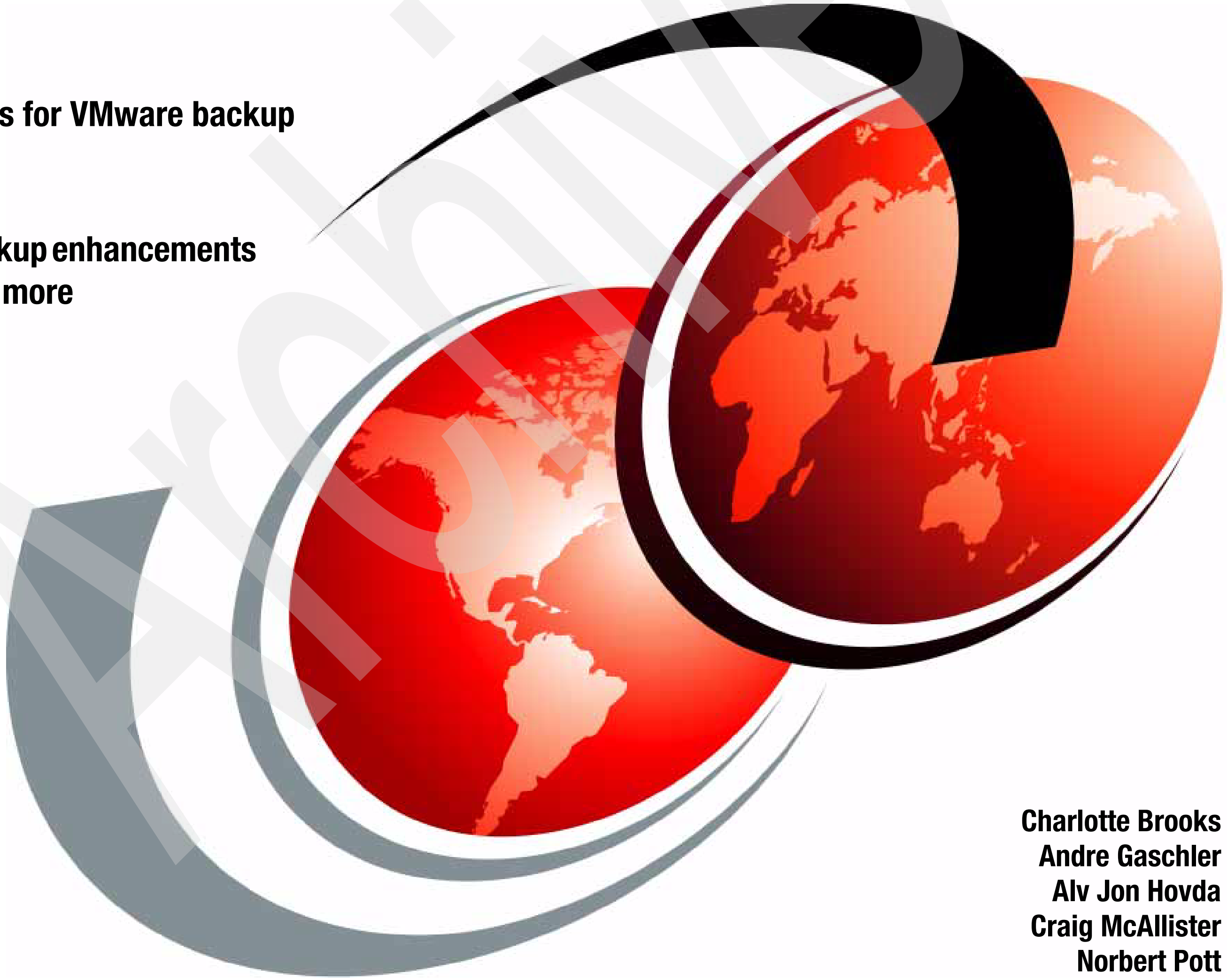
Tivoli. software

IBM Tivoli Storage Manager Versions 5.4 and 5.5 Technical Guide

The new functions in V5.4 and V5.5

Techniques for VMware backup

NDMP backup enhancements and much more



Charlotte Brooks
Andre Gaschler
Alv Jon Hovda
Craig McAllister
Norbert Pott

Redbooks

ibm.com/redbooks

International Technical Support Organization

IBM Tivoli Storage Manager Versions 5.4 and 5.5 Technical Guide

May 2008

SG24-7447-00

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

First Edition (May 2008)

This edition applies to Version 5.4 and Version 5.5 of IBM Tivoli Storage Manager.

Contents

Notices

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

Trademarks

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

Redbooks (logo) ®
AIX 5L™
AIX®
DB2®
Domino®
DS4000™
DS6000™
DS8000™
Enterprise Storage Server®
FlashCopy®
General Parallel File System™
GPFS™
HACMP™
i5/OS®
IBM®
Lotus Notes®
Lotus®
Notes®
OS/400®
POWER™
Redbooks®
SANergy®
SysBack™
System i™
System p™
System Storage™
System z™
Tivoli Enterprise Console®
Tivoli®
TotalStorage®
WebSphere®
z/OS®
zSeries®

The following terms are trademarks of other companies:

mySAP, SAP NetWeaver, SAP R/3, SAP, and SAP logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries.

Oracle, JD Edwards, PeopleSoft, Siebel, and TopLink are registered trademarks of Oracle Corporation and/or its affiliates.

Snapshot, Network Appliance, SnapLock, NetApp, and the NetApp logo are trademarks or registered trademarks of NetApp, Inc. in the U.S. and other countries.

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

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

Intel, Itanium-based, Itanium, Pentium 4, Pentium, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

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

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

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

Preface

This IBM® Redbooks® publication provides details of changes, updates, and new functions in IBM Tivoli® Storage Manager Version 5.4, and Version 5.5. We cover all the new functions of Tivoli Storage Manager that have become available since the publication of *IBM Tivoli Storage Manager Version 5.3 Technical Guide*, SG24-6638.

This book is for customers, consultants, IBM Business Partners, and IBM and Tivoli staff who are familiar with earlier releases of Tivoli Storage Manager and who want to understand what is new in Version 5.4 and Version 5.5. Hence, since we target an experienced audience, we use certain shortcuts to commands and concepts of Tivoli Storage Manager. If you want to learn more about Tivoli Storage Manager functionality, see *IBM Tivoli Storage Management Concepts*, SG24-4877, and *IBM Tivoli Storage Manager Implementation Guide*, SG24-5416.

This publication should be used in conjunction with the manuals and readme files provided with the products and is not intended to replace any information contained therein.

The team that wrote this book

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

Charlotte Brooks is an IBM Certified IT Specialist and Project Leader for Tivoli Storage and System Storage™ Solutions at the International Technical Support Organization, San Jose Center. She has extensive experience with IBM in storage hardware and software support, deployment, and management. She has written many IBM Redbooks publications, and has developed and taught IBM classes in all areas of storage and storage management. Before joining the ITSO, she was the Technical Support Manager for Tivoli Storage Manager in the Asia Pacific Region.

Andre Gaschler is an IT Specialist in the STG European Storage Competence Center Mainz, Germany. He has been working at IBM for 13 years. He has nine years of IT experience, including three years designing and implementing Tivoli Storage Manager Solutions on Windows® and AIX® platforms. He is a certified Tivoli Storage Manager Storage Administrator and a certified Tivoli Storage Manager Deployment Professional.

Alv Jon Hovda is a Senior IT Specialist for IBM ITS Norway. He has 12 years of experience in the Tivoli Storage Manager field, working with a number of different tape libraries. He holds a master's degree in engineering physics. He is Tivoli Storage Manager certified, and his areas of expertise include Tivoli Storage Manager and AIX. He has an author of *Implementing IBM Tape in UNIX Systems*, SG24-6502; *Implementing IBM Tape in Linux and Windows*, SG24-6268; and *Implementing IBM Tape in i5/OS*, SG24-7440.

Craig McAllister is a Tivoli Consultant who has specialized in storage management and closely related topics since 1998. He has worked for IBM United Kingdom since the year 2000 and he supports clients all over the region for presales and services engagements with Tivoli Storage Manager and TotalStorage® Productivity Center.

Norbert Pott is an IBM Tivoli Storage Manager Support Specialist in Germany. He works for the Tivoli Storage Manager back-end support team and provides support to customers worldwide. He has 26 years of experience with IBM, over 17 years of experience in IT, and more than 10 years of experience with the Tivoli Storage Manager product, starting with ADSM Version 2.1.5. His areas of expertise include Tivoli Storage Manager client development skill and in-depth knowledge when it comes to problem determination. He is an author of the IBM Redbooks publications *IBM Tivoli Storage Manager Version 5.3 Technical Workshop Presentation Guide*, SG24-6774; *IBM Tivoli Storage Manager Implementation Guide*, SG24-5416; and *IBM Tivoli Storage Management Concepts*, SG24-4877.

Figure 1 The team: Charlotte, Alv Jon, Andre, Norbert, Craig

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

Jason Basler, Stefan Bender, Janet Bolton, David Derk, Robert Elder, Ken Hannigan, Tashfique Hossain, Harry Husfelt, Alexei Kojenov, David Kosick, Zong Ling, Howard Martin, Don Moxley, Diem Nguyen, Joanne Nguyen, Charles Nichols, Thomas Schreiber, Michael Segapeli, Jack Steitz, Peter Symonds
IBM Tivoli Storage Manager development and test

Steve Fieler, Paul Vasquez
VMware

Gerd Becker
Empalis

Emma Jacobs, Deanna Polm, Sangam Racherla
International Technical Support Organization

Tom and Jenny Chang, and the staff of Garden Inn, Los Gatos

Become a published author

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

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

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

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

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

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

  ibm.com/redbooks

- Send your comments in an e-mail to:

  redbooks@us.ibm.com

- Mail your comments to:

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

Part 1

Introduction to IBM Tivoli Storage Manager

This part gives a brief introduction to IBM Tivoli Storage Manager and associated products.

1

IBM Tivoli Storage Manager overview

This chapter contains an overview of the new functionality and changes that come with the IBM Tivoli Storage Manager Version 5.5, as well as the cumulative changes in the releases since Version 5.3.0, when the previous Technical Guide was published.

In this chapter we provide information about the following major areas of change:

- Overview of server enhancements, additions, and changes
- Overview of client enhancements, additions, and changes
- Additional Tivoli Storage Manager features

For full details, always refer to the announcement letter, and to the installation and user guides for the relevant server. Announcement letters can be found using keyword Tivoli Storage Manager at:

http://www-01.ibm.com/common/ssi/index.wss

You can see the Version 5.5 announcement letter at:

http://www-01.ibm.com/common/ssi/index.wss?DocURL=http://www-01.ibm.com/common/ssi/rep_ca/6/877/ENUSZP07-0476/index.html&InfoType=AN&InfoSubType=CA&InfoDesc=Announcement+Letters&panelurl=index.wss%3F&paneltext=Announcement%20letter%20search

Information about Version 5.4 is found at:

http://www-01.ibm.com/common/ssi/index.wss?DocURL=http://www-01.ibm.com/common/ssi/rep_ca/2/877/ENUSZP07-0102/index.html&InfoType=AN&InfoSubType=CA&InfoDesc=Announcement+Letters&panelurl=index.wss%3F&paneltext=Announcement%20letter%20search

The Tivoli Storage Manager documentation is available at:

http://publib.boulder.ibm.com/infocenter/tivihelp/

1.1 Overview

IBM Tivoli Storage Manager protects data from hardware failures, errors, and unforeseen disasters by storing backup and archive copies on offline and off-site storage. Scaling to protect hundreds to thousands of computers running more than a dozen operating systems, ranging from mobile computers to mainframes and connected together via the Internet, WANs, LANs, or SANs, Storage Manager Extended Edition's centralized Web-based management, intelligent data move and store techniques, and comprehensive policy-based automation all work together to minimize administration costs and the impact to both computers and networks.

Optional software modules allow business-critical applications that must run 24x365 to utilize Storage Manager's centralized data protection with no interruption to their service. Optional software extensions also allow SAN-connected computers to use the SAN for data protection data movements, and provide Hierarchical Storage Management to automatically move unused data files from online disk storage to offline tape storage. Storage Manager Extended Edition expands on the data backup and restore and managed data archive and retrieve capabilities of the base Storage Manager by adding disaster planning capability, NDMP control for NAS filers, and support for large tape libraries. Figure 1-1shows the interrelation of the components in IBM Tivoli Storage Manager.

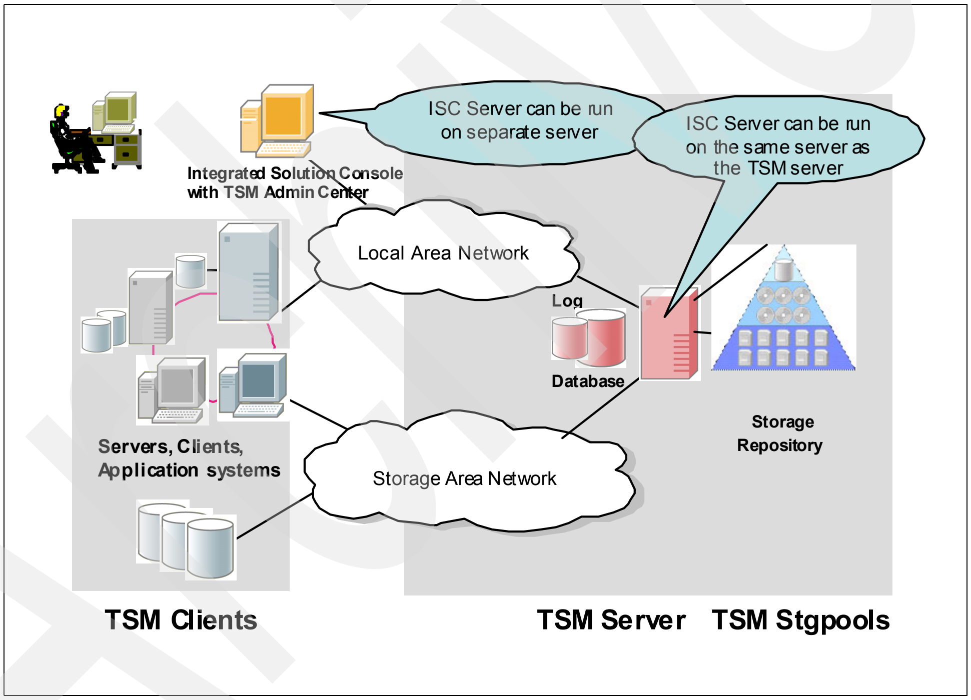

ISC Server can be run on separate server
ISC Server can be run on the same server as the TSM server
Integrated Solution Console with TSM Admin Center
Local Area Network
Log
Database
Storage Repository
Servers, Clients, Application systems
Storage Area Network
TSM Clients
TSM Server
TSM Stgpools

Figure 1-1 How the product components interrelate

Note: The Tivoli Storage Manager Server and the Administration Center can be installed on the same machine. The Administration Center requires a minimum additional 512 MB memory beyond the requirement for the Tivoli Storage Manager Server.

For the latest recommendations on Administration Center installation, use the keyword TSMADMINCENTER when you visit:

http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliStorageManager.html

Disaster preparation and recovery

Local copies of data do not protect against a local disaster. IBM Tivoli Storage Manager Extended Edition facilitates the tracking of the additional copies of your active data that IBM Tivoli Storage Manager creates for safekeeping at an off-site location. This is known as the Disaster Recovery Manager. IBM Tivoli Storage Manager Extended Edition prepares and keeps up to date a text file, the *recovery plan*, which contains detailed recovery steps and automated scripts to recover your server. Should a disaster strike and destroy your storage and computers, this plan and the off-site data copies gets your business back up and running quickly.

1.2 Product positioning

IBM Tivoli Storage Manager and its complementary products provide a comprehensive solution focused on the key data protection activities of backup, archive, recovery, space management, and disaster recovery planning.

IBM Tivoli Storage Manager helps ensure recoverability through the automated creation, tracking, and vaulting of reliable recovery points.

IBM Tivoli Storage Manager Extended Edition provides the following support:

- Base IBM Tivoli Storage Manager (for basic backup-archive using a tape library with up to four drives and 48 slots)
- Disaster Recovery Manager
- NDMP (for selected network-attached storage devices)
- Large tape libraries (more than four drives or 48 slots)

IBM Tivoli Storage Manager for Storage Area Networks and IBM Tivoli Storage Manager for Space Management can be used with either IBM Tivoli Storage Manager or IBM Tivoli Storage Manager Extended Edition.

Additional Tivoli products working in conjunction with Tivoli Storage Manager are described in "IBM Tivoli Storage Manager for products" on page 17.

1.3 Overview of the development timeline

IBM Tivoli Storage Manager started life as ADSTAR Distributed Storage Manager (ADSM). Figure 1-2 shows the release time line for the various versions of ADSM, and its subsequent and present name, IBM Tivoli Storage Manager, up to the current version.

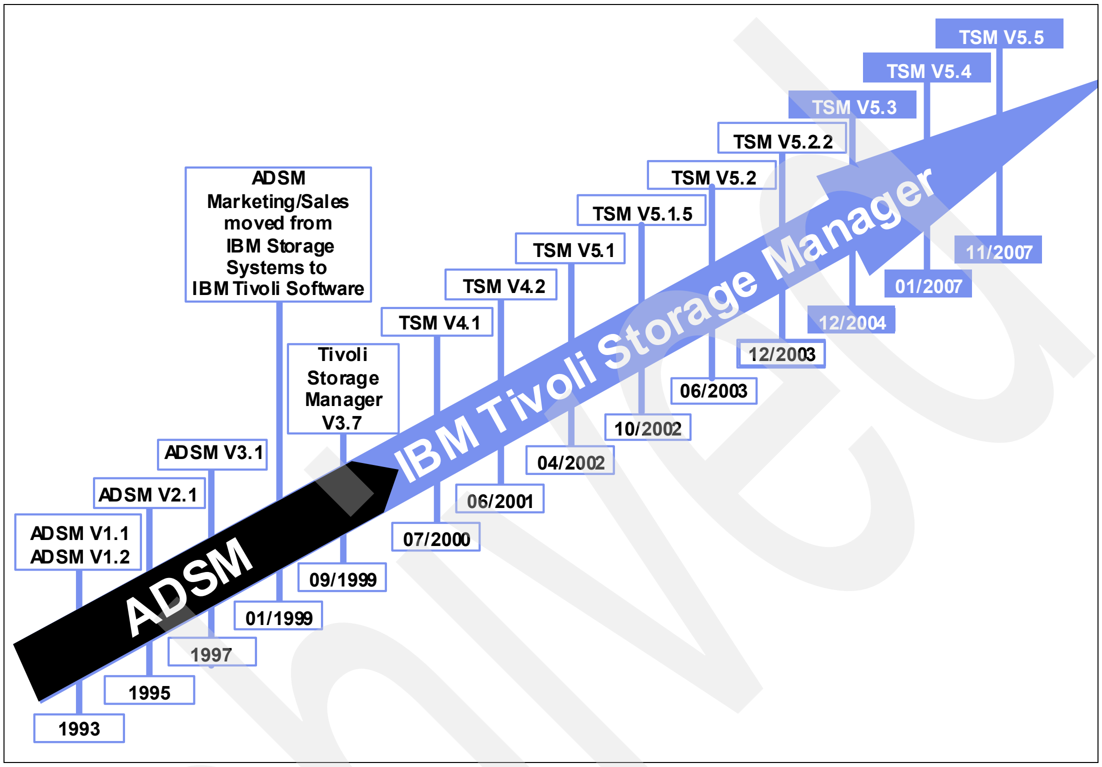


Figure 1-2 IBM Tivoli Storage Manager overall product progression

1.3.1 Client and server version compatibility

Generally, the migration plan for a Tivoli Storage Manager update allows clients and servers to be upgraded at different times. Although Tivoli Storage Manager is very flexible as to the versions of client code used, and also functions with most of the old and unsupported client code versions according to their functionality, it is best to follow these rules for updating to Version 5.n. See the announcement letters for more specific examples related to particular versions.

- A Tivoli Storage Manager Version 5.n-1 client can perform backup, restore, archive, and retrieve functions to a Tivoli Storage Manager Version 5.n server. So, for example, a V5.4 client can back up to a 5.5 server.
- A Tivoli Storage Manager Version 5.n client can perform backup, restore, archive, and retrieve functions to a Tivoli Storage Manager Version 5.n-1 server. So, for example, a V5.5 client can back up to a 5.4 server.
- A Tivoli Storage Manager Version 5.n-1 HSM client can perform migrate and recall functions to a Tivoli Storage Manager Version 5.n server. So, for example, a V5.4 HSM client can migrate to a 5.5 server.
- A Tivoli Storage Manager Version 5.n HSM client can perform migrate and recall functions to a Tivoli Storage Manager Version 5.n-1 server. So, for example, a V5.5 HSM client can migrate to a 5.4 server.

- Data that has been backed up from a Tivoli Storage Manager Version 5.n client to a Tivoli Storage Manager server can be restored using a Tivoli Storage Manager Version 5.n-1 client, except for files backed up using new functionality.
- Data that has been backed up from a Tivoli Storage Manager Version 5.n-2 or Version 5.n-1client to a Tivoli Storage Manager server can be restored using a Tivoli Storage Manager Version 5.n client.
- Tivoli Storage Manager Version 5.n-1 and Version 5.n command-line administrative clients can administer Tivoli Storage Manager Version 5.n-1 and Version 5.n servers.

You will find information about upgrading to and from various versions of Tivoli Storage Manager server and client in the appropriate installation guides. Also search the IBM Technotes database for specific instructions. In particular, you can find a Technote with direct links to the upgrade sections of each manual at:

http://www-1.ibm.com/support/docview.wss?rs=663&uid=swg21287023

1.4 New features overview

This section summarizes the various new features and changes to different Tivoli Storage Manager components. Many of these are considered in greater detail in subsequent chapters of this book. We start with highlights for the most recent version, Version 5.5, then present more specific details of all version releases, including Version 5.3.x, Version 5.4, and Version 5.5, for both server and client.

1.4.1 Highlights for Version 5.5

Version 5.5 includes the following new functions and capabilities:

- Enhanced disk utilization and performance
  - Sequential access disk pool volume concurrent retrieve access
  - Sequential access disk pool migration thresholds
- Windows support enhancements
  - Online image backup on Windows 64-bit operating systems
  - Open file support for Windows 64-bit operating systems
  - Files with up to 8184 character directory names
- Extending beyond traditional backup and recovery
  - Additional device and operating system support for Tivoli Storage Manager for Advanced Copy Services Version 5.5 (available March 28, 2008)
  - VSS Snapshot™ support for Microsoft® SQL Server® with Tivoli Storage Manager for Copy Services Version 5.5
- Server-managed encryption enhancements
  - Tivoli Storage Manager server-managed encryption keys for backup-archive client. Version 5.5 is enhanced so that the Tivoli Storage Manager generates, encrypts, stores, and manages the encryption key in the Tivoli Storage Manager database.
  - Support for AIX Version 6.1 Encrypted File System (EFS) backup. Tivoli Storage Manager Version 5.5 backs up files in either clear text (decrypted by EFS) or in raw (encrypted) format.

- Additional server enhancements
  - VMware Consolidated Backup (VCB) integration. The backup is performed from a VCB backup host, and can manage a virtual machine's backup data as though it had been backed up by a Tivoli Storage Manager client running on the virtual machine.
  - Backup, archive, and space management support for AIX Workload Partitions (WPAR). Tivoli Storage Manager Version 5.5 support enables backup and restore of local partition file data within the global partition using the local partition namespace available within the global partition.
  - SAN device mapping for Virtual Tape Libraries (VTL).
  - Internet Protocol Version 6 (IPV6) support.

1.4.2 Server enhancements, additions, and changes from Version 5.3

This section lists the functional enhancements, additions, and changes for the IBM Tivoli Storage Manager Server introduced from Version 5.3.0.

IBM Tivoli Storage Manager Version 5.3

Tivoli Storage Manager Version 5.2 and Version 5.3 coexisted and were both enhanced with new functionality and device support. Thus, many changes were introduced concurrently in the latest maintenance releases of Version 5.2 and in the early releases of Version 5.3. The changes introduced in Version 5.3.0 onwards are:

- New interface to manage servers: Administration Center
- Accurate SAN device mapping for UNIX® servers
- ACSLS library support enhancements
- Activity log management
- Check-in and check-out enhancements
- Collocation by group
- Communications options
- Database reorganization
- Disk-only backup
- Enhancements for server migration and reclamation processes
- Improved defaults
- Increased block size for writing to tape
- LAN-free environment configuration
- NDMP operations
- Net Appliance SnapLock® support
- Server processing control in scripts
- Simultaneous write inheritance improvements
- Space triggers for mirrored volumes
- Storage agent and library sharing failover
- Support for multiple IBM Tivoli Storage Manager client nodes
- IBM Tivoli Storage Manager scheduling flexibility
- Support for IBM 3592 including WORM
- Support for IBM 3592-2 made available with Version 5.3.3
- Tape encryption was introduced for 3592-2 in Version 5.3.4
- TS3400 Tape Library supported in Version 5.3.5
- General LTO3 support
- LTO WORM support for LTO3 made available from Version 5.3.1.2
- LTO4 support was added with Version 5.3.5
- LTO4 encryption support was available from Version 5.3.5.2
- Several operating platform improvements were introduced in Version 5.3.3.

IBM Tivoli Storage Manager Version 5.4

Tivoli Storage Manager Version 5.3 and Version 5.4 coexist and are both enhanced with new functionality and device support. Thus, many changes were introduced concurrently in the latest maintenance releases of Version 5.3 and in the early releases of Version 5.4. The changes as introduced in Version 5.4.0 onwards are:

- Tape encryption was introduced for 3592-2 in Version 5.4.0.
- TS3400 Tape Library supported in Version 5.4.1.
- LTO4 support was added with Version 5.4.1.
- LTO4 encryption support is available from Version 5.4.1.
- Enhanced storage pooling for faster restore and efficient storage utilization.
- Network Data Management Protocol (NDMP): off-site vaulting, NAS filer to Tivoli Storage Manager server.
- Backup set enhancements.
- Reduced memory utilization on backup.
- Windows Vista® support and Macintosh Intel® support.
- Linux® Logical Volume Manager 2 (LVM2).
- Novell Storage Services (NSS) File System on Open Enterprise (OES) Linux support.
- Data Protection for mySAP™ Administration Assistant enhancements and Universal Naming Convention (UNC).
- Additional device support for IBM Tivoli Storage Manager for Copy Services.
- Additional Volume Shadow Copy Service (VSS) *instant restore* support for Microsoft Exchange.
- Tivoli Storage Manager Administration Center enhancements.
- Improved security for scheduling the Tivoli Storage Manager client.
- Explicit overwrite of deleted data - data shredding.
- Windows 2003 System State backup with Backup Operator Account.
- Tivoli Storage Manager Express upgrade to Tivoli Storage Manager.
- Some server or client support for several operating systems has not been migrated to Version 5.4, most notably Windows 2000.
- With Version 5.4, IBM introduced processor value unit pricing for most Tivoli Storage Manager products.

IBM Tivoli Storage Manager Version 5.5

The Tivoli Storage Manager Version 5.4 and Version 5.5 coexist and are both enhanced with new functionality and device support. Thus, many changes are introduced concurrently in the latest maintenance releases of Version 5.4 and in the early releases of Version 5.5. The key enhancements as introduced in Version 5.5 are:

- Enhanced security with Tivoli Storage Manager server-managed encryption keys for the client
- Efficient use of sequential access disk pools
- Fault-tolerant export and import operations with restartable server-to-server export/import
- Fast, nondisruptive backups with Microsoft Exchange 2007 Volume Shadow Copy Service (VSS) support

- Integrated approach to protecting VMware with VMware Consolidated Backup (VCB) integration
- Broader support for application snapshots with:
  - Tivoli Storage Manager for Advanced Copy Services additional device and operating system support for DB2® snapshots
  - Tivoli Storage Manager for Copy Services VSS support for Microsoft SQL Server
- Backup, archive, and space management support for AIX Workload Partitions (WPAR)
- Internet Protocol Version 6 (IPv6) support
- Online image backup and open file support on Windows 64-bit operating systems
- AIX encrypted file system backup support

1.4.3 Client enhancements, additions, and changes

This chapter lists all the functional enhancements, additions, and changes for the IBM Tivoli Storage Manager Backup Archive Client introduced as of Version 5.3.

IBM Tivoli Storage Manager Version 5.3

Here we list changes introduced with the different maintenance releases of Version 5.3. Additional client support has been added at different maintenance releases, and also some client support has been dropped.

- IBM Tivoli Storage Manager Administration Center.
- The client application commands (**dsmc**, **dsmadmc**) do not run without a writable error log.
- Links from the backup-archive client GUI to the Tivoli Storage Manager and Tivoli Home Pages.
- New options, ERRORLOGMAX and SCHEDLOGMAX, and DSM_LOG environment variable changes.
- Enhanced client encryption.
- Shared memory protocol support extended to Windows and Linux platforms.
- Journal-based backup enhancements.
- Include-exclude enhancements.
- Enhancements to the QUERY SCHEDULE command.
- Dynamic client tracing.
- Client node proxy support (ASNODENAME).
- Java™ GUI and Web client enhancements.
- Support for deleting individual files from the TSM server.
- Open File Support (OFS) enhancements.
- Optimized option default values.
- Tivoli Storage Manager backup-archive client for HP-UX Itanium® 2.
- Offline image backups on Linux zSeries®.
- NDMP file-level restore.

Additions to Tivoli Storage Manager Version 5.3.2 clients are:

- Tivoli Storage Manager Backup-Archive Clients support event-based archive management policies.
- Connects to a Tivoli Storage Manager data retention server for policy-based retention.
- Options for processing access control lists (ACL) by Tivoli Storage Manager UNIX and Macintosh clients.
- New look for Tivoli Storage Manager client readmes.
- NFSV4 file system support (with restrictions) on AIX 5.3 and later.
- Support (with restrictions) of VxFS files using the Linux Backup-Archive clients.

Additions to Tivoli Storage Manager Version 5.3.3 clients are:

- Windows support for backing up NetApp® CIFS Share Definitions.
- JBB support for non-HSM AIX clients.
- Command-line parameters are available for the Tivoli Storage Manager Backup-Archive Java GUI.
- Several Solaris™ 10 support updates.
- Support for testflag MINPWLENGTH to change default length for PASSWORDACCESS GENERATE.
- An important fix for APAR IC49009 was added in Version 5.3.4.

IBM Tivoli Storage Manager Version 5.4

The changes introduced with Version 5.4 are:

- Password file format changes.
- AIX journal support for AIX clients.
- Linux LVM 2 volume manager image backup support.
- SLES 10 support on Linux clients.
- UNIX System Services V1R7 and V1R8 support.
- HACMP™ 5.4 support.
- HSM for WIndows supports failover in a Microsoft Cluster Server environment, automatic backup before migration, and Windows 2003.
- Asianux 2.0 support on Linux x86/x86_64 clients.
- Support for SRVRPREPOSTSCHEDDISABLED, SRVRPREPOSTSNAPDISABLED, and SCHEDRESTRETRDISABLED options.
- Reducing the memory used during the incremental backup function.
- Support for include.fs.
- Tivoli Storage Manager client support for Novell Storage Services file system extended attributes.
- Storage pools on GPFS™ file systems are supported.
- Local zone support for Solaris 10 x86 client.
- Dropped support for HP-UX 11i V1, RHEL 3, SLES 8, AIX Version 5.1, Solaris 8, and UNIX System Services V1R4, V1R5, and V1R6.

IBM Tivoli Storage Manager Version 5.5

Changes introduced with Version 5.5 are listed here:

- Transparent encryption support
- Secure socket layer (SSL) support
- TCP/IP Version 6 support
- AUDITLOGGING and AUDITLOGNAME options
- AIX JFS2 snapshot integration for snapshot-based image backup and snapshot-based file level backup and archive
- AIX JFS2 extended attributes (EA) support
- Support for AIX Encrypted File System (EFS)
- AIX workload partition (WPAR) support
- Solaris ZFS support
- Linux Itanium 2 support
- Red Hat Enterprise Linux 5.0 support
- AIX 6.1 support
- IMAGEGAPSIZE option
- Dropped support for AIX Version 5.2
- HSM for Windows reconciliation and improved storage pool utilization

1.5 Additional functionality overview

This section summarizes the status and new features and changes for different Tivoli Storage Manager components.

- Tivoli Storage Manager for SAN, additions, and changes
- Tivoli Storage Manager HSM for Windows Version 5.5, additions and changes
- Tivoli Storage Manager Space Management, additions and changes
- Tivoli Storage Manager for System Backup and Recovery (SysBack™) Version 6.1

1.5.1 Tivoli Storage Manager for SAN, additions and changes

IBM Tivoli Storage Manager for Storage Area Networks is a feature of Tivoli Storage Manager that enables LAN-free client data movement.

This feature allows the client system to directly write data to, or read data from, storage devices attached to a storage area network (SAN), instead of passing or receiving the information over the network. Data movement is thereby off-loaded from the LAN and from the Tivoli Storage Manager server, making network bandwidth available for other uses. For instance, using the SAN for client data movement decreases the load on the Tivoli Storage Manager server and allows it to support a greater number of concurrent client connections. The storage agent, a component of the feature, makes LAN-free data movement possible.

See also the relevant user guide for your system. For AIX it is *IBM Tivoli Storage Manager for SAN for AIX Storage Agent User's Guide, Version 5.4*, SC32-0129-00.

Enhancements in Version 5.3.0

Enhancements in Version 5.3.0 are:

- ACSLS library sharing is available.
- There is now multiple file system support for FILE device types.
- The minimum I/O to volumes associated with the FILE device class is 256 KB.

> **Note:** For certain tasks (for example, using the DIRMC client option to store directory information, or migrating very small files using the hierarchical space management (HSM) client), you can minimize wasted space on storage volumes in a FILE-type storage pool by specifying the NONBLOCK data format when defining the storage pool. In most situations, however, the NATIVE format is preferred.

Enhancements in Version 5.3.2

There is now LAN-free data movement in z/OS® SAN environments. Volumes are formatted as they are requested.

Enhancements in Version 5.4

The new QUERY DIRSPACE command lets you display the amount of total and available disk space for each directory in a FILE device class.

1.5.2 Tivoli Storage Manager HSM for Windows Version 5.5, additions and changes

IBM Tivoli Storage Manager HSM for Windows provides space management for Microsoft Windows NTFS file systems. File migration policies can be defined by an administrator using the HSM for Windows GUI. File migration eligibility is determined by include and exclude policy criteria such as file type (extension) and various criteria related to the age of a file (creation, modification, last access). HSM for Windows helps free administrators and users from file system pruning tasks. HSM for Windows is designed to assist administrators to more effectively manage Windows NTFS disk storage by automatically migrating files selected based on administrator established policy to less expensive storage devices, while preserving Windows NTFS file accessibility.

See also *IBM Tivoli Storage Manager HSM for Windows Administration Guide, Version 5.5*, SC32-1773, and *Using the Tivoli Storage Manager HSM Client for Windows*, REDP-4126.

Enhancements in Version 5.4

Enhancements in Version 5.4 are:

- Supports failover in a Microsoft Cluster Server environment in either an active/active or standby/active configuration. Support for this high-availability solution ensures that HSM for Windows will continue to migrate files and preserve file accessibility, even in the event of a failover of a node within the cluster.
- Includes an option to automatically invoke a Tivoli Storage Manager backup before files are migrated.
- Supports space management on Windows Server® 2003 R2.

Enhancements in Version 5.5

Enhancements in Version 5.5 are:

- Adds a reconciliation function to reconcile migrated files with files that may have subsequently been moved or deleted from the source file server.
- The integration between HSM for Windows and the backup-archive client has been improved to help ensure that there is always the current file content stored in the backup, even for migrated files.
- Several performance enhancements.

1.5.3 Tivoli Storage Manager for Space Management, additions and changes

The IBM Tivoli Storage Manager for Space Management client for UNIX and Linux (the HSM client) migrates files from your local file system to distributed storage and can then recall the files either automatically or selectively. Migrating files to storage frees space for new data on your local file system and takes advantage of lower-cost storage resources that are available in your network environment.

Tivoli Storage Manager for Space Management is available for AIX JFS2 and GPFS, Linux GPFS, Solaris VxFS, and HP-UX JFS file systems. Also refer to the *IBM Tivoli Storage Manager for Space Management for UNIX and Linux User's Guide, Version 5.5*, SC32-0148-01.

Enhancements in Version 5.3

Enhancements in Version 5.3 are:

- AIX JFS2 support
- Changes to the **dsmmigfs start**, **dsmmigfs stop**, and **dsmmigfs restart** commands (GPFS only)
- Changes to .SpaceMan directory files

Enhancements in Version 5.3.2

Enhancements in Version 5.3.2 are:

- AIX 5L™ Version 5.3 support.
- GPFS Version 2.3 support.
- IBM Tivoli Enterprise Space Management Console (HSM Java GUI) support.
- Option MINstreamfilesize is specific to a file system, and defines the number of bytes that must be recalled before HSM starts streaming data to the requesting application (to ensure a steady stream of data).

Enhancements in Version 5.3.3

Enhancements in Version 5.3.3 are:

- Solaris 10 SPARC Global Zones support.
- Solaris HSM requires VERITAS File system VxFS 4.1.
- The MINMigfilesize option is file-system specific.
- Support for **dsmmigrate** and **dsmrecall** within a GPFS cluster.
- Can use the **dsmdf** command with the -detail option to display information line by line.

Enhancements in Version 5.4

Enhancements in Version 5.4 are:

- Additional platform support:
  - Linux SLES 9, 10, Red Hat 4 GPFS 32-bit OS support
  - Linux SLES 9, Red Hat 4 GPFS 64-bit OS support
  - GPFS 3.1 support with one HSM managed storage pool per file system
  - Solaris VxFS with zones support
  - HACMP Version 5.3
- Supports NFS exported HSM managed file systems on:
  - AIX/JFS2
  - Solaris/VxFS
  - HP-UX/JFS
- Can process a list of files on which to act. The new filelist parameter is available in the HSM commands **`dsmmigrate`**, **`dsmrecall`**, **`dsmls`**, **`dsmattr`**.
- Compatible with AIX journal-based backup.
- JFS file systems are no longer supported.
- The export and import options are obsolete for the **`dsmmigfs`** command.

Enhancements in Version 5.5

Enhancements in Version 5.5 are:

- Increased performance and more efficient memory use.
- Can handle more files in a single namespace.
- GPFS policy-driven migration.
- Scout daemon **`dsmscoutd`** has several new parameters to manage the daemon and to provide information about the file system.
- A Complete File Index (CFI) database is implemented to speed up candidate selection and reconciliation.
- AIX 6.1 WPAR support.
- NFSv4 ACLs support for JFS2 and GPFS 3.2.
- HP-UX IA 64 support.

1.5.4 Tivoli Storage Manager for System Backup and Recovery Version 6.1

IBM Tivoli Storage Manager for System Backup and Recovery (also known as SysBack) provides system administrators and other system users with a simple, efficient way to back up and recover data from a command line or a SMIT menu-driven interface. SysBack lets you recover all or part of the system. SysBack is also flexible. You can install one system installation image to another system with either identical or different hardware configurations, called *cloning*. SysBack can be used as a stand-alone product or in conjunction with a Tivoli Storage Manager server.

Also refer to the *IBM Tivoli Storage Manager for System Backup and Recovery (SysBack) Installation and User's Guide, Version 6.1,* SC23-6543.

Enhancements in Version 6.1

Enhancements in Version 6.1 are:

- Supports the system boot process via CD and DVD devices when recovering the system using data stored in a Tivoli Storage Manager server.
- Supports the use of the Tivoli Storage Manager backup-archive client file-by-file backup data to recover the system during bare machine recovery processing.
- An LVM-only backup option is available for use together with Tivoli Storage Manager backup-archive client backups during the system install processing.
- LVM-only backups that back up just the LVM information for the complete system to CD and DVD, tape, virtual device, Tivoli Storage Manager server, and directory devices. These backups can be used:
  - As boot media
  - To recreate LVM structures in normal mode
  - As a part of the system installation and recovery process when restoring the system using backups generated by the Tivoli Storage Manager backup-archive client
- JFS2 Snapshot backups that create snapshot copies of JFS2 file systems and then use SysBack backup commands to back up those copies.
- New options to limit the amount of volume group, logical volume, file system, and physical disk information collected during a system-level backup.
- New backup option to allow backups to continue even when a missing or invalid backup object is specified to the backup command.
- Enhanced Network Install Debugging options.
- Automatic Backup and Restore Process Logging options.
- Activity Logging option provides an additional level of process information.
- SMIT menu panel to collect detailed environment information for your system and the SysBack product.

2

IBM Tivoli Storage Manager for products

This chapter gives a brief description of the recent changes in the additional IBM Tivoli Storage Manager products:

- Tivoli Storage Manager for Mail (Lotus® Domino®, Microsoft Exchange)
- Tivoli Storage Manager for Databases (Oracle®, Microsoft SQL)
- Tivoli Storage Manager for Enterprise Resource Planning (ERP)
- Tivoli Storage Manager for Advanced Copy Services
- Tivoli Storage Manager for Copy Services

The following previous products are no longer available:

- Tivoli Storage Manager for Hardware (replaced by Tivoli Storage Manager for Advanced Copy Services as of V5.3)
- Tivoli Storage Manager for Application Servers (stabilized at V5.3, end of support September 2008)

For further details about the separate products, see the relevant parts of the Tivoli Storage Manager announcement letters as found using the product keywords, for example, *Tivoli Storage Manager for Mail*, at:

`http://www-01.ibm.com/common/ssi/index.wss`

You can also consult the installation and users guides for the different products and platforms at:

`http://publib.boulder.ibm.com/infocenter/tivihelp`

Note: Be aware that these products have separate license features. Be sure to register these licences to ensure correct behavior.

2.1 IBM Tivoli Storage Manager for Mail

IBM Tivoli Storage Manager for Mail V5.5 consists of the following components:

- Data Protection for Lotus Domino V5.4.2.
- Data Protection for Microsoft Exchange V5.5

2.1.1 Data Protection for Lotus Domino

Data Protection for Domino is an application that backs up and restores Lotus Domino databases and transaction logs. When archival logging is used on the Domino Server, it archives transaction log files and retrieves them as required for database recovery.

Data Protection for Domino helps protect and manage Lotus Domino server data and offers the following actions and functions:

- Back up online Lotus Domino NSF databases.
- Back up and restore DB2-enabled Notes databases when a DB2-enabled Domino server is available.
- Maintain multiple backup versions of Domino databases.
- Archive Lotus Domino transaction log files when archival logging is in effect.
- Restore backup versions of a Lotus Domino database and apply changes since the last backup from the transaction log.
- Restore Domino databases to a specific point in time.
- Restore one or more archived transaction log files.
- Expire database backups automatically based on version limit and retention period.
- Expire archived transaction log files when no longer needed.
- Automate scheduled backups.
- Restore Domino databases to an alternate server or partition.
- Access Data Protection for Domino remotely using the Tivoli Storage Manager Web client.

New features

Data Protection for Lotus Domino V5.4.2 provides these new features:

- Domino DB2 enabled Notes databases

  Domino 8 (or later) provides DB2 as a data store for Domino NSF databases.
- Multiple TCP/IP sessions

  Multiple TCP/IP sessions can be used when backing up Domino NSF databases.

Supported environments

Supported environments are:

- Data Protection for Lotus Domino V5.4.2 for Windows

  Windows 2003 server, 32 bit or 64 bit

- Data Protection for Lotus Domino V5.4.2 for UNIX, Linux, and OS/400®:
  - AIX V5.2 or AIX 5.3 server, 32 bit or 64 bit
  - SUN Solaris 9 or 10, 64 bit
  - Red Hat Enterprise Linux 4 or 5, 32 bit or 64 bit, for x86 or IBM System z™
  - SuSE Linux, SLES 9 or 10, 32 bit or 64 bit, for x86 or IBM System z
  - i5/OS® V5R3 or V5R4, with OS/400 Option 30, QShell Interpreter

2.1.2 Data Protection for Microsoft Exchange Server

Data Protection for Exchange helps protect and manage Exchange Server data by making it easy to perform the following actions:

- Back up Exchange Server storage groups and transaction logs.
- Maintain multiple versions of Exchange Server storage group and transaction log backups.
- Restore storage group and transaction log backups and replay the transaction log files.
- Automatically inactivate previous backups when performing a full backup.

Data Protection for Exchange performs online backups and restores of Microsoft Exchange Server storage groups. With this release, you can perform backups and restores using a command-line interface (CLI) or graphical user interface (GUI).

New features

Data Protection for Exchange V5.5.0 provides these new features:

- Microsoft Exchange Server 2007 support for these operations:
  - Legacy backup
  - Legacy restore
  - VSS Backup
  - VSS Restore
  - VSS Fast Restore
  - VSS Instant Restore
- VERITAS Cluster Server (VCS) support, providing high availability cluster management for Exchange data.
- Microsoft Virtual Server support, providing server virtualization technology for Exchange data. Data Protection for Exchange supports backup and restore operations in a Microsoft Virtual Server environment.

Supported environments

The supported environments are:

- Support in x32 systems is provided for:
  - Microsoft Exchange Server 2003 SP2 or later
  - Windows Server 2003 SP2 or later
  - Windows Server 2003 R2 - SP2 or later
  - Microsoft Virtual Server 2005 R2 SP1 or later

- Support in x64 systems is provided for:
  - Microsoft Exchange Server 2007
  - Windows Server 2003 SP2 or later, x64 edition

2.2 IBM Tivoli Storage Manager for Databases

IBM Tivoli Storage Manager for Databases V5.5 consists of the following components:

- Data Protection for Microsoft SQL Server V5.5
- Data Protection for Oracle V5.4.1

IBM Tivoli Storage Manager for Databases performs online or offline backups of databases to IBM Tivoli Storage Manager. This integration maximizes the protection of data, thus providing a comprehensive storage management solution.

2.2.1 Data Protection for Microsoft SQL Server

These are the changes and improvements for Data Protection for Microsoft SQL Server V5.5:

- Support for Microsoft SQL Server 2005
- Microsoft Volume Shadow Copy Service (VSS) support
- VERITAS Cluster Server support
- Microsoft Virtual Server support
- Usability enhancements

The support may vary for the different versions of hardware. Always consult the announcement letter or the actual installation and user guide for additional details.

Supported environments

The supported environments are:

- Support in x32 systems is provided for:
  - Microsoft SQL Server 2000 SP4 or later: Standard or Enterprise Editions
  - Microsoft SQL Server 2005 SP2 or later: Standard or Enterprise Editions
  - Windows Server 2003 with SP2 or later: Standard, Enterprise, or Data Center editions
  - Windows Server 2003 R2 with SP2 or later: Standard, Enterprise, or Data Center editions

  Note that Microsoft Cluster Server (MSCS) and VERITAS Cluster Server (VCS) IBM System z 800 or 900 server are supported.

  Note that Microsoft Virtual Server 2005 R2 SP1 or later is supported
- Support in x64 systems is provided for:
  - Windows Server 2003 with SP2, or later: Standard, Enterprise, or Data Center x64 editions
  - Windows Server 2003 R2 with SP2, or later: Standard, Enterprise, or Data Center x64 editions
  - Microsoft Virtual Server 2005 R2 SP1 or later
  - Microsoft SQL Server 2005 SP2 or later: Standard or Enterprise x64 Editions

  Note that Microsoft Cluster Server (MSCS) and VERITAS Cluster Server (VCS) are supported.

- Support in IA64 systems is provided for:
  - Windows Server 2003 with SP2 or later: Standard, Enterprise, or Data Center Editions for Itanium-based™ systems
  - Microsoft SQL Server 2000 with SP4, or later: Standard or Enterprise 64-bit Editions
  - Microsoft SQL Server 2005 with SP2, or later: Standard or Enterprise Editions for Itanium-based systems

2.2.2 Data Protection for Oracle

The changes and improvements for Data Protection for Oracle include the following:

- Tivoli Storage Manager API password management (UNIX)

  Set a new password to be automatically generated.
- SuSE Linux Enterprise Server 10 (UNIX)
- Changed documentation example for scheduler procedure (Windows)

Supported environments

Data Protection for Oracle V5.4.1 is supported for AIX, HP-UX, Linux, and Solaris SPARC environments. Java V1.4.2 is generally required with these systems. For Solaris x86 and Windows environments, the Data Protection for Oracle version supported is V5.3.3.

The support will be for different versions of Oracle depending on operating system and version. Always consult the announcement letter or the actual installation and user guide for each product for additional details. The operating system support is as follows.

- Support in Data Protection for Oracle V5.4.1 in AIX environments is provided for:
  - AIX V5.2 (64 bit) or AIX V5.3 (32 bit or 64 bit)
  - AIX V5.2 (64 bit) or AIX V5.3 (64 bit) with GPFS V2.1 or V2.2 and HACMP/ES V4.5, V5.1, or V5.2
- Support in Data Protection for Oracle V5.4.1 in HP-UX environments is provided for:
  - HP-UX on PA-RISC: 64-bit HP-UX 11iv2
  - HP-UX on Itanium: HP-UX 11iv2 or 11iv3
- Support in Data Protection for Oracle V5.4.1 in Linux environments is provided for:
  - Linux on x86
    - SUSE Linux SLES 9 or 10
    - Red Hat Enterprise Linux 4
    - Asianux 2.0
  - Linux on x86_64
    - SUSE Linux SLES 9 or 10
    - Red Hat Enterprise Linux 4
    - Asianux 2.0
  - Linux on Power
    - SUSE Linux SLES 9
    - Red Hat Enterprise Linux 4

  - Linux on z64
    - SUSE Linux SLES 9, 64 bit
    - Red Hat Enterprise Linux 4, 64 bit
- Support in Data Protection for Oracle V5.4.1 in Solaris environments is provided for:
  - 32-bit Solaris 9 or Solaris 10
  - 64-bit Solaris 9 or Solaris 10
- Support in Data Protection for Oracle V5.3.3 in Solaris x86 environments is provided for:
  - Solaris on x86: Solaris 10 (32 bit)
  - Solaris on x86_64: Solaris 10 (64 bit)
- Support in Data Protection for Oracle V5.3.3 in Windows environments is provided for:
  - Windows on x32: Windows Server 2003 (32 bit)
  - Windows on x64: Windows Server 2003 (64 bit)
  - Windows on IA64: Windows Server 2003 (64 bit)

2.3 IBM Tivoli Storage Manager for ERP

Specifically designed and optimized for the SAP® environment, IBM Tivoli Storage Manager for Enterprise Resource Planning (ERP) provides automated data protection, reduces the CPU performance impact of data backups and restores on the SAP server, and greatly reduces the administrator workload necessary to meet data protection requirements. Tivoli Storage Manager for ERP builds on the SAP BRTools, a set of database administration functions integrated with SAP for database control and administration.

The Storage Manager for ERP software module allows multiple SAP servers to utilize a single Tivoli Storage Manager server to automatically manage the backup of SAP data. As the intelligent interface to the SAP database, Tivoli Storage Manager for ERP is SAP certified in heterogeneous environments, supporting large-volume data backups, data recovery, data cloning, and disaster recovery of multiple SAP servers.

The supported versions of Oracle or DB2 are as supported by SAP, with some restrictions depending on operating system and version. Always consult the announcement letter or the actual installation and user guide for each product for additional details.

New features

These are the new functions and improvements in IBM Tivoli Storage Manager for ERP V5.5. Note that SAP AG has discontinued the use of the term *mySAP* in favor of *SAP*.

- Data Protection for SAP for DB2
  - If DB2 V8.2 or later has been installed and the DB2 instance started, the DP for SAP installation program automatically sets the VENDOROPT parameter in the DB2 configuration and optionally also sets the LOGARCHMETHn and LOGARCHOPTn parameters to enable DB2 log archiving via DP for SAP.
  - The following enhancements have been added to the Administration Assistant:
    - The internal database can now be a DB2 database.
    - Thresholds can be defined to enable alerting under certain conditions via display indicators and e-mail.

  - The '-x' option of BackOM can be used in conjunction with the password option '-c password' to modify the password on all partitions of a partitioned database.
  - Internet Protocol V6 (IPv6) is supported by Data Protection for SAP and the Administration Assistant. Unless otherwise noted, any specification of an IP address in this document can be an IPv4 or IPv6 address. Examples continue to use the IPv4 address |format.
  - Information about the DB2 Single System View (SSV) capability is provided.
  - Information is provided about storing control files on remote Windows shares.
- Data Protection for SAP for Oracle
  - Thresholds can be defined in the Administration Assistant.
  - The Administration Assistant database can now be managed by IBM DB2 as an alternative to Apache Derby.
  - Internet Protocol V6 (IPv6) is supported by Data Protection for SAP and the Administration Assistant. Unless otherwise noted, any specification of an IP address in this document can be an IPv4 or IPv6 address. Examples continue to use the IPv4 address |format.
  - The RMAN information previously included as a separate chapter has been distributed to other sections of the book as appropriate.
  - Information is provided about storing control files on remote Windows shares.

Supported environments

Tivoli Storage Manager for ERP V5.5 support is provided for HP-UX with the DB2 UDB. For all other environments, the support is defined at the V5.4 level.

Data Protection for SAP V5.5 for Oracle is supported in the following environments:

- For AIX at V5.4.0.1
  - AIX V5.2 (64 bit) at ML02
  - AIX V5.3 (64 bit)
- For Solaris

  Solaris 9 or 10 (64 bit)
- For HP-UX V5.4.0
  - HP-UX 11i V2.0 (64 bit)
  - HP-UX 11i V3.0 (64 bit)
- For HP-UX Itanium V5.4.0
  - HP-UX 11i V2 (64 bit)
  - HP-UX 11i V3.0 (64 bit)
- For Linux x86 at V5.4.0
  - Red Hat Enterprise Advanced Server 4 or 5 (32 bit)
  - SLES 9 or 10 (32 bit)
- For Linux Itanium at V5.4.0

  SLES 9 (64 bit)
- For Linux x86_64 at V5.4.0
  - Red Hat Enterprise Advanced Server 4 or 5
  - SLES 9 or 10

- For Linux POWER™ at V5.4.0
  - Red Hat Enterprise Advanced Server 4 or 5
  - SLES 9 or 10
- For Windows 32 bit at V5.4.1

  Windows 2003 Enterprise Edition (32 bit or 64 bit)
- For Windows x64 at V5.4.1

  Windows 2003 Enterprise Edition (64 bit)

Data Protection for SAP V5.5 for DB2 UDB is supported in the following environments. The DB2 versions are as supported by SAP, with some restrictions. Always consult the newest announcement letter.

- For AIX at V5.4.0.1
  - AIX V5.2 (32 bit or 64 bit) at ML02
  - AIX V5.3 (64 bit)
- For HP-UX at V5.5

  HP-UX 11i V3.0 (64 bit)
- For Linux x86 at V5.4.:
  - Red Hat Enterprise Advanced Server 4 or 5
  - SLES 9 or 10 (Native Posix Threading Library)
- For Linux x86_64 at V5.4.0
  - Red Hat Enterprise Advanced Server 4 or 5
  - SLES 9 or10
- For Linux POWER at V5.4.0
  - Red Hat Enterprise Advanced Server 4 or 5
  - SLES 9 or10
- For Solaris SPARC at V5.4.0

  Solaris 9 or10 (64 bit)
- For Solaris x86_64 at V5.4.1

  Solaris 10 (64 bit)
- For Windows 32 bit at V5.4.0.1
  - Windows 2000 Server (32 bit), Advanced Server, Datacenter Server SP3
  - Windows 2003 Enterprise Edition (32 bit or 64 bit)
- For Windows x64_64 at V5.4.0.1

  Windows 2003 Enterprise Edition (64 bit)

2.4 IBM Tivoli Storage Manager for Hardware - end of support

Tivoli Storage Manager for Hardware (5608-APH) had end of support at V5.2, and was functionally replaced by Tivoli Storage Manager for Advanced Copy Services (5608-ACS) V5.3.

2.5 IBM Tivoli Storage Manager for Advanced Copy Services

Tivoli Storage Manager for Advanced Copy Services was introduced with the Tivoli Storage Manager V5.3 release, replacing Tivoli Storage Manager for Hardware.

Always consult the announcement letter or the actual installation and user guide for each product for additional details. For the Tivoli Storage Manager V5.5 announcement letter look up:

http://www-01.ibm.com/common/ssi/index.wss?DocURL=http://www-01.ibm.com/common/ssi/rep_ca/6/877/ENUSZP07-0476/index.html&InfoType=AN&InfoSubType=CA&InfoDesc=Announcement+Letters&panelurl=index.wss%3F&paneltext=Announcement%20letter%20search

IBM Tivoli Storage Manager for Advanced Copy Services uses copy services functions provided in the underlying storage hardware to perform the following tasks:

- Back up Oracle or DB2 databases to a local storage system or to a Tivoli Storage Manager server.
- Restore databases from local storage or Tivoli Storage Manager storage.

IBM Tivoli Storage Manager for Advanced Copy Services V5.5 contains the following components, either new or updated in this release:

- Data Protection for Snapshot Devices for DB2 Advanced Copy Services V5.5 (new) - supports IBM System Storage N series
- Data Protection for Disk Storage and SAN Volume Controller for Oracle V5.3.1.3
- Data Protection for Snapshot Devices for mySAP V5.4.1.1
- DB2 UDB and Hardware Devices Snapshot Integration Modules V5.3.4.8

Three of these components provide support for DB2 in different environments:

- For releases of DB2 prior to 9.5 in an SAP environment, use Data Protection for Snapshot Devices for mySAP V5.4.1.1.
- For releases for DB2 prior to V9.5 in a non-SAP environment, use DB2 UDB and Hardware Devices Snapshot Integration Modules V5.3.4.8.
- For DB2 V9.5 in either an SAP or non-SAP environment, use Data Protection for Snapshot Devices for DB2 ACS V5.5.

2.5.1 Short description

Tivoli Storage Manager for Advanced Copy Services helps protect mission-critical data that requires 24x7 availability. It offers ready-to-use, product-based solutions designed to implement high-efficiency backup and restore processes and helps eliminate backup-related performance issues.

- Provides a *near zero-impact* data backup and *near instant* recovery solution and helps eliminate backup-related performance impact on the production database or ERP servers
- Integrates snapshot capabilities with Tivoli Storage Manager and its data protection components for IBM DB2 UDB, Oracle, and mySAP
- Couples hardware-based and software-based FlashCopy® function of IBM Storage Subsystems (ESS, DS8000™, DS6000™, and SVC) with Tivoli Storage Manager

- Works with and requires either Tivoli Storage Manager or Tivoli Storage Manager Enterprise Edition and the corresponding data protection module—IBM Tivoli Storage Manager for Databases or IBM Tivoli Storage Manager for ERP
- Operating systems supported: primarily AIX, in some functions also Linux

DP for Snapshot Devices supports the following IBM systems:

- Enterprise Storage Server® (ESS) Model 800
- IBM System Storage DS6000
- IBM System Storage DS8000
- IBM System Storage SAN Volume Controller (SVC)
- IBM System Storage N series

One (and only one) of these systems must be configured for DP for Snapshot Devices, and the database must reside fully on this system. However, the use of an SVC allows it to manage one or more ESS or DS systems (as well as non-IBM storage hardware) within the framework of the SVC configuration.

Tivoli Storage Manager for Advanced Copy Services for DB2 UDB minimizes the impact of performing backups of DB2 UDB databases using Tivoli Storage Manager on database server systems. Tivoli Storage Manager for Advanced Copy Services for DB2 UDB off-loads the transfer of backup data from a production database server to a backup server. The DB2 UDB database must reside on storage subsystem volumes. Tivoli Storage Manager for Advanced Copy Services for DB2 UDB features high-efficiency backup and recovery of business-critical applications. This feature minimizes backup-related downtime and user disruption on the production system host.

2.5.2 Data Protection for Snapshot Devices for DB2 Advanced Copy Services V5.5 with FlashCopy Devices

In this section we discuss Data Protection for Snapshot Devices for DB2 Advanced Copy Services V5.5 with FlashCopy Devices.

Features

The FlashCopy Restore (FlashBack Restore) functionality of Data Protection for Snapshot Devices provides a fully automated tool for a fast restore of business-critical databases. Data Protection for Snapshot Devices exploits the Copy Services functionality (as implemented for the storage system) for both FlashCopy Backup and FlashCopy Restore.

The operating environment consists of DB2 running on an AIX server attached to one of the supported storage systems. This AIX server is the production system. Another AIX server, the backup system, is also attached to the same storage system to back up FlashCopy or snapshot copies of the production system to the Tivoli Storage Manager server. This is done by the concerted action of the two DP for Snapshot Devices.

Data Protection for ERP is required to perform the actual backup or restore to or from the Tivoli Storage Manager server.

Supported systems

Always consult the announcement letter or the actual installation and user guide for each product for additional details. There will be a number of requirements as to supported versions of additional products like the Oracle, Tivoli Storage Manager, Java, C++, and so on.

- Hardware
  - System p™ or p5 - two systems may be required.
  - IBM ESS, DS6000 or DS8000 storage system.
  - Storage system with a processor supported by the minimum required CIM agent.
  - IBM System Storage SAN Volume Controller V2.1 to V4.2.0.
- Software - basic
  - AIX V5.3 with 64-bit AIX kernel, at TL5 SP3 (minimum).
  - DB2 V9.5 for Linux, UNIX, and Windows.
  - DB2 Advanced Copy Services is part of the IBM DB2 High Availability (HA) Feature, and you must have a license for the DB2 HA Feature.

2.5.3 Data Protection for Snapshot Devices for DB2 Advanced Copy Services V5.5 with N series Snapshot Devices

In this section we discuss Data Protection for Snapshot Devices for DB2 Advanced Copy Services V5.5 with N series Snapshot Devices.

Features

This provides support for SAN-based IBM System Storage N series devices. These devices have an inherent snapshot capability that includes allocating the target disks. For system details, refer to *IBM System Storage N series*, SG24-7129.

Data Protection for ERP is required to perform the actual backup or restore to or from the Tivoli Storage Manager server.

Supported systems

Always consult the announcement letter or the actual installation and user guide for each product for additional details. There are a number of requirements as to supported versions of additional products like the DB2, Tivoli Storage Manager, Java, C++, and so on.

- Hardware
  - System p or p5 with AIX - two systems may be required.
  - x64 (64-bit AMD64 and Intel EM64T processors) with Linux (new in V5.5).
  - IBM System Storage N series.
- Software - basic
  - DB2 Advanced Copy Services is part of the IBM DB2 High Availability
  - AIX V5.3 with 64-bit AIX kernel, at TL5 SP3 (minimum)
  - Red Hat Enterprise Linux (RHEL) 4 Update 4, or RHEL 5
  - SUSE Linux Enterprise Server (SLES) 9 Service Pack 3, or 10 SP1

2.5.4 Data Protection for Disk Storage and SAN Volume Controller for Oracle V5.3.1.3

In this section we discuss Data Protection for Disk Storage and SAN Volume Controller for Oracle V5.3.1.3.

Features

Data Protection for FlashCopy for Oracle provides the following functions:

- Backs up Oracle databases with minimal impact and downtime on the production Oracle database server
- Restores Oracle databases from Tivoli Storage Manager storage, using RMAN
- Performs a quick restore using FlashCopy

Data Protection for Oracle is required.

Supported systems

Always consult the announcement letter or the actual installation and user guide for each product for additional details. There are a number of requirements as to supported versions of additional products like the DB2, Tivoli Storage Manager, Java, C++, and so on.

- Hardware
  - Two IBM System p compatible servers
  - IBM DS6000 or DS8000 storage system
  - Storage system with a processor supported by the minimum required CIM agent
  - IBM SAN Volume Controller V2.1 to V4.1
- Software - basic
  - Oracle Database 9i 9.2 (64 bit) (single or Real Application Cluster) 10g (64 bit) (single or Real Application Cluster)
  - AIX V5.2 (32 bit or 64 bit) ML9 or later or AIX V5.3 (32 bit or 64 bit) ML5 or later

2.5.5 Data Protection for Snapshot Devices for mySAP V5.4.1.1

In this section we discuss Data Protection for Snapshot Devices for mySAP V5.4.1.1 with FlashCopy Devices.

Features

Data Protection for FlashCopy for mySAP provides some active functions for interacting with DB2 or Oracle and Data Protection for mySAP, and some passive functions. For DB2 there are two major components: **`tdphdwdb2`** and **`splitint`**.

The active functions include:

- Highly available DB2 or Oracle database backup or restore using FlashCopy
- Integrating with DB2 functions or the Oracle **`brbackup`** functions to support running copy services functions, including FlashCopy and withdraw
- Keeping the progress of the Data Protection for FlashCopy functions in a housekeeping file to monitor the proper sequential usage of the functions
- Sending information to the Data Protection for mySAP administration assistant while Data Protection for FlashCopy is running

The passive functions include:

- With DB2, monitoring a running FlashCopy process when the FlashCopy is invoked with COPY, INCR options
- With Oracle integration with Tivoli Storage Manager Media Management functions

- Seamless augmentation of the functions of Data Protection for mySAP
- Centrally administered and scheduled backup operations

Data protection for ERP is required.

Supported systems

Always consult the announcement letter or the actual installation and user guide for each product for additional details. There are a number of requirements as to supported versions of additional products like the DB2, Tivoli Storage Manager, Java, C++, and so on.

- Hardware
  - Two IBM System p compatible servers
  - IBM ESS, DS6000 or DS8000 storage system
  - A system with a minimum required CIM agent
  - SAN Volume Controller V2.1 to V4.1
- Software - basic
  - SAP R/3® Release 4.5B to 4.6D or SAP NetWeaver® with SAP kernel Releases 6.10 to 7.00
  - AIX V5.2 (32 bit or 64 bit) ML9+ and PTF U488817 for APAR IY44637 or AIX V5.3 (32 bit or 64 bit) ML5+ and fix for PMR 28176,070,729 referring to AIX V5.2 fix IY62648
  - Either Oracle or DB2 UDB with SAP (See the announcement letter for further details.)

2.5.6 Data Protection for Snapshot Devices for mySAP V5.4.1.1 with N series devices

In this section we discuss Data Protection for Snapshot Devices for mySAP V5.4.1.1 with N series devices.

Features

Data Protection for FlashCopy for mySAP provides some active functions for interacting with DB2 or Oracle and Data Protection for mySAP, and some passive functions.

These functions are also available with the N series devices.

Data protection for ERP is required.

Supported systems

Always consult the announcement letter or the actual installation and user guide for each product for additional details. There are a number of requirements as to supported versions of additional products like the DB2, Tivoli Storage Manager, Java, C++, and so on.

- Hardware
  - Two IBM System p compatible servers
  - IBM System Storage N series
- Software - basic
  - SAP R/3 Release 4.5B to 4.6D or SAP NetWeaver with SAP kernel release 6.10 to 7.00
  - AIX V5.2 (32 bit or 64 bit) ML5+ and PTF U488817 for APAR IY44637 or AIX V5.3 (32 bit or 64 bit) ML1+ and fix for PMR 28176,070,729 referring to AIX V5.2 fix IY62648

  - Either Oracle or DB2 UDB with SAP (See the announcement letter for further details.)

2.5.7 DB2 UDB Integration Module V5.3.4.8

In this section we discuss DB2 UDB Integration Module V5.3.4.8.

Features

The DB2 UDB Integration Module is used in conjunction with the Hardware Devices Snapshot Integration Module and the Tivoli Storage Manager backup-archive Client. The following functions are provided:

- Multi-partition DB2 database and multiple backup server support
- Centralized configuration
- Integration with Tivoli Storage Manager command-line interface
- Multiple backup host support
- Multiple snapshot backups
- Policy-based management of snapshot backups

Supported systems

Always consult the announcement letter or the actual installation and user guide for each product for additional details. There are a number of requirements as to supported versions of additional products like Tivoli Storage Manager.

- Hardware: two or more System p or compatible servers
- Software - basic
  - DB2 UDB V8.2 (64 bit) or later
  - AIX V5.2 (32 bit or 64 bit) or V5.3 (32 bit or 64 bit)

2.5.8 Hardware Devices Snapshot Integration Module V5.3.4.8

The Hardware Devices Snapshot Integration Module works in conjunction with the DB2 UDB Integration Module and the Tivoli Storage Manager backup-archive Client.

Supported systems

Always consult the announcement letter or the actual installation and user guide for each product for additional details. There are a number of requirements as to supported versions of additional products like Tivoli Storage Manager, CIM agents, and so on.

