tape pool as the copy destination. With the above considerations in mind we create the include-exclude file that covers our requirements and add it to the end of the existing inclexcl.opt file as shown in Figure 15.

```
*
* bottom of the inclexcl.opt file:
*    here are the additional entries for the file system
*    /project

INCLUDE           ″/project/.../*″
                                * include all subdirs of /project for
                                * space management and backup
EXCLUDE.SPACEMGMT ″/project/definitions/.../*″
                                * the definitions subdir
                                * is excluded from space man.
INCLUDE           ″/project/data/.../*″  TAPEMIG
EXCLUDE.BACKUP    ″/project/data/.../*″
                                * excludes the data subdir from
                                * backup and gives them another
                                * management class for migration
```

Figure 15. Sample inclexcl.opt File: Additional Entries

Because of the bottom-up processing of the include-exclude file, all data under /project/data will be excluded from backup but included for migration and will use the TAPEMIG management class. All data under /project/definitions will be excluded from space management. The other data, which includes the development data, will be backed up and migrated with the default management class.

3.4.3 Advanced Recall Modes

For special situations HSM provides advanced recall modes. By changing the recall mode for a migrated file or the execution mode of a command, you can change how HSM recalls a migrated file.

3.4.3.1 Changing the Recall Mode of a File

HSM provides three different recall modes for a file:

Normal If the file is recalled by a process that does *not* modify it, it remains in a premigrated state. If it is recalled by a process that modifies it, it becomes a resident file.

Migrate-on-close If the file is recalled by a process that does *not* modify it, it is returned to a migrated state. The file is recalled to its original place in the file system only temporarily. If it is recalled by a process that modifies it, it becomes a resident file.

Read-without-recall When a process accesses the file, the file is recalled sequentially from ADSM storage without storing it on the local file system. Data is stored temporarily in a kernel memory buffer. The last piece of information read from the file is cached in a kernel memory buffer on the local workstation.
If memory is swapped or file attributes such as modification date and access time are modified, *normal* recall is used, and the file remains in a premigrated state.

We recommend using the read-without-recall mode only when one process accesses the file exclusively. We also recommend using read-without-recall mode only if you read the file sequentially. Accessing the file with multiple processes or seeking backward in the file is possible but causes significant performance degradation.

Do not use migrate-on-close or read-without-recall on file systems that are exported through NFS. NFS opens and closes a file many times and thus produces a lot of copy overhead. Therefore in all cases where an NFS client accesses HSM-managed data, the recall mode will be reset to normal, regardless of its previous setting. For more detailed information about NFS considerations refer to Chapter 6, “Migrating NFS File Systems” on page 71.

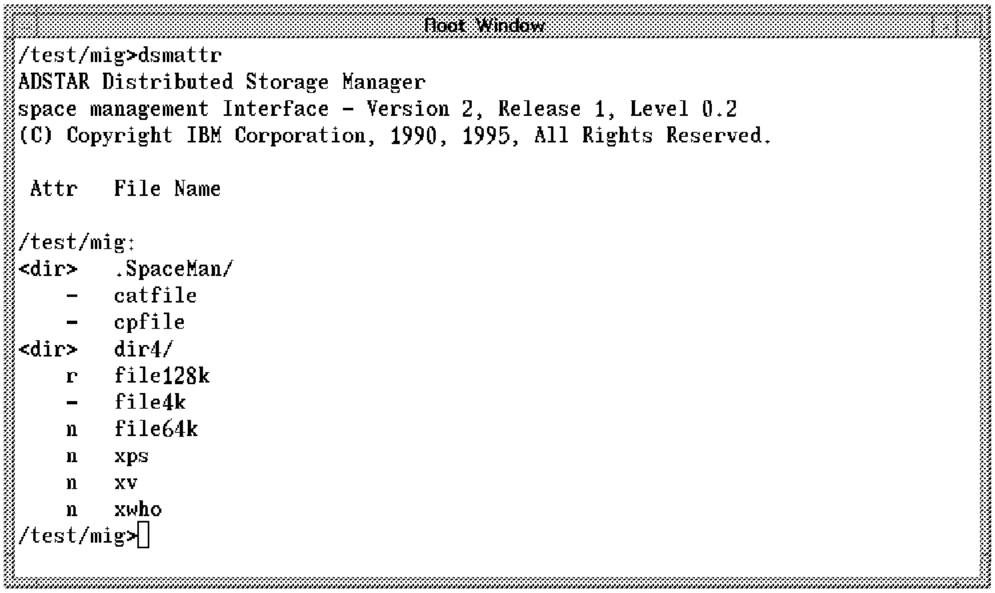
To set or display the recall modes of a migrated file, use the **dsmattr** command. There is no function in the GUI that supports this task. You cannot set the recall mode for a resident file or a premigrated file. The recall mode set for a migrated file remains associated with the file for only as long the file remains migrated.

In the examples that follow we show how you can change the recall mode of a single file to read-without-recall, change the recall mode of a whole subtree to migrate-on-close, and use the **dsmattr** command to display the current recall mode of a file.

To set migrated file `file128k` to read-without-recall use the following command:

```
dsmattr -recall=r file128k
```

To see the results of changing the recall mode of file128k use the **dsmattr** command as shown in Figure 16 on page 43.



```
/test/mig>dsmattr
ADSTAR Distributed Storage Manager
space management Interface - Version 2, Release 1, Level 0.2
(C) Copyright IBM Corporation, 1990, 1995, All Rights Reserved.

 Attr   File Name

/test/mig:
<dir>   .SpaceMan/
    -   catfile
    -   cpfile
<dir>   dir4/
    r   file128k
    -   file4k
    n   file64k
    n   xps
    n   xv
    n   xwho
/test/mig>
```

Figure 16. Dsmattr Command to Display the Recall Modes of Migrated Files

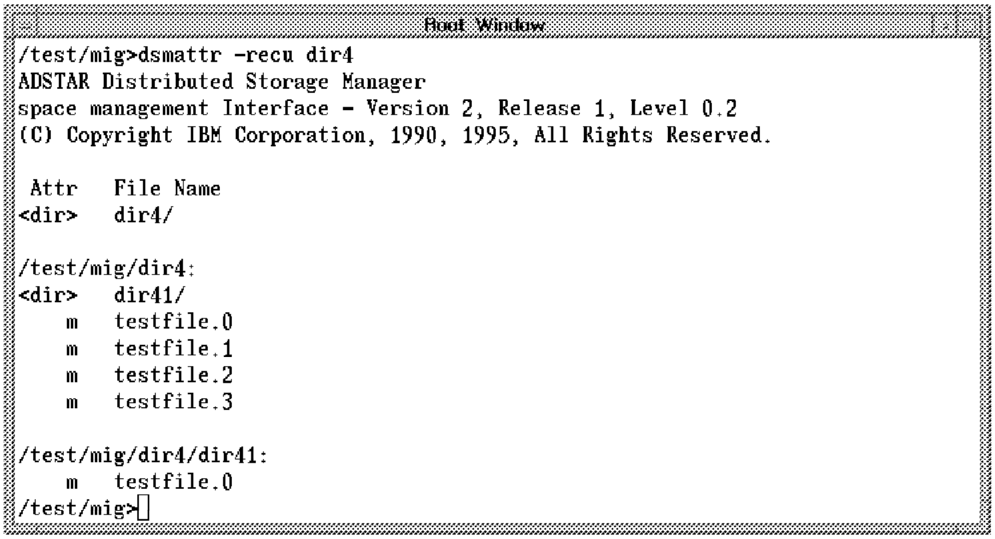
The file names are preceded by a single character that indicates the following:

-	File not migrated
n	Normal recall mode
m	Migrate-on-close recall mode
r	Read-without-recall mode

To set all migrated files in subdirectory tree dir4 to the migrate-on-close recall mode use the following command:

```
dsmattr -recall=m -recu dir4
```

Figure 17 on page 44 shows the results.



```
/test/mig>dsmattr -recu dir4
ADSTAR Distributed Storage Manager
space management Interface - Version 2, Release 1, Level 0.2
(C) Copyright IBM Corporation, 1990, 1995, All Rights Reserved.

 Attr   File Name
<dir>   dir4/

/test/mig/dir4:
<dir>   dir41/
    m   testfile.0
    m   testfile.1
    m   testfile.2
    m   testfile.3

/test/mig/dir4/dir41:
    m   testfile.0
/test/mig>
```

Figure 17. Dsmattr Command to Change the Recall Mode of Migrated Files to Migrate-on-Close

Figure 16 on page 43 shows that the recall mode of `file128k` has been changed to read-without-recall. Figure 17 shows that the recall modes of all files in `/test/mig/dir4` have been set to migrate-on-close.

Figure 17 shows how you can use the **dsmattr** command to list a directory tree. In our example we list the directory tree under `/test/mig/dir4` to show that the recursive change of the recall modes was successful.

3.4.3.2 Changing the Execution Mode of a Command

By *execution mode* we mean the way in which a command handles HSM-managed data. You can set up four different execution modes for a command:

Data access control mode

Determines whether a migrated file can be accessed by the command.
The possible values are **normal** for transparent access; **zero-length**, which indicates that all migrated files appear to be zero length; and **Error**, which indicates that the process cannot access the migrated file. The default value is **normal**.
Even when the data access control mode of a command is normal, some commands may not require a recall because the data needed for that command is available in the stub file. For a list of commonly used UNIX commands that may not cause a recall, refer to Appendix C, "Common UNIX Commands and Recall" on page 111.

Timestamp control mode

Determines whether the access time for a file is set to the current time, when the migrated file is accessed. You must have root user authority to change this execution mode.
The possible values for this mode are **normal**, which indicates that the access time of the file is changed when the file is accessed, and **preserve**, which indicates that the

access time and inode change time (ctime) do not change when the file is read or its attributes are changed. The default value is **normal**.

Out-of-space protection mode

Determines whether HSM attempts to recover from an out-of-space condition.
The possible values are **normal**, which indicates that HSM tries to recover from an out-of-space condition by migrating eligible files to ADSM storage and avoid returning input/output errors to user processes if possible, and **error**, which indicates that there is no interception of the out-of-space condition. The default value is **normal**.

Recall mode

Determines how HSM recalls a migrated file when it is accessed. The possible values are **normal** and **migonclose**, both of which have the same meaning they have when used to set the recall mode of a file. If the recall mode of a command is different from the recall mode of the file it is accessing, ADSM chooses the recall mode by preferring read-without-recall, then migrate-on-close, and finally normal. This mode is explained in detail in *ADSM: Using the UNIX Hierarchical Storage Management (HSM) Clients*.

If you want to use the UNIX **grep** command to search a directory, but to skip migrated files, you can change the data access mode to **error** before issuing the command. Also, if you want to prevent a command, such as a utility that creates backup versions of files, from updating access times, a root user can change the timestamp control mode of the command.

To change the execution mode of a command use the **dsmmode** command. There is no GUI function that covers this task. There are two ways to use the **dsmmode** command. First, you can enter the **dsmmode** command and its arguments. The command and its child processes will be immediately executed with the specified execution mode options.

Second, you can use **dsmmode** without specifying any other commands. A new shell will be started with the selected execution mode. All commands executed in this shell will use that execution mode. It is also possible to nest **dsmmode** commands within this shell.

For more information about the syntax of the **dsmmode** command refer to *ADSM: Using the UNIX Hierarchical Storage Management (HSM) Client*. The following is an example of using the **dsmmode** command to change the data access mode for the execution of the UNIX **grep** command:

```
dsmmode -dataaccess=z grep spaceman *
```

The **grep** command will be executed with the zero length data access mode. If a file is currently migrated, it is assumed that the file size is 0 bytes, so the **grep** command does not cause a recall of the file.

This example shows you how you can start a shell with the preserve timestamp control mode.

```
dsmmode -timestamp=p
```

All commands executed in this shell will preserve the existing values of access time (atime) and the inode change time (ctime) of any accessed file.

Chapter 4. Care and Feeding of HSM

This chapter is a collection of topics on the care and feeding of an HSM system once HSM is installed and running. The topics covered are:

- Scheduling space management tasks
- HSM control files and directories
- HSM and AIX interoperability
- Handling orphaned stub files
- Maintaining the space management daemons

4.1 Scheduling Space Management Tasks

You can use the client command schedule to perform space management tasks on a regular basis. This section provides some examples of scheduled space management tasks and briefly describes how to set them up.

4.1.1 Examples of Scheduled Space Management Tasks

If you have a heavily used system and need all of your performance for computing tasks, you might prefer to run all migration and reconciliation tasks when the system is not busy, perhaps at night. In this way migration will occur only as an emergency measure if the file systems suddenly fill up with data. For more information and recommendations on automating migration and reconciliation, refer to 2.3, “Nightly Migration and Reconciliation” on page 14.

If you know in advance that you will need a certain group of files, you can recall all of the files you need at once before you begin to work on them. An example would be some large data files that you will need for only one calculation at the end of the month. For this task you can set up a schedule.

To schedule the commands for reconciliation, migration, or recall use the UNIX cron scheduler or the ADSM central scheduler. If you use the UNIX cron scheduler, you have to set up and manage all scheduled tasks for each client individually. If you use the ADSM central scheduler, you can create central scheduled tasks for a group of similar clients. ADSM also provides central logging of the completion of schedules. In this section, we describe how to use ADSM scheduling to automate these tasks.

The following are some space management tasks that can be scheduled:

- Reconciliation, through the **dsmreconcile** command
- Threshold migration, through the **dsmautomig** command
- Selective migration, through the **dsmmigrate** command
- Selective recall, through the **dsmrecall** command

When determining the timing of space management tasks, keep in mind that you may already have other ADSM schedules defined, such as for backup.

4.1.2 Setup of ADSM Central Scheduled Tasks

The ADSM administrator and the root user of the client workstation can set up the central scheduler of ADSM to perform space management tasks at specified intervals or specific times. Central scheduling requires a cooperative effort between an ADSM server and the client node. The ADSM administrator has to perform the following tasks:

- Define schedules on the server
- Associate the client nodes with the schedules
- Specify how the client scheduler should contact the server
- Balance the scheduled work

The root user on the client workstation has to perform the following tasks:

- Set up client scheduling options in the client system options file (dsm.sys)
- Start the client scheduler or make an entry in the /etc/inittab file for automated start at any system reboot

The ADSM administrator defines the schedules through either the administrative GUI or command line interface. When defining the schedule, the ACTION should be COMMAND and the HSM command is specified on the OBJECTS parameter. The ADSM administrator must then associate the schedules with the HSM clients. For examples of schedules that we defined during our project see Appendix A, "Macros Used to Set Up Automation" on page 105.

After the ADSM administrator has set things up on the server side, the root user has some tasks to do on the client side. First the root user has to establish some scheduling-related options in dsm.sys. These already may be defined if you have been scheduling incremental backups for the system. For more information on the client scheduling options, refer to *ADSTAR Distributed Storage Manager Version 2: Using the UNIX Backup/Archive Clients*.

Second, the root user has to start the client scheduler, either automatically or manually. The following entry in /etc/inittab starts the scheduler automatically at any system reboot and restarts the scheduler if it goes down for any reason (the output is set to minimum):

entry in /etc/inittab

```
adsmsched:2:respawn:/usr/lpp/adsm/bin/dsmc sched -quiet >/dev/null
2>&1 # Start the ADSM Scheduler
```

To manually start the client scheduler, use the following command:

```
nohup dsmc sched > /dev/null 2>&1 &
```

4.2 HSM Control Files and Directories

Sometimes, if something goes wrong and the application returns cryptic error messages, it is good to have an understanding of the internals of the application. In this section we take a look under the surface of HSM. The information we provide is not required to use HSM. If you take pleasure in information for information′s sake, however, read on.

Note: Be very careful about changing the contents of any of the control files we discuss in this section. If you change or delete some of the files, you can seriously damage HSM. The HSM client cannot re-create all files. In the case of accidental loss of one or more control files, we highly recommend removing and adding space management to the affected file system or reinstalling HSM and re-creating the data files from your backup copy.

In this section we cover the following topics:

- File system changes at HSM installation time
- HSM control files
- .SpaceMan directory of an HSM-managed file system

4.2.1 File System Changes at HSM Installation Time

All HSM control files and executables are usually installed in the /usr/lpp/adsm directory. At HSM installation time, however, the installation process changes some operating system control files and creates some directories and files to integrate space management into the operating system. Below we briefly describe how these changes occur when you install the client code.

To define the FSM as a new virtual file system to your operating system, the installation process adds the following entry to the /etc/vfs file:

entry in /etc/vfs

```
fsm    15    /sbin/helpers/fsmvfsmnthelp    none
```

This entry defines the FSM with a file system ID of 15 and points to a mount helper for the FSM in the /sbin/helpers directory. The number 15 is usually chosen unless another virtual file system is already using it. If so, the install process chooses a lower number. At installation time the install process creates a symbolic link from this directory to the original location of the mount helper in the /usr/lpp/adsm/bin directory.

The installation process creates the rc.adsmhsm file in the /etc directory. The rc.adsmhsm file is the startup script for integrating space management in the AIX operating system. It:

- Sets the DSM_CONFIG, DSM_DIR, and DSM_LOG environment variables for the space management daemons
- Loads the ADSM space management kernel extension
- Starts the main dsmmonitord and dsmrecalld daemons
- Mounts FSM over all file systems that HSM will manage. The script uses the /etc/adsm/SpaceMan/config/dsmmigfstab file system table to determine which file systems are HSM-managed.
- Mounts native file systems nested in HSM-managed file systems

The /etc/rc.adsmhsm script has to be run once at system reboot. For this the installation process adds the following entry to the /etc/inittab file:

entry in /etc/inittab

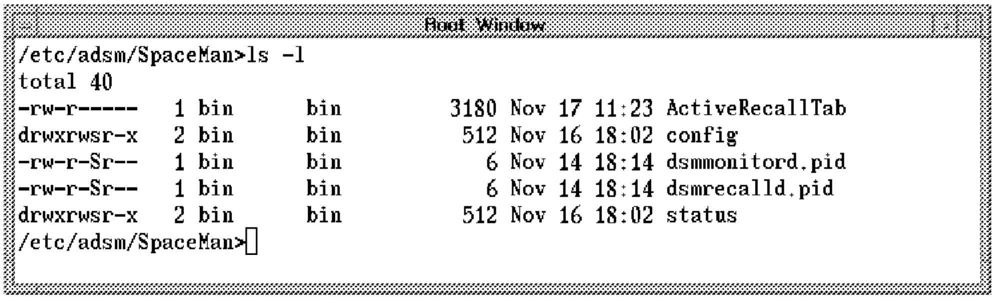
```
 adsmsmext:2:once:/etc/rc.adsmhsm # ADSM SpaceMan
```

The placement of this entry in /etc/inittab is important. It must be after TCP/IP is started, but before NFS is started.

For more information about the HSM startup process refer to 3.3.3, “Setting up Automated Space Management” on page 35.

4.2.2 HSM Control Files

The installation process creates the /etc/adsm/SpaceMan directory, where the control files for HSM are located. This directory contains the subdirectories and files shown in Figure 18.

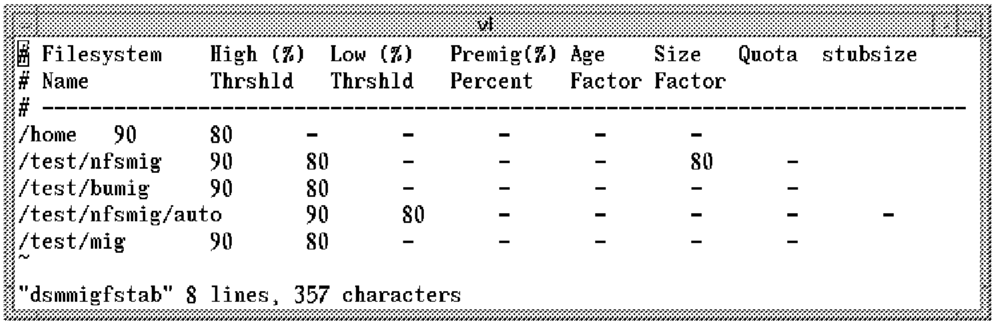


```
/etc/adsm/SpaceMan>ls -l
total 40
-rw-r-----   1 bin      bin        3180 Nov 17 11:23 ActiveRecallTab
drwxrwsr-x   2 bin      bin         512 Nov 16 18:02 config
-rw-r-Sr--   1 bin      bin           6 Nov 14 18:14 dsmmonitord.pid
-rw-r-Sr--   1 bin      bin           6 Nov 14 18:14 dsmrecalld.pid
drwxrwsr-x   2 bin      bin         512 Nov 16 18:02 status
/etc/adsm/SpaceMan>
```

Figure 18. The /etc/adsm/SpaceMan Directory

The ActiveRecallTab file contains information about the active recall processes. Commands such as **dsmrm** and **dsmq** use this file for their tasks. The file is automatically created and updated if a recall process is started or stopped.

The config subdirectory contains the space management file system table (dsmmigfstab shown in Figure 19). If you accidentally delete one of the subdirectories, it is not re-created automatically. You can create the subdirectories manually, but you have to be sure to protect their ownership and access rights.



```
# Filesystem    High (%)  Low (%)   Premig(%) Age    Size   Quota  stubsize
# Name          Thrshld   Thrshld   Percent   Factor Factor
# ---------------------------------------------------------------------------
/home   90      80      -       -       -       -       -
/test/nfsmig    90      80      -       -       -       80      -
/test/bumig     90      80      -       -       -       -       -
/test/nfsmig/auto       90      80      -       -       -       -       -
/test/mig       90      80      -       -       -       -       -
~

"dsmmigfstab" 8 lines, 357 characters
```

Figure 19. Space Management File System Table

There is a line in dsmmigfstab for each file system to which space management is added. Number entries in the space management file system table indicate user-configured values. Dashes indicate that the default value is to be used. For example, the value for the quota is always equal to the size of the current file system.

The order in which the file systems are listed is important. At system start, the file systems are mounted in the order in which they appear in dsmmigfstab. If one file system is nested within the other, the parent file system must be listed before the nested file system. For example, /test/nfsmig must be listed before /test/nfsmig/auto.

If you lose the dsmmigfstab file, all information about the HSM-managed file systems is lost. To recover, create an empty dsmmigfstab file with the following access rights and ownership and then edit the file, adding a line for each HSM-managed file system:

access rights and ownership of dsmmigfstab

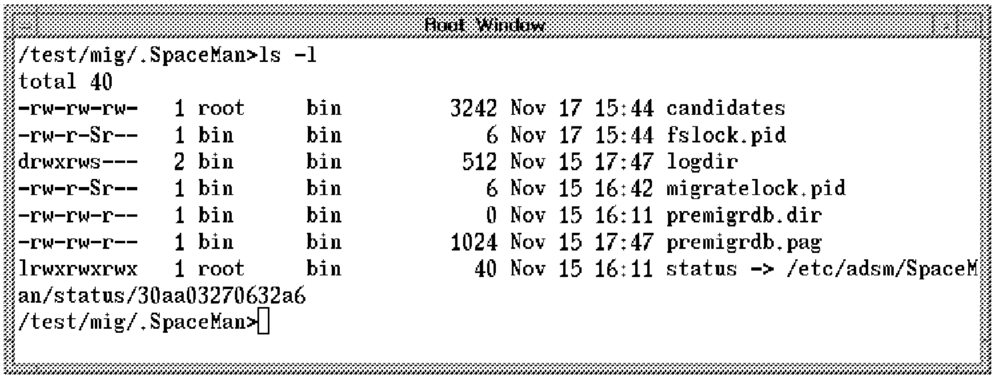
```
-rw-r--r--   1 bin      bin      0 Nov 13 13:46 dsmmigfstab
```

The dsmmonitord.pid and the dsmrecalld.pid files are lock files for the currently running monitor daemon and master recall daemon. These files prevent you from starting the monitor or the master recall daemon twice. If you accidentally delete these files, stop the daemons and start them again. The files will be created automatically. Be careful, however; if you forget to stop the daemons first, you can start the daemons twice, which may render HSM nonoperational.

The status subdirectory contains many small files. Each file belongs to an HSM-managed file system and contains space-management-related statistics. The statistics are used, for example, by the dsmdf command. The status file in the .SpaceMan directory of each HSM-managed file system is a link to one of these files.

4.2.3 .SpaceMan Directory of an HSM Managed File System

In addition to the space management control data for the entire client system, there is some file-system-specific control data. This data is located in the hidden subdirectory, .SpaceMan, in the root directory of each file system (Figure 20).



```
/test/mig/.SpaceMan>ls -l
total 40
-rw-rw-rw-   1 root    bin        3242 Nov 17 15:44 candidates
-rw-r-Sr--   1 bin     bin           6 Nov 17 15:44 fslock.pid
drwxrws---   2 bin     bin         512 Nov 15 17:47 logdir
-rw-r-Sr--   1 bin     bin           6 Nov 15 16:42 migratelock.pid
-rw-rw-r--   1 bin     bin           0 Nov 15 16:11 premigrdb.dir
-rw-rw-r--   1 bin     bin        1024 Nov 15 17:47 premigrdb.pag
lrwxrwxrwx   1 root    bin          40 Nov 15 16:11 status -> /etc/adsm/SpaceM
an/status/30aa03270632a6
/test/mig/.SpaceMan>
```

Figure 20. .SpaceMan Directory of /test/mig File System

The candidates file contains the list of migration candidates. It is created or updated at each reconciliation run. If you lose it, initiate a reconciliation for the affected file system.

The fslock.pid file is a file system lock file that prevents incompatible HSM programs from running concurrently (for example, running two reconcile processes at once). It is also a temporary file that will be re-created automatically. The migratelock.pid file is a lock file that will be created if migration is active for the current file system. These lock files are important in ensuring proper timing of HSM processes that are running simultaneously. If either of these files is lost, you should reboot your AIX system to ensure that the files are re-created properly.

The premigrdb.dir and premigrdb.pag files contain the premigration database of the file system. These files are updated during reconcile, recall, and automatic migration. If you lose either or both of these files, use the shell script described in Appendix D, “Fixfsm Script for Re-creating .SpaceMan Files” on page 113 to recover both files. You must recover both files even if only one is lost. You will lose all premigrated data for this file system, but the migrated data will not be affected.

The logdir subdirectory contains at least three files (1.reserved, 2.reserved, and 3.reserved), each of which occupies one block of disk space. During demand migration, if the file system has no free blocks left, one of these files is used for logging the migration transaction.

If a recall or migration is in progress, the logdir subdirectory also contains some transaction log files. These files are used at mount time to recover the state of files that were being migrated or recalled at the time of system failure. The files have the extension .migrate or .recall.

If during reconciliation some orphaned stub files were found, this directory contains an orphan.stubs file. The file is created automatically by the reconcile process. If you have removed or recovered all orphaned stub files, the orphan.stubs file will be removed during the next reconciliation run.

The status file is a link to one of the central status files in the /etc/adsm/SpaceMan/status directory. This file contains space-management-related statistics for the file system.

If you accidentally lose any files besides candidates, fslock.pid, and migratelock.pid, or if you lose the entire directory, you can use the shell script provided in Appendix D, “Fixfsm Script for Re-creating .SpaceMan Files” on page 113 to recover. If you do not want to use the script, or if all else fails, take the following steps:

1. Remove the .SpaceMan directory
2. Remove the entry for the file system from dsmmigfstab
3. Use the **dsmmigfs** command or the HSM GUI to add space management to the file system
4. Use the **dsmreconcile** command to reconcile the file system

This procedure will create a .SpaceMan directory and all require files. You will lose all premigrated data, but the migrated data will not be affected.