- Hardware
  - IBM ESS, DS6000, or DS8000 with advanced FlashCopy feature and supported CIM agent
  - A storage system with a processor supported by the minimum required CIM agent
  - SAN Volume Controller V2.1 to V4.1
- Software - basic
  - SAP R/3 Release 4.5B to 4.6D or SAP NetWeaver with SAP kernel release 6.10 to 7.00
  - AIX V5.2 (34 bit or 64 bit) ML9 or later or V5.3 (34 bit or 64 bit) ML5 or later
  - Either Oracle or DB2 UDB with SAP (See the announcement letter for further details.)

2.6 IBM Tivoli Storage Manager for Copy Services

IBM Tivoli Storage Manager for Copy Services V5.5 contains the following components:

- Microsoft Exchange VSS Integration Module V5.5
- Microsoft SQL VSS Integration Module V5.5 - new in this version
- Hardware Devices Snapshot Integration Module V5.5

Short description

Tivoli Storage Manager for Copy Services supports both Microsoft Exchange and Microsoft SQL Server.

The Microsoft Exchange VSS Integration Module is used in conjunction with Data Protection for Microsoft Exchange and the Tivoli Storage Manager Windows client. Together, these implement the VSS requestor interface to drive the Microsoft Volume Shadow Copy Services for backup and recovery of Exchange. With the addition of the Hardware Devices Snapshot Integration Module, you can also get the VSS Instant Restore function on SVC, DS6000, and DS8000. This component is simply a license file. When this component is installed, it enables VSS operations within the Data Protection for Microsoft Exchange interfaces. Since the Microsoft Exchange VSS Integration Module requires Data Protection for Exchange, refer to the requirements for Data Protection for Exchange.

The Microsoft SQL VSS Integration Module is used in conjunction with Data Protection for Microsoft SQL and the Tivoli Storage Manager Windows client. Together, these implement the VSS requestor interface to drive the Microsoft Volume Shadow Copy Services for backup and recovery of SQL. With the addition of the Hardware Devices Snapshot Integration Module, you can also get the VSS Instant Restore function on SVC, DS6000, and DS8000. This component is simply a license file. When this component is installed, it enables VSS operations within the Data Protection for Microsoft SQL interfaces. Since the Microsoft SQL VSS Integration Module requires Data Protection for SQL, refer to the requirements for Data Protection for SQL.

The Hardware Devices Snapshot Integration Module is used in conjunction with the Tivoli Storage Manager Windows client. Together, these implement the VSS Instant Restore functionality. Since the Hardware Devices Snapshot Integration Module requires the Tivoli Storage Manager V5.5 Windows client, refer to the requirements for the Tivoli Storage Manager V5.5 backup-archive Windows client.

Supported versions

The following software combinations are supported for basic VSS operations:

- Microsoft Windows 2003 (32 bit) with Exchange Server 2003
- Microsoft Windows 2003 (x64) with Exchange Server 2007
- Microsoft Windows 2003 (32 bit) with SQL Server 2005
- Microsoft Windows 2003 (x64) with SQL Server 2005
- Any VSS provider that is supported by the Microsoft rules for VSS providers

Tivoli Storage Manager supports any VSS Provider that strictly adheres to the Microsoft VSS Provider interface. Specifically, the following IBM storage products have been tested:

- IBM System Storage DS4000™, DS6000, and DS8000
- IBM System Storage SAN Volume Controller
- IBM N series, as well as NetApp FAS series

2.7 References

Generally, refer to the manuals and IBM Redbooks available for each of the discussed products. Some of these are also listed below.

For Data Protection for mail, refer to the following manuals:

- *Data Protection for Microsoft Exchange Server Installation and User's Guide,* SC32-9058
- *Data Protection for Microsoft SQL Server Installation and User's Guide,* SC32-9059
- *Data Protection for Lotus Domino for UNIX, Linux, and OS/400 Installation and User's Guide*, SC32-9056
- *Data Protection for Lotus Domino for Windows, Installation and User's Guide,* SC32-9057

For Data Protection for databases, refer to the following manuals:

- *Data Protection for Oracle for UNIX and Linux Installation and User's Guide,* SC32-9064
- *Data Protection for Oracle for Windows Installation and User's Guide,* SC32-9065

For Data Protection for ERP, refer to the following manuals:

- *Data Protection for SAP Installation and User's Guide for DB2,* SC33-6341
- *Data Protection for SAP Installation and User's Guide for Oracle*, SC33-6340

For Advanced Copy Services, refer to the following manuals and IBM Redbooks:

- *IBM Tivoli Storage Manager for Advanced Copy Services*, SG24-7474
- *Data Protection for Snapshot Devices for mySAP, Installation and User's Guide for Oracle,* SC33-8207
- *Data Protection for Snapshot Devices for mySAP Installation and User's Guide for DB2 UDB,* SC33-8208
- *Data Protection for FlashCopy Devices for Oracle Installation and User's Guide,* GC32-1772
- *IBM Tivoli Storage Manager Advanced Copy Services for DB2 Installation and User's Guide for DB2 UDB,* GC32-1780

For Copy Services, refer to the following manuals:

- *Using IBM Tivoli Storage Manager to Back Up Microsoft Exchange with VSS, SG24-7373*
- *Data Protection for Microsoft Exchange Server Installation and User's Guide,* SC32-9058
- *Data Protection for Microsoft SQL Server Installation and User's Guide,* SC32-9059

Part 2

Tivoli Storage Manager V5.3.x enhancements

This part describes enhancements for IBM Tivoli Storage Manager clients and servers since the V5.3.0 release. It also provides an introduction to a new product at that time, Tivoli Continuous Data Protection for Files.

3

Tivoli Storage Manager Version 5.3.x server enhancements

This chapter discusses major new V5.3 features and enhancements delivered in the IBM Tivoli Storage Manager server after V5.3.0.

3.1 3592 second generation - TS1120

Tivoli Storage Manager now supports 3592 generation 2 drives and media. Generation 2 drives use the same media as generation 1 drives, but provide higher performance and capacity than generation 1 drives because data is written at a higher density to tape.

Mixing the two generations of 3592 drives in a single library can create potential media problems because generation 1 drives cannot read generation 2 media. For example, if the two generations are mixed and an operation requires Tivoli Storage Manager to verify a generation 2 volume label using a generation 1 drive, the operation will fail. If possible, upgrade all drives in your library to generation 2.

Generation 2 3592 drives can be integrated into 349x, ACSLS and SCSI libraries.

3.2 Administration Center changes

The Administration Center, introduced in V5.3 as a replacement for the administrative Web interface, now supports disaster recovery manager functions. The Tivoli Storage Manager server must be licensed for IBM Tivoli Storage Manager Extended Edition to take advantage of these functions.

V5.3 of the Administration Center required you to click the **Go** button after making a selection from the table action list. The Go button has been eliminated, reducing the number of clicks required to perform an action.

3.3 WORM support

Tivoli Storage Manager supports DLT WORM and LTO WORM drives and tape media. Because they permit write operations only, WORM (write once, read many) media protects critical data from accidental or deliberate deletion.

In order to utilize DLT and LTO WORM, you need to define a specific WORM device class, as shown in Example 3-1.

Example 3-1 Define LTO device class with WORM support

```
DEFINE DEVCLASS <class name> LIBRARY=<library name> DEVTYPE=LTO WORM=YES
```

Tivoli Storage Manager can only distinguish WORM media from rewritable media when the media is mounted. All WORM media needs to either be checked in with CHECKLABEL=YES or labeled with the CHECKIN parameter specified. Any media that is checked in without mounting in the drive is considered rewritable.

3.4 Automatic volume labelling in non-SCSI libraries

The AUTOLABEL parameter for automatic volume labeling support can now be used for non-SCSI libraries, as an alternative to the DSMLABEL or LABEL LIBVOLUME commands.

Using the AUTOLABEL parameter allows volumes to be labeled as they are needed for backup operations and eliminates having to label all volumes before they are checked into Tivoli Storage Manager.

The DEFINE LIBRARY and UPDATE LIBRARY commands with AUTOLABEL can be used for the following additional library types: 349X, ACSLS, EXTERNAL, and MANUAL. The syntax changes are shown in Example 3-2.

Example 3-2 Update a library with the AUTOLABEL parameter

```
UPDATE LIBRARY <library name> AUTOLABEL=YES
```

The AUTOLABEL parameter defaults to YES for all non-SCSI libraries and to NO for SCSI libraries.

In a shared library environment, the library manager is responsible for labeling volumes, so there is no need to specify the AUTOLABEL parameter for a library type of SHARED.

4

Tivoli Storage Manager Version 5.3.x client enhancements

This chapter describes updates and additional functionality that became available for Tivoli Storage Manager V5.3.x clients after publication of *IBM Tivoli Storage Manager Version 5.3 Technical Guide*, SG24-6638.

4.1 Common client enhancements

The following updates are available in updates to V5.3 client code (and later releases).

4.1.1 New options for client access control list (ACL) processing

The Tivoli Storage Manager clients that support the backup of ACL information check every file during a backup to see whether the ACLs have changed. This can impact performance if there are a lot of files.

Two client options are available to control the processing of access control lists by Tivoli Storage Manager on platforms supporting ACL backup. Using these options limits the client’s functionality and data protection. Therefore, you should carefully evaluate turning on these options.

- SKIPACL

  When set to YES (the default is NO), the client skips ACL processing completely. No ACL data is backed up or restored. You should use this option only when ACLs are not defined on the file system or when the loss of data contained in the ACLs during restore is acceptable. The file mode permissions (rwx) continue to be backed up and restored as before.

- SKIPACLUPdatecheck

  During a backup, the Tivoli Storage Manager client by default performs an ACL checksum and size comparison before and after backup, and during incremental processing. It compares the ACL checksum from the previous backup with the current ACL to detect ACL updates. Set this option to YES (the default is NO) to disable the check for ACL updates. The current ACL data will be backed up if the file is selected for backup due to other reasons. If only ACLs are updated on a file, the next incremental backup will not recognize this ACL update and it will not be backed up.

> **Note:** SKIPACL=YES overrides SKIPACLUPDATECHECK settings.

4.1.2 Tivoli Storage Manager backup-archive Java GUI (dsmj)

The Tivoli Storage Manager backup-archive Java GUI (**dsmj**) now accepts command line parameters, such as Java runtime options specified with -X. This means that you can, for example, modify the Java heap size as shown in Example 4-1.

Example 4-1 Command-line parameters for dsmj

```
dsmj -Xms64m -Xmx512m -se=<servername>
```

4.1.3 Changed default password length for PASSWORDACCESS GENERATE

When using the PASSWORDACCESS GENERATE option, the Tivoli Storage Manager client automatically generates new passwords with a default length of 63 characters when the old password expires. If you do not want a 63-character password, you can cut the length back to the normal eight characters or to the minimum length of a password on the server using the testflag MINPWLENGTH. For example, add `testflag minpwlength:8` to dsm.opt to set the minimum password length to 8.

4.2 AIX-specific client enhancement

This enhancement only applies to the AIX client.

Journal-based backup (JBB) for AIX non-HSM clients

Journal-based backup, as an alternative to traditional progressive incremental backup, under certain circumstances, can increase backup performance. Beginning with Tivoli Storage Manager V5.3.3, JBB-backup is supported for AIX non-HSM clients. It was previously available for Windows clients. For more information about JBB, see *IBM Tivoli Storage Management Concepts*, SG24-4877.

4.3 Windows-specific client enhancements

These enhancements only apply to the Windows client.

4.3.1 IBM Tivoli Storage Manager HSM for Windows

IBM Tivoli Storage Manager HSM for Windows is a policy-based management system that became available with Tivoli Storage Manager V5.3.2 in October 2005. You can use it to migrate Windows files transparently from their original location to Tivoli Storage Manager storage, based on certain criteria. Files are recalled transparently from the server whenever required on the client.

You can migrate individual files, parts of Windows file systems, or complete file systems to a Tivoli Storage Manager server. Migrated files appear on the local file system as they did before they were migrated, except they occupy less disk space. Migrated files can be accessed like any other file, opened and updated.

IBM Tivoli Storage Manager HSM for Windows reduces the amount of effort required in manually managing client file space. It is designed to defer the need to purchase additional disk storage by automatically and transparently migrating rarely accessed files to less-expensive offline or near-line storage, while the files most frequently used remain in the local file system.

For detailed information, see *Using the Tivoli Storage Manager HSM Client for Windows*, REDP-4126. Tivoli Storage Manager V5.4 and V5.5 include some important enhancements and new functions for IBM Tivoli Storage Manager HSM for Windows, as described in Chapter 16, “HSM for Windows V5.4” on page 205, and Chapter 23, “HSM for Windows V5.5” on page 311.

4.3.2 Support for NetApp CIFS share definitions

The Tivoli Storage Manager Windows client can back up and restore NetApp CIFS share definitions. Note that the share definition includes the share permissions that are set on the filer. You can back up the CIFS share definition under the root directory, the mapped CIFS share, or the UNC name. This support requires that the NetApp filer is running DATA ONTAP software, which presents CIFS shares to remote clients as ordinary remote NTFS shares.

CIFS/NFS support enables you to take advantage of Tivoli Storage Manager progressive incremental backup, off-site vaulting, storage pool migration, collocation, and the Tivoli Storage Manager server data management capabilities.

With the capability to back up CIFS shares, you can choose between two methods for backing up and recovering NetApp filers:

- Image-based backup of the filer using Network Data Management Protocol (NDMP).
- Use the Tivoli Storage Manager backup-archive client to back up and restore remote shares or mounted volumes defined on the NetApp filer through common file sharing protocols.

A Tivoli Field Guide comparing the two methods, *Backing up Network Appliance Network Attached File Servers with Tivoli Storage Manager,* is available at:

`http://www-1.ibm.com/support/docview.wss?uid=swg27007516`

4.4 Apple Macintosh specific client enhancements

These enhancements only apply to the Apple Macintosh client.

4.4.1 Changing HFS paths to UNIX paths

The Tivoli Storage Manager Macintosh Client now uses UNIX file paths for options, schedules, and file system names on the Tivoli Storage Manager server. By default, the UNIX mount point is used to create file spaces on the server.

4.4.2 Access control list support

Beginning with Mac OS X 10.4.3, access control lists are fully supported by the Tivoli Storage Manager V5.3.3 Macintosh Client.

4.4.3 Extended attribute support

The Tivoli Storage Manager Macintosh client can back up and restore extended attribute data. The extended attribute data is automatically backed up with each object that has extended attributes.

Tivoli Storage Manager supports HFS, HFS+, HFSX, UFS, UDF, and ISO 9600 file systems, as defined in Table 4-1.

Table 4-1 Supported file systems with Tivoli Storage Manager Apple Macintosh client

File system	Tivoli Storage Manager support
Mac OS Standard (HFS)	▶ Case-insensitive, but case preserving ▶ Supports creation and modification dates as metadata ▶ Supports aliases ▶ 32-character limit for folder and file names
MAC OS Extended (HFS+)	▶ Case-insensitive, but case preserving ▶ Supports creation and modification dates as metadata ▶ Supports aliases ▶ 255-character limit for folder and file names
MAC OS Extended, Case-sensitive (HFSX)	▶ Case-sensitive ▶ Supports creation and modification dates as metadata ▶ Supports aliases ▶ 255-character limit for folder and file names

File system	Tivoli Storage Manager support
Mac OS Xsan (XSAN)	► Case-sensitive ► Supports modification dates as metadata ► Supports aliases and symbolic links ► 255-cCharacter limit for folder and file names
UNIX File System (UFS)	► Case-sensitive ► Supports modification dates as meta data ► Supports aliases and symbolic links ► 255-character limit for folders and file names
Universal Disk Format (UDF)	► The Universal Disk Format for DVD volumes ► Recognized as removable media
ISO 9660	► The standard format for CD-ROM volumes ► Recognized as removable media

The UFS and HFSX file systems are case-sensitive, whereas the HFS+ file system is case-insensitive but is case-preserving. Files backed up from a UFS or HFSX file system (case-sensitive) will not be restored properly to an HFS+ file system (case-insensitive) file system. For example, on a UFS file system, files Afile and afile are seen as different files. However, on a HFS+ file system the two files are seen as identical.

> **Note:** If case-sensitive HFSS or UFS file systems are used, it is very important that the data from the HFSX or UFS file system is not backed up to an HFS+ file system on the Tivoli Storage Manage server. Either a new name must be used on the system or the existing file space on the Tivoli Storage Manager server must to be renamed.

For example, consider a system that has a file system named Macintosh HD, and this system is repartitioned with a case-sensitive HFSX file system. Either the Macintosh HD file system on the Tivoli Storage Manager server needs to be renamed, or a new name must be used on the local system. If this is not done, Tivoli Storage Manager mixes the HFSX case-sensitive data with the HFS+ case-insensitive data that is already stored on the Tivoli Storage Manager server.

Aliases and symbolic links are backed up. However, Tivoli Storage Manager does not back up the data that the symbolic links point to.

> **Note:** When files backed up from an HFS volume are restored to a UFS volume, the resource forks do not have the correct owner. This can be corrected by using the `chown` command on the resource fork file.

4.5 Solaris-specific client enhancements

These enhancements only apply to the Solaris client.

4.5.1 Tivoli Storage Manager for Space Management (HSM) for Solaris update

The Solaris HSM client now supports VERITAS VxFS V4.1 and Solaris 10 SPARC (globalzone only).

4.5.2 Zones support for Solaris 10 platforms

Zones support has been added for the following Solaris 10 platforms: |

- Solaris 10 x86 32-bit and 64-bit limited support
  - Global zone only; local zones with 5.4 and newer
  - UFS only
  - TCP-IP only, no LAN-Free
- Solaris 10 SPARC Local Zones

The standard backup and archive operations can be performed from each local zone, just as these operations can be performed on any Solaris system without zoning.

4.6 HP UX specific client enhancement

This enhancement applies only to the HP backup-archive client.

HP-UX V11i V2 support

The Tivoli Storage Manager V5.3 backup-archive client supports HP-UX 11i V2.

5

Complementary products: Tivoli Continuous Data Protection for Files

The latest trend in the evolution of file backup is real-time protection, and Tivoli Continuous Data Protection for Files (CDP) delivers a compelling solution offering a unique blend of continuous data protection and scheduled data protection in a single product.

This chapter provides an introduction to CDP and to basic usage of the product, as well as links to external resources discussing the product in detail.

5.1 Introduction

Businesses today are increasingly concerned with protecting their data. Losing key business information can hamper productivity, delay projects, and divert resources and calls to the help desk. It can also harm organizations when they face regulatory scrutiny. In fact, many businesses today are legally required to use formal data protection.

Data corruption is an increasing concern, and companies are asking for better recovery-point capabilities. Often the most valuable files are those that users are working on currently, and it is often critical to be able to roll these back to a specific point in time. In addition, companies need sophisticated policy-based data management that enables them to focus on data with the most business value.

Most companies have solutions for protecting enterprise data in place, but data residing on workstations and mobile computers is often underprotected. According to some industry experts this data makes up to 60% of all corporate data. Loss of data here can significantly impact productivity and viability.

Here Tivoli Continuous Data Protection for Files comes in as a real-time, continuous data protection solution. You can deploy it to file servers, workstations, and user end points. Instead of waiting for a scheduled interval, Tivoli Continuous Data Protection for Files backs up the most important files the moment that they are created or saved, in real time. Backup versions are created transparently, eliminating any backup window. Less important files can still be backed up periodically on a scheduled basis.

To protect your files against corruption, file loss, system loss, or accidental deletion and make them available for date-based restore, Tivoli Continuous Data Protection for Files creates version-based copies of files. These copies can be stored on:

- Local disk for protection even when not connected to a network
- Network file system for remote-machine protection
- Tivoli Storage Manager or Tivoli Storage Manager Express for use in more enterprises where there is already such an infrastructure in place
- WebDAV server remote backup location provided by an Internet Service Provider (ISP)

You can back up to and restore from any of those locations, as shown in Figure 5-1 on page 47.

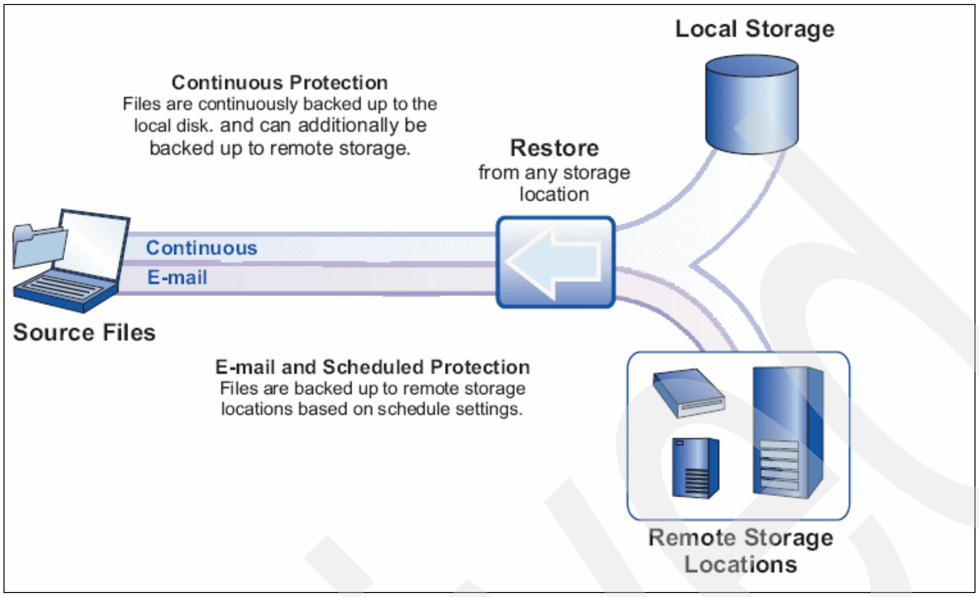

Local Storage
Continuous Protection
Files are continuously backed up to the local disk. and can additionally be backed up to remote storage.
Restore
from any storage location
Continuous
E-mail
Source Files
E-mail and Scheduled Protection
Files are backed up to remote storage locations based on schedule settings.
Remote Storage Locations

Figure 5-1 CDP storage locations: local and remote

Tivoli Continuous Data Protection for Files versions copies of the files to a local self-managed cache, deleting old versions to make room for new versions. In addition, it enables you to specify a remote file server or Tivoli Storage Manager for off-machine protection when a user is connected, so real-time backups still occur. Tivoli Storage Manager provides offsite copies of backup data for vaulting, auditable disaster recovery plan, and tape and media management.

With Tivoli Continuous Data Protection for Files, you can optimize recovery times for file servers and user end points. Typically, a file server is backed up once a night, and the degree of difference between the recoverable data and the latest version of the file can be significant if many changes are made between backups.

You can configure Tivoli Continuous Data Protection for Files to replicate changes to files. This meets the definition of continuous data protection established by the Storage Networking Industry Association (SNIA). Whenever a file is modified, it will be replicated to disk or tape (local or remote) according to the policy that you set and how the solution is deployed. You can easily restore the versions of the file that you need with minimized recovery times.

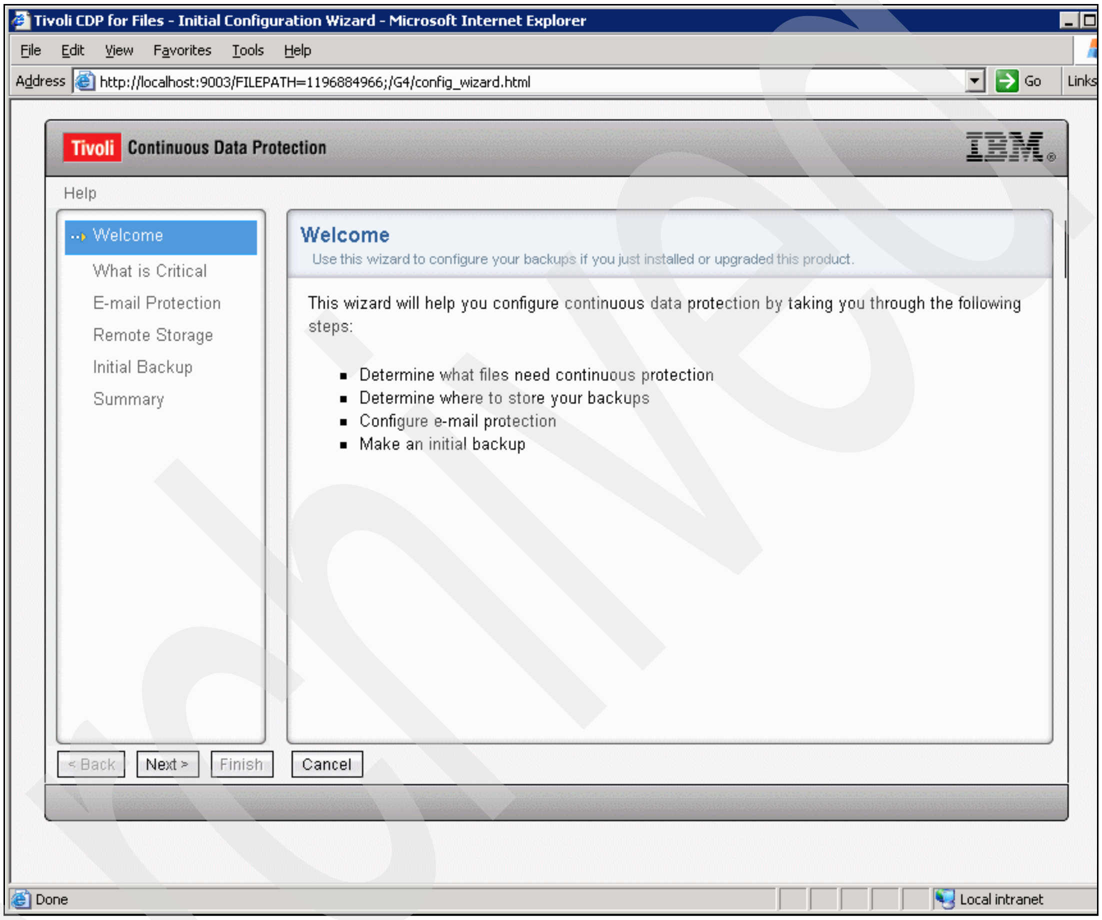
Tivoli Continuous Data Protection for Files is easy to configure and deploy. It can be installed and configured silently. Updated versions of Tivoli Continuous Data Protection for Files or centralized configurations and policies can also be automatically updated from a central location.

In addition, you can take advantage of the software’s vault features to secure files without administrator intervention. You can simply create folders and define a length of time for file retention, and drag-and-drop, copy, or save files to the appropriate defined folder. Those files cannot then be deleted or altered for the defined time period.

5.2 Implementation

Detailed discussion of Tivoli Continuous Data Protection for Files is beyond the scope of this book. Here we show you a basic default installation and configuration and provide images of the simplified user interface as available with CDP V3.1.2. For more information, see *Deployment Guide Series: Tivoli Continuous Data Protection for Files V3.1*, SG24-7423.

1. Once the installation is completed a welcome window and wizard is displayed, as shown in Figure 5-2. The wizard guides you through the backup configuration. Click **Next**.



http://localhost:9003/FILEPATH=1196884966;/G4/config_wizard.html

Welcome

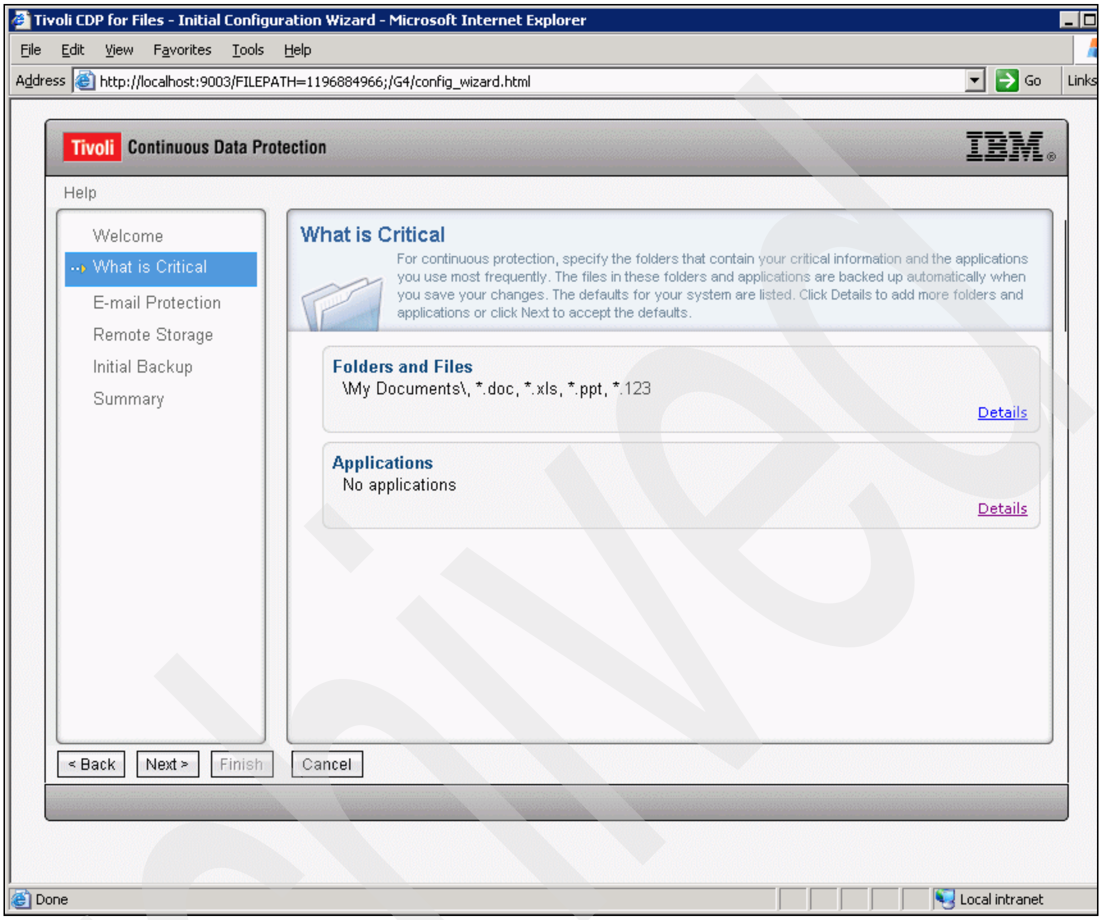
Use this wizard to configure your backups if you just installed or upgraded this product.

This wizard will help you configure continuous data protection by taking you through the following steps:

- Determine what files need continuous protection
- Determine where to store your backups
- Configure e-mail protection
- Make an initial backup

Figure 5-2 CDP Welcome wizard

2. On the next window (Figure 5-3 on page 49) you define the files, folders, and application data that you want to include and exclude for your backup operation. Click **Details** for Folders and Files.



http://localhost:9003/FILEPATH=1196884966;/G4/config_wizard.html

What is Critical

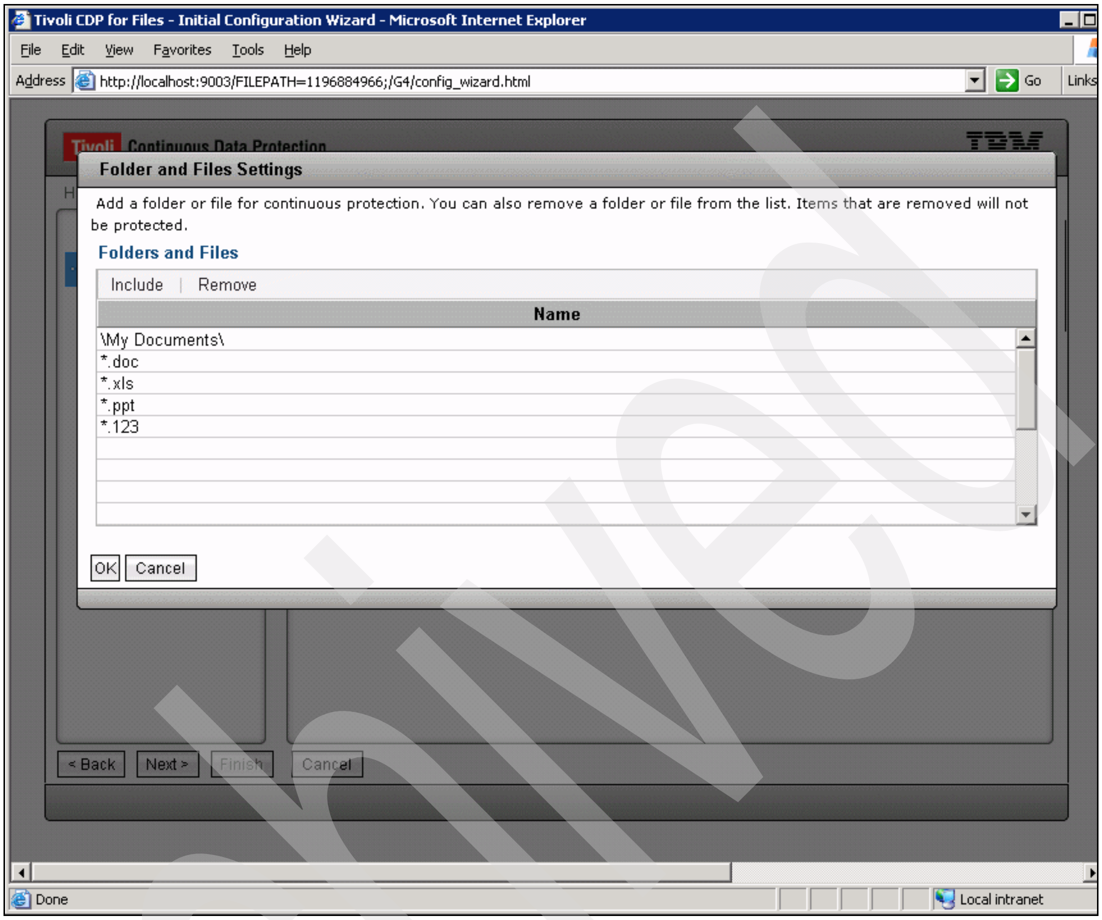
For continuous protection, specify the folders that contain your critical information and the applications you use most frequently. The files in these folders and applications are backed up automatically when you save your changes. The defaults for your system are listed. Click Details to add more folders and applications or click Next to accept the defaults.

Folders and Files
\My Documents\, *.doc, *.xls, *.ppt, *.123
Details

Applications
No applications
Details

Figure 5-3 CDP: What is Critical Window

3. Use the Folders and Files Settings window (Figure 5 on page 51) to define the files or folders for continuous data protection.


Tivoli CDP for Files - Initial Configuration Wizard - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://localhost:9003/FILEPATH=1196884966;/G4/config_wizard.html
Go
Links
Tivoli Continuous Data Protection
IBM
Include | Remove
OK Cancel
< Back Next > Finish Cancel
Done
Local intranet

Folder and Files Settings

Add a folder or file for continuous protection. You can also remove a folder or file from the list. Items that are removed will not be protected.

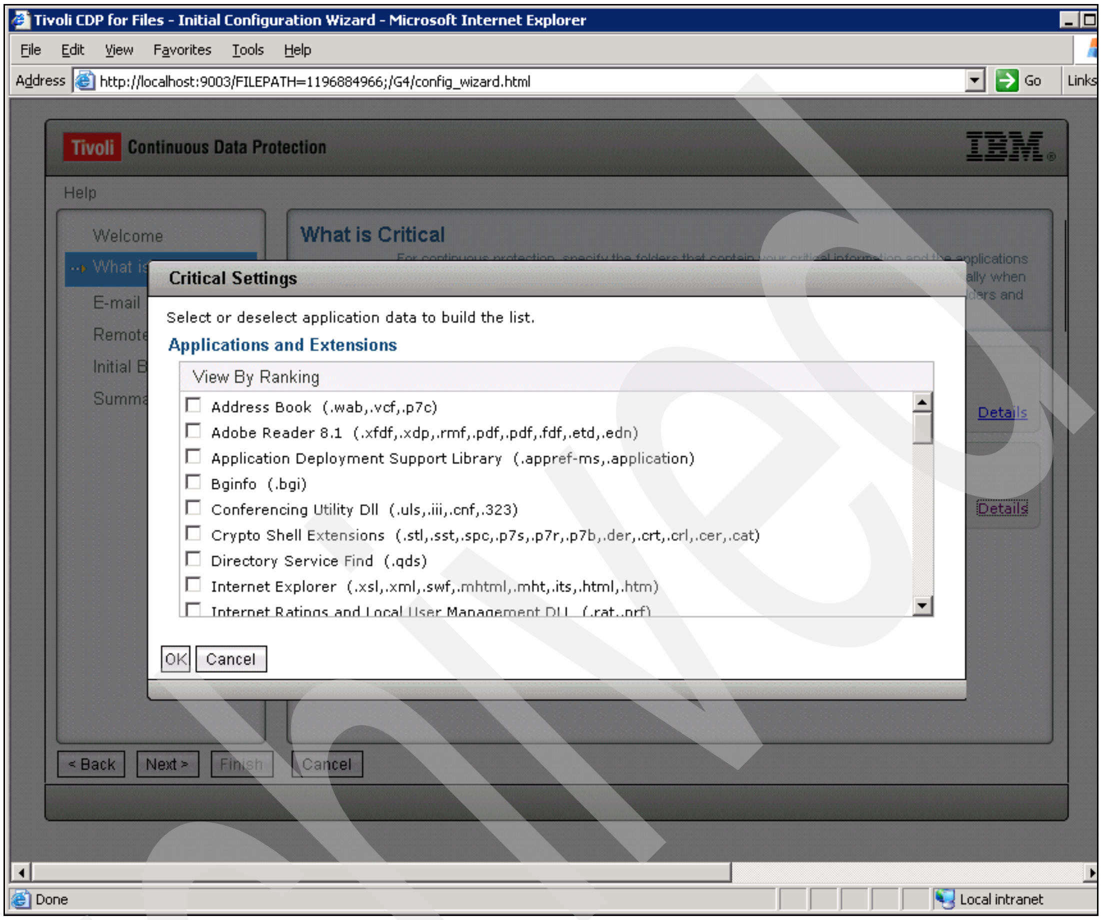
Folders and Files

Name
\My Documents\
*.doc
*.xls
*.ppt
*.123

Figure 5-4 CDP: Folder and Files Settings

4. When you have made your selections, click **OK**. You will return to Figure 5-2.

5. Click **Details** for Applications. In the panel shown in Figure 5-5 on page 51, you can define which application data you want to include in the backup. Select and deselect from the list provided, and click **OK**.


Tivoli CDP for Files - Initial Configuration Wizard - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://localhost:9003/FILEPATH=1196884966;/G4/config_wizard.html
Go Links
Tivoli Continuous Data Protection
IBM
Help
Welcome
What is
E-mail
Remote
Initial B
Summa
What is Critical
Details
Details
&lt; Back
Next &gt;
Finish
Cancel
Done
Local intranet

Critical Settings

Select or deselect application data to build the list.

Applications and Extensions

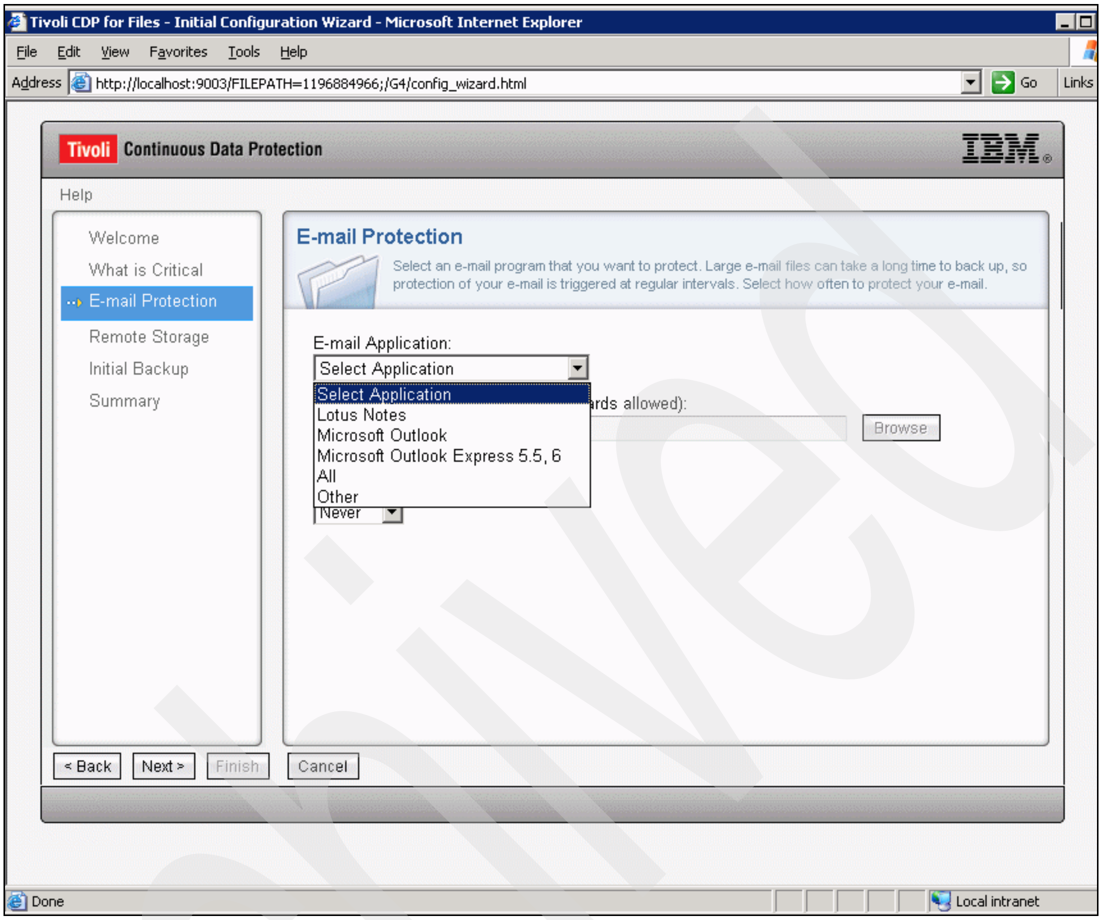
View By Ranking

□ Address Book (.wab,.vcf,.p7c)
□ Adobe Reader 8.1 (.xfdf,.xdp,.rmf,.pdf,.pdf,.fdf,.etd,.edn)
□ Application Deployment Support Library (.appref-ms,.application)
□ Bginfo (.bgi)
□ Conferencing Utility Dll (.uls,.iii,.cnf,.323)
□ Crypto Shell Extensions (.stl,.sst,.spc,.p7s,.p7r,.p7b,.der,.crt,.crl,.cer,.cat)
□ Directory Service Find (.qds)
□ Internet Explorer (.xsl,.xml,.swf,.mhtml,.mht,.its,.html,.htm)
□ Internet Ratings and Local User Management DLL (.rat,.nrf)

OK Cancel

Figure 5-5 CDP: critical settings, applications, and extensions

6. Again you will return to the window shown in Figure 5-2. Click **Next**. In the E-mail Protection window (Figure 5-6 on page 52) you can configure your e-mail backup settings.


Tivoli CDP for Files - Initial Configuration Wizard - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://localhost:9003/FILEPATH=1196884966;/G4/config_wizard.html
Go Links
Tivoli Continuous Data Protection
IBM
Help
Welcome
What is Critical
E-mail Protection
Remote Storage
Initial Backup
Summary
rds allowed):
Browse
Never
< Back
Next >
Finish
Cancel
Done
Local intranet

E-mail Protection

Select an e-mail program that you want to protect. Large e-mail files can take a long time to back up, so protection of your e-mail is triggered at regular intervals. Select how often to protect your e-mail.

E-mail Application: Select Application

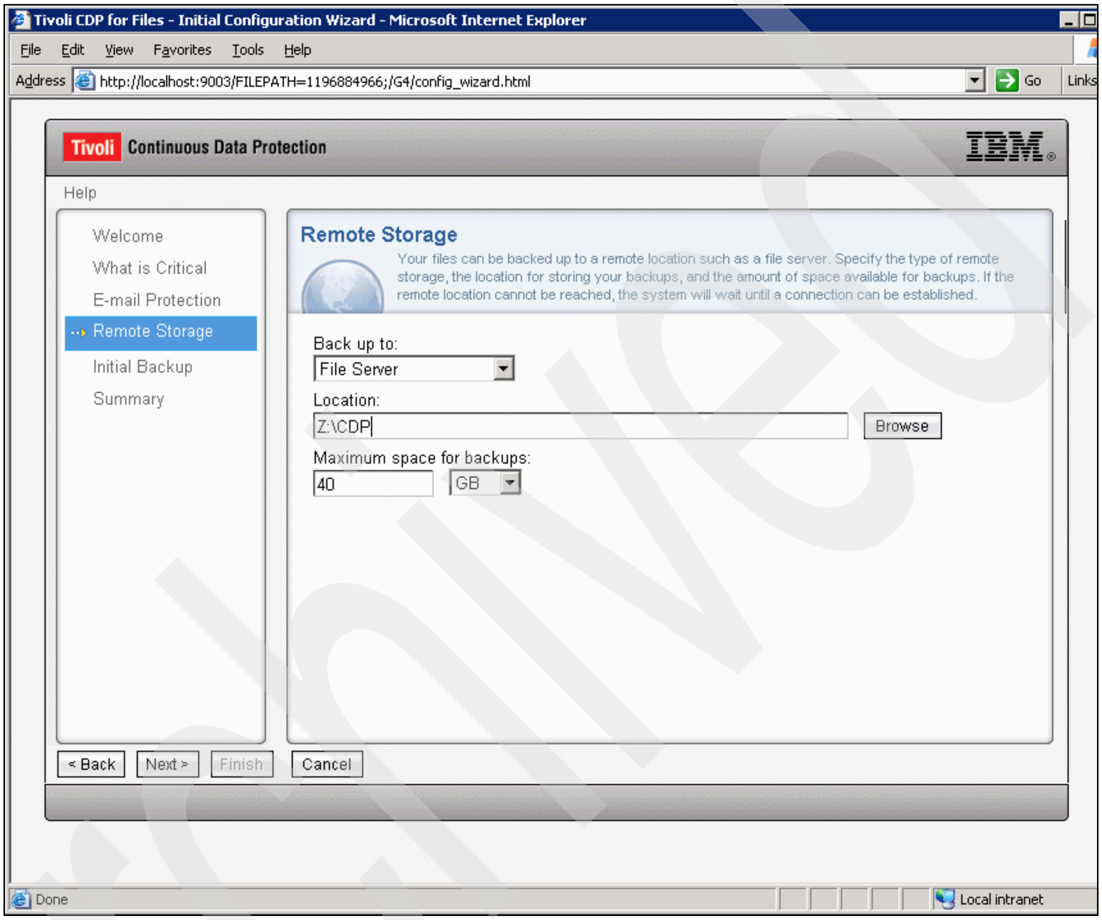
- Select Application
- Lotus Notes
- Microsoft Outlook
- Microsoft Outlook Express 5.5, 6
- All
- Other

Figure 5-6 CDP: e-mail protection

7. Choose from the list of supported applications, specify the e-mail application data folder, and define how often you want your e-mail data to be processed. Once completed click **Next**.

8. On the Remote Storage window (Figure 5-7 on page 53), you can define where to store your data. You can select from:

   – External Storage
   – File Server
   – Tivoli Storage Manager
   – Web server (WebDAV)


Tivoli CDP for Files - Initial Configuration Wizard - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://localhost:9003/FILEPATH=1196884966;/G4/config_wizard.html
Go
Links
Tivoli Continuous Data Protection
IBM
Help
Welcome
What is Critical
E-mail Protection
Remote Storage
Initial Backup
Summary
Browse
< Back
Next >
Finish
Cancel
Done
Local intranet

Remote Storage

Your files can be backed up to a remote location such as a file server. Specify the type of remote storage, the location for storing your backups, and the amount of space available for backups. If the remote location cannot be reached, the system will wait until a connection can be established.

Back up to: File Server

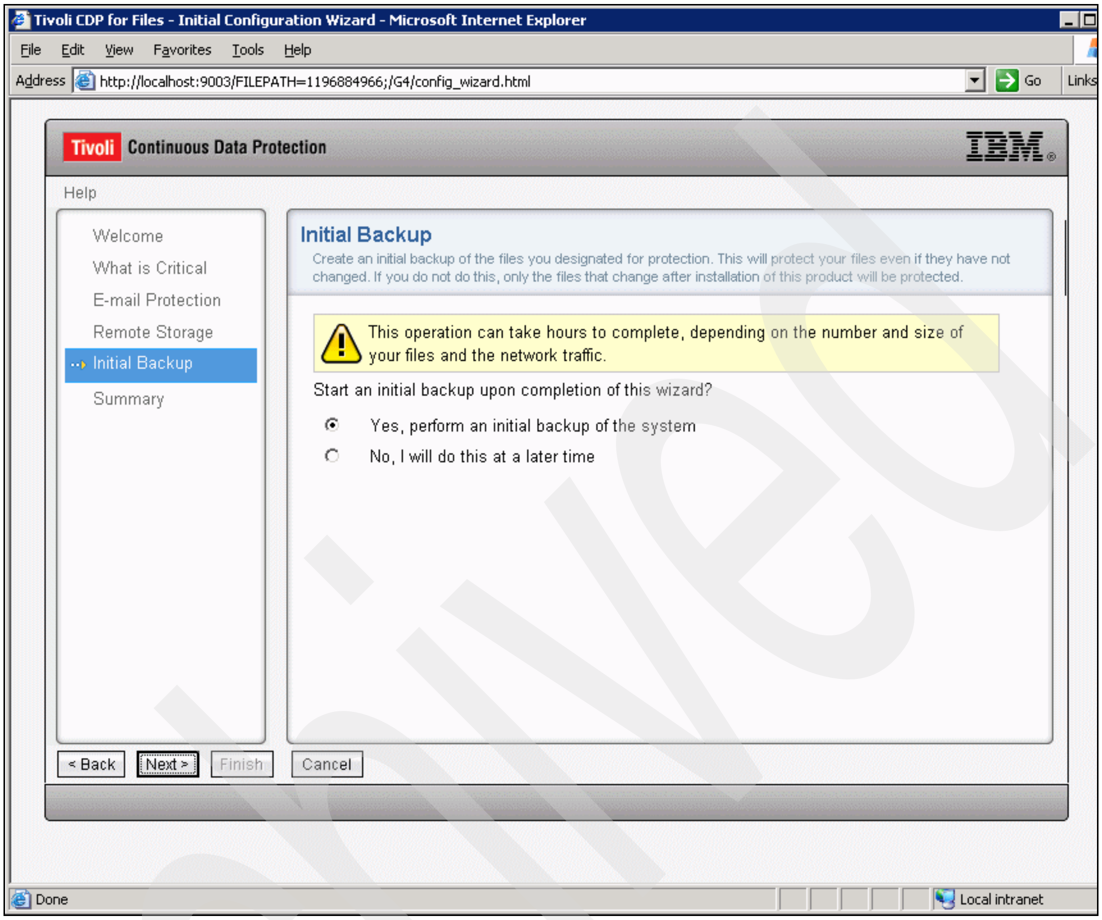
Location: Z:\CDP

Maximum space for backups: 40 GB

Figure 5-7 CDP: remote storage

In this example we choose **File Server** and select to store data to the Z:\CDP folder. We accept the other defaults.

9. Click **Next** and specify whether you want an initial backup to be taken, as shown Figure 5-8 on page 54.



Initial Backup

Create an initial backup of the files you designated for protection. This will protect your files even if they have not changed. If you do not do this, only the files that change after installation of this product will be protected.

⚠ This operation can take hours to complete, depending on the number and size of your files and the network traffic.

Start an initial backup upon completion of this wizard?

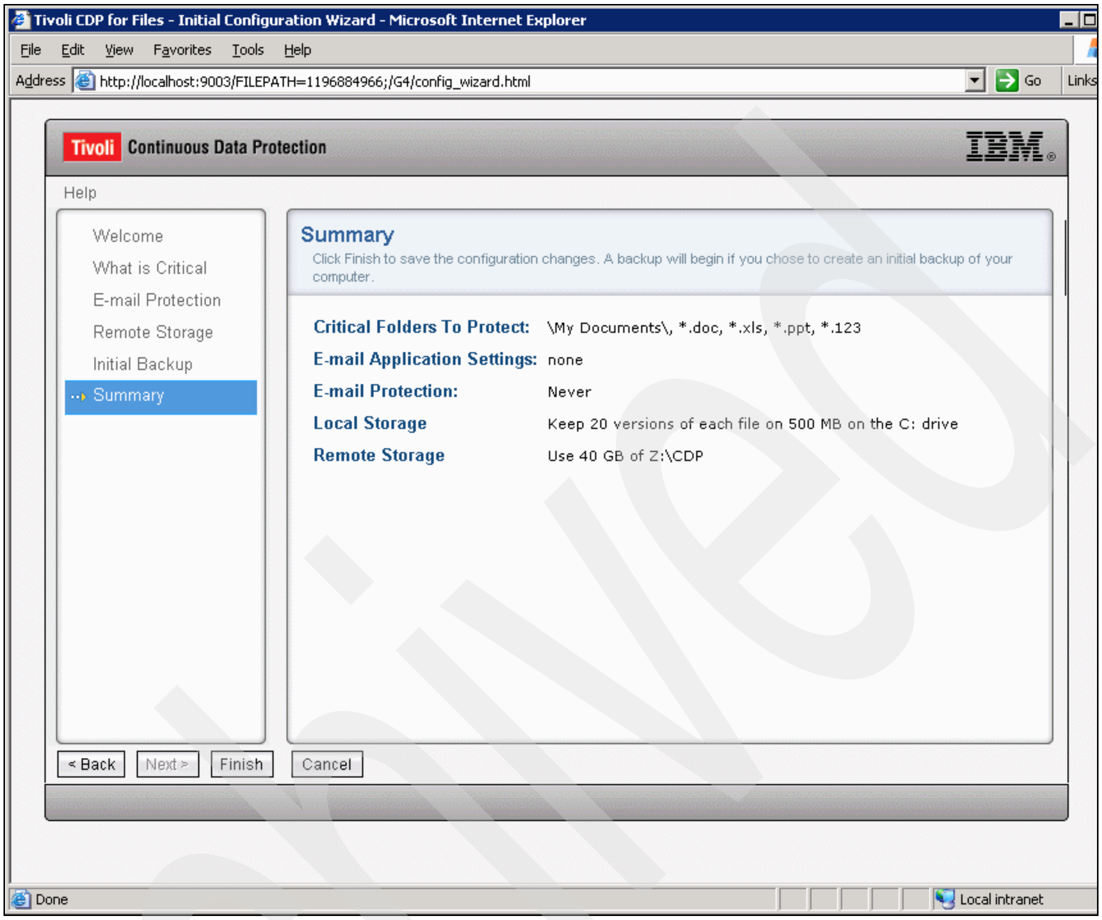
● Yes, perform an initial backup of the system

○ No, I will do this at a later time

Figure 5-8 CDP: Initial Backup selection

10. As we want to back up files that already exist, we select **Yes**. If you do not do this, only files that change after installation of the product will be backed up. Be aware that the initial backup can take some time, depending on the amount of data to process.

11. Click **Next**. Review your settings on the Summary window (Figure 5-9 on page 55) and click **Finish**.


Tivoli CDP for Files - Initial Configuration Wizard - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://localhost:9003/FILEPATH=1196884966;/G4/config_wizard.html
Go
Links
Tivoli Continuous Data Protection
IBM
Help
Welcome
What is Critical
E-mail Protection
Remote Storage
Initial Backup
Summary
< Back
Next >
Finish
Cancel
Done
Local intranet

Summary

Click Finish to save the configuration changes. A backup will begin if you chose to create an initial backup of your computer.

Critical Folders To Protect: \My Documents\, *.doc, *.xls, *.ppt, *.123

E-mail Application Settings: none

E-mail Protection: Never

Local Storage: Keep 20 versions of each file on 500 MB on the C: drive

Remote Storage: Use 40 GB of Z:\CDP

Figure 5-9 CDP: initial settings summary

12. You have now completed the basic set up of Tivoli Continuous Data Protection for Files. You can access the program through a small icon in your system tray, as shown in Figure 5-10.

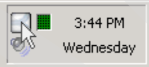


Figure 5-10 CDP: access via the system tray

13.The main window (Figure 5-11 on page 56) appears. Here you can change the configuration changes in the Settings tab, initiate restores via the Restore tab, or configure central administration settings.

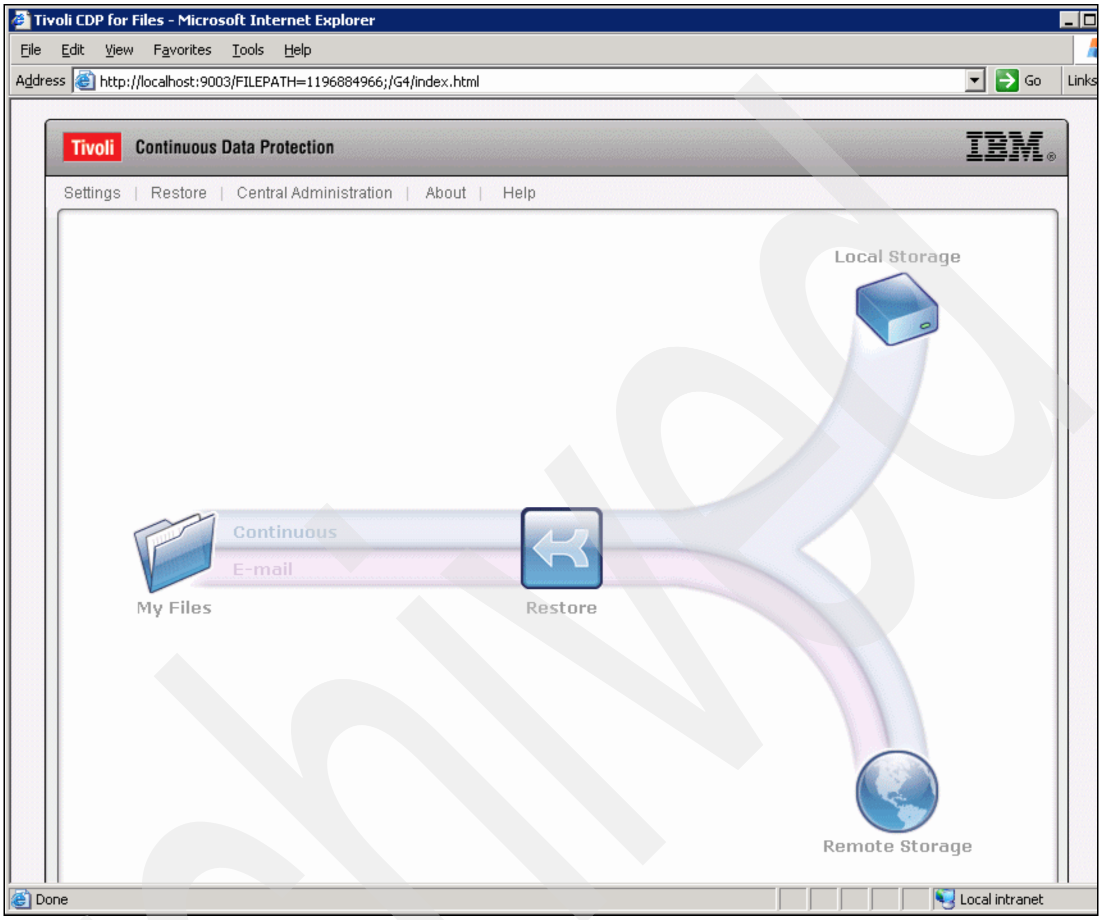

Tivoli CDP for Files - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://localhost:9003/FILEPATH=1196884966;/G4/index.html
Go
Links
Tivoli Continuous Data Protection
IBM
Settings | Restore | Central Administration | About | Help
Local Storage
Continuous
E-mail
My Files
Restore
Remote Storage
Done
Local intranet

Figure 5-11 CDP: main window

14. For our simple scenario, we want to configure local storage to use for backups. Move the mouse pointer over the local storage icon. The local storage information pops up, as shown in Figure 5-12 on page 57.

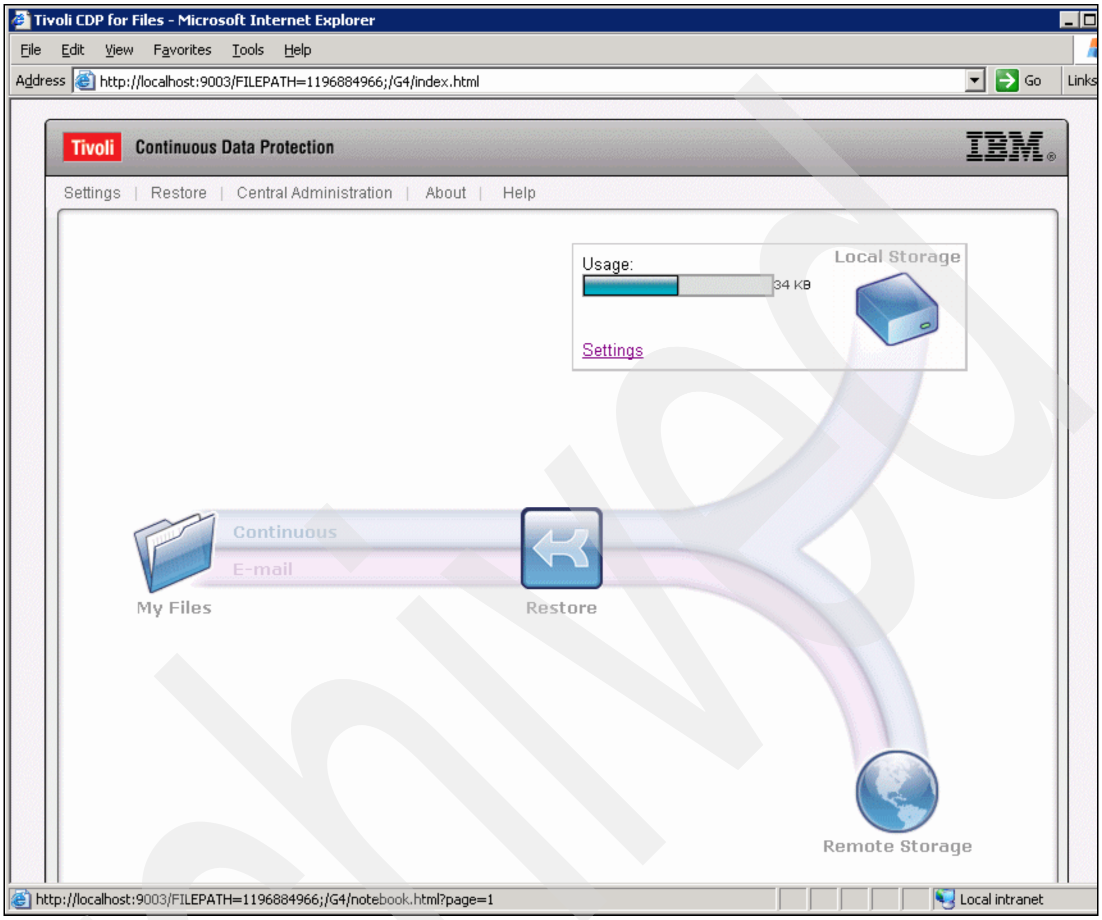
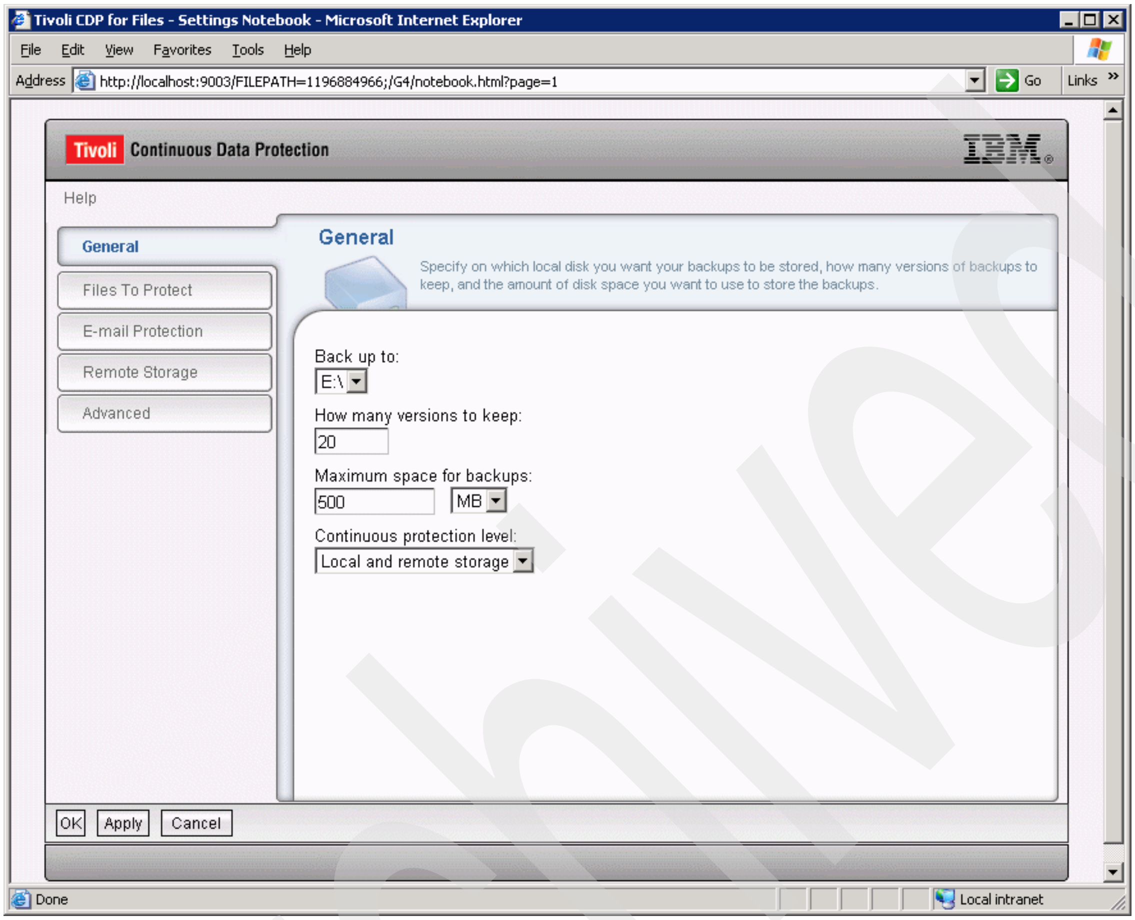

Tivoli CDP for Files - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://localhost:9003/FILEPATH=1196884966;/G4/index.html
Go
Links
Tivoli Continuous Data Protection
IBM
Settings | Restore | Central Administration | About | Help
Usage:
34 KB
Local Storage
Settings
Continuous
E-mail
My Files
Restore
Remote Storage
http://localhost:9003/FILEPATH=1196884966;/G4/notebook.html?page=1
Local intranet

Figure 5-12 CDP: local storage information

15. Click **Settings** to display the Local Storage Settings window (Figure 5-13 on page 58). Here you can make changes to the available disk resources for the system that you are using, how many versions of the files to keep, or how much disk space to use.



Tivoli CDP for Files - Settings Notebook - Microsoft Internet Explorer

Address: http://localhost:9003/FILEPATH=1196884966;/G4/notebook.html?page=1

Tivoli Continuous Data Protection

General

Specify on which local disk you want your backups to be stored, how many versions of backups to keep, and the amount of disk space you want to use to store the backups.

Back up to: E:\

How many versions to keep: 20

Maximum space for backups: 500 MB

Continuous protection level: Local and remote storage

Figure 5-13 CDP: local storage settings

The previous figures should give you a brief idea how to configure and use Tivoli Continuous Data Protection for Files. It is easy and intuitive to use and the initial setup takes only a few minutes.

For further detailed information about deployment of Tivoli Continuous Protection for Files see the references provided in 5.3, “Summary” on page 58.

5.3 Summary

Tivoli Continuous Data Protection for Files provides invisible, real-time file replication meeting the continuous data protection definitions as established by the Storage Networking Industry Association (SNIA).

The product highlights are:

- Real-time data protection

  When a file is created or changed:

  - A copy is stored on local disk.
  - Another copy can be sent to a file server of network attached storage (NAS).
  - Another copy can be sent to an IBM Tivoli Storage Manager server or a WebDAV-enabled Web server.
- Supports file include/exclude options
- Tolerates transient networks
- Provides versioning of files for point-in-time recovery
- Archive retention
- Scalable
- Small foot print, installs in minutes
- Central administration
- Supports push install
- Absolutely no server component required
- For remote target supports:
  - Any file server
  - WebDAV server
  - Tivoli Storage Manager or Tivoli Storage Manager Express server
    - Encryption
    - Compression
- E-mail database support for:
  - Lotus Notes®
  - Microsoft Outlook® files
- Windows Vista support

For detailed information about deployment best practices, integration with your mail program, case studies, troubleshooting, and more see:

- *Deployment Guide Series: Tivoli Continuous Data Protection for Files*, SG24-7235
- *Deployment Guide Series: Tivoli Continuous Data Protection for Files V3.1*, SG24-7423

Part 3

Tivoli Storage Manager V5.4 server enhancements

This part presents enhancements to Tivoli Storage Manager V5.4 servers. First we detail the supported operating systems and summarize the new features and functions, then subsequent chapters present further details of the most significant new features.