4.3 HSM and AIX Interoperability

This section is written for root users who administer an HSM-managed client host. We show how the following tasks change after HSM is added to the system:

- Unmount, mount, enlarge, check, or delete an HSM-managed JFS
- Add a nested JFS to an HSM-managed JFS
- Change the TCP/IP host name

We explain in detail all NFS-related tasks in Chapter 6, “Migrating NFS File Systems” on page 71 and discuss backup of the entire system in Chapter 7, “Recovery with ADSM and HSM” on page 87.

4.3.1 Unmount, Mount, Enlarge, Check, or Delete an HSM-Managed JFS

In this section we discuss the influence of space management on basic administrative tasks for UNIX file systems.

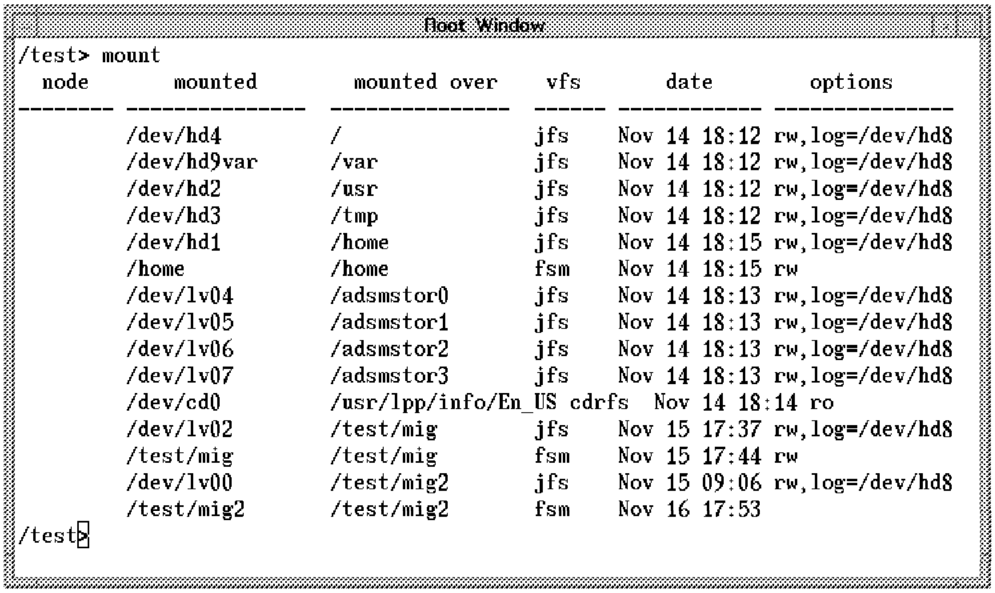
4.3.1.1 Unmount an HSM-Managed JFS

For some low-level file system maintenance tasks it is necessary to unmount a file system temporarily. If you have added space management to that file system, you have some additional tasks to carry out because an FSM is mounted over the file system and a space management process could be in progress. Therefore, first ensure that no process is accessing the file system. Then perform the following steps to unmount the HSM-managed /test/mig2 file system.

1. Deactivate space management for the file system to terminate all active space management processes and prevent new space management activities. Use the HSM GUI or the command line interface. Issue the following command on the command line:

```
dsmmigfs deactivate /test/mig2
```

2. Unmount the FSM. To see which FSMs are mounted over which JFSs, use the **mount** command. Figure 21 shows the output of the command. For each HSM-managed file system, an FSM is mounted over the JFS.



```
/test> mount
  node       mounted        mounted over    vfs       date        options
-------- --------------- --------------- ------ ------------ ---------------
         /dev/hd4        /               jfs    Nov 14 18:12 rw,log=/dev/hd8
         /dev/hd9var     /var            jfs    Nov 14 18:12 rw,log=/dev/hd8
         /dev/hd2        /usr            jfs    Nov 14 18:12 rw,log=/dev/hd8
         /dev/hd3        /tmp            jfs    Nov 14 18:12 rw,log=/dev/hd8
         /dev/hd1        /home           jfs    Nov 14 18:15 rw,log=/dev/hd8
         /home           /home           fsm    Nov 14 18:15 rw
         /dev/lv04       /adsmstor0      jfs    Nov 14 18:13 rw,log=/dev/hd8
         /dev/lv05       /adsmstor1      jfs    Nov 14 18:13 rw,log=/dev/hd8
         /dev/lv06       /adsmstor2      jfs    Nov 14 18:13 rw,log=/dev/hd8
         /dev/lv07       /adsmstor3      jfs    Nov 14 18:13 rw,log=/dev/hd8
         /dev/cd0        /usr/lpp/info/En_US cdrfs  Nov 14 18:14 ro
         /dev/lv02       /test/mig       jfs    Nov 15 17:37 rw,log=/dev/hd8
         /test/mig       /test/mig       fsm    Nov 15 17:44 rw
         /dev/lv00       /test/mig2      jfs    Nov 15 09:06 rw,log=/dev/hd8
         /test/mig2      /test/mig2      fsm    Nov 16 17:53
/test>
```

Figure 21. mount Command Output

To unmount the FSM issue the following command:

```
umount /test/mig2
```

3. Unmount the original JFS by issuing the UNIX **umount** command again:

```
umount /test/mig2
```

4.3.1.2 Mount an HSM-Managed JFS

If you want to mount the temporarily unmounted HSM-managed file system, follow these steps:

1. Mount the FSM:

   ```
   mount -v fsm /test/mig2
   ```

   Do not forget to use the -v option. This command mounts the JFS and the FSM over it.

2. Reactivate space management for the file system:

   ```
   dsmmigfs reactivate /test/mig2
   ```

4.3.1.3 Enlarge an HSM-Managed JFS

When you enlarge an HSM-managed file system, the size changes are visible for HSM at the time of change. If you have not set your own values for the quota, a new quota (equal to the new size of your file system) will be calculated. If you have changed the quota to a fixed value, you have to check whether it will be large enough. If necessary, you have to enlarge the quota.

Keep in mind that enlarging a JFS will give you more space, but the number of inodes available may be limited. When HSM migrates files, it saves space, but the stub file still occupies an inode.

4.3.1.4 Check an HSM-Managed JFS

To test the integrity of the file system use the UNIX **fsck** command. The command does not recall any data.

4.3.1.5 Delete an HSM-Managed JFS

To explain how you can delete an HSM-managed file system we use the /test/mig2 file system that resides on node bering. Remember, before you can delete a file system you have to remove space management from it. When you remove space management from a file system, all migrated data will be recalled, and there may not be enough space for all the data. In the steps that follow we provide a possible workaround for this critical situation.

Note: This procedure deletes all HSM-managed data from the file system. Use this procedure only when you intend to remove the file system.

1. To remove the entire file space from server storage, issue the following command from the ADSM administrative command line:

   ```
   delete filespace bering /test/mig2 type=spacemanaged
   ```

2. To run reconciliation on the client for this file system, use the following command from the HSM client command line:

   ```
   dsmreconcile /test/mig2
   ```

Reconciliation updates all databases with the fact that the migrated data is removed and creates a list of the orphaned stub files in the /test/mig2/.SpaceMan/orphan.stubs file.

3. To remove the orphaned stub files use the del_orphan script shown in Figure 25 on page 60. To run the script issue the following command:

```
del_orphan < /test/mig2/.SpaceMan/orphan.stub
```

4. After you have removed all orphaned stub files, you can remove space management from the file system. Remember, when you remove space management, the FSM will be unmounted from the file system. Therefore before you issue the following command, ensure that no process is accessing any data from the file system:

```
dsmmigfs remove /test/mig2
```

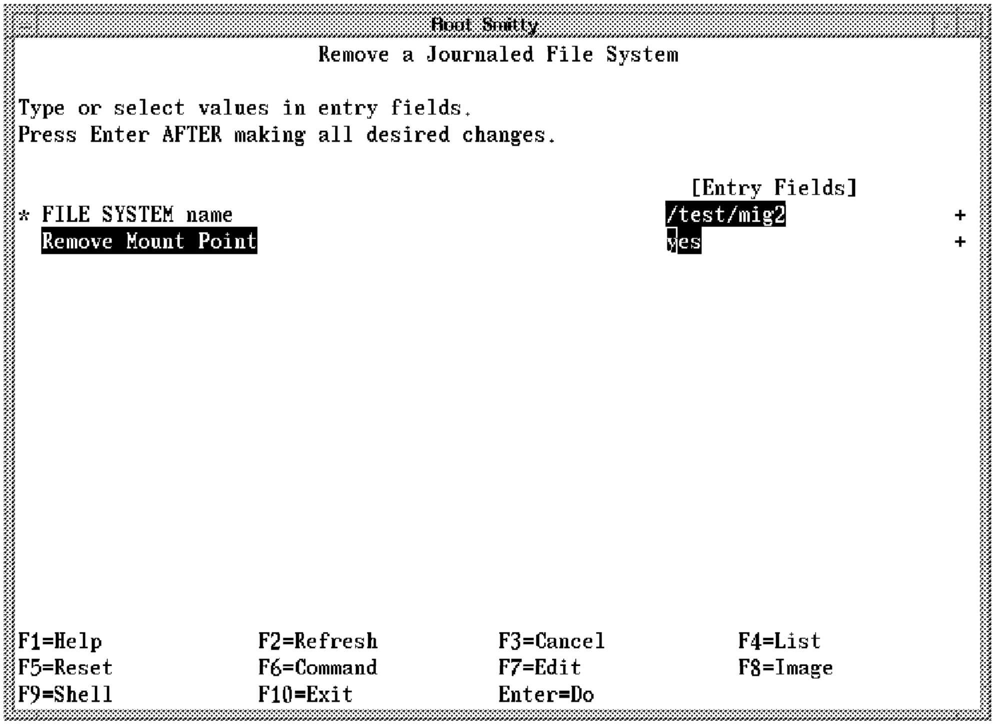
5. Before you can delete the JFS you have to unmount it. Issue the following command:

```
umount /test/mig2
```

6. Now you can delete the file system. Using the AIX System Management Interface Tool (SMIT) issue the following command:

```
smitty rmjfs
```

   On the **Remove a Journaled File System** screen (Figure 22 on page 56) select the file system you want to remove. You also have to specify whether you want to remove the mount point. Press Enter to delete the file system and the logical volume on which it resides.



Root Smitty

```
                        Remove a Journaled File System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                   [Entry Fields]
* FILE SYSTEM name                                 /test/mig2                +
  Remove Mount Point                               yes                       +

F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

Figure 22. SMIT Screen to Remove a JFS

4.3.2 Add a Nested JFS to an HSM-Managed JFS

When you add a nested JFS to an HSM-managed JFS, you can set up the nested file system so that it will be managed by HSM, or you can exclude it from HSM management. We discuss both setups below.

4.3.2.1 Add an HSM-Managed Nested JFS

The setup for adding a nested JFS that will be HSM-managed is the same as the setup for adding space management to a nonnested JFS. See 3.3, “Setting Up the HSM Client” on page 27.

The only thing you have to do is add HSM to the parent file system while the nested JFS is unmounted. If you have already mounted both file systems, you have to unmount the nested JFS before you add HSM to the parent file system.

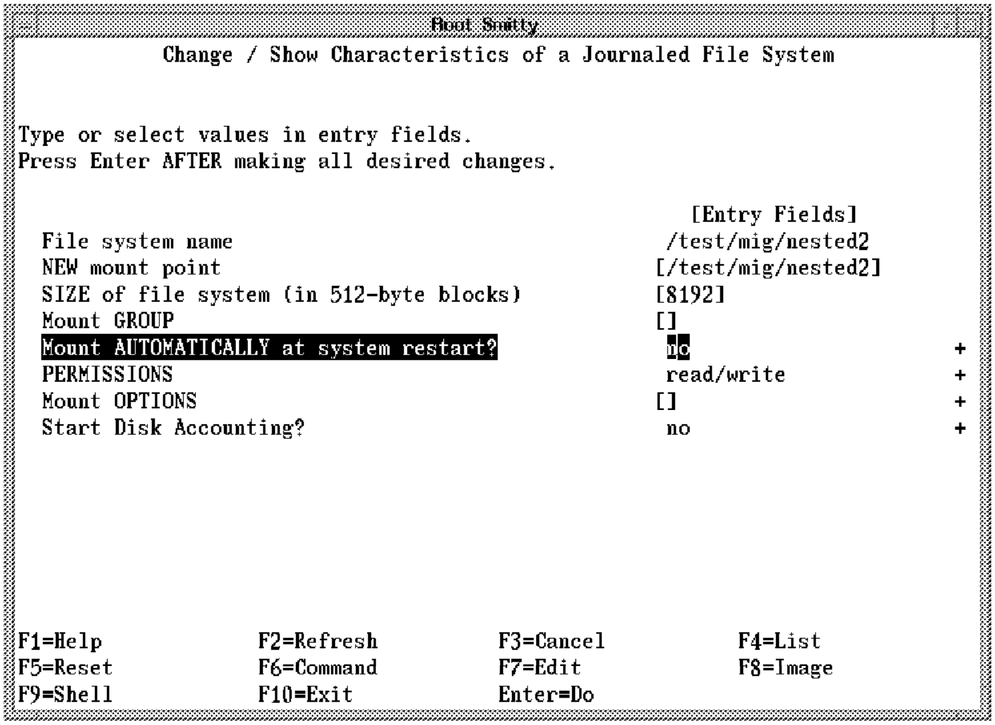
4.3.2.2 Add a Non-HSM-Managed JFS

If the file system has been created and will be mounted automatically at system restart time, follow these steps:

1. Change the characteristics of the file system. Start AIX SMIT with the following command:

   ```
   smitty chjfs
   ```

   First you have to select the file system you will change. In our example the file system is /test/mig/nested2. On the **Change/Show Characteristics of Journaled File System** screen (Figure 23 on page 57) set the **Mount AUTOMATICALLY at system restart?** option to **no**. Press Enter to proceed and leave SMIT.



```
                                Root Smitty
              Change / Show Characteristics of a Journaled File System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                                        [Entry Fields]
  File system name                                    /test/mig/nested2
  NEW mount point                                    [/test/mig/nested2]
  SIZE of file system (in 512-byte blocks)           [8192]
  Mount GROUP                                        []
  Mount AUTOMATICALLY at system restart?              no                     +
  PERMISSIONS                                         read/write             +
  Mount OPTIONS                                      []                      +
  Start Disk Accounting?                              no                     +

F1=Help             F2=Refresh          F3=Cancel           F4=List
F5=Reset            F6=Command          F7=Edit             F8=Image
F9=Shell            F10=Exit            Enter=Do
```

Figure 23. SMIT Screen to Change File System Characteristics

2. Edit the /etc/rc.adsmhsm script. Go to the end of the script and add the following line in the nested JFS section:

entry in /etc/rc.adsmhsm

```
mount /test/mig/nested2
```

The parent file system and the FSM of the parent file system will be mounted before the nested JFS is mounted.

If you are creating a new nested JFS, set the **Mount AUTOMATICALLY at system restart?** option to **no** while defining the JFS to AIX. To add space management to the parent directory, the nested JFS has to be unmounted.

4.3.3 Change the TCP/IP Host Name

Sometimes the TCP/IP host name of a workstation is changed. When this happens, the client node name of the HSM client is also changed. You cannot use the NODENAME option for this client, so the client will not able to recall its data from the server. To resolve this problem the ADSM administrator must perform the following tasks on the ADSM server:

1. Rename the node name on the ADSM server. The ADSM administrator can perform this task by issuing the following command (the old node name was unixcl and the new node name is bering):

```
rename node unixcl bering
```

All data and definitions associated with unixcl are now associated with bering. Be sure that the node name you use for renaming is unique.

2. For security reasons it is a good idea to change the client password. Issue the following command at the server:

   ```
   update node bering f15ch
   ```

   The new password is f15ch.

4.4 Handling Orphaned Stub Files

An orphaned stub file is a stub file for which no corresponding file exists in ADSM server storage. Every time reconciliation runs, the reconcile process compares the stub files in the local file system with the migrated files in ADSM server storage. If an orphaned stub file is found, its name is recorded in an orphan.stubs file in the .SpaceMan directory and the following message is sent:

```
ANS9036W dsmreconcile: migrated file(s) are missing on the server for
10 stub file(s).
Look in the '/test/mig/.SpaceMan/orphan.stubs' for file names.
```

If you set the ERRORPROG option in the client system options file, the stub file message is also sent to the program you specified.

The way in which orphaned stub files are handled depends on how the stub files became orphaned: A media failure could have occurred on an ADSM server storage device that contained migrated data, a user modified the dsm.sys file to point to a different migration server, or the ADSM administrator deleted the files from ADSM server storage.

4.4.1 Media Failure

If a stub file becomes orphaned as a result of a media failure on a storage device used for storing the migrated data in ADSM server storage, here is how to handle it. ADSM provides protection against data loss at the ADSM server through storage pool backup and recovery. If your location is using storage pool backup (and we strongly recommend that you use it), the ADSM administrator can recover the data lost as a result of the media failure. However, if a migrated file cannot be re-created, the end user or root user can restore a backup version of the file, if you created one with the ADSM backup-archive client, and the backup copy was not affected by the media failure.

4.4.2 dsm.sys Modified to Point to a Different Server

If you have modified the MIGRATESERVER option, the DEFAULTSERVER option, or the order of server stanzas in dsm.sys so that the HSM client contacts a server other than the server to which the data was migrated, you can resolve the problem in two ways.

If there is enough free space in the file system follow these steps:

1. Change the options back to the old values.
2. Recall all affected files. Use the shell script shown in Figure 24 on page 59.

```
#!/bin/ksh
#  ==============================================================
#   ADSTAR Distributed Storage Manager (ADSM):
#   Script for automatic recall of all orphaned stub files in a file
#   system
#   platform: AIX
#   usage:  recall_orphan < orphan.stub
#  ==============================================================
#  created by:  Roland Leins
#               IBM Informationssysteme GmbH
#               ST&E Germany
#  last update: 16.11.1995
#  ==============================================================

read stub

while [ ”$stub” != ”” ]
do
  dsmrecall $stub
  read stub
done

exit
```

Figure 24. Script for Recalling All Orphaned Stub Files

To run the shell script issue the following command:

```
recall_orphan < /test/mig2/.SpaceMan/orphan.stub
```

3. Change the options back to their new values. Then you can migrate the files again or keep them resident and wait for a threshold migration.

If there is not enough free space in the file system, resolve the orphaned stub files by exporting the migrated data from the old server and import it to a new server.

4.4.3 Migrated File Deleted

An ADSM administrator can delete from ADSM storage all files within a file space (file system) and all files belonging to one owner from a file space. In these cases, the stub files are no longer valid and should be erased. Use the shell script shown in Figure 25 on page 60.

```
#!/bin/ksh
# ====================================================================
#   ADSTAR Distributed Storage Manager (ADSM):
#   Script for automatic remove of all orphaned stub files in a file
#   system
#   platform: AIX
#   usage:  del_orphan < orphan.stub
# ====================================================================
#  created by:  Roland Leins
#               IBM Informationssysteme GmbH
#               ST&E Germany
#  last update: 16.11.1995
# ====================================================================

read stub

while [ ″$stub″ != ″″ ]
do
  rm $stub
  read stub
done

exit
```

Figure 25. Script for Deleting All Orphaned Stub Files

To run the shell script issue the following command:

```
del_orphan < /test/mig2/.SpaceMan/orphan.stub
```

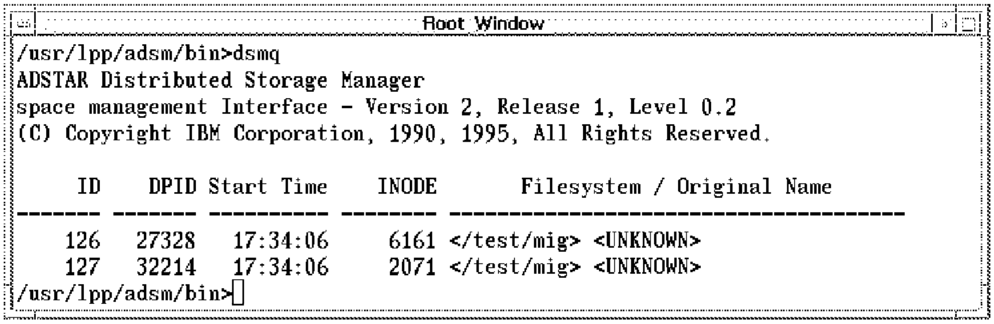
4.5 Maintaining the Space Management Daemons

In this section we explain how to start, stop, or restart the space management daemons.

Note: Stopping and restarting the space management daemons will interrupt all HSM activity on the system. This will have a major impact on your users. It is best to perform these functions at a time when there is little activity on the system.

To stop the space management daemons, perform the following steps.

1. Use the **dsmq** command to determine whether any recall processes are active or queued. The output (Figure 26 on page 61) lists all active or queued recall processes. The ID column lists the HSM internal recall IDs, which you need for step 2.



```
/usr/lpp/adsm/bin>dsmq
ADSTAR Distributed Storage Manager
space management Interface - Version 2, Release 1, Level 0.2
(C) Copyright IBM Corporation, 1990, 1995, All Rights Reserved.

     ID    DPID Start Time    INODE       Filesystem / Original Name
------- ------- ---------- -------- --------------------------------------
    126   27328   17:34:06     6161 </test/mig> <UNKNOWN>
    127   32214   17:34:06     2071 </test/mig> <UNKNOWN>
/usr/lpp/adsm/bin>
```

Figure 26. Using the dsmq Command to List Active or Queued Recall Processes

2. Remove each recall request from the queue. Use the **dsmrm** command, with the recall ID obtained from the **dsmq** command:

   ```
   dsmrm 126
   ```

   This command removes the recall process with ID 126. Repeat this step for all recall processes you found in step 1.

   In step 2 you break a running recall process. **Warn your users that HSM will be temporarily shut down**. While HSM is down, “transparent” recall is not transparent at all! But do not worry about losing data. The stub file for the stopped recall process remains in the local file system, and the file remains in a migrated state. The stub file will be deleted only if the original file is completely recalled.

3. After you have stopped all recall processes, you have to kill the dsmmonitord. Use the following command to obtain the ID of the dsmmonitord process:

   ```
   ps -ef | grep dsmmonitord | grep -v grep | awk '{print $2}'
   ```

   Using the ID of the dsmmonitord process, issue the **kill** command:

   ```
   kill 16632
   ```

4. To verify that all daemons have been killed issue the following commands:

   ```
   ps -ef | grep monitord | grep -v grep
   ps -ef | grep recalld | grep -v grep
   ```

   If all processes have been killed, you should not get a return code. If you get a return code, you have to perform steps 1 through 4 again.

To start (or restart) the space management daemons issue the following commands:

```
dsmmonitord
dsmrecalld
```

Chapter 5. How to Use HSM

In this chapter we describe how to use HSM. Two interfaces are available to the HSM client, the command line interface and the GUI. We use the command line interface to show you how to use some basic HSM functions. We take you step by step through a selective migrate and selective recall of files and show you how to use other HSM commands to view the results. We also show how the file states change and when a file is migrated. To some commands, such as **ls**, the migrated files still appear to be on the local file system.

5.1 HSM Command Line Interface and GUI

Most HSM functions are available through either the command line or the GUI. Some functions are available only through one or the other.

5.1.1 Command Line Only Functions

The following functions are available only through the command line interface:

- ***dsmattr*** - set and display recall modes for migrated files
- ***dsmdu*** - display space usage information for files and directories
- ***dsmmigquery -SORTEDMigrated*** - display all migrated files in the most efficient order for recall
- ***dsmls*** - display all information about the file system except the recall mode
- ***dsmmigundelete*** - re-create deleted stub files
- ***dsmmode*** - set and display execution modes
- ***dsmq*** - display status of recall process
- ***dsmrm*** - remove a recall process from the queue

5.1.2 GUI Only Functions

The following functions are available only through the GUI:

- Display a graphical view of the local disk and server space
- Display a tree view of local file system and files to be selected for migration and recall
- Preview how much space will be saved as you select files
- Automatically refresh file system information (at user defined- intervals)

5.2 Exercises Using HSM

In this section we show you how to carry out a few simple HSM tasks. Once you have HSM installed, you can follow the steps outlined here or simply read this chapter, observing the output in the figures. We present the commands required and explain the results expected in the following scenarios:

- Selective migrate and selective recall
- Threshold migration

5.2.1 Selective migrate and selective recall

If you know that you will not use specific files for an extended period of time, you can selectively migrate them to ADSM storage to free additional space on the local file system. The files you migrate must be at least the minimum size required for migration eligibility.

As a root user can you selectively migrate all files on your workstation that are eligible for selective migration. If you are not a root user, you can selectively migrate any file you own that is eligible for selective migration.

Use selective recall to bring back specific migrated files to your local file system. HSM recalls files in the most efficient, time-saving order. It recalls first all files that are stored on a disk storage device and then all files stored on a tape storage device.

As a root user you can selectively recall any migrated files from your workstation. If you are not a root user, you can selective recall any migrated files you have permission to access. With selective recall, all files are stored on the original file system.

For the following selective migrate and selective recall example we migrate a 16 KB file and a 1 MB file:

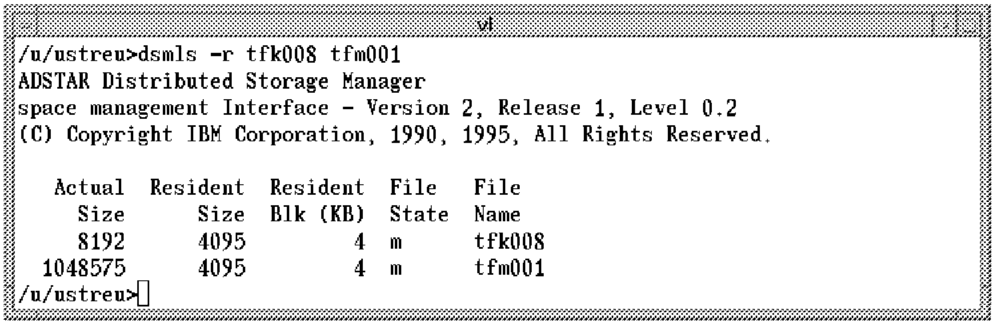
1. Selectively migrate files tfk008 and tfm001, using the **dsmmigrate** command:

```
dsmmigrate /u/ustreu/tfk008  /u/ustreu/tfm001
```

2. Check results of the migration, using the **dsmls** command:

```
dsmls -r /u/ustreu
```

Figure 27 shows the results. Both files are in the migrated state.



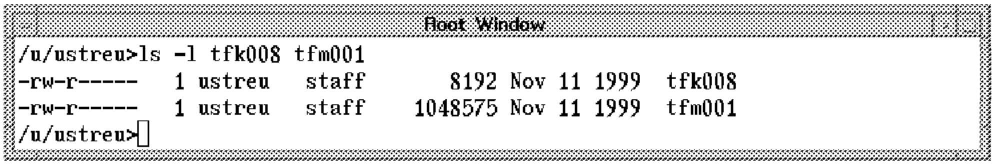
```
/u/ustreu>dsmls -r tfk008 tfm001
ADSTAR Distributed Storage Manager
space management Interface - Version 2, Release 1, Level 0.2
(C) Copyright IBM Corporation, 1990, 1995, All Rights Reserved.

   Actual  Resident  Resident  File   File
     Size      Size  Blk (KB)  State  Name
     8192      4095         4  m      tfk008
  1048575      4095         4  m      tfm001
/u/ustreu>
```

Figure 27. Files after Selective Migrate

Compare Figure 27 with the output (Figure 28 on page 65) of the following **ls** command:

```
ls -l tfk008 tfm001
```

With the **ls** command you cannot distinguish whether the file has been migrated to an ADSM server or resides on your local file system.



```
/u/ustreu>ls -l tfk008 tfm001
-rw-r-----   1 ustreu   staff       8192 Nov 11 1999  tfk008
-rw-r-----   1 ustreu   staff    1048575 Nov 11 1999  tfm001
/u/ustreu>
```

Figure 28. ls Command Output

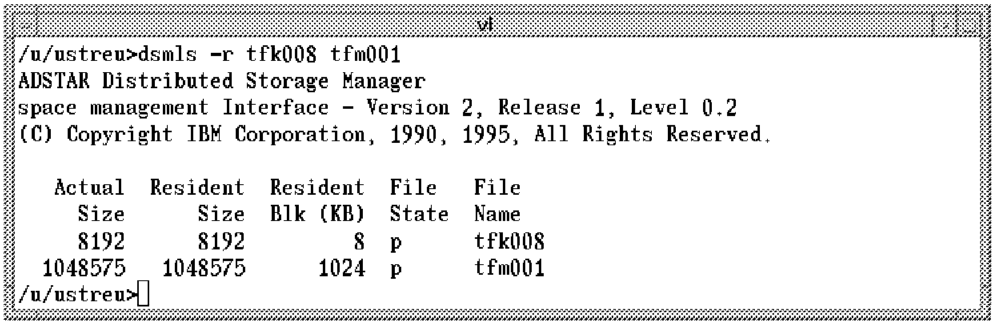
3. Selectively recall the files you have migrated, using the **dsmrecall** command:

```
dsmrecall /u/ustreu/tfk008  /u/ustreu/tfm001
```

4. Check the results of the recall, using the **dsmls** command:

```
dsmls -r tfk008 tfm001
```

The results are shown in Figure 29. Because you did not modify the files after recalling them, the recalled files are in a premigrated state.



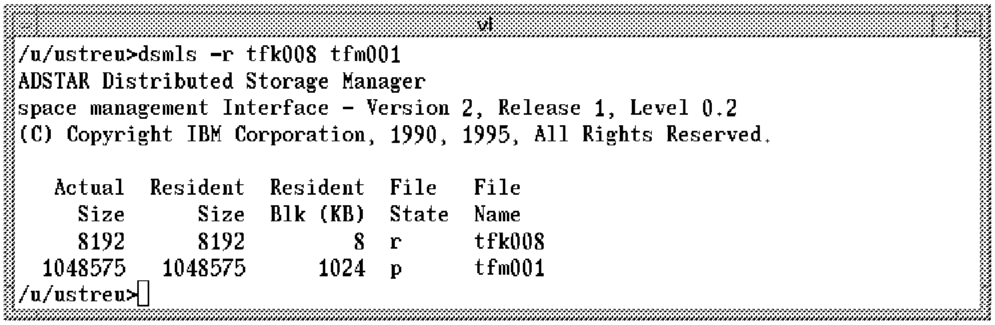
```
/u/ustreu>dsmls -r tfk008 tfm001
ADSTAR Distributed Storage Manager
space management Interface - Version 2, Release 1, Level 0.2
(C) Copyright IBM Corporation, 1990, 1995, All Rights Reserved.

   Actual  Resident  Resident  File   File
     Size      Size  Blk (KB)  State  Name
     8192      8192         8  p      tfk008
  1048575   1048575      1024  p      tfm001
/u/ustreu>
```

Figure 29. Files after Selective Recall

5. Modify one file by using the **touch** command:

```
touch -t 1111111199 tfk008
```

6. Check the results, using the **dsmls** command again. The output is shown in Figure 30. Because you modified tfk008, it is shown as resident, and the old copy of tfk008 that was in ADSM storage will be deleted.



```
/u/ustreu>dsmls -r tfk008 tfm001
ADSTAR Distributed Storage Manager
space management Interface - Version 2, Release 1, Level 0.2
(C) Copyright IBM Corporation, 1990, 1995, All Rights Reserved.

   Actual  Resident  Resident  File   File
     Size      Size  Blk (KB)  State  Name
     8192      8192         8  r      tfk008
  1048575   1048575      1024  p      tfm001
/u/ustreu>
```

Figure 30. Files after Modifying tfk008

5.2.2 Threshold Migration

In this exercise, we cause threshold migration to occur by filling up the /STREU/migtst file system beyond the high threshold. At that point, automatic threshold migration is performed until the low threshold is reached, and premigration will be done down to the premigration percentage.

1. Update the /STREU/migtst file system to have a high threshold of 85%, a low threshold of 75%, and a premigration percentage of 20% (which means it will premigrate down to the 55% level). Use the **dsmmigfs update** command:

```
dsmmigfs update /STREU/migtst -ht=85 -lt=75 -p=20
```

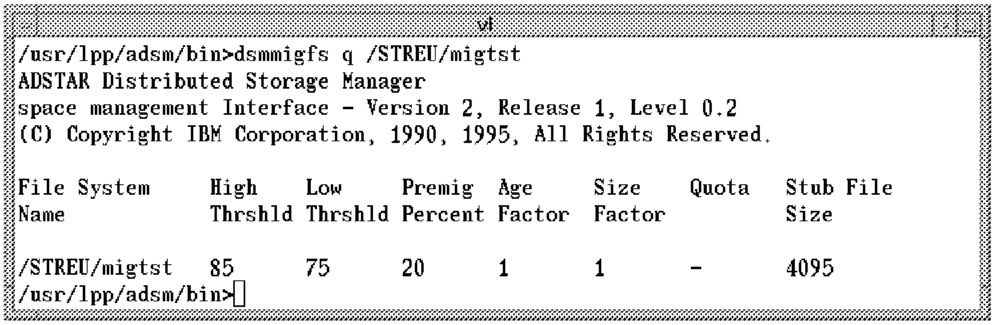
The size of the /STREU/migtst file system is 3908 KB. By applying the threshold percentages, we come up with the following absolute values for this file system:

```
Total file system size:     3908 KB
High threshold (85%):       3322 KB
Low threshold (75%):        2931 KB
Premigration threshold 55%: 2149 KB
```

2. Check the results, using the **dsmmigfs q** command:

```
dsmmigfs q /STREU/migtst
```

Figure 31 shows the space management settings.



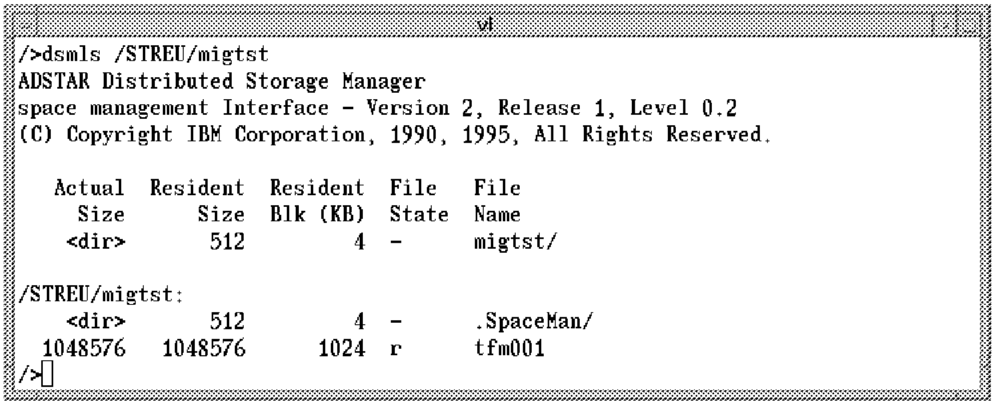
```
/usr/lpp/adsm/bin>dsmmigfs q /STREU/migtst
ADSTAR Distributed Storage Manager
space management Interface - Version 2, Release 1, Level 0.2
(C) Copyright IBM Corporation, 1990, 1995, All Rights Reserved.

File System     High    Low     Premig  Age     Size    Quota   Stub File
Name            Thrshld Thrshld Percent Factor  Factor          Size

/STREU/migtst   85      75      20      1       1       -       4095
/usr/lpp/adsm/bin>
```

Figure 31. Output after Updating the Thresholds

3. Use the **dsmls** command to display information about the file system:

```
dsmls /STREU/migtst
```

Figure 32 on page 67 shows that there is one file in the file system. That file is resident and is 1024 KB. When 1024 KB are added to the 4 KB used by the .Spaceman directory, the total space used in the file system is 1028 KB.



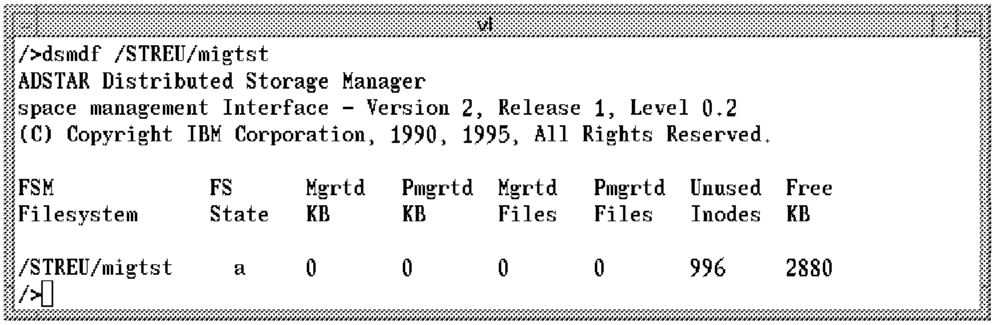
```
/>dsmls /STREU/migtst
ADSTAR Distributed Storage Manager
space management Interface - Version 2, Release 1, Level 0.2
(C) Copyright IBM Corporation, 1990, 1995, All Rights Reserved.

   Actual  Resident  Resident  File   File
     Size      Size  Blk (KB)  State  Name
    <dir>       512         4  -      migtst/

/STREU/migtst:
    <dir>       512         4  -      .SpaceMan/
  1048576   1048576      1024  r      tfm001
/>
```

Figure 32. dsmls /STREU/migtst Command Output

4. Use the **dsmdf** command to show that no files have been migrated:

```
dsmdf /STREU/migtst
```

Figure 33 shows the output of the command.



```
/>dsmdf /STREU/migtst
ADSTAR Distributed Storage Manager
space management Interface - Version 2, Release 1, Level 0.2
(C) Copyright IBM Corporation, 1990, 1995, All Rights Reserved.

FSM             FS      Mgrtd   Pmgrtd  Mgrtd   Pmgrtd  Unused  Free
Filesystem      State   KB      KB      Files   Files   Inodes  KB

/STREU/migtst     a     0       0       0       0       996     2880
/>
```

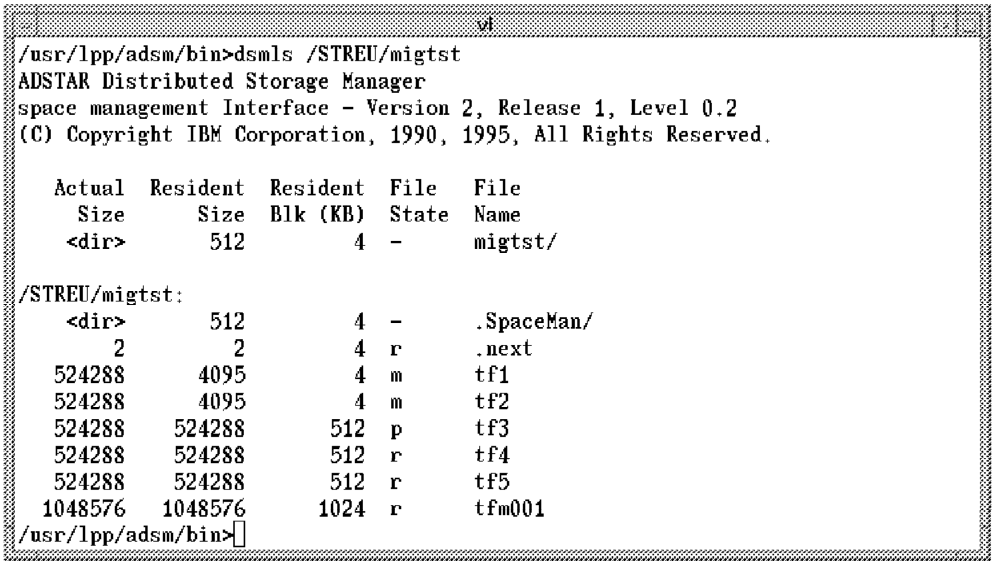
Figure 33. dsmdf /STREU/migtst Command Output

5. To cause threshold migration to occur, you have to exceed the high threshold of 85%, or 3322 KB. Create a 4 KB directory and five 512 KB files, bringing the total used space in the file system to 3592 KB, or 92% full. In this scenario, we set CHECKTHRESHOLDS in dsm.sys to 1 so that HSM checks the thresholds every minute.

6. After threshold migration is finished, check the results by using the **dsmls** command:

```
dsmls /STREU/migtst
```

Figure 34 on page 68 shows the results of the **dsmls** command.



```
/usr/lpp/adsm/bin>dsmls /STREU/migtst
ADSTAR Distributed Storage Manager
space management Interface - Version 2, Release 1, Level 0.2
(C) Copyright IBM Corporation, 1990, 1995, All Rights Reserved.

   Actual  Resident  Resident  File   File
     Size      Size  Blk (KB)  State  Name
    <dir>       512         4  -      migtst/

/STREU/migtst:
    <dir>       512         4  -      .SpaceMan/
        2         2         4  r      .next
   524288      4095         4  m      tf1
   524288      4095         4  m      tf2
   524288    524288       512  p      tf3
   524288    524288       512  r      tf4
   524288    524288       512  r      tf5
  1048576   1048576      1024  r      tfm001
/usr/lpp/adsm/bin>
```

Figure 34. dsmls Output after Threshold Migration

As you can see, files tf1–tf5 and the .next directory were created. Files tf1 and tf2 were migrated, and tf3 was premigrated. The current amount of space occupied in this file system is 2576 KB, which is below the low threshold of 2931 KB (75%). When you subtract 512 KB for premigrated file tf3, you see that there are 2064 KB in resident files and stub files, which is below the premigration threshold of 2149 KB (55%). Figure 35 on page 69 illustrates these calculations.

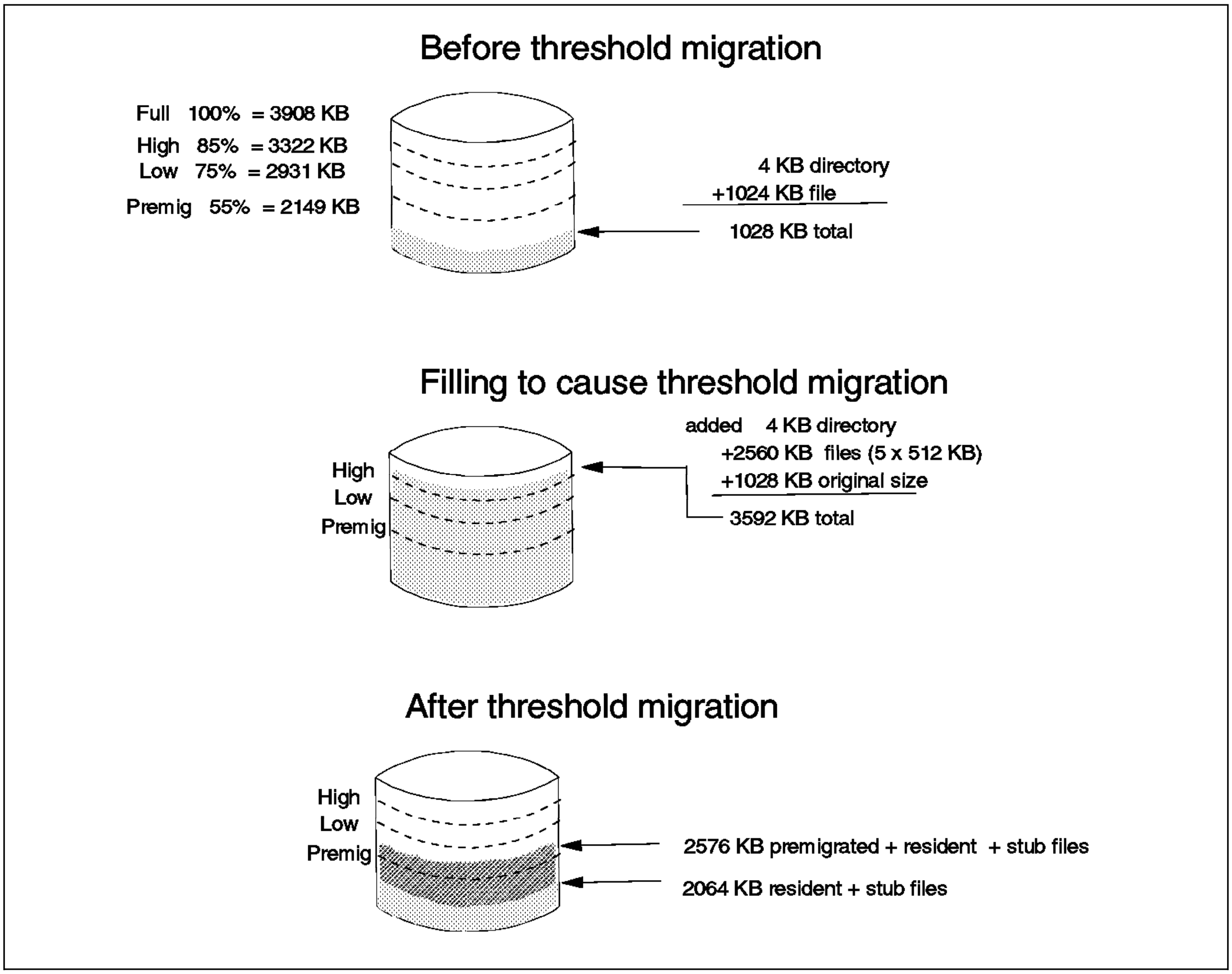


Figure 35. Before, during, and after Threshold Migration

Chapter 6. Migrating NFS File Systems

In this chapter we describe how HSM works in an NFS environment. We provide some NFS setup considerations when using HSM over NFS and present scenarios on how HSM and NFS work together.

6.1 Concept of HSM over NFS

In an NFS environment, the NFS server is the machine that provides the file systems, directories, and other resources for other machines to use. The NFS client is the machine that uses the resources provided by the NFS server.

In an ADSM environment, the ADSM server provides the ability and resources for its clients to back up and restore, archive and retrieve, and migrate and recall their data. The HSM client can migrate its data to the ADSM server to make good use of local storage space. The HSM client also transparently recalls the migrated data when it is accessed.

To put HSM over NFS means that you can have the HSM client and NFS server in one machine (see Figure 36). All NFS clients in the environment can mount to the NFS exported file systems to use NFS server resources. The HSM client can migrate the data from the NFS server to the ADSM server to make good use of the local storage space of the NFS server. When the data is migrated, the NFS clients′ data actually resides in ADSM server storage.

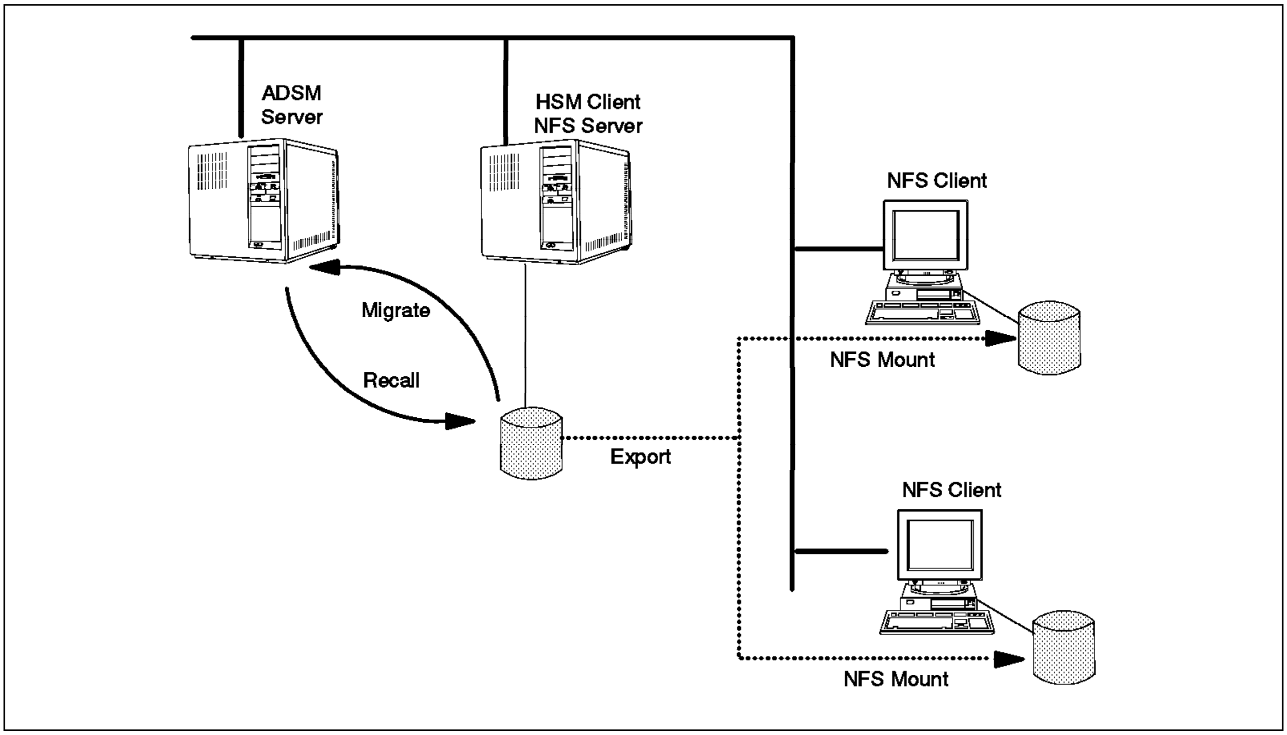


Figure 36. LAN Environment of HSM over NFS

6.2 Setting Up an HSM over NFS Environment

We assume that you are using NFS and want to add HSM. For information about setting up an NFS environment, refer to *Using NFS in a Multivendor Environment*.

6.2.1 Adding Space Management over NFS

You can add space management over NFS before you export any file system. If you already have exported your file systems, however, you must take care when adding space management. Follow these steps:

1. Have all NFS clients unmount the exported file system.

   To see which clients are currently mounting exported file systems, use the following command on the NFS server:

   ```
   showmount -a
   ```

   To unmount the file system, issue the following command on the NFS client:

   ```
   umount /filesystem
   ```

   In our scenario, for a predefined mount or manual mount, unmount the local mount, /u/mntpoint. For an automount, have your NFS client return to the home directory and stop the automount daemon.

   To stop the automount daemon, use smit:

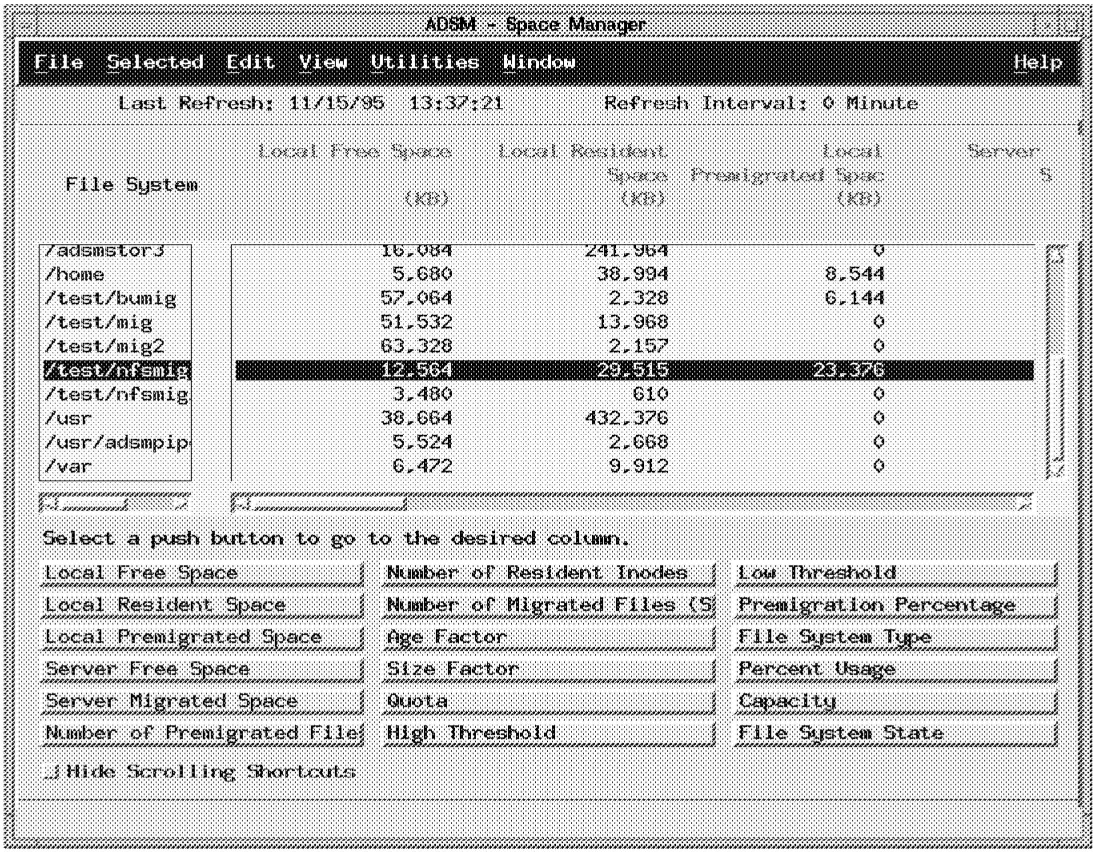
   ```
   smit
     Communication Application and Services
       NFS
         Network File System (NFS)
           Configure NFS on This System
             Stop Automounter
   ```

   Note: Do not use the **kill -9** command to stop the automount daemon because the automount daemon will not clean up before exiting.

   Note: ADSM lets you add HSM to the file system even though it is in use. But HSM does not take full control of the NFS client data. If you neither unmount the NFS client nor stop the automount daemon, you may lose changes you have made to the files in this session. Thus the changes you made to your mounted file system could be lost.

2. Add space management to the file system on the NFS server.

   To add space management to the file system, use either the HSM GUI or the command line. To start the HSM GUI issue the **dsmhsm** command in the `/usr/lpp/adsm/bin` directory. In the **Storage Management** window, click on the **Space Manager** icon to get the **ADSM-Space Manager Window** (Figure 37 on page 73).



Last Refresh: 11/15/95 13:37:21 Refresh Interval: 0 Minute

File System	Local Free Space (KB)	Local Resident Space (KB)	Local Premigrated Spac (KB)	Server S
/adsmstor3	16,084	241,964	0	
/home	5,680	38,994	8,544	
/test/bumig	57,064	2,328	6,144	
/test/mig	51,532	13,968	0	
/test/mig2	63,328	2,157	0	
/test/nfsmig	12,564	29,515	23,376	
/test/nfsmig	3,480	610	0	
/usr	38,664	432,376	0	
/usr/adsmpip	5,524	2,668	0	
/var	6,472	9,912	0	

Select a push button to go to the desired column.

Figure 37. Adding HSM over NFS Server File System

Now select the file system to which you want to add space management. Then click on **Selected** in the action bar and **Add Space Management** in the pull-down menu.

Or, issue the following command:

```
dsmmigfs add /test/nfsmig
```

3. Export the file system on the NFS server.

   To export the file system, issue the following command:

   ```
   exportfs /test/nfsmig
   ```

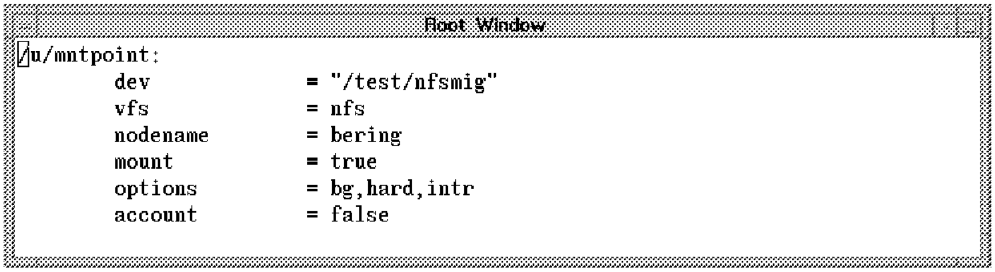
4. Have all NFS clients remount the exported NFS file system.

   For a manual mount, you can specify whichever options you want. For automount, you do not have to remount the file system because the automount daemon will remount it for you when you access the local mount point. And you may have the original options defined in the map file you created. If you have stopped the automount daemon as we suggested, you can start it again.

   For a predefined mount, because you have predefined information in the /etc/filesystems file, you can simply issue the following command:

   ```
   mount /u/mntpoint
   ```

Figure 38 on page 74 shows the NFS client mount point information for our scenario.