6

Version 5.4 server supported environments

This chapter describes the following Tivoli Storage Manager Version 5.4 functions:

- Server operating system levels supported
- New devices supported
- Administration Center support

The major new features of Tivoli Storage Manager Version 5.4 are described in detail in separate chapters.

For full details, always refer to the announcement letter, the installation and user guides, and the readme files for the relevant server. Announcement letters can be found using keywords *Tivoli Storage Manager* at:

```
http://www-01.ibm.com/common/ssi/index.wss
```

or directly for Version 5.4 at:

```
http://www-01.ibm.com/common/ssi/index.wss?DocURL=http://www-01.ibm.com/common/
ssi/rep_ca/2/877/ENUSZP07-0102/index.html&InfoType=AN&InfoSubType=CA&InfoDesc=A
nnouncement+Letters&panelurl=index.wss%3F&paneltext=Announcement%20letter%20sea
rch
```

You will find the Version 5.4 manuals and server readme files in the Previous Versions section of:

```
http://publib.boulder.ibm.com/infocenter/tivihelp
```

6.1 Server operating systems supported

You can find the readmes for Tivoli Storage Manager Version 5.4 and 5.4.1, respectively, at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v1r1/topic/com.ibm.itsmreadme.doc/relnote_server540.html

http://publib.boulder.ibm.com/infocenter/tivihelp/v1r1/topic/com.ibm.itsmreadme.doc/readme_server541.html

An overview of all the supported operating systems with the corresponding version of Tivoli Storage Manager can be found at:

http://www-1.ibm.com/support/docview.wss?rs=663&context=SSGSG7&uid=swg21243309&loc=en_US&cs=utf-8&lang=en

6.1.1 AIX supported levels for Tivoli Storage Manager

The Tivoli Storage Manager V5.4 server on AIX is supported at:

- AIX V5.2 64 bit
- AIX V5.3 64 bit

Note: 32-bit AIX is supported by Tivoli Storage Manager V5.3.

6.1.2 HP-UX supported levels for Tivoli Storage Manager

The Tivoli Storage Manager V5.4 server on HP-UX is supported in PA-RISC and Itanium environments.

PA-RISC server requirements

The Tivoli Storage Manager V5.4 server on HP-UX PA-RISC is supported at HP-UX 11i V2 64 bit.

Itanium server requirements

The Tivoli Storage Manager server on HP-UX Itanium is supported at HP-UX level 11iV2.

6.1.3 Linux supported levels for Tivoli Storage Manager

The Tivoli Storage Manager V5.4 server on Linux is supported for x86, z Linux, and POWER versions.

Linux x86 server requirements

The Tivoli Storage Manager V5.4 server on Linux x86 is supported at:

- Red Hat Enterprise Linux 4 (AS, WS, ES)
- Red Hat Enterprise Linux 5
- SUSE Linux Enterprise Server 9 and 10
- Asianux 2.0 - Red Flag DC 5.0, Miracle Linux 4.0, and Haansoft Linux 2006
- V2.3.3 or later of the GNU C libraries installed on the target machine

Linux x86_64server requirements

The Tivoli Storage Manager V5.4 server on Linux x86_64 is supported at:

- Red Hat Enterprise Linux 4 (AS, WS, ES)
- Red Hat Enterprise Linux 5
- SUSE Linux Enterprise Server 9 and 10
- Asianux 2.0 - Red Flag DC 5.0, Miracle Linux 4.0, and Haansoft Linux 2006
- V2.3.3 or later of the GNU C libraries installed on the target machine

Linux System z server requirements

The Tivoli Storage Manager V5.4 server on Linux for System z is supported at these versions, 64-bit only:

- Red Hat Enterprise Linux 4 and 5
- SUSE Linux Enterprise Server 9 and 10
- V2.3.3 or later of the GNU C libraries

Linux on POWER server requirements

The Tivoli Storage Manager V5.4 server on Linux IBM System p and IBM System i™ is supported at:

- Red Hat Enterprise Linux 4 (on POWER 5 processors only)
- Red Hat Enterprise Linux 5
- SUSE Linux Enterprise Server 9 and 10 (on POWER 5 processors only)
- Asianux 2.0 - Red Flag DC 5.0 and Haansoft Linux 2006
- V2.3.3, or later of the GNU C libraries installed on the target machine

6.1.4 Solaris supported levels for Tivoli Storage Manager

The Tivoli Storage Manager V5.4 server on Solaris is supported in SPARC and x86 versions.

Solaris SPARC server requirements

The Tivoli Storage Manager V5.4 server on Solaris SPARC is supported at:

- Solaris 9 64-bit
- Solaris 10 64-bit

Solaris x86_64 server requirements

The Tivoli Storage Manager V5.4 server on Solaris x86_64 is supported at Solaris 10 64-bit.

6.1.5 Windows supported levels for Tivoli Storage Manager

The Tivoli Storage Manager V5.4 server on Windows is supported at:

- Windows Server 2003 (Standard, Enterprise, or Datacenter) Edition
- Windows Server 2003 SP1 (Enterprise or Datacenter) Edition 64 bit
- Windows Server 2003 (Standard, Enterprise, or Datacenter) x64 Edition

Notes: Windows Storage Server versions are supported.

All service packs are supported, including R2.

Windows 2000 Server is supported on Tivoli Storage Manager V5.3 server.

6.1.6 z/OS server requirements for Tivoli Storage Manager

The Tivoli Storage Manager V5.4 server on z/OS is supported at:

- z/OS V1R7
- z/OS V1R8 or later

6.2 Special device considerations

Refer to the following Web site for the list of devices that are currently supported by Tivoli Storage Manager (5608-ISM) and for those that are supported by Tivoli Storage Manager Extended Edition (5608-ISX). Libraries that have more than four drives or more than 48 tape slots require the extended edition license. This has been changed since Version 5.3, where the requirements were greater than three drives or 40 slots for Tivoli Storage Manager Extended Edition.

http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliStorageManager.html

In addition, this Web site provides access to a knowledge base of solutions, hints and tips, technical notes, readme files, product fixes and refreshes, product documentation, and more. This knowledge database is located under Self Help.

Specifically, detailed current device support for AIX, HP, Solaris, and Windows can be found at:

http://www.ibm.com/software/sysmgmt/products/support/IBM_TSM_Supported_Devices_for_AIXHPSUNWIN.html

Detailed current device support for Linux can be found at:

http://www.ibm.com/software/sysmgmt/products/support/IBM_TSM_Supported_Devices_for_Linux.html

For a summary of new devices supported as of Version 5.4 or Version 5.4.1 use the announcement letter, or the specific readme files found at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v1r1/topic/com.ibm.itsmreadme.doc/reln_server.html

New device support

Tivoli Storage Manager V5.4 includes the following new devices with AIX, HP-UX, Linux, Solaris, and Windows unless otherwise indicated:

- Sun™ StorageTek™ T10000 drives and media. New recording formats are available for the ECARTRIDGE device type.
- Exabyte and IBM VXA-3 drives and media. New recording formats are available for the 8 MM device class.
- Sony SDX-800V - an enhanced AIT-3 drive. New recording formats are available for the 8 MM device type.
- Quantum DLT-S4 and Quantum DLT-V4 drives with read-write and WORM capabilities. ACSLS libraries that support the DLT-S4 drive also support read-write and WORM capabilities. New recording formats are available for the DLT device class.

Additionally, the following device support has been added:

- V5.4 new drive support
  - Quantum LTO-3 WORM
  - Sony SDX-1100
  - Sony SDX-1100 WORM
- V5.4 new library support
  - Fujitsu ETERNUS LT250
  - HP StorageWorks DAT72x10
  - NEC T40A2
  - Quantum DX3000
  - Quantum DX5000
- V5.4.1 new drive support
  - Dell PowerVault 100T DAT72
  - Quantum LTO-3 HH
  - Plasmon UDO-2
  - Tandberg 820LTO
- V5.4.1new library support
  - Cristie GigaStream T-Series
  - Overland ARCvault 12
  - Overland ARCvault 24
  - Overland ARCvault 48

6.3 Administration Center requirements

For a summary of Administration Center requirements as of Version 5.4, use the announcement letter, and the specific readme file found at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v1r1/topic/com.ibm.itsmreadme.doc/relnote_adminctr540.html

6.3.1 Administration Center introduction

The Administration Center is a Web-based interface that can be used to centrally configure and manage IBM Tivoli Storage Manager servers. It provides wizards to help guide you through common configuration tasks.

The Administration Center is installed as an IBM Integrated Solutions Console component. The Integrated Solutions Console allows you to install components provided by multiple IBM applications, and access them from a single interface.

Backward compatibility

In order to administer Tivoli Storage Manager servers V5.4 and later, you must install or upgrade to the Tivoli Storage Manager Administration Center V5.4.

The Tivoli Storage Manager Administration Center V5.4 is compatible with the Integrated Solutions Console V6.0.1.1. If you currently have downlevel versions of the Administration Center and Integrated Solutions Console installed, you must upgrade both.

With Tivoli Storage Manager Administration Center, the Integrated Solutions Console is a basic component and will be included with the installation media. For additional information about Integrated Solutions Console see:

http://www.ibm.com/developerworks/autonomic/csa.html?S_TACT=105AGX09&S_CMP=LP

6.3.2 Administration Center system requirements

Detailed hardware and software requirements for the Administration Center can be found in Technote 1195062, at:

http://www-1.ibm.com/support/docview.wss?uid=swg21195062

Web interface

The Tivoli Storage Manager Administration Center Web interface for the server and a Web client interface for client machines requires a Java Swing-capable (at JRE™ 1.4.2) Web browser:

- Microsoft Internet Explorer® 6.0 or later with Java Plug-in 1.4.2
- Mozilla 1.5 or later

Refer to the backup-archive client requirements section for the specific operating system levels supported for the Web clients. TCP/IP is the only communication protocol supported for this client interface.

For the latest recommendation on the Administration Center installation, use keyword TSMADMINCENTER when you visit:

http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliStorageManager.html

General system requirements

The machine hosting the Administration Center and Integrated Solutions Console requires the following:

- Disk space: To install the console on a system for the first time, the user needs:
  - 982 MB to satisfy the installation program disk space check
  - An additional 100 MB of temporary space (which is also checked during the installation)
  - 500 MB for the completed installation
- Virtual memory/swap space: equal to double the system's physical memory. At a minimum, this should be at least equal to the system's physical virtual memory.
- Network connectivity: To use the console across a network, the following items are required for the machine:
  - Network adapter and connection to a physical network that can carry IP packets, for example, Ethernet
  - Static IP address
  - Configured fully qualified host name.

    The Integrated Solutions Console must be able to resolve an IP address from its fully qualified host name.

System-specific requirements

The Tivoli Storage Manager Administration Center server requires the following hardware and software:

- AIX server:
  - AIX V5.1 with ML4, AIX V5.2 with ML1 + APAR IY44183, AIX V5.3 with ML1.
  - Processor: Power4 450 MHz at a minimum; production environments should consider higher speeds.
  - Physical memory: 512 MB or more.
- Windows server:
  - Windows 2000 (Professional, Server, or Advanced Server) with SP4.
  - Windows Server 2003 (Standard, Enterprise, or Datacenter) Edition.
  - Processor: CPU speeds of late model, midrange to high-end servers are recommended. Pentium® 800 MHz or equivalent at a minimum. Production environments should consider the Pentium 4™ processor at 1.4 GHz or higher.
  - Physical memory: 512 MB or more.
  - File system: We recommend the NTFS file system.
- Linux server:
  - SUSE Linux Enterprise Server (SLES) 8, SUSE Linux Enterprise Server (SLES) 9, Red Hat Enterprise Linux 3 Update 3, or Red Hat Enterprise Linux 4
  - Processor: CPU speeds of late model, midrange to high-end servers are recommended. Pentium 800 MHz or equivalent at a minimum. Production environments should consider the Pentium 4 processor at 1.4 GHz or higher.
  - Processor: Power4 450 MHz at a minimum. Production environments should consider higher speeds.
  - Physical memory: 512 MB or more
- Solaris server:
  - Solaris 8 or 9.
  - Processor: Ultra™ 60 at 450 MHz at a minimum. Sun Blade 2000 workstation at 1 GHz or higher is recommended.
  - Physical memory: 512 MB or more.

The machine hosting the Tivoli Storage Manager Administration Center server can be the same machine as the Tivoli Storage Manager server if it meets the requirements for both servers. In this case, the physical memory requirements must be added for both servers.

6.4 Servers not migrated

The following Tivoli Storage Manager server operating systems, if supported in V5.3, were not migrated to V5.4 and are not supported in V5.4:

- z/OS V1R4, V1R5, and V1R6
- HP-UX 11i V1 and HP-UX 32 bit, all versions
- AIX V5.1 and AIX 32 bit, all versions
- Solaris 8
- Red Hat Enterprise Linux Server 3
- SLES 8

- Red Flag 4.1/Asianux 1.0
- Windows 2000

6.5 DSMLABEL command

The DSMLABEL command is no longer included in the Tivoli Storage Manager distributions. The functionality to label tapes is available with the LABEL LIBVOLUME command.

7

Active-data pools

As the amount of data that customers store to Tivoli Storage Manager servers increases, there are increasing demands on the ability to recover in an acceptable time. Under normal circumstances, data that is initially stored in disk storage pools is migrated to tape pools, in order to free space in the disk pool for new data. This migration, along with the mixing of active and inactive data in the disk pool, lengthens recovery times.

Tivoli Storage Manager V5.4 introduces a new type of storage pool for fast restore and efficient storage pool utilization, known as active-data pools. This chapter discusses the concepts and provides implementation examples for active-data pools.

7.1 Introduction to active-data pools

Active-data pools have been designed to provide Tivoli Storage Manager administrators with the ability to segregate active and inactive files in the servers storage hierarchy. Active data storage pools (ADPs) allow you to organize active data that is likely to be restored so that restores would not need to access tapes containing inactive data. If you keep many versions of files, searching tapes for active versions of files that are mixed with inactive versions can take a long time. By storing only the active versions together on tapes, the time it takes to sort through the inactive files is eliminated. For Tivoli Storage Manager, this means keeping only the active versions of files in a storage pool strictly defined for such a purpose.

7.1.1 Definition

Setting up an ADP depends on whether your intended use is for faster client restore or onsite/off-site storage of active data. You first need to determine which nodes' data you want to store in an ADP. If you want an ADP for fast client restore, you define an ADP with a FILE device class. Define an ADP with a device class of any removable media if your intended use is for onsite/off-site storage of active data.

You define an ADP with the DEFINE STGPOOL command, specifying POOLTYPE=ACTIVEDATA. A storage pool so defined will contain only active versions of client backup data and must be assigned to a sequential access device class. For the purposes of faster client restore, the ADP should be assigned to a FILE device class. For the purposes of storing active data offsite, the device class can be any removable sequential device class, such as tape or optical.

Figure 7-1 shows the three different types of storage pool now available with Tivoli Storage Manager, and the eligible device classes that can be used for each.

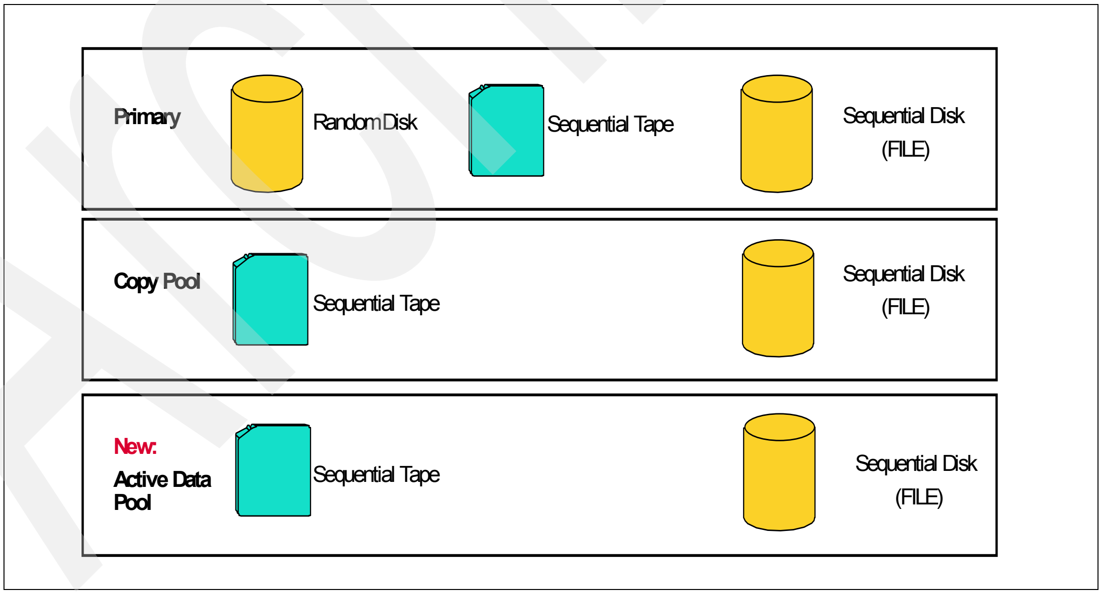


Figure 7-1 Tivoli Storage Manager: storage pool types

Types of active-data pools

There are two main reasons to implement ADPs: for faster onsite client restore or to have active data available off site. ADPs for faster client restore are typically configured on sequential-access disk, whereas ADPs for off-site storage are on tape or other removable media.

- Benefits of active data storage pools on sequential-access disk
  - Optimized access to active versions for faster restore

    During client restore operations from primary storage pools, the server may need to position past inactive files that do not need to be restored. When active files are segregated from inactive files, restoring active files, exporting active files, and generating backup sets can be much faster.
  - Reduced size of pools if only active versions are stored

    To save storage space, you may decide to store only active data in an active data storage pool. If you vault data electronically to a remote location you can potentially save bandwidth by copying only active data.
  - Reduced data movement in preparation for restore of active data

    In some situations, such as staging active data to a diskpool prior to a client restore, you might want to move only the active data rather than also moving inactive data that will not be restored. Having active data collocated in a single storage pool eliminates the need to stage active data.
- Benefits of active data storage pools on tape or other removable media
  - Reduced storage requirements

    Reduce the amount of tapes to protect your active data against media failure or disaster.
  - Simplified tape management

    If you vault your tapes to a remote location, potentially fewer tapes allow for simplified tape management.
  - Faster restores in the event of requiring offsite tapes for recovery, since only active data is stored

Summary of how to set up active-data pools

There are three steps to configure and use active-data pools:

1. Define one or more active-data pools, as shown in 7.2.1, “Set up an active-data pool for fast client restore” on page 78, and 7.2.2, “Set up an active-data pool to reduce resources” on page 81.
2. Decide which nodes will be eligible to use active-data pools, and include those nodes in a domain that is configured to allow this. This process defines the *eligibility* to use an ADP. It does not of itself put any data into the active-data pool. Details are given in 7.1.2, “Eligibility to use active-data pools” on page 74.
3. Copy the data from the specific primary storage pools to one or more active data pools. There are two ways to do this, which are described in 7.1.3, “Writing data to an ADP” on page 75.

Important: At the time of writing, if you plan to distribute active-data pool definitions from a Tivoli Storage Manager configuration server, make sure to apply APAR IC55242. This is required to ensure that correct values are shown for active-data pools on managed servers.

7.1.2 Eligibility to use active-data pools

To make a node eligible to use an ADP, define a new domain, or update an existing domain with the parameter ACTIVEDESTINATION=a*ctive_data_pool_name-list*. The list consists of one or more active-data pools. Then associate the client nodes whose data you want to store in the specified ADP to that domain. This operation has no effect on the primary storage pools used for the client's data as defined in the management class copy group. Depending on how many active-data pools you define, you may have a single domain with the ACTIVEDESTINATION parameter, or several domains, each pointing to different active-data pool lists.

The ACTIVEDESTINATION list identifies the ADPs to which the nodes assigned to the DOMAIN are authorized to write backup data. When a client backup session is in progress, or when the new server command COPY ACTIVEDATA is executed, the ACTIVEDESTINATION parameter is checked, so that data is written to the ADP only if the node owning the data is assigned to a domain that has the ADP listed. If this check fails then no data is written to the ADP.

As an example, consider the following configuration (shown in Figure 7-2):

- Storage pool DISK1 is defined as a primary storage pool, and storage pool ADP1 is defined as an active-data pool on sequential disk.
- A domain FASTRESTORE with nodes NODE1 and NODE2 assigned to it, and with ACTIVEDESTINATION=ADP1 and associated backup copy group destination, is DISK1.
- Another domain NORMALRESTORE has NODE 3 assigned to it but does not include an ACTIVEDESTINATION definition. Its backup copy group destination is also DISK1.

If all three nodes have data in storage pool DISK1, when active backup data is being copied into ADP1, only the active backup data from NODE1 and NODE 2 will be copied. Because NODE3 is assigned to a domain that does not have ADP1 in its ACTIVEDESTINATION, it is not authorized to store its data there. Therefore, files E and F from NODE3 are not copied to the active-data pool ADP1.

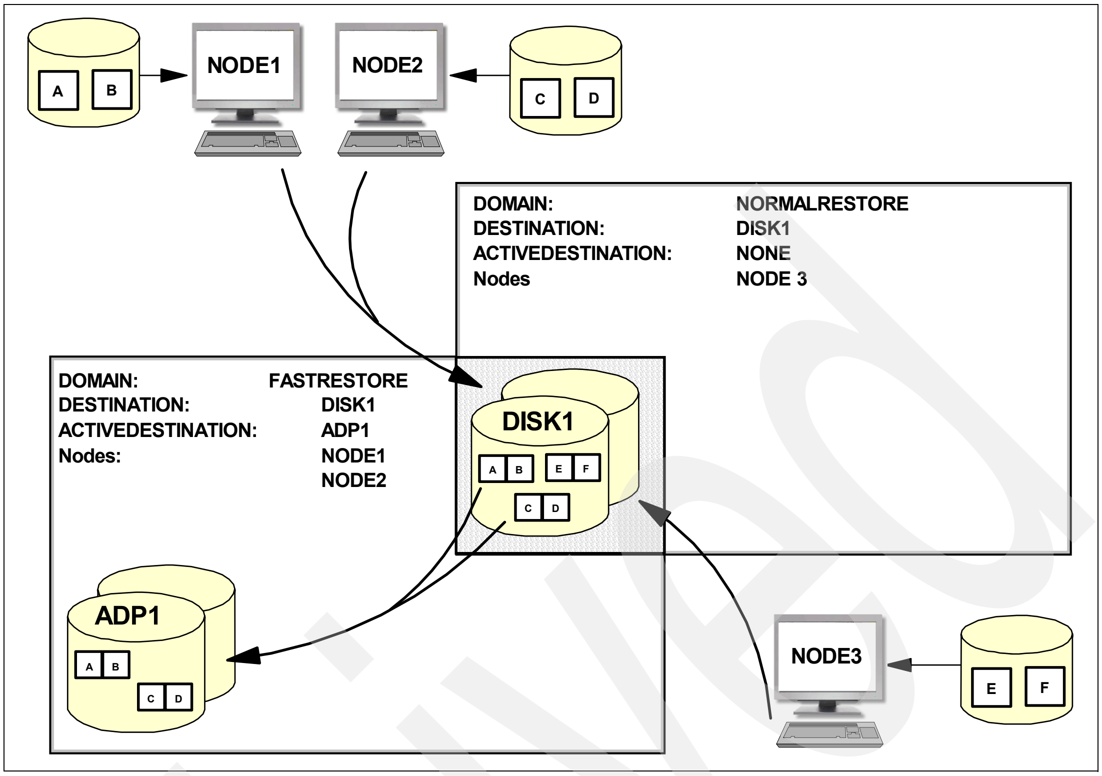


Figure 7-2 Data flow with ACTIVEDESTINATION option

7.1.3 Writing data to an ADP

Similarly to copy storage pools, Tivoli Storage Manager provides two ways to write data to an ADP:

- Implicitly, using simultaneous write during client backup into an ADP
- Explicitly and asynchronously, using the COPY ACTIVEDATA command

Simultaneous write during client backup into an ADP

To write data from eligible nodes to an ADP during a client backup session, use the ACTIVEDATAPOOLS parameter on the DEFINE STGPOOL or UPDATE STGPOOL commands. This parameter defines a list of ADPs to be simultaneously written to during a client backup session.

When one or more ADPs is associated with a primary storage pool, any data written to the primary storage pool destination during an eligible node's client backup session will be simultaneously written to the ADP. Remember that a primary storage pool can also specify one or more copy storage pools for simultaneous write, using the COPYSTGPOOLS parameter. The total combined number of pools that can be listed in the COPYSTGPOOLS and ACTIVEDATAPOOLS parameters cannot exceed three.

Figure 7-3 shows a client backup session. The data is written to the primary pool, defined in the management class, and simultaneously written to an active-data pool. This will occur provided that the node is eligible to write to the active-data pool (that is, providing that the node is registered in a domain that lists the active-data pool as an active destination).

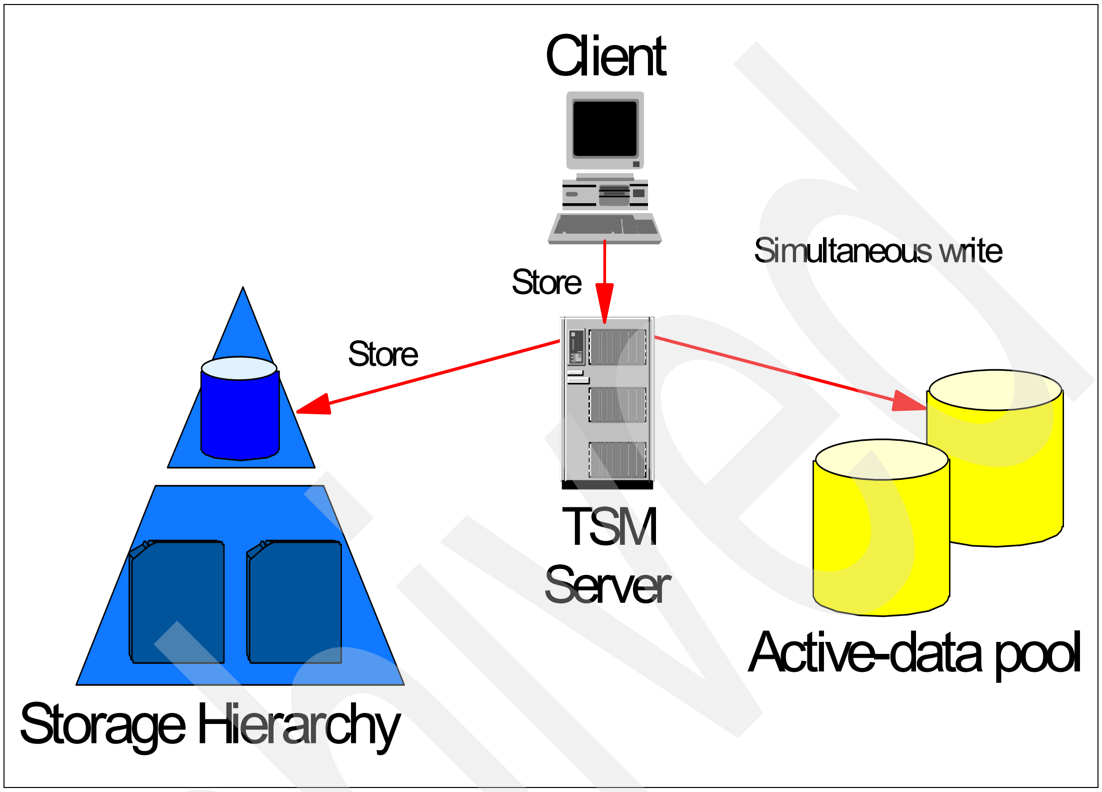


Figure 7-3 ADP: simultaneous write

The simultaneous write from the primary to the active-data pool is available for non-LANFREE operations only. See, "Asynchronous write using the COPY ACTIVEDATA command" on page 76 to manage client objects that are backed up LANFREE.

Note: The function provided by the ACTIVEDATAPOOLS parameter is not intended to replace the COPY ACTIVEDATA command. If you use the ACTIVEDATAPOOLS parameter, you should still regularly use the COPY ACTIVEDATA command to ensure that the active-data pools contain all active data of the primary storage pool.

Note: The COPYCONTINUE parameter for a storage pool only applies to copy storage pools and has no effect on active-data pools. If an error occurs while writing to an active-data pool during simultaneous write, it is removed from the sessions pool list and the client is notified to retry the backup. If the client decides to retry the backup, only the remaining copy or active-data storage pools will be written to and not the failing active-data pools. This action is similar to how failing copy storage pools are handled with the COPYCONTINUE=YES parameter.

Asynchronous write using the COPY ACTIVEDATA command

The COPY ACTIVEDATA command begins a server process that incrementally copies only active backup data from a primary storage pool to an ADP. The node the data belongs to must be authorized via the DOMAIN to store data into the ADP. No inactive files, whether non-aggregated files or logical files within an aggregate, are copied. Archive and space-managed objects are not copied either.

Figure 7-4 shows the process. The client backs up data as usual to the primary storage pool. Later, when the COPY ACTIVEDATA command is issued or scheduled, any active data objects that do not already exist in the active-data storage pool are copied there.

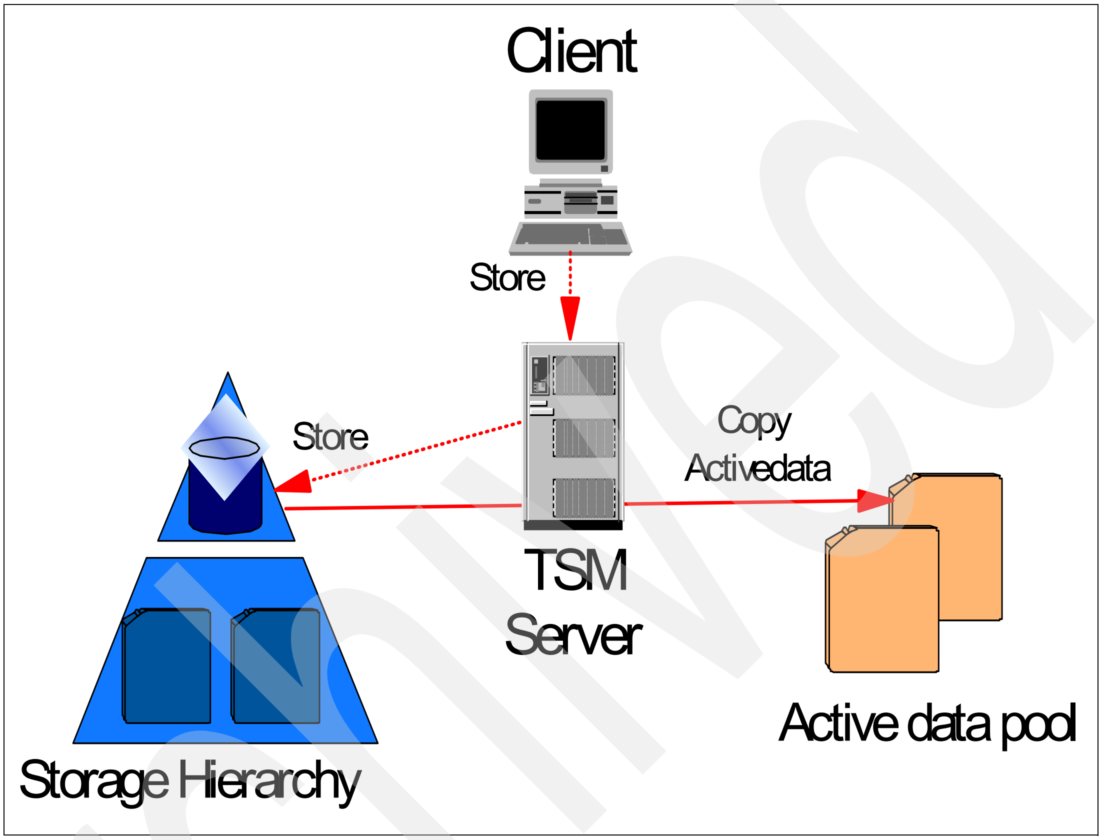


Figure 7-4 ADP: COPY ACTIVEDATA command

If migration for a storage pool starts while active data is being copied, some files might be migrated before they are copied. For this reason, you should copy active data from storage pools that are higher in the migration hierarchy before copying active data from storage pools that are lower. For example, copy active data from disk storage pools before copying the data from tape storage pools.

The COPY ACTIVEDATA command and MOVE DATA or MOVE NODEDATA commands reconstruct aggregates as they are copied or moved within an active-data pool.

Note: Do not specify RECONSTRUCT=NO on the MOVE DATA or MOVE NODEDATA commands when dealing with active-data pools.

7.2 Implementation

In this section we work through a sample implementation of active-data pools. Our example uses nodes ACTNODE1 and ACTNODE2. We configure ACTNODE1 for fast client restore and ACTNODE2 for reduced resource usage.

The following definitions exist on the server before any of the definitions below are made:

- Domain: STANDARD
- Policy set: STANDARD
- Management class: STANDARD
- Copy group: STANDARD
- Copy destination: BACKUPPOOL
- Device classes: DISK, FILECLASS, LTO4

Storage pool BACKUPPOOL with a DISK device class is defined as the first-level primary storage pool. All data enters the storage hierarchy here.

7.2.1 Set up an active-data pool for fast client restore

To do this:

1. We define an active-data pool (as shown in Example 7-1) using a FILE device class type, as recommended for fast client restore.

Example 7-1 Define an active-data pool

```
tsm: TSMAIX55>DEFINE STGPOOL ADPPOOL FILECLASS POOLTYPE=ACTIVEDATA MAXSCRATCH=1000
ANR2200I Storage pool ADPPOOL defined (device class FILECLASS).
```

2. Define a new domain, listing the newly defined active-data pool, as in Example 7-2.

Example 7-2 Define a domain with an ACTIVEDESTINATION parameter

```
tsm: TSMAIX55>DEFINE DOMAIN ACTIVEDOMAIN ACTIVEDESTINATION=ADPPOOL
ANR1500I Policy domain ACTIVEDOMAIN defined.
```

3. Define the policy, management class, and copygroup to be used with the new domain, as shown in Example 7-3, and then activate the policy set. If you decide to use an existing domain and want to allow all nodes assigned to the domain to store data in the active-data pool, then you would skip these steps. Simply update the existing domains so that the ACTIVEDESTINATION is set to the active-data pool.

Example 7-3 Define the policy

```
tsm: TSMAIX55>DEFINE POLICYSET ACTIVEDOMAIN ACTIVEPOLICY
ANR1510I Policy set ACTIVEPOLICY defined in policy domain ACTIVEDOMAIN.

tsm: TSMAIX55>DEFINE MGMTCLASS ACTIVEDOMAIN ACTIVEPOLICY ACTIVEMGMT
ANR1520I Management class ACTIVEMGMT defined in policy domain ACTIVEDOMAIN, set
ACTIVEPOLICY.

tsm: TSMAIX55>DEFINE COPYGROUP ACTIVEDOMAIN ACTIVEPOLICY ACTIVEMGMT
DESTINATION=BACKUPPOOL VERE=10 VERD=10
ANR1530I Backup copy group STANDARD defined in policy domain ACTIVEDOMAIN, set
ACTIVEPOLICY, management class ACTIVEMGMT.

tsm: TSMAIX55>ASSIGN DEFMGMTCLASS ACTIVEDOMAIN ACTIVEPOLICY ACTIVEMGMT
ANR1538I Default management class set to ACTIVEMGMT for policy domain
ACTIVEDOMAIN, set ACTIVEPOLICY.

tsm: TSMAIX55>ACTIVATE POLICYSET ACTIVEDOMAIN ACTIVEPOLICY
```

```
ANR1554W DEFAULT Management class ACTIVEMGMT in policy set ACTIVEDOMAIN
ACTIVEPOLICY does not have an ARCHIVE copygroup:  files will not be archived by
default if this set is activated.

Do you wish to proceed? (Yes (Y)/No (N)) y
ANR1554W DEFAULT Management class ACTIVEMGMT in policy set ACTIVEDOMAIN
ACTIVEPOLICY does not have an ARCHIVE copygroup:  files will not be archived by
default if this set is activated.
ANR1514I Policy set ACTIVEPOLICY activated in policy domain ACTIVEDOMAIN.
```

4. We assign node ACTNODE1 to ACTIVEDOMAIN, as shown in Example 7-4.

Example 7-4   Assign a node to the domain that uses the active-data pool

```
tsm: TSMAIX55>UPD NODE ACTNODE1 DOMAIN=ACTIVEDOMAIN
ANR2063I Node ACTNODE1 updated.
```

5. Optionally, now you could configure the primary storage pool BACKUPPOOL for simultaneous write to the active-data pool. We do this in step 8. For now we define schedules to automatically reclaim ADPPOOL and to copy new active data from BACKUPPOOL. The commands are scheduled to run daily in the morning, as shown in Example 7-5.

Example 7-5   Scheduled active data reclamation and copy

```
tsm: TSMAIX55>DEFINE SCHEDULE RECLAIM_ADPPOOL TYPE=ADMINISTRATIVE CMD="RECLAIM STG
ADPPOOL THRESH=1" ACTIVE=YES STARTTIME=07:00 PERIOD=1
ANR2577I Schedule RECLAIM_ADPPOOL defined.
tsm: LOCHNESE>DEFINE SCHEDULE COPYACTIVE_BACKUPPOOL TYPE=ADMINISTRATIVE CMD="COPY
ACTIVEDATA BACKUPPOOL ADPPOOL" ACTIVE=YES STARTTIME=08:00 PERIOD=1
ANR2577I Schedule COPYACTIVE_BACKUPPOOL defined.
```

6. Now the setup is complete. Let us test to see how the active-data pool is used. We incrementally back up data in a directory on ACTNODE1 a number of times, making sure that several objects have changed. This generates active and inactive data in the primary storage pool. Example 7-6 shows the occupancy of BACKUPPOOL. Note that its definition at this stage does not include the ACTIVEDATAPOOLS parameter, so there is no automatic (synchronous) write to the active-data pool.

Example 7-6   Initial occupancy, no active-data pool use yet

```
tsm: TSMAIX55>Q OCC ACTNODE1

Node Name    Type  Filespace      FSID    Storage       Number of     Physical      Logical
                   Name                   Pool Name         Files        Space        Space
                                                                      Occupied     Occupied
                                                                          (MB)         (MB)
----------   ----  ----------    -----   ----------    ---------     ---------    ---------
ACTNODE1     Bkup  \\eifel\c$        2   BACKUPPOOL          255          0.44         0.44
```

7. We can wait till the schedule defined in Example 7-5 executes, or to test quickly, we can explicitly copy the active files to ADPPOOL, using the COPY ACTIVEDATA command, as shown in Example 7-7.

Example 7-7 COPY ACTIVEDATA command

```
tsm: TSMAIX55>copy activedata backuppool adppool wait=yes
ANR0984I Process 10 for COPY ACTIVEDATA started in the FOREGROUND at 15:06:29.
ANR2110I COPY ACTIVEDATA started as process 10.
ANR1178I Copying active files from  primary storage pool BACKUPPOOL to active data
pool ADPPOOL started as process 10.
ANR1184I Copy active data process 10 ended for storage pool BACKUPPOOL.
ANR0986I Process 10 for COPY ACTIVEDATA running in the FOREGROUND processed 155
items for a total of 299,008 bytes with a completion state of SUCCESS at 15:06:29.
ANR1318I Copying active data from primary storage pool BACKUPPOOL to active data
pool ADPPOOL has ended.  Files Copied Up: 155, Bytes Copied Up: 299008, Unreadable
Files: 0, Unreadable Bytes: 0.
```

Note that a smaller amount of data and number of files are copied, compared with the total storage pool occupancy, since only active data is copied, and no inactive objects are copied.

8. Now we enable synchronous write for BACKUPPOOL using the command:

   `UPDATE STGPOOL BACKUPPOOL ACTIVEDATAPOOL=ADPPOOL`

9. Now we update 100 of the files and re-run the client backup. Since we have enabled synchronous write, the new data automatically gets written also to the active-data pool. Example 7-8 on page 80 shows that there are now an additional 100 files in the pool—255 compared to 155 as moved in Example 7-7 on page 80. With this server setup now, every time ACTNODE1 stores data into BACKUPPOOL, the data will also be written into ADPPOOL. The schedule, COPYACTIVE_BACKUPPOOL, ensures that any data that was not stored during simultaneous write is copied to the active-data pool. These writes only occur for nodes belonging to the domain ACTIVEDOMAIN.

Example 7-8 QUERY OCCUPANCY with ACTIVEDATAPOOL defined

```
tsm: TSMAIX55>Q OCC ACTNODE1

Node Name    Type   Filespace     FSID    Storage       Number of     Physical      Logical
                    Name                  Pool Name         Files        Space        Space
                                                                      Occupied     Occupied
                                                                          (MB)         (MB)
----------   ----  ----------    -----   ----------    ---------     ---------     ---------
ACTNODE1     Bkup  \\eifel\c$        2   ADPPOOL             255          0.44          0.44
ACTNODE1     Bkup  \\eifel\c$        2   BACKUPPOOL          355          0.60          0.60
```

10. Finally, reclaim the active-data pool so any unused space is freed because of the reconstruction of the objects, as shown in Example 7-9.

Example 7-9 Reclaim an ADP

```
tsm: TSMAIX55>RECLAIM STG ADPPOOL THRESH=1 WAIT=YES
ANR0984I Process 12 for SPACE RECLAMATION started in the FOREGROUND at 15:42:00.
ANR2110I RECLAIM STGPOOL started as process 12.
ANR4930I Reclamation process 12 started for primary storage pool ADPPOOL manually,
threshold=1,
duration=None.
ANR1040I Space reclamation started for volume /tsm/stg/activedata/00000021.BFS,
storage pool
ADPPOOL (process number 12).
ANR1044I Removable volume /tsm/stg/activedata/00000021.BFS is required for space
reclamation.
ANR1041I Space reclamation ended for volume /tsm/stg/activedata/00000021.BFS.
ANR4932I Reclamation process 12 ended for storage pool ADPPOOL.
ANR0986I Process 12 for SPACE RECLAMATION running in the FOREGROUND processed 255
items for a total
of 459,854 bytes with a completion state of SUCCESS at 15:42:00.
ANR4936I Reclamation of storage pool ADPPOOL has ended. Files reclaimed: 255,
Bytes reclaimed:
459854, Files reconstructed: 255, Unreadable files: 0.
```

After the reclamation, Example 7-10 shows the change in occupancy of the active-data pool. The reclamation process is analogous to expiration processing for the Tivoli Storage Manager server database. In this example it removes the inactive versions of the 100 updated files in ADPPOOL.

Example 7-10 Active-data pool occupancy after reclamation

```
tsm: TSMAIX55>Q OCC ACTNODE1

Node Name   Type   Filespace     FSID    Storage       Number of     Physical      Logical
                   Name                  Pool Name         Files        Space        Space
                                                                     Occupied     Occupied
                                                                         (MB)         (MB)
----------  ----  ----------    -----   ----------    ---------     ---------     ---------
ACTNODE1    Bkup  \\eifel\c$        2   ADPPOOL             155          0.21          0.21
ACTNODE1    Bkup  \\eifel\c$        2   BACKUPPOOL          355          0.60          0.60
```

At this point the setup of the active-data pool for fast client restore is complete.

7.2.2 Set up an active-data pool to reduce resources

As described in “Types of active-data pools” on page 72, you can also set up active-data pools on removable media for offsite storage, which reduces the storage resources containing a node’s data. We show how to do that in this section.

1. As shown in Example 7-11, we define an active-data pool to use tape volumes.

Example 7-11 Define active-data pool to reduce resources

```
tsm: TSMAIX55>DEFINE STGPOOL AD2TAPEPOOL LTO4 POOLTYPE=ACTIVEDATA MAXSCRATCH=1000
ANR2200I Storage pool AD2TAPEPOOL defined (device class LTO4).
```

2. Define a domain that you will assign your client nodes to. If you decide to use an existing domain, update the domains ACTIVEDESTINATION parameter as desired. Example 7-12 shows the definition for a new domain.

Example 7-12 Define new domain

```
tsm: TSMAIX55>DEFINE DOMAIN ACTIVE2TAPEDOMAIN ACTIVEDESTINATION=AD2TAPEPOOL
ANR1500I Policy domain ACTIVE2TAPEDOMAIN defined.
```

3. Configure the details for the policy set, copygroup, and management class, as shown in Example 7-13. If you have used an existing domain, you can skip this step.

Example 7-13 Set up policy set, management class, and copy group

```
tsm: TSMAIX55>DEFINE POLICYSET ACTIVE2TAPEDOMAIN ACTIVE2TAPEPOLICY
ANR1510I Policy set ACTIVE2TAPEPOLICY defined in policy domain ACTIVE2TAPEDOMAIN.

tsm: TSMAIX55>DEFINE MGMTCLASS ACTIVE2TAPEDOMAIN ACTIVE2TAPEPOLICY ACTIVE2TAPEMGMT
ANR1520I Management class ACTIVE2TAPEMGMT defined in policy domain
ACTIVE2TAPEDOMAIN, set ACTIVE2TAPEPOLICY.

tsm: TSMAIX55>DEFINE COPYGROUP ACTIVE2TAPEDOMAIN ACTIVE2TAPEPOLICY ACTIVE2TAPEMGMT
DESTINATION=BACKUPPOOL VERE=10 VERD=10
ANR1530I Backup copy group STANDARD defined in policy domain ACTIVE2TAPEDOMAIN,
set ACTIVE2TAPEPOLICY, management class ACTIVE2TAPEMGMT.

tsm: TSMAIX55>ASSIGN DEFMGMTCLASS ACTIVE2TAPEDOMAIN ACTIVE2TAPEPOLICY
ACTIVE2TAPEMGMT
ANR1538I Default management class set to ACTIVE2TAPEMGMT for policy domain
ACTIVE2TAPEDOMAIN, set ACTIVE2TAPEPOLICY.

tsm: TSMAIX55>ACTIVATE POLICYSET ACTIVE2TAPEDOMAIN ACTIVE2TAPEPOLICY
ANR1554W DEFAULT Management class ACTIVE2TAPEMGMT in policy set ACTIVE2TAPEDOMAIN
ACTIVE2TAPEPOLICY does not have an ARCHIVE copygroup:  files will not be archived
by default if this set is activated.

Do you wish to proceed? (Yes (Y)/No (N)) y
ANR1554W DEFAULT Management class ACTIVE2TAPEMGMT in policy set ACTIVE2TAPEDOMAIN
ACTIVE2TAPEPOLICY does not have an ARCHIVE copygroup:  files will not be archived
by default if this set is activated.
ANR1514I Policy set ACTIVE2TAPEPOLICY activated in policy domain
ACTIVE2TAPEDOMAIN.
```

4. Set up schedules to reclaim the active-data pool and to copy active data, as shown in Example 7-14.

Example 7-14 Define schedules for active-data pools

```
tsm: TSMAIX55>DEFINE SCHEDULE RECLAIM_AD2TAPEPOOL TYPE=ADMINISTRATIVE CMD="RECLAIM
STG AD2TAPEPOOL THRESH=1" ACTIVE=YES STARTTIME=07:30 PERIOD=1
ANR2577I Schedule RECLAIM_AD2TAPEPOOL defined.

tsm: TSMAIX55>DEFINE SCHEDULE COPYACTIVE2TAPE_BACKUPPOOL TYPE=ADMINISTRATIVE
CMD="COPY ACTIVEDATA BACKUPPOOL AD2TAPEPOOL" ACTIVE=YES STARTTIME=08:30 PERIOD=1
ANR2577I Schedule COPYACTIVE2TAPE_BACKUPPOOL defined.
```

5. Assign the nodes that you selected to be a member of the domain created, as shown in Example 7-15. If you updated an existing domain you can skip this step.

Example 7-15 Assign node to ADP domain

```
tsm: TSMAIX55>UPD NODE ACTNODE2 DOMAIN=ACTIVE2TAPEDOMAIN
ANR2063I Node ACTNODE2 updated.
```

6. We did not configure the active-data pool for synchronous write. The storage pool BACKUPPOOL is still set to synchronously write to the active-data pool ADPPOOL, as defined in step 8 on page 80.

   Example 7-16 shows the data occupancy after some backups are done for node ACTNODE2. You can see that ACTNODE2 only occupies space in the primary pool, since the node is not eligible to write to ADPPOOL, and BACKUPPOOL is not configured to synchronously write to AD2TAPEPOOL.

Example 7-16 QUERY OCCUPANCY before reclamation

```
tsm: TSMAIX55>Q OCC ACTNODE*

Node Name   Type   Filespace     FSID    Storage       Number of     Physical      Logical
                   Name                  Pool Name         Files        Space        Space
                                                                     Occupied     Occupied
                                                                         (MB)         (MB)
----------  ----  ----------    -----   ----------    ---------     ---------     ---------
ACTNODE1    Bkup  \\eifel\c$        2   ADPPOOL             155          0.21          0.21
ACTNODE1    Bkup  \\eifel\c$        2   BACKUPPOOL          355          0.60          0.60
ACTNODE2    Bkup  \\eifel\c$        1   BACKUPPOOL          255          0.45          0.45
```

7. We define a schedule in Example 7-14 called COPYACTIVE2TAPE_BACKUPPOOL to copy the active data to the tape active-data pool. To force the copy to happen immediately, we use the COPY ACTIVEDATA command, as shown in Example 7-17.

Example 7-17 Copy active data immediately

```
tsm: TSMAIX55>COPY ACTIVEDATA BACKUPPOOL AD2TAPEPOOL WAIT=YES
ANR0984I Process 13 for COPY ACTIVEDATA started in the FOREGROUND at 16:45:27.
ANR2110I COPY ACTIVEDATA started as process 13.
ANR1178I Copying active files from  primary storage pool BACKUPPOOL to active data
pool AD2TAPEPOOL started as process 13.
ANR1184I Copy active data process 13 ended for storage pool BACKUPPOOL.
ANR0986I Process 13 for COPY ACTIVEDATA running in the FOREGROUND processed 155
items for a total of 303,104 bytes with a completion state of SUCCESS at 16:47:41.
ANR1318I Copying active data from primary storage pool BACKUPPOOL to active data
pool AD2TAPEPOOL has ended.  Files Copied Up: 155, Bytes Copied Up: 303104,
Unreadable Files: 0, Unreadable Bytes: 0.
```

8. The QUERY OCCUPANCY command verifies that the active data for node ACTNODE2 is now stored in AD2TAPEPOOL configured above, as shown in Example 7-18.

Example 7-18 QUERY OCCUPANCY after copying active data

```
tsm: TSMAIX55>Q OCC ACTNODE*

Node Name   Type   Filespace     FSID    Storage       Number of     Physical      Logical
                   Name                  Pool Name         Files        Space        Space
                                                                     Occupied     Occupied
                                                                         (MB)         (MB)
----------  ----  ----------    -----   ----------    ---------     ---------     ---------
ACTNODE1    Bkup  \\eifel\c$        2   ADPPOOL             155          0.21          0.21
ACTNODE1    Bkup  \\eifel\c$        2   BACKUPPOOL          355          0.60          0.60
ACTNODE2    Bkup  \\eifel\c$        1   AD2TAPEPOOL         155          0.28          0.28
ACTNODE2    Bkup  \\eifel\c$        1   BACKUPPOOL          255          0.45          0.45
```

9. With the Tivoli Storage Manager server setup based on the commands above, data is written to AD2TAPEPOOL only when the schedule COPYACTIVE2TAPE_BACKUPPOOL is run or if the COPY ACTIVEDATA command is used. We chose this setup as it does not require a mount point in the tape library during backup, which would be required if synchronous write was configured. If you want to configure for synchronous write, update the ACTIVEDATAPOOLS parameter for your primary storage pool to point to the active-data pool, as shown in Example 7-19.

   Example 7-19 Allow synchronous write to active-data pool

   ```
   tsm: TSMAIX55>UPDATE STGPOOL BACKUPPOOL ACTIVEDATAPOOLS=ADPPOOL, AD2TAPEPOOL
   ANR2202I Storage pool BACKUPPOOL updated.
   ```

   Note that although we have configured two active-data pools for synchronous write from BACKUPPOOL, since our two policy domains each specify a different active-data pool destination, only one pool is used for synchronous write by each client.

You can now start including your active-data pool volumes as part of your physical or electronic vaulting configuration. Doing this saves you storage and bandwidth by copying and restoring only the active data.

If you are using active-data pools to replace a current copy storage pool, you could delete the schedule to back up your primary pool, and update the primary pool so that no copy storage pool is defined. Once all active data has been copied to the active-data pool you then could delete the copy storage pool. Only perform these steps if you are replacing the copy storage pool with the active-data pool. We generally recommend that both be maintained if having the ability to restore inactive versions of backup data is required. Also, if the copy storage pool contains archive or HSM files, do not delete the copy storage pool.

7.2.3 Restore client objects from an ADP

When restoring client data, the server selects the active version of a file from an active-data pool when appropriate. The following restore order applies:

1. Active-data pool (FILE)
2. DISK (random)
3. FILE (primary or copyboy)
4. Active-data pool sequential onsite
5. Sequential onsite-volume (primary or copy)
   priority considers:
   a. mounted (idle)
   b. automated
   c. manual
6. Sequential offsite-volume (primary, copy or ADP)

Restore when there is no ADP

To simulate a restore without an ADP configured, we set the active-data pool's volume to UNAVAILABLE. We configured BACKUPPOOL to migrate to a tape primary storage pool, and set the migration thresholds to 0 to empty BACKUPPOOL completely. We then started a client restore. Since the data was not available in BACKUPPOOL, and the tape volume in the active-data pool was UNAVAILABLE, the restore then mounted two tape volumes from the tape primary pool, as shown in the activity log records in Example 7-20.

Example 7-20 Volume selection during restore where ADP is not available

```
ANR0406I Session 123 started for node ACTNODE1 (WinNT).
ANR1183I Initial determination of removable volumes required for a restore request
from session 123 is complete. Additional volumes may still be required.
ANR8337I LTO volume 936AAFL4 mounted in drive DRIVE1 (/dev/rmt0).
ANR0510I Session 123 opened input volume 936AAFL4.
ANR0514I Session 123 closed volume 936AAFL4.
ANR8468I LTO volume 936AAFL4 dismounted from drive DRIVE1 (/dev/rmt0) in library
3200LTO4.
ANR8337I LTO volume 937AAFL4 mounted in drive DRIVE1 (/dev/rmt0).
ANR0510I Session 123 opened input volume 937AAFL4.
ANR0514I Session 123 closed volume 937AAFL4.
```

The client restore statistics are shown in Example 7-21.

Example 7-21 Client restore, no ADP

```
tsm> res c:\demodata\ -repl=yes
ANS1247I Waiting for files from the server...

Total number of objects restored:       104
Total number of objects failed:           0
Total number of bytes transferred:    173.03 KB
Data transfer time:                   78.70 sec
Network data transfer rate:            2.19 KB/sec
Aggregate data transfer rate:          1.38 KB/sec
Elapsed processing time:            00:02:04
```

Restore when an ADP exists and is available

We changed the access mode for the ADP volumes to read/write and performed the same restore operation. The server activity log shows that this time, the data is restored from the ADP, as shown in Example 7-22.

Example 7-22 Volume selection during ADP NQR restore

```
ANR0406I Session 125 started for node ACTNODE1 (WinNT).
ANR1183I Initial determination of removable volumes required for a restore
request from session 125 is complete. Additional volumes may still be required.
ANR8340I FILE volume /tsm/stg/activedata/0000002B.BFS mounted.
ANR0510I Session 125 opened input volume /tsm/stg/activedata/0000002B.BFS.
ANR0514I Session 125 closed volume /tsm/stg/activedata/0000002B.BFS.
```

Compare the client restore statistics shown in Example 7-23 with those of Example 7-21 on page 85. The amount of data restored is the same. However, the data transfer rate and total processing time are much faster, since the data was restored from a disk storage pool containing only the active data, rather than having to mount multiple tape volumes and searching past inactive data.

Example 7-23 Client restore from ADP

```
tsm> res c:\demodata\ -repl=yes
ANS1247I Waiting for files from the server...

Total number of objects restored:       104
Total number of objects failed:           0
Total number of bytes transferred:    173.03 KB
Data transfer time:                     1.18 sec
Network data transfer rate:           146.26 KB/sec
Aggregate data transfer rate:          26.17 KB/sec
Elapsed processing time:            00:00:06
```

Client restores can start almost immediately from an ADP, as there is no overhead in the mount processing for volumes and skipping over inactive object versions is not necessary. This is just a simple example to show you the benefit of ADP setup for important nodes where you want a fast restore for active versions of data.

7.2.4 Restore a storage pool or volume from an ADP

You may want to use ADPs to restore primary storage pools or volumes, as an alternative to restoring from a copy storage pool. Two new parameters are available with the RESTORE STGPOOL and RESTORE VOLUME command, ACTIVEDATAONLY and ACTIVEDATAPOOL. If the ACTIVEDATAONLY=YES parameter is specified during a storage pool or volume restore, only volumes from ADPs will be selected. If you want to restore from a specific ADP, specify ACTIVEDATAONLY=YES as well as ACTIVEDATAPOOL=<*active_data_pool_name*>.

You cannot specify the COPYSTGPOOL parameter together with the ACTIVEDATAONLY parameter. You have to choose one or other to restore from.

During a storage pool or volume restore from an ADP, only the active versions of files are available for restore since the active-data pool does not store inactive versions of files.

> **Note:** Objects that are inactive in the primary storage pool or volume being restored from an ADP are deleted from the server resulting in the loss of the inactive files.

In case you need to restore a primary storage pool or volume, you should always choose to restore from a copy storage pool if available. Restoring from a copy storage pool will recover all active and inactive files.

7.2.5 Manage objects in an ADP

You can think of an ADP as a collocated storage pool of active data. When client objects are backed up they become the active version and cause deactivation of the previously active versions, rendering them inactive. When logical files in an aggregate that are stored in an ADP are deactivated, the reclaimable space of volumes they are stored on increases immediately to reflect the space occupied by the inactive files. This means that reclamation begins sooner for volumes that contain inactive files in ADPs. If a non-aggregated file is deactivated in an ADP, it is deleted from the pool.

Figure 7-5 on page 87 demonstrates the collocation of active data within an ADP.

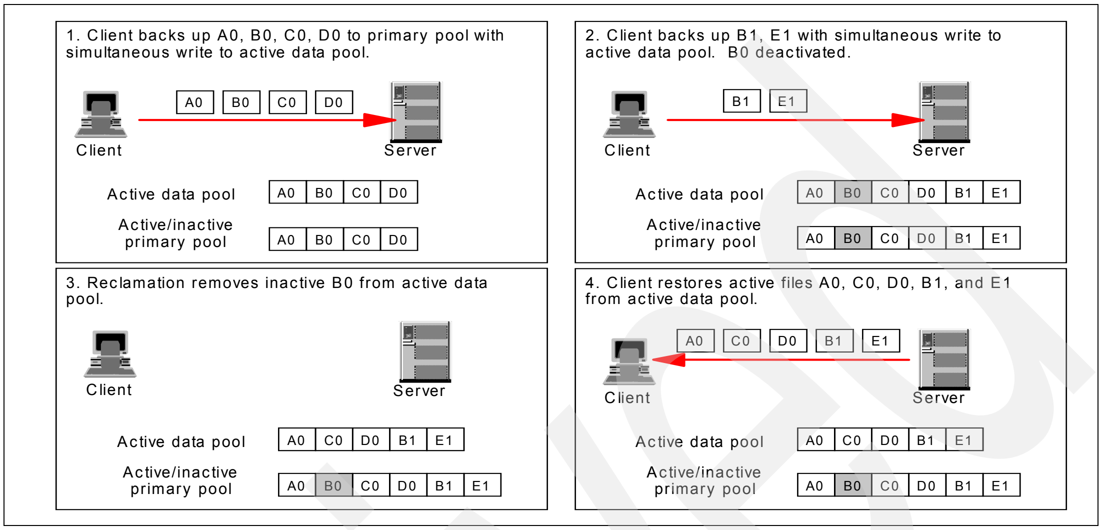

1. Client backs up A0, B0, C0, D0 to primary pool with simultaneous write to active data pool.
A0
B0
C0
D0
Client
Server
Active data pool
A0
B0
C0
D0
Active/inactive primary pool
A0
B0
C0
D0
2. Client backs up B1, E1 with simultaneous write to active data pool. B0 deactivated.
B1
E1
Client
Server
Active data pool
A0
B0
C0
D0
B1
E1
Active/inactive primary pool
A0
B0
C0
D0
B1
E1
3. Reclamation removes inactive B0 from active data pool.
Client
Server
Active data pool
A0
C0
D0
B1
E1
Active/inactive primary pool
A0
B0
C0
D0
B1
E1
4. Client restores active files A0, C0, D0, B1, and E1 from active data pool.
A0
C0
D0
B1
E1
Client
Server
Active data pool
A0
C0
D0
B1
E1
Active/inactive primary pool
A0
B0
C0
D0
B1
E1

Figure 7-5 Collocation of active data using ADP

ADP volumes will be reclaimed based on the percent reclaimable of each volume. As explained above, deactivation of files has the effect of causing the volumes percent reclaimable to increase and the volume to be reclaimed sooner than if it resided in a primary or copy sequential storage pool. Reclamation still occurs at regular intervals and removes inactive files from an ADP. Inactive files do not get copied to the target volume during reclamation, and the database is updated to show the inactive files as being removed.

Treatment of grouped data in an ADP: Grouped objects include system state and sub-file backups.

- Peer groups

  Group members are maintained in an active-data pool based on the active/inactive state of the leader. Inactive group members remain in the active-data pool until the leader becomes inactive. Once (and only when) the leader becomes inactive, the group will be removed from the active-data pool. If a group leader is a group member, a recursive check is made to find the top leader and act on its active/inactive state.

- Delta/base groups

  An inactive base is maintained in the active-data pool as long as any delta is active. Once all deltas become inactive along with the base, then the delta group is deleted.

- Attribute groups (TOCs)

  Attribute groups are not allowed to store TOCs in an active-data pool.

7.3 Summary

Tivoli Storage Manager introduces a new type of storage pool, the active-data pool, for storing only the active (current) versions of your backup data.

To obtain the benefits of an ADP, as a Tivoli Storage Manager administrator you now know that you need to perform the following tasks:

1. Determine the primary purpose of the ADP (fast restores, reducing the number of volumes, or saving bandwidth) and define a storage pool using the appropriate device type.
2. Define or update a domain definition, specifying the ADP in which active node data will be stored.
3. Identify the nodes whose active data will be stored in the ADP and then assign the nodes to the domain.
4. Set up a schedule to copy the active data from primary storage pools to the ADP.
5. Configure simultaneous write operations to the ADP, if desired.
6. Monitor reclamation frequency for the ADP and, if necessary, tweak the thresholds.
7. Create a conventional copy storage pool to hold both active and inactive data (best practice).

The current versions of your backup data can now be grouped on disk during client backup to provide fast client restore times of backup data. Client restores for important nodes can begin almost immediately upon request without any further intervention or data staging.

Active-data pools complement copy storage pools when used for node and primary storage pool recovery. Active-data pools can be used for a fast recovery of your critical nodes, which have had their data backed up to active-data pools. Copy storage pools can be used to recover less critical nodes and any data objects that are damaged in primary pools.

8

Data shredding for disk storage pools

In this chapter we discuss:

- Data shredding - what it is
- Configuring Tivoli Storage Manager data shredding

Data shredding is also sometimes referred to as data wiping.

You will find a discussion of all aspects of Tivoli Storage Manager data security in *IBM Tivoli Storage Manager: Building a Secure Environment*, SG24-7505.

8.1 What is data shredding

Shredding is useful for confidentiality, because files are not entirely deleted using the operating system's default delete function. Typically, standard delete functions mark the space occupied by the file as free and update file system metadata structures, leaving the actual file contents intact on the physical medium. If the file system continues to be used, eventually this space will be assigned to other files and overwritten. However, if the file system has not been used intensively since the file was deleted, recovery or forensic tools have a good likelihood of retrieving deleted data in part or in whole by accessing the medium at low level.

Physical shredding

As with paper shredding, physical shredding is destroying the media on which the data is stored. Currently, this is the standard process for destroying data on optical formats (laser disc, CD, DVD, optical platter, and so forth) and microforms (microfiche and microfilm), but might also be used on magnetic media. The material is not available for reuse. However, pieces up to .625 of an inch might still remain after the process is complete.

Explicit overwrite of deleted data - data shredding

In computing, *data shredding* (often also known as *data wiping*) is the act of deleting a computer file securely, so that it cannot be restored by any means. This is done using special shredder software. Data shredding usually involves overwriting a file multiple times. Shredding a file is analogous to shredding a document using a paper shredder.

8.1.1 Introduction to data shredding with Tivoli Storage Manager

Shredding is the destruction of deleted data to make it difficult to discover and reconstruct that data later. Tivoli Storage Manager V5.4 and later support shredding data in random-access disk storage pools. You can shred sensitive data either automatically or manually.

Without shredding, after client data has been deleted (for example, if it has expired from the Tivoli Storage Manager database or by using a DELETE FILESPACE command) it might still be possible to recover the client data if you have the time and advanced tools. For sensitive data, this condition is a potential security exposure. The destruction of deleted data, also known as shredding, lets you store sensitive data so that it is physically overwritten one or more times after it is deleted. Tivoli Storage Manager performs shredding only on data in random-access disk storage pools. You can configure the server to ensure that sensitive data is stored only in storage pools in which shredding is enforced (*shred* pools).

Shredding occurs only after a data deletion commits and takes some time to complete after it is initiated. The space that is occupied by the data to be shredded remains occupied while the shredding takes place and is not available as free space for new data until the shredding is complete.

Tivoli Storage Manager V5.4 adds explicit overwrite of deleted data—data shredding functionality. This function allows the creation of data pools where expired files will be overwritten by a random write pattern. The number of overwrites is configurable. The objective is to make the data unreadable by forensic disk recovery tools.

We strongly recommend that write caching is disabled for any disk devices used to store sensitive data, because caching adversely affects shredding performance. For performance reasons, you need to also use Tivoli Storage Manager policy to ensure that only data that really needs to be shredded is written to shreddable storage pools.

Note: In order for the shredding to be effective, every shred pattern must be written in order to the physical disk platter and errors must be reported synchronously and accurately. Achieving this behavior may require updating write cache settings in the disk, disk subsystem, operating system, and so on, to be *write-through*, or *inhibit cache write*, or *preserve write order*. It may be necessary to completely disable write caching.

8.1.2 Why use data shredding

When Tivoli Storage Manager expires data, the server database reference to the location of the object within the storage pools is deleted. By default, Tivoli Storage Manager does not physically delete the data, which therefore still exists on the volume or tape cartridge. When you set up a storage pool for data shredding, the data is physically overwritten on the disk on the next run of the SHRED DATA command, or as soon as possible, if the SHREDDING parameter is set to AUTOMATIC.

Using shredding for sensitive data enforces the data's physical deletion from Tivoli Storage Manager storage volumes. Good candidates for data shredding are data that is not encrypted, confidential data, or data, which is required by your security policy to be deleted permanently after it expires. Figure 8-1 on page 91 shows before and after illustrations for data that is deleted from a shreddable storage pool.