```
/u/mntpoint:
        dev             = "/test/nfsmig"
        vfs             = nfs
        nodename        = bering
        mount           = true
        options         = bg,hard,intr
        account         = false
```

Figure 38. NFS Client Mount Point in /etc/filesystems File

6.3 Data Access Issues and Recommendations

In an HSM over NFS environment, you have more system components than HSM without NFS because the NFS clients remotely access HSM-managed data. In this section we describe some checkpoints that you can use when NFS clients cannot access data. We also provide some NFS setup considerations that affect how applications running on NFS clients handle timeouts.

6.3.1 Checkpoints of Data Access Failure

NFS clients get few messages when they cannot access the data they need. Sometimes they cannot even tell whether a data access failure results from poor performance or something worse. In an HSM over NFS environment, when an NFS client cannot access the data it needs, the reasons can be varied. There could be a problem with the network, NFS client, NFS server, HSM client, ADSM server, or ADSM storage pool. Below we suggest some points for you to check to determine the reason for the failure.

6.3.1.1 HSM Client Checkpoints

First and simplest, go back to the NFS server and use **dsmls** to check the status of the file. If it is in a migrated state, try to selectively recall the file. This process can quickly identify whether the failure is in your ADSM or NFS environment.

6.3.1.2 NFS Client Checkpoints

If you can selectively recall the data on the NFS server, check your NFS client. If the NFS server has gone down, obviously the NFS clients cannot get to their mount point. The NFS clients will get the “timed out” message if it is a soft mount, or the “server not responding, still trying” message if it is a hard mount. You can also check the following:

- Your network connection
- A valid local mount point exists and you are accessing the right mount point
- NFS status on the NFS client. Use the following commands to verify that the inetd, portmap, biod, and mountd daemons are running:

```
lssrc -s inetd
lssrc -s portmap
lssrc -s biod
lssrc -s mountd
```

The command output will show such information as subsystem name, group, PID, and status of each daemon.

6.3.1.3 NFS Server Checkpoints

At the NFS client, issue the following command:

```
/usr/bin/rpcinfo -p bering
```

If the NFS server bering is running, you can see a list of programs, versions, and port numbers. If the NFS server does not respond, log in to the NFS server and check that the inetd daemon is running. Use the following command:

```
lssrc -s inetd
```

Ensure that the file system is exported. Use the following command on the NFS server:

```
showmount -e bering
```

The command output will show all file systems that NFS server bering has exported.

6.3.1.4 ADSM Server Checkpoints

When you check the ADSM part of your system, you have to check the network connection, whether TCP/IP is running if you are using TCP/IP, and whether the ADSM server is running. You can view the dsmerror.log file in the /usr/lpp/adsm/bin directory or the specific file system mount point to find some useful information.

Finally, check the status of the ADSM server by having the ADSM administrator use any one of the following ADSM commands:

```
q act
q proc
q sessions
```

6.3.2 ADSM Setup Considerations

In an NFS environment, it is important to set PASSWORDACCESS to GENERATE and TAPEPROMPT to NO in the dsm.sys. See “Client System Options File” on page 28 for a discussion on these and other dsm.sys options.

6.3.3 NFS Setup Considerations

NFS clients get few messages when they cannot access data that has been migrated. You have to consider whether to use hard mount or soft mount. When using soft mount, consider what to specify for a timeout value.

6.3.3.1 Hard Mount and Soft Mount

For an OS/2 NFS client, you can only use the soft-mount option when you mount a file system. For AIX, HP, and Sun NFS clients you can use either the hard-mount or soft-mount option. When the network or server has problems, programs that access hard-mounted remote files fail differently from those that access soft-mounted remote files.

If NFS fails to respond to a hard-mount request, at the NFS client you can get the following message:

```
NFS server hostname not responding, still trying
```

Hard-mounted remote file systems cause programs to hang until the NFS server responds because the NFS client retries the mount request until it succeeds. Use the `-bg` flag with the mount command when performing a hard mount so that, if the server does not respond, the client will retry the mount in the background. Also, use the `-intr` flag with the mount command when performing a hard mount so that you can interrupt the hanging program from the keyboard.

If NFS fails to respond to a soft-mount request, at the NFS client you can get the following message:

```
Connection timed out
```

Soft-mounted remote file systems return an error after trying unsuccessfully for a while. Unfortunately, many programs do not check return conditions on file system operations, so you do not see this error message when accessing soft-mounted files. However, this NFS error message will print on the NFS server console.

If the NFS client uses hard mount, when you access data that is already migrated and the storage pool in the ADSM server is not available for some reason, the NFS client will hang until the storage pool becomes available and the NFS client can get its data.

If the NFS client uses soft mount, when you access data that is already migrated, the soft mount could time out, allowing the application on the NFS client to access the stub file. The application can then overwrite the stub file, preventing future access to the real migrated file that is on the ADSM server. If the stub file is not re-created before the migrated copy expires (or the older version of the file is restored before it expires), the data will be lost.

6.3.3.2 NFS Timeout

If you use soft mount to mount a remote file system, usually you can use the default NFS timeout value, and it works well. In some cases, when your ADSM or NFS server is very busy, or the ADSM server has a slow device as its storage device, or you have a busy network, you may have to change the default timeout value to avoid NFS timeout when accessing data from NFS clients.

The AIX NFS client has two NFS client timeout parameters:

- -o n

  Sets the NFS timeout to the tenths of a second specified by n. Use this variable to avoid situations where the server or network load can cause inadequate response time. The default value is 7.

- -r n

  Sets the number of NFS retransmissions to the number specified by n. The default value is 3.

To reset these values issue the following command:

```
chnfsmnt -f /u/mntpoint -d /test/nfsmig -h bering -o 10 -r 5
```

The OS/2 NFS client has two timeout parameters when you start NFS:

- -tn

  Sets the timeout value in seconds for a remote procedure call (RPC) request. The default value is 1.

- -rn

  Sets the number of RPC retries that the OS/2 NFS client sends to the server before ending the access attempt. The default value is 5.

To reset these values issue the following command:

```
nfsstart -t6 -r12
```

Be careful when you set these parameters and ensure that your network works well with the value you set. A high value can lead to long data access time when a packet drops from the network. Not only that, using a high value for these parameters can occupy more NFS server resources, and additional drops may occur.

6.4 Performance Recommendations

Here are some recommendations that can affect the performance of your HSM system in an NFS environment. We look at:

- Setting the recall mode
- Setting the number of recall daemons
- Securing NFS
- Setting the MTU size

6.4.1 Setting the Recall Mode

A recall mode of migrate-on-close or read-without-recall should not be set for a file that resides on a file system which has been exported by an NFS server. Because NFS opens and closes a file many time times when it is accessed by an NFS client, performance can be severely affected.

Understand how HSM handles recall modes with NFS. Even if you set the recall mode to migrate-on-close or read-without-recall on an exported NFS file system, ADSM is smart enough to identify who is accessing the data. If an HSM client is accessing that file, the recall mode you set will take effect, and the recall mode behaves just as you set it. If, however, an NFS client is accessing that file, to avoid performance problems, ADSM automatically changes the recall mode for that file to normal. The file will not be in a migrated state after the NFS client closes it. If the NFS client does not change the file, it is in a premigrated state. If the NFS client changes the file, it is in a resident state.

6.4.2 Setting the Number of Recall Daemons

A recall daemon is a program that recalls a migrated file from an ADSM storage pool to an HSM client. A recall daemon can recall only one file at a time. You can have more than one recall daemon running at a time. If all recall daemons are busy, another file cannot be recalled until a recall daemon is available.

Because the HSM client also acts as an NFS server, some of your NFS client′s data may already have migrated to the ADSM server. When an NFS client accesses its migrated data, it needs a recall daemon. For performance reasons, you may need more recall daemons than usual to run at the same time in order for your NFS clients to retrieve their data.

To set the minimum and maximum number of recall daemons that can run at one time, use the MINRECALLDAEMONS and MAXRECALLDAEMONS options in dsm.sys. The values range from 2 to 99. The default is 20. Recall daemons can be started automatically.

6.4.3 Securing NFS

Secure NFS affects system performance in two ways. In the initial RPC connection, both the client and server have to calculate the common key, which takes about 2 sec. Nevertheless, once the key is calculated, it is stored in server cache and does not have to be calculated for every initial RPC connection. The Data Encryption Standard (DES) encryption operations have a more considerable impact on system performance. Each RPC transaction requires four DES operations:

1. The client encrypts the request time stamp.
2. The server decrypts the time stamp.
3. The server encrypts the reply time stamp.
4. The client decrypts the reply time stamp.

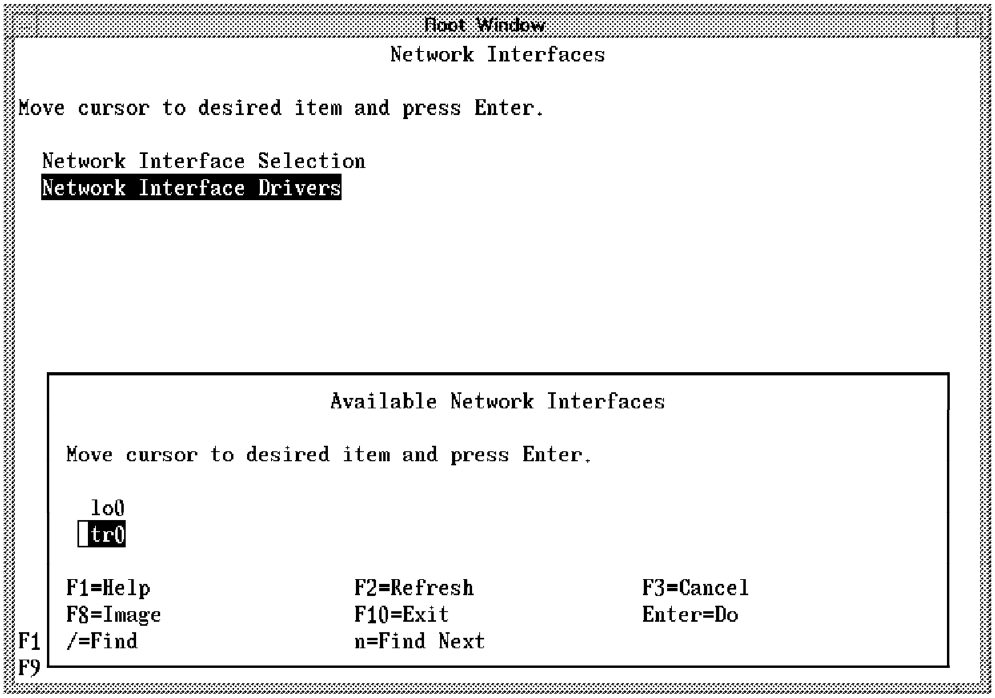
You must weigh the benefits of increased security against performance. If your environment requires secure NFS, you must be aware that HSM requires end users to have a higher toleration of slow response times for access to their data.

6.4.4 Setting the MTU Size

Generally, when you move large amounts of data through a network in batch, a bigger maximum transmission unit (MTU) size can reduce system processing time and significantly improve read/write operations. The value you set for the MTU size depends on your network environment and some other settings such as transmission queue size. You can tune the MTU size to fit your system and get better system performance.

To set the MTU size, you can use SMIT:

```
smit
  Communications Applications and Services
    TCP/IP
      Further Configuration
        Network Interfaces (see Figure 39)
          Network Interface Drivers
```



```
Root Window
                          Network Interfaces

Move cursor to desired item and press Enter.

  Network Interface Selection
  Network Interface Drivers

          Available Network Interfaces

   Move cursor to desired item and press Enter.

     lo0
    tr0

   F1=Help             F2=Refresh          F3=Cancel
   F8=Image            F10=Exit            Enter=Do
F1 /=Find              n=Find Next
F9
```

Figure 39. Using SMIT to Set MTU Size

From the list of **Available Network Interfaces** click on the interface you are using and then change the **Maximum IP Packet Size**. The ranges of values you can use to set the **Maximum IP Packet Size** for different network interface drivers are:

Ethernet:	60 through 1500
802.3:	60 through 1492
Token-Ring(4Mb):	60 through 4056
Token-Ring(16Mb):	60 through 17792

For more information about NFS performance tuning, refer to *AIX Version 3.2 and 4.1 Performance Monitoring and Tuning Guide*.

6.5 Migration and Recall Scenarios

In this section we describe some migration and recall scenarios in an HSM over NFS environment. Our environment is illustrated in Figure 40. We have an AIX machine to act as ADSM server. We have the HSM client and NFS server on another AIX machine. We have another AIX machine and one OS/2 machine as the NFS clients. The host names of the machines are as follows:

Host Name	Function
u03aix	AIX ADSM server
bering	AIX HSM client, NFS server
severn	AIX NFS client
ungava	OS/2 NFS client

The file system exported by the NFS server bering is /test/nfsmig.
The local mount point for the NFS client severn is /u/mntpoint
The local mount point for the NFS client ungava is drive Z.

File system /test/nfsmig is managed by HSM to provide space management function. On the NFS clients, we use basic commands and applications to see how HSM transparently recalls data for NFS clients. xv is an application on AIX that we use to create and retrieve image files. *Freelance Graphics* is an application on OS/2 that we use to create and retrieve image presentations.

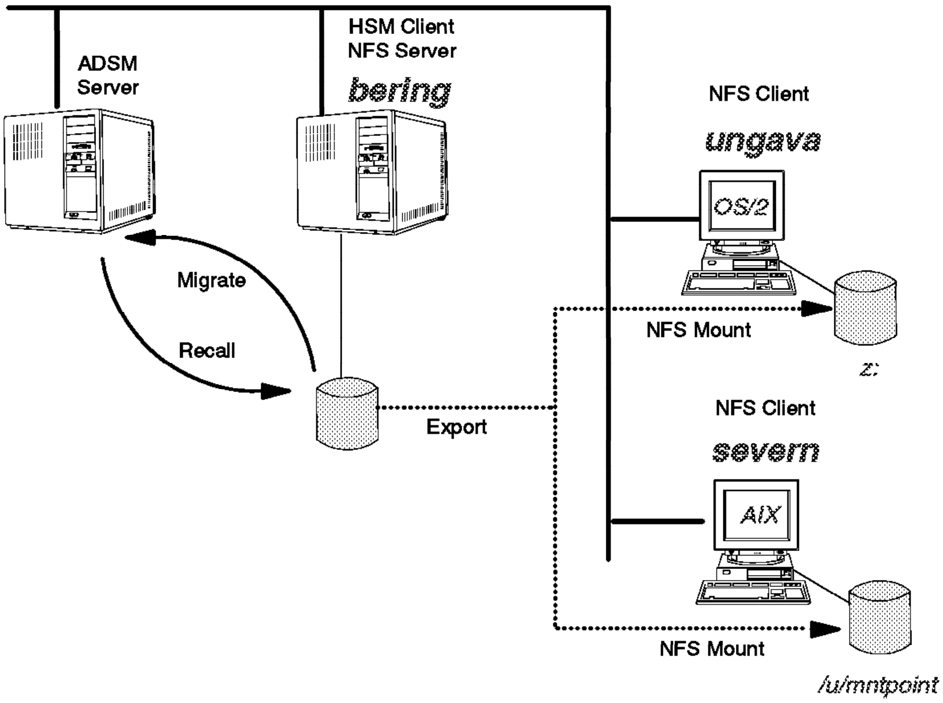


Figure 40. Environment for HSM over NFS Scenarios

6.5.1 Selective Migration of AIX and OS/2 NFS Client Data

We selectively migrate AIX and OS/2 NFS client data to the ADSM server, following the steps listed below. The size of the files that have to be migrated must be bigger than both the size you set for stub file plus 1 and the block size of the exported NFS file system.

1. Create a text file, txtos2, using the E editor on OS/2 NFS client ungava, drive z:

   Note: If you want to share text files between AIX users and the OS/2 NFS client, use the -c option when you mount the OS/2 machine to the AIX NFS server for conversion of “line-feed” to “carriage-return and line-feed.” Otherwise, do not use the -c option.

2. Create an image file, imgos2.pre, using Freelance Graphics on OS/2 NFS client ungava, drive z:

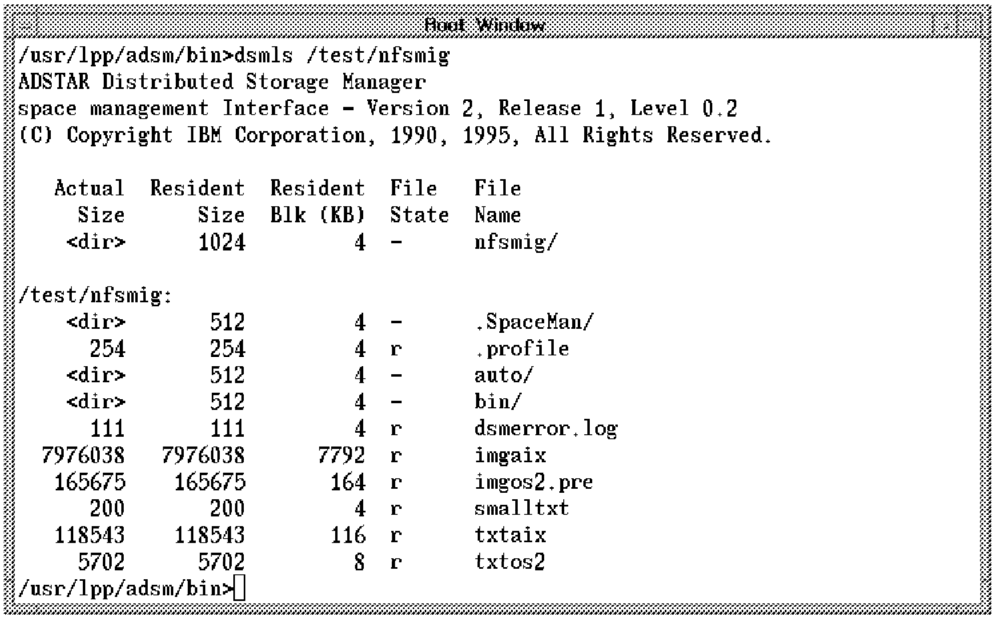
3. Create a text file, txtaix, using the vi editor on AIX NFS client severn in the /u/mntpoint directory.

4. Create an image file, imgaix, using xv on AIX NFS client severn in the /u/mntpoint directory. The image file must be more than 7 MB.

5. On NFS server bering, check the status of the files, using the following command:

   ```
   dsmls /test/nfsmig
   ```

   Figure 41 shows the output of the command. The NFS clients′ data resides on the NFS server exported file system with the migration status of resident.



```
/usr/lpp/adsm/bin>dsmls /test/nfsmig
ADSTAR Distributed Storage Manager
space management Interface - Version 2, Release 1, Level 0.2
(C) Copyright IBM Corporation, 1990, 1995, All Rights Reserved.

   Actual  Resident  Resident  File   File
     Size      Size  Blk (KB)  State  Name
    <dir>      1024         4  -      nfsmig/

/test/nfsmig:
    <dir>       512         4  -      .SpaceMan/
      254       254         4  r      .profile
    <dir>       512         4  -      auto/
    <dir>       512         4  -      bin/
      111       111         4  r      dsmerror.log
  7976038   7976038      7792  r      imgaix
   165675    165675       164  r      imgos2.pre
      200       200         4  r      smalltxt
   118543    118543       116  r      txtaix
     5702      5702         8  r      txtos2
/usr/lpp/adsm/bin>
```

Figure 41. Check Status of NFS Client Files before Migration

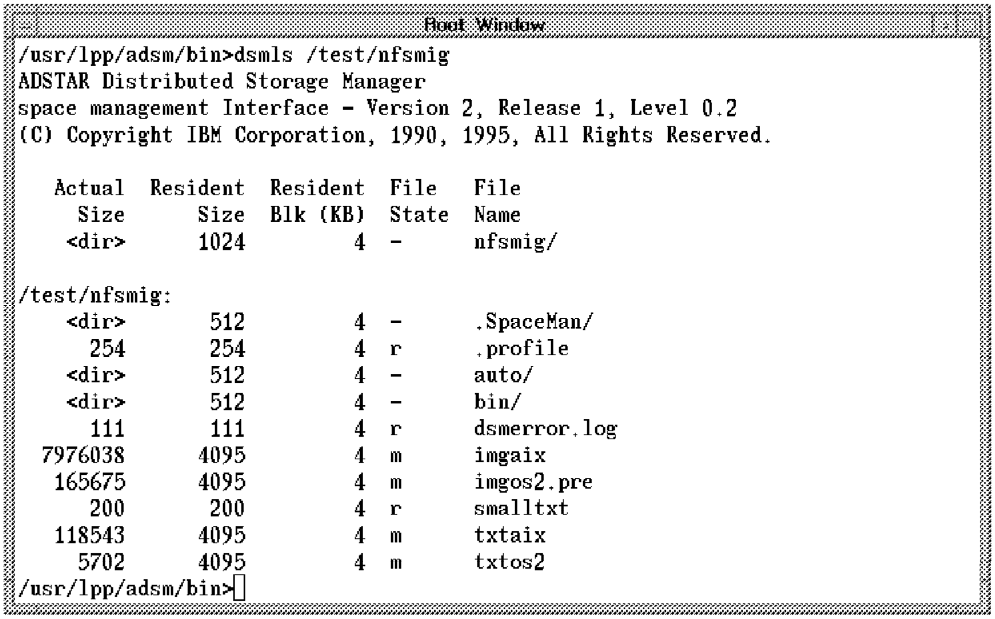
6. On NFS server bering, migrate the files in /test/nfsmig to the ADSM server, using the following command:

   ```
   dsmmigrate -D /test/nfsmig/txt* /test/nfsmig/img*
   ```

7. On NFS server bering, recheck the status of the files, using the following command:

```
dsmls /test/nfsmig
```

Figure 42 shows the output of the command. The AIX and OS/2 NFS client data has been migrated to the ADSM server.



```
/usr/lpp/adsm/bin>dsmls /test/nfsmig
ADSTAR Distributed Storage Manager
space management Interface - Version 2, Release 1, Level 0.2
(C) Copyright IBM Corporation, 1990, 1995, All Rights Reserved.

   Actual  Resident  Resident  File   File
     Size      Size  Blk (KB)  State  Name
    <dir>      1024         4  -      nfsmig/

/test/nfsmig:
    <dir>       512         4  -      .SpaceMan/
      254       254         4  r      .profile
    <dir>       512         4  -      auto/
    <dir>       512         4  -      bin/
      111       111         4  r      dsmerror.log
  7976038      4095         4  m      imgaix
   165675      4095         4  m      imgos2.pre
      200       200         4  r      smalltxt
   118543      4095         4  m      txtaix
     5702      4095         4  m      txtos2
/usr/lpp/adsm/bin>
```

Figure 42. Check Status of NFS Client Files after Migration

You can use the **ls** command on AIX NFS client severn or the **dir** command on OS/2 NFS client ungava to list the files without having to recall the data.

6.5.2 Transparent Recall for NFS Clients

In our scenarios, both AIX and OS/2 NFS clients can transparently access their data from the ADSM server storage pool. To have HSM transparently recall the data for NFS clients, follow these steps:

1. On NFS server bering, use **dsmls** to check the file status of NFS clients to be "migrated."

2. Access the OS/2 NFS client text file.

   On OS/2 NFS client ungava, drive z: issue the following command:

   ```
   e txtos2
   ```

   HSM automatically recalls data for the OS/2 NFS client. You can access the file and continue editing it.

3. Access the OS/2 NFS client image file.

   On OS/2 NFS client ungava, start the Freelance Graphics application and open file `z:\imgos2.pre`. You can access the Freelance Graphics file after HSM recalls the data.

   Note: Although an ADSM recall is taking place, all you will notice is a longer wait time for HSM to recall the data.

4. Access the AIX NFS client text file.

   On AIX NFS client severn, issue the following command:

   ```
   vi /u/mntpoint/txtaix
   ```

5. Access the AIX NFS client image file.

   On AIX NFS client severn, start the xv application and load file /u/mntpoint/imgaix. In our configuration, the ADSM for AIX V2 server used 8 mm tape. With an 8 mm tape as the storage pool and basic token ring network, it will take more than 2 min for the NFS client to get the file.

6. At any time during the transparent recall process on NFS server bering, you can use the **dsmls** command to see whether the file has been changed to premigrated status, if you do not modify the file from NFS client, or resident status, if you modify and save the file.

Data retrieval time can affect transparent recall for NFS clients. As you can see from the above scenario, it takes about 2 min to recall a 7 MB file from the ADSM tape storage pool to the HSM client and then send it to the NFS client. The end user must be patient when accessing a big file and keep in mind that the data may already be in the ADSM storage pool, especially if the storage pool is a removable medium such as tape and the tape is not in the drive and you have to mount it manually or have the tape library mount it within the NFS timeout limit.

6.5.3 Hard Mount and Soft Mount

The AIX, HP, and Sun NFS clients provide the option of hard mounting or soft mounting when you mount to a remote file system. The default for AIX is hard mount. The OS/2 NFS client supports only soft mount.

Hard mount and soft mount behave differently when the NFS client cannot get its data from the NFS server.

In our scenarios we migrate the data to tape and then ignore the tape mount request in order to force a timeout. In this way we can see the results of working with NFS hard-mount and soft-mount.

6.5.3.1 Accessing OS/2 NFS Client Data

For a soft-mount, each application handles a timeout error from NFS differently. As you can see below, the type and editor commands and the Freelance Graphics application each return different error messages from the same NFS timeout.

1. On OS/2 NFS client ungava, issue this command:

   ```
   type txtos2
   ```

   On the NFS Control console, you will see many messages like this:

   ```
   NFS-Biod x : RPC_TIMED_OUT
   RPC_TIMED_OUT >>>RETRY!<<<
   ```

   On OS/2 NFS client ungava, you get the following message:

```
The network request is not supported
```

So the system hangs until the NFS client times out; then the system returns to its normal stage.

2. On OS/2 NFS client ungava, issue the following command:

```
e txtos2
```

After the timeout, you get the following message:

```
This program is not responding to system requests.
Select ENTER to end it. Data will not be saved.
```

This message is due to the internal design of the e editor and OS/2 operating system.

3. On OS/2 client ungava, start the Freelance Graphics application and open the z:\imgos2.pre file. The Freelance Graphics application hangs until NFS times out. After the timeout, you get the following message:

```
Can not open the file, it is not a Freelance file
```

The Freelance Graphics application can read the stub file and some leading data but cannot access all of the data in the file.

6.5.3.2 Accessing AIX NFS Client Data

In this scenario, we access a migrated file with soft mount and hard mount to show the different results that occur.

1. For AIX NFS client severn, we keep the predefined default mount option, which is hard mount, and then use vi to edit the txtaix file.

   The vi session hangs until the tape is inserted in the drive. Then HSM recalls the data for the NFS client. We can also interrupt the process from the keyboard because we use the -intr option when mounting the remote file system. When using a hard mount, be sure to use the -intr option.

2. Using the HSM client on NFS server bering, selectively migrate the txtaix file.

3. On AIX NFS client severn, unmount /test/nfsmig, mount it again with the -o soft option and vi the file:

```
umount /u/mntpoint
mount -o soft bering:/test/nfsmig /u/mntpoint
vi /u/mntpoint/txtaix
```

After the NFS timeout, vi opens a new file with the same file name without giving any message. If the ADSM administrator sees the tape mount request and mounts the tape for the NFS server, the recall of the original file is completed because the recall is still running. At the NFS client, you do not know what has happened except the unexpected long waiting time before the NFS timeout. If you save the new file and quit vi, you get this message:

```
"txtaix" NFS getattr failed for server bering: RPC: Unable to receive,
{new file}
```

The file has already been changed, however. Because it is a new file, you cannot recall it. If you try selective recall at the NFS server, you get the following message:

```
No migrated files matching 'txtaix' were found.
```

The original stub file is damaged. You have to recover your file. A simple way is to use ADSM restore.

Note: For some applications, NFS soft mount may be dangerous to your data.

6.5.4 Not Enough Local Space during Recall

In this scenario, we show you how HSM protects local space from an out-of-space-condition. We create an out-of-space condition on the exported NFS server file system, /test/nfsmig. Then on the NFS client we try to access the /test/nfsmig/imgaix file on the NFS server, but it already has been migrated to the ADSM server. Thus an out-of-space condition occurs.

At this time, HSM automatically starts demand migration to migrate some files to the ADSM server. Space becomes available on the exported NFS server file system. The application that retrieves the /test/nfsmig/imgaix file can now continue to process.

You can expect a longer data access time than usual because ADSM is dealing with an out-of-space condition. But your application on the NFS client can get the data and continue processing.

Chapter 7. Recovery with ADSM and HSM

Backing up your files protects against accidental or intentional corruption or loss of your data. You should maintain current backup versions of all of your important files regardless of whether they are resident, migrated, or premigrated.

Using the ADSM backup-archive client, you can back up and restore migrated and premigrated files in the same way that you back up and restore files that are not migrated.

In addition, if stub files are accidentally deleted from a local file system, or if you lose one or more local file systems or the entire system, you can re-create the stub files for migrated files instead of restoring backup versions of the files. You can also re-create stub files for premigrated files if the original copies of the files are accidentally deleted from local file systems.

This chapter discusses the following topics:

- Using one ADSM server for backup and migration
- Using separate ADSM servers for backup and migration
- Recovery checklist
- Recovering data when using separate servers for backup and migration
- Recovery for an entire AIX system containing migrated files

7.1 Using One ADSM Server for Backup and Migration

When you are using the same ADSM server for backup and migration, recovering a single file or group of files is a simple matter of using the backup-archive client. When you specify the RESTOREMIGSTATE parameter on the **dsmc restore** command, ADSM restores the file to a migrated state. Support for the RESTOREMIGSTATE parameter was made available in PTF IP20673.

7.2 Using Separate ADSM Servers for Backup and Migration

When you use separate ADSM servers for backup and migration, RESTOREMIGSTATE does not apply, so you must either restore the files to a resident state or use the **dsmmigundelete** command.

For a single file or a small group of files, using the restore function of the backup-archive client is the recommended approach for recovery. Even if the lost or corrupted file has been migrated, we recommend this approach for two reasons. First of all, the **dsmmigundelete** command works only at a file system granularity. It is not possible to run the **dsmmigundelete** command for just one file or a directory. Second, before restoring the stub files for a file system, it is important to know whether or not reconciliation has run since the file system was lost or corrupted. If reconciliation has been run, specify the **dsmmigundelete** command for the file system with the EXPIRING parameter. This will re-create stub files for migrated files and premigrated files even if they have been marked for expiration.

Whether or not to use the EXPIRING parameter depends on when reconcile has run. Figure 43 on page 88 shows the timing of reconcile. An HSM client has a file system called /test/mig2 that contains three migrated files. At noon, the user intentionally deletes file3. Actually, it is the stub file that is deleted. At 3 p.m., reconcile runs, and file3 is marked for expiration in the ADSM server database. At 5 p.m., the user accidentally deletes file1 and file2.

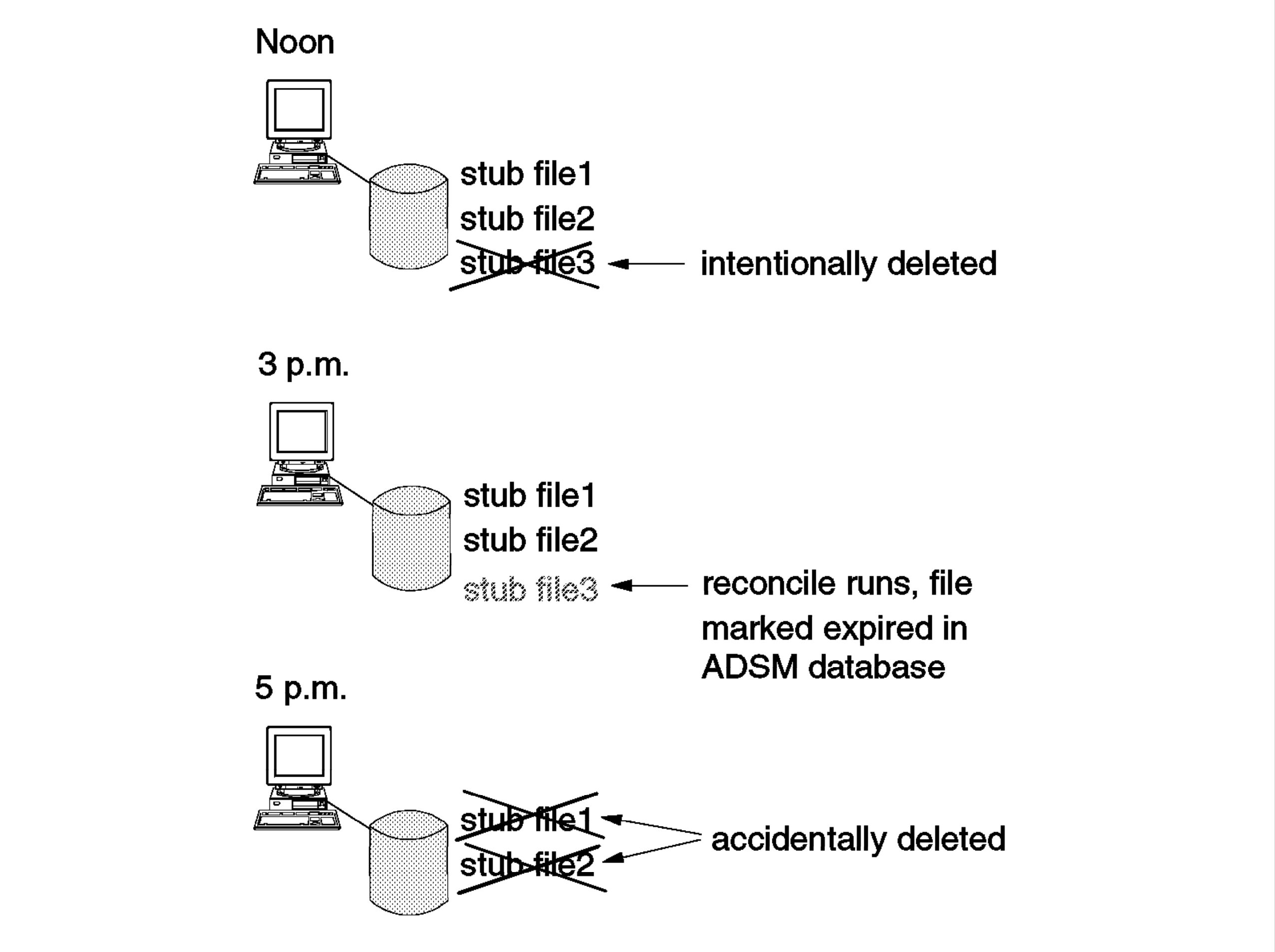


Figure 43. Timing of Reconcile and Deleted Stub Files

Figure 44 shows what happens when the **dsmmigundelete** command is specified for this file system without the EXPIRING parameter, namely, the stub files are re-created for file1 and file2 only.

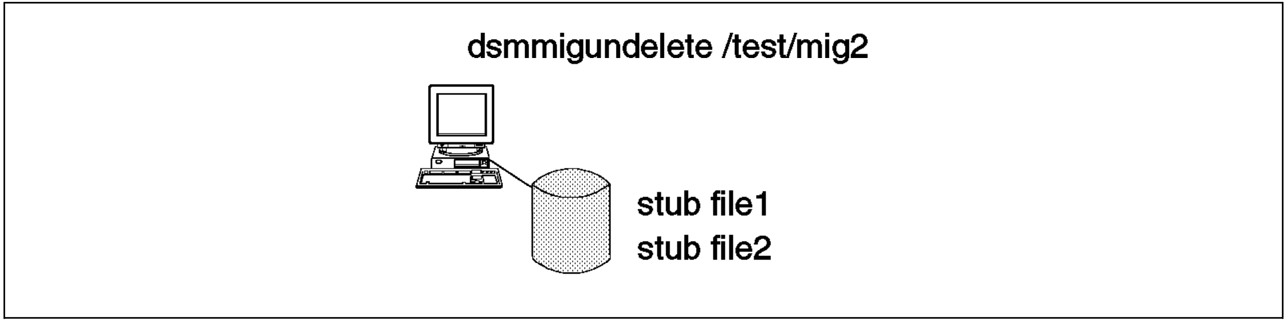


Figure 44. Dsmmigundelete without the EXPIRING Parameter

If the **dsmmigundelete** command is specified for this file system with the EXPIRING parameter, stub files are re-created for file1, file2, and file3 (see Figure 45 on page 89). A stub file is re-created for file3 because of the EXPIRING parameter even though the user intentionally deleted the file. The user then has to redelete the file.

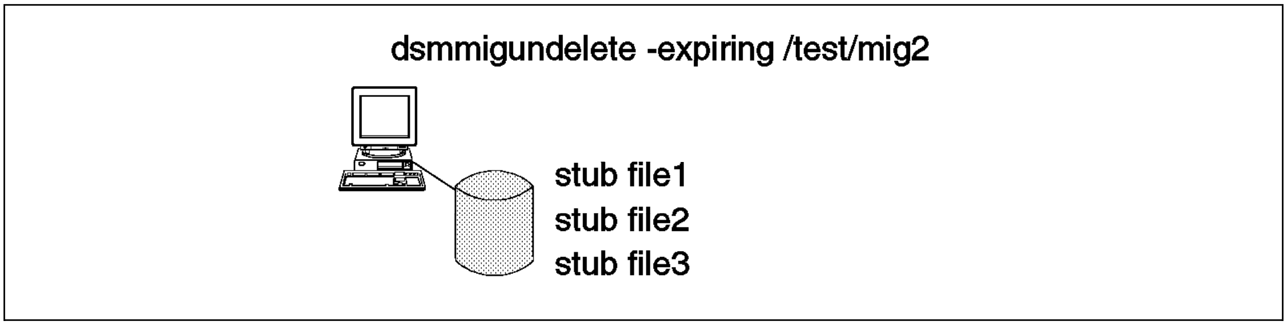


Figure 45. Dsmmigundelete with the EXPIRING Parameter

The key point here is knowing when to specify the EXPIRING parameter, and it can be difficult to determine when reconciliation was last run. A successful execution of reconciliation does not produce messages in either the activity log of the ADSM server or logs maintained on the HSM client.

We recommend that reconciliation be controlled by a scheduled client command so that it can be more easily determined when the process last executed. You must set the RECONCILEINTERVAL option on dsm.sys to 0 so that reconcile will not continue to run periodically. If the administrator uses this technique to schedule reconciliation, it is usually possible to tell when reconciliation last ran. However, it is still possible for reconciliation to run for other reasons that cannot be controlled by the administrator. For example, reconciliation occurs whenever the migration candidates list is empty or does not exist. Also, reconciliation can occur if demand migration occurs and there are no candidates left in the list.

Either the administrator command line client or the administrative GUI could be used to set up the scheduled client command. The following is an example of such a scheduled client command to run reconciliation every night at midnight for client bering:

```
DEFine Schedule standard daily_reconcile type=client
  action=command STARTTime=00:00 objects=″dsmreconcile″
DEFine association standard daily_reconcile bering
```

You must also set the RECONCILEINTERVAL option in the dsm.sys file to 0 to ensure that reconcile will run only during the scheduled time.

7.3 Recovery Checklist

To re-create file systems or physical disks should they become accidentally deleted or corrupted, the HSM administrator should save the following information:

- File system information
- Volume group information
- Space management settings for file systems

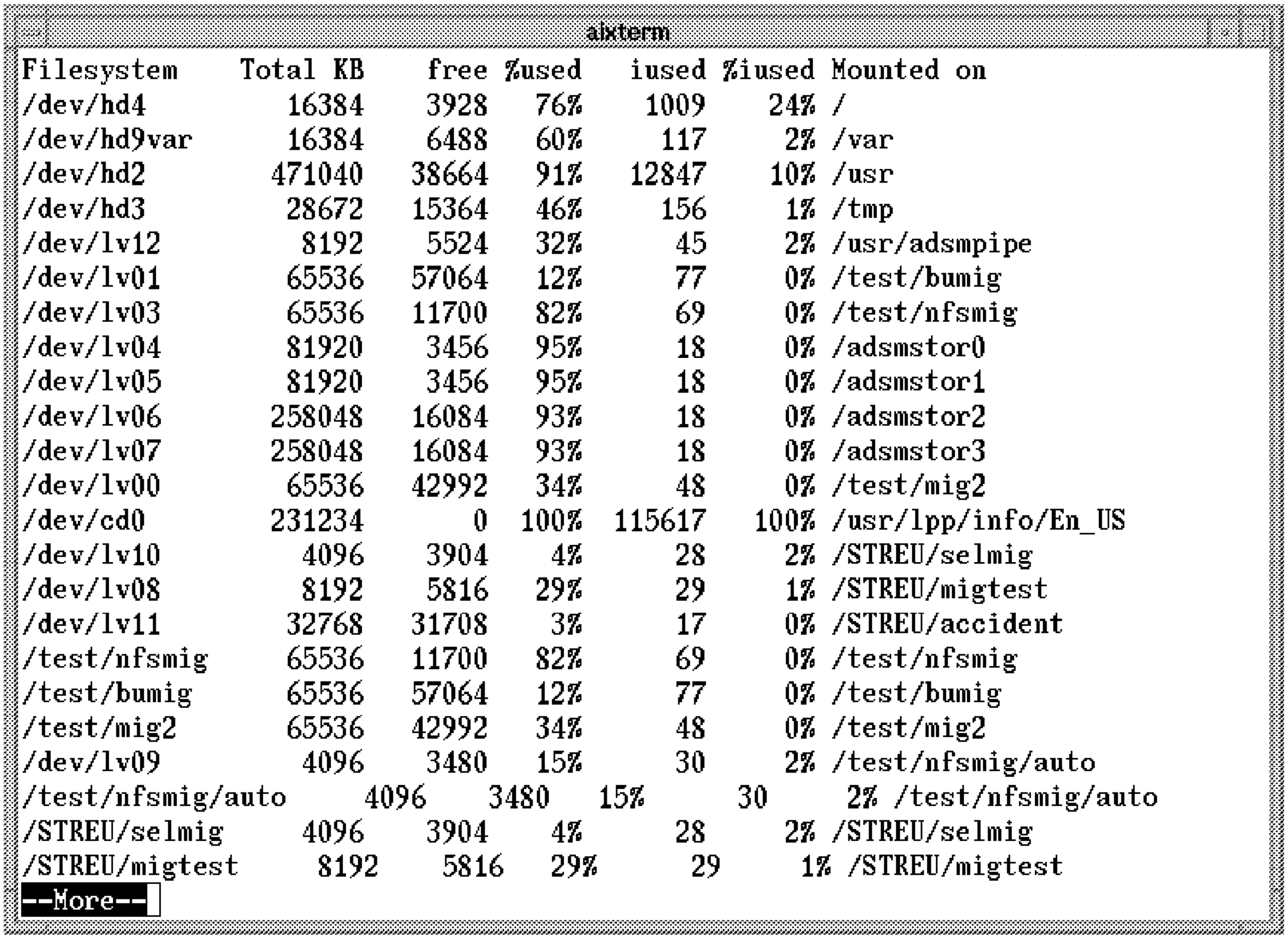
- Listings of files that have been hard-linked
- Listings of file names that have had their recall mode changed by dsmattr
- Paging space definitions (the AIX **mksysb** command does not save these)

7.3.1 File System Parameter Information

To re-create the file systems, file system parameter information such as file system name, mount point, and size must be saved. To save this information, execute the **df -i** command and then redirect the output to a temporary file to be printed off and saved with the system recovery instructions:

```
df -i > /tmp/query_file_system_info
```

Figure 46 shows the output of the **df -i** command.



```
Filesystem    Total KB    free %used   iused %iused Mounted on
/dev/hd4         16384    3928   76%    1009    24% /
/dev/hd9var      16384    6488   60%     117     2% /var
/dev/hd2        471040   38664   91%   12847    10% /usr
/dev/hd3         28672   15364   46%     156     1% /tmp
/dev/lv12         8192    5524   32%      45     2% /usr/adsmpipe
/dev/lv01        65536   57064   12%      77     0% /test/bumig
/dev/lv03        65536   11700   82%      69     0% /test/nfsmig
/dev/lv04        81920    3456   95%      18     0% /adsmstor0
/dev/lv05        81920    3456   95%      18     0% /adsmstor1
/dev/lv06       258048   16084   93%      18     0% /adsmstor2
/dev/lv07       258048   16084   93%      18     0% /adsmstor3
/dev/lv00        65536   42992   34%      48     0% /test/mig2
/dev/cd0        231234       0  100%  115617   100% /usr/lpp/info/En_US
/dev/lv10         4096    3904    4%      28     2% /STREU/selmig
/dev/lv08         8192    5816   29%      29     1% /STREU/migtest
/dev/lv11        32768   31708    3%      17     0% /STREU/accident
/test/nfsmig     65536   11700   82%      69     0% /test/nfsmig
/test/bumig      65536   57064   12%      77     0% /test/bumig
/test/mig2       65536   42992   34%      48     0% /test/mig2
/dev/lv09         4096    3480   15%      30     2% /test/nfsmig/auto
/test/nfsmig/auto     4096    3480   15%      30     2% /test/nfsmig/auto
/STREU/selmig     4096    3904    4%      28     2% /STREU/selmig
/STREU/migtest     8192    5816   29%      29     1% /STREU/migtest
--More--
```

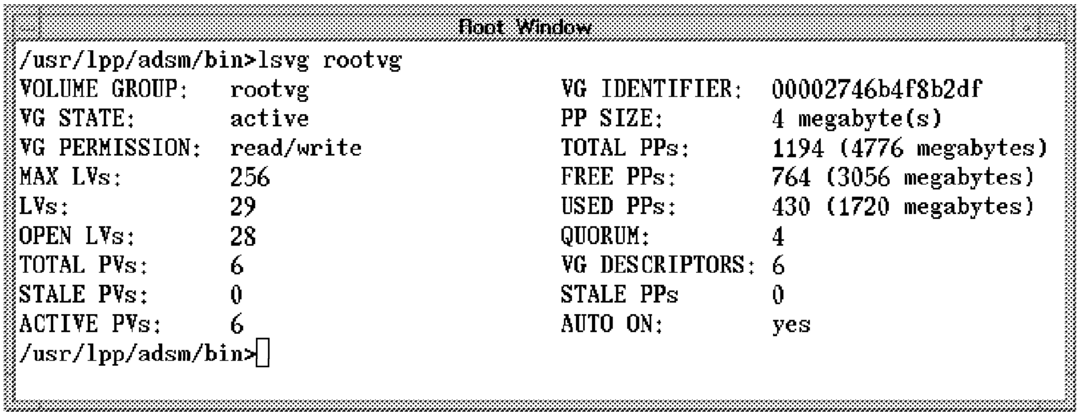
Figure 46. Sample Output from df -i Command

7.3.2 Volume Group Information

To re-create a volume group, information such as physical partition size and number of physical partitions must be saved. To save this information, execute the **lsvg <volume group name>** (where volume group name is the volume group for which you want information listed) and then redirect the output to a temporary file to be printed off and saved with the system recovery instructions. An example of this command for the root volume group (rootvg) is:

```
lsvg rootvg > /tmp/query_volume_group_info
```

Figure 47 shows the output of the **lsvg** command.



```
/usr/lpp/adsm/bin>lsvg rootvg
VOLUME GROUP:   rootvg                  VG IDENTIFIER:  00002746b4f8b2df
VG STATE:       active                  PP SIZE:        4 megabyte(s)
VG PERMISSION:  read/write              TOTAL PPs:      1194 (4776 megabytes)
MAX LVs:        256                     FREE PPs:       764 (3056 megabytes)
LVs:            29                      USED PPs:       430 (1720 megabytes)
OPEN LVs:       28                      QUORUM:         4
TOTAL PVs:      6                       VG DESCRIPTORS: 6
STALE PVs:      0                       STALE PPs       0
ACTIVE PVs:     6                       AUTO ON:        yes
/usr/lpp/adsm/bin>
```

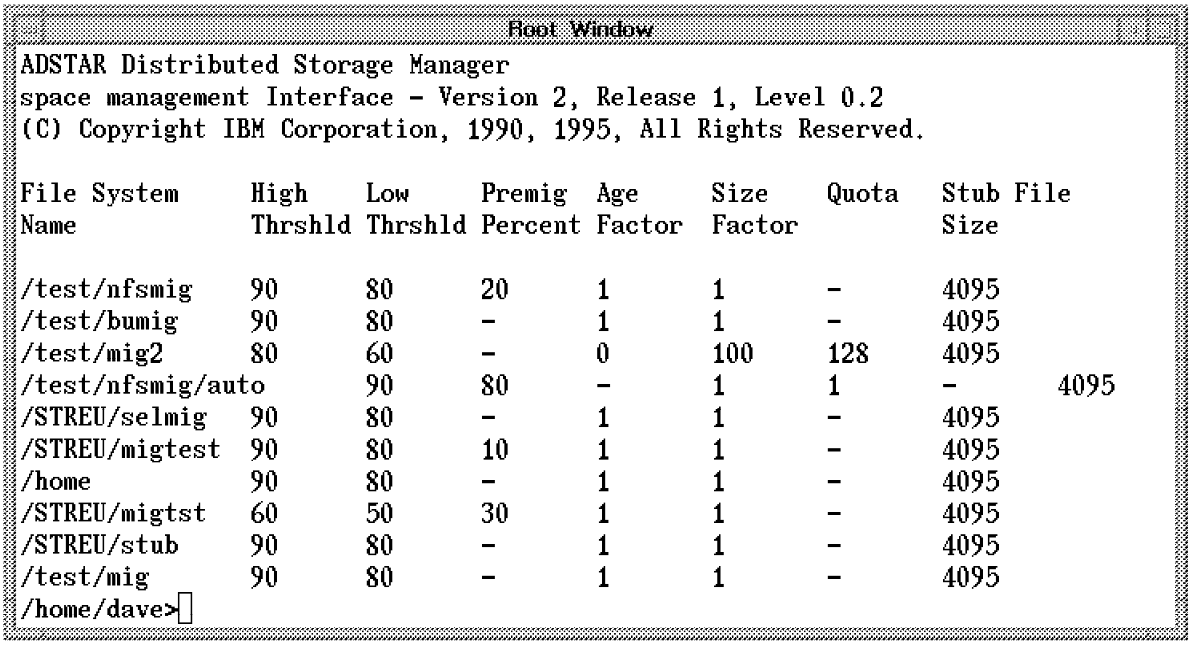
Figure 47. Sample Output from lsvg Command

7.3.3 Space Management Settings for File Systems

To reactivate space management for a file system, such information as threshold settings and stub file size must be saved. To save this information, execute the **dsmmigfs q** command and then redirect the output to a temporary file to be printed off and saved with the system recovery instructions:

```
dsmmigfs q > /tmp/query_space_management_info
```

Figure 48 on page 92 shows the output of the **dsmmigfs q** command.



```
ADSTAR Distributed Storage Manager
space management Interface - Version 2, Release 1, Level 0.2
(C) Copyright IBM Corporation, 1990, 1995, All Rights Reserved.

File System     High    Low     Premig  Age     Size    Quota   Stub File
Name            Thrshld Thrshld Percent Factor  Factor          Size

/test/nfsmig    90      80      20      1       1       -       4095
/test/bumig     90      80      -       1       1       -       4095
/test/mig2      80      60      -       0       100     128     4095
/test/nfsmig/auto       90      80      -       1       1       -       4095
/STREU/selmig   90      80      -       1       1       -       4095
/STREU/migtest  90      80      10      1       1       -       4095
/home           90      80      -       1       1       -       4095
/STREU/migtst   60      50      30      1       1       -       4095
/STREU/stub     90      80      -       1       1       -       4095
/test/mig       90      80      -       1       1       -       4095
/home/dave>
```

Figure 48. Sample Output from dsmmigfs q Command

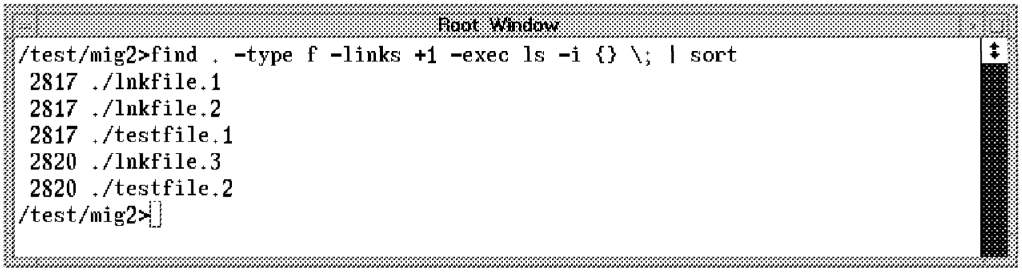
7.3.4 Files That Have Been Hard-Linked

The **dsmmigundelete** command does not support hard-linked files. You cannot re-create a stub file for a hard-linked file unless all the files that are hard-linked together have been deleted from the local file system.

Note: This step is not necessary if you are using **dsmc restore -restoremigstate=yes** to re-create stub files.

When one file in a set of hard-linked files is migrated, all of the hard-linked files in the set become stub files. When the **dsmmigundelete** command re-creates a stub file for a hard-linked file, the stub file has the same name as the file that was originally migrated. Stub files are not re-created for any other files that were previously in the hard-linked set of files. To re-create the set the root user must therefore save the names of any files that have been hard-linked together.

Files that have been hard-linked together share the same inode. Therefore you list inodes with more than one link for all files in a file system and then sort them to determine which files are hard-linked. In Figure 49, we have two sets of hard-linked files: `testfile.1` is hard-linked with files `lnkfile.1` and `lnkfile.2`, and `testfile.2` is hard-linked with file `lnkfile.3`.