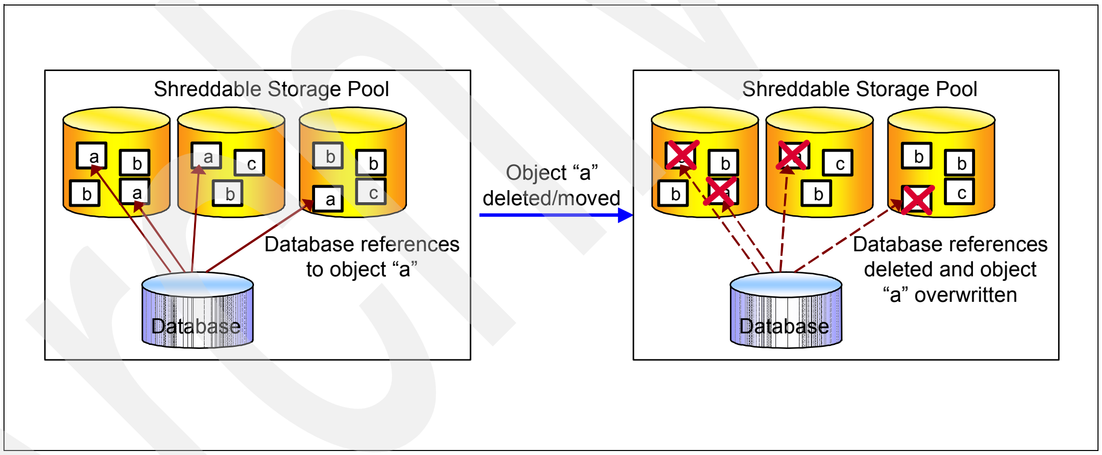


Figure 8-1 How data shredding works

8.2 Configuring data shredding with Tivoli Storage Manager

Tivoli Storage Manager performs shredding only on data in random-access disk storage pools. You can configure the server to ensure that sensitive data is stored only in storage pools in which shredding is enforced (shred pools). Shredding occurs only after a data deletion commits, but it is not necessarily completed immediately after the deletion. The space occupied by the data to be shredded remains occupied while the shredding takes place, and is not available as free space for new data until the shredding is complete.

Shredding performance is affected by the amount of data to be shredded, the number of times that data is to be overwritten, and the speed of the disk and server hardware. You can specify that the data is to be overwritten up to 10 times. Overwriting data more times gives greater security, since it lowers the likelihood of recovery, but it will also use more Tivoli Storage Manager server resources and impact performance.

In general, one shredding pass is sufficient in most circumstances. The first pass overwrites data so that it cannot be recovered by typical software-based forensic discovery tools. Performing additional shredding passes provides additional protection only against the use of specialized hardware or firmware forensic tools. The incremental benefit of each additional pass is less than linear. However, the performance overhead and degradation of each pass *is* linear. That is, the first shred pass of a specific amount of data takes about twice as long as it took to originally back up the data, two shred passes about three times as long, and so on.

Shredding can be done either automatically after the data is deleted or manually by command. The advantage of automatic shredding is that it is performed without administrator intervention whenever deletion of data occurs. This limits the time that sensitive data might be compromised. Automatic shredding also limits the time in which the space used by deleted data is occupied. However, the automatic shredding might impact server performance. Specifying manual shredding allows it to be performed when this process does not interfere with other server operations.

> **Note:** Tivoli Storage Manager data shredding is only implemented with random access storage pools.

8.2.1 Setting up shredding

This section describes how to configure Tivoli Storage Manager so that data identified as sensitive is stored only in storage pools that enforce shredding after that data is deleted. The process is:

1. Specify that you want data to be shredded either automatically after it is deleted or manually by an administrator. Specify how shredding is to be done using the SHREDDING server option in dsmserv.opt. If this parameter is not defined, the default is:

   ```
   shredding automatic
   ```

   You can also set the shredding option dynamically by using the SETOPT command. See Example 8-1.

Example 8-1 Setting shredding dynamically to manual

```
tsm: KODIAK>setopt shredding manual

Do you wish to proceed? (Yes (Y)/No (N)) y
ANR2119I The SHREDDING option has been changed in the options file.
```

2. Set up one or more random access disk storage pool hierarchies that will enforce shredding and specify how many times the data is to be overwritten after deletion. This is shown in Example 8-2, where we define two shredding pools so that SHREDPOOL-1 migrates to SHREDPOOL-2.

Example 8-2 Define a hierarchy of shredding and non-shredding pools

```
tsm: KODIAK>define stgpool shredpool-2 disk shred=10
ANR2200I Storage pool SHREDPOOL-2 defined (device class DISK).
tsm: KODIAK>define stgpool shredpool-1 disk shred=1
ANR2200I Storage pool SHREDPOOL-1 defined (device class DISK).
tsm: KODIAK>update stgpool shredpool-1 next=shredpool-2
ANR2202I Storage pool SHREDPOOL-1 updated
tsm: KODIAK>update stgpool shredpool-2 next=tapebackup
ANR1309W Shred value zero for storage pool TAPEBACKUP may render deleted data non
shreddable.
ANR2202I Storage pool SHREDPOOL-2 updated.
```

The SHRED parameter indicates how many times the data is to be overwritten. You can set the SHRED parameter to any value from 1 to 10.

> **Note:** The server issues a warning when the NEXTSTGPOOL is a non-shreddable pool.

If the value of SHRED is 0, which is the default, no shredding is performed. Caching is not allowed on a shreddable pool. Therefore, the CACHE parameter must be set to NO on the storage pool.

3. Define volumes to those pools and specify disks for which write caching can be disabled, as in Example 8-3.

Example 8-3 Define volumes in shredding pools

```
tsm: KODIAK> define volume shredpool-1 /tsm/stg/shred1.dsm formatsize=10
ANR2491I Volume Creation Process starting for /tsm/stg/shred1.dsm
Process Id 148
ANS8003I Process number 148 started.
```

4. Similarly, we define a volume in the SHREDPOOL-2 called shred2.dsm:

```
define volume shredpool-2 /tsm/stg/shred2.dsm formatsize=10
```

5. Define and activate a policy for the sensitive data, as in Example 8-4. The policy binds the data to a management class whose copy groups specify the shred storage pools.

Example 8-4 Set up the policy to use shredding

```
tsm: KODIAK>define domain shredding
ANR1500I Policy domain SHREDDING defined.

define policyset shredding shredding
ANR1510I Policy set SHREDDING defined in policy domain SHREDDING.

tsm: KODIAK>define mgmtclass shredding shredding shredding
ANR1520I Management class SHREDDING defined in policy domain SHREDDING, set
SHREDDING.
tsm: KODIAK>define copygroup shredding shredding shredding type=backup
destination=shredpool-1
```

```
ANR1530I Backup copy group STANDARD defined in policy domain SHREDDING, set
SHREDDING, management class SHREDDING.

tsm: KODIAK>define copygroup shredding shredding shredding type=archive
destination=shreddingpool-
ANR1535I Archive copy group STANDARD defined in policy domain SHREDDING, set
SHREDDING, management class SHREDDING.

tsm: KODIAK>assign defmgmtclass shredding shredding shredding
ANR1538I Default management class set to SHREDDING for policy domain SHREDDING,
set SHREDDING.

tsm: KODIAK>validate policyset shredding shredding
tsm: KODIAK>activate policyset shredding shredding

Do you wish to proceed? (Yes (Y)/No (N)) y
ANR1514I Policy set SHREDDING activated in policy domain SHREDDING.
```

6. Identify those client nodes whose data must be shredded after deletion and assign them to the new domain. We redefined the node to Tivoli Storage Manager:

   ```
   update node KODIAK domain=shredding
   ```

7. We now write data in the shredding storage pool by running a backup from the client node.
8. We then delete it from the Tivoli Storage Manager database using the DELETE FILESPACE command, as shown in Example 8-5 on page 94.

Example 8-5 Deleting all file spaces

```
tsm: KODIAK>del files kodiak *
ANR2238W This command will result in the deletion of all inventory references
to the data on file spaces that match the pattern * (fsId=3) for node KODIAK,
whereby rendering the data unrecoverable.
Do you wish to proceed? (Yes (Y)/No (N)) y
ANS8003I Process number 10 started.

tsm: KODIAK>q files
ANR2034E QUERY FILESPACE: No match found using this criteria.
ANS8001I Return code 11.
```

You can see that the Tivoli Storage Manager database has no record of the data.

9. However, directly viewing the disk volume, the data can still be seen in the storage pool volume, as shown in Example 8-6. At some stage, the space in the volume is overwritten with new data, but this might not happen for some time.

Example 8-6 Contents of storage pool before shredding

```
SEFR^B ^A^A+^A'˜^A,+Ñ^B^D^D^C^O^D^A^S^Z=^GD^DH|^D^G+^S^M4^A-FREDAIXSTANDAR
D/usr/tivoli/tsm/client/ba/bin/test.txtSTANDARDDEFAULTroot^G    ^Vf^L^AM-^@^BI^O
^G^APM-^^M-^AñE=»¦E=»¦E=¦?^DM-^@^C^O^D^BM-^@this is a test.
this is a test.
this is a test.
this is a test.
this is a test.
this is a test.
this is a test.
this is a test.
SEFR^B ^B^A'˜TANDAR^O¦^A^F^O+'^P^F^O=^Am^E^O·^B^E^P^D^B^O^P^NARCHIVEPOOL^E^P^X
```

10. Then shred the data to overwrite it in the storage pool. Because we specified to use manual shredding with the SHREDDING server option in Example 8-1 on page 92, we start the shredding process with the SHRED DATA command. This command lets you specify how long the process runs before it is cancelled (the default allows the process to run until all of the data is shredded) and how the process responds to an I/O error during shredding. See the administrator’s reference for your server platform for full details of the syntax and these options. For objects that cannot be shredded, the server reports each object:

    ```
    SHRED DATA DURATION=20
    ```

    To monitor the data shredding process and to see how much data is waiting to be shredded, use the QUERY SHREDSTATUS command. The server reports a summary of the number and size of objects waiting to be shredded. More information is displayed if the QUERY SHREDSTATUS FORMAT=DETAILED command is used.

    Example 8-7 and Example 8-8 show the output of the QUERY SHREDSTATUS FORMAT=DETAILED command when shredding is not running and when shredding is running.

Example 8-7 Query shredding status with manual shredding and no SHRED DATA is running

```
tsm: KODIAK>q shredstatus format=detailed

       Shredding Active: No
 Objects Awaiting Shred: 471
    Occupied Space (MB): 7
Data Left To Shred (MB): 72
```

Example 8-8 Query shredding status with manual shredding and SHRED DATA is running

```
tsm: KODIAK>q shredstatus format=detailed

       Shredding Active: Yes
 Objects Awaiting Shred: 442
    Occupied Space (MB): 4
Data Left To Shred (MB): 36
```

Note that the line Data Left to Shred shows the actual data multiplied by the shred parameter. When the data-shredding process completes, a message is issued in the activity log (Example 8-9) that reports the amount of data that was successfully shredded and the amount of data that was skipped, if any.

Example 8-9 Result of shredding in activity log

```
ANR1326I Shredding process complete after shredding 7,545,305 bytes and skipping 0
bytes.
```

If automatic shredding is used, it starts automatically when shreddable data is deleted. When shredding starts, you see this activity log message:

```
ANR1329I Automatic shredding started
```

When shredding ends, you see a message like this in the activity log:

```
ANR1327I Automatic shredding stopped. Total bytes shredded was 6,916,840 and
total bytes skipped was 0 bytes
```

11. Finally, looking through the contents of the storage pool volume after shredding, we can no longer see any intelligible data, as shown in Example 8-10.

Example 8-10 Contents of the storage pool volume after shredding

```
^_^BSEFR^D ^A^A+^A'¯^DM-^[Ñ+i^\+bSf;eF8¦B¦$e^N¦t½"¦Uz.-µM-^P^B9% N¦-kG^^íynM-^G=

@-FM-^Y=M-^Nj(,óM-^P^?b«{=ñM-^B_G¿++¦^Eb
H(eºíM-^QB·^W^L^N^C/·"M-^Lq$.^LºM-^Z^Bá^PMNpx~G^UM-^S2n¿M-^AV--XZM-^N{,|óºcL«|M-
^R"M-^BM-^C7++-M-^Z+bA¦ÑeM-^H^ZgB-^S ^N+(i"pM-^MH.-:[^BM-^GtqNM-^TKM-^YGM-^L)(nI
H-+M-^^M-^N^LM-^PHó>(T«?'QM-^B¬^?^X+<M-^Seb°|ÑeTM-^V»+_^N%^Fd"¦ja.^NG~^Be^P+N+Gd
M-^CM-^HvnjM-^Jn-[QpM-^N^]_=óUM-^MB«¦=LM-^BQaa+-^G+b/P9e-V+B-$¦^N÷óM"^Q+^E.-_M-^
Q^B+Ñ7NvChG·^K%n^KM-^D5-b
pM-^N«+¦ó8RM-^B«^?-^RM-^Bx^Yi+M-^^6^Gbµ=M-^Re+M-^Z-B^V¦O^NG^KB"Fe=.^Pk^B<=tNºFG±

?~n,!M-^X-Td¬M-^N+?+ó^C9=«M-^@^]}M-^B^_d^[+M-^OaTb^](^De^LísB¦W¦^N^X^?X"?^D.-¦^V
```

8.2.2 Storage pool shredding considerations

At the time of writing, there are several current limitations for disk storage pool shredding:

- Only storage pools with a device class of DISK can be shredded.
- Centera and Snaplock storage pools do not allow shredding.
- If you enable shredding on a storage pool by specifying a SHRED value greater than zero, the value of the CACHE parameter must be NO. See Example 8-11.

  Example 8-11 Cache must be NO when SHRED value is greater than 0

  ```
  tsm: Kodiak>upd stgp SHREDPOOL-2 cache=yes
  ANR2588E UPDATE STGPOOL: Storage pool "SHREDPOOL-2" cannot have CACHE set
  to YES with a non zero SHRED attribute.
  ANS8001I Return code 3.
  ```

- You can set the NEXTSTGPOOL parameter for a shredded pool to point to a non-shredding pool. This might be a random access pool without shredding defined or a sequential access pool, which is incapable of data shredding. If you set the NEXTSTGPOOL to one of these types of pools, only data actually on the shreddable pool is shredded when eligible. You get a warning message when a shreddable pool's NEXTSTGPOOL parameter is set to point to a non-shreddable pool, as in Example 8-2 on page 93.

- When data on a shreddable pool migrates to the next storage pool in the storage hierarchy, when the migration is complete, the data in the source storage pool is shredded. As we just saw, the NEXTSTGPOOL of a shreddable pool does not have to be another shreddable pool. When defining the next storage pool as a non-shreddable pool, the server prints a warning message. If you force a migration process to start, you will then get a server warning that this is a non-shreddable pool. See Example 8-12.

Example 8-12 Forcing a migration to a non-shreddable pool will give a warning

```
tsm: KODIAK>update stg shredpool-2 hi=0 lo=0
ANR1309W Shred value zero for storage pool TAPEBACKUP may render deleted
data non shreddable.
ANR2202I Storage pool SHREDPOOL-2 updated.
```

However, if the migration is an automatic migration, the server does not print any warning message during the migration. This situation is typically the case if the NEXTSTGPOOL points to a pool using tape, as seen in the activity log for an automatic migration (Example 8-13).

Example 8-13 Automatic migration to a non-shreddable pool provide no messages

```
ANR0984I Process 152 for MIGRATION started in the BACKGROUND at 09:46:48.
ANR1000I Migration process 152 started for storage pool SHREDPOOL-2
automatically, highMig=0, lowMig=0, duration=No.
ANR0513I Process 152 opened output volume 686AAFL4.
ANR1001I Migration process 152 ended for storage pool SHREDPOOL-2.
ANR0986I Process 152 for MIGRATION running in the BACKGROUND processed 1 items
for a total of 20,480 bytes with a completion state of SUCCESS at 09:46:49.
ANR1329I Automatic shredding started.
ANR1327I Automatic shredding stopped. Total bytes shredded was 16,665 and total
bytes skipped was 0 bytes.
```

Note: If the storage pool specified in NEXTSTGPOOL is non-shreddable, the server will not print any warning message during migration.

Backing up or moving data from a shreddable pool

Data in a shreddable pool can be backed up to a copy storage pool with the BACKUP STGPOOL command or moved with the MOVE DATA command:

- If the destination is a non-shreddable pool, you must specify SHREDTONOSHRED=YES to force the backup to occur, as in Example 8-14.
- If the SHREDTONOSHRED keyword is not specified, the default value is NO and the server prints an error message and does not allow the backup, as in Example 8-15 on page 98.

When the command is complete, the original data has been shredded.

Example 8-14 MOVE DATA with SHREDTONOSHRED=YES

```
tsm: KODIAK>move data /tsm/stg/shred2.dsm stgpool=tapebackup shredtonoshred=yes
ANR2233W This command will move all of the data stored on volume
/tsm/stg/shred2.dsm to other volumes in storage pool TAPEBACKUP; the data
will be inaccessible to users until the operation completes.

Do you wish to proceed? (Yes (Y)/No (N)) y
ANS8003I Process number 19 started.
```

Example 8-15 MOVE DATA without SHREDTONOSHRED, default = no

```
tsm: KODIAK>move data /tsm/stg/shred2.dsm stgpool=tapebackup
ANR2233W This command will move all of the data stored on volume
/tsm/stg/shred2.dsm to other volumes in storage pool TAPEBACKUP; the data
will be inaccessible to users until the operation completes.

Do you wish to proceed? (Yes (Y)/No (N)) y
ANR1317E MOVE DATA: Storage pool TAPEBACKUP is not a shreddable pool.
ANS8001I Return code 3.
```

Note: Data defined for data shredding can be copied or moved to non-shreddable storage pools by explicitly allowing this.

These data copies should then be stored with extra care. You should also consider using encryption for such data.

Deleting data from a shreddable pool

When any data in a shreddable pool is deleted by any server function, such as EXPIRE INVENTORY, DELETE FILESPACE, or DELETE VOLUME, the data is shredded. When an object is deleted that has version copies in both shreddable and non-shreddable pools, the server only shreds the copies in the shreddable pools and does not print any warning message during deletion.

Important: Only data copies in a shreddable pool are shredded. You must make sure that any other copies are handled and discarded securely.

Shreddable pools and backup sets

Sensitive data can be exported and included in backup sets. By definition, those copies of the data are not shreddable. You must specify ALLOWSHREDDABLE=YES to allow data from a shreddable pool to be included in backup sets.

- For a GENERATE BACKUPSET command you must specify ALLOWSHREDDABLE=YES to include the shreddable files in the backupset.
- If the ALLOWSHREDDABLE keyword is not specified, the default value is NO and the server prints an error message for every shreddable file, and does not include this file in the backup set. This warning message appears in the activity log as the backup set is generated, but does not appear at the command line. See Example 8-16 for the command-line entries. Example 8-17 shows excerpts from the activity log.

Example 8-16 Command line to generate backup set without ALLOWSHREDDABLE

```
tsm: KODIAK>gen backupset grizzly test-backupset devc=lto4
ANR1112W : No table of contents destination storage pool available for backup set
for node GRIZZLY (data type File). The table of contents will not be created.
ANS8003I Process number 159 started.
```

Example 8-17 Activity Log output for GENERATE BACKUPSET without ALLOWSHREDDABLE

```
ANR3544E Generation of backup set for GRIZZLY as TEST-BACKUPSET.138619 (data type
File) skipped shreddable data object in file space / (fsId 2), file name
/lpp/bos/deinstl/bos.rte.boot/5.3.0.40/ bos.rte.boot.al, type File.
........ several similar messages skipped here.
ANR3501I Backup set for GRIZZLY as TEST-BACKUPSET.138619 (data type File)completed
successfully - processed 1216 files.
```

```
ANR1361I Output volume 725AAFL4 closed.
ANR0515I Process 159 closed volume 725AAFL4.
ANR3547I Backup set TEST-BACKUPSET.138619 used volume 725AAFL4.
ANR1779I GENERATE BACKUPSET process completed: 1 backupset(s) were generated or
defined out of 1 backupset(s) requested by the command's specifications.
ANR0986I Process 159 for GENERATE BACKUPSET running in the BACKGROUND processed
1216 items for a total of 14,468,945 bytes with a completion state of SUCCESS at
12:11:02.
```

9

Tape data encryption

In September 2006, IBM System Storage TS1120 Tape Drive introduced integrated encryption technology, which allows data encryption to be performed by the tape drive hardware instead of at the software level. Encryption is performed at full drive speed after data compression, which results in little or no additional overhead in encrypting data on tape drives.

With the IBM TS1040 LTO4 tape drives introduced in early 2007, hardware encryption was made available also with the LTO technology. Tivoli Storage Manager V5.4.1 and later support the LTO4 devices, including encryption support. This chapter primarily emphasizes the setup of encryption with Tivoli Storage Manager in the LTO4 environment, since this is the most recent encryption platform available. However, it also points out differences between LTO4 and TS1120 encryption setup.

> **Note:** TS1120 encryption setup is extensively covered in Chapter 6 of *IBM Tivoli Storage Manager: Building a Secure Environment*, SG24-7505.

Topics that we discuss in this chapter include:

- General introduction to encryption
- Overview of tape hardware encryption
- IBM Encryption Key Manager (EKM) server installation, backup, and recovery
- Encryption options with the LTO 4 and the TS1120 tape drives
- Configuring Tivoli Storage Manager with various encryption options
- Recommended best practices
- References

Other vendors have encryption-capable tape drives that might provide similar capabilities from a Tivoli Storage Manager perspective. Consult the vendor Web sites or other documentation for information about how to configure these devices.

We describe only Tivoli Storage Manager here. Consult the independent software vendor (ISV) matrix for LTO for information about other vendor applications that support any of the encryption methods:

http://www-03.ibm.com/systems/storage/tape/pdf/compatibility/lto_isv_matrix.pdf

9.1 Introduction to encryption

Encryption is the process of transforming plain text into an unintelligible format, also known as *cipher text,* so that anyone who does not have the encryption key cannot access the data. Encryption is a critical technique for securing data, because even if an intruder gains physical access, they cannot interpret any of the information. If you do not know how the data was encrypted, it can range from hard to virtually impossible to decrypt the data.

Encryption can be implemented in hardware or software:

- Hardware-based encryption

  Hardware-based encryption is performed by special processors in certain types of hardware (such as a tape drive, a network router, or a specialized appliance), which are very fast and can encrypt in real time. There is no impact to the data transfer rate and no CPU resources on the computer server are needed, because the encryption is off-loaded to other hardware.

- Software-based encryption

  Software-based encryption uses the server CPU to do the work. Because most computer CPUs are not specialized for encryption, this can take longer and consume CPU resources that otherwise are available for other operations.

Tivoli Storage Manager can support both software encryption and hardware encryption. Software encryption is implemented within the Tivoli Storage Manager client. Hardware encryption is available with certain tape drives.

While there are many methods of encryption, modern encryption methods can be classified as either symmetric or asymmetric encryption.

9.1.1 Symmetric encryption

Symmetric encryption is also referred to as *private-key cryptography*, because a single secret key is used to both encrypt and decrypt the plain text. Several of the common symmetric encryption algorithms are Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES (TDES), and Skipjack.

Plain text can then be encrypted into cipher text using a symmetric encryption key. The decryption process uses an identical key to transform the cipher text back to plain text. An advantage of using symmetric encryption is the encryption speed, which is much faster than asymmetric encryption. The major drawback of symmetric encryption is related to sharing the private or secret key with the receiving party. How do we transmit this secret key to the recipient without anyone tampering with it? A common method of overcoming this problem is to use asymmetric key encryption to transmit the secret key.

9.1.2 Asymmetric encryption

Asymmetric encryption, on the other hand, uses a private/public key pair for the encryption process. A public key is used to encrypt the data and a private key is used to decrypt the data. The private/public keys are generated so that it is impossible to determine one key by using the other key. The public/private key pair eliminates the inherent problem of having to distribute the secret key that is required in the symmetric key encryption process.

9.1.3 Certificates, keystores, and key managers

A *digital certificate* is a digitally signed certificate that uniquely identifies the ownership of an an entity. Digital certificates are used in the asymmetric key cryptography process that uses a pair of digital keys, the public and private key pair for the encryption process.

A digital certificate is used to verify the ownership of a key when it is transmitted. The digital certificate verifies that it really came from the designated source.

The type of information that is stored within a digital certificate is:

- Key label
- Key size
- The subject distinguished name, for example, cn=AJcert1
- Name of the issuer
- The validity of the certificate

Digital certificates are normally signed by a certificate authority. A *certificate authority* is an entity that issues a signed digital certificate for use by another entity, that is, another person or server. Examples of commercially available certificate authorities are Verisign and Thawte. In addition, you can also create your own certification authority using OpenSSL, which is part of the open source project. The point is that if a key is sent embedded in a certificate from a trusted authority, you can then trust the contents, that is, the key itself.

A *keystore* is a repository for digital certificates. These certificates represent public and private encryption keys. Keystores are normally created and managed by a key management tool, also known as a *key manager*.

9.1.4 Tivoli Storage Manager client data encryption

When Tivoli Storage Manager client encryption is used, the data is encrypted by the client itself, and the data is therefore protected as soon as it leaves the client for its entire life span in the Tivoli Storage Manager storage hierarchy.

Most Tivoli Storage Manager clients, at V5.4.0 or later, can encrypt data using either DES56 or AES128 software encryption. Information regarding these encryption standards is available at the National Institute of Standards and Technology Web site:

http://csrc.nist.gov/CryptoToolkit/tkencryption.html

Both DES and AES are block ciphers and use symmetric key algorithms, which require substantially less CPU power than asymmetric algorithms. Symmetric key encryption schemes require the use of a shared secret key.

Prior to Tivoli Storage Manager V5.5, encryption using the backup-archive client required either that the user remember the encryption key password during restore or that the password be stored locally on the client system. Tivoli Storage Manager V5.5 is enhanced so that the Tivoli Storage Manager generates, encrypts, stores, and manages the encryption key in the Tivoli Storage Manager database. See 22.1, “Transparent client encryption” on page 288, for more information.

9.2 Introduction to tape hardware encryption

IBM offers hardware encryption on the IBM System Storage TS1120 and LTO4 tape drives. Tape hardware encryption performs the encryption of data as the data is written, and allows the use of AES256 encryption for any tapes that are written on the device, without any loss of performance as software-based encryption methods incur.

Below we discuss the use of each of these methods specifically with the IBM LTO4 tape drive in a Tivoli Storage Manager environment. The implementation with IBM TS1120 has been thoroughly described in *IBM Tivoli Storage Manager: Building a Secure Environment*, SG24-7505.

Data encryption can be enabled or managed at one of three levels: application, system, or library, as shown in Figure 9-1. *Application-managed encryption (AME)* is managed within a software application that uses the tape drive. Currently, IBM Tivoli Storage Manager is the only application that supports IBM Tape encryption. In this case, Tivoli Storage Manager manages the keys that are used for encryption.

The other two methods, *system-managed encryption (SME)* and *library-managed encryption (LME)*, use an external encryption key manager. You can also configure Tivoli Storage Manager to work with either of these methods. The external key manager that is required is a separately installed product called *IBM Encryption Key Manager (EKM)*.

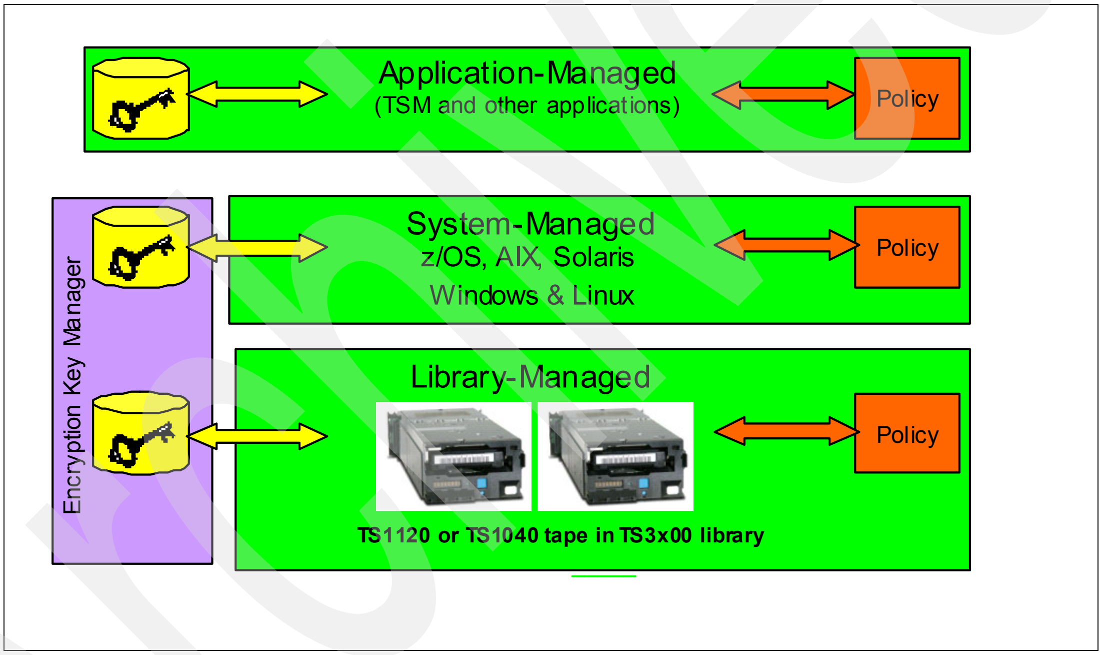


Figure 9-1 IBM Tape encryption methods

Application-managed encryption

Application-managed encryption (AME) for the IBM tape drive is performed through the application itself (in this case, Tivoli Storage Manager server). That is, the server functions as the key manager. The encryption policy that identifies where encryption is implemented is specified in the Tivoli Storage Manager device class definition using a new parameter, DRIVEENCRYPTION. See 9.3, “Tivoli Storage Manager with AME” on page 107, for more details.

Library-managed encryption

With LME, the tape library controls whether a specific cartridge is encrypted. By default, all tape cartridges within a library-managed logical library are enabled for encryption. In addition, LME provides you with the option to use barcode encryption policies (BEP, for the IBM

System Storage TS3500 only) to define which VOLSER within the logical library is encrypted. See 9.5, “Tivoli Storage Manager with LME” on page 123, for more details.

System-managed encryption

With SME, encryption within a logical tape library is determined at the tape drive level, because all of the tape drives within the logical library do not need to have encryption enabled. See 9.6, “Tivoli Storage Manager with SME” on page 126, for more details.

Both LME and SME require the use of the EKM. AME does not need or use EKM.

9.2.1 Overview of encryption methods

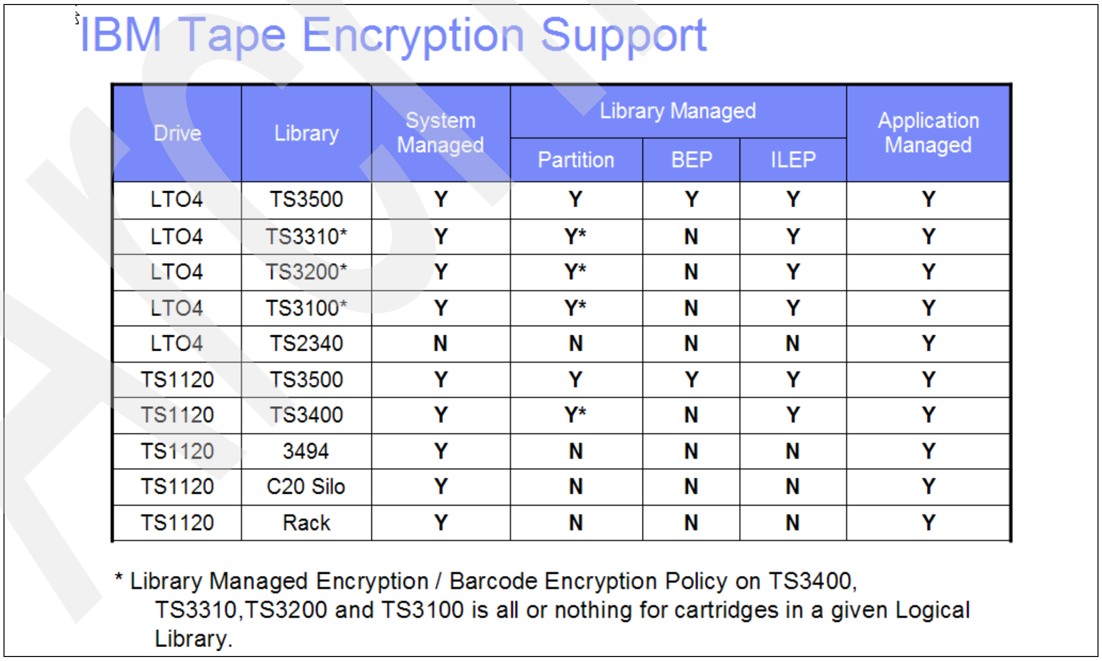
The IBM Tape drive encryption solution consists of three major components:

- LTO4 or TS1120 tape drive, either standalone or in a tape library
- Encryption key manager software (for SME and LME only)
- Encryption configuration policy

The following sections provide a high-level overview of the components. For more detailed information refer to:

- *IBM Encryption Key Manager component for the Java platform Introduction, Planning, and User's Guide*, GA76-0418
- *IBM System Storage Tape Encryption Solutions*, SG24-7320
- *IBM System Storage Tape Library Guide for Open Systems*, SG24-5946.

Figure 9-2 shows which encryption methods are supported with the different tapes and libraries.



IBM Tape Encryption Support

Drive	Library	System Managed	Library Managed			Application Managed
			Partition	BEP	ILEP	
LTO4	TS3500	Y	Y	Y	Y	Y
LTO4	TS3310*	Y	Y*	N	Y	Y
LTO4	TS3200*	Y	Y*	N	Y	Y
LTO4	TS3100*	Y	Y*	N	Y	Y
LTO4	TS2340	N	N	N	N	Y
TS1120	TS3500	Y	Y	Y	Y	Y
TS1120	TS3400	Y	Y*	N	Y	Y
TS1120	3494	Y	N	N	N	Y
TS1120	C20 Silo	Y	N	N	N	Y
TS1120	Rack	Y	N	N	N	Y

* Library Managed Encryption / Barcode Encryption Policy on TS3400, TS3310,TS3200 and TS3100 is all or nothing for cartridges in a given Logical Library.

Figure 9-2 Encryption methods supported for IBM tape hardware

> **Note:** Internal Label Encryption Policy (ILEP) is an enhancement to LME to specifically utilize NetBackup tape pools. For details use the VERITAS NetBackup documentation.

9.2.2 Encryption capable tape drives

The IBM Tape encryption solution uses an Advanced Encryption Standard (AES) algorithm with a key length of 256 bits. AES is a symmetric encryption key method, which means that the same key (private or secret key) is used for both encryption and decryption. The keys are identical.

All TS1120 tape drives shipped after the encryption announcement in late 2006 are automatically *encryption-capable*. All LTO4 tape drives are also automatically encryption-capable. Earlier TS1120-E05 tape drives can be upgraded to be encryption-capable by ordering chargeable feature codes 5592 or 9592.

However, the library must also be encryption-enabled:

- For all libraries, whether using 1120 or LTO4 tape drives, feature code 9900 must be specified.
- AME is available for all libraries at no charge, as long as feature code 9900 is specified.
- A TS1120 tape drive can be installed in TS3400 and TS3500 tape libraries, and provides encryption at no additional charge.
- LTO4 tape drives can be installed in TS3100, TS3200, TS3310, and TS3500 tape libraries. Transparent LTO encryption (that is, LME and SME) requires the chargeable feature code 5900 to be installed in the tape library, except for the TS3500, which uses feature code1604. When you order this feature code, you will receive a license string that must be entered on the library to enable the use of LME and SME. Consult the documentation for your library for details of how to do this.
- SME may not be supported for all operating systems environments. Verify the supported systems for each tape library.

Refer also to the tape documentation available at:

http://www.ibm.com/systems/storage/tape/

9.2.3 Tivoli Storage Manager configuration for encryption

The *encryption policy* is the process of defining which data to encrypt. The IBM Tape encryption solution provides policy options at three levels: the application layer, the system layer, and the library layer (AME, SME, and LME). IBM supports two methods for managing the encryption keys: either through the application (in open systems with AME) or through the EKM, with SME or LME.

We describe all three encryption methods that you can use with Tivoli Storage Manager, beginning with AME, which is the simplest, since it does not require EKM. Then we cover installation and configuration of the EKM because this application is required for both LME and SME. See 9.4, “Install and configure EKM” on page 110. There are also several common library configurations and device configurations for both LME and SME. We discuss these configurations in 9.4.5, “EKM configuration at the tape library” on page 123. Finally, we describe the specific configuration details for LME and SME individually.

> **Note:** *All* tape drives within a logical library must use the same encryption method. Mixing different encryption methods within the same logical library is not supported.
>
> ALMS is available as an option with the TS3500 tape library, providing enhanced flexibility and capabilities for partitioning the library. We would always recommend that you use ALMS if you have a TS3500.

9.3 Tivoli Storage Manager with AME

Application-managed encryption requires specific support from the application. For up-to-date information about applications that support AME on LTO drives and libraries, see:

http://www-03.ibm.com/systems/storage/tape/pdf/compatibility/lto_isv_matrix.pdf

In this mode, the application (which we describe using Tivoli Storage Manager) acts as the key manager and is responsible for managing the encryption keys. EKM is not used (and therefore does not have to be installed and configured) in this mode of encryption.

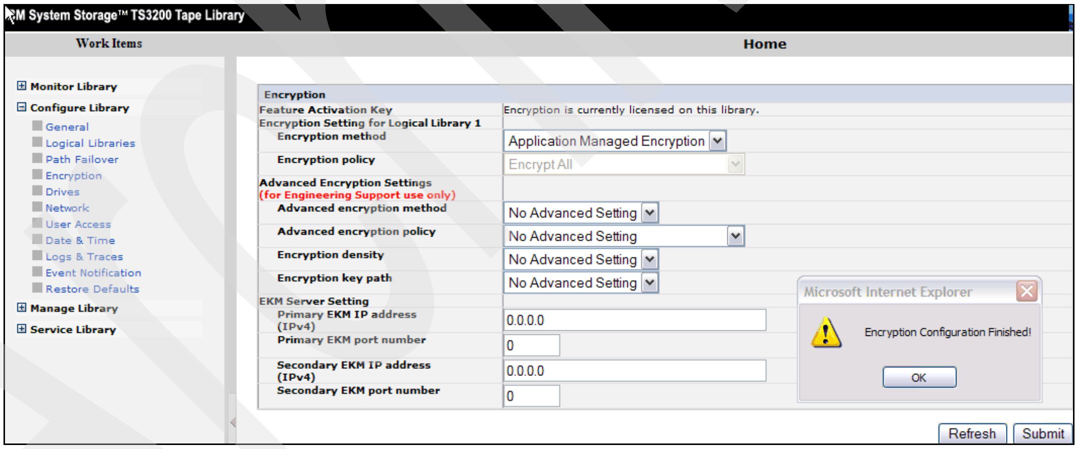
9.3.1 Configure the library to use AME

Check that the tape library firmware and tape drive firmware are at the correct levels to support encryption. This should generally be the latest available firmware, which you can download from:

ftp://ftp.ibm.com/storage

See your device documentation for instructions to update the firmware.

Configure the library to use AME. Use the Tape Library Specialist for your library. Figure shows the panel for the TS3200. To get there, navigate to **Configure Library ∅ Encryption** from the left panel, select **Application Managed Encryption** from the Encryption method pull-down, and click **Submit**. The configuration may take some time. Wait for the confirmation. Note that even though in our picture the feature activation key indicates that encryption is currently licensed on this library, this is not required if using AME.



Encryption	
Feature Activation Key	Encryption is currently licensed on this library.
Encryption Setting for Logical Library 1	
Encryption method	Application Managed Encryption
Encryption policy	Encrypt All
Advanced Encryption Settings (for Engineering Support use only)	
Advanced encryption method	No Advanced Setting
Advanced encryption policy	No Advanced Setting
Encryption density	No Advanced Setting
Encryption key path	No Advanced Setting
EKM Server Setting	
Primary EKM IP address (IPv4)	0.0.0.0
Primary EKM port number	0
Secondary EKM IP address (IPv4)	0.0.0.0
Secondary EKM port number	0

Encryption Configuration Finished!

Figure 9-3 Configure the TS3200 for AME

Now you can configure the tape device class to use AME, as described in the next section. When a backup is directed to an AME-configured device class, the procedure is:

1. The tape drive mounts a tape for encryption and sends the tape ID (VOLSER) to Tivoli Storage Manager.
2. Tivoli Storage Manager then generates a 256-bit AES data key, encrypts the data key, and stores the encrypted data key and the tape identifier in the Tivoli Storage Manager database.
3. The tape drive encrypts the data to the tape using the AES algorithms and the data key that was sent to the tape drive.

This option is the easiest to set up when Tivoli Storage Manager is the primary backup and restore software in a Windows, UNIX, or Linux environment, because generating, maintaining, and expiring the data keys is done transparently within Tivoli Storage Manager. However, encryption using AME is limited to Tivoli Storage Manager backup/archive data only. Backup sets and Tivoli Storage Manager database backup and export tapes are not encrypted by Tivoli Storage Manager when you use AME. Therefore, you need to manage these volumes with greater security, especially because the Tivoli Storage Manager database contains the secret keys that are used to encrypt and decrypt encrypted tapes. By contrast, SME and LME encrypts all Tivoli Storage Manager tapes.

> **Note:** The symmetric key is used to encrypt the data, and there is a separate key generated for each encrypted tape. Tapes encrypted with AME can only be decrypted with data keys that are stored in the Tivoli Storage Manager server database. Unlike LME and SME, the data key is *not* stored in a separate EKM database or on the tape cartridge. Therefore, you must make sure to secure Tivoli Storage Manager database backups, because without the database, which contains the encryption keys, you will not be able to decrypt any backed up data.
>
> Data that is encrypted using Tivoli Storage Manager with AME is *incompatible with SME* and *LME*. You cannot convert to LME or SME to recover the data.

9.3.2 AME configuration details

Our test environment uses Tivoli Storage Manager V5.5 on AIX, an IBM System Storage TS3200 Tape Library, and two LTO4 tape drives. We enable the encryption policy for AME with Tivoli Storage Manager.

Define a storage pool to use the encrypted device class

The steps are:

1. Define the library, drives, and paths as usual. There is no difference here whether you are using encryption or not. Our library is called 3200LTO4 with drives DRIVE1 and DRIVE2.
2. Define a device class (TSM-AME-ENC in our example) specifying the parameter DRIVEENCRYPTION=ON. This option indicates that Tivoli Storage Manager is providing the AME. See Example 9-1.

Example 9-1 Define the device class

```
tsm: TSMAIX55> define devclass TSM-AME-ENC library=3200LTO4 driveencrypt=on
```

3. Define a storage pool and associate it with the device class. See Example 9-2.

Example 9-2 Define storage pool T

```
tsm: TSMAIX55> define stgpool TSM-AME-POOL TSM-AME-ENC maxscr=10
```

4. We query the device class that we just created. See Example 9-3.

Example 9-3 Verify the storage pool and the device class that we created

```
tsm: TSMAIX55>q devclass tsm-ame-enc f=d

Device Class Name: TSM-AME-ENC
        Device Access Strategy: Sequential
            Storage Pool Count: 1
                   Device Type: LTO
```

```
                        Format: DRIVE
         Est/Max Capacity (MB):
                   Mount Limit: DRIVES
              Mount Wait (min): 60
         Mount Retention (min): 60
                  Label Prefix: ADSM
                       Library: 3200LTO4
                     Directory:
                   Server Name:
                  Retry Period:
                Retry Interval:
                        Shared:
            High-level Address:
              Minimum Capacity:
                          WORM: No
              Drive Encryption: On
               Scaled Capacity:
Last Update by (administrator): ADMIN
Last Update Date/Time: 11/14/07   13:37:43
```

Note: Drive Encryption is set to ON for Tivoli Storage Manager with AME.

5. Back up some data to the newly created encrypted device class.
6. To verify that the data stored on tape is encrypted with AME by Tivoli Storage Manager, query the tape volume in the storage pool that was used, as shown in Example 9-4. Note the field Drive Encryption Key Manager has the value *Tivoli Storage Manager*.

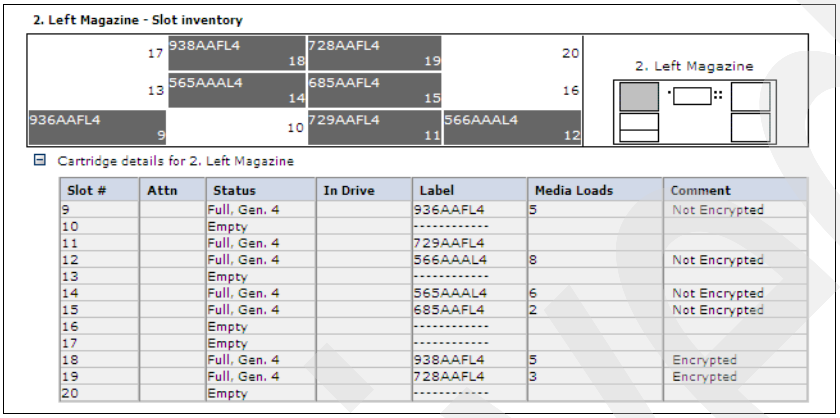
Example 9-4 Verify AME

```
tsm: TSMAIX55>query volume 938aafl4 f=d

Volume Name: 938AAFL4
             Storage Pool Name: TSM-AME-POOL
             Device Class Name: TSM-AME-ENC
            Estimated Capacity: 1,600,000.0
       Scaled Capacity Applied:
                      Pct Util: 0.1
                 Volume Status: Filling
                        Access: Read/Write
        Pct. Reclaimable Space: 0.0
               Scratch Volume?: Yes
               In Error State?: No
      Number of Writable Sides: 1
       Number of Times Mounted: 4
             Write Pass Number: 1
     Approx. Date Last Written: 11/21/07   10:05:09
        Approx. Date Last Read: 11/21/07   10:12:19
           Date Became Pending:
        Number of Write Errors: 0
         Number of Read Errors: 0
               Volume Location:
Volume is MVS Lanfree Capable : No
Last Update by (administrator):
         Last Update Date/Time: 11/21/07   09:28:42
```

```
          Begin Reclaim Period:
            End Reclaim Period:
  Drive Encryption Key Manager: Tivoli Storage Manager
```

7. You can also verify the status of the tape from the Tape Library Specialist. Select **Monitor Library ∅ Inventory** and expand the **Cartridge details** panel for the magazine where your tape is located. The panel shown in Figure 9-4 confirms that our tape volume is encrypted.



Slot #	Attn	Status	In Drive	Label	Media Loads	Comment
9		Full, Gen. 4		936AAFL4	5	Not Encrypted
10		Empty		------------		
11		Full, Gen. 4		729AAFL4		
12		Full, Gen. 4		566AAAL4	8	Not Encrypted
13		Empty		------------		
14		Full, Gen. 4		565AAAL4	6	Not Encrypted
15		Full, Gen. 4		685AAFL4	2	Not Encrypted
16		Empty		------------		
17		Empty		------------		
18		Full, Gen. 4		938AAFL4	5	Encrypted
19		Full, Gen. 4		728AAFL4	3	Encrypted
20		Empty		------------		

Figure 9-4 Inventory details confirming tape is encrypted in TS3200

> **Note:** With AME, the data keys that pertain to encrypted tapes are stored within the Tivoli Storage Manager database. It is important to keep the Tivoli Storage Manager database in a secure environment. Ideally, Tivoli Storage Manager database backup tapes also need to be kept separately from the data tapes, so that data is not compromised even if the Tivoli Storage Manager database is stolen. See *IBM Tivoli Storage Manager: Building a Secure Environment*, SG24-7505, for more information about security considerations.

9.4 Install and configure EKM

EKM is a Java-based application for performing key management. It is used for cryptographic key management when the backup application is not performing this function within the actual application. That is, EKM is required for IBM tape encryption using SME and LME, but not for AME.

At the time of writing, a small list of vendors is offering applications that can work with LME, SME, or both encryption methods. For details, see the independent software vendor (ISV) matrix for LTO referenced in the introduction.

We describe the encryption methods with EKM using Tivoli Storage Manager.

Encryption Key Manager (EKM) software

EKM can be downloaded from:

http://www.ibm.com/support/docview.wss?&uid=ssg1S4000504

At the time of writing, EKM is supported on z/OS, i5/OS, AIX, Linux, HP-UX, Sun Solaris, and Windows. You will find downloadable versions for all operating systems at this Web site. You can also obtain information relating to prerequisites and dependencies at the Web site.

Note: EKM code is required for enabling LME and SME with IBM TS1120 and LTO 4 Tape Drives. At the time of writing, in order to run the Encryption Key Manager with HP-UX, Sun Solaris, and Microsoft Window, the IBM TotalStorage Productivity Center - Limited Edition (TPC-LE) licensed program product 5608-VC6 is required.

TPC-LE is no longer available after February 8, 2008. It is replaced by IBM TotalStorage Productivity Center - Basic Edition, licensed program product 5608-B01. TPC Basic Edition includes the Encryption Key Manager code for HP-UX, Sun Solaris, and Microsoft Windows. However, note that TPC Basic Edition is a *chargeable* program product, whereas TPC-LE is a *no-charge* offering. Make sure to order TPC Basic Edition if you will run EKM on HP-UX, Solaris, or Windows.

Basically, encryption is similar for any type of tape drive. However, there are some significant differences in how the encryption keys are handled in the TS1120 compared to LTO4.

IBM TS1120

EKM uses both symmetric and asymmetric encryption to encrypt the data when writing and reading to a TS1120 encryption-enabled tape drive. Figure 9-5 shows a summary of the encryption process.

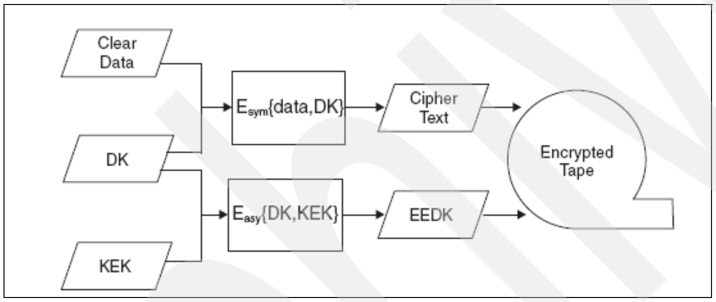


Figure 9-5 TS1120 encryption process

The process is:

1. When a scratch tape is first mounted, the tape drive communicates with the EKM to obtain the key necessary to encrypt the data.
2. EKM generates a random symmetric data encryption key. This is a secret key. It is also called the *data key* (DK) in EKM terminology. AES 256-bit encryption is used. The DK is used to encrypt the clear text to and form cipher text.
3. *Key labels* or aliases are associated with each tape drive that uses EKM. These key labels are linked to public key certificates stored within the keystore.
4. The DK is wrapped with the *public key* that is associated with the tape drive's key label. This public key is also called the *key encryption key* (KEK). The wrapped data key, along with key label information about which the private key is required to unwrap the symmetric key, forms a digital envelope called an *externally encrypted data key* (EEDK) structure.
5. Both the EEDK and the *wrapped DK* are stored on the tape.

The same encryption key (also known as the data key or DK) is used if more data is later appended to the same tape. It is then first read from the tape and used to encrypt the additional data.

LTO4

LTO4 tape encryption differs from the TS1120 tape encryption. EKM uses only the symmetric encryption to encrypt the data when writing and reading a LTO4 encryption-enabled tape drive. The LTO4 cannot store a wrapped form of the symmetric encryption key on the tape cartridge like the TS1120. The symmetric encryption key is stored in the keystore attached to the EKM. An associated key identifier or alias maps to the data key in the keystore. This alias is stored with each block of data on the tape. AES 256-bit encryption is used, like the TS1120, to encrypt and decrypt the data on the data cartridge.

Figure 9-6 shows the LTO4 encryption process.

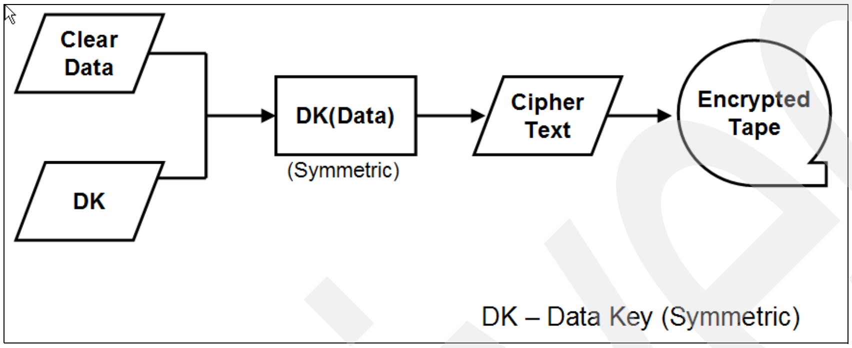


Figure 9-6 LTO4 encryption process

The process for a write request to the LTO4 with encryption is:

1. The LTO4 tape drive receives a mount request for write with beginning of tape (BOT) with encryption.
2. The LTO4 initiates a session with the EKM. The LTO4 communicates through the library using the TCP/IP protocol. The LTO4 requests a data key and passes an optional key label.
3. The EKM authenticates the LTO4 in its drive table.
4. The EKM retrieves a pre-generated AES-256 data key from the keystore.
5. The EKM sends a data key and a key identifier to the LTO4 in a secure manner.
6. The LTO4 receives the key structures and embeds the key identifier in the data and encrypts and writes the data to the tape.

The same encryption key (also known as the data key or DK) is used for restore or if more data is later appended to the same tape. The key identifier is retrieved from the tape and used to identify the corresponding AES key, which is then sent to the tape in a secure manner

EKM components

EKM consists of three components: the Java security keystore, the EKM configuration file, and the tape drive table. We describe how to configure EKM and each of these components in 9.4.2, “Configure EKM” on page 116.

Java security keystore

The *Java security keystore*, as the name implies, is a Java-based application used to hold the certificates and the keys that are used by EKM for cryptographic operations. EKM supports multiple Java keystores that offer various operational characteristics. Currently, the supported IBM keystores are:

- JCEKS
- JCE4758KS/JCECAAKS
- JCE4785RACFKS/JCECCARACFKS
- JCERACFKS
- PKCS11ImplKS
- IBMi5OSKeyStore

See the *IBM Encryption Key Manager component for the Java platform Introduction, Planning, and User's Guide*, GA76-0148, for detailed information about the EKM and its supported keystores. We show you how to create the keystore in "Create the keystore" on page 116.

EKM configuration file

This file controls the properties for EKM. The administrator needs to customize this file for the correct EKM operation. More details are in "Modify the EKM configuration file" on page 118.

Tape drive table

The tape drive table file is a binary file. You cannot edit it. The tape drive table file is used to track the tape devices with which EKM communicates to encrypt the data, linking the key labels with the key certificates in the keystore. "Define the tape drives" on page 121 shows how to update this drive table. The drive table file is stored in the location that is indicated by the config.drivetable.file.url parameter in the EKM configuration file.

Note: The EKM server needs to be up and running when you perform tape encryption and decryption. For redundancy reasons, there should be more than one EKM server. Data needs to be synchronized among the various servers. The TS3x00 libraries allow you to define up to four EKM servers. See the *IBM Encryption Key Manager component for the Java platform Introduction, Planning, and User's Guide*, GA76-0418, for more details.

9.4.1 Install EKM

EKM is a Java-based application that is used as the key manager when you configure Tivoli Storage Manager with LME or SME.

The configuration is largely the same for both LME and SME. Therefore, we present a single configuration sequence for you to use with either encryption method, and highlight any differences between the encryption methods.

Before installing EKM, verify that you have a supported operating system platform at:

http://www.ibm.com/support/docview.wss?&uid=ssg1S4000504

At this Web site you can also download the EKM application, documentation, a sample configuration file, and the correct Java Runtime Environment (JRE) that is required for the supported platforms. Encryption requires either Java 1.4.2 or Java 5.0. If you have an earlier JRE, make sure to update it.

The installation and configuration procedure is:

1. Install or update the JRE.

2. Install the *unrestricted policy files*. These files are needed by EKM to generate the encryption keys.
3. Install the EKM software.
4. Decide which keystore type to use. See “Java security keystore” on page 113.

   Also see the section “Which keystore is right for you” in the *IBM Encryption Key Manager component for the Java platform Introduction, Planning, and User’s Guide*, GA76-0418, for assistance on deciding which keystore type to use. Some keystores are, for example, only supported on particular operating system platforms.
5. Create the keystore and the required encryption keys.
6. Customize the EKM configuration file.
7. Start the EKM.
8. Define the tape drives with which the EKM communicates.

As an illustration, we show how to set up the EKM in an AIX environment using a Java Cryptographic Extension Keystore (JCEKS). The JCEKS keystore is a UNIX System Services Java file-based keystore that is supported on all platforms that can run the EKM. This keystore is password-protected and Triple Data Encryption Standard (DES)-encrypted.

For the details about installing the EKM on Windows, see *IBM System Storage Tape Encryption Solutions*, SG24-7320. The base EKM installation will be independent of the tape hardware used.

Install the IBM Java Runtime Environment

We downloaded the AIX Java package from this Web site and installed it according to the instructions:

http://www-128.ibm.com/developerworks/java/jdk/aix/service.html

For testing purposes we installed the Tivoli Storage Manager server and the EKM application on the same system. In an operational environment you would typically use a different system for your EKM Keystore, or for redundancy even use multiple systems.

The steps we took are:

1. We used the Java5-64 bit version of the JRE. If you do not already have an IBM registration ID, you need to register (which is free) before you can download this package. In our example, we downloaded the file j532redist.tar to a new /usr/java50 subdirectory and ran the command **tar -xvf j564redist.tar**. Example 9-5 shows the files and directories extracted.

   Example 9-5 Output from installation of the Java Runtime Environment

   ```
   /usr/java50 # ls -la
   total 183976
   drwxr-xr-x   4 bin      bin            256 Nov 21 17:04 .
   drwxr-xr-x  34 root     system        4096 Nov 15 09:01 ..
   -rw-r-----   1 root     system    94187520 Nov 21 17:04 j564redist.tar
   drwxr-xr-x  31 bin      bin           4096 Nov 18 2005  license
   drwxr-xr-x   7 bin      bin            256 Oct 31 04:21 sdk
   ```

2. Set the Java home directory. We modified .profile to include the environment variables shown in Example 9-6 because we use the Korn shell. Remove any possible Java 1.4 references from the PATH and add the new Java 5.0.

Example 9-6 Set JAVA_HOME

```
...
# Java 1.5.0 additions
P8=/usr/java50/sdk/jre/bin
P9=/usr/java50/sdk/bin
JAVA_HOME=/usr/java50/sdk/jre
CLASSPATH=/usr/java50/sdk/jre/lib
PATH=$PATH:$JAVA_HOME:$P8:$P9:.
```

3. After reloading the profile, confirm that the Java version is correct (Example 9-7 on page 115).

Example 9-7 Java version output

```
/home/root> java -version
java version "1.5.0"
Java(TM) 2 Runtime Environment, Standard Edition (build pap64devifx-20071025
(SR6b))
IBM J9 VM (build 2.3, J2RE 1.5.0 IBM J9 2.3 AIX ppc64-64 j9vmap6423-20071007
(JIT enabled)
J9VM - 20071004_14218_BHdSMr
JIT  - 20070820_1846ifx1_r8
GC   - 200708_10)
JCL  - 20071025
```

4. In our experience it is also necessary to set the primary new Java modules in executable mode. Specifically, add the x-mode to the files in /usr/java50/sdk/bin and to selected files in /usr/java50/sdk/jre/bin.

Install the unrestricted policy files

Regardless of which version of Java you use, you must replace the US_export_policy.jar file and local_policy.jar file in your $JAVA_HOME/lib/security directory with the versions downloaded from IBM. These unrestricted policy files are required by the EKM so that it can serve the AES keys.

Note that you must be a registered IBM user to access these files. Registration is free and simple. Download the files from:

https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk

The new policy files are shown in Example 9-8.

Example 9-8 Unrestricted policy files copied

```
/home/root> cd $JAVA_HOME/lib/security
/usr/java50/sdk/jre/lib/security> ls -al
total 128
drwxr-xr-x   2 bin      bin             256 Nov 14 17:54 .
drwxr-xr-x  11 bin      bin            4096 Oct 30 04:39 ..
-rw-r--r--   1 bin      bin            2199 Nov 14 17:57 US_export_policy.jar
-rw-r--r--   1 bin      bin           40624 Oct 30 04:39 cacerts
-rw-r--r--   1 bin      bin            2646 Oct 30 04:39 java.policy
-rw-r--r--   1 bin      bin            9609 Oct 30 04:39 java.security
```

```
-rw-r--r--    1 bin       bin             2212 Nov 14 17:57 local_policy.jar
```

Install the EKM jar and configuration file

The steps to install the EKM jar and configuration file are:

1. Download the latest EKM jar file, IBMKeyManagementServer.jar, from this Web site:

   http://www.ibm.com/support/docview.wss?&uid=ssg1S4000504

2. Copy the file IBMKeyManagementServer.jar file into the $JAVA_HOME/lib/ext directory, as in Example 9-9.

Example 9-9 Location of IBMKeyManagementServer.jar file

```
/usr/java50/sdk/jre/lib/ext> ls -al
total 7624
drwxr-xr-x   2 root     sys            512 Oct 09 08:43 .
drwxr-xr-x  10 root     sys           1024 Oct 09 08:43 ..
-rw-r--r--   1 bin      bin         183719 Oct 30 04:39 CmpCrmf.jar
-rw-r-----   1 root     system      459018 Nov 15 09:16 IBMKeyManagementServer.jar
...
```

3. From the same Web site, also download the sample EKM configuration files, KeyManagerConfig.properties and CliKeyManagerConfig.properties, and copy them to your base EKM directory /usr/ekm.

9.4.2 Configure EKM

There are two steps to configure EKM: create the keystore and modify the EKM configuration files.

Create the keystore

The keystore is used to store the encrypted keys and certificates. We use the keytool utility, located in the $JAVA_HOME/bin directory. This directory was added to our path in Example 9-6 on page 115.

We recommend that you use the *Keytool User Guide for SDK 1.4.2* or *5.0* as a reference, depending on the Java version that you are using. It is available at:

http://www-128.ibm.com/developerworks/java/jdk/security/142/secguides/keytoolDocs/KeyToolUserGuide-142.html

http://www-128.ibm.com/developerworks/java/jdk/security/50/secguides/keytoolDocs/KeyToolUserGuide-150.html

In our example, we use the JCEKS keystore, because this keystore is supported on all the EKM platforms.

> **Note:** There have been some changes in the keytool utility. In earlier versions of the user guides you may find the **`keytool -genkey`** followed by a **`keytool -selfcert`** command. This can now be done with one single command, **`keytool -genseckey`**. The old commands are still available, and the -genkey parameter is still used for TS1120 and RSA definitions.
>
> Refer to *IBM Encryption Key Manager component for the Java platform Introduction, Planning, and User's Guide*, GA76-0418, and the Keytool user guides mentioned for details.

When creating the keystore, remember that the LTO4 drive and the TS1120 use different encryption levels:

- LTO4: AES encryption with 256 bits
- TS1120: RSA encryption with 2048 bits

In this example we provide the definitions for the LTO4. See the other guides referenced for TS1120 definitions.

1. In Example 9-10 on page 117, we use **keytool** to create a self-signed symmetric key pair with the AES encryption algorithm. We recommend that you create a dedicated directory, for example, /usr/ekm before, you run the **keytool** commands. The first command (with the -genseckey option) creates the specified keystore file because it does not already exist, AJkeys.jcks, in our example. We also specify an EKM password with the -keypass parameter (passphrase, in our example), which is used whenever we start or run the EKM program.

   We create 17 certificates: AJcert3, and similarly AJcert4, and then the range IBM01–0F. The **keytool** command generates the keystore in the current directory, so be sure to change to the wanted directory first (in our example /usr/ekm).

Example 9-10 Commands to create keystore and generate self-signed certificates

```
#Command to generate a single key AJcert3
keytool -genseckey -alias AJcert3 -dname CN=AJcom -keystore AJkeys.jcks -provider
IBMJCE -keyalg AES -keysize 256 -keypass "passphrase" -storepass "passphrase"
-storetype JCEKS -validity 999

#Command to generate a range of keys IBM01 - IBM0F
keytool -genseckey -aliasrange IBM01-0f -dname CN=AJcom -keystore AJkeys.jcks
-provider IBMJCE -keyalg AES -keysize 256 -keypass "passphrase" -storepass
"passphrase" -storetype JCEKS -validity 999
```

2. We can list our generated certificates in the keystore, as shown in Example 9-11.

Example 9-11 List the certificates that are stored in the keystore

```
/usr/ekm # keytool -list -storetype JCEKS -keystore AJkeys.jcks -storepass
passphrase -provider IBMJCE

Keystore type: JCEKS
Keystore provider: IBMJCE

Your keystore contains 17 entries

ajcert3, Nov 22, 2007, SecretKeyEntry,
ajcert4, Nov 22, 2007, SecretKeyEntry,
ibm000000000000000009, Nov 22, 2007, SecretKeyEntry,
ibm000000000000000008, Nov 22, 2007, SecretKeyEntry,
ibm000000000000000007, Nov 22, 2007, SecretKeyEntry,
ibm00000000000000000f, Nov 22, 2007, SecretKeyEntry,
ibm000000000000000006, Nov 22, 2007, SecretKeyEntry,
ibm00000000000000000e, Nov 22, 2007, SecretKeyEntry,
ibm000000000000000005, Nov 22, 2007, SecretKeyEntry,
ibm00000000000000000d, Nov 22, 2007, SecretKeyEntry,
ibm000000000000000004, Nov 22, 2007, SecretKeyEntry,
ibm00000000000000000c, Nov 22, 2007, SecretKeyEntry,
ibm000000000000000003, Nov 22, 2007, SecretKeyEntry,
ibm00000000000000000b, Nov 22, 2007, SecretKeyEntry,
ibm00000000000000000a, Nov 22, 2007, SecretKeyEntry,
ibm000000000000000002, Nov 22, 2007, SecretKeyEntry,
ibm000000000000000001, Nov 22, 2007, SecretKeyEntry,
```

Modify the EKM configuration file

Example 9-12 on page 118 shows the modified KeyManagerConfig.properties file. We copied the sample file to the /usr/ekm directory and modified it as shown. It now points to our certificate file and our drive table file location /usr/ekm/keymanager/drivetable (indicated by the config.drivetable.file.url parameter). JCEKS is the default keystore type. Therefore, we did not have to alter these parameters. We set the tape discovery (drive.acceptUnknownDrives) to true. That adds the tape drives to the drive table as they are being used. However, this is not as secure as adding each tape manually.

The symmetricKeySet parameter listing must be added, identifying the actual keys used. The LTO4 encryption will use one pregenerated key for each tape. If there are not enough individual keys, they will be used in a round-robin fashion.

Also specify the full paths of any file to avoid possible ambiguities. The reference to config.drivetable.file.url is a URL reference and must be specified with the multiple slash characters (/).

Example 9-12 Customized KeyManagerConfig.properties file

```
TransportListener.ssl.port = 443
config.keystore.password.obfuscated = 450AB5A6B8B8B5ADB7A6B8AA
TransportListener.tcp.port = 3801
TransportListener.ssl.keystore.password.obfuscated = 020A72637575726A74637567
Admin.ssl.keystore.name = /usr/ekm/AJkeys.jcks
TransportListener.ssl.clientauthentication = 0
TransportListener.ssl.ciphersuites = JSSE_ALL
Audit.handler.file.size = 10000
drive.acceptUnknownDrives = true
Audit.metadata.file.name = /usr/ekm/metadata/EKMData.xml
TransportListener.ssl.truststore.name = /usr/ekm/AJkeys.jcks
Audit.handler.file.directory = /usr/ekm/logs
TransportListener.ssl.protocols = SSL_TLS
Admin.ssl.keystore.password.obfuscated = 060A76677979766E7867796B
config.keystore.file = /usr/ekm/AJkeys.jcks
TransportListener.ssl.keystore.name = /usr/ekm/AJkeys.jcks
Audit.eventQueue.max = 0
Audit.handler.file.name = kms_audit.log
Audit.event.outcome = success,failure
Audit.event.types = all
symmetricKeySet = ajcert3,ajcert4,ibm01-0f
config.drivetable.file.url = FILE:///usr/ekm/keymanager/drivetable
Admin.ssl.truststore.name = /usr/ekm/AJkeys.jcks
```

Modify the EKM client configuration file

Example 9-13 shows the modified CliKeyManagerConfig.properties file. We copied the sample file to the /usr/ekm directory and modified it as shown. This connects now to the keystore, and is used to start up the client session. All EKM commands are then issued in the client session.

Example 9-13 Customized CliKeyManagerConfig.properties

```
TransportListener.ssl.truststore.name=/usr/ekm/AJkeys.jcks
debug.output.file=debug
TransportListener.ssl.ciphersuites=JSSE_ALL
TransportListener.ssl.host=localhost
TransportListener.ssl.keystore.type=jceks
TransportListener.ssl.keystore.password.obfuscated=D80A48394B4B48404A394B3D
TransportListener.ssl.truststore.type=jceks
debug.output=simple_file
TransportListener.ssl.port=443
TransportListener.ssl.keystore.name=/usr/ekm/AJkeys.jcks
TransportListener.ssl.protocols=SSL_TLS
```

9.4.3 Start the EKM server

Example 9-15 on page 120 shows how to start EKM with the **EKMLaunch** command. This is quite different from earlier versions of EKM, so for versions with a build date of 05032007 or earlier, you must use the command **KMSAdminCmd** instead of **EKMLaunch**. You will find this difference in the examples of earlier guides. Use the latest version of *IBM Encryption Key Manager component for the Java platform Introduction, Planning, and User's Guide*, GA76-0418, for a reference.