```
/test/mig2>find . -type f -links +1 -exec ls -i {} \; | sort
 2817 ./lnkfile.1
 2817 ./lnkfile.2
 2817 ./testfile.1
 2820 ./lnkfile.3
 2820 ./testfile.2
/test/mig2>
```

Figure 49. Sample Output Listing Hard-Linked Files

The **find** command can be issued for all file systems beginning with root, or it can be issued once for each file system that contains hard-linked files and has been added to space management. The form of the command you use depends on how many file systems have been added to space management. To obtain a list of hard-linked files for the entire system or the current path, execute the following commands and then redirect the output to a temporary file to be printed off and saved with the system recovery instructions:

Command to display hard-linked files for entire system

```
find / -type f -links +1 -exec ls -i {} \; | sort
 > /tmp/query_hardlinked_files_info
```

Command to display hard-linked files for current path

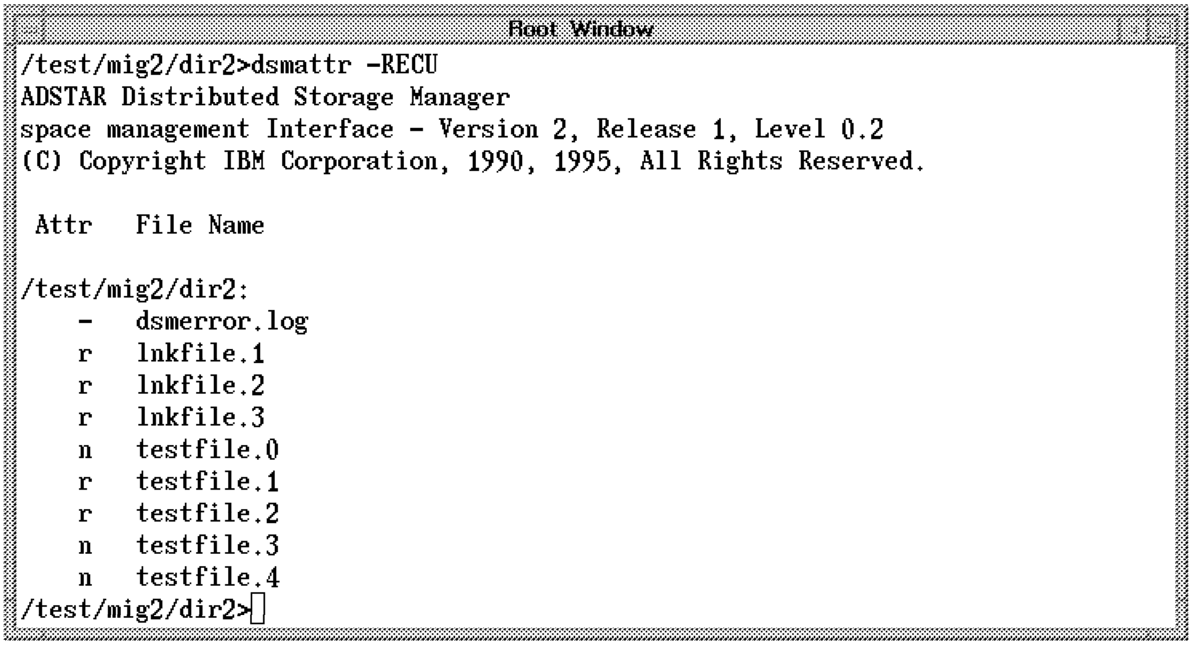
```
find . -type f -links +1 -exec ls -i {} \; | sort
 > /tmp/query_hardlinked_files_info
```

7.3.5 File Names That Have Had Their Recall Mode Changed by dsmattr

To re-create the space management recall modes for files that have had the modes changed with the **dsmattr** command, you should save listings showing which file names have been changed. To do this, use the RECURSIVE parameter with the **dsmatttr** command to traverse all subdirectories of the file system and then redirect the output to a temporary file to be printed off and saved with the system recovery instructions:

```
dsmmattr -RECU > /tmp/query_dsm_attr_info
```

Figure 50 on page 94 shows the output. Files `lnkfile.1`, `lnkfile.2`, `lnkfile.3`, `testfile.1`, and `testfile.2` have had their recall mode changed to read-without-recall (denoted by the *r*). The remaining files have a normal recall mode.



```
/test/mig2/dir2>dsmattr -RECU
ADSTAR Distributed Storage Manager
space management Interface - Version 2, Release 1, Level 0.2
(C) Copyright IBM Corporation, 1990, 1995, All Rights Reserved.

 Attr   File Name

/test/mig2/dir2:
    -   dsmerror.log
    r   lnkfile.1
    r   lnkfile.2
    r   lnkfile.3
    n   testfile.0
    r   testfile.1
    r   testfile.2
    n   testfile.3
    n   testfile.4
/test/mig2/dir2>
```

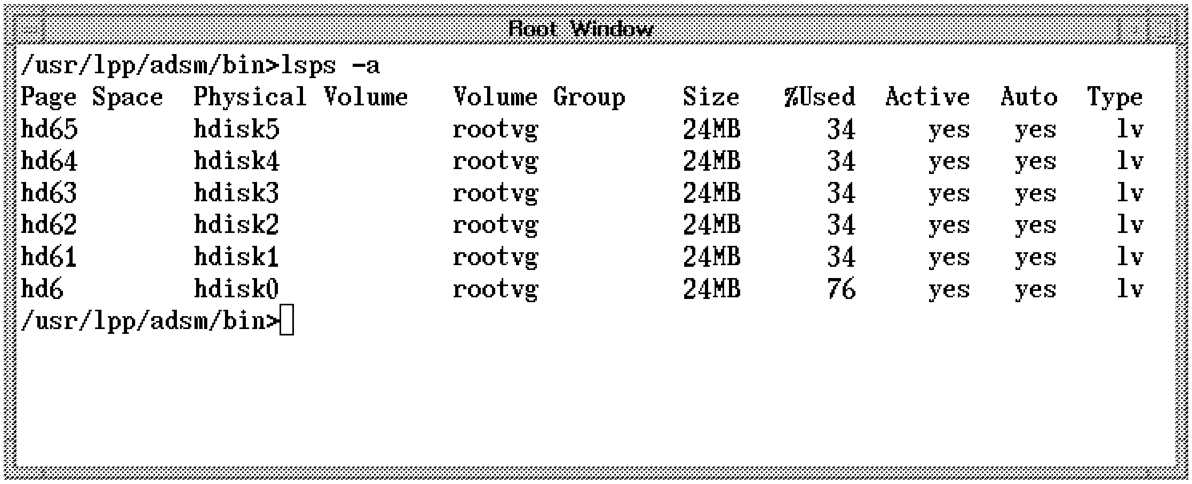
Figure 50. Sample Output from dsmattr Command

7.3.6 Paging Space Definitions

The **mksysb** command does not save paging space definitions. If you have changed your paging space definitions from the defaults that came with the system, you should save those definitions. Save them to an output file for use later should you have to re-create the entire system. Execute the **lsps -a** command and then redirect the output to a temporary file to be printed off and saved with the system recovery instructions:

```
lsps -a > /tmp/query_pgspce_info
```

Figure 51 shows the output of the **lsps -a** command.



```
/usr/lpp/adsm/bin>lsps -a
Page Space  Physical Volume   Volume Group    Size   %Used  Active  Auto  Type
hd65        hdisk5            rootvg          24MB      34     yes   yes    lv
hd64        hdisk4            rootvg          24MB      34     yes   yes    lv
hd63        hdisk3            rootvg          24MB      34     yes   yes    lv
hd62        hdisk2            rootvg          24MB      34     yes   yes    lv
hd61        hdisk1            rootvg          24MB      34     yes   yes    lv
hd6         hdisk0            rootvg          24MB      76     yes   yes    lv
/usr/lpp/adsm/bin>
```

Figure 51. Sample Output from lsps -a Command

7.4 Recovering Data When Using One ADSM Server

We look at how to recover files, groups of files, and an entire file system when you use one ADSM server for both your backup and migration storage pools.

7.4.1 Recovering a File or Group of Files

When you are using the same ADSM server for backup and migration, recovering a single file or group of files is a simple matter of using the backup-archive client. When you specify the RESTOREMIGSTATE parameter on the **dsmc restore** command, ADSM restores the file to a migrated state.

This support is available with PTF IP20673. If you are not at this level of ADSM, or, if you are using separate servers for backup and migration, you must use the steps described in 7.5, “Recovering Data When Using Separate Servers for Backup and Migration.”

7.4.2 Recovering an Entire File System

If a file system that contains migrated files is lost or corrupted, the system administrator (root user) can re-create the file system using steps 1 through 4 in 7.5, “Recovering Data When Using Separate Servers for Backup and Migration” to rebuild the file system and the **dsmc restore** command to restore all files including the migrated files. For example, to restore all files in file system /test/mig2/*, re-creating stub files if the file was migrated at the last incremental backup, use the following command:

```
dsmc restore -subdir=yes -restoremigstate=yes /test/mig2/*
```

7.5 Recovering Data When Using Separate Servers for Backup and Migration

If you are using separate servers for backup and migration, you have no way of restoring an individual file to a migrated state. If you have lost a single file, simply restore that file, using the backup-archive client, and it will come back as resident. If you have lost an entire file system that contained migrated files, use the following procedure to re-create the file system:

1. Use SMIT or line commands to re-create the file systems.

   The output saved from the **df -i** command as described in 7.3.1, “File System Parameter Information” on page 90 can be used as guidance to re-create the file system. For example, to create the /test/mig2 file system, issue the following command:

   ```
   crfs -v jfs -g′rootvg′ -a size=′131072′ -m′/test/mig2′ -A′yes′ -p′rw′
   -t′no′
   ```

2. Mount the file system.

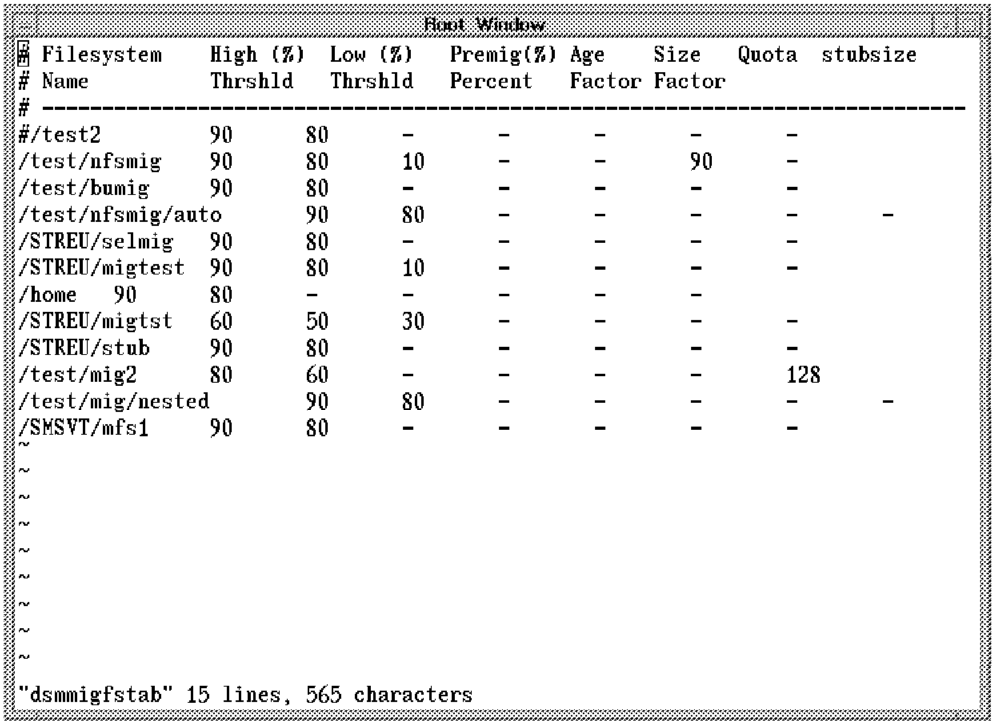
   For example, to mount the /test/mig2 file system, issue the following command:

   ```
   mount -v′jfs′ /dev/lv00 /test/mig2
   ```

3. Remove the entry for the file system in dsmmigfstab.

To avoid having duplicate entries in the space management configuration file, remove the entry for the file system from the /etc/adsm/SpaceMan/config/dsmmigfstab file (shown in Figure 52 on page 96), using the editor of your choice.

A duplicate entry will not harm the HSM operation, but it may be confusing to the root user.



```
# Filesystem    High (%)  Low (%)   Premig(%) Age    Size   Quota  stubsize
# Name          Thrshld   Thrshld   Percent   Factor Factor
# -----------------------------------------------------------------------------
#/test2         90      80      -       -       -       -       -
/test/nfsmig    90      80      10      -       -       90      -
/test/bumig     90      80      -       -       -       -       -
/test/nfsmig/auto       90      80      -       -       -       -       -
/STREU/selmig  90       80      -       -       -       -       -
/STREU/migtest 90       80      10      -       -       -       -
/home   90      80      -       -       -       -       -
/STREU/migtst  60       50      30      -       -       -       -
/STREU/stub     90      80      -       -       -       -       -
/test/mig2      80      60      -       -       -       -       128
/test/mig/nested        90      80      -       -       -       -       -
/SMSVT/mfs1     90      80      -       -       -       -       -
~
~
~
~
~
~
~
~
~
"dsmmigfstab" 15 lines, 565 characters
```

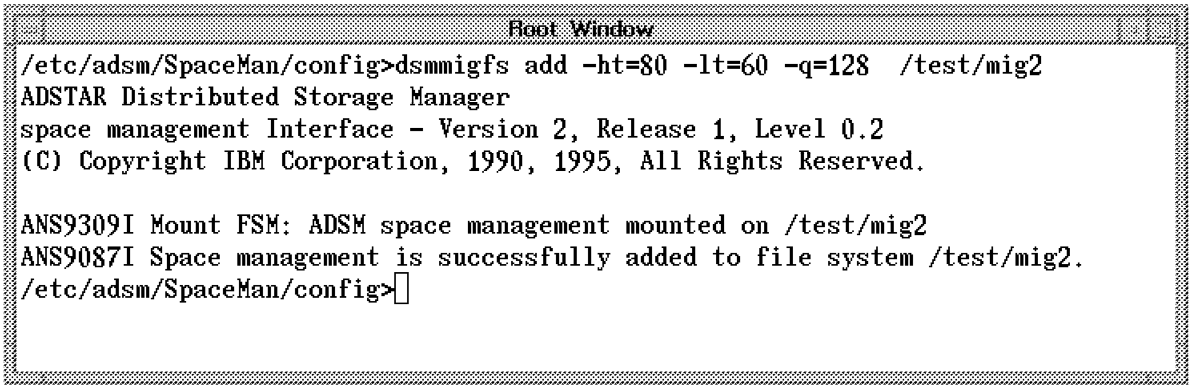
Figure 52. Sample /etc/adsm/SpaceMan/config/dsmmigfstab

4. Add space management to the file system.

   You can add space management through the HSM GUI or by issuing the **dsmmigfs** command. Use the threshold and quota values obtained from the listing saved in 7.3.3, “Space Management Settings for File Systems” on page 91. For example, to add space management to the /test/mig2 file system, with a high threshold of 80% and a low threshold of 60% and a quota of 128 MB, issue the following command:

   ```
   dsmmigfs add -HT=80 -Lt=60 -Q=128 /test/mig2
   ```

   Figure 53 on page 97 shows the output of the **dsmmigfs** command.



```
/etc/adsm/SpaceMan/config>dsmmigfs add -ht=80 -lt=60 -q=128  /test/mig2
ADSTAR Distributed Storage Manager
space management Interface - Version 2, Release 1, Level 0.2
(C) Copyright IBM Corporation, 1990, 1995, All Rights Reserved.

ANS9309I Mount FSM: ADSM space management mounted on /test/mig2
ANS9087I Space management is successfully added to file system /test/mig2.
/etc/adsm/SpaceMan/config>
```

Figure 53. Output from the dsmmigfs add Command

5. Restore the directories.

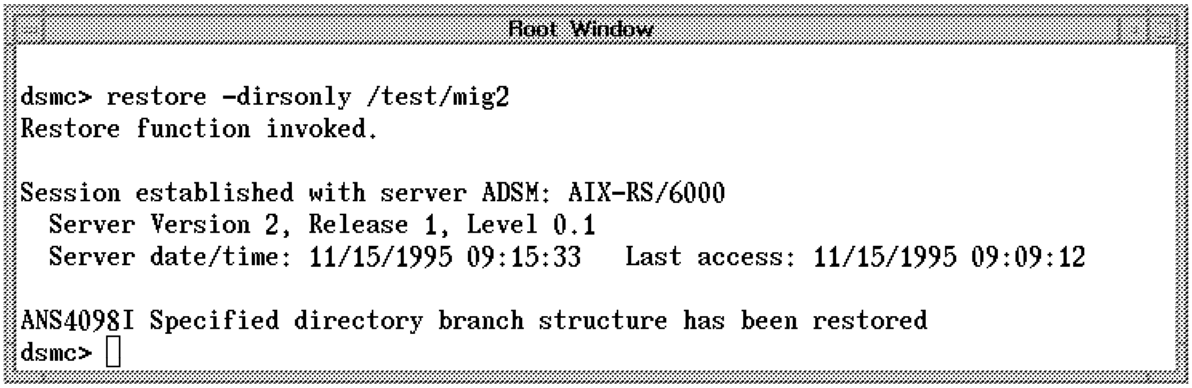
   Files are the only type of data migrated by HSM. HSM does not support the migration of directories. Therefore, you must re-create the directory structure of the file system before you can re-create the stub files for migrated and premigrated files. To restore the directory structure of the file system, issue the **dsmc restore** command with the -DIRSONLY option.

   Note: To re-create the directory structure of a file system, the file system must have been backed up with an incremental backup. Archiving of a file system does not save the access permissions of the directory structure and therefore cannot be used to re-create the directories. In addition, empty directories are not archived and therefore cannot be retrieved. When a retrieve is done for a file in a directory that does not exist, the ADSM backup-archive client re-creates the directory using the access permissions from the ADSM backup-archive client. This may produce erroneous results. The only way to rebuild the directory structure correctly (using the ADSM backup-archive client) is to do a **dsmc restore** from incremental backups that have been made. These backups must be incremental; selective backups do not save the directory structure.

   For example, to restore just the directory structure of the /test/mig2 file system, issue the following command:

   ```
   dsmc restore -dirsonly /test/mig2
   ```

   Figure 54 shows the output from the **restore -dirsonly** command.



```
dsmc> restore -dirsonly /test/mig2
Restore function invoked.

Session established with server ADSM: AIX-RS/6000
  Server Version 2, Release 1, Level 0.1
  Server date/time: 11/15/1995 09:15:33   Last access: 11/15/1995 09:09:12

ANS4098I Specified directory branch structure has been restored
dsmc>
```

Figure 54. Output from the restore -dirsonly Command

6. Recreate the stub files.

   Issue the **dsmmigundelete** command to re-create stub files for migrated files and premigrated files.

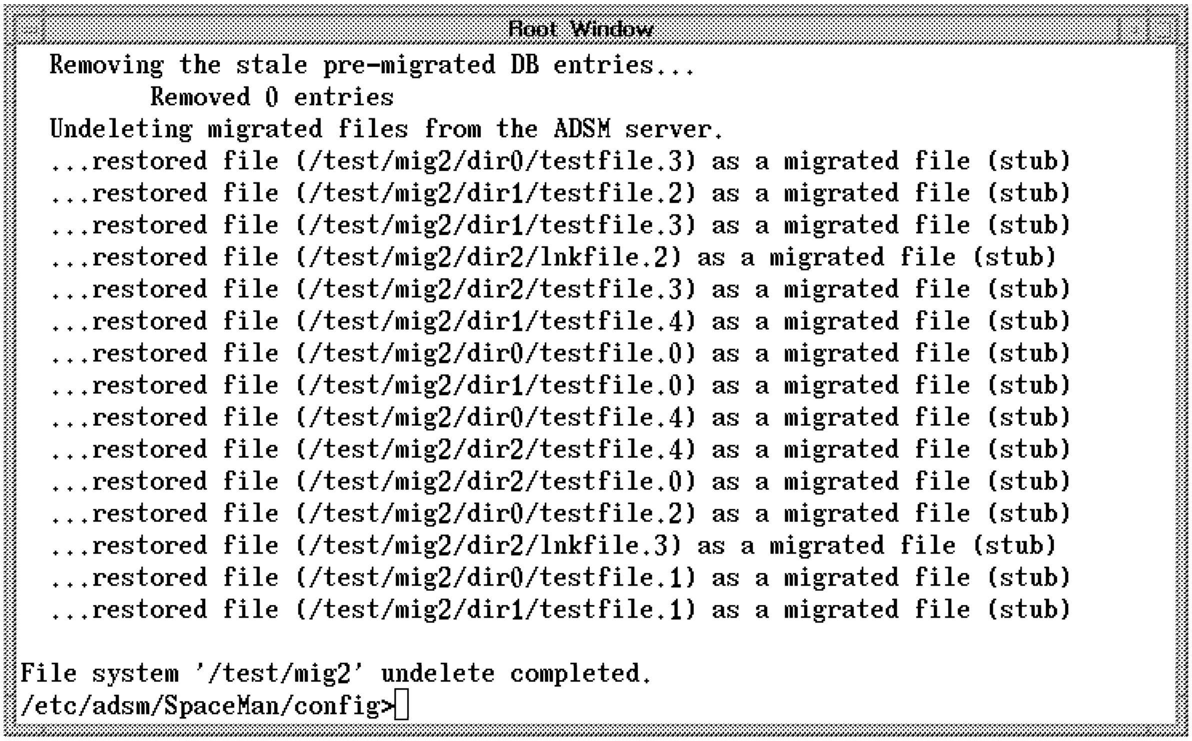
   For example, to re-create stub files for migrated and premigrated files for the /test/mig2 file system that have not yet been marked for expiration, issue the following command:

   ```
   dsmmigundelete /test/mig2
   ```

   When the **dsmmigundelete** command re-creates the stub file, the stub file size is always 511 bytes of space and does not contain any leading bytes of data from the file. Ordinarily, when an AIX command (such as the head AIX command) reads the stub file, it does not cause a recall of the file because the information it needs is in the leader data. When the **dsmmigundelete** command re-creates the stub file, the recall mode is always set to normal. Thus, when any AIX command is issued against a stub file that has been re-created with the **dsmmigundelete** command, a normal recall occurs.

   If multiple migrated files in ADSM storage have been marked for expiration and have the same name, HSM re-creates a stub file for the file with the more recent modification time.

   Figure 55 shows the output from the **dsmmigundelete** command.



```
  Removing the stale pre-migrated DB entries...
         Removed 0 entries
  Undeleting migrated files from the ADSM server.
  ...restored file (/test/mig2/dir0/testfile.3) as a migrated file (stub)
  ...restored file (/test/mig2/dir1/testfile.2) as a migrated file (stub)
  ...restored file (/test/mig2/dir1/testfile.3) as a migrated file (stub)
  ...restored file (/test/mig2/dir2/lnkfile.2) as a migrated file (stub)
  ...restored file (/test/mig2/dir2/testfile.3) as a migrated file (stub)
  ...restored file (/test/mig2/dir1/testfile.4) as a migrated file (stub)
  ...restored file (/test/mig2/dir0/testfile.0) as a migrated file (stub)
  ...restored file (/test/mig2/dir1/testfile.0) as a migrated file (stub)
  ...restored file (/test/mig2/dir0/testfile.4) as a migrated file (stub)
  ...restored file (/test/mig2/dir2/testfile.4) as a migrated file (stub)
  ...restored file (/test/mig2/dir2/testfile.0) as a migrated file (stub)
  ...restored file (/test/mig2/dir0/testfile.2) as a migrated file (stub)
  ...restored file (/test/mig2/dir2/lnkfile.3) as a migrated file (stub)
  ...restored file (/test/mig2/dir0/testfile.1) as a migrated file (stub)
  ...restored file (/test/mig2/dir1/testfile.1) as a migrated file (stub)

File system '/test/mig2' undelete completed.
/etc/adsm/SpaceMan/config>
```

Figure 55. Output from the dsmmigundelete Command

7. Restore the resident files.

   Issue the **dsmc restore** command with the REPLACE=NO option to restore backup versions of previously resident files. For example, to restore backup versions of all remaining files in the /test/mig2 file system, issue the following command:

```
dsmc restore -replace=no -subdir=yes /test/mig2/*
```

Note: ADSM restores the hard links during the restore process if the hard links were backed up.

8. Reset special recall mode for files.

   When a stub file is re-created through the **dsmmigundelete** command, the recall mode for the file name is reset to normal. Any file name that has had its recall mode changed by the **dsmattr** command must be set again. Use the output from the **dsmattr** command as described in 7.3.5, “File Names That Have Had Their Recall Mode Changed by dsmattr” on page 93. For example, to re-create the recall mode for the files listed in Figure 50 on page 94, use the following commands:

   ```
   dsmattr -r testfile.1
   dsmattr -r testfile.2
   ```

9. Re-create hard links for migrated and premigrated files.

   Using the output from 7.3.4, “Files That Have Been Hard-Linked” on page 92, re-create any hard-linked files that may exist on the file system. For example, to re-create hard links for the files listed in Figure 49 on page 92, use the following commands:

   ```
   ln testfile.1 lnkfile.1 lnkfile.2
   ln testfile.2 lnkfile.3
   ```

   You only have to re-create hard links for the files that were migrated because the **dsmc restore** command restores hard-linked files. If you are working with a large list and are not sure which files were migrated, there is no harm in issuing the **ln** command for files that are already hard-linked.

7.6 Recovery of an Entire AIX System Containing Migrated Files

When the entire AIX system has been lost because of a system or media failure, you must:

1. Restore the operating system
2. Restore the communications software
3. Restore the HSM and backup-archive client
4. Rebuild your volume group definitions (use SMIT or line commands)
5. Rebuild your file system definitions (use SMIT or line commands)
6. Add HSM to file systems previously defined
7. Restore the directory structure for the file systems
8. Re-create stub files for files previously migrated
9. Restore all other files not migrated, using the ADSM backup-archive client.

ADSM can recover your files only if you run the ADSM backup-archive client. It can re-create stub files for migrated files and premigrated files only if you run the HSM client. If the file system that contains your ADSM client code is lost, you must first reinstall the ADSM client code before you can recover your other files.

Note: We recommend that the ADSM client code be installed in the rootvg volume group. If the ADSM server resides on the same machine as the HSM client, we also recommend that the ADSM server code and the ADSM database reside in the root volume group. These data files should reside in the root volume group for ease of recovery but should exist in their own file systems. If these recommendations are followed, **mksysb** can be used to create a bootable tape that already contains the ADSM client code and, if applicable, the ADSM server code and ADSM database. A mksysb bootable tape should be re-created every time a software upgrade or change to the operating system occurs. In addition to a mksysb bootable tape, we recommend that daily ADSM database backups be performed. To help automate the recovery process, output from the **lsvf** and **df -i** commands could be used as input to shell scripts that could rebuild the volume groups and file systems should a complete system rebuild ever be required.

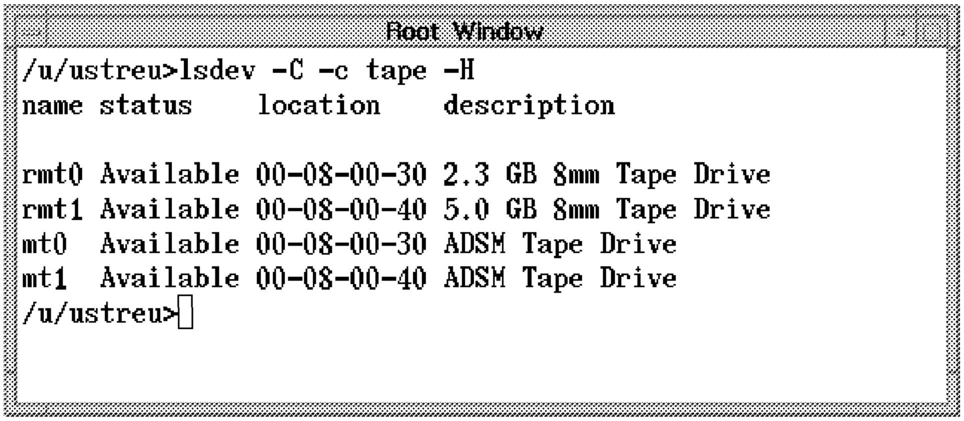
7.6.1 Creating a Bootable Tape with mksysb

Use the following procedure to build a mksysb bootable image:

1. List available tape devices that the mksysb tape create process can use. Issue the following command:

```
lsdev -C -c tape -H
```

Figure 56 shows the sample output from this command.



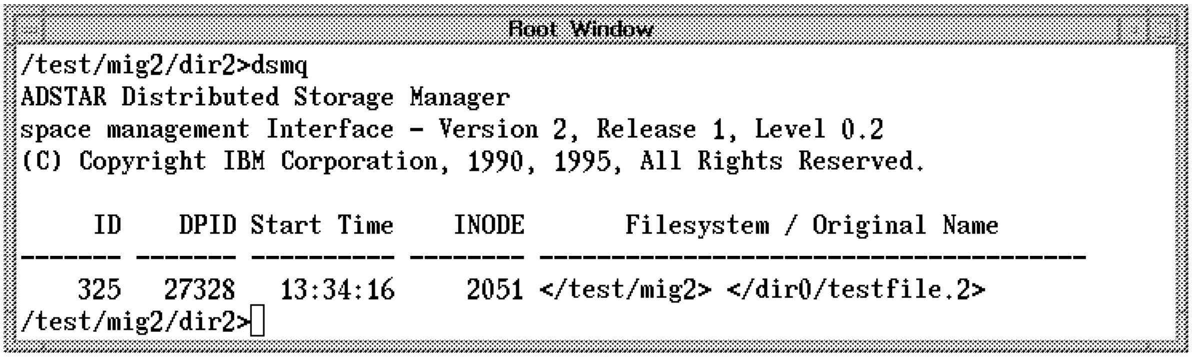
```
/u/ustreu>lsdev -C -c tape -H
name status    location    description

rmt0 Available 00-08-00-30 2.3 GB 8mm Tape Drive
rmt1 Available 00-08-00-40 5.0 GB 8mm Tape Drive
mt0  Available 00-08-00-30 ADSM Tape Drive
mt1  Available 00-08-00-40 ADSM Tape Drive
/u/ustreu>
```

Figure 56. Sample Output from lsdev Command

2. Stop all running processes for the HSM client. Processes must not change system files while the mksysb bootable tape is being created. To stop all HSM processes:

   a. Issue the **dsmq** command to obtain the recall daemon process ID for each recall process that is currently in the queue.

      Figure 57 on page 101 shows the output of the **dsmq** command.