Two logs in /usr/ekm can be used to verify that the startup is successful, native_stderr.log and native_stdout.log. Example 9-14 native_stdout.log shows the response that you could expect with a successful login. The logs will be generated in the current directory at startup, so we recommend running the startup commands from your EKM directory (/usr/ekm in our configuration).

Example 9-14 Listing of the native logs:

```
/usr/ekm # pg native_stderr.log
[Fatal Error] :-1:-1: Premature end of file.

/usr/ekm # pg native_stdout.log
Server initialized
Loaded drive key store successfully
Starting the Encryption Key Manager 2.1-20070924
Processing Arguments
Contact IBM support at 1-800-IBM-SERV (1-800-426-7378) or through your normal
business channel.
Processing
Server is started
```

Possible error codes are well described in the user's guide.

Additionally, the file /usr/ekm/logs/kms_audit.log keeps a cumulative audit log indicating the success of each step of EKM usage.

EKMLaunch starts the server in the background. After startup, we can start the client connection process with **KMSAdminCmd**. This command returns a hash symbol (#) prompt. We then log in to the EKM admin session to run the EKM commands, including the command to halt EMK again (**stopekm**). By default, the client user must log in to the server using ID EKMAdmin and password changeME. This password should then be changed wth the **chgpasswd** command. In Example 9-15 we show the login and some of the commands.

Example 9-15 EKM startup and use

```
/usr/ekm # java com.ibm.keymanager.EKMLaunch KeyManagerConfig.properties
Starting EKM Server...
Please check the logs to make sure EKM Server has started successfully.
/usr/ekm #
/usr/ekm # java com.ibm.keymanager.KMSAdminCmd
/usr/ekm/CliKeyManagerConfig.properties -i
#
# login -ekmuser EKMAdmin -ekmpassword changeME
User successfully logged in
#
# status
Server is running. TCP port: 3801, SSL port: 443
#
# listconfig
Audit.eventQueue.max=0
Admin.ssl.keystore.password.obfuscated=060A76677979766E7867796B
TransportListener.ssl.keystore.password.obfuscated=020A72637575726A74637567
TransportListener.tcp.port=3801
Admin.ssl.truststore.name=/usr/ekm/AJkeys.jcks
drive.acceptUnknownDrives=true
config.drivetable.file.url=FILE:///usr/ekm/keymanager/drivetable
Admin.ssl.keystore.name=/usr/ekm/AJkeys.jcks
Audit.event.outcome=success,failure
Audit.metadata.file.name=/usr/ekm/metadata/EKMData.xml
TransportListener.ssl.keystore.name=/usr/ekm/AJkeys.jcks
Audit.handler.file.size=10000
config.keystore.password.obfuscated=450AB5A6B8B8B5ADB7A6B8AA
TransportListener.ssl.clientauthentication=0
config.keystore.file=/usr/ekm/AJkeys.jcks
Audit.handler.file.name=kms_audit.log
TransportListener.ssl.port=443
Audit.event.types=all
TransportListener.ssl.truststore.name=/usr/ekm/AJkeys.jcks
TransportListener.ssl.ciphersuites=JSSE_ALL
TransportListener.ssl.protocols=SSL_TLS
symmetricKeySet=ajcert3,ajcert4,ibm01-0f
Audit.handler.file.directory=logs
#
# list
Keystore entries: 17

ajcert4, Fri Nov 16 08:39:08 CST 2007, keyEntry, AES, Active:True
ajcert3, Fri Nov 16 08:37:35 CST 2007, keyEntry, AES, Active:True
ibm000000000000000009, Thu Nov 22 10:57:56 CST 2007, keyEntry, AES, Active:True
ibm000000000000000008, Thu Nov 22 10:57:56 CST 2007, keyEntry, AES, Active:True
ibm000000000000000007, Thu Nov 22 10:57:56 CST 2007, keyEntry, AES, Active:True
ibm00000000000000000f, Thu Nov 22 10:57:56 CST 2007, keyEntry, AES, Active:True
```

```
ibm000000000000000006, Thu Nov 22 10:57:56 CST 2007, keyEntry, AES, Active:True
ibm00000000000000000e, Thu Nov 22 10:57:56 CST 2007, keyEntry, AES, Active:True
ibm000000000000000005, Thu Nov 22 10:57:56 CST 2007, keyEntry, AES, Active:True
ibm00000000000000000d, Thu Nov 22 10:57:56 CST 2007, keyEntry, AES, Active:True
ibm000000000000000004, Thu Nov 22 10:57:56 CST 2007, keyEntry, AES, Active:True
ibm00000000000000000c, Thu Nov 22 10:57:56 CST 2007, keyEntry, AES, Active:True
ibm000000000000000003, Thu Nov 22 10:57:56 CST 2007, keyEntry, AES, Active:True
ibm00000000000000000b, Thu Nov 22 10:57:56 CST 2007, keyEntry, AES, Active:True
ibm000000000000000002, Thu Nov 22 10:57:56 CST 2007, keyEntry, AES, Active:True
ibm00000000000000000a, Thu Nov 22 10:57:56 CST 2007, keyEntry, AES, Active:True
ibm000000000000000001, Thu Nov 22 10:57:55 CST 2007, keyEntry, AES, Active:True
#
# version
build-level = -20070924
#
# stopekm
EKMServer:  shut down complete.
/usr/ekm #
```

> **Note:** If you add new certificates while EKM is running, you must restart EKM in order to detect them.

Define the tape drives

To have tape drives automatically added when they are detected by EKM, we entered the *drive.acceptUnknownDrives = true* parameter in the EKM configuration file. This allows the EKM tape drive table to be automatically populated whenever a new tape drive contacts the EKM. From a security perspective, this parameter should be disabled to have full control of which tape drives are added.

Instead of automatically adding tape drives, add them manually using the **adddrive** command from the EKM prompt. You need the tape drive serial number to use the **adddrive** command. You can find the serial number inside Tivoli Storage Manager, as shown in Example 9-16.

Example 9-16 Display tape drive serial number

```
tsm: TSMAIX55>q drive f=d

Library Name: 3200LTO4
Drive Name: DRIVE1
Device Type: LTO
On-Line: Yes
Read Formats: ULTRIUM4C,ULTRIUM4,ULTRIUM3C,ULTRIUM3,ULTRIUM2C,ULTRIUM2
Write Formats: ULTRIUM4C,ULTRIUM4,ULTRIUM3C,ULTRIUM3
Element: 256
Drive State: EMPTY
Volume Name:
Allocated to:
WWN: 2001000E1110E588
Serial Number: 1310025518
Last Update by (administrator): ADMIN
Last Update Date/Time: 11/14/07   11:19:49
Cleaning Frequency (Gigabytes/ASNEEDED/NONE): NONE
```

Associated with each certificate is a *label* or *alias*. You can configure each tape drive with one or more certificate labels (certificates defined in Example 9-10 on page 117). You use the

EKM command **adddrive** to do this, within an EKM client session (session shown in Example 9-15 on page 120). The syntax for adding a tape drive identifying two possible key aliases that may be associated with the tape is:

```
# adddrive -drivename <serialnumber> [-rec1 <alias1>] [-rec2 <alias2>]
```

Example 9-17 shows our two drives added to the drive table.

Example 9-17 List drives defined to EKM

```
# listdrives
Drive entries: 2
SerialNumber = 001310025521
SerialNumber = 001310025518
```

For LTO4, there is only one key alias associated with each tape. This is different from TS1120, which can associate with two different keys, and thus provides for safer sharing of the tape with other organizations.

9.4.4 Register the EKM server with the tape library

To allow the tape library to communicate with the EKM server, you need to register all of your EKM servers within the Tape Library Specialist. You can register up to four EKM servers depending on the tape library. Refer to 9.4.5, “EKM configuration at the tape library” on page 123, to learn how to register your EKM servers.

If you have multiple EKM servers, you need to keep them synchronized, which can be done manually or automatically. For details, refer to the section “Synchronizing data between two EKM servers” in the *IBM Encryption Key Manager component for the Java platform Introduction, Planning, and User’s Guide*, GA76-0418, and *IBM Tivoli Storage Manager: Building a Secure Environment*, SG24-7505.

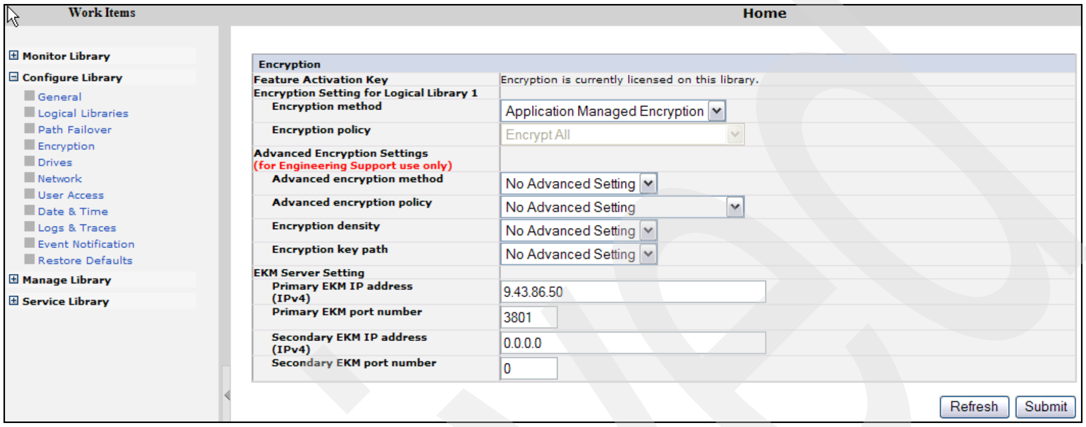
Managing certificates within the EKM

The administration of security policies differs from company to company. Depending on the security policies, an organization might want to regularly change the password. However, once you have set the keystore password, do not change it unless its security has been breached. The passwords are obfuscated to eliminate any security exposure. Changing the keystore password requires that the password on every key in that keystore be changed individually using the **keytool** command.

Note: Do not remove any certificates from the keystore because this prevents an encrypted tape from being read.

9.4.5 EKM configuration at the tape library

Use the Tape Library Specialist and modify the library EKM address panel to include the TCP/IP addresses of the EKM servers. Encryption must have been enabled for the library, as discussed in “Encryption capable tape drives” on page 106. For the TS3200, we see that the feature activation key indicates that encryption is licensed. To configure the EKM address, select **Configure Library ∅ Encryption** and set the EKM server settings as shown in Figure 9-7 on page 123.



Encryption	
Feature Activation Key	Encryption is currently licensed on this library.
Encryption Setting for Logical Library 1	
Encryption method	Application Managed Encryption
Encryption policy	Encrypt All
Advanced Encryption Settings (for Engineering Support use only)	
Advanced encryption method	No Advanced Setting
Advanced encryption policy	No Advanced Setting
Encryption density	No Advanced Setting
Encryption key path	No Advanced Setting
EKM Server Setting	
Primary EKM IP address (IPv4)	9.43.86.50
Primary EKM port number	3801
Secondary EKM IP address (IPv4)	0.0.0.0
Secondary EKM port number	0

Figure 9-7 Set EKM IP address

Enter the IP address of the key manager server. Port 3801 is the default port. Click **Submit** and wait for confirmation.

You are now ready to configure Tivoli Storage Manager for your chosen encryption method, LME or SME.

9.5 Tivoli Storage Manager with LME

With LME, the library manages the encryption policy. By default, the encryption policy encrypts all tape cartridges within a logical library. The data key is stored in the keystore, and depending on which type of tape, the key is stored on the tape as well (TS1120), or a key identifier is stored on the tape (LTO4). On the TS3500, LME provides you with the option to use a *barcode encryption policy* or *scratch encryption policy* (these terms are used interchangeably) to customize further which VOLSERs within the logical library to encrypt.

To enable LME within Tivoli Storage Manager, set the device class parameter DRIVEENCRYPTION to ALLOW. Then configure EKM as the key manager.

When a tape is mounted in the library, the library, through its encryption policies, determines whether the tape is encrypted or unencrypted. If it is an encrypted tape, or the data are to be encrypted, the drive sends a request via TCP/IP through the library to the EKM for the correct keys to encrypt the data to tape. Both symmetric and asymmetric encryption keys may be used in this process depending on the tape drive. Refer to 9.4, “Install and configure EKM” on page 110, for a description of how the encryption process occurs.

Since SME and LME both use the same EKM keystore, they are transparent to each other. In other words, a tape that is encrypted using SME can be decrypted using LME, and vice versa, provided they both have access to the same EKM keystore and both use the same device driver.

Note: LME is performed at the tape cartridge level. The default LME setting is to encrypt all cartridges in a logical library. Usage of the barcode encryption policy (BEP) is optional and is only available with LME for the TS3500 tape library. BEP is used to further define which tape cartridges to encrypt and which tape cartridges to leave unencrypted. The maximum allowable BEP is 300 for the entire TS3500 tape library. BEP is set up using the TS3500 Tape Library Specialist.

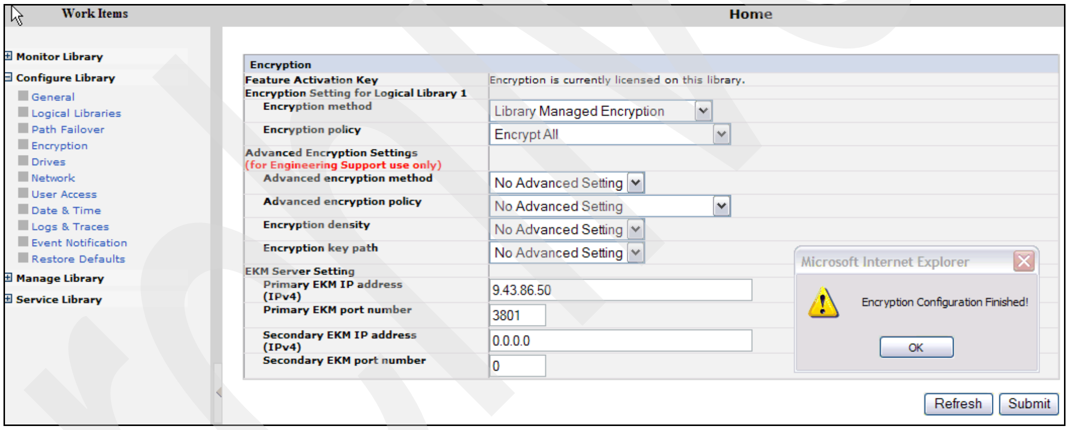
Enable the logical library for LME

As generally recommended, check that the tape library firmware and tape drive firmware are at the correct levels to support encryption. This should generally be the latest available firmware, which you can download from:

ftp://ftp.ibm.com/storage

See your device documentation for instructions to update the firmware.

LME for a logical tape library is enabled through the Tape Library Specialist. Use the Tape Library Specialist and modify the encryption method to LME. For the TS3200, select **Configure Library ∅ Encryption.** Select **Library Managed Encryption** from the Encryption method pull-down and click **Submit**. The display may change several times, wait for the completion message (shown in Figure on page 124).



Encryption

Feature Activation Key: Encryption is currently licensed on this library.

Encryption Setting for Logical Library 1

Encryption method: Library Managed Encryption

Encryption policy: Encrypt All

Advanced Encryption Settings (for Engineering Support use only)

Advanced encryption method: No Advanced Setting

Advanced encryption policy: No Advanced Setting

Encryption density: No Advanced Setting

Encryption key path: No Advanced Setting

EKM Server Setting

Primary EKM IP address (IPv4): 9.43.86.50

Primary EKM port number: 3801

Secondary EKM IP address (IPv4): 0.0.0.0

Secondary EKM port number: 0

Encryption Configuration Finished!

Figure 9-8   Set the TS3200 to LME

Verify Tivoli Storage Manager with LME

To verify Tivoli Storage Manager with LME:

1. Define a new device class, setting the parameter DRIVEENCRYPTION to ALLOW in order to enable LME. Example 9-18 shows the setting of this parameter for a device class named tsm-lme-dev. Set a storage pool to use this device class.

Example 9-18   TSM-LME-DEV device class with drive encryption value set to ALLOW

```
tsm: TSMAIX55>q devc tsm-lme-dev f=d

             Device Class Name: TSM-LME-DEV
        Device Access Strategy: Sequential
            Storage Pool Count: 1
                   Device Type: LTO
                        Format: DRIVE
         Est/Max Capacity (MB):
                   Mount Limit: DRIVES
```

```
              Mount Wait (min): 60
         Mount Retention (min): 60
                  Label Prefix: ADSM
                       Library: 3200LTO4
                     Directory:
                   Server Name:
                  Retry Period:
                Retry Interval:
                        Shared:
            High-level Address:
              Minimum Capacity:
                          WORM: No
              Drive Encryption: Allow
               Scaled Capacity:
Last Update by (administrator): ADMIN
         Last Update Date/Time: 11/16/07   10:06:23

tsm: TSMAIX55>q stg tsm-lme-pool f=d

               Storage Pool Name: TSM-LME-POOL
               Storage Pool Type: Primary
               Device Class Name: TSM-LME-DEV
....
```

2. Back up some data to this storage pool. The library loads a scratch tape, and since this was the first tape being used, the EKM drive table is updated with this tape information, as seen from the /usr/ekm/logs/kms_audit.log file (Example 9-19).

Example 9-19 kms_audit.log file showing new tape drive found

```
Runtime event:[
  timestamp=Thu Nov 22 16:36:20 CST 2007
  ComponentId=[threadId=Thread[Thread-17,5,KeyManagementServerV2-Processors]]
  event source=com.ibm.keymanager.j.gb
  outcome=[result=successful]
  event type=SECURITY_RUNTIME
  resource=[name= Drive Serial Number: 001310025518 WWN: 50050763124263C4 VolSer: 
938AAF;type=file]
  action=start
  ]
```

3. The tape volume shows that this is a library managed tape (Example 9-20). On the TS3200 Tape Library Specialist, when looking at the tape library inventory, a volume is only identified as encrypted, not by which method, as seen in Figure 9-4 on page 110.

Example 9-20 LME tape volume used

```
tsm: TSMAIX55>q vol 939AAFL4 f=d

                   Volume Name: 939AAFL4
             Storage Pool Name: TSM-LME-POOL
             Device Class Name: TSM-LME-DEV
            Estimated Capacity: 1,600,000.0
       Scaled Capacity Applied:
                      Pct Util: 0.0
                 Volume Status: Filling
```

```
                        Access: Read/Write
        Pct. Reclaimable Space: 0.0
               Scratch Volume?: Yes
               In Error State?: No
      Number of Writable Sides: 1
       Number of Times Mounted: 1
             Write Pass Number: 1
     Approx. Date Last Written: 11/22/07   16:43:55
        Approx. Date Last Read: 11/22/07   16:43:47
           Date Became Pending:
        Number of Write Errors: 0
         Number of Read Errors: 0
               Volume Location:
Volume is MVS Lanfree Capable : No
Last Update by (administrator):
         Last Update Date/Time: 11/22/07   16:43:33
          Begin Reclaim Period:
            End Reclaim Period:
  Drive Encryption Key Manager: Library
```

9.6 Tivoli Storage Manager with SME

Similar to LME, the encryption process is transparent to Tivoli Storage Manager. In contrast to LME, SME is enabled at the tape drive level. Therefore, not all tape drives within an SME system need to have encryption enabled. The data key is stored in the keystore, and additionally, the data key (TS1120) or a key identifier (LTO4) is stored on the tape.

To enable SME within Tivoli Storage Manager, the device class parameter DRIVEENCRYPTION is set to ALLOW. As with LME, SME uses the EKM to act as the key manager. In the case of Tivoli Storage Manager deployed in an AIX or Solaris environment, the key manager communicates with the Atape device driver to manage the encryption policies. Thus, the tape drive definitions must also be updated to reflect this.

Note: SME is, at the time of writing, available for Tivoli Storage Manager servers running on AIX, Solaris, Windows, Linux, and z/OS operating systems.

In this mode, the encryption process is transparent to the application that provides the data.

SME configuration details

Setting up SME on the LTO4 tape drive is similar to LME in that key management is still done by the EKM. We described how to set up EKM in “Install and configure EKM” on page 110.

As generally recommended, check that the tape library firmware and tape drive firmware are at the correct levels to support encryption. This should generally be the latest available firmware, which you can download from:

ftp://ftp.ibm.com/storage

See your device documentation for instructions to update the firmware.

We set up SME using the IBM AIX Atape device driver for the LTO4 drives. The configuration steps required to enable SME are:

1. Install or update the Atape device driver to the current level.
2. Enable the logical library for SME through the tape library specialist.
3. Update the Atape EKM proxy configuration file.
4. Update the Atape device driver configuration.
5. Verify that you have Tivoli Storage Manager with SME.

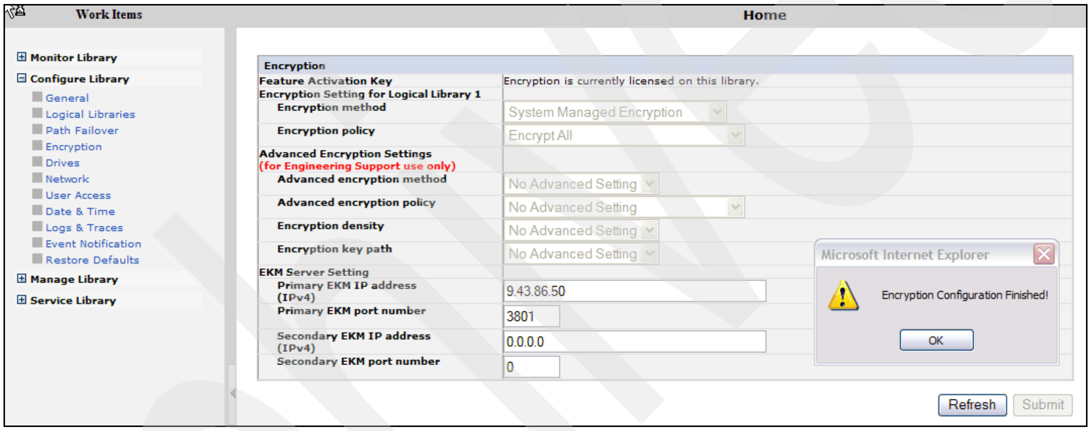
Install or update the Atape device driver

Upgrade to the latest version of the Atape device driver. You can download this version from:

ftp://ftp.software.ibm.com/storage/devdrvr

Enable the logical library for SME

SME for a logical tape library is enabled through the Tape Library Specialist. For the TS3200, select **Configure Library ∅ Encryption**, and select **System Managed Encryption** from the Encryption method pull-down. Also, if necessary, enter the TCP/IP address and port of the EKM servers as for LME. Click **Submit**. The display may change several times. Wait for the completion message (Figure 9-9 on page 127).



Encryption

Feature Activation Key	Encryption is currently licensed on this library.
Encryption Setting for Logical Library 1	
Encryption method	System Managed Encryption
Encryption policy	Encrypt All
Advanced Encryption Settings (for Engineering Support use only)	
Advanced encryption method	No Advanced Setting
Advanced encryption policy	No Advanced Setting
Encryption density	No Advanced Setting
Encryption key path	No Advanced Setting
EKM Server Setting	
Primary EKM IP address (IPv4)	9.43.86.50
Primary EKM port number	3801
Secondary EKM IP address (IPv4)	0.0.0.0
Secondary EKM port number	0

Microsoft Internet Explorer

Encryption Configuration Finished!

OK

Figure 9-9 Set the TS3200 for SME

Update the Atape EKM proxy configuration file

The Atape configuration must be aware of the addresses that the EKM servers need to be made known to Atape. The Atape EKM configuration file is called ibmekm.conf and is located in the /etc directory. In our example, Tivoli Storage Manager and EKM are both installed on the same server.

We modify the /etc/ibmekm.conf file to include the TCP/IP address and port that are used by the EKM server, as shown in Example 9-21.

Example 9-21 Modified copy of /etc/ibmekm.conf file

```
#  The Encryption Key Server address:port can be a local loop back
#  address 127.0.0.1:port if the server is on the same host or a network
#  address:port if external to the host. Up to 16 server address:port
#  entries are supported if there are multiple TCP/IP connections to the same
#  server and/or multiple servers.
#  server timeout address:port
ekmtest   10   127.0.0.1:3801
```

The entry in Example 9-21 indicates that the EKM application is installed on a server called ekmtest (note that this server parameter is not currently used, therefore it can be set to any value), with local loop back address, and is using port 3801 with a timeout of 10 seconds. If the EKM server is installed on another server, the timeout value must be increased to allow for potential network delay.

Atape device driver configuration

Two new attributes have been added to the tape drives for encryption. These attributes are listed in Example 9-22.

Example 9-22 Encryption attributes in the device driver

```
# lsattr -El rmt0| grep encrypt
drv_encryption  yes                Drive Encryption Support                    False
sys_encryption  no                 Use System Encryption FCP Proxy Manager     True
wrt_encryption  off                System Encryption for Write Commands at BOP True
```

Set the value of the sys_encryption attribute to yes to enable device driver SME for each tape drive.

The wrt_encryption attribute controls whether the device driver sets the tape drive to encryption-enabled for write commands. When set to off, the tape drive uses encryption for read operations, and write operations do not use encryption. When set to on, the tape drive uses encryption for both read and write operations. When set to custom, the device driver does not modify the current tape drive setting. The custom setting is intended for applications using SME to control write encryption without device driver intervention.

To enable SME, the sys_encryption parameter must be set to yes and the wrt_encryption parameter must be set to on.

These tape drive parameters can be modified using SMIT on AIX. Select **Change/Show Characteristics of a Tape Drive** and enable the parameters **Use System Encryption FCP Proxy Manager** and **System Encryption for Write Commands at BOP**. Repeat the process for all of the drives in the logical library. Example 9-23 shows the settings for one of the tape drives.

Example 9-23 Encryption attributes that are set for a tape drive

```
Change / Show Characteristics of a Tape Drive

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

                                                          [Entry Fields]
  Tape Drive                                            rmt0
  Tape Drive type                                       3580
  Tape Drive interface                                  fcp
  Description                                           IBM 3580 Ultrium Tape Drive
(FCP)
  Status                                                Available
  Location                                              1Z-08-01
  Parent adapter                                        fscsi0
  Connection address                                    2
  SCSI ID                                               0x10ae1
  Logical Unit ID                                       0x0
  World Wide Port Name                                  0x2002000e1110e588
  World Wide Node Name                                  0x2001000e1110e588
  New Logical Name                                     []
  Enable Alternate Pathing Support                   no +
  Block Size (0=Variable Length)                    [0] +#
  Use Hardware Compression on Tape                   yes +
  Use Autoloading Feature at End-of-Tape             no +
  (IBM 3581 and IBM 3583 with single drive only)
  Activate volume information logging                no +
  Maximum size of log file (in # of entries)        [500] +#
  Backward Space/Forward Space Record Mode           SCSI +
  Use Immediate Bit in Rewind Commands               no +
  Trailer Label Processing                           no +
  Use System Encryption FCP Proxy Manager            yes +
  System Encryption for Write Commands at BOP        on +
```

Example 9-24 on page 129 shows that both tape drives, rmt0 and rmt1, now have SME enabled.

Example 9-24 lsattr output

```
/usr/ekm # lsattr -El rmt0 |grep encrypt
drv_encryption yes              Drive Encryption Support                   False
sys_encryption yes              Use System Encryption FCP Proxy Manager     True
wrt_encryption on               System Encryption for Write Commands at BOP True

/usr/ekm # lsattr -El rmt1 |grep encrypt
drv_encryption yes              Drive Encryption Support                   False
sys_encryption yes              Use System Encryption FCP Proxy Manager     True
wrt_encryption on               System Encryption for Write Commands at BOP True
```

Verify Tivoli Storage Manager with SME

The device class parameters are the same for LME and SME (that is, set DRIVEENCRYPTION to ALLOW on the device class).

In Example 9-20 on page 125 we backed up some data to the previously created storage pool, which is configured using the LME device class TSM-LME-DEV. Now we backed up additional data using this device class, and a tape previously written using LME was mounted, and the volume was still identified as encrypted by LME (Example 9-25). Remember that SME and LME volumes can be encrypted by both methods.

Example 9-25 LME tape in use

```
q vol 939AAFL4 f=d

                   Volume Name: 939AAFL4
             Storage Pool Name: TSM-LME-POOL
             Device Class Name: TSM-LME-DEV
            Estimated Capacity: 1,600,000.0
       Scaled Capacity Applied:
                      Pct Util: 0.0
                 Volume Status: Filling
                        Access: Read/Write
        Pct. Reclaimable Space: 0.0
               Scratch Volume?: Yes
               In Error State?: No
      Number of Writable Sides: 1
       Number of Times Mounted: 2
```

```
            Write Pass Number: 1
    Approx. Date Last Written: 11/24/07   10:41:15
       Approx. Date Last Read: 11/22/07   16:43:47
          Date Became Pending:
       Number of Write Errors: 0
        Number of Read Errors: 0
              Volume Location:
Volume is MVS Lanfree Capable : No
Last Update by (administrator): ADMIN
        Last Update Date/Time: 11/24/07   10:36:53
         Begin Reclaim Period:
           End Reclaim Period:
  Drive Encryption Key Manager: Library
```

We then changed to a new device class set for SME, and made another backup. We noticed that a scratch tape was mounted, and this time the tape volume was listed as using system managed encryption (Example 9-26).

Example 9-26 SME tape volume used

```
q vol 566aaal4 f=d

                  Volume Name: 566AAAL4
            Storage Pool Name: TSM-SME-POOL
            Device Class Name: TSM-SME-DEV
           Estimated Capacity: 1,600,000.0
      Scaled Capacity Applied:
                     Pct Util: 0.0
                Volume Status: Filling
                       Access: Read/Write
       Pct. Reclaimable Space: 0.0
              Scratch Volume?: Yes
              In Error State?: No
     Number of Writable Sides: 1
      Number of Times Mounted: 2
            Write Pass Number: 1
    Approx. Date Last Written: 11/24/07   09:53:23
       Approx. Date Last Read: 11/24/07   09:30:15
          Date Became Pending:
       Number of Write Errors: 0
        Number of Read Errors: 0
              Volume Location:
Volume is MVS Lanfree Capable : No
Last Update by (administrator):
        Last Update Date/Time: 11/24/07   09:30:12
         Begin Reclaim Period:
           End Reclaim Period:
  Drive Encryption Key Manager: System
```

Since SME and LME both use the same EKM keystore, they are transparent to each other. In other words, a tape that is encrypted using SME can be decrypted using LME, and the reverse is also true, provided that they both have access to the same EKM keystore and both use the same device driver. Our tests verified this.

9.7 EKM server backup and recovery considerations

The operation of encryption with TS1120 and LTO4 is basically the same. For further details about how to secure the encryption information, the encryption keys for AME, or the EKM keystore for LME and SME, refer to *IBM Tivoli Storage Manager: Building a Secure Environment*, SG24-7505. Here is a summary of the information they contain:

- Use multiple EKM keystores and keep them synchronized.
- If using AME, keep Tivoli Storage Manager database tapes, which are unencrypted, in a secure location, separate from the storage pool tapes. AME stores all the data keys in the Tivoli Storage Manager database, so if the database tape is kept with the copy storage pool tapes, this can compromise the data.
- Back up the critical EKM files (that is, the drive table, the keystore, and the configuration file) by using another secure mechanism (for example, tar, WinZip, or similar) that is independent of the tape encryption. This backup should *not* be encrypted, but must be stored securely, and preferably in another secure location (for example, a vault).

Important: Losing the keystore password results in the loss of all digital certificates stored within the keystore. There is no recovery process from this situation.

9.8 References

References for this chapter include:

- *IBM Encryption Key Manager component for the Java platform Introduction, Planning, and User's Guide*, GA76-0418

  This Guide is the basis for EKM installation, and also provides a good general description with some special considerations for LTO4.
- *IBM Tivoli Storage Manager: Building a Secure Environment*, SG24-7505

  In Part 2, this guide has a very good description of implementing the EKM using the TS11200.
- *IBM System Storage Tape Encryption Solutions*, SG24-7320

  This guide is primarily for the System z, but the general description of encryption is generic across systems. Specifically, Chapter 7 addresses the TS1120 in an Open Systems environment.
- *Keytool User Guide for SDK 1.4.2*, available at:

  http://www-128.ibm.com/developerworks/java/jdk/security/142/secguides/keytoolDocs/KeyToolUserGuide-142.html
- *KeyTool User Guide for SDK 1.5,* available at*:*

  http://www-128.ibm.com/developerworks/java/jdk/security/50/secguides/keytoolDocs/KeyToolUserGuide-150.html
- *IBM System Storage Tape Library Guide for Open Systems*, SG24-5946

  This provides a short introduction to the concepts and encryption methods.
- *IBM Tape Device Drivers - Encryption Support*, GA32-0565
- *IBM System Storage TS1120 Tape Drive and Controller Operator Guide 3592 Models J1A, E05, J70 and C06*, GA32-0556

- The different tape library operators guides

10

NDMP

This chapter describes the new functions in Tivoli Storage Manager Version 5.4 for backup of a Network Attached Storage (NAS) file server by using the Network Data Management Protocol (NDMP). These functions are:

- Back-end data movement for NDMP backup images
- Filer-to-server backup

For information about the implementation of backing up a NAS file server by using NDMP refer to the *Tivoli Storage Manager Administrator's Guide* and the IBM Redbooks publication *Using the IBM System Storage N Series with IBM Tivoli Storage Manager*, SG24-7243.

10.1 Tivoli Storage Manager and NDMP

Tivoli Storage Manager Extended Edition can use Network Data Management Protocol (NDMP) to perform high-performance, scalable backups and restores of a Network Attached Storage (NAS) file server.

NDMP is an open standard network protocol that allows storage-management applications to control backup and recovery of an NDMP-compliant device over a network. This avoids installation of third-party backup software on the protected device. The NAS vendor deals with file system, bulk data transfer and secondary storage devices, and the backup vendors can then focus on control of backup and recovery operations and data management.

NDMP defines a mechanism and protocol for controlling backup, recovery, and other transfers of data between primary and secondary storage. It provides full or differential (files that have changed since last full backup) backup of a file system image at a directory or file system level, as well as restores of an entire file system or selected files and directories within the file system.

The NDMP client-server architecture separates the control and data flow:

- Data Management Application (DMA), also known as the NDMP client, which is typically a backup application. Since NDMP Version 4 support, NDMP clients are called DMAs.

  The DMA initiates, controls, and monitors NDMP sessions for backup and recovery of data and tracks and manages backups and media.
- The NDMP server performs one or more services:
  - The data service transfers data to and from primary storage (typically a NAS file system).
  - The tape service transfers data to and from secondary storage (typically a tape drive) and allows the DMA to manipulate and access secondary storage (tape positioning and I/O).
  - The SCSI service passes low-level SCSI commands from the DMA to a SCSI device (typically a media changer).

Tivoli Storage Manager V5.4 and later support NDMP V4 in two different configurations. We describe these in this chapter:

- Filer-to-attached-library
- Filer-to-server (new in V5.4)

10.1.1 Filer-to-attached-library

In the filer-to-attached-library configuration, the NAS device has access to a locally attached tape library. The library robotics can be controlled (via SCSI or Fibre Channel) by either the NAS device or the Data Management Application (DMA), which is the Tivoli Storage Manager server. Both options are shown in Figure 10-1 on page 135.

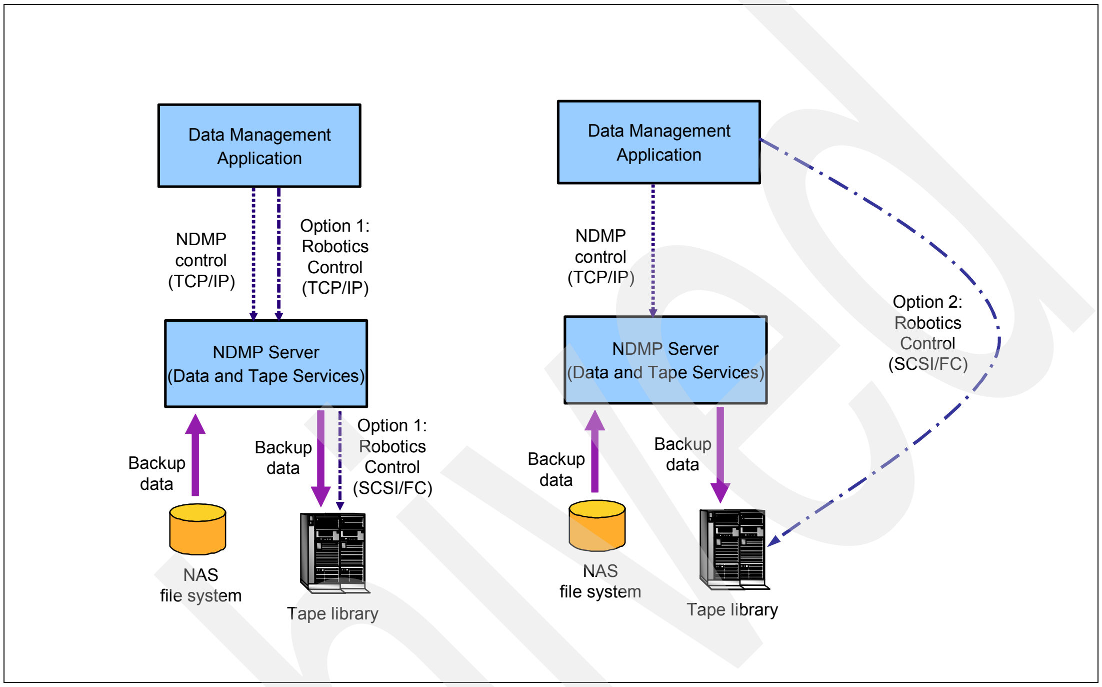

Data Management Application
NDMP control (TCP/IP)
Option 1: Robotics Control (TCP/IP)
NDMP Server (Data and Tape Services)
Backup data
Backup data
Option 1: Robotics Control (SCSI/FC)
NAS file system
Tape library
Data Management Application
NDMP control (TCP/IP)
Option 2: Robotics Control (SCSI/FC)
NDMP Server (Data and Tape Services)
Backup data
Backup data
NAS file system
Tape library

Figure 10-1 Filer-to-attached-library configuration options for library robotics control

The filer-to-attached-library configuration is the configuration that is used for the back-end data movement support described in 10.2, "Back-end data movement for NDMP backup images" on page 136.

For more details about the implementation of backing up a NAS file server by using a filer-to-attached-library configuration refer to the *Tivoli Storage Manager Administrator's Guide* and *Using the IBM System Storage N Series with IBM Tivoli Storage Manager*, SG24-7243.

10.1.2 Filer-to-server

With the filer-to-server configuration, the library is attached to the DMA (Tivoli Storage Manager Server). The NAS device does not have access to the library, as shown in Figure 10-2 on page 136. This configuration is also known as *3-way NDMP backup*. The backup data from the NAS device is transferred over the network (TCP/IP) to the Tivoli Storage Manager server.

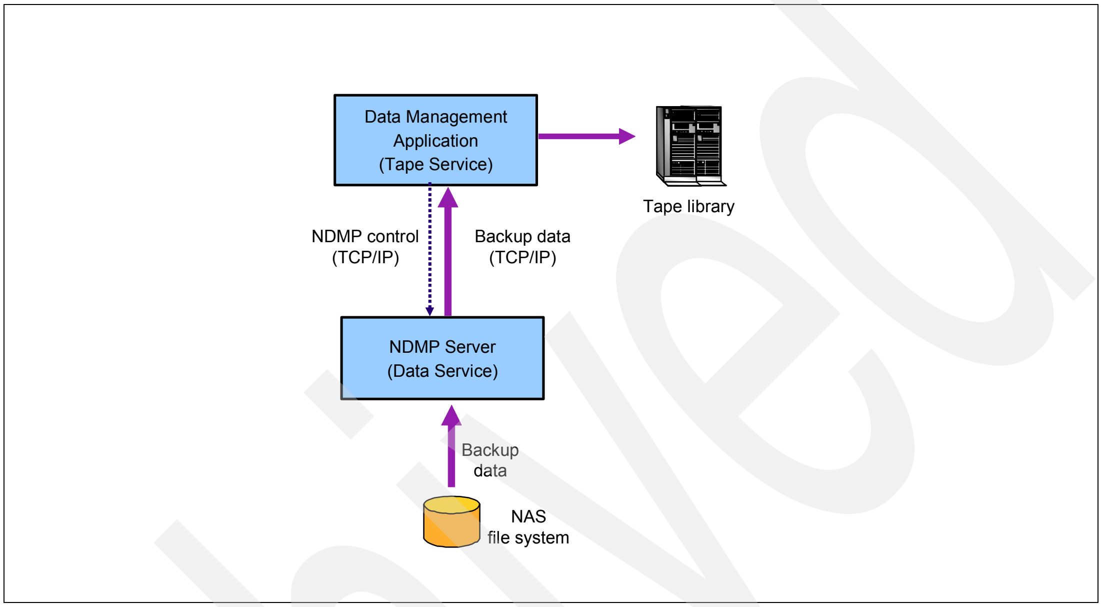


Figure 10-2 Filer-to-server configuration

Further information and implementation details about the filer-to-server configuration are described in 10.3, “Filer-to-server backup” on page 149.

10.2 Back-end data movement for NDMP backup images

Tivoli Storage Manager V5.4 supports back-end data movement of tape volumes containing NDMP-generated backup images using the NDMP tape-to-tape copy function.

The Tivoli Storage Manager Server asks the NDMP tape-to-tape copy function to copy either the entire tape to another tape, or to copy only one or a few backup images from one tape to another tape within a single NAS device.

In Figure 10-3 you can see how the Tivoli Storage Manager server directs the NAS device to perform the tape-to-tape copy operation.

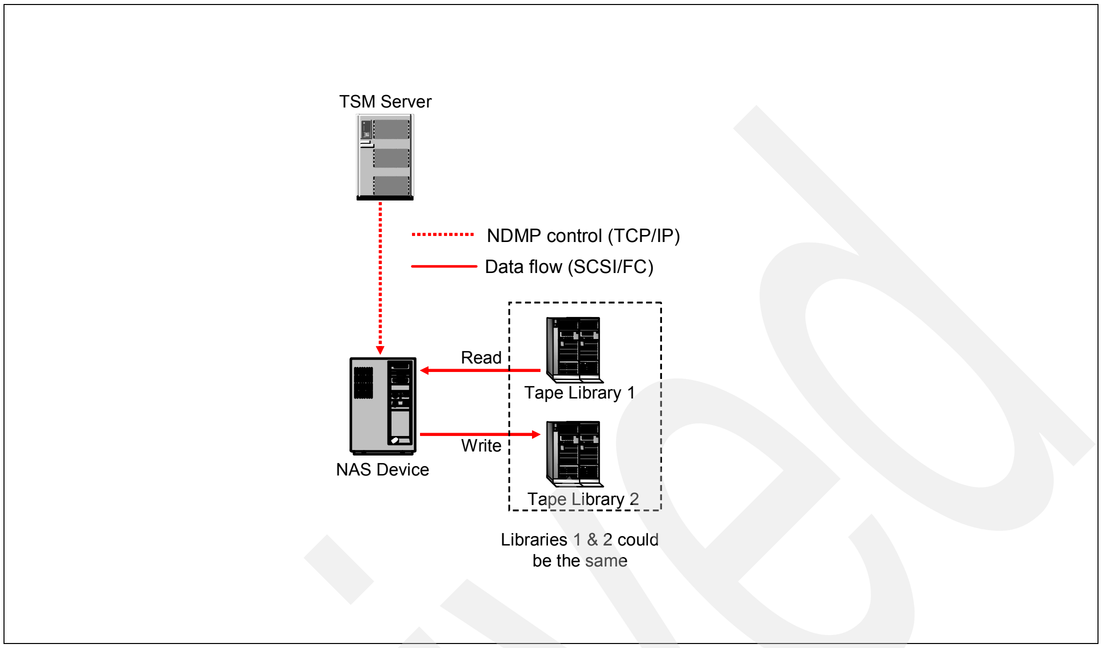


Figure 10-3 Back-end data movements by the NDMP tape-to-tape copy function

The NAS device itself copies the data from the input tape to the output tape, not the Tivoli Storage Manager server. Therefore, the NAS device requires access to the tape library, whereas the Tivoli Storage Manager server does not need to have drive access. It is only required to have two available drive paths from a single NAS data mover defined on the Tivoli Storage Manager server. The source and destination drives can be in the same or different libraries. If two libraries are used, they can be of different device types that are supported by NDMP.

During Tivoli Storage Manager back-end data movements, the Tivoli Storage Manager server uses a NAS data mover that supports the same data format as the source data to be copied, and that has two available mount points and paths to the drives. The data mover that performs the Tivoli Storage Manager back-end data movements can transfer data for any node, not just the specific node corresponding to the data mover.

The NDMP tape-to-tape copy function can be used to create copy storage pools from primary storage pools that contain NDMP-generated backup images. This improves the data availability of the NAS file system and allows you to create volumes for off-site vaulting, which could be managed by the Disaster Recovery Manager (DRM). The BACKUP STGPOOL command is used for this.

Additionally, it is possible to use the MOVE DATA command to move the NDMP-generated backup images from one storage pool volume to another. The target storage pool must have the same NDMP data format as the source storage pool.

Data migration and space reclamation are not supported for storage pools using NDMP data format. However, you can use intra-pool data movement (within the same storage pool) for space recovery. Intra-pool data movements can be performed with primary storage pools and copy storage pools. If the copy storage pool volumes are off site, the Tivoli Storage Manager Server obtains the images that are on the off-site volume from either a primary storage pool or another on-site copy storage pool volume. These images are then written to the destination volumes in the original copy storage pool.

Inter-pool data movement (to another storage pool) can be used for migration to a new device type. For example, the source primary storage pool may be in a library with DLT tape drives and the target primary storage pool may be in a library with LTO drives. Inter-pool data movements can only be performed with primary storage pools.

10.2.1 Configuration of our environment

The setup of our environment is shown in Figure 10-4.

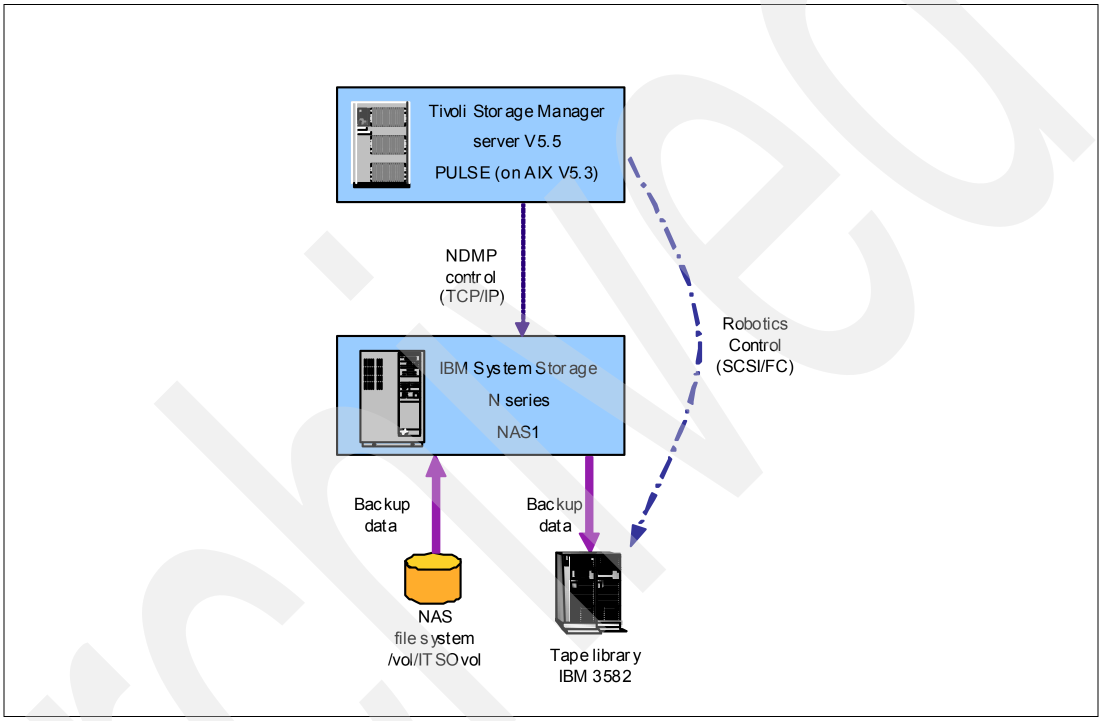


Figure 10-4 Filer-to-attached-library configuration

We identified the device names for the tape drives on the NAS device using the **sysconfig -t** command. This command lists all tape devices, as shown in Example 10-1.

Example 10-1 Display tape device names

```
Nas1> sysconfig -t

    Tape drive (JDSWITCH5:8.17)  IBM     ULT3580-TD2
    rst0l  -  rewind device,        format is: LTO-I tape only 100GB
    nrst0l -  no rewind device,     format is: LTO-I tape only 100GB
    urst0l -  unload/reload device, format is: LTO-I tape only 100GB
    rst0m  -  rewind device,        format is: LTO-I tape 200GB cmp
    nrst0m -  no rewind device,     format is: LTO-I tape 200GB cmp
    urst0m -  unload/reload device, format is: LTO-I tape 200GB cmp
    rst0h  -  rewind device,        format is: LTO-II tape only 200GB
    nrst0h -  no rewind device,     format is: LTO-II tape only 200GB
    urst0h -  unload/reload device, format is: LTO-II tape only 200GB
    rst0a  -  rewind device,        format is: LTO-II tape 400GB cmp
    nrst0a -  no rewind device,     format is: LTO-II tape 400GB cmp
    urst0a -  unload/reload device, format is: LTO-II tape 400GB cmp

    Tape drive (JDSWITCH5:9.18)  IBM     ULT3580-TD2
    rst1l  -  rewind device,        format is: LTO-I tape only 100GB
    nrst1l -  no rewind device,     format is: LTO-I tape only 100GB
    urst1l -  unload/reload device, format is: LTO-I tape only 100GB
    rst1m  -  rewind device,        format is: LTO-I tape 200GB cmp
    nrst1m -  no rewind device,     format is: LTO-I tape 200GB cmp
    urst1m -  unload/reload device, format is: LTO-I tape 200GB cmp
    rst1h  -  rewind device,        format is: LTO-II tape only 200GB
    nrst1h -  no rewind device,     format is: LTO-II tape only 200GB
    urst1h -  unload/reload device, format is: LTO-II tape only 200GB
    rst1a  -  rewind device,        format is: LTO-II tape 400GB cmp
    nrst1a -  no rewind device,     format is: LTO-II tape 400GB cmp
    urst1a -  unload/reload device, format is: LTO-II tape 400GB cmp
Nas1>
```

Example 10-2 shows the commands used to set up the Tivoli Storage Manager server.

Example 10-2   Configuration of environment for back-end data movement

```
DEFINE LIBRARY LIB3582 LIBTYPE=SCSI AUTOLABEL=YES

DEFINE PATH PULSE LIB3582 SRCT=SERVER DESTT=LIBRARY DEVICE=/DEV/SMC5 ONLINE=YES
AUTODETECT=YES

DEFINE DRIVE LIB3582 DRIVE01

DEFINE DRIVE LIB3582 DRIVE02

DEFINE PATH PULSE DRIVE01 SRCT=SERVER DESTT=DRIVE LIBRARY=LIB3582
DEVICE=/DEV/RMT29 ONLINE=YES AUTODETECT=YES

DEFINE PATH PULSE DRIVE02 SRCT=SERVER DESTT=DRIVE LIBRARY=LIB3582
DEVICE=/DEV/RMT30 ONLINE=YES AUTODETECT=YES

DEFINE DEVCLASS LTO LIBRARY=LIB3582 DEVT=LTO

DEFINE DEVCLASS NASCLASS LIBR=LIB3582 DEVTYPE=NAS MOUNTRETENTION=0
ESTCAPACITY=200G

DEFINE STGP NASTAPE NASCLASS POOLTYPE=PRIMARY DATAFORMAT=NETAPPDUMP MAXSCRATCH=20

DEFINE STGP NASTAPE2 NASCLASS POOLTYPE=PRIMARY DATAFORMAT=NETAPPDUMP MAXSCRATCH=20

DEFINE STGP NASTOCPOOL DISK POOLTYPE=PRIMARY

DEFINE VOLUME NASTOCPOOL /TSMSTG/TOC01.DSM FORMAT=1024

DEFINE STGP NASTAPECOPY NASCLASS POOLTYPE=COPY DATAFORMAT=NETAPPDUMP MAXSCRATCH=20

DEFINE DOMAIN FILER-TO-LIBRARY

DEFINE POLICYSET FILER-TO-LIBRARY STANDARD

DEFINE MGMT FILER-TO-LIBRARY STANDARD STANDARD
```

```
ASSIGN DEFMGMTCLASS FILER-TO-LIBRARY STANDARD STANDARD

DEFINE COPYGROUP FILER-TO-LIBRARY STANDARD STANDARD DESTINATION=NASTAPE
TOCDESTINATION=NASTOCPOOL

DEFINE COPYGROUP FILER-TO-LIBRARY STANDARD STANDARD TYPE=ARCHIVE
DESTINATION=NASTAPE

ACTIVATE POLICYSET FILER-TO-LIBRARY STANDARD

REGISTER NODE NASTOLIB ?*****? DOMAIN=FILER-TO-LIBRARY TYPE=NAS

DEFINE DATAMOVER NASTOLIB TYPE=NAS HLADDRESS=NAS1.STORAGE.TUCSON.IBM.COM
LLADDRESS=10000 USERID=ROOT PASSWORD=?*****? DATAFORMAT=NETAPPDUMP

DEFINE PATH NASTOLIB DRIVE01 SRCTYPE=DATAMOVER DESTTYPE=DRIVE LIBRARY=LIB3582
DEVICE=RST0H

DEFINE PATH NASTOLIB DRIVE02 SRCTYPE=DATAMOVER DESTTYPE=DRIVE LIBRARY=LIB3582
DEVICE=RST1H
```

In order to use all the back-end movement commands that we show in the following sections, you need at least two available drive paths from a single NAS data mover defined as shown in Example 10-3. These were defined in the DEFINE PATH commands at the end of Example 10-2 on page 139.

Example 10-3 Drive path definition for a single data mover

```
tsm: PULSE>query path nastolib

Source Name     Source Type     Destination     Destination     On-Line
                                Name            Type
-----------     -----------     -----------     -----------     -------
NASTOLIB        DATAMOVER       DRIVE01         DRIVE           Yes
NASTOLIB        DATAMOVER       DRIVE02         DRIVE           Yes


tsm: PULSE>
```

10.2.2 Useful commands on the NAS device

With the command **mt -t *<tapedrive>* status**, you can check on the NAS device if a tape is currently mounted in the drive, as shown in Example 10-4.

Example 10-4 Check the drive status on the NAS device

```
Nas1> mt -t rst0h status
Tape drive: IBM     ULT3580-TD2
    Status: offline
    Format: LTO-II tape only 200GB
    fileno = -1  blockno = -1  resid = 0
Nas1> mt -t rst0h status
Tape drive: IBM     ULT3580-TD2
    Status: in use
    Format: LTO-II tape only 200GB
    fileno = 1  blockno = 0  resid = 0
Nas1>
```

In Example 10-5 you could see how to use the **sysstat** command to monitor the drive usage. Whenever tape I/O is performed you can see this in the Tape kB/s column.

Example 10-5 Display the system status for a NAS filer with sysstat

```
Nas1> sysstat
 CPU    NFS   CIFS   HTTP      Net kB/s     Disk kB/s      Tape kB/s    Cache
                               in   out     read  write    read write     age
  0%      0      0      0       0     0        3     32       0     0     >60
  7%      0      0      0       0     0       17     69    8054  8045     >60
 18%      0      0      0       1     0        3     34   24309 24309     >60
 19%      0      0      0       0     0        4     61   25794 25794     >60
 12%      0      0      0       1     0        3     32   16510 16518     >60
  0%      0      0      0       0     0       15     61       0     0     >60
  0%      0      0      0       0     0        3     32       0     0     >60
  0%      0      0      0       0     0       20     68       0     0     >60
  0%      0      0      0       0     0        3     34       0     0     >60
  0%      0      0      0       0     0       14     32       0     0     >60
  0%      0      0      0       0     0        4     67       0     0     >60
  0%      0      0      0       0     0        3     32       0     0     >60
Nas1>
```

The command **ndmpd version** helps you to identify the NDMP version that your NAS device supports, as shown in Example 10-6.

Example 10-6 Display NDMP version

```
Nas1> ndmpd version
ndmpd highest version set to: 4
Nas1>
```

10.2.3 Backup storage pool

To back up a primary storage pool that contains NDMP-generated backup images you need a copy storage pool that has the same data format as the primary storage pool on the Tivoli Storage Manager server. Our primary storage pool is called NASTAPE, and our copy storage pool is called NASTAPECOPY, as shown in Example 10-7. Note the data format, NetApp Dump.

Example 10-7 Primary and copy storage pool with the same data format

```
tsm: PULSE>query stg nastape format=detail

               Storage Pool Name: NASTAPE
               Storage Pool Type: Primary
               Device Class Name: NASCLASS
              Estimated Capacity: 4,096 G
              Space Trigger Util:
                        Pct Util: 0.8
                        Pct Migr:
                     Pct Logical: 100.0
                    High Mig Pct:
                     Low Mig Pct:
                 Migration Delay:
              Migration Continue: Yes
             Migration Processes:
           Reclamation Processes:
               Next Storage Pool:
            Reclaim Storage Pool:
          Maximum Size Threshold:
                          Access: Read/Write
                     Description:
               Overflow Location:
           Cache Migrated Files?:
                      Collocate?: Group
           Reclamation Threshold:
       Offsite Reclamation Limit:
 Maximum Scratch Volumes Allowed: 20
  Number of Scratch Volumes Used: 1
   Delay Period for Volume Reuse: 0 Day(s)
          Migration in Progress?:
            Amount Migrated (MB):
Elapsed Migration Time (seconds):
        Reclamation in Progress?:
  Last Update by (administrator): ADMIN
           Last Update Date/Time: 16.11.2007 11:47:43
        Storage Pool Data Format: NetApp Dump
            Copy Storage Pool(s):
             Active Data Pool(s):
         Continue Copy on Error?: Yes
                        CRC Data: No
                Reclamation Type: Threshold
     Overwrite Data when Deleted:

tsm: PULSE>query stg nastapecopy format=detail

               Storage Pool Name: NASTAPECOPY
               Storage Pool Type: Copy
               Device Class Name: NASCLASS
              Estimated Capacity: 4,096 G
              Space Trigger Util:
                        Pct Util: 0.0
                        Pct Migr:
                     Pct Logical: 100.0
                    High Mig Pct:
                     Low Mig Pct:
                 Migration Delay:
              Migration Continue: Yes
             Migration Processes:
           Reclamation Processes:
               Next Storage Pool:
            Reclaim Storage Pool:
          Maximum Size Threshold:
                          Access: Read/Write
                     Description:
               Overflow Location:
           Cache Migrated Files?:
```

```
                      Collocate?: No
           Reclamation Threshold:
       Offsite Reclamation Limit:
 Maximum Scratch Volumes Allowed: 20
  Number of Scratch Volumes Used: 1
   Delay Period for Volume Reuse: 0 Day(s)
          Migration in Progress?:
            Amount Migrated (MB):
Elapsed Migration Time (seconds):
        Reclamation in Progress?:
  Last Update by (administrator): ADMIN
           Last Update Date/Time: 16.11.2007 12:58:19
        Storage Pool Data Format: NetApp Dump
            Copy Storage Pool(s):
             Active Data Pool(s):
         Continue Copy on Error?:
                        CRC Data: No
                Reclamation Type: Threshold
     Overwrite Data when Deleted:

tsm: PULSE>
```

To back up the primary storage pool, using the back-end data movement, use the command BACKUP STGPOOL, as shown in the Example 10-8. Note the ANR2768I message, which shows that the NDMP data move is performing the operation. We now have a copy storage pool backup of our primary storage pool with NDMP-generated backup images.

Example 10-8 Backup storage pool output running in the foreground

```
tsm: PULSE>backup stgp nastape nastapecopy wait=yes
ANR0984I Process 18 for BACKUP STORAGE POOL started in the FOREGROUND at
15:24:51.
ANR2110I BACKUP STGPOOL started as process 18.
ANR1210I Backup of primary storage pool NASTAPE to copy storage pool
NASTAPECOPY started as process 18.
ANR2768I Process 18 will use data mover NASTOLIB for the operation.
ANR1212I Backup process 18 ended for storage pool NASTAPE.
ANR0986I Process 18 for BACKUP STORAGE POOL running in the FOREGROUND processed
1 items for a total of 31,534,245,888 bytes with a completion state of SUCCESS
at 15:44:42.
ANR1214I Backup of primary storage pool NASTAPE to copy storage pool
NASTAPECOPY has ended.  Files Backed Up: 1, Bytes Backed Up: 31534245888,
Unreadable Files: 0, Unreadable Bytes: 0.

tsm: PULSE>
```

10.2.4 Restore volume and restore storage pool

In case one of your primary storage pool volumes containing NDMP-generated backup images becomes unreadable or damaged, you can use the RESTORE VOLUME command to recreate the volume from a copy storage pool volume, as shown in Example 10-9. Again, note the message ANR2768I.

Example 10-9 Restore volume output running in the foreground

```
tsm: PULSE>restore volume 471AGQ wait=yes
ANR2041W This command attempts to restore all files in storage pool NASTAPE
which reside on one of the volumes specified in the command; existing
references to files on these volumes will be deleted from the database after
the files have been restored.

Do you wish to proceed? (Yes (Y)/No (N)) yes
ANR2114I RESTORE VOLUME: Access mode for volume 471AGQ updated to "destroyed".
ANR0984I Process 7 for RESTORE VOLUME started in the FOREGROUND at 17:41:45.
ANR1232I Restore of volumes in primary storage pool NASTAPE started as process
7.
ANR2768I Process 7 will use data mover NASTOLIB for the operation.
ANR1235I Restore process 7 ended for volumes in storage pool NASTAPE.
ANR0986I Process 7 for RESTORE VOLUME running in the FOREGROUND processed 3
items for a total of 1,228,454,912 bytes with a completion state of SUCCESS at
17:47:21.
ANR1240I Restore of volumes in primary storage pool NASTAPE has ended.  Files
Restored: 3, Bytes Restored: 1228454912, Unreadable Files: 0, Unreadable Bytes:
0.

tsm: PULSE>
```

In Example 10-10 we restore the complete storage pool NASTAPE with the RESTORE STGPOOL command.

Example 10-10 Restore storage pool output running in the foreground

```
tsm: PULSE>restore stg nastape wait=yes
ANR2040W This command attempts to restore all files in storage pool NASTAPE
which have previously been found to be damaged or which reside on a volume with
access mode "destroyed"; existing references to files in storage pool NASTAPE
will be deleted from the database after the files have been restored.

Do you wish to proceed? (Yes (Y)/No (N)) yes
ANR0984I Process 9 for RESTORE STORAGE POOL started in the FOREGROUND at
17:55:15.
ANR1230I Restore of primary storage pool NASTAPE started as process 9.
ANR2768I Process 9 will use data mover NASTOLIB for the operation.
ANR1234I Restore process 9 ended for storage pool NASTAPE.
ANR0986I Process 9 for RESTORE STORAGE POOL running in the FOREGROUND processed
3 items for a total of 1,228,454,912 bytes with a completion state of SUCCESS
at 18:00:47.
ANR1238I Restore of primary storage pool NASTAPE has ended.  Files Restored: 3,
Bytes Restored: 1228454912, Unreadable Files: 0, Unreadable Bytes: 0.

tsm: PULSE>
```

10.2.5 Using Disaster Recovery Manager (DRM)

The copy storage pool that you have created for your NDMP-generated backup images could be managed with the Tivoli Storage Manager server's Disaster Recovery Manager.

Make sure that you have included the primary storage and copy storage pools that contain the NAS data in your DRM setup. Use the QUERY DRMSTATUS command, as in Example 10-11.

Example 10-11 Query DRM status

```
tsm: PULSE>query drmstatus

              Recovery Plan Prefix:
          Plan Instructions Prefix:
        Replacement Volume Postfix: @
             Primary Storage Pools:
                Copy Storage Pools:
       Not Mountable Location Name: NOTMOUNTABLE
                      Courier Name: COURIER
                   Vault Site Name: VAULT
  DB Backup Series Expiration Days: 60 Day(s)
Recovery Plan File Expiration Days: 60 Day(s)
                      Check Label?: Yes
         Process FILE Device Type?: No
                 Command File Name:

tsm: PULSE>
```

If the fields are empty, as in the example, then all primary and copy storage pools are managed with DRM. If you need to change the fields, use the commands SET DRMPRIMSTGPOOL and SET DRMCOPYSTGPOOL. For more information about the usage and setup of DRM refer to the *Tivoli Storage Manager Administrator's Guide*.

In Example 10-12 we move the mountable volume 470AGQ from the copy storage pool NASTAPECOPY to the off-site state VAULT.

Example 10-12 Process volume with DRM to state VAULT

```
tsm: PULSE>query drm 470AGQ format=detail

           Volume Name: 470AGQ
                 State: Mountable
 Last Update Date/Time: 16.11.2007 17:19:48
              Location:
           Volume Type: CopyStgPool
Copy Storage Pool Name: NASTAPECOPY
     Automated LibName: LIB3582


tsm: PULSE>move drm 470AGQ wherestate=mountable wait=yes
ANR0984I Process 3 for MOVE DRMEDIA started in the FOREGROUND at 17:25:47.
ANR0609I MOVE DRMEDIA started as process 3.
ANR0610I MOVE DRMEDIA started by ADMIN as process 3.
ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME for volume 470AGQ in library LIB3582
starting.
```

```
ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME for volume 470AGQ in library LIB3582
completed successfully.
ANR6683I MOVE DRMEDIA: Volume 470AGQ was moved from MOUNTABLE state to
NOTMOUNTABLE.
ANR6682I MOVE DRMEDIA command ended: 1 volumes processed.
ANR0611I MOVE DRMEDIA started by ADMIN as process 3 has ended.
ANR0987I Process 3 for MOVE DRMEDIA running in the FOREGROUND processed 1 items
with a completion state of SUCCESS at 17:26:53.

tsm: PULSE>move drm 470AGQ wherestate=notmountable tostate=vault wait=yes
ANR0984I Process 4 for MOVE DRMEDIA started in the FOREGROUND at 17:27:32.
ANR0609I MOVE DRMEDIA started as process 4.
ANR0610I MOVE DRMEDIA started by ADMIN as process 4.
ANR6683I MOVE DRMEDIA: Volume 470AGQ was moved from NOTMOUNTABLE state to
VAULT.
ANR6682I MOVE DRMEDIA command ended: 1 volumes processed.
ANR0611I MOVE DRMEDIA started by ADMIN as process 4 has ended.
ANR0987I Process 4 for MOVE DRMEDIA running in the FOREGROUND processed 1 items
with a completion state of SUCCESS at 17:27:32.

tsm: PULSE>query drm 470AGQ format=detail

           Volume Name: 470AGQ
                 State: Vault
 Last Update Date/Time: 16.11.2007 17:27:32
              Location: VAULT
           Volume Type: CopyStgPool
Copy Storage Pool Name: NASTAPECOPY
     Automated LibName:

tsm: PULSE>
```

10.2.6 Move data

The MOVE DATA command is very useful to manage your NAS data, because you cannot use migration or reclamation processes to reorganize and optimize the volume usage for storage pools that contain NDMP-generated backup images.

The command can be used *intra-pool* using the format MOVE DATA <VOLUMENAME> to move the data within the same storage pool. Or it can be used for inter-pool data movement with the command MOVE DATA <VOLUMENAME> STG=<TARGET STORAGE POOL> to move the data to another storage pool with the same data format as the source storage pool.

Intra-pool data movement

Intra-pool movement is allowed for primary storage pool and copy storage pool volumes, whereas inter-pool movement is only allowed for primary storage pool volumes.

If a MOVE DATA command is used against an off-site copy storage pool volume, the Tivoli Storage Manager server obtains the images that are on the off-site volume from either a primary storage pool or another on-site copy storage pool volume. These images are then written to the destination volumes in the original copy storage pool.