```
/test/mig2/dir2>dsmq
ADSTAR Distributed Storage Manager
space management Interface - Version 2, Release 1, Level 0.2
(C) Copyright IBM Corporation, 1990, 1995, All Rights Reserved.

     ID    DPID Start Time    INODE      Filesystem / Original Name
------- ------- ---------- -------- -------------------------------------
    325   27328   13:34:16     2051 </test/mig2> </dir0/testfile.2>
/test/mig2/dir2>
```

Figure 57. Sample Output from dsmq Command

b. Use the **dsmrm** command to remove each recall process from the queue. For example, in Figure 57, the **dsmrm** command could be used to remove process ID 325.

c. Use the **kill** command to kill the space monitor daemon (dsmmonitord) and any recall daemons (dsmrecalld) that are running.

d. Verify that the daemons are no longer running, using a command such as the following:

```
ps -ef | grep dsm
```

3. Before performing the mksysb, check for non-JFS file systems mounted on logical volumes in the root volume group. Unmount these file systems before you create the mksysb bootable tape.

4. Use SMIT or a shell script to create the mksysb tape.

Note: We recommend that you create a mksysb tape for each AIX HSM client. The **mksysb** command retains the TCP/IP address of the system on which it was run. If you use one mksysb tape for multiple AIX HSM clients, you must change the TCP/IP address before you connect the machine to the network. To use SMIT, do the following:

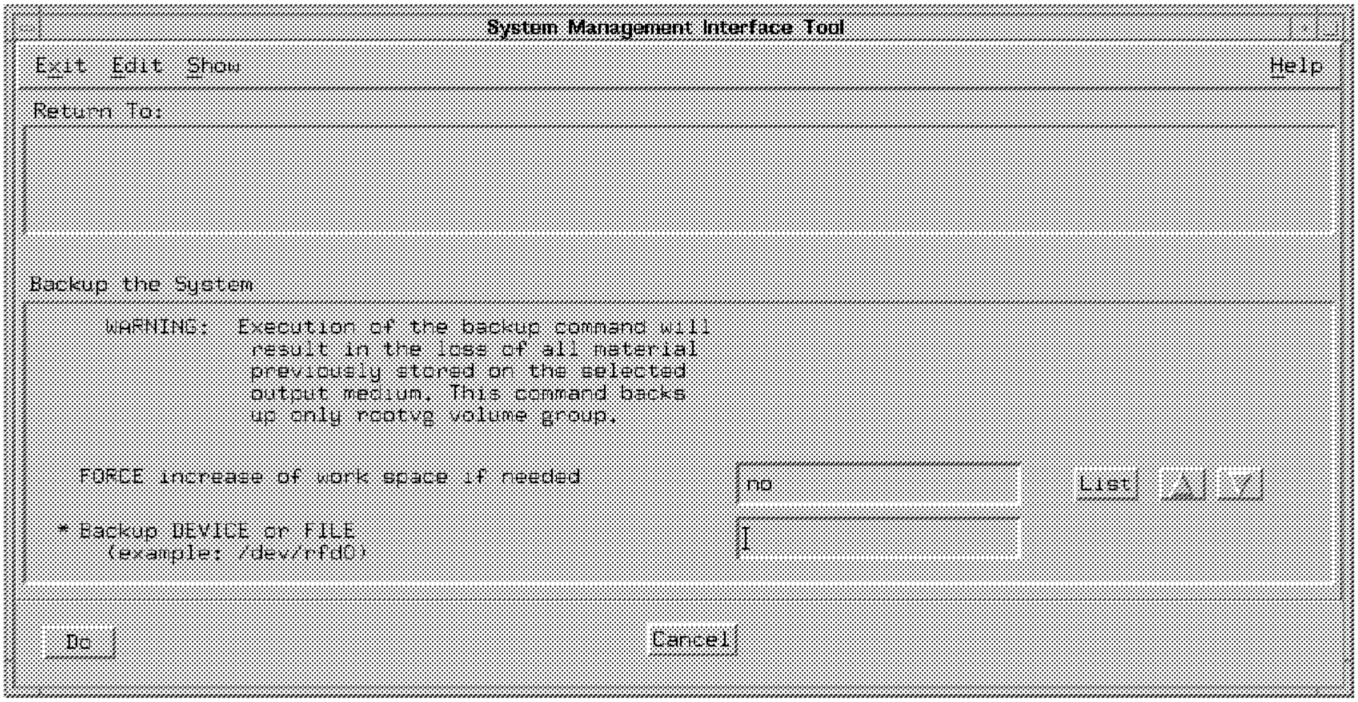
a. Make available to AIX a tape device that is bootable. We recommend that, for 8 mm tape devices, the AIX tape device driver be used for the mksysb.

Note: We recommend that the drive you use for building the bootable image be cleaned on a regular basis, and the tapes used for the mksysb process be replaced on a periodic basis.

If the ADSM tape device driver is currently being used for backup-archive functions, it should be made unavailable to AIX, and the AIX device driver should be made available. The output from the `lsdev` command should indicate that the `/dev/rmtx` is available and that the `/dev/mtx` device driver is defined (but not available) to AIX. If this is not the case, use SMIT to make the `/dev/mtx` device driver unavailable (but kept in the database), and then make the `/dev/rmtx` device available.

b. Use SMIT to create the mksysb tape. When you type in the **smit mksysb** (or smit -C mksysb if you are using AIXWindows) command, you see a dialog window similar to that shown in Figure 58 on page 102. Set the **FORCE increase of work space if needed** field to **yes**. Press the TAB key when the cursor is on **no** to change the default value to **yes**. In the

Backup DEVICE or FILE field enter the name of the device you made available in step 4a (for example, /dev/rmt1).



```
     WARNING:  Execution of the backup command will
               result in the loss of all material
               previously stored on the selected
               output medium. This command backs
               up only rootvg volume group.

   FORCE increase of work space if needed            no

 * Backup DEVICE or FILE
     (example: /dev/rfd0)
```

Figure 58. Sample Dialog Window from smit mksysb Command

If you want to execute the mksysb process outside SMIT, you could use the following shell script:

Sample shell script for the mksysb process

```
rmdev -l mt1
mkdev -l rmt1
mkszfile -f && mksysb /dev/rmt1
mkdev -l mt1
```

Note that the script is only an example. You will have to customize it for your environment. In our example, we assume that /dev/rmt1 is the device to be used for the mksysb process. The script makes the /dev/mt1 device unavailable to AIX, makes the /dev/rmt1 device available to AIX, performs the **mkszfile** to build the /.fs.size file containing the list of file systems to be backed up, performs the mksysb process, and makes the /dev/mt1 device available again to AIX.

7.6.2 Recovering an Entire AIX System with the mksysb Tape

To recover an entire AIX system, do the following:

1. Boot from the mksysb tape.

   First recover the AIX base operating system (BOS), communications software, and ADSM HSM client and backup-archive client code. If this code has been made part of the root volume group, the mksysb tape is used to boot from and re-create the system. To boot from the mksysb tape:

a. Place the powered-off system unit in service mode. The system unit must be placed in service mode to boot from any device other than the hard disk.

b. Turn on the system unit and wait until you see this message:

```
″********** Please define the System Console **********″.
```

Follow the instructions on the screen to initialize the System Console (F1 or #1 on most systems), the only terminal active during the restoration.

c. After a few more minutes, you are presented with a menu of options. Select **Install a system that was created with the SMIT ″Backup the System″ function or the mksysb command** (usually #2 on most systems).

d. Select the correct language for the system to use.

e. Verify that the system will be booting from tape and the number of disks is correct.

f. When the base system is installed, you will see instructions to remove the tape, turn the key from service to normal, and press Enter. The system will reboot again, and all data in the root volume group will be restored.

2. Re-create the paging space.

   Use the listing described in 7.3.6, “Paging Space Definitions” on page 94. (Note: If you have not made changes to the page space since the system was installed, you can skip this step.) To re-create the first page space listed in Figure 51 on page 94, use the following command:

   ```
   mkps -s′24′ -a′′ rootvg hdisk5
   ```

3. Re-create the volume group definitions. Using the saved output from the **lsvg** (see 7.3.2, “Volume Group Information” on page 91), use SMIT to re-create the volume group definitions.

4. Re-create the file system definitions for file systems not managed by HSM.

   Using the saved output from 7.3.1, “File System Parameter Information” on page 90, use SMIT to re-create the file system definitions for file systems not managed by HSM.

5. Restore the root directory, using the ADSM backup-archive client. Use the following command:

   ```
   dsmc restore -subdir=no -replace=yes /
   ```

6. Restore data for all file systems not managed by HSM.

   Use the ADSM backup-archive client to restore the file system. If you are not sure which files have had space management added to them, refer to the output from the **dsmmigfs q** command. All file systems not listed in this command output are not managed by space management. For example, to restore file system /adsmstor0, use the following command:

   ```
   dsmc restore -subdir=yes -replace=yes /adsmstor0/*
   ```

Note: We recommend that you restore the /etc directory to an alternative directory and then compare the differences. For example, the passwords file may have changed or the AIX object database manager (ODM) may be different.

7. Restart the space monitor daemon and recall daemons.

   The HSM space management client must be running before any space management commands can be executed. To restart the space monitor daemon, use the **dsmmonitord** command. To restart the recall daemon, use the **dsmrecalld** command.

8. Recover the file systems managed by HSM.

   Follow the steps described in 7.4, "Recovering Data When Using One ADSM Server" on page 95 or 7.5, "Recovering Data When Using Separate Servers for Backup and Migration" on page 95 for every HSM-managed file system listed in the output saved, as described in 7.3.3, "Space Management Settings for File Systems" on page 91.

Appendix A. Macros Used to Set Up Automation

The following ADSM macro defines schedules to perform reconcile, automatic migration, and resetting of age and size priority on a nightly basis.

```
/**********************************************************************/
/*   Name:   Sweep.macro                                              */
/*   Function: Define and associate schedules to perform nightly      */
/*             reconcile and automatic migration                      */
/**********************************************************************/
/* Reset the score so that age is more important than size            */
/* You will need to do this for every HSM-managed file system         */
/* Note: remember to set RECONCILEINTERVAL to 0 in dsm.sys            */
/**********************************************************************/
DEFine Schedule standard score_by_age_home type=client -
     action=command STARTTime=21:50 -
     objects=″dsmmigfs update -age=1 -size=0 /home″
/**/
DEFine Schedule standard score_by_age_test type=client -
     action=command STARTTime=21:50 -
     objects=″dsmmigfs update -age=1 -size=0 /test/*″
/**/
/**********************************************************************/
/* Reconcile all file systems and then start automatic migration      */
/**********************************************************************/
DEFine Schedule standard nightly_reconcile_automig type=client -
       action=command STARTTime=00:00 -
       objects=″dsmreconcile;dsmautomig″
/**/
/**********************************************************************/
/* Reset the score to so that age and size are 1:1                    */
/* and build a new candidates list for the new score values           */
/* You will need to do this for every HSM-managed file system         */
/**********************************************************************/
DEFine Schedule standard reset_score_home type=client -
     action=command STARTTime=06:00 -
     objects=″dsmmigfs update -age=1 -size=1 /home;dsmreconcile -c /home″
/**/
DEFine Schedule standard reset_score_test type=client -
     action=command STARTTime=06:00 -
     objects=″dsmmigfs update -age=1 -size=1 /home;dsmreconcile -c /home″
/**/
/**********************************************************************/
/* Associate the schedules with the HSM clients                       */
/* You will need to do this for every HSM client                      */
/**********************************************************************/
DEFine association standard score_by_age_home bering
DEFine association standard score_by_age_test bering
DEFine association standard nightly_reconcile_automig bering
DEFine association standard reset_score_home bering
DEFine association standard reset_score_test bering
```

Appendix B. Determining Average and Distribution of File Sizes

This appendix describes how you can obtain information on the average file size and distribution of file sizes on an HSM client.

1. Create listing of files.
   Execute the following command to list all plain files that are larger than 4096 and redirect the output to a file called `filesize_info`.

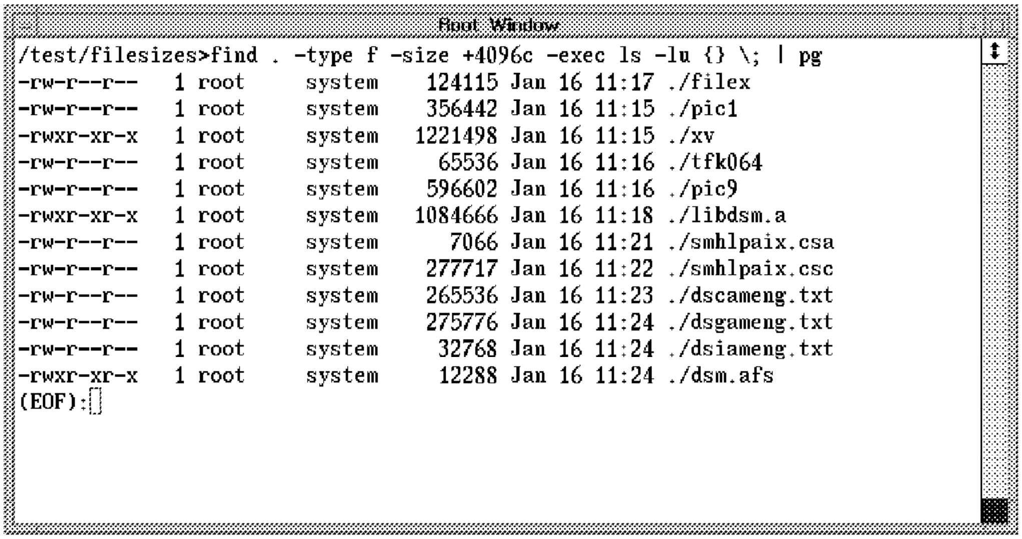
   List all plain files on the system

   ```
   find / -type f -size +4096c -exec ls -lu {} \; > /tmp/filesize_info
   ```

   List all plain files in the current path

   ```
   find . -type f -size +4096c -exec ls -lu {} \; > /tmp/filesize_info
   ```

   A sample output listing is shown in Figure 59.



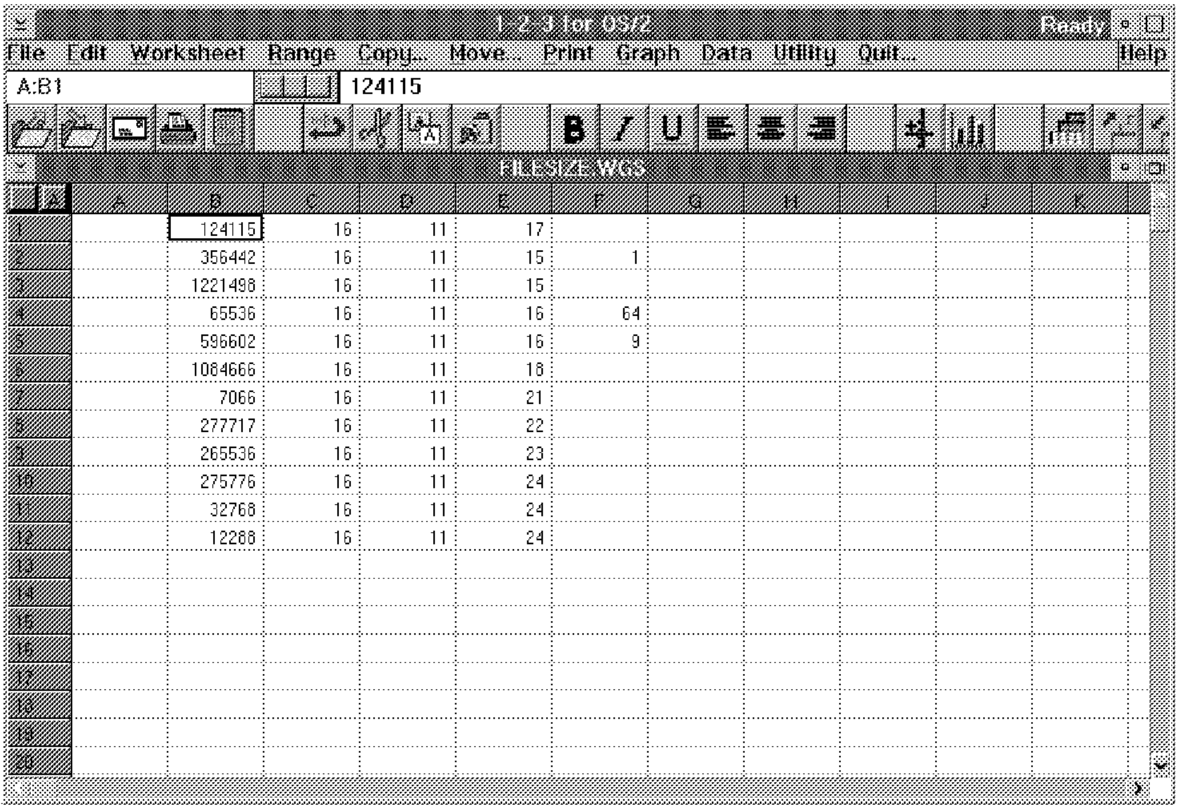
```
/test/filesizes>find . -type f -size +4096c -exec ls -lu {} \; | pg
-rw-r--r--   1 root     system    124115 Jan 16 11:17 ./filex
-rw-r--r--   1 root     system    356442 Jan 16 11:15 ./pic1
-rwxr-xr-x   1 root     system   1221498 Jan 16 11:15 ./xv
-rw-r--r--   1 root     system     65536 Jan 16 11:16 ./tfk064
-rw-r--r--   1 root     system    596602 Jan 16 11:16 ./pic9
-rwxr-xr-x   1 root     system   1084666 Jan 16 11:18 ./libdsm.a
-rw-r--r--   1 root     system      7066 Jan 16 11:21 ./smhlpaix.csa
-rw-r--r--   1 root     system    277717 Jan 16 11:22 ./smhlpaix.csc
-rw-r--r--   1 root     system    265536 Jan 16 11:23 ./dscameng.txt
-rw-r--r--   1 root     system    275776 Jan 16 11:24 ./dsgameng.txt
-rw-r--r--   1 root     system     32768 Jan 16 11:24 ./dsiameng.txt
-rwxr-xr-x   1 root     system     12288 Jan 16 11:24 ./dsm.afs
(EOF):
```

Figure 59. Sample Output Listing File Sizes

   The **ls -lu** command will list the access time of each file instead of the modification time. We exclude files that are smaller than 4096 because they will not be migrated by HSM. If you have defined a block size that is smaller than 4095 on your system, you will have to change this value.

2. Import the listing into a spreadsheet.

   FTP and import the `filesize_info` file into your favorite spreadsheet application. In our environment we used Lotus 1-2-3 for OS/2. First, we edited the file and removed the columns preceding the file size. We then imported the file as numeric, which ignored all of the text. Figure 60 on page 108 shows the results of the import.


1-2-3 for OS/2
Ready
File Edit Worksheet Range Copy... Move... Print Graph Data Utility Quit... Help
FILESIZE.WG3

A:B1 124115

	A	B	C	D	E	F	G	H	I	J	K
1		124115	16	11	17						
2		356442	16	11	15	1					
3		1221498	16	11	15						
4		65536	16	11	16	64					
5		596602	16	11	16	9					
6		1084666	16	11	18						
7		7066	16	11	21						
8		277717	16	11	22						
9		265536	16	11	23						
10		275776	16	11	24						
11		32768	16	11	24						
12		12288	16	11	24						

Figure 60. Importing filesize_info

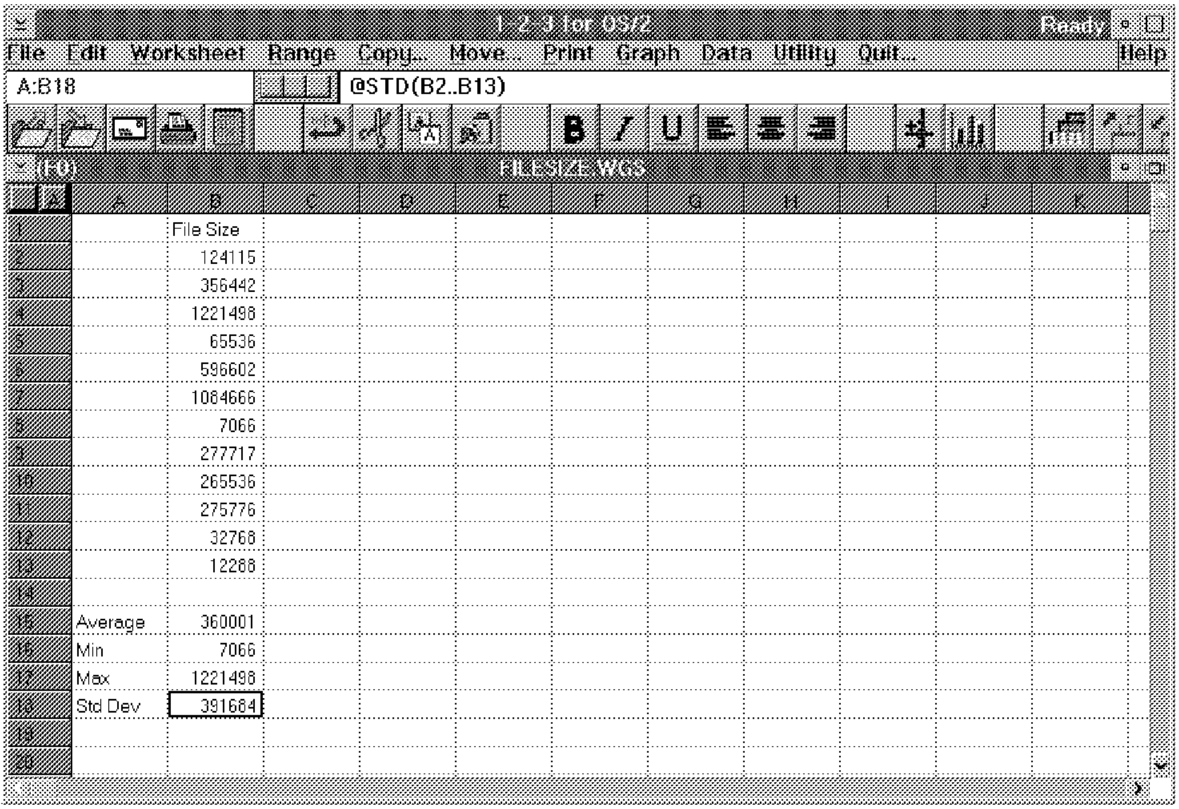
3. Calculate the average file size.
   Use the spreadsheet to calculate the average file size and to graph the file size distribution. If you are using this information to get a general idea of when migrates and recalls occur (as described in 2.6, "Monitoring HSM Activity" on page 16), you can also calculate the standard deviation.

   We removed all columns except for file size, added some simple labels, and used the following Lotus 1-2-3 functions to calculate:

   ```
   @AVG  average file size
   @MIN  minimum file size
   @MAX  maximum file size
   @STD  standard deviation of file size based on population
   ```

   The results are shown in Figure 61 on page 109.

   Note: If you are using the average file size and standard deviation to determine when migrates and recalls occur (2.6, "Monitoring HSM Activity" on page 16) and you are using client compression, you must divide all file sizes in half before calculating the average file size and standard deviation.



1-2-3 for OS/2
Ready
File Edit Worksheet Range Copy... Move... Print Graph Data Utility Quit... Help
(F0)
FILESIZE.WG3

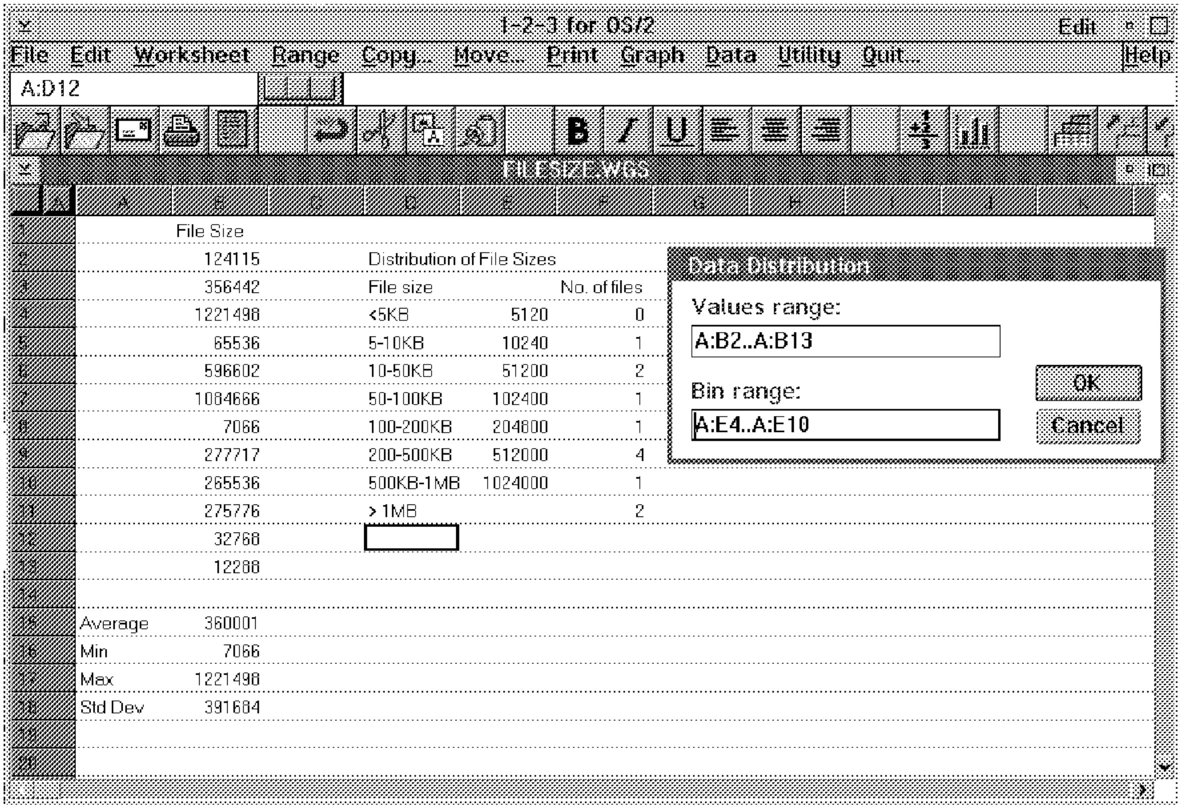
A:B18 @STD(B2..B13)

	A	B
1		File Size
2		124115
3		356442
4		1221498
5		65536
6		596602
7		1084666
8		7066
9		277717
10		265536
11		275776
12		32768
13		12288
14		
15	Average	360001
16	Min	7066
17	Max	1221498
18	Std Dev	391684
19		
20		

Figure 61. Calculating Average File Size

4. Determine the distribution of file sizes.

   Use the Data Distribution function to display the distribution of file sizes (see Figure 62 on page 110).



A:D12

	A	B	C	D	E	F
1		File Size				
2		124115		Distribution of File Sizes		
3		356442		File size		No. of files
4		1221498		<5KB	5120	0
5		65536		5-10KB	10240	1
6		596602		10-50KB	51200	2
7		1084666		50-100KB	102400	1
8		7066		100-200KB	204800	1
9		277717		200-500KB	512000	4
10		265536		500KB-1MB	1024000	1
11		275776		> 1MB		2
12		32768				
13		12288				
14						
15	Average	360001				
16	Min	7066				
17	Max	1221498				
18	Std Dev	391684				
19						
20						

Values range: A:B2..A:B13

Bin range: A:E4..A:E10

Figure 62. File Size Distribution

Finally, if you want to get fancy, you can create a graph showing the distribution of file sizes along with the distribution. We do not show you how to do this in this book.

Appendix C. Common UNIX Commands and Recall

Because ADSM stores file information and leader data in the stub file of a migrated file, some UNIX commands can be satisfied without having to recall the file. Table 1 lists some commonly used UNIX commands that may not require a recall.

Table 1. UNIX Commands That May Not Require Recall

	Migrated File Recalled?
ls	No
find	No
mv	No
touch	No*
file	No**
head	No**
chmod	No
chown	No
chgrp	No
df	No
du	No
rm/del	No
> (redirect STDOUT to file)	No

Note:

***** If the file is premigrated, its state is changed to resident.

****** A migrated file is recalled when accessed by this command only if the stub file does not contain leader data.

Table 2 lists some commonly used UNIX commands that generally cause a transparent recall when the data access mode of the command is **Normal**.

Table 2 (Page 1 of 2). UNIX Commands That Usually Cause a Recall

Command	**Migrated File Recalled?**
grep	Yes
look	Yes
cat	Yes
lc	Yes
wc	Yes
ccom	Yes
mail	Yes
cp	Yes
rcp	Yes
spell	Yes
tail	Yes
editors such as vi, emacs, frame	Yes

Table 2 (Page 2 of 2). UNIX Commands That Usually Cause a Recall

Command	**Migrated File Recalled?**
ctags/etags	Yes
< (redirect STDIN)	Yes
>> (redirect STDOUT append)	Yes*
tar	Yes

Note:

***** If the file is premigrated, its state is changed to resident.

Appendix D. Fixfsm Script for Re-creating .SpaceMan Files