Example 10-13 shows intra-pool movement for a copy storage pool volume that is off site. The data is copied from the off-site volume 475AGQ, since the source volume is off site.

Example 10-13 MOVE DATA output from an off-site tape

```
tsm: PULSE>query drm 470AGQ format=detail

           Volume Name: 470AGQ
                 State: Vault
 Last Update Date/Time: 16.11.2007 17:27:32
              Location: VAULT
           Volume Type: CopyStgPool
Copy Storage Pool Name: NASTAPECOPY
     Automated LibName:


tsm: PULSE>query volume 470AGQ format=detail

                   Volume Name: 470AGQ
             Storage Pool Name: NASTAPECOPY
             Device Class Name: NASCLASS
            Estimated Capacity: 204,800.0
       Scaled Capacity Applied:
                      Pct Util: 0.6
                 Volume Status: Filling
                        Access: Offsite
        Pct. Reclaimable Space: 99.4
               Scratch Volume?: Yes
               In Error State?: No
      Number of Writable Sides: 1
       Number of Times Mounted: 6
             Write Pass Number: 1
     Approx. Date Last Written: 16.11.2007 17:19:48
        Approx. Date Last Read: 16.11.2007 17:55:49
           Date Became Pending:
        Number of Write Errors: 0
         Number of Read Errors: 0
               Volume Location: VAULT
Volume is MVS Lanfree Capable : No
Last Update by (administrator): ADMIN
         Last Update Date/Time: 16.11.2007 18:16:35
          Begin Reclaim Period:
            End Reclaim Period:
  Drive Encryption Key Manager:

tsm: PULSE>move data 470AGQ wait=yes
ANR2232W This command will move all of the data stored on volume 470AGQ to
other volumes within the same storage pool; the data will be inaccessible to
users until the operation completes.

Do you wish to proceed? (Yes (Y)/No (N)) yes
ANR0984I Process 10 for MOVE DATA started in the FOREGROUND at 18:18:03.
ANR1140I Move data process started for volume 470AGQ (process ID 10).
ANR1157I Removable volume 475AGQ is required for move process.
ANR2768I Process 10 will use data mover NASTOLIB for the operation.
ANR1141I Move data process ended for volume 470AGQ.
```

```
ANR0986I Process 10 for MOVE DATA running in the FOREGROUND processed 3 items
for a total of 1,228,454,912 bytes with a completion state of SUCCESS at
18:22:39.
ANS8003I Process number 10 started.

tsm: PULSE>
```

Example 10-14 shows that after the move of data, the copy storage pool volume is now empty and has changed to status *Vault retrieve*.

Example 10-14 Volume status after MOVE DATA

```
tsm: PULSE>q drm 470AGQ f=d

           Volume Name: 470AGQ
                 State: Vault retrieve
 Last Update Date/Time: 16.11.2007 18:24:32
              Location: VAULT
           Volume Type: CopyStgPool
Copy Storage Pool Name: NASTAPECOPY
     Automated LibName:


tsm: PULSE>q vol 470AGQ

Volume Name               Storage      Device       Estimated    Pct   Volume
                          Pool Name    Class Name    Capacity   Util   Status
------------------------  -----------  ----------  ---------  -----  --------
470AGQ                    NASTAPECOPY  NASCLASS          0.0    0.0  Empty
```

Inter-pool data movement

Example 10-15 shows inter-pool data movement from a volume in storage pool NASTAPE to the storage pool NASTAPE2.

Example 10-15 MOVE DATA from one storage pool to another

```
tsm: PULSE>move data 475AGQ stg=nastape2 wait=yes
ANR2233W This command will move all of the data stored on volume 475AGQ to
other volumes in storage pool NASTAPE2; the data will be inaccessible to users
until the operation completes.

Do you wish to proceed? (Yes (Y)/No (N)) yes
ANR0984I Process 11 for MOVE DATA started in the FOREGROUND at 18:33:57.
ANR1140I Move data process started for volume 475AGQ (process ID 11).
ANR2768I Process 11 will use data mover NASTOLIB for the operation.
ANR1141I Move data process ended for volume 475AGQ.
ANR0986I Process 11 for MOVE DATA running in the FOREGROUND processed 3 items
for a total of 1,228,454,912 bytes with a completion state of SUCCESS at
18:39:41.

tsm: PULSE>
```

10.3 Filer-to-server backup

Tivoli Storage Manager Server V5.4 supports an additional NAS backup configuration option in which there is no need for a tape library to be attached to any NAS device. If you have several NAS file servers located in different locations, you might prefer to send the backup data to a single Tivoli Storage Manager server rather than attaching a tape library to each NAS device.

This configuration is called *filer-to-server configuration* or *3-way NDMP Backup* and requires NDMP V4 support of the NAS device. The Tivoli Storage Manager server functions as the NDMP tape server in this configuration. The implemented NDMP tape server is based on NDMP V4 and has the following functions only:

- Only the mover interface is implemented and has no direct access to tape devices.
- NAS backup images are stored in Tivoli Storage Manager server's storage hierarchy.
- The Tivoli Storage Manager Tape server can only be accessed from within Tivoli Storage Manager server. No other DMA may communicate with it, including DMAs of other Tivoli Storage Manager servers.
- No user configuration is needed unless the default NDMP tape server port is unavailable (for example, firewall restrictions).
- Supports multiple concurrent NDMP operations.

Figure 10-5 on page 149 shows the filer-to-server configuration, where the Data Management Application (DMA) is the Tivoli Storage Manager server. Note that there is no tape device attached to the NAS device.

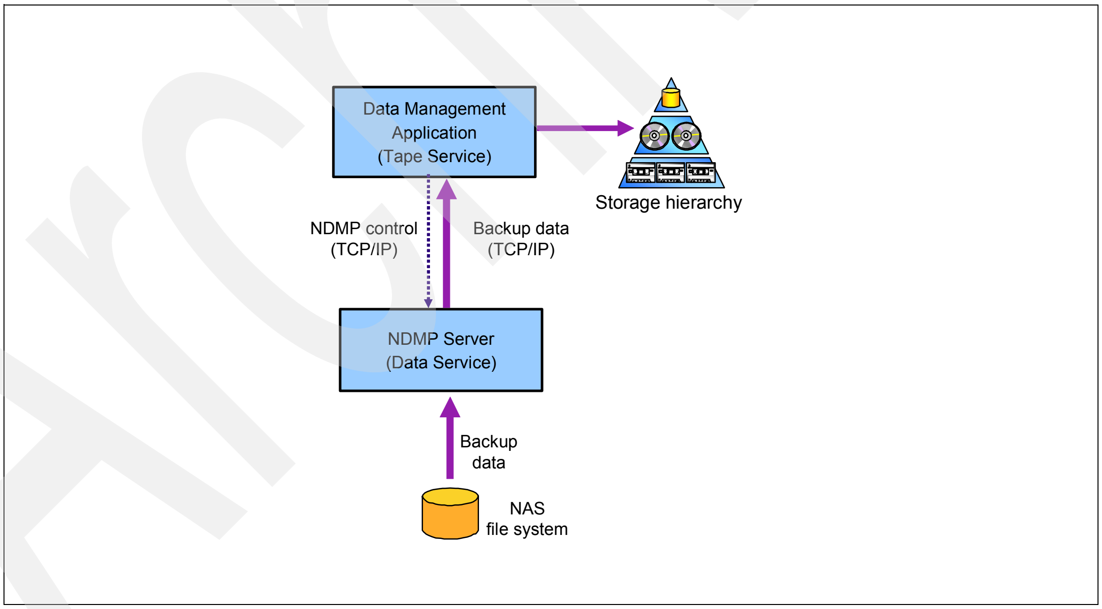


Figure 10-5 Filer-to-server configuration with Tivoli Storage Manager server storage

Note: In a filer-to-server configuration all backup data is sent over the network (TCP/IP) from the NAS device to the Tivoli Storage Manager server.

All existing NAS backup functions are supported for the filer-to-server configuration:

- TOC creation
- File-level restore (FLR)
- Direct Access Recovery (DAR)

For more details about these functions refer to the *Tivoli Storage Manager Administrator's Guide* and *Using the IBM System Storage N Series with IBM Tivoli Storage Manager*, SG24-7243.

10.3.1 How backup images are managed

The NDMP-generated backup images of the NAS file systems are stored in Tivoli Storage Manager native storage pools that use block headers (the default). Because the NAS backup data is then in the Tivoli Storage Manager server's storage hierarchy, you have the following benefits:

- Management classes for NDMP data do not have to be associated with a storage pool whose device class is of device type NAS. This allows for storage to disk volumes, as well as tape.
- Tivoli Storage Manager back-end data management is now possible, via move data, migration, backup of storage pools, and reclamation processes in the same storage pools as other Tivoli Storage Manager data.
- CRC checking is available when data is moved via Tivoli Storage Manager processes.
- NAS data can be protect via DRM, along with other Tivoli Storage Manager data.
- NAS backups can be validated via Tivoli Storage Manager AUDIT commands.

In order to back up a NAS device to a Tivoli Storage Manager native storage pool, configure the copy group to point to the desired native storage pool. The destination storage pool provides the information about the library and drives used for backup and restore. Ensure that there is sufficient space in your target storage pool to contain the NDMP-generated backup images of the NAS device.

NDMP-generated backup images can be backed up to sequential, disk, or file type devices. Defining a separate device class is not necessary.

10.3.2 How restore of NDMP backup images are managed

Now that filer-to-server configurations are available, depending on your Tivoli Storage Manager server setup, it is possible that a restore operation will require you to access some data in storage pools with device type NAS (for example, NETAPPDUMP) and some data in storage pools with native Tivoli Storage Manager device classes (for example, file type).

Data stored in traditional Tivoli Storage Manager storage pools with native device classes will be restored using the filer-to-server function. Data from storage pools whose device class has device type NAS will be restored using the same NDMP protocols that Tivoli Storage Manager has supported already in previous releases (also known as filer-to-attached-library configuration).

Tivoli Storage Manager always uses the appropriate protocol during restore operations, when data from both NAS device classes and traditional Tivoli Storage Manager device classes are required in the same set of operations. This is transparent. No interface changes are required to handle restore operations, regardless of the backup mechanisms.

This allows you a lot of flexibility in how you store NDMP-generated backup images. For example, you could choose to direct full backup images to a NAS device class with the filer-to-attached-library configuration, while sending differential backup images to a native device class with the filer-to-server configuration.

10.3.3 Set up a filer-to-server configuration

To back up a NAS device via the filer-to-server configuration perform the following steps:

1. Register a domain or use an existing domain that has a management class pointing to a storage pool with a native device class.
2. Update the copy group in this domain with the destination of the TOC storage pool.
3. Register a node of type NAS in the domain.
4. Define a datamover from type NAS for this node.

1. The environment that we used for the filer-to-server backup is shown in Figure 10-6 on page 151 and the commands for the configuration are shown in Example 10-16.

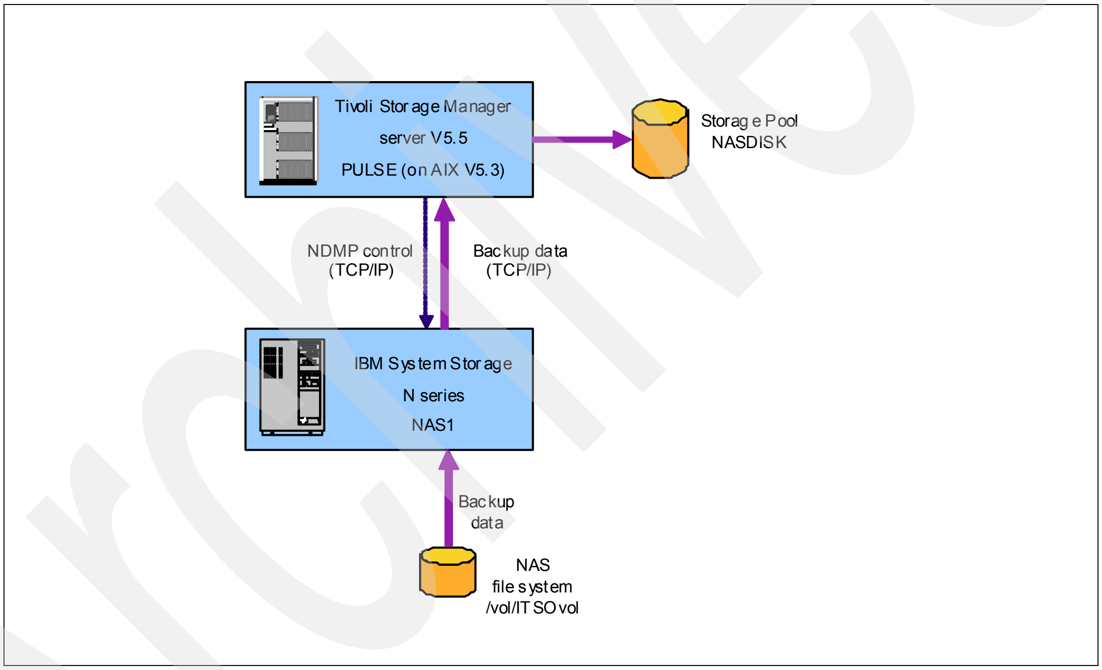


Figure 10-6 Filer-to-server configuration

Example 10-16 Filer-to-server configuration

```
DEFINE STGP NASDISK DISK POOLTYPE=PRIMARY DATAFORMAT=NATIVE
DEFINE VOLUME NASDISK /TSMSTG/DISK01.DSM FORMAT=1024
DEFINE STGP NASTOCPOOL DISK POOLTYPE=PRIMARY
DEFINE VOLUME NASTOCPOOL /TSMSTG/TOC01.DSM FORMAT=1024
DEFINE DOMAIN FILER-TO-SERVER
DEFINE POLICYSET FILER-TO-SERVER STANDARD
DEFINE MGMT FILER-TO-SERVER STANDARD STANDARD
ASSIGN DEFMGMTCLASS FILER-TO-SERVER STANDARD STANDARD
DEFINE COPYGROUP FILER-TO-SERVER STANDARD STANDARD DESTINATION=NASDISK
TOCDESTINATION=NASTOCPOOL
DEFINE COPYGROUP FILER-TO-SERVER STANDARD STANDARD TYPE=ARCHIVE
DESTINATION=NASDISK
```

```
ACTIVATE POLICYSET FILER-TO-SERVER STANDARD
REGISTER NODE NASTODISK ?*****? DOMAIN=FILER-TO-SERVER TYPE=NAS
DEFINE DATAMOVER NASTODISK TYPE=NAS HLADDRESS=NAS1.STORAGE.TUCSON.IBM.COM
LLADDRESS=10000 USERID=ROOT PASSWORD=?*****? DATAFORMAT=NETAPPDUMP
```

2. When you have finished your configuration you can back up the NAS device using the command BACKUP NODE, as shown in Example 10-17.

Example 10-17   Back up a NAS device with a filer-to-server configuration

```
tsm: PULSE>backup node nastodisk /vol/ITSOvol wait=yes
ANR0984I Process 13 for BACKUP NAS (FULL) started in the FOREGROUND at
19:12:29.
ANR1063I Full backup of NAS node NASTODISK, file system /vol/ITSOvol, started
as process 13 by administrator ADMIN.
ANR1067I NAS Backup to TSM Storage process 13 completed.
ANR0986I Process 13 for BACKUP NAS (FULL) running in the FOREGROUND processed 1
items for a total of 248,481,792 bytes with a completion state of SUCCESS at
19:13:00.
ANS8003I Process number 13 started.

tsm: PULSE>
```

3. Verify your backup and the location where the data is stored with the commands shown in Example 10-18.

Example 10-18   Verify the location of the backup

```
tsm: PULSE>query nasbackup nastodisk /vol/ITSOvol

Node Name    Filespace   Object Type    Object  Creation   Has Table Image
             Name                    Size (MB)    Date     of Conte- Storage
                                                           nts (TOC- Pool Name
                                                           )?
------------ ----------- ----------- --------- ---------- --------- ----------
NASTODISK    /vol/ITSOv- Full Image      237.0 16.11.2007 Yes       NASDISK
              ol                                19:12:24

tsm: PULSE>query volume stg=nasdisk

Volume Name               Storage      Device      Estimated    Pct   Volume
                          Pool Name    Class Name   Capacity   Util   Status
------------------------  -----------  ----------  ---------  -----  --------
/tsmstg/disk01.dsm        NASDISK      DISK          1,024.0   23.1  On-Line

tsm: PULSE>query content /tsmstg/disk01.dsm

Node Name        Type  Filespace   FSID  Client's Name for File
                       Name
---------------  ----  ----------  ----  --------------------------------------
NASTODISK        Bkup  /vol/ITSO-     1  /NAS/ IMAGE
                        vol

tsm: PULSE>
```

Filer-to-attached-library together with a filer-to-server configuration

The Tivoli Storage Manager server is able to use both configurations together to provide flexibility in how to organize the NDMP-generated backup images of the NAS file systems. To use our filer-to-attached-library configuration from 10.2, “Back-end data movement for NDMP backup images” on page 136, we need to add an additional management class that points to a storage pool with the native device class. The additional configuration steps are listed in Example 10-19.

Example 10-19 Enhance the filer-to-attached-library configuration to use filer-to-server as well

```
DEFINE MGMT FILER-TO-LIBRARY STANDARD MC_NASDISK
DEFINE COPYGROUP FILER-TO-LIBRARY STANDARD DISK DESTINATION=NASDISK
TOCDESTINATION=NASTOCPOOL
DEFINE COPYGROUP FILER-TO-LIBRARY STANDARD DISK TYPE=ARCHIVE DESTINATION=NASDISK
ACTIVATE POLICYSET FILER-TO-LIBRARY STANDARD
```

To keep the amount of backup data small in our test environment we create a virtual filespace mapping for the NAS device, as shown in Example 10-20.

Example 10-20 Virtual filespace mapping

```
DEFINE VIRTUALFSMAPPING NASTOLIB /ITSO /VOL/VOL0 /HOME/ITSO
```

Example 10-21 shows a full and differential backup of the /ITSO fileset.

Example 10-21 Backup node with full and differential mode

```
tsm: PULSE>backup node nastolib /ITSO mode=full wait=yes
ANR0984I Process 15 for BACKUP NAS (FULL) started in the FOREGROUND at
20:32:15.
ANR1063I Full backup of NAS node NASTOLIB, file system /ITSO, started as
process 15 by administrator ADMIN.
ANR1067I NAS Backup process 15 completed.
ANR0986I Process 15 for BACKUP NAS (FULL) running in the FOREGROUND processed 1
items for a total of 73,137,152 bytes with a completion state of SUCCESS at
20:35:07.
ANS8003I Process number 15 started.

tsm: PULSE>backup node nastolib /ITSO mode=differential mgmt=mc_nasdisk wait=yes
ANR0984I Process 19 for BACKUP NAS (DIFFERENTIAL) started in the FOREGROUND at
20:45:29.
ANR1064I Differential backup of NAS node NASTOLIB, file system /ITSO, started
as process 19 by administrator ADMIN.
ANR1067I NAS Backup to TSM Storage process 19 completed.
ANR0986I Process 19 for BACKUP NAS (DIFFERENTIAL) running in the FOREGROUND
processed 1 items for a total of 35,706,880 bytes with a completion state of
SUCCESS at 20:46:49.
ANS8003I Process number 19 started.

tsm: PULSE>
```

Verify the location of the NDMP images with the QUERY NASBACKUP command, as shown in Example 10-22. We can see that each backup has gone to a different storage pool, as requested.

Example 10-22 Query nasbackup output for full and differential backup

```
tsm: PULSE>query nasbackup nastolib /ITSO

Node Name    Filespace   Object Type    Object  Creation  Has Table Image
             Name                     Size (MB)    Date    of Conte- Storage
                                                          nts (TOC- Pool Name
                                                          )?
------------ ----------- ----------- --------- ---------- --------- ----------
NASTOLIB     /ITSO       Full Image       69.7 16.11.2007 Yes       NASTAPE
                                                20:32:13
NASTOLIB     /ITSO       Differenti-      34.1 16.11.2007 Yes       NASDISK
                          al Image              20:45:24

tsm: PULSE>
```

With the **sysstat** command on the NAS device in Example 10-23 we can monitor the full backup. The data is transferred directly to the tape drive from the NAS device. During the differential backup, the data is transferred via the network to the Tivoli Storage Manager server.

Example 10-23 Sysstat shows data flow during full and differential backup of the NAS device

```
Nas1> sysstat
 CPU    NFS   CIFS   HTTP      Net kB/s    Disk kB/s     Tape kB/s    Cache
                               in   out     read  write    read write     age
  0%      0      3      0       1     0        3     32       0     0     >60
  0%      0      2      0       1     0        4     61       0     0     >60
  0%      0      0      0       0     0        3     32       0     0     >60
  0%      0      0      0       0     0       15     63       0     0     >60
  4%      0      0      0       0     0      101    232       0     0     >60
 24%      0      0      0       0     0      383  20354       0    61     >60
 12%      0      0      0       0     0     4787   2274       0  4864     >60
 82%      0      0      0       0     1       40   4920       0    17     >60
 99%      0      0      0       0     0        3     38       0     0     >60
 99%      0      0      0       0     0        6     71       0     0     >60
 98%      0      0      0       0     0       13     37       0     0     >60
 99%      0      0      0       0     0        3     34       0     0     >60
 98%      0      0      0       0     0        4     61       0     0     >60
 99%      0      0      0       0     0       14     32       0     0     >60
 89%      0      0      0       0    15       81   6592       0     0     >60
 97%      0      0      0      45  2879     1055    769       0     0     >60
 92%      0      0      0      46  2326     1769   6337       0     0     >60
 99%      0      0      0       0     0       14     37       0     0     >60
 98%      0      0      0       0     0        4     73       0     0     >60
Nas1>
```

10.3.4 Special considerations in a filer-to-server configuration

Note the following considerations and limitations for NDMP-generated backup images that are stored in Tivoli Storage Manager server's storage hierarchy:

- Simultaneous write is not supported for NAS backup images.
- The backup mode for NDMP-generated data in the filer-to-server configuration remains image-based. This means that NDMP-generated data will not be created in progressive incremental mode.
- NAS backup data cannot be moved between NAS type storage pools (for example, NETAPPDUMP) and native storage pools.
- Export and import of NAS images and NAS nodes is not supported.
- The communication session from the filer to the server is established on the network that was identified through the gethostbyname function of the Tivoli Storage Manager server. Make sure that you have appropriate name resolution in place.

10.3.5 Firewall considerations

Filer-to-server firewall considerations are more stringent than they are when using filer-to-attached-library because communications can be initiated by either the Tivoli Storage Manager server or the NAS file server. It may be necessary to specify port numbers in the firewall rules to allow traffic to pass to and from the NAS devices. These two options in the Tivoli Storage Manager server options file are relevant:

- NDMPPortrange
- NDMPControlport

Port number control for the NAS devices is vendor-specific. Consult your vendor documentation for details.

NDMPPortrange

The NDMPPORTRANGE option specifies the range of port numbers through which Tivoli Storage Manager cycles to obtain a port number for accepting a session from a NAS device for data transfer. The syntax in the Tivoli Storage Manager server options file is:

```
NDMPPortrange port-number-low, port-number-high
```

The low and high port numbers are the low and high port numbers through which Tivoli Storage Manager cycles when needing a port number for accepting a session from a NAS device for data transfer. The default is 0,0, which means that Tivoli Storage Manager lets the operating system provide a port (ephemeral port). The minimum port number is 1024. The maximum port number is 32767.

If all ports specified are in use when a NAS device attempts to connect to the server, the operation fails.

If a single port number is specified (no comma and no port number for the high value), the default for the high port number is the low port number plus 100.

NDMPControlport

The NDMPCONTROLPORT specifies the port number to be used by Tivoli Storage Manager for internal communications for certain NDMP operations. The Tivoli Storage Manager server does not function as a general purpose NDMP tape server. The syntax in the Tivoli Storage Manager server options file is:

```
NDMPControlport port-number
```

The port number must be from 1024 to 32767. The default is 10000.

11

Backup sets

This chapter describes the backup set enhancements in Tivoli Storage Manager V5.4. First we provide a brief overview of backup sets. Then we discuss the following new V5.4 functions that can be used with a backup set:

- Creattion of a backup set table of contents (TOC).
- Generation of backup sets to a specific point-in-time.
- Multiple nodes data included in backup set.
- Support of image data in backup sets.
- Display of contents of a backup set and selection of individual files for restore.
- Improved tracking of backup sets.

For more information about backup sets refer to the *Tivoli Storage Manager Administrator's Guide*.

11.1 What is a backup set

A backup set is a collection of backed up data from a Tivoli Storage Manager client, stored and managed as a single object on sequential media in server storage. The Tivoli Storage Manager server creates copies of existing *active versions* of a client's backed up objects that are within the one or more file spaces specified with the GENERATE BACKUPSET command, and consolidates them onto sequential media. Therefore, a backup set does not require allocation of any additional space in the Tivoli Storage Manager database. An incremental backup must be completed for a client node before the server can generate a backup set for this client node. The backup set process is also known as *instant archive*.

Figure 11-1 shows the data flow when a backup set is generated.

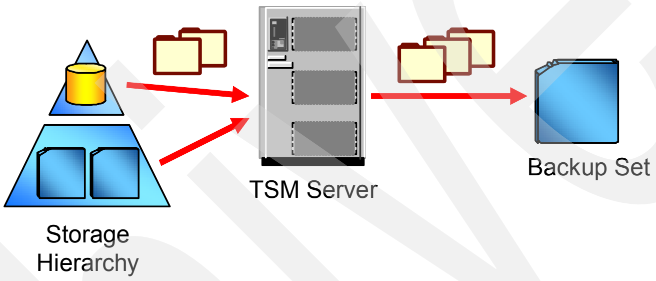


Figure 11-1 Data flow for backup set generation

When generating a backup set, you must specify a sequential device class that is associated with the media to which the backup set will be written. You can write backup sets to sequential tape and the device class FILE. The tape volumes containing the backup set are not associated with storage pools and, therefore, are not migrated through the storage pool hierarchy. For the device class FILE, the server creates each backup set with a file extension of OST. You can copy the FILE device class volumes (the OST files) to any removable media such as a USB hard disk drive.

The backup object types supported for backup sets include:

- Directories
- Files
- Image data (new in V5.4)

When generating backup sets, the server will search for the active version of a file in the following search order:

1. An active-data pool associated with a FILE device class
2. A random-access disk (DISK) storage pool
3. A primary or copy storage pool associated with a FILE device class
4. An active-data pool associated with onsite removable media (tape or optical)
5. A mounted (idle) sequential-access volume from a primary, copy, or active-data pool
6. A sequential-access volume available in an automated library
7. A sequential-access volume available in a manual library

If you regularly generate backup sets, for performance reasons you should consider either storing active backup data in an active-data pool associated with a FILE device class or collocating the primary storage pool in which the client node data is stored. Active-data pools are described in Chapter 7, “Active-data pools” on page 71. With collocation, less time is spent searching database entries, and fewer mount operations are required.

As well as restoring from the Tivoli Storage Manager server, data from backup sets can be restored from the Tivoli Storage Manager client, without requiring a connection to the Tivoli Storage Manager server. This is called a *local* backup set restore.

If you want to be able to restore backup set data locally with a Tivoli Storage Manager client generate the backup set to any sequential access devices whose device types are supported on both the client and server machines (for example, FILE device class or CD-ROM).

Figure 11-2 shows the process of how data is restored from a backup set.

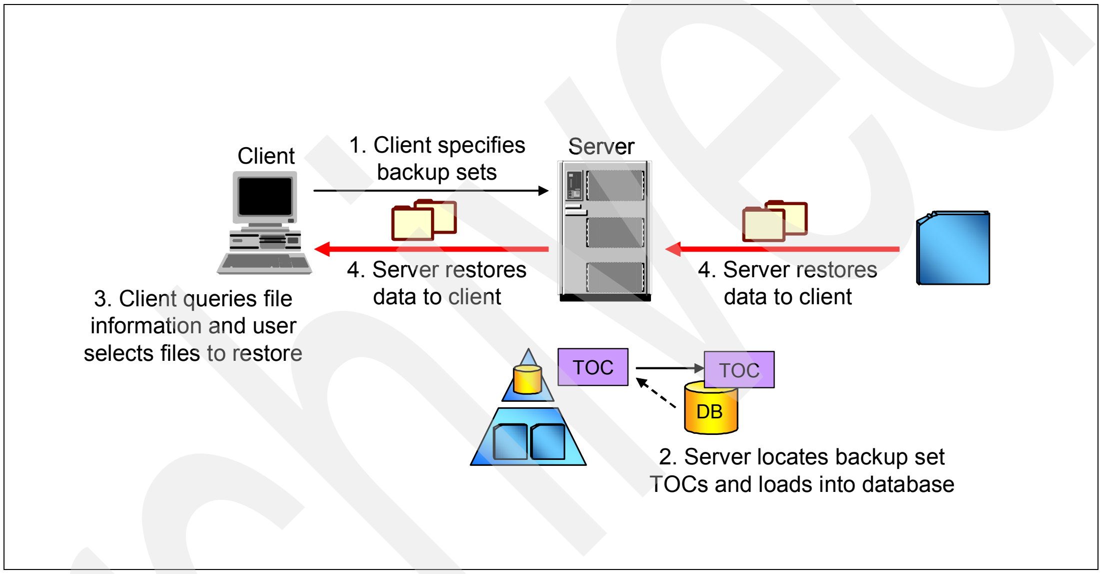

Client
1. Client specifies backup sets
Server
4. Server restores data to client
4. Server restores data to client
3. Client queries file information and user selects files to restore
TOC
TOC
DB
2. Server locates backup set TOCs and loads into database

Figure 11-2 Restore from a backup set

11.2 Create a backup set table of contents (TOC)

In V5.4, a table of contents is generated when a new backup set is created. It contains entries for each object stored in the backup set. These entries define the position of the object within the backup set. In order to query the contents of a backup set and choose files to restore, the TOC needs to be loaded into the server database, because it is stored in a storage pool instead of the Tivoli Storage Manager database.

You can specify the parameter TOC=YES with the GENERATE BACKUPSET command to create a TOC. Other values for the TOC parameter are NO and PREFERRED (the default). The TOC parameter is ignored when generating image and application backup sets, since a table of contents is always generated for these backup set types.

The restore process in Figure 11-2 on page 159 uses a TOC. You can query a backup set table of contents to select individual files for restore. See 11.6, “Display backup set: Select individual files for restore” on page 166, for details.

The TOCMGMTCLASS parameter specifies the management class to which the TOC should be bound. If you do not specify a management class, the TOC is bound to the default management class for the policy domain to which the node is assigned.

If you are creating a table of contents, you must define the TOCDESTINATION attribute in the backup copy group for the specified (or default) management class. These parameters specify the storage pool where the TOC is stored. Depending on how often you need to load the TOC for restores, you should consider using a disk storage pool as a destination for faster access.

It is also important that the retention of the backup copy group, from the management class used for the TOC, has at least the same retention period as the retention that you use for your backup set. This avoids the situation where your backup set is still available, but your TOC is already deleted.

If your TOC is deleted or you never had a TOC, you can use the GENERATE BACKUPSETTOC command to recreate or create a TOC.

When you delete a backup set, or if the backup set expires after the amount of days specified with the RETENTION parameter, the TOC is also deleted or expired, even if the retention of the backup copy group has not been reached.

11.3 Generate backup sets to a specific point-in-time

You can generate a backup set to a specific point-in-time using the PITDATE and PITTIME parameters on the GENERATE BACKUPSET command. When the PITDATE and PITTIME are specified, the backup set will contain files that were *active at the specified date and time,* even if the files are inactive at the time that the GENERATE BACKUPSET command is issued.

Backup sets are generated to a point-in-time by using one of two date and time specifications:

- The date and time specified on the GENERATE BACKUPSET command with PITDATE and PITTIME
- The date and time the that the GENERATE BACKUPSET command is issued

Point-in-time backup set generation works best if a recent date and time is specified. This means that files that have expired or are marked as expire-immediately cannot be included in the backup set.

The advantage of the PITDATE and PITTIME parameters is that you can generate a backup set more independently of the backup completion time of a node. For example, you could start a GENERATE BACKUPSET Sunday afternoon (because you have idle time on the Tivoli Storage Manager server at this time frame) with PITDATE=TODAY-1 and PITTIME=06:00:00 to include the data from the Friday night backup.

In Example 11-1 we show how to specify the PITDATE and PITTIME parameters when you generate a backup set.

Example 11-1 Generate a backup set with point-in-time specification

```
tsm: HAGGIS>generate backupset pfalz ITSO_PIT_BKUPSET * devcl=bkupset retention=
3 description="ITSO Backupset for Node PFALZ using PIT" toc=yes pitdate=today-5
pittime=06:00:00 datatype=file wait=yes
ANR0984I Process 9 for GENERATE BACKUPSET started in the FOREGROUND at
19:13:19.
ANR3500I Backup set for node PFALZ as ITSO_PIT_BKUPSET.27438117 (data type
File) being generated.
ANR3501I Backup set for PFALZ as ITSO_PIT_BKUPSET.27438117 (data type File)
completed successfully - processed 130 files.
ANR3547I Backup set ITSO_PIT_BKUPSET.27438117 used volume
E:\BACKUPSET\97342799.ost.
ANR1779I GENERATE BACKUPSET process completed: 1 backupset(s) were generated or
defined out of 1 backupset(s) requested by the command's specifications.
ANR0986I Process 9 for GENERATE BACKUPSET running in the FOREGROUND processed
130 items for a total of 20,145,735 bytes with a completion state of SUCCESS at
19:13:20.

tsm: HAGGIS>
```

11.4 Stacked backup sets

The Tivoli Storage Manager server V5.4 can generate a stacked backup set. A stacked backup set can contain different types of data for a given node (FILE data, IMAGE data, and APPLICATION data) and can contain data for multiple nodes.

A separate backup set is generated for each specified data type and each specified node, but all the backup sets are stored together on a single set of output media. Stacking of backup sets allows administrators to make more effective use of their tape media. It also allows administrators to keep certain backups together for easier tracking and recovery.

During the restore, when a stacked backup set is used, the client only processes data for the specified node. Data for other nodes is skipped.

In , “Multiple nodes data included in backup set” on page 162, we explain how to include multiple nodes in a single backup set.

The parameter DATATYPE specifies which kind of data type should be included in the backup set. Only data types for which backup data exists on the Tivoli Storage Manager server are allowed. You can use the following values for DATATYPE:

- ALL - all available data types for the specific node
- FILE - file and directory backup data
- IMAGE - image-based generated backup data
- APPLICATION - data backed up by application using the Tivoli Storage Manager API

> **Note:** If you have upgraded your Tivoli Storage Manager server V5.4 from Tivoli Storage Manager Express you can specify DATATYPE=APPLICATION when making a backup set. For more information about this topic, see the *Tivoli Storage Manager Administrator’s Guide*.

If you specify DATATYPE=FILE when you generate a backup set, the backup set is generated as it was for a pre-V5.4 server. When you generate a backup set with DATATYPE=ALL and imaged based backup data is available, it is included in the stacked backup set together with the file data. DATATYPE=IMAGE is explained in 11.5, “Support image data in backup sets” on page 163.

Multiple nodes data included in backup set

With the GENERATE BACKUPSET command, you can specify multiple nodes or node groups, and you can use wildcards with node names to include them in the backup set. A separate backup set is generated for each specified node, but all of the backup sets are stored together on the same set of output volumes.

In Example 11-2 we use the GENERATE BACKUPSET command and specify two node names separated by a comma to be included in the backup set.

Example 11-2 Generate backup set with two different node names

```
tsm: KODIAK>generate backupset irim,iffets ITSO_BKUPSET * devcl=lto4 retention=3
 description="ITSO Backupset for Node IRIM and IFFETS" toc=yes datatype=file wai
t=yes
ANR0984I Process 162 for GENERATE BACKUPSET started in the FOREGROUND at
14:27:44.
ANR3500I Backup set for node IRIM as ITSO_BKUPSET.144070 (data type File) being
generated.
ANR3501I Backup set for IRIM as ITSO_BKUPSET.144070 (data type File) completed
successfully - processed 2735 files.
ANR3500I Backup set for node IFFETS as ITSO_BKUPSET.144070 (data type File)
being generated.
ANR3501I Backup set for IFFETS as ITSO_BKUPSET.144070 (data type File)
completed successfully - processed 2735 files.
ANR3547I Backup set ITSO_BKUPSET.144070 used volume 747AAFL4.
ANR1779I GENERATE BACKUPSET process completed: 2 backupset(s) were generated or
defined out of 2 backupset(s) requested by the command's specifications.
ANR0986I Process 162 for GENERATE BACKUPSET running in the FOREGROUND processed
5470 items for a total of 1,042,027,389 bytes with a completion state of
SUCCESS at 14:29:10.

tsm: KODIAK>
```

As shown in Example 11-3, you can also define a group of nodes using the DEFINE NODEGROUP and DEFINE NODEGROUPMEMBER commands first. We then create the backup and specify the nodegroup name (ALL_SERVER) along with the GENERATE BACKUPSET command.

Example 11-3 Generate backup set for a node group

```
tsm: KODIAK>define nodegroup all_server

tsm: KODIAK>define nodegroupmember all_server irim,iffets
ANR4789I Node IFFETS associated to node group ALL_SERVER.
ANR4789I Node IRIM associated to node group ALL_SERVER.
ANR4787I DEFINE NODEGROUPMEMBER: 2 members defined in the node group
ALL_SERVER.

tsm: KODIAK>generate backupset all_server ITSO_BKUPSET * devcl=lto4 retention=3
description="ITSO Backupset for Node IRIM and IFFETS" toc=yes datatype=file wait
```

```
=yes
ANR0984I Process 163 for GENERATE BACKUPSET started in the FOREGROUND at
14:31:55.
ANR3500I Backup set for node IFFETS as ITSO_BKUPSET.144075 (data type File)
being generated.
ANR3501I Backup set for IFFETS as ITSO_BKUPSET.144075 (data type File)
completed successfully - processed 2735 files.
ANR3500I Backup set for node IRIM as ITSO_BKUPSET.144075 (data type File) being
generated.
ANR3501I Backup set for IRIM as ITSO_BKUPSET.144075 (data type File) completed
successfully - processed 2735 files.
ANR3547I Backup set ITSO_BKUPSET.144075 used volume 748AAFL4.
ANR1779I GENERATE BACKUPSET process completed: 2 backupset(s) were generated or
defined out of 2 backupset(s) requested by the command's specifications.
ANR0986I Process 163 for GENERATE BACKUPSET running in the FOREGROUND processed
5470 items for a total of 1,042,027,389 bytes with a completion state of
SUCCESS at 14:33:15.
```

11.5 Support image data in backup sets

When generating a backup set, you can specify with the DATATYPE=IMAGE parameter to include image data. For example, the command GENERATE BACKUPSET PFALZ ITSO_IMG_BKUPSET * DEVCL=LTO DATATYPE=IMAGE would include the image data from the node PFALZ in the backup set.

An image backup set includes the image and all files and directories changed or deleted since the image was backed up, depending on the point in time when the backup set is generated. Tables of contents (TOC) are automatically generated for any backup sets that contain image data. If the GENERATE BACKUPSET command cannot generate tables of contents for these backup sets, then it fails.

First, we create an image backup of the node PFALZ.

The backup set in Example 11-4 on page 163 was generated directly after the image backup was completed.

Example 11-4 Backup set with image data directly after the image backup

```
tsm: HAGGIS>generate backupset pfalz ITSO_IMG_BKUPSET * devclass=bkupset
retention=3 description="ITSO Backupset for Node PFALZ" toc=yes datatype=image
wait=yes
ANR0984I Process 6 for GENERATE BACKUPSET started in the FOREGROUND at
14:02:00.
ANR3500I Backup set for node PFALZ as ITSO_IMG_BKUPSET.27438108 (data type
Image) being generated.
ANR3501I Backup set for PFALZ as ITSO_IMG_BKUPSET.27438108 (data type Image)
completed successfully - processed 5 files.
ANR3547I Backup set ITSO_IMG_BKUPSET.27438108 used volume
E:\BACKUPSET\97334920.ost.
ANR1779I GENERATE BACKUPSET process completed: 1 backupset(s) were generated or
defined out of 1 backupset(s) requested by the command's specifications.
```

```
ANR0986I Process 6 for GENERATE BACKUPSET running in the FOREGROUND processed 5
items for a total of 9,751,380,081 bytes with a completion state of SUCCESS at
14:06:20.
```

We then created some new files on PFALZ and backed them up. In Example 11-5 we generate a backup set for the node PFALZ, after these additional files were stored.

Example 11-5 Generate an image backup set with subsequently changed files

```
tsm: HAGGIS>generate backupset pfalz ITSO_IMG_BKUPSET * devclass=bkupset
retention=3 description="ITSO Backupset for Node PFALZ" toc=yes datatype=image
wait=yes
ANR0984I Process 5 for GENERATE BACKUPSET started in the FOREGROUND at
16:02:05.
ANR3500I Backup set for node PFALZ as ITSO_IMG_BKUPSET.27438100 (data type
Image) being generated.
ANR3501I Backup set for PFALZ as ITSO_IMG_BKUPSET.27438100 (data type Image)
completed successfully - processed 19 files.
ANR3547I Backup set ITSO_IMG_BKUPSET.27438100 used volume
E:\BACKUPSET\97331325.ost.
ANR1779I GENERATE BACKUPSET process completed: 1 backupset(s) were generated or
defined out of 1 backupset(s) requested by the command's specifications.
ANR0986I Process 5 for GENERATE BACKUPSET running in the FOREGROUND processed
18 items for a total of 9,717,635,772 bytes with a completion state of SUCCESS
at 16:06:20.
```

If you compare the number of items that were included in the respective backup sets, you can see that 18 items were included in Example 11-5 on page 164, compared to five items in Example 11-4 on page 163. This is because the files and directories that were backed up after the image are also included in the backup set, even if you have specified the DATATYPE=IMAGE parameter.

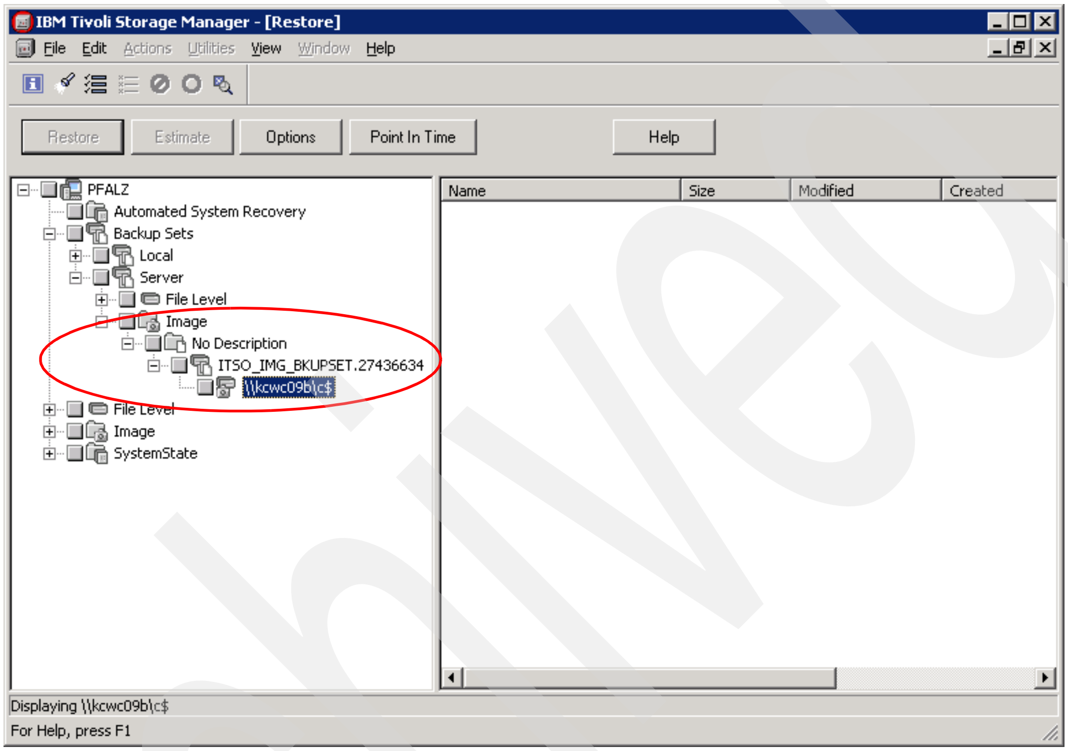
Example 11-6 shows how we can query the contents of the second backup set and display the additional files in the IBMTOOLS directory.

Example 11-6 Query backup set contents

```
tsm: HAGGIS>query backupsetcontent pfalz ITSO_IMG_BKUPSET.27438100 datatype=image

Node Name                 Filespace      Client's Name for File
                          Name
---------------------     ----------     ------------------------------------------
PFALZ                     \\kcwc09b\c$   \TSMIMAGE-WINNT\FULL
PFALZ                     \\kcwc09b\c$   \TSMIMAGE-WINNT\VOL_EXTENTS
PFALZ                     \\kcwc09b\c$   \TSMIMAGE-WINNT\VOL_DATA
PFALZ                     \\kcwc09b\c$   \TSMIMAGE-WINNT\OBF_EXTENTS
PFALZ                     \\kcwc09b\c$   \TSMIMAGE-WINNT\OBF_DATA
PFALZ                     \\kcwc09b\c$   \IBMTOOLS
PFALZ                     \\kcwc09b\c$   \IBMTOOLS\7APM12WW
PFALZ                     \\kcwc09b\c$   \IBMTOOLS\7APM12WW\FLASH32.DLL
PFALZ                     \\kcwc09b\c$   \IBMTOOLS\7APM12WW\NT4PNP.SYS
PFALZ                     \\kcwc09b\c$   \IBMTOOLS\7APM12WW\PKGMGR
PFALZ                     \\kcwc09b\c$   \IBMTOOLS\7APM12WW\SETUP.EXE
PFALZ                     \\kcwc09b\c$   \IBMTOOLS\7APM12WW\SHFOLDER.EXE
PFALZ                     \\kcwc09b\c$   \IBMTOOLS\7APM12WW\SWI.XML
PFALZ                     \\kcwc09b\c$   \IBMTOOLS\7APM12WW\SWI32.SYS
PFALZ                    \\kcwc09b\c$   \IBMTOOLS\7APM12WW\SWI32.VXD
PFALZ                    \\kcwc09b\c$   \IBMTOOLS\7APM12WW\TPILIBB.DLL
PFALZ                    \\kcwc09b\c$   \IBMTOOLS\7APM12WW\TPISETUP.DAT
PFALZ                    \\kcwc09b\c$   \IBMTOOLS\7APM12WW\TPISETUP.DLL
```

You can select an image for a restore from the backup set using the Tivoli Storage Manager backup-archive client GUI, as shown in Figure 11-3.



Displaying \\kcwc09b\c$

For Help, press F1

Figure 11-3 Image restore from a backup set using the backup-archive GUI

You can also use the CLI to display the contents of a backup set, as shown in Example 11-7, and restore the image with the command:

```
RESTORE IMAGE -BACKUPSETNAME=ITSO_IMG_BKUPSET.27436634.
```

Example 11-7 Using the CLI to display the backup set content

```
tsm> query backupset
Session established with server HAGGIS: Windows
  Server Version 5, Release 5, Level 0.0
  Server date/time: 12/07/2007 15:59:15  Last access: 12/07/2007 15:48:05


   Backup Set Name                 Generation Date   Retention Description
   ------------------------------ ------------------- ---------- -----------
 1 ITSO_BKUPSET.27433772          12/07/2007 11:42:25 1          ITSO Backupset
 for Node PFALZ
 2 ITSO_IMG_BKUPSET.27436634      12/07/2007 15:27:20 365        No Description
```

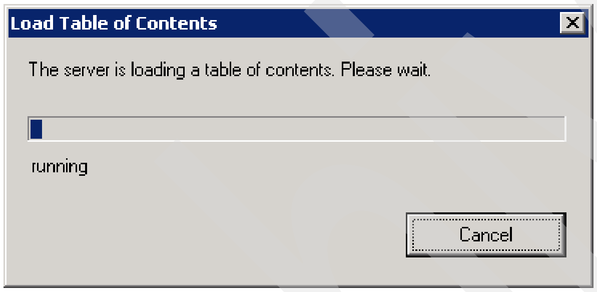
```
tsm> query image -backupsetname=ITSO_IMG_BKUPSET.27436634
   Image Size Stored Size FSType     Backup Date     Mgmt Class A/I Image Name
  ---------- ----------- ------ ------------------- ---------- --- ----------
 1   74.52 GB     9.03 GB  NTFS  12/07/2007 14:34:05     -       A  \\kcwc09b\c$
```

The image data within the backup set cannot be restored using local backup set restore with the backup-archive client. If you have a backup set generated that contains files and image data, only the files will be selectable for the restore if you use the local backup set restore.

11.6 Display backup set: Select individual files for restore

The Tivoli Storage Manager backup-archive client CLI before V5.4 could already restore individual files from a backup set, but the user had to know the exact path and name of the file to restore. With the V5.4 client you can now display and select individual files for a restore.

When you expand a backup set in the GUI, the TOC is loaded into the Tivoli Storage Manager database, as shown in Figure 11-4.



The server is loading a table of contents. Please wait.

running

Figure 11-4 Loading the TOC into the Tivoli Storage Manager database

In Figure 11-5 on page 167 the TOC is loaded and you can browse through the directory structure and select individual files for the restore.

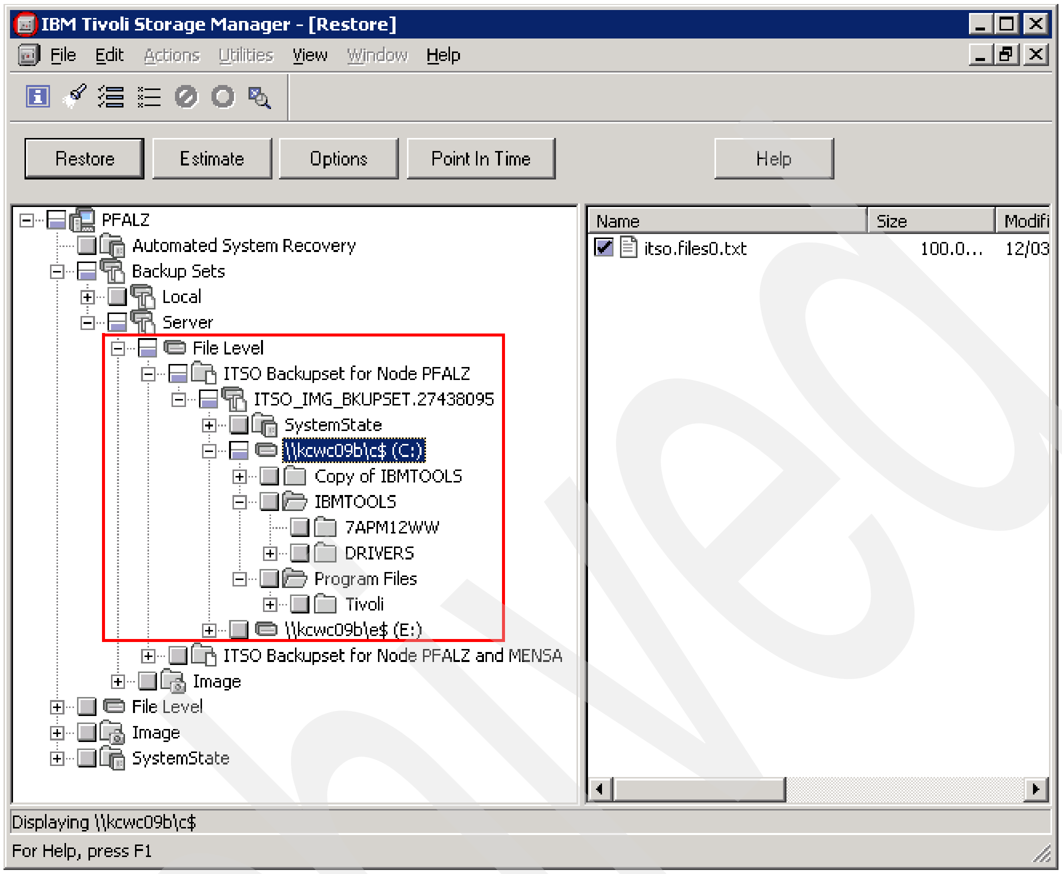
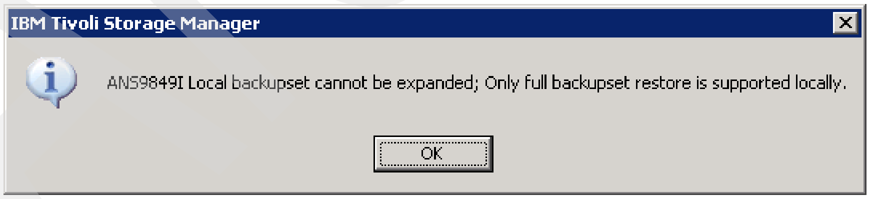


Figure 11-5 Select individual files from a backup set for a restore

Note that this function is only supported if the backup set resides on the Tivoli Storage Manager server. If you load a backup set locally and try to expand it, the information message shown in Figure 11-6 is displayed. This is because the TOC is stored in the Tivoli Storage Manager storage pool, as described in 11.2, “Create a backup set table of contents (TOC)” on page 159.



ANS9849I Local backupset cannot be expanded; Only full backupset restore is supported locally.

Figure 11-6 Information message displays when local backup set is expanded

11.7 Improved tracking of backup sets

The QUERY BACKUPSET command is enhanced in V5.4. The command displays information about all backup sets, whether they are on their own media or stacked together with other backup sets onto one media. If you specify the FORMAT=DETAIL parameter, the included filespaces and the volumes that are used for a backup set are also displayed, as shown in Example 11-8 on page 168.

Example 11-8 query backupset output

```
tsm: KODIAK>query backupset format=detail

                 Node Name: IFFETS
           Backup Set Name: ITSO_BKUPSET.144075
                 Data Type: File
                 Date/Time: 12/10/2007 14:31:55
          Retention Period: 3
         Device Class Name: LTO4
               Description: ITSO Backupset for Node IRIM and IFFETS
Has Table of Contents (TOC)?: Yes
           Filespace names: ASR SYSTEM OBJECT \\klchl2m\c$
              Volume names: 748AAFL4

                 Node Name: IRIM
           Backup Set Name: ITSO_BKUPSET.144075
                 Data Type: File
                 Date/Time: 12/10/2007 14:31:55
          Retention Period: 3
         Device Class Name: LTO4
               Description: ITSO Backupset for Node IRIM and IFFETS
Has Table of Contents (TOC)?: Yes
           Filespace names: ASR SYSTEM OBJECT \\klchl2m\c$
              Volume names: 748AAFL4

tsm: KODIAK>
```

12

Administration Center

This chapter describes the new functions in Administration Center that were introduced in V5.4.

The following updates were made to the Administration Center interface:

- Update of the administrator password for the Administration Center user to a group of selected servers
- Command-line applet usability fixes
- Administration Center tutorials translated
- Support for additional commands: AUDIT LIBRARY, AUDIT VOLUME, QUERY NODEDATA, MOVE NODEDATA, QUERY MEDIA, and MOVE MEDIA

The Administration Center has also been updated to support new functions in Tivoli Storage Manager:

- Tivoli Storage Manager V5.4
  - Use the Tivoli Storage Manager server as the NDMP tape server (network filer-to-Tivoli Storage Manager server backup).
  - Create media for off-site vaulting from NDMP-generated images.
  - Destruction of expired data (data shredding) for random-access disk.
  - Tape drive encryption.
  - Optical device support on Linux.
- Tivoli Storage Manager V5.5

  Restartable export

12.1 Administration Center

The Administration Center Web-interface provides an easy way to manage multiple server instances from a single browser window. It is available as of Tivoli Storage Manager V5.3, and is hosted in the Integrated Solution Console (ISC) framework. ISC is a general framework, supporting multiple modules that serve different purposes. The Administration Center module enables you to manage and monitor your Tivoli Storage Manager environment specifically.

12.1.1 Installation

Both products, Administration Center and Integrated Solutions Console, are distributed separately. ISC is available via regular system order, while the Administration Center is available via the normal IBM service FTP site. To install:

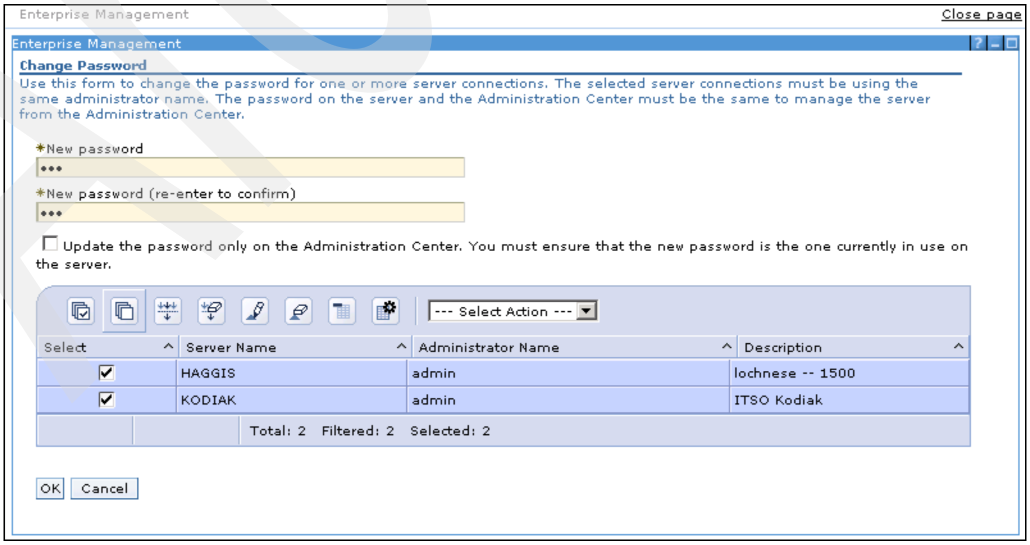
1. Install the ISC.
2. Install the Administration Center into ISC.

Since ISC is built on top of WebSphere® Application Server and PortalBase, it requires significant system resources. We recommend installing it on a different machine than the one running the Tivoli Storage Manager server.

For more information about the installation refer to the *IBM Tivoli Storage Manager Version 5.3 Technical Guide*, SG24-6638.

12.2 Update Administration Center password for multiple servers

You can change the administrator password for the Administration Center user for one or more server connections at the same time. To do this, in Enterprise Management, select **Change Password** from the pull-down. Select one or more servers for which you want to update the password and enter the new password, as shown in Figure 12-1.



Change Password

Use this form to change the password for one or more server connections. The selected server connections must be using the same administrator name. The password on the server and the Administration Center must be the same to manage the server from the Administration Center.

*New password
•••

*New password (re-enter to confirm)
•••

□ Update the password only on the Administration Center. You must ensure that the new password is the one currently in use on the server.

Select	Server Name	Administrator Name	Description
☑	HAGGIS	admin	lochnese -- 1500
☑	KODIAK	admin	ITSO Kodiak

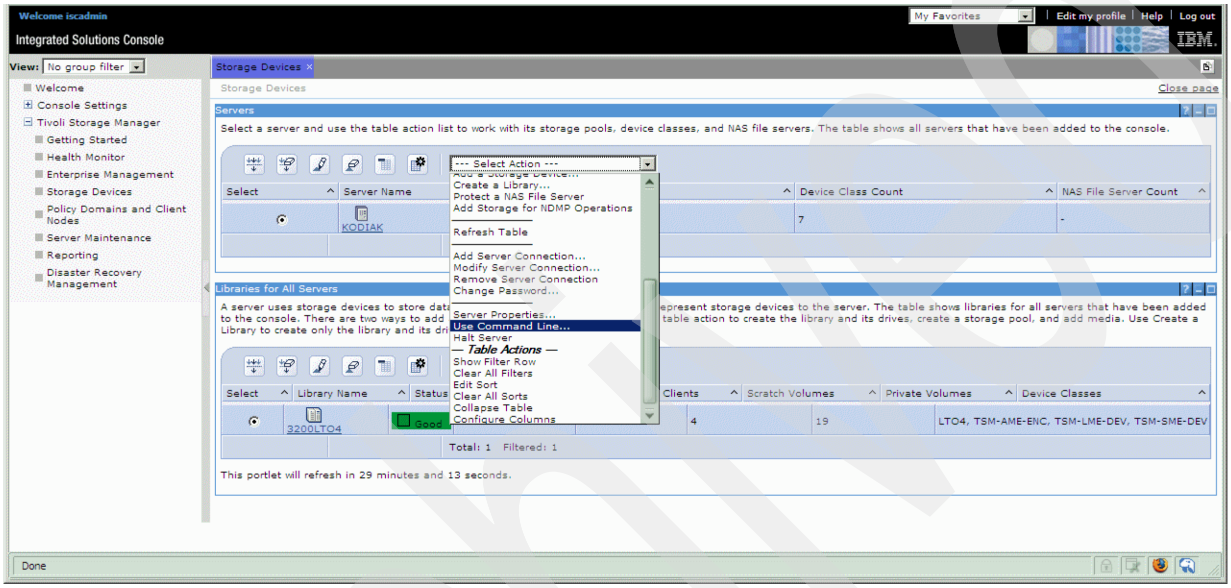
Total: 2 Filtered: 2 Selected: 2

Figure 12-1 Update the administrator password for the Administration Center

12.3 Using the command line in the Administration Center

When you are logged into the Administration Center:

1. Open a command line, as shown in Figure 12-2, by selecting any one of **Health Monitor**, **Enterprise Management**, **Storage Devices**, **Policy Domains and Client Nodes**, **Server Maintenance**, or **Disaster Recovery Management** in the Navigation menu on the left. Our example shows Storage Devices.
2. Select the server for which you like to open the command line (KODIAK in our example).
3. Select **Use Command Line** from the **Select Action** drop-down menu.



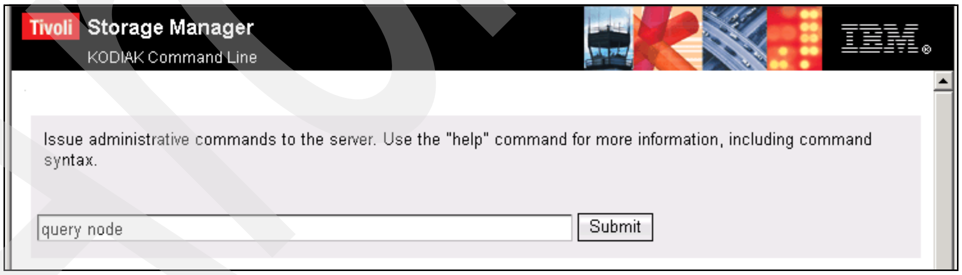
Select a server and use the table action list to work with its storage pools, device classes, and NAS file servers. The table shows all servers that have been added to the console.

A server uses storage devices to store data ... to the console. There are two ways to add ... Library to create only the library and its dri... epresent storage devices to the server. The table shows libraries for all servers that have been added ... table action to create the library and its drives, create a storage pool, and add media. Use Create a

This portlet will refresh in 29 minutes and 13 seconds.

Figure 12-2 Start the command line from the Administration Center

The command line opens in a separate browser window, as shown in Figure 12-3.



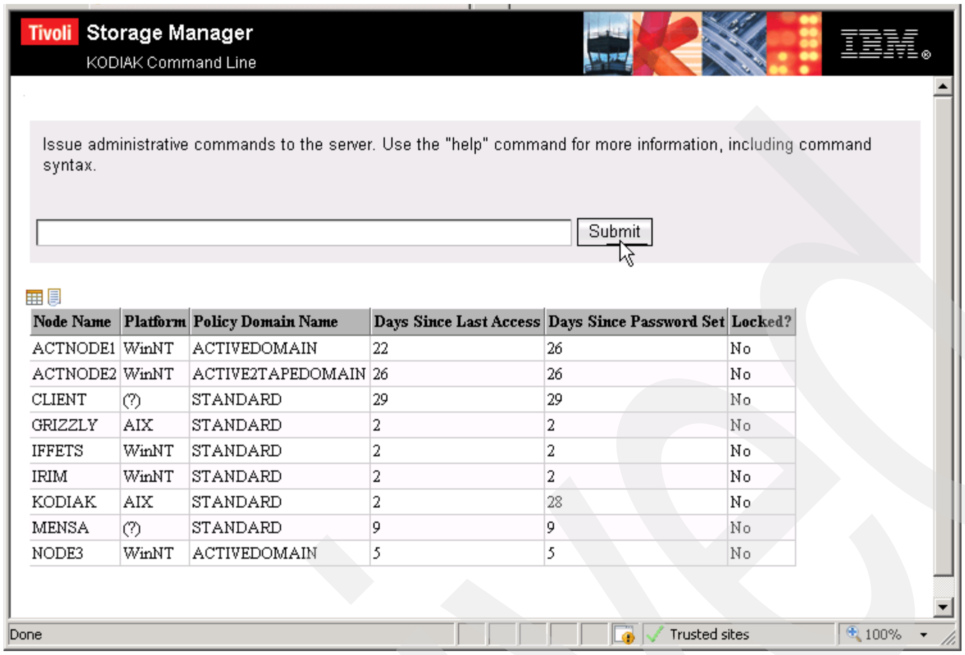
Issue administrative commands to the server. Use the "help" command for more information, including command syntax.

query node

Figure 12-3 Command line browser window from the Administration Center

Note: JAVA Version 1.4.2 should be installed to run the command line.

You can enter a Tivoli Storage Manager administrative command. Press Enter or click **Submit** to execute the command on the server, as shown in Figure 12-4 on page 172.



Issue administrative commands to the server. Use the "help" command for more information, including command syntax.

Node Name	Platform	Policy Domain Name	Days Since Last Access	Days Since Password Set	Locked?
ACTNODE1	WinNT	ACTIVEDOMAIN	22	26	No
ACTNODE2	WinNT	ACTIVE2TAPEDOMAIN	26	26	No
CLIENT	(?)	STANDARD	29	29	No
GRIZZLY	AIX	STANDARD	2	2	No
IFFETS	WinNT	STANDARD	2	2	No
IRIM	WinNT	STANDARD	2	2	No
KODIAK	AIX	STANDARD	2	28	No
MENSA	(?)	STANDARD	9	9	No
NODE3	WinNT	ACTIVEDOMAIN	5	5	No

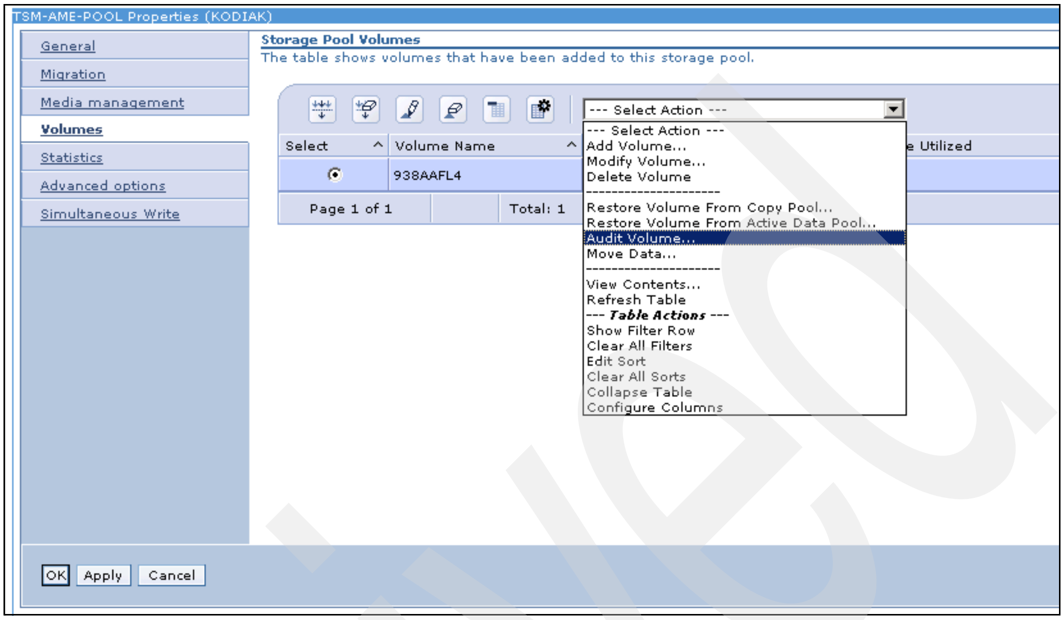
Figure 12-4 Command output in the Administration Center

12.3.1 New commands

The following commands are now available in the Administration Center:

- AUDIT LIBRARY: **Storage Devices** ∅ **Libraries** table. Select **Audit Library** from the pull-down.