```
#!/bin/ksh
###########################################################################
# ADSTAR Distributed Storage Manager (ADSM)
# Script for recreating any important deleted files in the .SpaceMan
# directory of an HSM file system
# platform AIX
# usage:  fixfsm filesystem_path
###########################################################################
# created by:  Stefan R. Steiner
#              IBM Almaden Research Center
#              San Jose, CA  USA
# last update: 7.2.1996
###########################################################################

# Set common script variables
smdir=/etc/adsm/SpaceMan
configdir=${smdir}/config
statusdir=${smdir}/status
fstab=${configdir}/dsmmigfstab

#####################################
# Script functions
#####################################

RootCheck() {
# Function: make sure we are running as root
  user=whoami
  if    [ ″$user″ != ″root″ ]
  then  echo ″You must be logged in as root to run this command″
        exit 1
  fi
# End of RootCheck function
}

FindFSMs() {
#
# Function: gets a list of all of the FSMs in the system
#
   awk ′ {
      if (substr($1,1,1) == ″/″)
         printf (″%s ″, $1)
   } ′ $fstab
# End of FindFSMs function.
}

CheckValidFSM() {
#
# Function: determines if the file system is an ADSM file system
#
   if awk ′/^\// {print $1}′ $fstab | grep ^${fsmpath}$ > /dev/null
   then
     echo ″Fixing ADSM HSM file system: $fsmpath″
   else
     echo ″Error: $fsmpath is not an ADSM HSM file system″
     echo ″       found in $fstab″
     exit 2
   fi
# End of CheckValidFSM function.
}

FixDotSpaceMan() {
#
# Function: fixes and recreates any needed missing files in .SpaceMan
#
   spacemandir=$fsmpath/.SpaceMan
   shouldreboot=0

   # Make sure .SpaceMan is not a file
   if [[ -f $spacemandir ]]
   then
      echo ″Error: $spacemandir is an existing file. Please remove″
      echo ″       the file and restart this script″
      exit 3
   fi

   # Create .SpaceMan directory if it doesn′t exist
   if [[ ! -d $spacemandir ]]
   then
      echo ″  Creating $spacemandir directory″
      mkdir $spacemandir || exit 4
      shouldreboot=1
   fi

   # Update the .SpaceMan directory permissions
   chown bin.bin $spacemandir || exit 5
   chmod 02770 $spacemandir || exit 6

   # Create .SpaceMan/logdir if it doesn′t exist
   if [[ ! -d $spacemandir/logdir ]]
   then
      echo ″  Creating $spacemandir/logdir directory″
      mkdir $spacemandir/logdir || exit 7
      shouldreboot=1
   fi

   # Update the .SpaceMan/logdir directory permissions
   chown bin.bin $spacemandir/logdir || exit 8
   chmod 02770 $spacemandir/logdir || exit 9

   # Make sure BOTH of the premigration database files exist
   if [[ ! -f $spacemandir/premigrdb.dir || ! -f $spacemandir/premigrdb.pag ]]
   then
      echo ″  One or both premigrdb files is missing, recreating an empty″
      echo ″    premigration database. Note that all files that were″
      echo ″    premigrated will now be resident.″
      rm -f $spacemandir/premigrdb.dir $spacemandir/premigrdb.pag
      touch $spacemandir/premigrdb.dir $spacemandir/premigrdb.pag || exit 12
      shouldreboot=1
   fi

   # Update the .SpaceMan/premigrdb file permissions
   chown bin.bin $spacemandir/premigrdb.dir $spacemandir/premigrdb.pag || exit 13
   chmod 0660 $spacemandir/premigrdb.dir $spacemandir/premigrdb.pag || exit 14
   # Remove the candidates file since reconcile is going to run and recreate it
   rm -f $spacemandir/candidates

   # Make sure the status file exists
   if [[ ! -f $spacemandir/status ]]
   then
      echo ″  Recreating the .SpaceMan/status file″
      statname=′R′$(date +%y%m%d%H%M%S)
      touch $statusdir/$statname || exit 15
      chown bin.bin $statusdir/$statname || exit 16
      chmod 0660 $statusdir/$statname || exit 17
      ln -fs $statusdir/$statname $spacemandir/status || exit 18
      shouldreboot=1
   fi

   # Update the permission on the .pid lock files
   chown -f bin.bin $spacemandir/fslock.pid $spacemandir/migratelock.pid
   chmod -f 0644 $spacemandir/fslock.pid $spacemandir/migratelock.pid

   if [[ $shouldreboot = 1 ]]
   then
      echo ″Finished, some files were missing, so please run:″
      echo ″  dsmreconcile $fsmpath″
      echo ″When it is finished, it is recommended that you reboot the system″
   else
      echo ″Finished, some access permission might have been changed but″
      echo ″no important files were recreated.″
   fi
# End of FixDotSpaceMan function.
}


##############################################
# Script start
##############################################

# Make sure the root user is running this script
RootCheck

# Make sure the script is being used correct, one and only one parameter
# is allowed.
if [ $# -ne 1 ]
then
   echo ″$0 syntax: $0 filesystem_path″
   exit 2
fi

# fsmpath will contain the file system to fix the HSM .SpaceMan directory
fsmpath=$1

# Make sure the file system is a valid ADSM HSM file system
CheckValidFSM

# Now (if necessary) fix the .SpaceMan directory
FixDotSpaceMan

exit 0
```

Glossary

The terms in this glossary are defined as they pertain to the ADSM library. If you do not find a term you are looking for, you can refer to the *IBM Dictionary of Computing*, McGraw-Hill, 1994. In the United States and Canada you can order this publication by calling McGraw Hill at 1-800-2MC-GRAW.

This glossary may include terms and definitions from:

- The *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright (ANSI). Copies may be purchased from the American National Standards Institute, 11 West 42nd Street, New York, New York 10036.
- The *Information Technology Vocabulary*, developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC2/SC1).

A

administrative client. A program that runs on a file server, workstation, or mainframe. This program allows an ADSM administrator to control and monitor an ADSM server by using ADSM administrative commands.

administrator. A user who is registered with an ADSM server as an administrator. Administrators are assigned one or more privilege classes that determine which administrative tasks they can perform.

ADSTAR Distributed Storage Manager (ADSM). A client/server program product that provides storage management services to customers in a multivendor computer environment.

age factor. A value that determines the weight given to the age of a file when HSM prioritizes eligible files for migration. The age of the file in this case is the number of days since the file was last accessed. The age factor is used with the size factor to determine migration priority for a file. See also *size factor*.

archive. The process of copying one or more files to a long-term storage device. When you archive a file, you can specify whether to delete the file from your local file system after it is copied to ADSM storage or leave the original file intact.

archive copy group. A policy object that contains attributes that control the generation, destination, and expiration of archived copies of files. An archive copy group is stored in a management class.

archived copy. A copy of a file that resides in an ADSM archive storage pool.

automatic migration. The process HSM uses to automatically move files from a local file system to ADSM storage according to options and settings chosen by a root user on your workstation. This process is controlled by the space monitor daemon (**dsmmonitord**). See also *threshold migration* and *demand migration*.

automatic reconciliation. The process HSM uses to reconcile your file systems at regular intervals set by a root user on your workstation. This process is controlled by the space monitor daemon (**dsmmonitord**). See also *reconciliation*.

B

backup. The process of copying one or more files to a backup storage pool to protect against data loss.

backup-archive client. A program that runs on a file server, PC, or workstation that provides a means for ADSM users to back up, archive, restore, and retrieve files.

backup copy group. A policy object that contains attributes which control the generation, destination, and expiration of backup versions of files. A backup copy group is stored in a management class.

C

central scheduling. A function that allows an ADSM administrator to schedule backup, archive, and space management operations from a central location. The operations can be scheduled on a periodic basis or an explicit date.

client node. A file server or workstation on which ADSM has been installed and that has been registered with an ADSM server.

client/server. A communications network architecture in which one or more programs (clients) request computing or data services from another program (the server).

client system options file. An editable file that contains communication, authorization, central scheduling, backup, archive, and space management options. The options in a client system options file are set by a root user on your workstation. The file name is **dsm.sys** and is stored in your ADSM installation directory.

client user options file. A user-editable file that contains options that identify the ADSM server to contact, specify backup, archive, restore, retrieve, and space management options, and set date, time, and number formats. The file name is **dsm.opt** and is stored in your ADSM installation directory.

copy group. A policy object that contains attributes which control the generation, destination, and expiration of backup versions of files and archived copies of files. There are two types of copy groups: a backup copy group and an archive copy group. Copy groups are stored in management classes.

D

data access control mode. One of four execution modes provided by the **dsmmode** command. Execution modes enable you to change the space-management-related behavior of commands that run under **dsmmode**. The data access control mode controls whether a command accesses a migrated file, sees a migrated file as zero-length, or receives an input/output error if it attempts to access a migrated file. See also *execution mode*.

default management class. The management class ADSM assigns to a file if a root user does not explicitly assign one to a file using an INCLUDE option in your include-exclude options file.

demand migration. The process HSM uses to respond to an out-of-space condition on a file system. HSM migrates files to ADSM storage until space usage drops to the low threshold set for the file system. If the high threshold and low threshold are the same, HSM attempts to migrate one file.

destination. A copy group attribute that specifies the storage pool to which a file is backed up, archived, or migrated. At installation, ADSM provides three storage destinations: BACKUPPOOL, ARCHIVEPOOL, and SPACEMGTPOOL.

dsm.opt file. See *client user options file*.

dsm.sys file. See *client system options file*.

E

exclude. The process of specifying a file or group of files in your include-exclude options file with an exclude option to prevent them from being backed up or migrated. You can exclude a file from backup and space management, backup only, or space management only.

execution mode. A mode that controls the space-management-related behavior of commands that run under the **dsmmode** command. The **dsmmode** command provides four execution modes—a data access control mode that controls whether a migrated file can be accessed; a timestamp control mode that controls whether the access time for a file is set to the current time when the file is accessed; an out-of-space protection mode that controls whether HSM intercepts an out-of-space condition on a file system; and a recall mode that controls whether a file is stored on your local file system when accessed or on your local file system only while it is being accessed and then migrated back to ADSM storage when it is closed.

expiring file. A migrated or premigrated file that has been marked for expiration and removal from ADSM storage. If a stub file or an original copy of a premigrated file is deleted from a local file system, or if the original copy of a premigrated file is updated, the corresponding migrated or premigrated file is marked for expiration the next time reconciliation is run. It expires and is removed from ADSM storage after the number of days specified with the MIGFILEEXPIRATION option have elapsed.

F

file server. A dedicated computer and its peripheral storage devices that are connected to a local area network that stores both programs and files that are shared by users on the network.

file size. For migration prioritization purposes, the size of a file in 1-KB blocks.

file state. The state of a file that resides in a file system to which space management has been added. A file can be in one of three states—resident, premigrated, or migrated. See also *resident file*, *premigrated file*, and *migrated file*.

file system migrator (FSM). A kernel extension that is mounted over an operating system file system when space management is added to the file system. The file system migrator intercepts all file system operations and provides any space management support that is required. If space management support is not required, the operation is performed by the operating system file system.

G

graphical user interface (GUI). A type of user interface that takes advantage of a high-resolution monitor; includes a combination of graphics, the object-action paradigm, and the use of pointing devices, menu bars, overlapping windows, and icons.

H

hierarchical storage management client. A program that runs on a workstation or file server to provide space management services. It automatically migrates eligible files to ADSM storage to maintain specific levels of free space on local file systems and automatically recalls migrated files when they are accessed. It also enables users to migrate and recall specific files.

high threshold. The percentage of space usage on a local file system at which HSM automatically begins migrating eligible files to ADSM storage. A root user sets this percentage when adding space management to a file system or updating space management settings. Contrast with *low threshold*.

I

include-exclude options file. A file, created by a root user on your workstation, that contains include and exclude options. An exclude option can be used to exclude a file from backup and space management, backup only, or space management only. An include option can be used to include specific files for backup and space management and to assign a specific management class to a file.

inode. A data structure that describes the individual files in an operating system. There is one inode for each file. The number of inodes in a file system, and therefore the maximum number of files a file system can contain, is set when the file system is created. Hard-linked files share the same inode.

inode number. A number that specifies a particular inode in a file system.

L

leader data. Leading bytes of data from a migrated file that are stored in the file′s corresponding stub file on the local file system. The amount of leader data stored in a stub file depends on the stub size specified. The required data for a stub file consumes 511 bytes of space. Any remaining space in a stub file is used to store leader data. If a process accesses only the leader data and does not modify that data, HSM does not have to recall the migrated file to the local file system.

low threshold. A percentage of space usage on a local file system at which HSM automatically stops migrating files to ADSM storage during a threshold or demand migration process. A root user sets this percentage when adding space management to a file system or updating space management settings. Contrast with *high threshold*.

M

management class. A policy object that contains a collection of space management attributes and backup and archive copy groups. The space management attributes contained in a management class assigned to a file determine whether the file is eligible for automatic or selective migration. The attributes in the backup and archive copy groups determine whether a file is eligible for incremental backup and specify how ADSM manages backup versions of files and archived copies of files.

migrate-on-close recall mode. A mode that causes HSM to recall a migrated file to its originating file system only temporarily. If the file is not modified, HSM returns the file to a migrated state when it is closed. However, if the file is modified, it becomes a resident file. You can set the recall mode for a migrated file to migrate-on-close by using the **dsmattr** command, or set the recall mode for a specific execution of a command or series of commands to migrate-on-close by using the **dsmmode** command. Contrast with *normal recall mode* and *read-without-recall recall mode.*

migrated file. A file that has been copied from a local file system to ADSM storage and replaced with a stub file on the local file system. Contrast with *resident file* and *premigrated file.*

migration. The process of copying a file from a local file system to ADSM storage and replacing the file with a stub file on the local file system. See also *threshold migration*, *demand migration*, and *selective migration.*

migration candidates list. A prioritized list of files that are eligible for automatic migration at the time the list is built. Files are prioritized for migration based on the number of days since they were last accessed, their size, and the age and size factors specified for a file system.

N

native file system. A file system to which you have not added space management.

normal recall mode. A mode that causes HSM to copy a migrated file back to its originating file system when it is accessed. If the file is not modified, it becomes a premigrated file. If the file is modified, it becomes a resident file. Contrast with *migrate-on-close recall mode* and *read-without-recall recall mode.*

O

orphaned stub file. A stub file for which no migrated file can be found on the ADSM server your client node is currently contacting for space management services. A stub file can become orphaned, for example, if you modify your client system options file to contact a server for space management that is different from the server to which the file was migrated.

out-of-space protection mode. One of four execution modes provided by the **dsmmode** command. Execution modes enable you to change the HSM-related behavior of commands that run under **dsmmode**. The out-of-space protection mode controls whether HSM intercepts out-of-space conditions. See also *execution mode*.

originating file system. The file system from which a file was migrated. When a file is recalled through normal or migrate-on-close recall mode, it is always returned to its originating file system.

P

premigrated file. A file that has been copied to ADSM storage but has not been replaced with a stub file on the local file system. An identical copy of the file resides both on the local file system and in ADSM storage. When free space is needed, HSM verifies that the file has not been modified and replaces the copy on the local file system with a stub file. HSM premigrates files after automatic migration is complete if there are additional files eligible for migration, and the premigration percentage is set to allow premigration. Contrast with *migrated file* and *resident file*.

premigrated files database. A database that contains information about each file that has been premigrated to ADSM storage. The database is stored in a hidden directory called **.SpaceMan** in each file system to which space management has been added. HSM updates the premigrated files database whenever it premigrates and recalls files and during reconciliation.

premigration. The process of copying files that are eligible for migration to ADSM storage, but leaving the original file intact on the local file system.

premigration percentage. A space management setting that controls whether the next eligible candidates in a file system are premigrated following threshold or demand migration. The default for premigration percentage is the difference between the percentage specified for the high threshold and the percentage specified for the low threshold for a file system.

Q

quota. The total number of megabytes of data that can be migrated and premigrated from a file system to ADSM storage. The default for quota is the same number of megabytes as allocated for the file system itself.

R

read-without-recall recall mode. A mode that causes HSM to read a migrated file from ADSM storage without storing it back on the local file system. The last piece of information read from the file is stored in a buffer in memory on the local file system. However, if a process that accesses the file writes to or modifies the file or uses memory mapping, HSM copies the file back to the local file system. Or, if the migrated file is a binary executable file, and the file is executed, HSM copies the file back to the local file system. You can change the recall mode for a migrated file to read-without-recall by using the **dsmattr** command. Contrast with *normal recall mode* and *migrate-on-close recall mode*.

recall. The process of copying a migrated file from ADSM storage back to its originating file system. See also *transparent recall*, *selective recall*, and *recall mode*.

recall mode. 1) One of four execution modes provided by the **dsmmode** command. Execution modes enable you to change the HSM-related behavior of commands that run under **dsmmode**. The recall mode controls whether an unmodified, recalled file is returned to a migrated state when it is closed. 2) A mode assigned to a migrated file with the **dsmattr** command that determines how the file is processed when it is recalled. It determines whether the file is stored on the local file system, migrated back to ADSM storage when it is closed, or read from ADSM storage without storing it on the local file system.

reconciliation. The process of synchronizing a file system to which you have added space management with the ADSM server you contact for space management services and building a new migration candidates list for the file system. HSM performs reconciliation automatically at intervals specified with the RECONCILEINTERVAL option in your client system options file. A root user can also start reconciliation manually at any time.

resident file. A file that resides on a local file system. It has not been migrated or premigrated, or it has been recalled from ADSM storage and modified. When first created, all files are resident. Contrast with *premigrated file* and *migrated file.*

restore. The process of copying a backup version of a file from ADSM storage to a local file system. You can restore a file to its original location or a new location.

retrieve. The process of copying an archived copy of a file from ADSM storage to a local file system, either its original location or a new location.

S

selective migration. The process of copying user-selected files from a local file system to ADSM storage and replacing the files with stub files on the local file system. Contrast with *threshold migration* and *demand migration*.

selective recall. The process of copying user-selected files from ADSM storage back to a local file system. Contrast with *transparent recall*.

server. A program that runs on a mainframe, workstation, or file server that provides shared services such as backup, archive, and space management to other (often remote) programs called *clients*.

session. A period of time in which a user can communicate with an ADSM server to perform backup, archive, restore, and retrieve requests or space management tasks such as migrating and recalling selected files.

size factor. A value that determines the weight given to the size of a file when HSM prioritizes eligible files for migration. The size of the file in this case is the size in 1-KB blocks. The size factor is used with the age factor to determine migration priority for a file. See also *age factor.*

space management. The process of keeping sufficient free storage space available on a local file system for new data and making the most efficient and economical use of distributed storage resources.

space management settings. Settings that specify the stub file size, quota, age factor, size factor, high threshold, low threshold, and premigration percentage for a file system. A root user selects space management settings when adding space management to a file system or updating space management.

space monitor daemon. An ADSM HSM daemon that checks space usage on all file systems for which space management is active and automatically starts threshold migration when space usage on a file system equals or exceeds its high threshold. How often the space monitor daemon checks space usage is determined by the CHECKTHRESHOLDS option in your client system options file. In addition, the space monitor daemon starts reconciliation for your file systems at the intervals specified with the RECONCILEINTERVAL option in your client system options file.

storage pool. A named set of storage volumes that is used as the destination for backup versions of files, archived copies of files, or migrated files.

stub file. A file that replaces the original file on a local file system when the file is migrated to ADSM storage. A stub file contains the information necessary to recall a migrated file from ADSM storage. It also contains additional information that HSM can read to eliminate the need to recall a migrated file.

stub file size. The size of a file that replaces the original file on a local file system when the file is migrated to ADSM storage. The size specified for stub files determines how much leader data can be stored in the stub file. The default for stub file size is the block size defined for a file system minus 1 byte.

T

threshold migration. The process of moving files from a local file system to ADSM storage according to the high and low thresholds defined for the file system. Threshold migration is started automatically by HSM and can be started manually by a root user. Contrast with *demand migration* and *selective migration*.

timestamp control mode. One of four execution modes provided by the **dsmmode** command. Execution modes enable you to change the space-management-related behavior of commands that run under **dsmmode**. The timestamp control mode controls whether commands preserve the access time for a file or set it to the current time. See also *execution mode*.

transparent recall. The process HSM uses to automatically recall a file to your workstation or file server when the file is accessed. The recall mode set for a file and the recall mode set for a process that accesses the file determine whether the file is stored on the local file system, stored on the local file system only temporarily if it is not modified, or read from ADSM storage without storing it on the local file system. See also *recall mode*. Contrast with *selective recall*.

W

workstation. A programmable, high-level workstation (usually on a network) with its own processing hardware.

List of Abbreviations

ADSM	ADSTAR Distributed Storage Manager
BOS	base operating system
FSM	file system migrator
GUI	graphical user interface
HSM	Hierarchical Storage Management
IBM	International Business Machines Corporation
ITSO	International Technical Support Organization
KB	kilobyte
LAN	local area network
NFS	Network File System
MB	megabyte
SMIT	System Management Interface Tool
TCP/IP	Transmission Control Protocol/Internet Protocol

Index

ITSO Redbook Evaluation

International Technical Support Organization
Using ADSM Hierarchical Storage Management
April 1996

Publication No. SG24-4631-00

Your feedback is very important to help us maintain the quality of ITSO redbooks. **Please fill out this questionnaire and return it using one of the following methods:**

- Mail it to the address on the back (postage paid in U.S. only)
- Give it to an IBM marketing representative for mailing
- Fax it to: Your International Access Code + 1 914 432 8246
- Send a note to REDBOOK@VNET.IBM.COM

Please rate on a scale of 1 to 5 the subjects below.
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction ____

Organization of the book	____	Grammar/punctuation/spelling	____
Accuracy of the information	____	Ease of reading and understanding	____
Relevance of the information	____	Ease of finding information	____
Completeness of the information	____	Level of technical detail	____
Value of illustrations	____	Print quality	____

Please answer the following questions:

a) Are you an employee of IBM or its subsidiaries: Yes____ No____

b) Do you work in the USA? Yes____ No____

c) Was this redbook published in time for your needs? Yes____ No____

d) Did this redbook meet your needs? Yes____ No____

If no, please explain:

____

____

What other topics would you like to see in this redbook?

____

____

What other redbooks would you like to see published?

____

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)

_______________________ _______________________
Name Address

_______________________ _______________________
Company or Organization

_______________________ _______________________
Phone No.

ITSO Redbook Evaluation
SG24-4631-00

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM International Technical Support Organization
Department 471/E2
650 Harry Road
San Jose, CA
USA 95120-6099

Fold and Tape **Please do not staple** Fold and Tape

Cut or Fold
Along Line

Printed in U.S.A.

SG24-4631-00