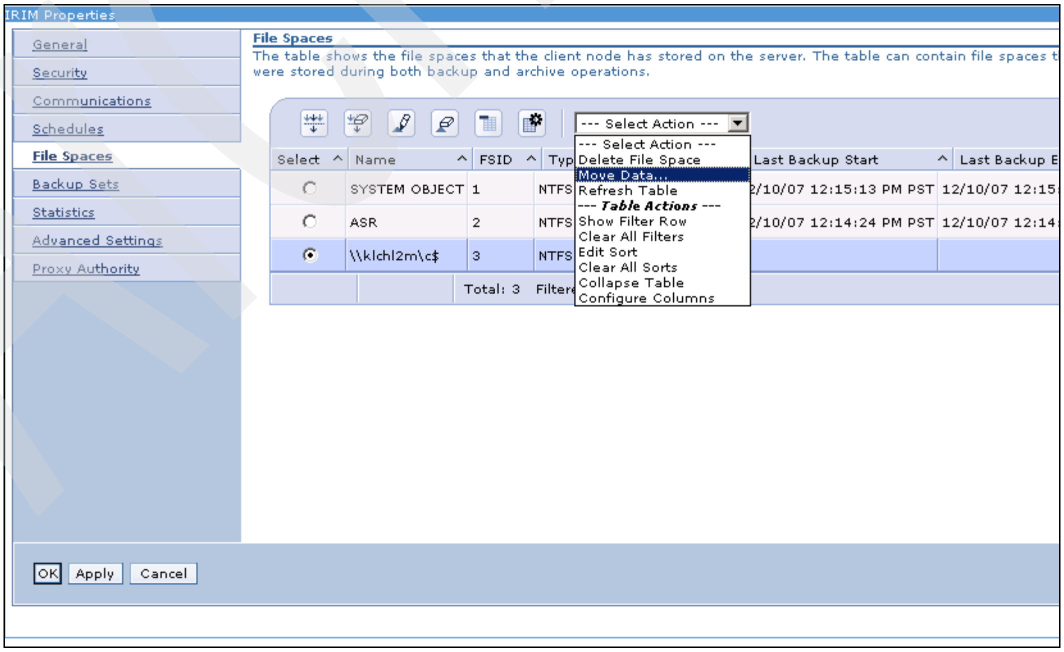
- AUDIT VOLUME: **Storage Devices** ∅ **View Storage Pools**. Click a storage pool. Select **Volumes** in the Properties section. Click a volume. Select **Audit Volume** from the pull-down, as shown in Figure 12-5.



Select	Volume Name	e Utilized
●	938AAFL4	
Page 1 of 1	Total: 1	

Figure 12-5 Audit volume

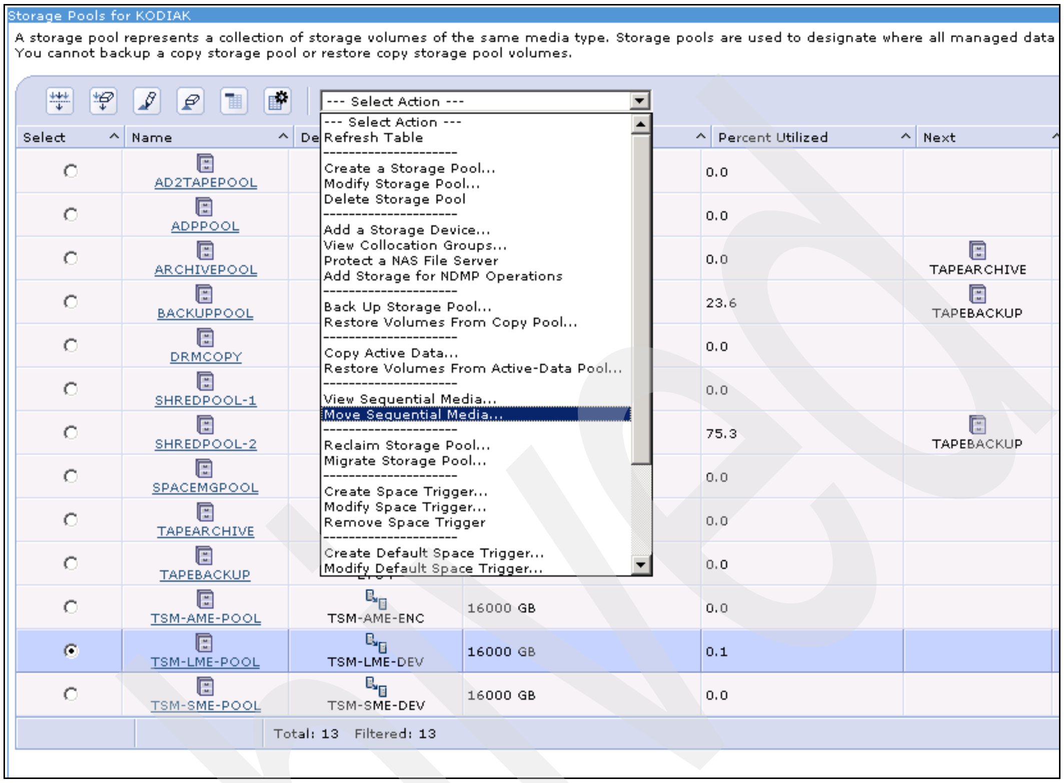
- QUERY NODEDATA and MOVE NODEDATA: **Policy Domains and Client Nodes** ∅ **View Policy Domains**. Click a Policy domain. Expand the **Client Nodes** section. Click a node. Click **File Spaces** in the Properties page. Select a file space. Select **Move Data** from the pull-down, as shown in Figure 12-6. This opens the Move Nodedata panel. The Query Nodedata information is used automatically to gather information about the storage pools.



Select	Name	FSID	Typ	Last Backup Start	Last Backup E
○	SYSTEM OBJECT	1	NTFS	2/10/07 12:15:13 PM PST	12/10/07 12:15
○	ASR	2	NTFS	2/10/07 12:14:24 PM PST	12/10/07 12:14
●	\\klchl2m\c$	3	NTFS		
		Total: 3	Filter		

Figure 12-6 Move Nodedata

- QUERY MEDIA and MOVE MEDIA: **Storage Devices ∅ View Storage Pools**. Select a storage pool. Select **View Sequential Media** or **Move Sequential Media**, as shown in Figure 12-7 on page 174.



Storage Pools for KODIAK

A storage pool represents a collection of storage volumes of the same media type. Storage pools are used to designate where all managed data
You cannot backup a copy storage pool or restore copy storage pool volumes.

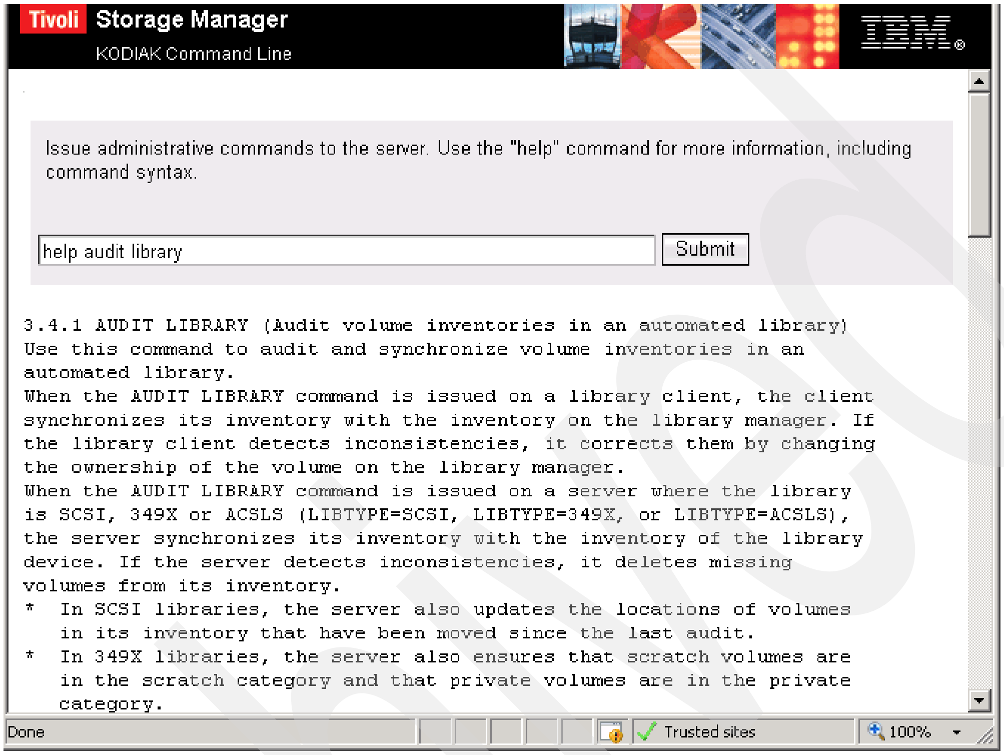
Select	Name	De		Percent Utilized	Next
○	AD2TAPEPOOL			0.0	
○	ADPPOOL			0.0	
○	ARCHIVEPOOL			0.0	TAPEARCHIVE
○	BACKUPPOOL			23.6	TAPEBACKUP
○	DRMCOPY			0.0	
○	SHREDPOOL-1			0.0	
○	SHREDPOOL-2			75.3	TAPEBACKUP
○	SPACEMGPOOL			0.0	
○	TAPEARCHIVE			0.0	
○	TAPEBACKUP			0.0	
○	TSM-AME-POOL	TSM-AME-ENC	16000 GB	0.0	
●	TSM-LME-POOL	TSM-LME-DEV	16000 GB	0.1	
○	TSM-SME-POOL	TSM-SME-DEV	16000 GB	0.0	

Total: 13 Filtered: 13

Figure 12-7 Move Sequential Media

When you select **View Sequential Media**, you will see a filtering table to display the media in the storage pool. When you select **Move Sequential Media**, a wizard to move storage pool volumes starts.

If you are not familiar with any of the commands above, you can enter HELP followed by the command in the Administration Center command line to get more details about the command itself. For example, the command HELP AUDIT LIBRARY displays further information about the AUDIT LIBRARY command, as shown in Figure 12-8 on page 175



Issue administrative commands to the server. Use the "help" command for more information, including command syntax.

help audit library

```
3.4.1 AUDIT LIBRARY (Audit volume inventories in an automated library)
Use this command to audit and synchronize volume inventories in an
automated library.
When the AUDIT LIBRARY command is issued on a library client, the client
synchronizes its inventory with the inventory on the library manager. If
the library client detects inconsistencies, it corrects them by changing
the ownership of the volume on the library manager.
When the AUDIT LIBRARY command is issued on a server where the library
is SCSI, 349X or ACSLS (LIBTYPE=SCSI, LIBTYPE=349X, or LIBTYPE=ACSLS),
the server synchronizes its inventory with the inventory of the library
device. If the server detects inconsistencies, it deletes missing
volumes from its inventory.
*  In SCSI libraries, the server also updates the locations of volumes
   in its inventory that have been moved since the last audit.
*  In 349X libraries, the server also ensures that scratch volumes are
   in the scratch category and that private volumes are in the private
   category.
```

Figure 12-8 Display command help information in the command line

13

QUERY DIRSPACE command

This chapter introduces the new QUERY DIRSPACE command that allows you to identify available space for a given file device class.

13.1 QUERY DIRSPACE

The QUERY DIRSPACE command allows you to determine the actual amount of total and available space for each directory in a FILE device class.

The total space reported for a device class is not necessarily the sum of all directories in the device class. If two or more directories reside in the same file system, the command reports each directory individually, making it seem as if there is more storage available than there actually is. If no two directories of a single device class reside in the same file system, then the total space for the device class will be the sum of each individual directory.

Example 13-1 shows the QUERY DIRSPACE output for multiple device classes configured to a single filespace (/tsm/stg/).

Example 13-1 QUERY DIRSPACE, multiple device classes in one file system

```
tsm: TSMAIX55>query dirspace file*

Device Class   Directory                                  Estimated   Estimated
Name                                                       Capacity   Available
------------   ----------------------------------------   ---------   ---------
FILECLASS      /tsm/stg/activedata                          4,800 M     2,297 M
FILECLASS2     /tsm/stg/fileclass2                          4,800 M     2,297 M
```

Example 13-2 shows the real space left in /tsm/stg.

Example 13-2 File system free space left

```
[root@Kodiak:]/ # df -k /tsm/stg
Filesystem    1024-blocks      Free %Used    Iused %Iused Mounted on
/dev/tsmstg       4915200   2353316   53%        9     1% /tsm/stg
```

In Example 13-3, we update one of the device classes to include another directory in the same file system, as well as another file system.

Example 13-3 Include other directories to the device class

```
tsm: TSMAIX55>update devc FILECLASS DIR="/tsm/stg/activedata,/tsm/stg/backupdata
              ,/tmp"
ANR2205I Device class FILECLASS updated.
```

We redisplay the QUERY DIRSPACE output in Example 13-4. Note that the capacity in /tsm/stg is still reported multiple times, even though it is obviously the same file system.

Example 13-4 UERY DIRSPACE, multiple directories for one device class in one file system

```
tsm: TSMAIX55>query dirspace file*

Device Class   Directory                                  Estimated   Estimated
Name                                                       Capacity   Available
------------   ----------------------------------------   ---------   ---------
FILECLASS      /tsm/stg/activedata                          4,800 M     2,298 M
FILECLASS      /tsm/stg/backupdata                          4,800 M     2,298 M
FILECLASS      /tmp                                           992 M       775 M
FILECLASS2     /tsm/stg/fileclass2                          4,800 M     2,298 M
```

Example 13-5 shows the output with file device classes configured to different drives on a Windows box.

Example 13-5 QUERY DIRSPACE, single device class per file system

```
tsm: LOCHNESE>query dirspace

Device Class   Directory                                  Estimated   Estimated
Name                                                       Capacity   Available
------------   ----------------------------------------   ---------   ---------
DBBKUP         E:\TSMDBBKUP                               476,937 M   443,366 M
FILECLASS      C:\TSMDATA\SERVER1                         152,625 M   133,131 M
```

The QUERY DIRSPACE command is available for all Tivoli Storage Manager server platforms except z/OS.

Part 4

Tivoli Storage Manager V5.4 client enhancements

This part presents enhancements to Tivoli Storage Manager V5.4 clients. First we detail the supported operating systems and summarize the new features and functions, then subsequent chapters present further details of the most significant new features.

14

Version 5.4 client supported environments

This chapter describes the following Tivoli Storage Manager Version 5.4 client functions:

- Supported client OS levels, including Mac OSX Intel
- Summary of additional client functionality

The major new client features of Tivoli Storage Manager V5.4 are described in detail in separate chapters.

For full details, always refer to the announcement letter and to the installation and user guide for the relevant server. Announcement letters can be found using the keywords *Tivoli Storage Manager* at:

http://www-01.ibm.com/common/ssi/index.wss

or directly for V5.4 as:

http://www-01.ibm.com/common/ssi/index.wss?DocURL=http://www-01.ibm.com/common/ssi/rep_ca/2/877/ENUSZP07-0102/index.html&InfoType=AN&InfoSubType=CA&InfoDesc=Announcement+Letters&panelurl=index.wss%3F&paneltext=Announcement%20letter%20search

You will find the V5.4 manuals and client readme files in the Previous Versions section of:

http://publib.boulder.ibm.com/infocenter/tivihelp

14.1 Client operating systems supported in V5.4

You will find the client readmes and Release Notes for Tivoli Storage Manager V5.4 and V5.4.1 at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v1r1/topic/com.ibm.itsmreadme.doc/reln_client.html

The client installation and user guides can be found at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v1r1/topic/com.ibm.itsmc.doc_5.4/clients.html

An up-to-date overview of all the supported operating systems with the corresponding version of Tivoli Storage Manager client can be found at:

http://www-1.ibm.com/support/docview.wss?rs=663&context=SSGSG7&uid=swg21243309&loc=en_US&cs=utf-8&lang=en

Generally, the migration plan for a Tivoli Storage Manager update allows clients and servers to be upgraded at different times. Also see 1.3.1, "Client and server version compatibility" on page 6. Although Tivoli Storage Manager is very flexible as to the versions of client code used, when possible always upgrade the client code to keep the server and client versions in sync. However, when a certain client is no longer supported, the old and unsupported client code versions most often continue to work according to its original functionality.

14.1.1 AIX clients for Tivoli Storage Manager V5.4

The Tivoli Storage Manager V5.4 client on AIX is supported at:

- AIX backup-archive client
  - AIX V5.2 (32 bit or 64 bit)
  - AIX V5.3 (32 bit or 64 bit)
  - Java JRE 1.4.1+, or 1.5 for the Java GUI
  - File systems supported for backup-archive operations
    - JFS
    - JFS2
    - GPFS V2.3 PTF 11 (2.3.0.11) or later PTF, or V3.1 PTF 8 (3.1.0.8) or later PTF
    - VERITAS (VxFS) 4.0
  - Client capabilities
    - Administrative client command-line interface (CLI)
    - Backup-archive CLI
    - Backup-archive Java Graphical User Interface (Java GUI)
    - Backup-archive Web Client Interface
    - Tivoli Storage Manager API
    - X/Open API (32 bit)
- With HACMP
  - AIX V5.2 or V5.3 (32 bit or 64 bit)
  - HACMP 5.3 or 5.4
- AIX HSM client
  - AIX V5.2.1 or AIX V5.3 (32 bit or 64 bit with GPFS; 64 bit with JFS2)
  - GPFS V2.3 PTF 11 (2.3.0.11) or later PTF, or V3.1 PTF 8 (3.1.0.8) or later PTF
  - Java JRE 1.4.1 or later
  - Client capabilities

    - HSM Client CLI (requires Tivoli Storage Manager for Space Management)
    - HSM Java GUI

- With HACMP
  - AIX V5.2.1, or later (32 bit and 64 bit)
  - HACMP 5.3

14.1.2 Apple Macintosh backup-archive client for Tivoli Storage Manager V5.4

The Tivoli Storage Manager V5.4 client on Apple Macintosh is supported at:

- Macintosh OS X, V10.4.7 or later
- Client capabilities
  - Administrative client CLI
  - Backup-archive Web Client Interface
  - Backup-archive Java Graphical User Interface (Java GUI)

14.1.3 Hewlett-Packard HP-UX clients for Tivoli Storage Manager V5.4

The Tivoli Storage Manager V5.4 client on HP-UX is supported at:

- An HP-UX PA-RISC backup-archive client
  - HP-UX 11i V2 (32 bit or 64 bit)
  - HP-UX 11i V3 from V5.4.1
  - HP-UX V11i V1 from V5.4.2 (in March 2008)
  - Java JRE 1.4.1 or later
  - Client capabilities
    - Administrative client CLI
    - Backup-archive CLI
    - Backup-archive Java Graphical User Interface (Java GUI)
    - Backup-archive Web Client Interface
    - Tivoli Storage Manager API
    - X/Open API (32 bit)
- Hewlett-Packard HP-UX PA-RISC HSM client
  - HP-UX 11i V2 (32 bit or 64 bit)
  - File system
    - VERITAS file system (VxFS) 4.1 with Patch from VERITAS PHKL_29896 and PHCO_29897
    - VERITAS Volume Manager (VxVM) 3.5 or later, OnlineJFS 3.3 or 3.5 with a valid license
  - Client capabilities
    - HSM Client CLI
    - HSM Java GUI
- Hewlett-Packard HP-UX Itanium backup-archive client
  - HP-UX level 11iV2 or later (64 bit)
  - HP-UX 11i V3 from V5.4.1

  - Java JRE 1.4.1 or later
  - Client capabilities
    - Administrative Client CLI
    - Backup-archive CLI
    - Backup-archive Java Graphical User Interface (Java GUI)
    - Backup-Archive Web Client Interface
    - Tivoli Storage Manager API

14.1.4 Linux clients for Tivoli Storage Manager V5.4

The Tivoli Storage Manager V5.4 client on Linux is supported at:

- Linux for x86/86_64 backup-archive client
  - Red Hat Enterprise Linux 4 (AS,WS,ES)
  - Red Hat Enterprise Linux 5 from V5.4.1
  - SLES 9 and 10
  - Asianux 2.0
  - Novell OES
  - Java JRE 1.4.1 or later
  - Client capabilities:
    - Administrative Client CLI
    - Backup-archive CLI
    - Backup-archive Java Graphical User Interface (Java GUI)
    - Backup-archive Web Client Interface
    - Tivoli Storage Manager API
- Linux for x86/86_64 HSM client
  - Red Hat Enterprise Linux 4
  - SLES 9 and 10
  - File system - GPFS V2.3 PTF 11 (2.3.0.11), or later PTF, or V3.1 PTF 8 (3.1.0.8), or later PTF
  - Java JRE 1.4.1 or later
  - Client capabilities
    - HSM Client CLI
    - HSM Java GUI
- Linux for POWER backup-archive client
  - SLES 9 and 10
  - Red Hat Enterprise Linux 4 (AS,WS,ES)
  - Red Hat Enterprise Linux 5 from V5.4.1
  - Java JRE 1.4.1+ or 1.5
  - Client capabilities
    - Administrative Client CLI

        - Backup-archive CLI
        - Backup-archive Java Graphical User Interface (Java GUI)
        - Backup-archive Web Client Interface
        - Tivoli Storage Manager API
- Linux for IBM System z backup-archive client
    - SLES 9 and 10 for System z
    - Red Hat Enterprise Linux 4 (AS,WS,ES)
    - Red Hat Enterprise Linux 5 from V5.4.1
    - Java JRE 1.4.1 or later
    - Client capabilities
        - Administrative Client CLI
        - Backup-archive CLI
        - Backup-archive Web Client Interface
        - Tivoli Storage Manager API

14.1.5 Novell NetWare backup-archive client for Tivoli Storage Manager V5.4

The Tivoli Storage Manager V5.4 client on Novell NetWare is supported at:

- Novell NetWare 6.5 SP5+ (OES SP2)
- Client capabilities
    - Backup-archive CLI
    - Backup-archive Web Client Interface
    - Tivoli Storage Manager API

14.1.6 OS/400 API client for Tivoli Storage Manager V5.4

The Tivoli Storage Manager V5.4 API client on OS/400 is supported at:

- OS/400 i5/OS V5R3 or i5/OS V5R4
- Client capabilities: Tivoli Storage Manager API

14.1.7 Solaris clients for Tivoli Storage Manager V5.4

The Tivoli Storage Manager V5.4 client on Solaris is supported at:

- A Solaris SPARC backup-archive client
    - Solaris 9 (32 bit or 64 bit)
    - Solaris 10 (32 bit or 64 bit)
    - JRE 1.4.1 or later
    - Client capabilities
        - Administrative Client CLI
        - Backup-archive CLI
        - Backup-archive Java Graphical User Interface (Java GUI)
        - Backup-archive Web Client Interface
        - Tivoli Storage Manager API

        - X/Open API (32 bit)
- Solaris SPARC HSM client
    - Solaris 9 (32 bit or 64 bit)
    - Solaris 10 (32 bit or 64 bit)
    - VERITAS File System (VxFS) 4.1
    - Java JRE 1.4.1 or later
    - Client capabilities
        - HSM Client CLI
        - HSM Java GUI
- Solaris X86/X86_64 backup-archive client
    - Solaris 10 (32 bit or 64 bit)
    - JRE 1.4.1 or higher
    - Client capabilities
        - Administrative Client CLI
        - Backup-archive CLI
        - Backup-archive Java Graphical User Interface (Java GUI)
        - Backup-archive Web Client Interface
        - Tivoli Storage Manager API

14.1.8 Windows backup-archive client for Tivoli Storage Manager V5.4

The Tivoli Storage Manager V5.4 client on Microsoft Windows is supported at:

- Windows XP Professional (32 bit and 64 bit, SP 2, or later)
- Windows Server 2003 Server, Web server, Enterprise Server, Datacenter, and Storage Server (32 bit and 64 bit as appropriate)
- Windows Server 2003 Server R2, Enterprise Server R2, Datacenter R2, and Storage Server R2 (x32 and x64 as appropriate, toleration only)
- Windows Vista
- Citrix Presentation Server for Windows 2003 (32 bit)
- Windows Pre-installation Environments (Windows PE, 32 bit only) for recovery scenarios
- Client capabilities
    - Administrative Client CLI
    - Backup-archive CLI
    - Backup-archive GUI
    - Backup-archive Web Client Interface
    - Tivoli Storage Manager API
    - ODBC (32 bit mode applications only)

> **Note:** Windows 2000 is supported by the Tivoli Storage Manager V5.3 client.
>
> Only 64-bit clients can run on 64-bit machines.

14.1.9 z/OS UNIX System Services, Tivoli Storage Manager V5.4

The Tivoli Storage Manager V5.4 client on z/OS UNIX System Services is supported at client and API:

- z/OS V1R7 or z/OS V1R8
- Restrictions - Tivoli Storage Manager server functions are not included in this client:
  - SQLDB: Certain SQL select statements using the path for the files backed up by a z/OS UNIX System Services client might not work properly.
  - Server command 'query content'.
  - Cross client restore.
- Client capabilities
  - Administrative Client CLI
  - Backup-archive CLI
  - Backup-archive Web Client Interface
  - Tivoli Storage Manager API

14.1.10 IBM Tivoli Storage Manager HSM for Windows V5.4

Tivoli Storage Manager HSM for Windows is further described in Chapter 16, “HSM for Windows V5.4” on page 205:

- Any of the following Windows versions that support NTFS V5
  - Windows 2003 Server
  - Windows 2003 Server R2 (32 bit)
  - Windows 2003 Enterprise Server (32 bit)
  - Windows 2003 Enterprise Server R2 (32 bit)
- Tivoli Storage Manager V5.4 Windows backup-archive client
- Tivoli Storage Manager Windows Client API V5.4

14.1.11 NDMP requirements

Tivoli Storage Manager Extended Edition includes support for NDMP-controlled backup and restore operations. This is further described in Chapter 10, “NDMP” on page 133. The requirements are:

- A Tivoli Storage Manager Extended Edition server on Windows Server 2003, AIX 64 bit, Solaris 64 bit, HP 64 bit, or Linux.
- NDMP is supported on all the operating systems that are supported by the Tivoli Storage Manager Extended Edition server except for the z/OS operating system.
- A Tivoli Storage Manager Extended Edition supported backup-archive client on Windows, Solaris SPARC (32 bit or 64 bit), or AIX (32 bit or 64 bit) can be used for initiating backup and restore operations.

14.2 Additional client functionality

Some of these added functionalities are further described in individual chapters.

14.2.1 Windows client V5.4 additional functionality

These are the major new functions and enhancements to the Windows client.

Windows Vista support

Tivoli Storage Manager V5.4 provides backup and restore support for Microsoft Windows Vista similar to what is available to Windows XP and Windows 2003. The Vista V5.4 or V5.5 client does not (at the time of writing) support automatic system recovery backup and restore. Table 14-1 shows the features supported.

Table 14-1 Supported features on WIndows Vista

Feature	Vista 32 bit	Vista 64-bit x64
Journal-based backup	Yes	Yes
Online image backup	Yes	Yes
Offline image backup	Yes	Yes
System state support with Volume Shadowcopy Services (VSS)	Yes	Yes
Open file support (OFS)	Yes	Yes
LAN-free operations	No	No
Automated system recovery (ASR)	No	No

VMware consolidated backup

The Tivoli Storage Manager backup-archive client for Windows can be used in conjunction with VMware's integration module for VMware consolidated backup. Consolidated backup enables off-host backup of virtual machines, eliminating backup load from the ESX Server, accelerating backups, and shortening backup windows.

For more details, see Chapter 24, “VMware consolidated backup with Tivoli Storage Manager V5.5” on page 325.

14.2.2 UNIX client in a cluster

The CLUSTERNODE=yes parameter is no longer required to provide failover support and correct encryption for the stored password for the UNIX backup-archive client in a clustered environment. Note that the CLUSTERNODE parameter is still required when using Windows clustering. For more details see:

http://publib.boulder.ibm.com/infocenter/tivihelp/v1r1/topic/com.ibm.itsmfdt.doc/ans50000515.htm#clucfg

For information about requirements to migrate an existing cluster environment to the 5.4 or later client, see:

http://publib.boulder.ibm.com/infocenter/tivihelp/v1r1/topic/com.ibm.itsmfdt.doc/ans50000518.htm#migleg

14.2.3 Linux Logical Volume Manager 2 (LVM2)

The Tivoli Storage Manager Linux client supports LVM2 for image backup. LVM2 refers to a new userspace toolset that provides logical volume management facilities on Linux. The image backup function with LVM1 is available with older releases of Tivoli Storage Manager. Tivoli Storage Manager V5.4 only supports image backup with LVM2.

14.2.4 Macintosh OS X client V5.4 updates

The Tivoli Storage Manager client for Macintosh now supports Macintosh OS X on both PPC and Intel. The enhancements to the Macintosh OS X client include:

- Universal binary support - You can now install and use Tivoli Storage Manager on both PPC and Intel-based Macintosh systems.
- Option file and error log names - The Macintosh client has been changed to use the same option file and error log names as the other Tivoli Storage Manager clients. The Tivoli Storage Manager User Preferences file is now the dsm.opt file and the Tivoli Storage Manager System Preferences file is now the dsm.sys file. During installation, the previous option files are renamed.
- Support for the Web interface - The Macintosh client now supports the Web interface for remote backup and restore capability.

14.2.5 NetWare NSS support on Open Enterprise Linux

The Tivoli Storage Manager Linux x86 client supports the backup and restore of the Novell Storage Services (NSS) File System on Open Enterprise Server (OES).

This includes the backup and restore of the extended attributes, including access control lists (ACLs). The support for extended attributes includes support of file systems that implement POSIX ACLs using extended attributes. The file systems that now have extended attribute support include Linux file systems ReiserFS, ext2, ext3, and XFS.

14.2.6 Clients not migrated to V5.4

The following operating system versions, supported in V5.3, do not have a V5.4 client available. The V5.3 clients for these operating systems can be used with V5.4 Tivoli Storage Manager servers for as long as V5.3 is supported:

- Macintosh 10.3
- Red Hat Enterprise Linux 3
- SLES 8
- Red Flag 4.1
- NetWare 5.1
- Solaris 8
- OS/400 V5R2 (API client)
- z/OS V1R4, V1R5, and V1R6
- Windows 2000
- AIX V5.1
- AIX JFS HSM

15

Backup-archive client memory management

Tivoli Storage Manager V5.4 provides a new method in the backup-archive client for executing progressive incremental backups. This new method reduces the amount of virtual memory used by the Tivoli Storage Manager backup-archive client process and makes it possible to back up much larger file systems as defined by the number of files and directories in that file system. This chapter discusses details of the changes to memory management, which are applicable to all the Tivoli Storage Manager backup-archive clients.

15.1 Memory management for progressive incremental backup

The number of files being created in a single directory or within a single file system continues to grow in real application environments. The Tivoli Storage Manager backup-archive client has been changed to better cope with the very large numbers of directory and file system entries.

The following memory management options are available for progressive incremental backup. The MEMORYEFFICIENT option can be put in the client options file (dsm.opt), in the client system options file in a server stanza (dsm.sys), or specified as a command-line parameter:

- MEMORYEFFICIENT=NO (default)
  - One server query
  - Requires most memory
- MEMORYEFFICIENT=YES
  - One server query per directory
  - Reduces memory requirements
- MEMORYEFFICIENT=DISKCACHEMETHOD (new)
  - One server query
  - Using local database instead of memory

Before going into the details of the new management option, let us look at some relevant information about what happens during progressive incremental backups.

Each time a progressive incremental backup is run, the local client node is checked for files that have been added, modified, or deleted since the last backup. Then a decision is made to either back up, expire, or update the file.

For a progressive incremental backup, three lists are built in client memory, as shown in Figure 15-1 on page 194:

- A list of the active objects known to the Tivoli Storage Manager server
- A list containing objects on the client disk
- The objects that are to be expired, updated, or backed up

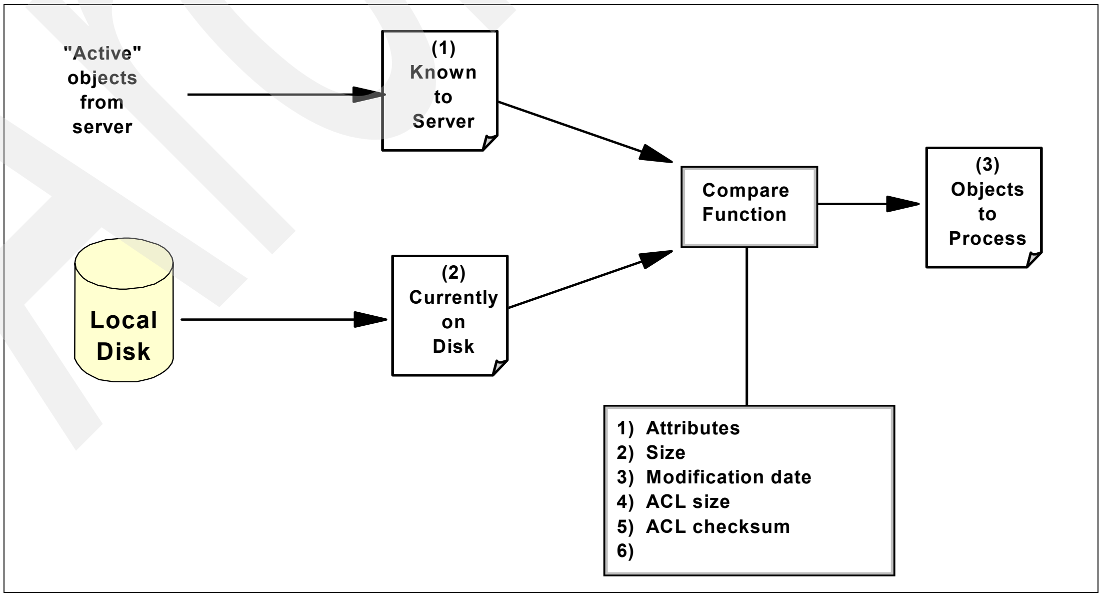


Figure 15-1 Progressive incremental backup: in memory lists

15.1.1 MEMORYEFFICIENT=NO

Using the default MEMORYEFFICIENT=NO option, the client only sends a single query to the Tivoli Storage Manager server to retrieve the list of known active objects. This is the preferred method, as the server can optimize the queries against the database. However, it requires the client to store the entire list in its memory for further processing. This can result in out-of-memory conditions on memory-constrained clients or if there is a very large number of objects to process, as shown in Example 15-3.

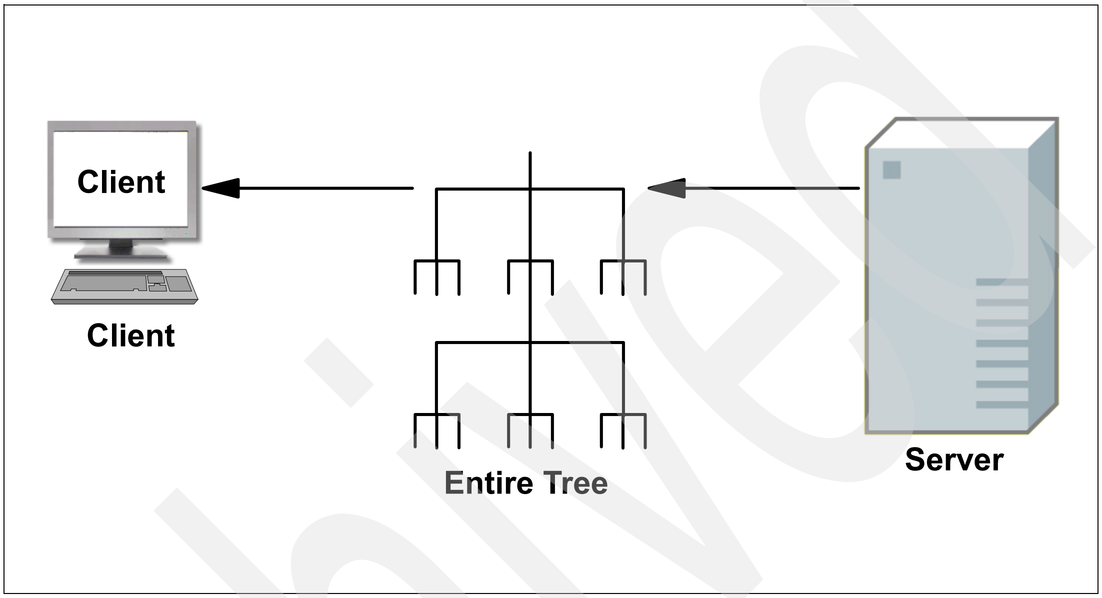


Figure 15-2 Incremental backup: MEMORYEFFICIENT=NO

15.1.2 MEMORYEFFICIENT=YES

With MEMORYEFFICIENT=YES, a query for known active objects is issued to the Tivoli Storage Manager server for each single directory. This results in less memory being used on the client, at the expense of more database queries issued against the server. From the server’s database perspective, it is much more efficient to handle one query compared to several smaller ones, as with this option. However, for a client with many directories, this reduces memory utilization.

A situation in which this option is not effective is when there are a very large number of entries within a single directory. Also, even if many directory entries are already stored on the Tivoli Storage Manager server, this option does not diminish the necessity to build the initial directory list in client memory.

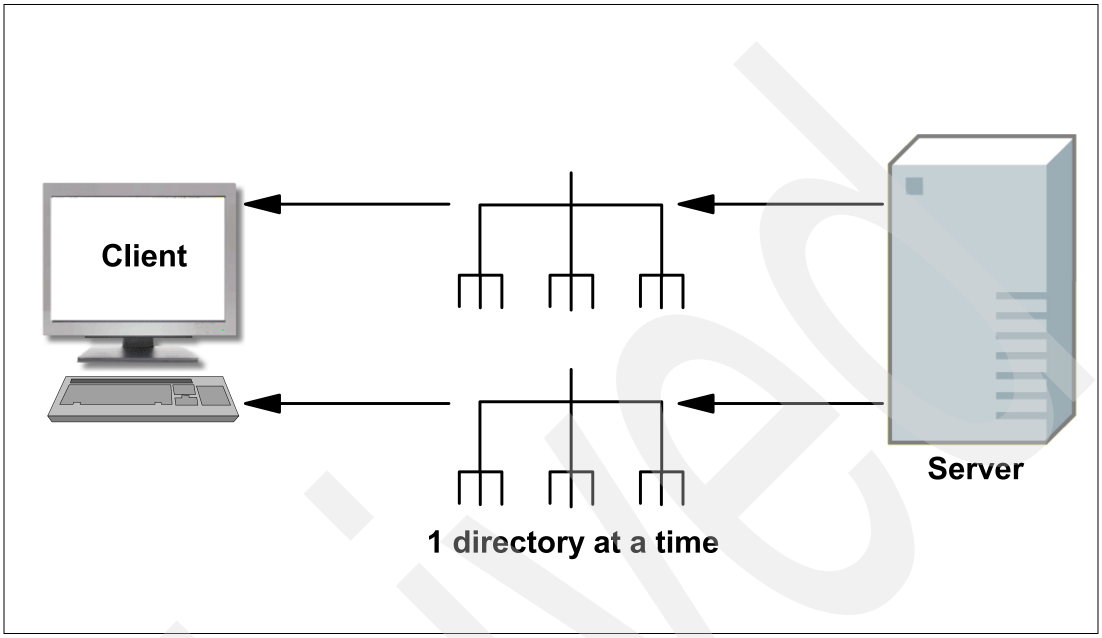


Figure 15-3 Incremental backup: MEMORYEFFICIENT=YES

15.1.3 MEMORYEFFICIENT=DISKCACHEMETHOD

The Tivoli Storage Manager V5.4 client provides an option, MEMORYEFFICIENT=DISKCACHEMETHOD, which can significantly reduce the memory requirements during a full file system incremental backup command by creating a disk cache file on the Tivoli Storage Manager client machine. The option has been introduced as a third possibility for the MEMORYEFFICIENT parameter. You can set it globally in the appropriate client option file, or for individual filespaces by using the INCLUDE.FS option, as shown with Example 15-1. For supported methods for specifying this option, see the client manual for your client node's operating system.

Example 15-1 INCLUDE.FS with DISKCACHEMETHOD parameter

```
DOMAIN C: E:
include.fs c: memoryefficient=diskcachemethod diskcachelocation=e:\tsmdiskcache
include.fs e: memoryefficient=diskcachemethod diskcachelocation=c:\tsmdiskcache
```

A general guideline for when to use this option is when a filespace cannot be processed by existing methods due to *out of memory* messages during incremental processing of a full filespace. In this case you would see a message like: `ANS1030E The operating system refused a Tivoli Storage Manager request for memory allocation`, as shown in Example 15-3 on page 199.

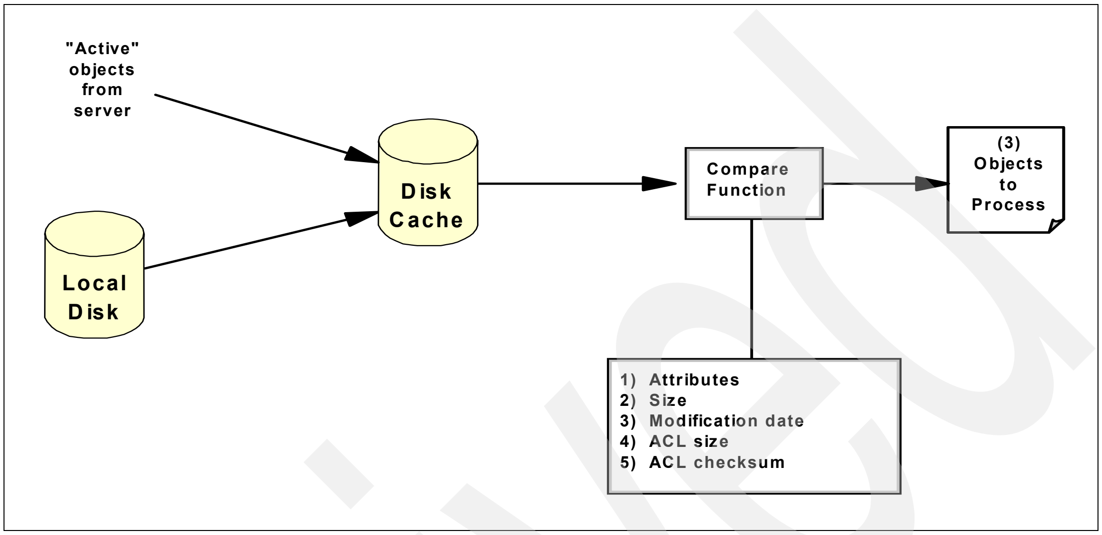


Figure 15-4 Incremental backup: MEMORYEFFICIENT=DISKCACHEMETHOD

When this option is specified, a local cache database (requiring local disk space on the client node) is used to store the active items known to the Tivoli Storage Manager server. The Tivoli Storage Manager client uses the database when scanning the local file system to process an incremental backup of a filespace.

As with MEMORYEFFICIENT=NO, the client issues a single query to the server for all active objects in the Tivoli Storage Managers server filespace. The responses are used to populate the local cache database by using the name of the object for the key and the server attributes of the object for the data.

Once all server responses have been received, the client builds a list of directories in memory, and traverses through all branches finding files and directories. For each object found, the cache database is queried for the corresponding server version. If the object is not found in the database it is immediately added to the objects to be backed up. If the object is found in the database, the cache database record is updated to indicate that the file was found on the client. The client then checks the object's attributes and, if necessary, it adds the file to the list of objects to be either backed up or updated.

After the local objects have been processed, the cache database is queried to find the objects that were not found on the client file system. The query returns all objects found in the cache database, and the objects that were not already processed will be reported to the server as deleted. Once this is complete, the disk cache file is deleted.

Figure 15-5 on page 198 compares the processes involved using MEMORYEFFICIENT=NO and MEMORYEFFICIENT=DISKCACHE.

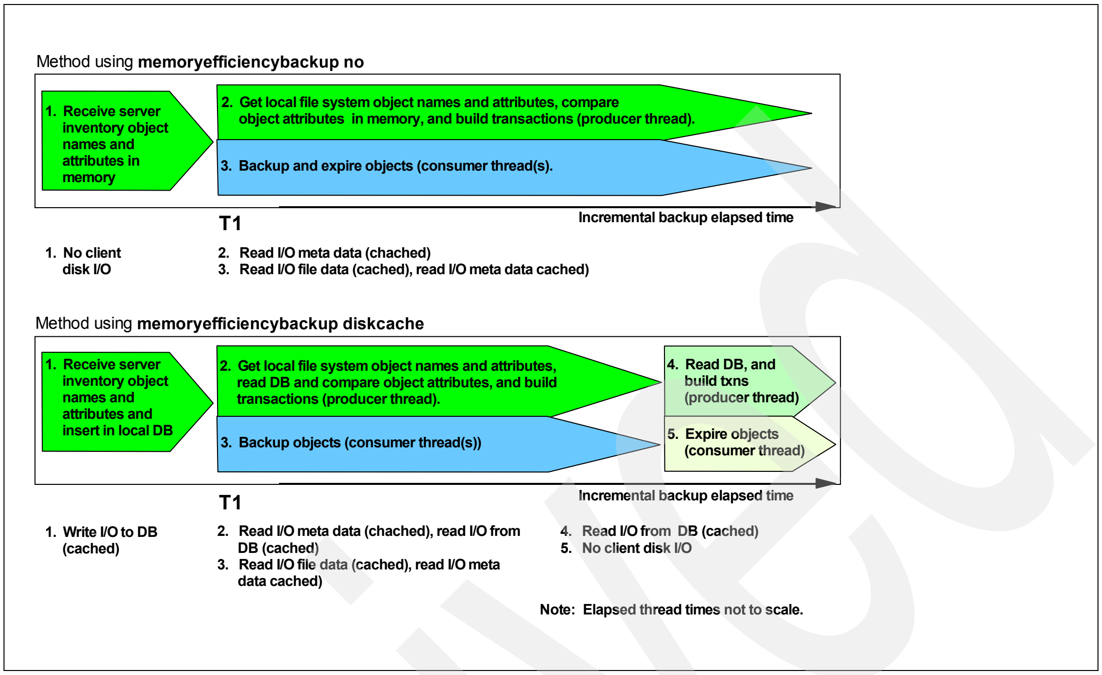

Method using **memoryefficiencybackup no**
1. Receive server inventory object names and attributes in memory
2. Get local file system object names and attributes, compare object attributes in memory, and build transactions (producer thread).
3. Backup and expire objects (consumer thread(s).
T1
Incremental backup elapsed time
1. No client disk I/O
2. Read I/O meta data (chached)
3. Read I/O file data (cached), read I/O meta data cached)
Method using **memoryefficiencybackup diskcache**
1. Receive server inventory object names and attributes and insert in local DB
2. Get local file system object names and attributes, read DB and compare object attributes, and build transactions (producer thread).
3. Backup objects (consumer thread(s))
4. Read DB, and build txns (producer thread)
5. Expire objects (consumer thread)
T1
Incremental backup elapsed time
1. Write I/O to DB (cached)
2. Read I/O meta data (chached), read I/O from DB (cached)
3. Read I/O file data (cached), read I/O meta data cached)
4. Read I/O from DB (cached)
5. No client disk I/O
Note: Elapsed thread times not to scale.

Figure 15-5 Process comparison: MEMORYEFFICIENT=NO versus DISKCACHEMETHOD

Configuring the DISKCACHELOCATION

When using DISKCACHEMETHOD, the time to determine which objects need to be processed is mostly affected by performance of the client's processor and disk. To improve processor performance, you can replace slower processors by faster ones or install additional processors, which is outside the control of Tivoli Storage Manager.

The client provides a DISKCACHELOCATION option, which can be specified in either dsm.opt (Windows) or dsm.sys (UNIX/Linux/Mac). The syntax is:

```
DISKCACHELOCATION <path>
```

If you do not specify a DISKCACHELOCATION, by default, the cache database is written to the root of the same volume as the data being backed up. To reduce I/O contention, we recommend locating the disk cache file on a disk volume separate from the client data. You can do this on a file system level via the INCLUDE.FS statement.

Consider that with the current implementation, an entry in the cache database occupies about 2 KB of disk space. This results in a database size between 2 GB and 4 GB for 1,000,000 files, depending on the randomness of the keys. Make sure there is enough disk space available on the volume and path specified by DISKCACHELOCATION.

Note: Use local disk for the disk cache. Do not locate the disk cache file on a remote disk such as a network share or NFS mounted volume. The additional I/O delay will significantly degrade incremental backup elapsed time.

For detailed recommendations see "Optimizing TSM Client Incremental Backup Performance when using the Disk Cache Method" at:

http://www-1.ibm.com/support/docview.wss?&uid=swg21254744

15.1.4 Using the DISKCACHEMETHOD option

Here we provide a small implementation example of the MEMORYEFFICIENT=DISKCACHEMETHOD option. To do so, we created a client node with a large number of files (over eight million). We define a DOMAIN statement to include only that volume, in this case the E: drive.

Note that this is a simple test only, designed to show the functionality. It is not designed to demonstrate real performance numbers.

1. The initial backup of the directory and its volume is not a problem, as the server does not yet have any information about the volume. Therefore, every object found needs to be sent to the server, as shown in Example 15-2.

Example 15-2 First backup, creating filespace on the server

```
C:\Tivoli\TSM\baclient>dsmc incr -optfile=node1.opt
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 5, Level 0.0
  Client date/time: 12/04/2007 07:36:59
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.

Node Name: NODE1
Session established with server HAGGIS: Windows
  Server Version 5, Release 5, Level 0.0
  Server date/time: 12/04/2007 07:37:00  Last access: 12/03/2007 20:44:35



Incremental backup of volume '\\lochnese\e$'
Successful incremental backup of '\\lochnese\e$'



Total number of objects inspected: 8,224,440
Total number of objects backed up: 8,224,440
Total number of objects updated:          0
Total number of objects rebound:          0
Total number of objects deleted:          0
Total number of objects expired:          0
Total number of objects failed:           0
Total number of subfile objects:          0
Total number of bytes transferred:   21.39 GB
Data transfer time:                  228.73 sec
Network data transfer rate:        98,071.80 KB/sec
Aggregate data transfer rate:        870.28 KB/sec
Objects compressed by:                    0%
Subfile objects reduced by:               0%
Elapsed processing time:           07:09:35
```

2. We run an incremental backup with the default setting of MEMORYEFFICIENT=NO. Example 15-3 shows how we fail with the unpopular ANS1030E message.

Example 15-3 ANS1030E on backup of large file system

```
C:\Tivoli\TSM\baclient>dsmc i -optfile=node1.opt
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
```

```
  Client Version 5, Release 5, Level 0.0
  Client date/time: 12/04/2007 15:26:38
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.

Node Name: NODE1
Session established with server HAGGIS: Windows
  Server Version 5, Release 5, Level 0.0
  Server date/time: 12/04/2007 15:26:38  Last access: 12/04/2007 07:37:05


Incremental backup of volume '\\lochnese\e$'

Total number of objects inspected:        1
Total number of objects backed up:        0
Total number of objects updated:          0
Total number of objects rebound:          0
Total number of objects deleted:          0
Total number of objects expired:          0
Total number of objects failed:           0
Total number of subfile objects:          0
Total number of bytes transferred:       0  B
Data transfer time:                    0.00 sec
Network data transfer rate:            0.00 KB/sec
Aggregate data transfer rate:          0.00 KB/sec
Objects compressed by:                    0%
Subfile objects reduced by:               0%
Elapsed processing time:           00:05:50
ANS1030E The operating system refused a TSM request for memory allocation.
```

3. Tracking the session on the Tivoli Storage Manager server via the QUERY SESSION command, we know that this happened after sending about 2.2 GB worth of metadata to the client in the server's list of objects available. Example 15-4 shows the command output right after the metadata has been sent to the client's producer thread.

Example 15-4   QUERY SESSION for backup session

```
tsm: HAGGIS>q se 34

  Sess Comm.  Sess     Wait   Bytes   Bytes Sess  Platform Client Name
Number Method State    Time    Sent   Recvd Type
------ ------ ------ ------ ------- ------- ----- -------- -------------------
    34 Tcp/Ip    Run    0 S   2.2 G     559  Node    WinNT NODE1
```

4. Before using the new DISKCACHEMETHOD option we first do a backup with the MEMORYEFFICIENT=YES option as a comparison. In Example 15-5, we specify the option as a command line parameter.

Example 15-5   Subsequent backup, MEMORYEFFICIENT=YES

```
C:\Tivoli\TSM\baclient>dsmc i -optfile=node1.opt -memoryefficient=yes
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 5, Level 0.0
  Client date/time: 12/04/2007 16:11:22
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.

Node Name: NODE1
```

```
Session established with server HAGGIS: Windows
  Server Version 5, Release 5, Level 0.0
  Server date/time: 12/04/2007 16:11:22  Last access: 12/04/2007 15:26:38


Incremental backup of volume '\\lochnese\e$'
Successful incremental backup of '\\lochnese\e$'


Total number of objects inspected: 8,224,440
Total number of objects backed up:       0
Total number of objects updated:         0
Total number of objects rebound:         0
Total number of objects deleted:         0
Total number of objects expired:         0
Total number of objects failed:          0
Total number of subfile objects:         0
Total number of bytes transferred:       0 KB
Data transfer time:                   0.00 sec
Network data transfer rate:           0.00 KB/sec
Aggregate data transfer rate:         0.00 KB/sec
Objects compressed by:                   0%
Subfile objects reduced by:              0%
Elapsed processing time:          01:57:29
```

Keep in mind that even this backup would fail if you were backing up a filespace with so many files in a single directory that the client cannot allocate enough memory for the lists to process. With our test setup, the client was using up to 234 MB, as shown in Figure 15-6 on page 201 This number can widely vary depending on the number of files in a single directory.

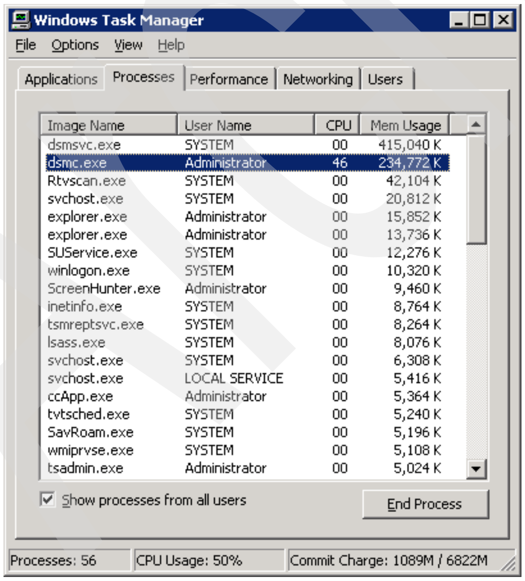


Image Name	User Name	CPU	Mem Usage
dsmsvc.exe	SYSTEM	00	415,040 K
dsmc.exe	Administrator	46	234,772 K
Rtvscan.exe	SYSTEM	00	42,104 K
svchost.exe	SYSTEM	00	20,812 K
explorer.exe	Administrator	00	15,852 K
explorer.exe	Administrator	00	13,736 K
SUService.exe	SYSTEM	00	12,276 K
winlogon.exe	SYSTEM	00	10,320 K
ScreenHunter.exe	Administrator	00	9,460 K
inetinfo.exe	SYSTEM	00	8,764 K
tsmreptsvc.exe	SYSTEM	00	8,264 K
lsass.exe	SYSTEM	00	8,076 K
svchost.exe	SYSTEM	00	6,308 K
svchost.exe	LOCAL SERVICE	00	5,416 K
ccApp.exe	Administrator	00	5,364 K
tvtsched.exe	SYSTEM	00	5,240 K
SavRoam.exe	SYSTEM	00	5,196 K
wmiprvse.exe	SYSTEM	00	5,108 K
tsadmin.exe	Administrator	00	5,024 K

☑ Show processes from all users

Processes: 56 CPU Usage: 50% Commit Charge: 1089M / 6822M

Figure 15-6 MEMORYEFFICIENT=YES, memory usage

5. Now we run the same backup with MEMORYEFFICIENT=DISKCACHEMETHOD specified as a command line parameter, as shown in Example 15-6. We also modified the options file to specify DISKCACHELOCATION C:\TSMDISKCACHE, since our source data is on drive E. This minimizes the effect of disk I/O contention.

Example 15-6 Subsequent backup: MEMORYEFFICIENT=DISKCACHEMETHOD

```
C:\Tivoli\TSM\baclient>dsmc i -optfile=node1.opt -memoryefficient=diskcachemethod
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 5, Level 0.0
  Client date/time: 12/04/2007 19:30:45
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.

Node Name: NODE1
Session established with server HAGGIS: Windows
  Server Version 5, Release 5, Level 0.0
  Server date/time: 12/04/2007 19:30:45  Last access: 12/04/2007 18:08:50


Incremental backup of volume '\\lochnese\e$'
Using disk caching for backup of filespace \\lochnese\e$
Successful incremental backup of '\\lochnese\e$'


Total number of objects inspected: 8,224,440
Total number of objects backed up:        0
Total number of objects updated:          0
Total number of objects rebound:          0
Total number of objects deleted:          0
Total number of objects expired:          0
Total number of objects failed:           0
Total number of subfile objects:          0
Total number of bytes transferred:       0  B
Data transfer time:                    0.00 sec
Network data transfer rate:            0.00 KB/sec
Aggregate data transfer rate:          0.00 KB/sec
Objects compressed by:                    0%
Subfile objects reduced by:               0%
Elapsed processing time:           02:28:11
```

While running this backup, the client never used more than 15 MB of memory, therefore saving memory for other running applications. Compare this with the 234 MB we were using with MEMORYEFFICENT=YES as documented above. With the DISKCACHEMETHOD option, even with very large numbers of files in a single file system, the client would not run into the ANS1030E condition. You can use the option to successfully initialize a journal database that otherwise would fail because of the out-of-memory condition.

Once the backup was complete, we checked the cache database. Example 15-7 shows that we are using 11 GB of disk space for the cache database.

Example 15-7 Cache database

```
>dir c:\tsmdiskcache\.TsmCacheDir
 Volume in drive C has no label.
 Volume Serial Number is DCDC-8C9E
 Directory of c:\tsmdiskcache\.TsmCacheDir

12/04/2007  07:30 PM    <DIR>          .
12/04/2007  07:30 PM    <DIR>          ..
12/04/2007  09:58 PM    11,724,270,740 TsmCache__10803696.tsmDB
               1 File(s) 11,724,270,740 bytes
               2 Dir(s)  96,481,951,744 bytes free
```

The cache database is temporary and transitory in nature. The space allocated will be freed once the backup is complete. Since the file can become very large, make sure that large file support (> 2 GB) is enabled for the file system that you are using.

15.2 Summary

Using MEMORYEFFICIENT=DISKCACHEMETHOD allows you to set up progressive incremental backups on client nodes that are either memory constrained or that reach address boundaries for the operating system processing the number of files in a single file system.

The are only two configuration options required to enable this function:

- The MEMORYEFFICIENT option with the DISKCACHEMETHOD parameter
- The DISKCACHELOCATION option to define where to put the cache database

In general, using the disk cache method is expected to be slower than any of the memory resident methods. Remember that the purpose of this parameter is to reduce the amount of memory required. In some circumstances, you might find the disk cache method faster compared to the MEMORYEFFICIENT=YES option if your system starts paging because of memory allocated for object comparison.

16

HSM for Windows V5.4

This chapter describes the following enhancements to the Tivoli Storage Manager HSM for Windows client in V5.4:

- Backup integration - Backup before migrate
- Support of Microsoft cluster environments (MSCS)
- Recall quotas

Additional enhancements in the IBM Tivoli Storage Manager Hierarchical Storage Management client were released in V5.5. These are discussed in Chapter 23, “HSM for Windows V5.5” on page 311.

For more details about the installation and configuration of the HSM client refer to the *Tivoli Storage Manager HSM for Windows Administration Guide*, SC32-1733 and *Using the Tivoli Storage Manager HSM Client for Windows*, REDP-4126.

16.1 Hierarchical Storage Management

IBM Tivoli Storage Manager for HSM for Windows (referred to subsequently as the “HSM client”) provides Hierarchical Storage Management (HSM) services for Windows NTFS file systems under Windows 2003. Using the HSM client, individual files from directories or complete NTFS file systems can be migrated to remote storage in an IBM Tivoli Storage Manager server (any platform). The migration can be controlled by a policy that can include parameters like file size, age, or last access. If you use a policy, only files that match the policy rules are migrated.

The HSM client always supports one version below, the equal version or one version higher than the HSM client version with regards to the Tivoli Storage Manager server level. This is called n+/-1 support. As an example, an HSM client V5.4 is supported with a Tivoli Storage Manager server V5.3, V5.4, or V5.5.

The HSM client acts as a Tivoli Storage Manager client. It uses the Tivoli Storage Manager client’s archiving API. Migrated files from the HSM client are stored in native *archive storage pools* on the Tivoli Storage Manager server (defined with TYPE=ARCHIVE on the DEFINE COPYGROUP command), not in HSM pools (MIGDESTINATION on the DEFINE MGMTCLASS command), which are used only by the Tivoli Storage Manager for Space Management client (HSM for UNIX). We recommend setting the retention for the archive copy group that is used to NOLIMIT.

A migrated file leaves a small piece of the file (stub file) on the NTFS file system. Stub files contain the necessary metadata to recall the migrated files. The metadata information includes the Tivoli Storage Manager server (where the files are migrated to) and the file server (where the files are migrated from). A reparse point is attached to the stub file and builds the interface for HSM for Windows to the NTFS file system. A reparse point has a Microsoft registered reparse ID, which is world-wide unique. At any time that an application tries to access the content of a stub file (with an HSM client reparse point), the file system filter of the HSM client is informed about this and HSM can recall the file.

Attention: The host name, IP port, and server name of the Tivoli Storage Manager, as well as the host name of the file server, are included in the stub file. If you change any of these Tivoli Storage Manager server settings, or the host name of the file server, files previously migrated will not be able to be recalled.

Figure 16-1 on page 207 shows an HSM for Windows environment including the Tivoli Storage Manager server and client.

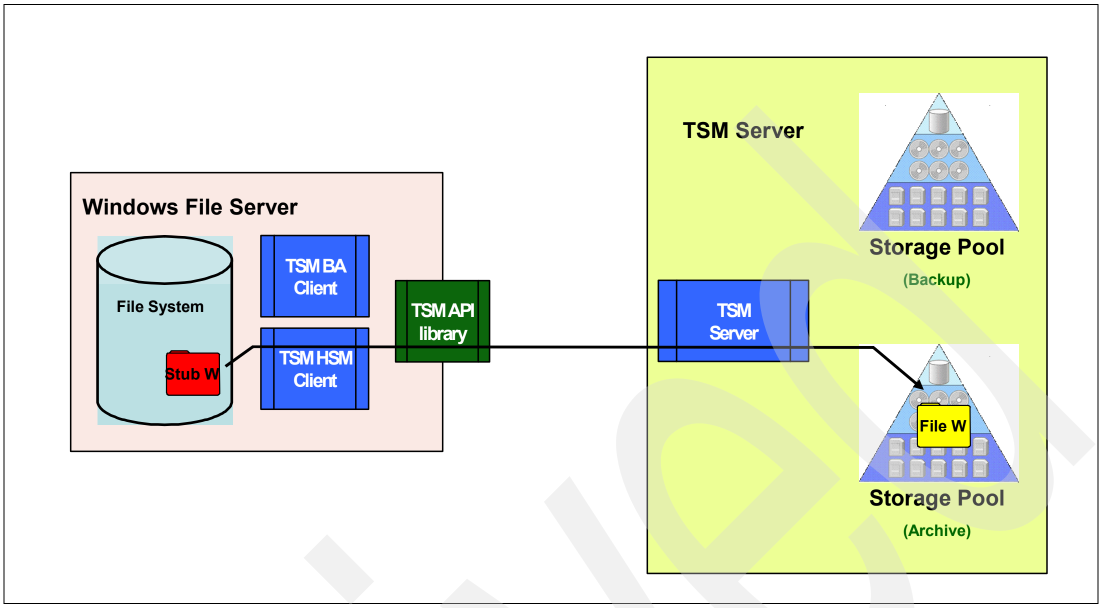


Figure 16-1 HSM environment

The migration of files is transparent to Windows users and applications. That is, Windows users can see and access migrated files like any other file that is present on the file system. The difference is that when a migrated file is opened, it will be transparently retrieved and copied back to the local Windows system. You can identify migrated files by the changed file icon (Figure 16-2) and the offline attribute that is set in Windows Explorer, as shown in Figure 16-3.

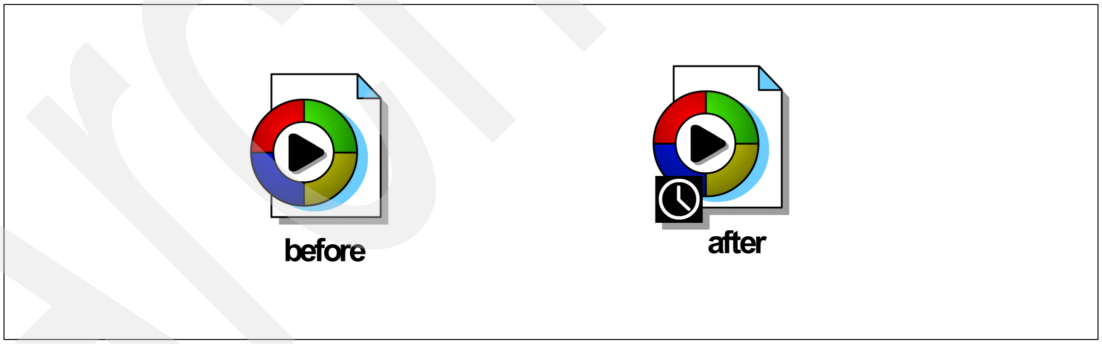
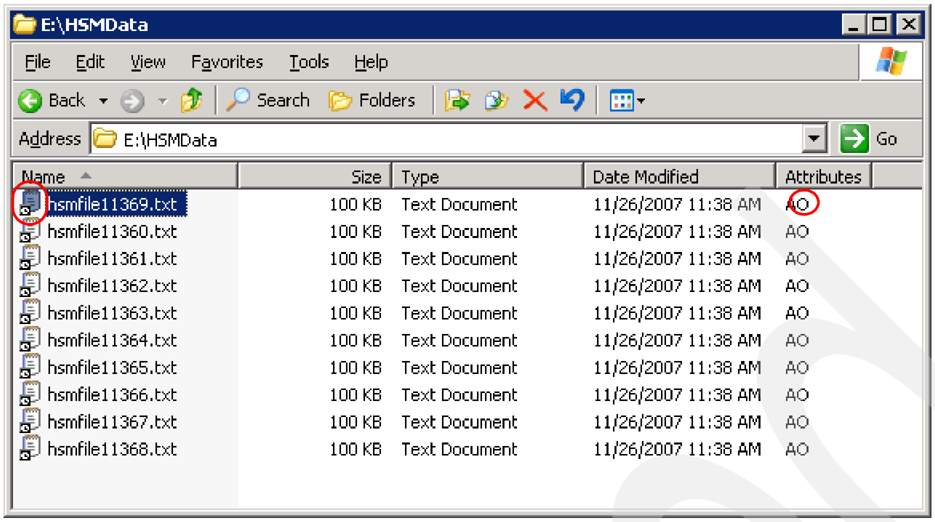


Figure 16-2 Different icons before and after migration

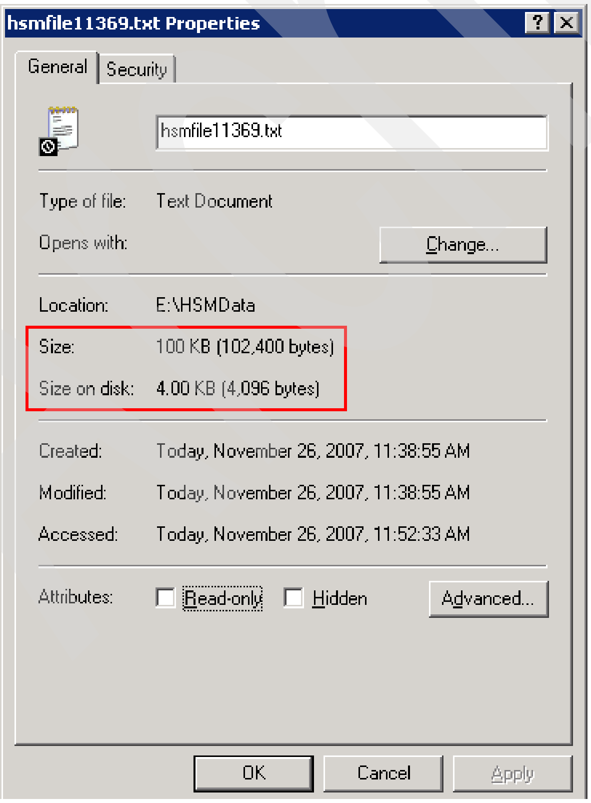


Name	Size	Type	Date Modified	Attributes
hsmfile11369.txt	100 KB	Text Document	11/26/2007 11:38 AM	AO
hsmfile11360.txt	100 KB	Text Document	11/26/2007 11:38 AM	AO
hsmfile11361.txt	100 KB	Text Document	11/26/2007 11:38 AM	AO
hsmfile11362.txt	100 KB	Text Document	11/26/2007 11:38 AM	AO
hsmfile11363.txt	100 KB	Text Document	11/26/2007 11:38 AM	AO
hsmfile11364.txt	100 KB	Text Document	11/26/2007 11:38 AM	AO
hsmfile11365.txt	100 KB	Text Document	11/26/2007 11:38 AM	AO
hsmfile11366.txt	100 KB	Text Document	11/26/2007 11:38 AM	AO
hsmfile11367.txt	100 KB	Text Document	11/26/2007 11:38 AM	AO
hsmfile11368.txt	100 KB	Text Document	11/26/2007 11:38 AM	AO

Figure 16-3 Migrated files with the HSM client

The changed file icon is also called an overlay icon, which the operating system puts over the existing icon to indicate the state of the file. Windows XP or Windows Server 2003 adds a clock to the icon. As shown in Figure 16-2, Windows Vista uses a cross (x) instead of a clock.

Figure 16-4 shows the file properties. The difference between the Size and Size on disk fields allows you to identify a migrated file. The Size field still shows the original file size, while the Size on disk field shows the actual file size of the stub file, which is one cluster of the disk. The cluster size is mostly 4 KB, but it can be larger, depending on the disk configuration.



hsmfile11369.txt

Type of file: Text Document

Opens with:

Location: E:\HSMData

Size: 100 KB (102,400 bytes)

Size on disk: 4.00 KB (4,096 bytes)

Created: Today, November 26, 2007, 11:38:55 AM

Modified: Today, November 26, 2007, 11:38:55 AM

Accessed: Today, November 26, 2007, 11:52:33 AM

Attributes: □ Read-only □ Hidden

Figure 16-4 Migrated file properties

When original files are replaced by stub files, the stub files themselves are backed up by the Tivoli Storage Manager backup-archive client when a full backup or an incremental backup is initiated, because the files have changed. They became stub files. Stub files are backed up again if the Tivoli Storage Manager server determines that the stub file has changed (for example, security attributes for the existing stub have changed).

You should review your actual backup policies when stub files are backed up, because the stub file may cause a new active version of the file on the Tivoli Storage Manager server. It may be necessary to increase the number of existing versions (VEREXISTS) for your backup policies depending on your requirements. We recommend keeping at least two deleted versions (VERDELETED) in your backup policies, one for the latest original file version (with the content) and another one for the version of the stub file.

The backup-archive client handles stub files differently with the enhanced backup integration provided with the HSM client V5.5 together with the backup-archive client V5.5. The enhanced integration ensures that the backup-archive client, independently of the HSM client, always maintains a copy of the complete file in the backup pool, whether this file is migrated or not. Each stub file always has an associated current copy of the complete file in the backup pool. The stub file and the complete file version are associated with each other and managed as a single version of the file in the Tivoli Storage Manager server. For more information about the enhanced backup integration, see 23.1, “Backup integration” on page 312.

16.2 HSM for Windows client installation

There are two steps to install the HSM client:

1. Install the software.
2. Customize with the configuration wizard.

We summarize the installation process here. For detailed information refer to *Tivoli Storage Manager HSM for Windows Administration Guide*, SC32-1733.

Install the software

The HSM client software can be installed in either user mode or network mode. In user mode you step through a series of installation windows to collect the necessary information and manage the installation. A network installation only copies the product to a network drive for a shared installation.

During installation, the file system filter driver is installed, which requires a reboot to load. You also need to reboot if you deinstall the software.

If you add new hard disks or volumes to a server already running the HSM client, the recall service (hsmservice.exe) running as a Windows service (IBM TSM HSM Recall Service) must be restarted.

Run the configuration wizard

After installing the software and rebooting, start the GUI to invoke the configuration wizard by selecting **Start** ∅ **Programs** ∅ **Tivoli Storage Manager** ∅ **HSM GUI**.

The configuration wizard helps you to configure your HSM client. You are prompted for the following:

- Create a new option file or use an existing one.

- TCP/IP address and port of the Tivoli Storage Manager server.
- Password access settings (generate or prompt).
- Node name that is used for the HSM client.
- Password for this node.
- Initial filespace that should be used for HSM. This filespace is created at the end of the configuration wizard. More filespaces can be created later in the GUI as well. The filespace creation can also be skipped at this point.
- Back up migratable files: Should files be backed up before a migration job is run? The default is yes. More information about this option is in 16.3, “Backup integration - backup before migrate” on page 210.
- Cluster configuration - This page appears only if a Microsoft Cluster Service (MSCS) on your machine is detected. See 16.4, “Microsoft cluster environments (MSCS)” on page 214.
- The last page of the wizard is the summary page, where you can review all entered information. After clicking **Finish**, the HSM client connects to the Tivoli Storage Manager server and opens the GUI where you can create the migration jobs.

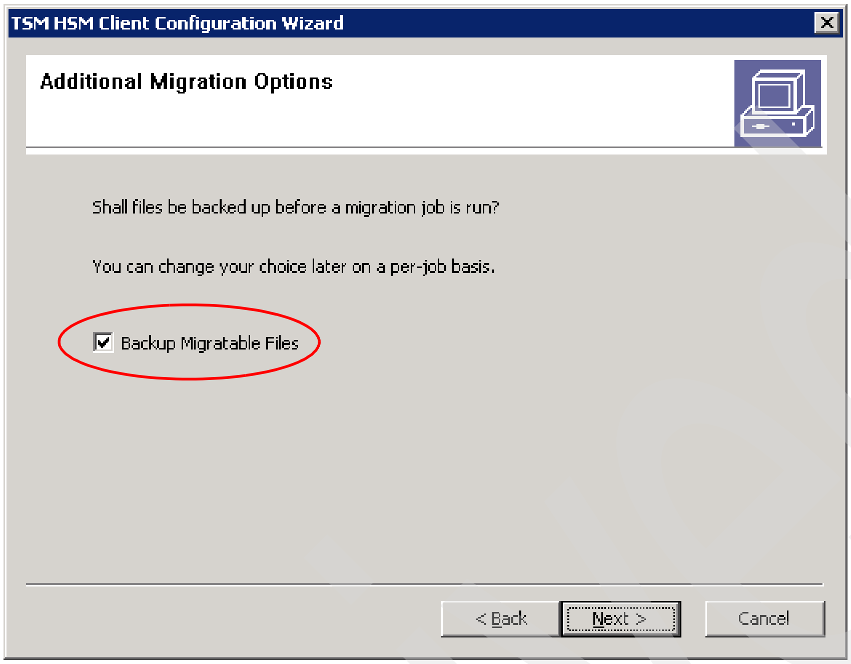
If necessary, you can start the configuration wizard again by selecting **Tools** ∅ **Configuration Wizard** in the HSM GUI.

Note: We recommend using at least one filespace per local volume to migrate files. Do not migrate files from several local volumes to one single filespace.

16.3 Backup integration - backup before migrate

The *backup before migrate* function allows you to invoke an incremental backup of a file with the Tivoli Storage Manager backup-archive client immediately before a file is migrated and stubbed. This helps ensure that the latest content of a file is also stored in your Tivoli Storage Manager backup environment before it is migrated within the HSM environment. The backup before migrate function backs up only resident files that would be migrated, not stub files.

With the HSM client V5.4 the backup before migrate function is enabled by default. You can change this with the configuration wizard, as shown in Figure 16-5.


TSM HSM Client Configuration Wizard
Additional Migration Options

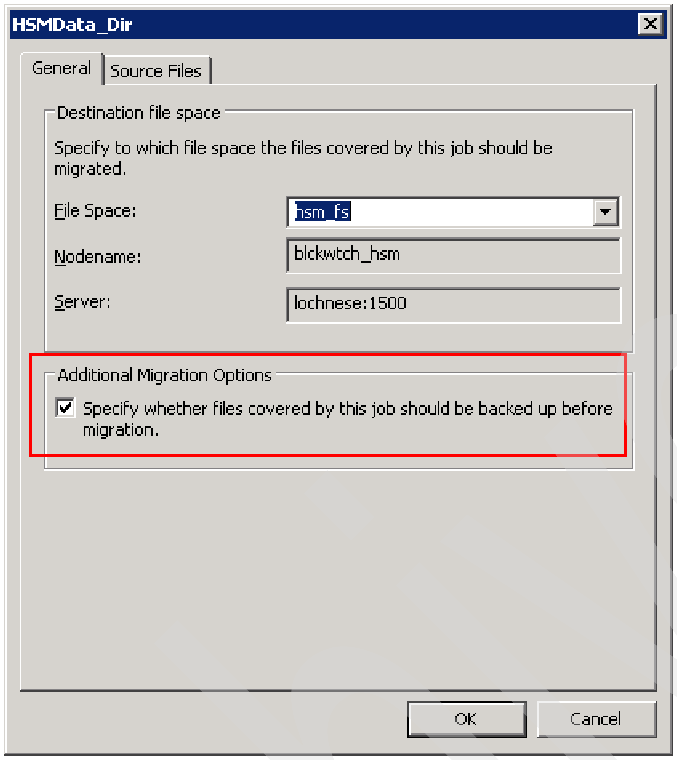
Shall files be backed up before a migration job is run?

You can change your choice later on a per-job basis.

☑ Backup Migratable Files

Figure 16-5 Backup before migrate dialogue during installation

As shown in Figure 16-6 on page 212, you can also enable or disable the backup before migration option for each migration job later on during the job definition. The initial selection you make with the configuration wizard will be automatically applied to each newly defined job, unless you override it.



Destination file space

Specify to which file space the files covered by this job should be migrated.

File Space: hsm_fs

Nodename: blckwtch_hsm

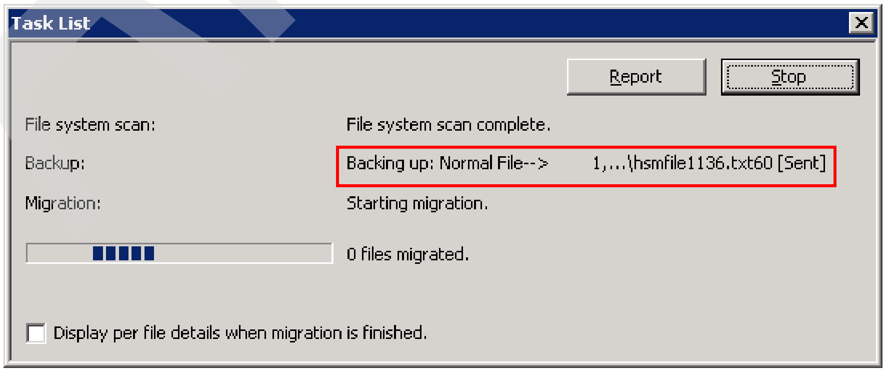
Server: lochnese:1500

Additional Migration Options

☑ Specify whether files covered by this job should be backed up before migration.

Figure 16-6 Backup before migration definition per-job basis

When the backup before migration option is selected for a job, the HSM client generates the input for the Tivoli Storage Manager backup-archive client based on the files selected for migration. The list of source files for the backup before migrate is written to a temporary backup filelist file in the TEMP directory of the HSM client. The file names of the files to back up are stored in the backup filelist file as absolute UNC path names. After a (non-empty) list of files has been successfully written to the backup filelist file, **dsmc** is executed as an external process, with the filelist pathfilename as argument. Figure 16-7 (taken from a V5.5 HSM client) shows how the HSM client displays the backup process while the migration job is running.



File system scan: File system scan complete.

Backup: Backing up: Normal File--> 1,...\hsmfile1136.txt60 [Sent]

Migration: Starting migration.

0 files migrated.

☐ Display per file details when migration is finished.

Figure 16-7 Backup before migrate is displayed during a migration job

When the backup completes successfully (**dsmc** operation), file migration is started. If the backup operation returns an error, the result depends on what interface is used for the HSM client.

- For the HSM for Windows command-line interface, **dsmclc** terminates.
- For the GUI, **dsmgui** displays a pop-up to notify you of the problem, and the migration terminates.

If the migration is terminated because of an error during the backup process, check the backup log (default C:\Program Files\Tivoli\TSM\hsmclient\logs) for error messages.

> **Tip:** You might see the message:
>
> ```
> ANS1009W An error occurred processing the operating system include/exclude
> statements. The error was detected while processing:
> HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBac
> kup\DRM. RC = 13.
> ```
>
> See `http://www-1.ibm.com/support/docview.wss?uid=swg21243837` for information and a workaround.

Further information about the backup before migration is in 16.4.4, “Backup before migrate in a cluster environment” on page 218.

16.4 Microsoft cluster environments (MSCS)

Tivoli Storage Manager for HSM for Windows V5.4 can be installed in a Microsoft cluster in both active-standby and active-active configurations. The software package and the installation of the HSM client is the same as in a non-clustered environment. Figure 16-8 shows a sample cluster environment.

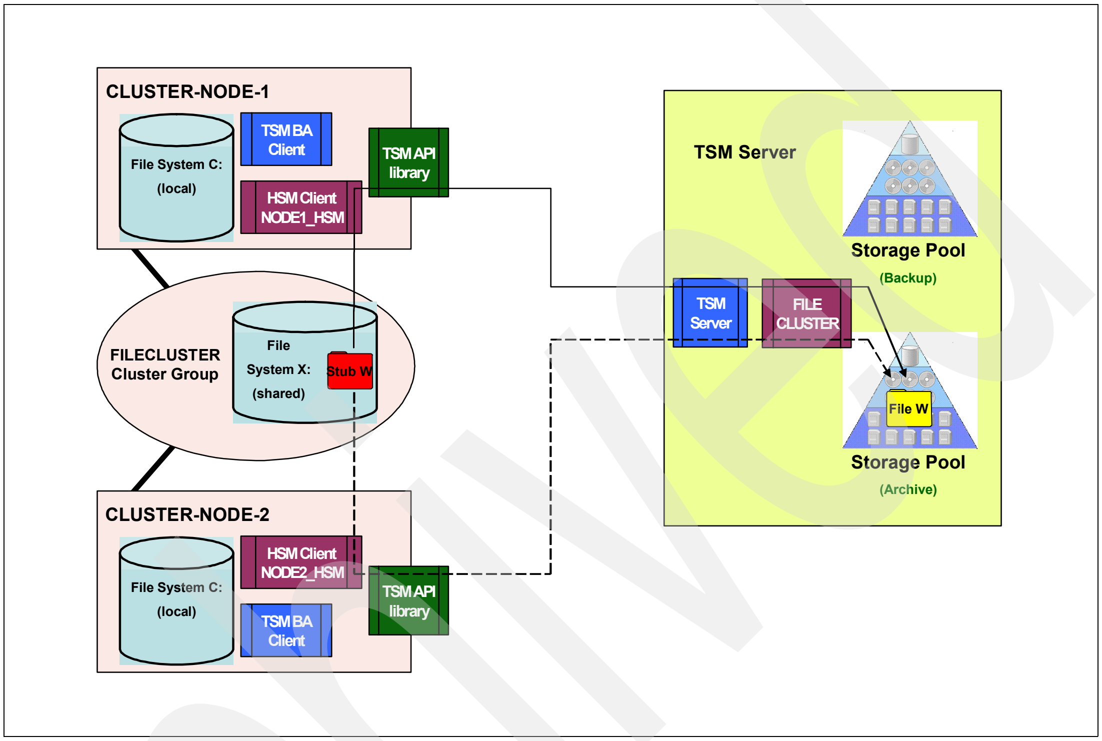


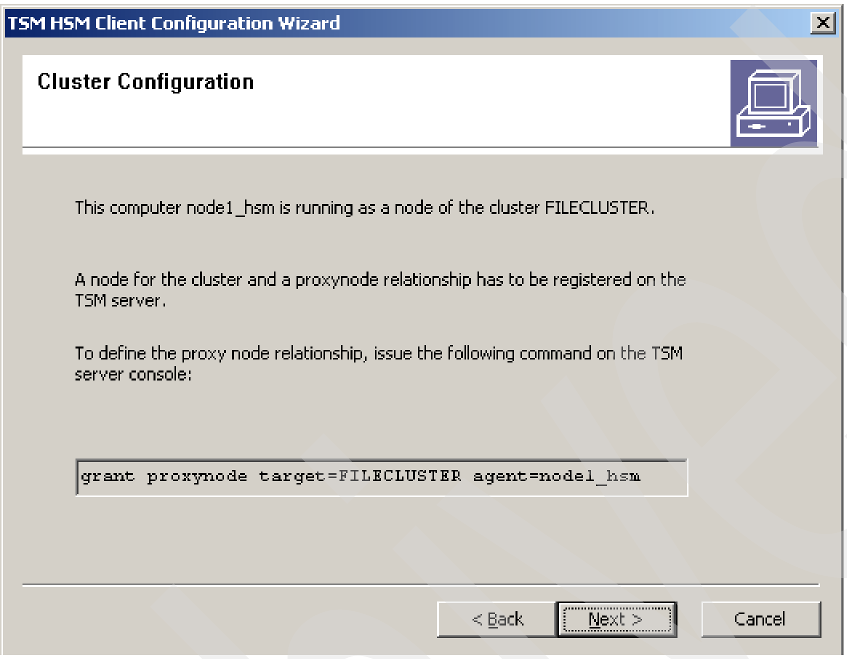
Figure 16-8 HSM client in an MSCS environment

You must install the software on both cluster nodes if you want to be able to recall files after a failover or to run migration jobs on both nodes. Some additional installation steps are required in order to run in a clustered environment:

- Configuration wizard - GRANT PROXYNODE
- Cluster and volume name mapping

16.4.1 Configuration wizard - GRANT PROXYNODE

When a cluster is detected, the configuration wizard displays an additional panel (Figure 16-9 on page 215), which instructs you to run the GRANT PROXYNODE command on your Tivoli Storage Manager server.



This computer node1_hsm is running as a node of the cluster FILECLUSTER.

A node for the cluster and a proxynode relationship has to be registered on the TSM server.

To define the proxy node relationship, issue the following command on the TSM server console:

```
grant proxynode target=FILECLUSTER agent=node1_hsm
```

Figure 16-9 Cluster configuration page from the configuration wizard

You have to run this command before continuing with the configuration wizard because the HSM client immediately connects to the Tivoli Storage Manager server when the wizard completes. This connection fails if the proxynode definition has not been defined.

This command is necessary to give both HSM clients on each cluster node the ability to access the data that was migrated by HSM to the Tivoli Storage Manager server. For our configuration we enter:

- On cluster node 1: GRANT PROXYNODE TARGET=FILECLUSTER AGENT=NODE1_HSM
- On cluster node 2: GRANT PROXYNODE TARGET=FILECLUSTER AGENT=NODE2_HSM

Example 16-1 shows the output from the Tivoli Storage Manager server.

Example 16-1 Grant proxynode command on the Tivoli Storage Manager server

```
tsm: BLCKWTCH>grant proxynode target=filecluster agent=node1_hsm
ANR0140I GRANT PROXYNODE: success.  Node NODE1_HSM is granted proxy authority
to node FILECLUSTER.

tsm: BLCKWTCH>grant proxynode target=FILECLUSTER agent=node2_hsm
ANR0140I GRANT PROXYNODE: success.  Node NODE2_HSM is granted proxy authority
to node FILECLUSTER.
```

The TARGET parameter specifies the nodename on the Tivoli Storage Manager server that is used by the HSM client to write the migrated data to. If a suitable node does not already exist, you must create it before running the GRANT PROXYNODE command. The wizard is suggesting the generic cluster name as the target node, but you could use any other node name as well. The AGENT parameters are the nodenames for each HSM client on the cluster nodes that are needed to access the Tivoli Storage Manager server. This is different from the non-cluster installation. In a non-cluster environment, the HSM data is stored under nodename NODE1_HSM (the nodename for the HSM client), whereas in the cluster environment the data is stored under the nodename FILECLUSTER. See also Figure 16-8 on page 214.

Note: In our configuration, we used the cluster name FILECLUSTER for both the nodename on the Tivoli Storage Manager server for the HSM data as well as for the incremental backups of the backup-archive client. Therefore, this nodename already exists. It is not required to use the cluster name for the nodename, and you could also define two separate nodes, one for the HSM data and another for the incremental backup data.

16.4.2 Cluster and volume name mapping

When operating in a cluster environment, the HSM client needs to handle the volume name mapping differently in order to correctly recall and retrieve files on shared disks based on the information stored in the stub file. Compared with a single server environment, in a cluster environment, all the nodes in the cluster need to be able to recall and retrieve the migrated files in case of a failover by using the HSM client.

During file migration, the HSM client stores the complete UNC pathname of a file in the Tivoli Storage Manager database as well as in the reparse point left in the stub on the client's local disk. This pathname includes the *host name of the node*. Therefore, in a *non-cluster configuration*, it would include the name CLUSTER-NODE-1. The recall operation, the IBM TSM HSM Recall Service (hsmservice.exe), looks for the pathname found in the reparse data and verifies that it is a local path. This is important, as the driver that restores the file can only work on local NTFS disks. Because this pathname contains the name of CLUSTER-NODE-1 as the host name, the recall operation will succeed.

If the HSM client in a *cluster configuration* would also include in the path name the local *hostname of the node,* CLUSTER-NODE-1, the recall operation after failover to node CLUSTER-NODE-2 would fail because the pathname in the reparse data contains the name of CLUSTER-NODE-1 as the host name instead of CLUSTER-NODE-2. The same would happen for a retrieve operation.

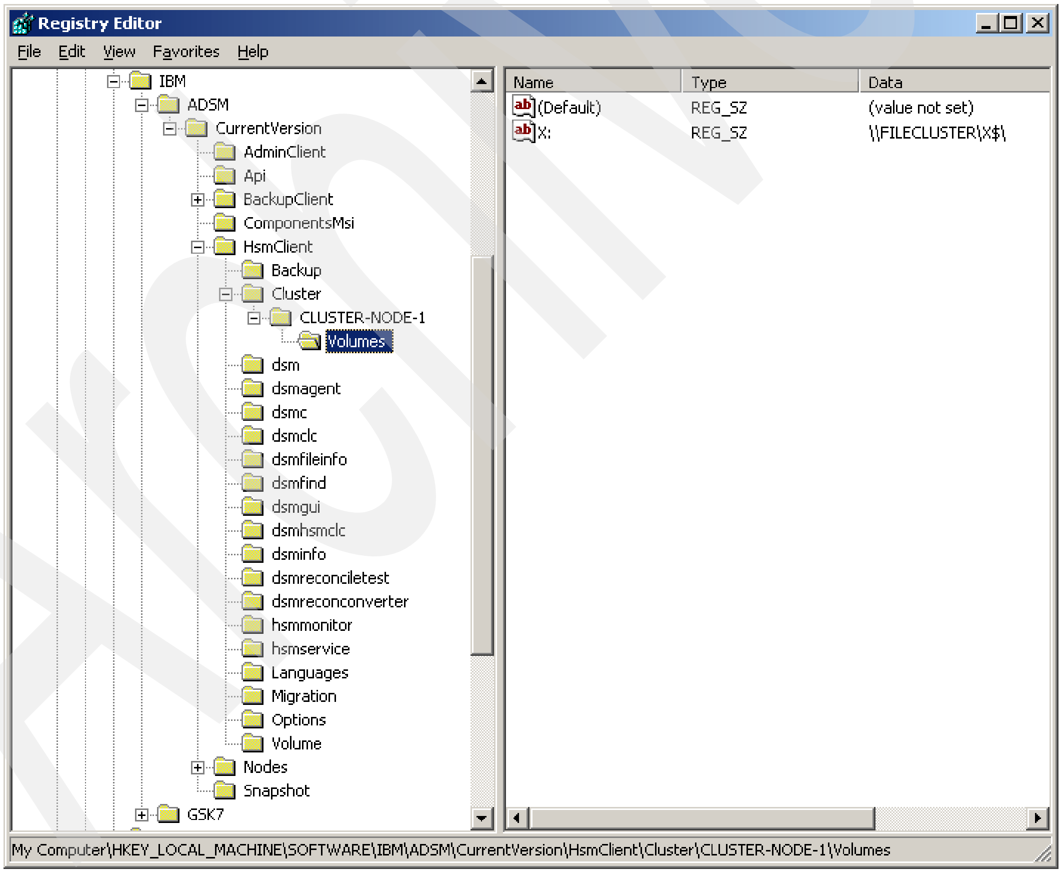
In order to address these node name issues, the HSM client maps the node names and volumes in a cluster to the *generic cluster name* and its volumes to include the generic cluster name in the path name. This mapping is done automatically for any cluster resource volume of any cluster group that can fail over and that is configured with the HSM for Windows client.

The mapping is done *automatically* when the HSM client first starts up. In our simple example, we have only one shared drive, X. It is remapped as shown in Table 16-1. The remapping is stored in the registry, as shown in Figure 16-10. Review the automatic mappings and see if all mappings are done correctly before you start your first migration job.

> **Attention:** These settings define the host and drive names on which data is stored. These settings are stored in the reparse points that are part of the stub files that are needed to recall files. Changing this mapping after a file has been migrated makes user recall impossible.

Table 16-1 Drive and volume name mapping

Name	Type	Data
X:	REG_SZ	\\FILECLUSTER\X$\



Name	Type	Data
(Default)	REG_SZ	(value not set)
X:	REG_SZ	\\FILECLUSTER\X$\

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ADSM\CurrentVersion\HsmClient\Cluster\CLUSTER-NODE-1\Volumes

Figure 16-10 Drive and volume name mapping in the registry

The HSM client checks the mappings and replaces the node name for each volume defined by the cluster name. This applies to all operations involving:

- Reparse data in the stub files
- Path names in Tivoli Storage Manager server database
- Search and retrieve operations

This means that recall and retrieve operations work when a cluster failover occurs. The scenario will then be as follows:

1. Files are migrated from volume X: by CLUSTER-NODE-1.
2. CLUSTER-NODE-1 fails.
3. Cluster group FILECLUSTER fails over to CLUSTER-NODE-2.
4. Recall of migrated files from X: on CLUSTER-NODE-2 is successful.
5. Retrieve of migrated files from X: is also successful on CLUSTER-NODE-2.

16.4.3 Migration jobs after cluster failover

In a failover situation, HSM migration jobs defined on CLUSTER-NODE-1 may no longer be executable from CLUSTER-NODE-2. Since the HSM job files are by default stored on CLUSTER-NODE-1's C drive and include the local host name in the HSM job definition, they will not be accessible or executable if this node fails.

To avoid this, we recommend creating a second separate job on the second node with the same definition and execute this job after a failover. This could easily be done by copying the job file and editing the job then.

You could store the HSM job files on a shared cluster disk volume by modifying the location of the job files directory using the HSM for Windows client GUI (**Tools** ∅ **Preferences** ∅ **Path Configuration**) on both cluster nodes. In a failover, the job files will then be visible to the other cluster node, but not be executable. Already existing job files must be copied manually to the shared drive, using Windows Explorer.

In an active-active cluster configuration you should make sure to use different names for the HSM jobs on each cluster node (for example, include the cluster node name in the HSM job name) so that you do not overwrite existing HSM jobs from the other node.

16.4.4 Backup before migrate in a cluster environment

Backup before migrate requires careful consideration in a cluster environment, depending on how you are doing your backup of the cluster and how you have configured your Tivoli Storage Manager backup-archive client. There are two key questions when using this function in a clustered environment. The answers to these provide guidance on whether you should use backup before migrate, or an alternative method to ensure backup.

Questions to answer

The questions to answer are:

- Which option file is used for the incremental backup process?
- Which node and filespace are applied to the incremental backup?

File backup in a clustered environment

Before we can answer these questions and explain how a backup before migrate would work in a cluster environment, we need to explain how backup is configured and working in the cluster environment.

As Figure 16-11 on page 219 shows, we have a backup for the local drive C: of each cluster node and a backup of the shared cluster disk X:. The backup of the cluster disk can fail over from CLUSTER-NODE-1 to CLUSTER-NODE-2 in this cluster environment.

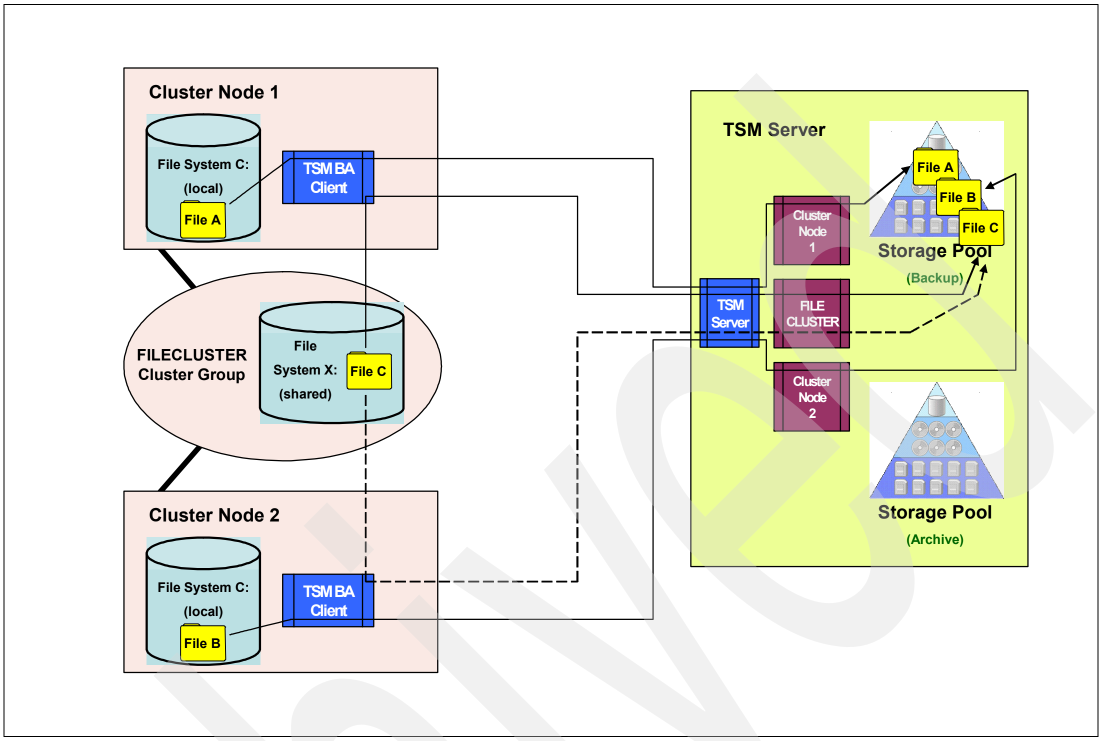


Figure 16-11 Backup in a cluster environment

Option files used

For this backup scenario, each node requires two option files for the Tivoli Storage Manager backup-archive client:

- dsm.opt for the backup of the local drive C: specifying:
  - CLUSTERNODE=NO
  - NODENAME CLUSTER-NODE-1 or CLUSTER-NODE-2, as applicable
- dsm_cluster.opt for the backup of the shared drive X: specifying:
  - CLUSTERNODE=YES
  - NODENAME FILECLUSTER

Filespaces created after backup

On the Tivoli Storage Manager server, after running backups, we can see which filespaces are created with the QUERY FILESPACE command, as shown in Example 16-2.

Example 16-2 Query filespace for a cluster environment

```
tsm: BLCKWTCH>query filespace *cluster*

Node Name       Filespace   FSID Platform Filespace Is Files-    Capacity   Pct
                Name                      Type        pace           (MB)  Util
                                                    Unicode?

--------------- ----------- ---- -------- --------- --------- ----------- -----
CLUSTER-NODE-1  \\cluster--    1 WinNT    NTFS         Yes        3,059.2  60.4
                 node-1\c$
```

```
CLUSTER-NODE-2  \\cluster--    1 WinNT    NTFS         Yes         3,059.2  60.0
                 node-2\c$
FILECLUSTER     \\fileclus-    1 WinNT    NTFS         Yes         1,022.0   2.8
                 ter\x$

tsm: BLCKWTCH>
```

Each cluster node has a filespace for the local backup of its C: drive, and there is also a filespace for the shared drive X: associated with the FILECLUSTER node.

> **Note:** We use a simple active-standby cluster configuration to explain the backup in a cluster environment and the usage of the backup before migrate function. The behavior could be extended to an active-active configuration with more cluster groups as well.

> **Note:** For more details about the Tivoli Storage Manager backup-archive client configuration in a cluster environment refer to Appendix D, “Configuring the backup-archive client in a cluster server environment,” in the *Windows Backup-Archive Clients Installation and User’s Guide*, SC32-0146.

Using backup before migrate in a clustered environment

Now, building on the same configuration, what happens if we define an HSM migration job that triggers migration of file C” on the shared drive (X) using backup before migrate? In Example 16-3 we redisplay the filespaces on the Tivoli Storage Manager server after the HSM job is executed successfully.

Example 16-3 Filespace after backup before migration HSM job is run

```
tsm: BLCKWTCH>query filespace *cluster*

Node Name       Filespace   FSID Platform Filespace Is Files-    Capacity   Pct
                Name                      Type        pace           (MB)  Util
                                                    Unicode?
--------------- ---------- ---- -------- --------- --------- ----------- -----
CLUSTER-NODE-1  \\cluster--    1 WinNT    NTFS         Yes         3,059.2  60.4
                 node-1\c$
CLUSTER-NODE-1  \\cluster--    2 WinNT    NTFS         Yes         1,022.0   2.8
                 node-1\x$
CLUSTER-NODE-2  \\cluster--    1 WinNT    NTFS         Yes         3,059.2  60.0
                 node-2\c$
FILECLUSTER     \\fileclus-    1 WinNT    NTFS         Yes         1,022.0   2.8
                 ter\x$
FILECLUSTER     hsm            2 WinNT    API:TSM      Yes            10.0 100.0
                                           HSM Cli-
                                           ent for
                                           Windows
```

Compared with Example 16-2 on page 219, we can see two new filespaces, one for CLUSTER-NODE-1 and the other for the FILECLUSTER node. Figure 16-12 shows what happened.

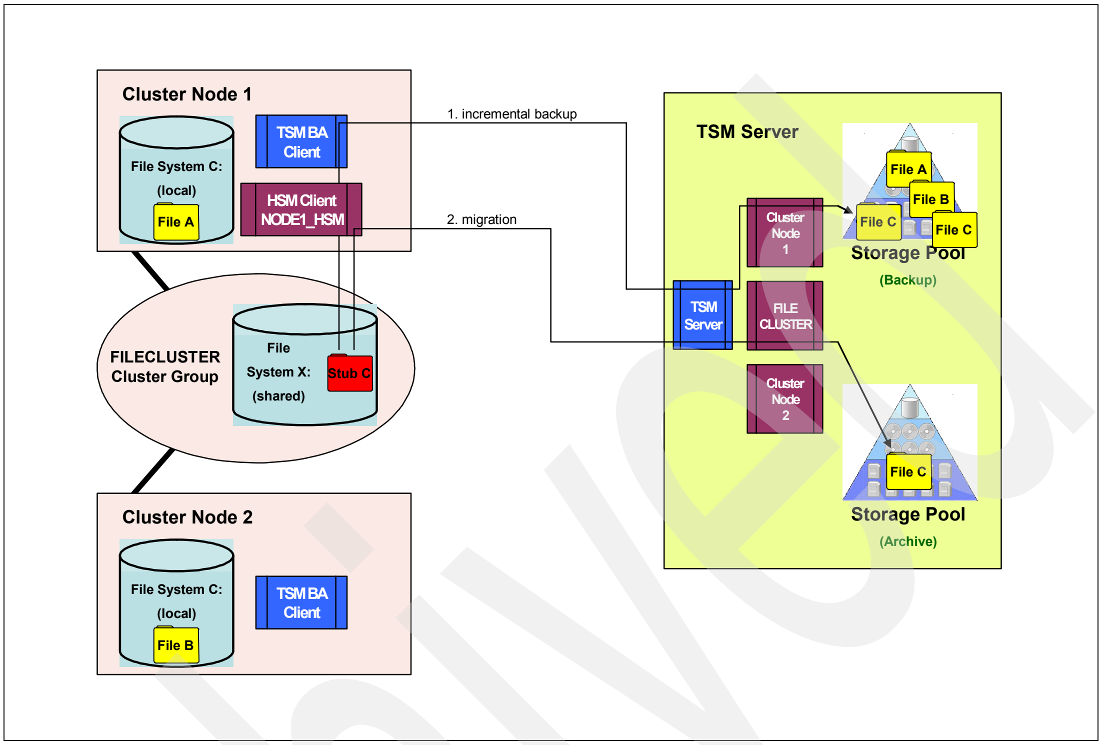


Figure 16-12 Backup before migrate in a cluster scenario

The incremental backup that is executed by the HSM client uses the default option file (from those defined in “Option files used” on page 219) to control the backup session. This is the dsm.opt option file that is used for the backup of the local C: drive on the cluster node and includes the option CLUSTERNODE=NO and NODENAME CLUSTER-NODE-1. Therefore, a new filespace \\CLUSTER-NODE-1\X$ is created under the nodename CLUSTER-NODE-1 and a new copy of the file C within this filespace is stored on the Tivoli Storage Manager server.

After the backup completes, the file is migrated by the HSM client to the Tivoli Storage Manager server under nodename FILECLUSTER to the filespace HSM. The migration works as explained in 16.4.2, “Cluster and volume name mapping” on page 216. The stub file is left on the shared disk.

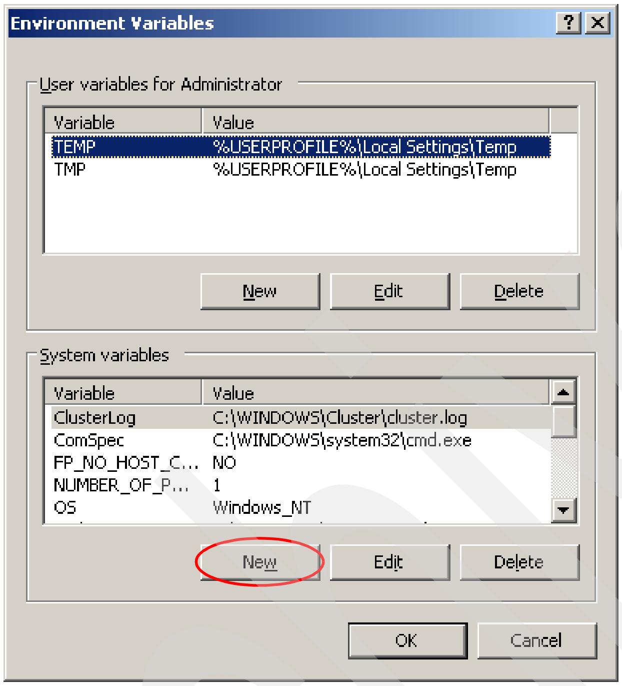
Using this configuration then requires more storage space to store the extra backups, and can also make it difficult to locate the correct file version to restore. Therefore, if we want backup before migrate to work more efficiently, we need to make sure that the correct options file is used for both the HSM for Windows client and the backup-archive client.

Specify the options file

There are two ways to specify the options file to be used:

- Method 1: Use the DSM_CONFIG environment variable.

  You can set the DSM_CONFIG environment variable to specify dsm_cluster.opt (in our configuration, see “Option files used” on page 219), as shown in Figure 16-13 and Figure 16-14 on page 222. Run **Start** ∅ **Control Panel** ∅ **System** ∅ **Advanced** ∅ **Environment Variables** and add a new variable called DSM_CONFIG with the value C:\Program Files\Tivoli\TSM\baclient\dsm_cluster.opt.



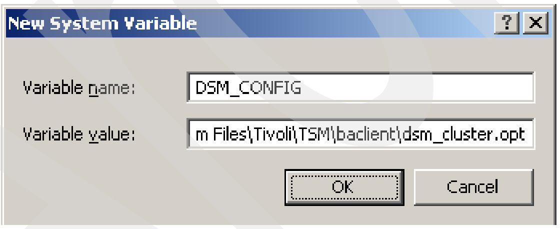
User variables for Administrator

Variable	Value
TEMP	%USERPROFILE%\Local Settings\Temp
TMP	%USERPROFILE%\Local Settings\Temp

System variables

Variable	Value
ClusterLog	C:\WINDOWS\Cluster\cluster.log
ComSpec	C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_C...	NO
NUMBER_OF_P...	1
OS	Windows_NT

Figure 16-13 Add a new environment variable



Variable name: DSM_CONFIG

Variable value: m Files\Tivoli\TSM\baclient\dsm_cluster.opt

Figure 16-14 Specify properties for new environment variable

After restarting the HSM client, the client uses the dsm_cluster.opt for the incremental backup process. However, if you set this variable, your Tivoli Storage Manager backup-archive client will also use the same client options file. To force it to use the correct options file, you must specify the option -optfile=dsm.opt when backing up the C drive with the backup-archive client. Do not modify an installed scheduler service, since it is already configured with the correct options file.

- Method 2: Run the HSM client via a batch file.

  You can also write a small batch program that sets DSM_CONFIG before starting the HSM for Windows client and clears it when you close the HSM for Windows client. Example 16-4 gives a sample batch file to do this.

Example 16-4 Batch file to start the HSM for Windows client GUI with cluster option file

```
@ECHO OFF
TITLE HSM for Windows in a cluster environment
SET DSM_CONFIG=C:\Program Files\Tivoli\TSM\baclient\dsm_cluster.opt
"C:\Program Files\Tivoli\TSM\hsmclient\dsmgui.exe"
SET DSM_CONFIG=
```

After setting the options file

After you use one of these two methods to start the HSM for Windows client using the options file for your cluster backup (dsm_cluster.opt), when an HSM job starts, the job will fail. You will see this error message in the HSM backup log file:

```
12/01/2007 00:42:29 ANS1228E Sending of object
'\\cluster-node-1\x$\HSMData\itso.files0.txt' failed
```

12/01/2007 00:42:29 ANS1151E '\\cluster-node-1\x$' is not a cluster disk.

Remember that the HSM for Windows client creates a temporary backup filelist with absolute UNC path names, which is then executed by **dsmc** as an external process, with the filelist parameter as argument. The **dsmc** uses the dsm_cluster.opt options file with CLUSTERNODE=YES set. The backup-archive client identifies the file space \\CLUSTER-NODE-1\X$ as a non-cluster disk, since the actual cluster disk is \\FILECLUSTER\X$.

Change parameters in the option file and rename the filespace

To use the backup before migrate function now with your cluster options file two more changes are required:

- In the dsm_cluster.opt options file, change the parameter CLUSTERNODE=YES to CLUSTERNODE=NO and add the domain parameter with DOMAIN \\CLUSTER-NODE-1\X$.
- Rename the filespace \\FILECLUSTER\X$ for the node FILECLUSTER on the Tivoli Storage Manager server from \\FILECLUSTER\X$ to \\CLUSTER-NODE-1\X$ with the command RENAME FILESPACE FILECLUSTER \\FILECLUSTER\X$ \\CLUSTER-NODE-1\X$ NAMETYPE=UNICODE, as shown in Example 16-5.

Example 16-5 Rename the cluster filespace on the Tivoli Storage Manager server

```
tsm: BLCKWTCH>query filespace filecluster

Node Name       Filespace   FSID Platform Filespace Is Files-    Capacity   Pct
                Name                      Type        pace           (MB)  Util
                                                    Unicode?
--------------- ----------- ---- -------- --------- --------- ----------- -----
FILECLUSTER     \\fileclus-    1 WinNT    NTFS         Yes        1,022.0   2.8
                 ter\x$
FILECLUSTER     hsm            2 WinNT    API:TSM      Yes           10.1 100.0
                                           HSM Cli-
                                           ent for
                                           Windows
```

```
tsm: BLCKWTCH>rename filespace filecluster \\filecluster\x$ \\cluster-node-1\x$
nametype=unicode

Do you wish to proceed? (Yes (Y)/No (N)) yes
ANR0822I RENAME FILESPACE: Filespace \\filecluster\x$ (fsId=1) successfully
renamed to \\cluster-node-1\x$ for node FILECLUSTER.

tsm: BLCKWTCH>query filespace filecluster

Node Name       Filespace   FSID Platform Filespace Is Files-    Capacity   Pct
                Name                      Type        pace           (MB)  Util
                                                    Unicode?
--------------- ----------- ---- -------- --------- --------- ----------- -----
FILECLUSTER     \\cluster--    1 WinNT    NTFS         Yes        1,022.0   2.8
                 node-1\x$
FILECLUSTER     hsm            2 WinNT    API:TSM      Yes           10.1 100.0
                                           HSM Cli-
                                           ent for
                                           Windows
```

Restart the HSM client after making these changes. The backup before migration now runs without a failure using the FILECLUSTER nodename with the \\CLUSTER-NODE-1\X$ filespace.

You can start a normal backup for the shared cluster disk X: (which is using the dsm_cluster.opt options file) using the CLI as shown in Example 16-6 or a scheduler service. It is not possible to use GUI, because the GUI displays only the local drives for selection for a backup. This is because CLUSTERNODE=NO is specified in the options file.

Example 16-6 Back up the shared cluster disk

```
C:\Program Files\Tivoli\TSM\baclient>dsmc -optfile=dsm_cluster.opt
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 5, Level 0.0
  Client date/time: 12/01/2007 01:38:16
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.

Node Name: FILECLUSTER
Session established with server BLCKWTCH: Windows
  Server Version 5, Release 5, Level 0.0
  Server date/time: 12/01/2007 01:38:28  Last access: 12/01/2007 01:37:04

tsm> incremental

Incremental backup of volume '\\cluster-node-1\x$'
Directory-->                   0 \\cluster-node-1\x$\HSMData [Sent]
Normal File-->         1,048,576 \\cluster-node-1\x$\HSMData\itso.files11.txt [S
ent]
Normal File-->         1,048,576 \\cluster-node-1\x$\HSMData\itso.files12.txt [S
ent]
Successful incremental backup of '\\cluster-node-1\x$'


Total number of objects inspected:       52
Total number of objects backed up:        3
Total number of objects updated:          0
Total number of objects rebound:          0
Total number of objects deleted:          0
Total number of objects expired:          0
Total number of objects failed:           0
Total number of subfile objects:          0
Total number of bytes transferred:    2.00 MB
Data transfer time:                    0.04 sec
Network data transfer rate:        43,593.93 KB/sec
Aggregate data transfer rate:        143.82 KB/sec
Objects compressed by:                    0%
Subfile objects reduced by:               0%
Elapsed processing time:           00:00:14
```

Attention: With the parameter CLUSTERNODE=NO your backup for the shared cluster disk X: no longer fails over to the cluster node 2 in case of a cluster failover.

Conclusion and answers

Now we can answer the two questions that we asked previously in “Questions to answer” on page 218 related to using backup before migrate in a cluster environment.

- *Question:* Which options file is used for the incremental backup process?

  Answer: The HSM client uses, by default, the options file dsm.opt to execute the incremental backup process before the migration is started. This behavior can be changed by using the DSM_CONFIG variable to set a specific option file or by using a batch file.

- *Question:* Which node and filespace are applied to the incremental backup?

  Answer: The HSM client always includes the local UNC path when the backup filelist is created. This means that the incremental backup uses a filespace name that includes the local UNC name. If this filespace does not exist, a new one will be created, so that you will see \\CLUSTER-NODE-1\X$, as opposed to \\FILECLUSTER\X$.

If you have a cluster environment and want to use the HSM client to migrate files from the shared cluster disks you should consider whether to use the backup before migrate function because, as we have seen, this requires some changes for your current backup environment.

To minimize the impact to your current backup environment we recommend that you take advantage of the backup integration with the backup-archive client V5.5 together with the HSM client V5.5. The enhanced integration ensures that the backup-archive client, independently of the HSM client, always maintains a copy of the complete file in the backup pool, whether this file is migrated or not. Each stub file always has an associated current copy of the complete file in the backup pool. The stub file and the complete file version are associated with each other and managed as a single version of the file in the Tivoli Storage Manager server. In this way, you can avoid using backup before migrate, and its required changes. For more detail about the enhanced backup integration refer to 23.1, “Backup integration” on page 312.

If you decide to use backup before migrate in your cluster environment you should review your backup environment and decide whether you can use the default setup where the dsm.opt option file is used for backup before migrate operations. As we have seen, this causes another copy of your data to be stored under a different nodename and filespace.

When your cluster environment makes it necessary to use the backup before migration function with the option file from your cluster backup, we summarize here the changes which you need to perform, as described in this chapter:

- Set the environment variable DSM_CONFIG to point to the correct cluster option file (for example, dsm_cluster.opt) either for the entire system or using a BATCH file to start the HSM for Windows client GUI.
- Change in your cluster option file CLUSTERNODE=YES to CLUSTERNODE=NO and add a domain statement for the shared disk drive with the local host name in your options file, for example, DOMAIN \\CLUSTER-NODE-1\X$.
- Rename the filespace of the shared cluster disk on your Tivoli Storage Manager server to include the local host name instead of the cluster name, for example, \\FILECLUSTER\X$ ∅ \\CLUSTER-NODE-1\X$.

16.5 Recall quotas

The HSM client allows you to create file recall quotas to limit the number of possible file recalls for a specific time period. The recall quotas help to prevent uncontrolled mass recalls that could be triggered, for example, by a user who starts a copy process for a high amount of data that contains migrated files (stub files). Mass recalls could impact your free disk space as well as affect the overall system and network performance. Therefore, we recommend configuring recall quotas. Quotas have no effect on explicit file retrieval with the HSM client GUI.

Set recall quotas

You can use a system-wide (default quota) quota or create quotas for particular Windows (local or domain) users and groups. Quotas can be configured using the HSM GUI **Tools** ∅ **Quotas** ∅ **Define Quotas**, as shown in Figure 16-15.

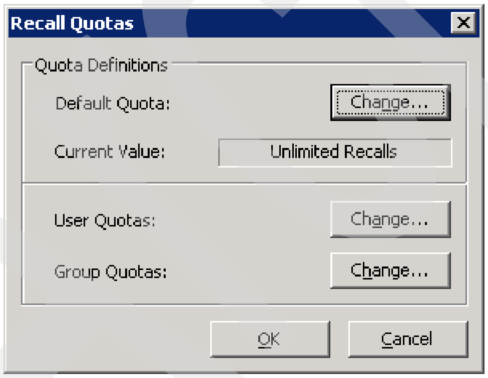
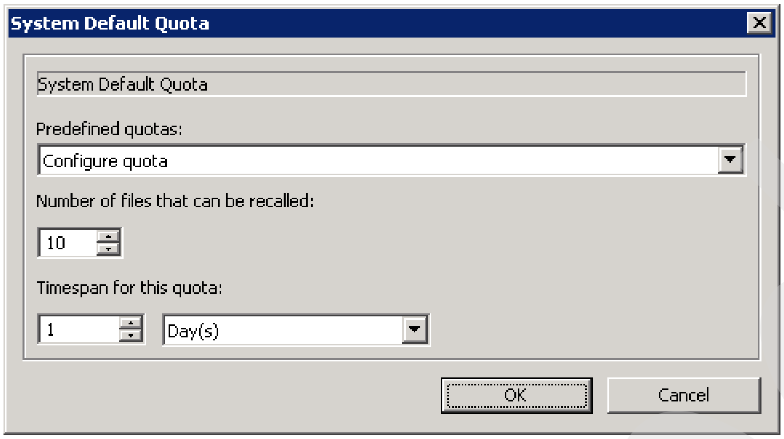

Current Value: Unlimited Recalls

Figure 16-15 Recall quotas

Figure 16-16 shows the dialogue to set the system default quota.



Predefined quotas: Configure quota

Number of files that can be recalled: 10

Timespan for this quota: 1 Day(s)

Figure 16-16 Set system default quota

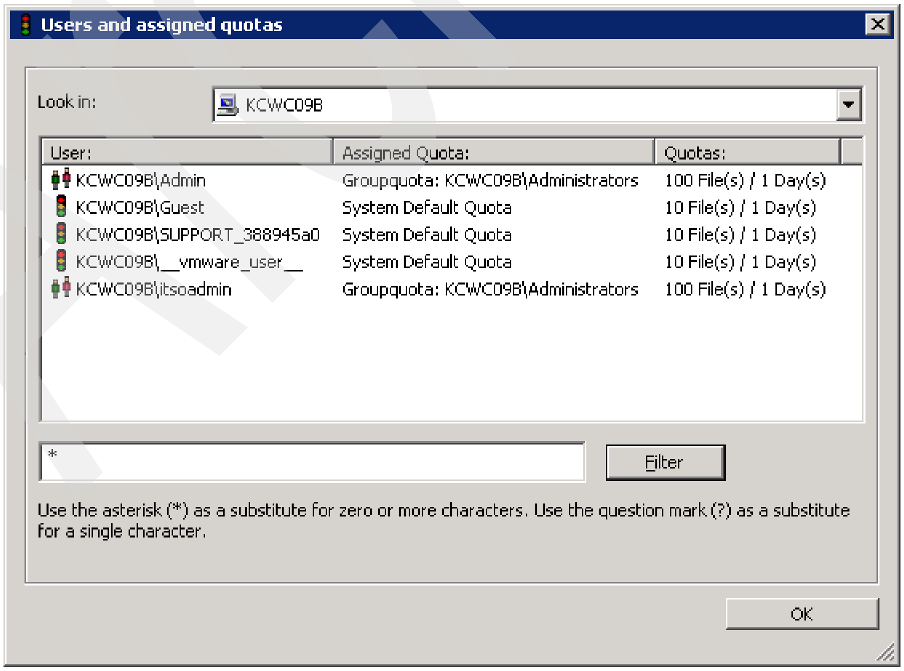
You can define the number of files that can be recalled for the specified time interval. In our example we can recall 10 files within one day. It is not necessary to restart the HSM GUI or the system after defining a recall quota. Quotas can be set and changed online.

The default quota defines the general number of possible file recalls in a time period for a group and users for whom no specific quota has been defined.

When a file recall quota is exceeded, a subsequent file recall request is rejected, an error is returned to the application, and the file remains migrated. The error message that is displayed can vary depending on the application.

View recall quotas

You can display the recall quotas that are applied for a system in the HSM GUI by selecting **Tools** ∅ **Quotas** ∅ **View Quotas**, as shown in Figure 16-17.



Look in: KCWC09B

User:	Assigned Quota:	Quotas:
KCWC09B\Admin	Groupquota: KCWC09B\Administrators	100 File(s) / 1 Day(s)
KCWC09B\Guest	System Default Quota	10 File(s) / 1 Day(s)
KCWC09B\SUPPORT_388945a0	System Default Quota	10 File(s) / 1 Day(s)
KCWC09B__vmware_user__	System Default Quota	10 File(s) / 1 Day(s)
KCWC09B\itsoadmin	Groupquota: KCWC09B\Administrators	100 File(s) / 1 Day(s)

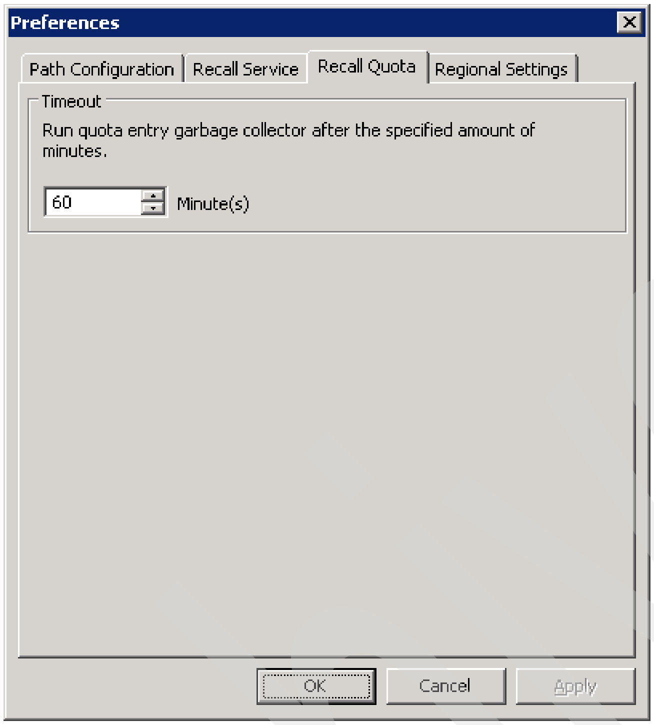
*

Use the asterisk (*) as a substitute for zero or more characters. Use the question mark (?) as a substitute for a single character.

Figure 16-17 View recall quotas

Recall quota entries deletion interval

The recall quota entries deletion interval is used by the HSM client GUI to define the interval that the program uses to delete recall quota entries. These entries are created to track quota allocations. The interval can be changed with the preferences editor in the HSM GUI T**ools** ∅ **Preferences** ∅ **Recall Quota**, as shown in Figure 16-18 on page 228.



Timeout

Run quota entry garbage collector after the specified amount of minutes.

60 Minute(s)

Figure 16-18 Recall quota entries deletion interval setting

Use the Minute(s) box to define the number of minutes for the interval the recall service uses to delete expired quota entries.

16.6 Hints and tips for using HSM

In this section we discuss hints and tips for using the HSM client.

16.6.1 Preserve the last access date of a file

Any application that touches a file may implicitly cause that file's last access date to be changed to the time that the application touches it. This is a function of the file system, not the application.

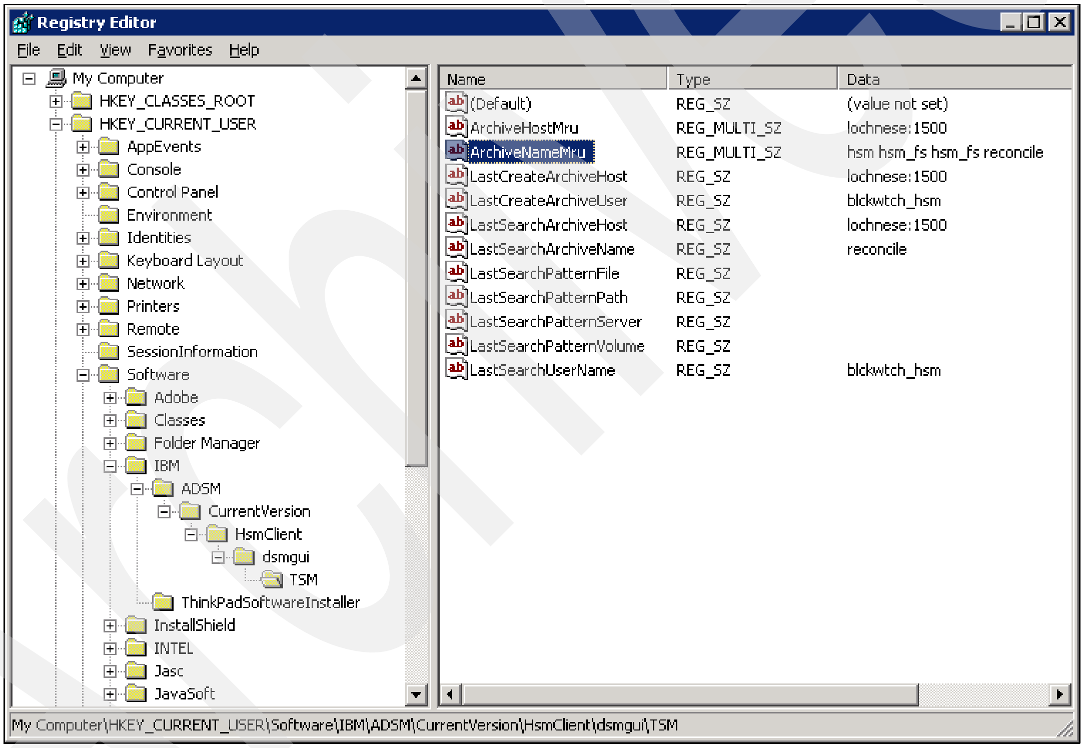
Because of this, when the Tivoli Storage Manager backup-archive client backs up or archives a file, it may trigger an update to the file's last access date. This can cause problems for the HSM client if you use a policy that includes the last access date of a file, because the files will then not be migrated as expected.

By default, the Tivoli Storage Manager client will not reset the last access date of any backed up or archived files to their original value following the backup or archive operation. This behavior can be changed by adding PRESERVELASTACCESSDATE YES to the backup client options file.

This option applies to files only and resets the last access date of any specified files to their original value following the backup or archive operation. Resetting the last access date incurs additional overhead that may impact backup and archive performance. The last access date should be reset only if you are using another application, such as a Storage Resource Management (SRM) or Hierarchical Storage Management (HSM) that relies on accurate last access dates.

16.6.2 How to clear the selectable filespace list in the HSM GUI

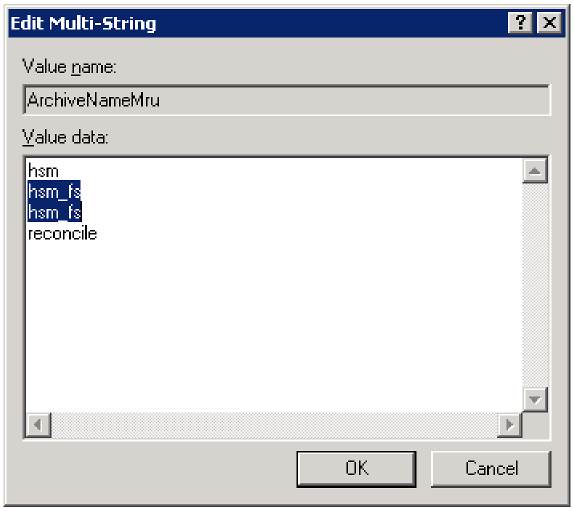
Filespaces that you created with the configuration wizard or the HSM GUI are always selectable as destinations in a HSM job definition, even if the filespace no longer exists on the Tivoli Storage Manager server (for example, if you deleted them manually). If you select such a filespace as migration destination, the migration job will fail. Therefore, we recommend clearing the filespace list in the HSM GUI. This could be done by editing the registry key HKEY_CURRENT_USER\Software\IBM\ADSM\CurrentVersion\HsmClient\dsmgui\TSM\ArchiveNameMru (Figure 16-19) and deleting the filespace names that are no longer available, as shown in Figure 16-20 on page 230 and Figure 16-21 on page 230.



Name	Type	Data
(Default)	REG_SZ	(value not set)
ArchiveHostMru	REG_MULTI_SZ	lochnese:1500
ArchiveNameMru	REG_MULTI_SZ	hsm hsm_fs hsm_fs reconcile
LastCreateArchiveHost	REG_SZ	lochnese:1500
LastCreateArchiveUser	REG_SZ	blckwtch_hsm
LastSearchArchiveHost	REG_SZ	lochnese:1500
LastSearchArchiveName	REG_SZ	reconcile
LastSearchPatternFile	REG_SZ	
LastSearchPatternPath	REG_SZ	
LastSearchPatternServer	REG_SZ	
LastSearchPatternVolume	REG_SZ	
LastSearchUserName	REG_SZ	blckwtch_hsm

My Computer\HKEY_CURRENT_USER\Software\IBM\ADSM\CurrentVersion\HsmClient\dsmgui\TSM

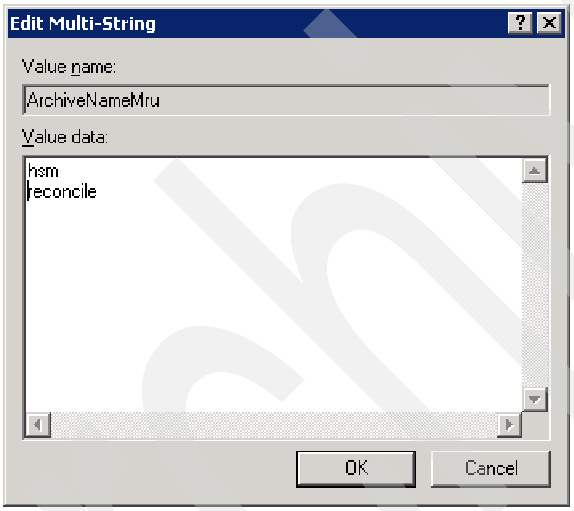
Figure 16-19 Using registry editor to clear filespace list



ArchiveNameMru

```
hsm
hsm_fs
hsm_fs
reconcile
```

Figure 16-20 Delete unnecessary entries



ArchiveNameMru

```
hsm
reconcile
```

Figure 16-21 Save the cleared list

17

VMware backup with Tivoli Storage Manager V5.4

This chapter describes the various methods of backup for VMware in Tivoli Storage Manager V5.4.

IBM recommends that, where possible, you should use the Tivoli Storage Manager V5.5 support for VMware Consolidated Backup in preference to any of the Tivoli Storage Manager 5.4 methods mentioned here (including VCB for Tivoli Storage Manager 5.4), since the newer level is easier to use and has more functionality.

17.1 VMware overview

VMware provides software virtualization *(hypervisor)* support for Intel-based hardware. It allows the use of multiple operating system images and operating system types, hosted from the same physical hardware, which in turn generally allows greater overall utilization of that shared hardware. Each operating system image virtualized in this way will be referred to as a *guest* from now on.

There are a number of types of VMware server available. For the rest of this chapter we discuss the VMware ESX server, since that is the enterprise version and will most likely be used for production services.

A number of VMware guests hosted on the same ESX server usually run in parallel. While this provides great benefits for various types of application, it may cause some issues with backup and recovery if traditional backup techniques are used without consideration of the underlying equipment.

There are a few different approaches to backup available with VMware, which we summarize in this chapter.

For more information about VMware see:

http://www.vmware.com

17.2 VMware backup options with Tivoli Storage Manager V5.4

In this section we describe three options to back up a VMware ESX environment with Tivoli Storage Manager V5.4.

17.2.1 Install Tivoli Storage Manager client on each guest

It is possible to install a Tivoli Storage Manager client on each of the guests and perform regular incremental file-level backups. For many small-scale installations, this may be sufficient. However, guests can encounter performance issues while backup processing is in progress, due to contention for CPU, disk storage, Fibre Channel, network, or other system resources.

Since the guests share the same hardware, these performance issues may affect all the guests, even if only some of them are actually backing up at that time. If these problems occur, it may be useful to limit the number of parallel backups taking place on one physical ESX server at a given time, for example, using the Tivoli Storage Manager scheduler to control that.

When using this backup method, the principal restriction is that LAN-free backup is not supported. The Tivoli Storage Manager client runs as a guest of an ESX server and there is no virtualized tape interface for it, so all the backup data has to travel over the LAN to the Tivoli Storage Manager server.

Since virtualizing I/O is difficult, the load imposed by virtualizing the disk and network traffic mean that backup in this way has a slightly higher impact on a guest than it would in an unvirtualized environment.

The Tivoli Storage Manager backup-archive client journaling features are supported for virtualized guests, and since they may help cut down on the I/O load on the system overall, if Tivoli Storage Manager must be installed on each guest, this may be a useful feature.

Another downside to this approach is the effort required to install and maintain multiple Tivoli Storage Manager clients. While this affects non-virtualized environments, typically one of the reasons to virtualize is to simplify and consolidate workloads and administrative overhead. Therefore, having to run a client on each guest runs counter to this intention.

17.2.2 Install a Tivoli Storage Manager client on the ESX console

It is possible to install a Tivoli Storage Manager client on the ESX service console itself in order to directly back up the actual files that comprise the guests. Since ESX is based on Linux, we install the Tivoli Storage Manager Linux client, and back up the VMware “vmdk” files as regular files straight to Tivoli Storage Manager. This allows us to back up full guests as a single entity, and do full guest system restores. You can use VMware snapshot technology to get a consistent backup from running guests. For more information about snapshot, see “VMware VCB snapshot” on page 329.

LAN-free backup is not supported from the ESX console. Therefore, all the traffic from the backup must use the LAN, with the same implications as if we used a file-level client on each guest. Another issue is that there is no real incremental backup function with this type of backup. It is all or nothing. We recommend that if you must use ESX service console backup at all, you use selective backup as opposed to regular incremental for this reason.

Note: The ESX service console has limited resources, which makes backups performed in this way slow. We do not recommend running the Tivoli Storage Manager client on the ESX console in production environments. Using this form of backup may starve your production guests of processor resources.

Single file restores are not trivial using this method of backup. If a guest is backed up into Tivoli Storage Manager in this way, you must first restore the entire guest, and import that back into VMware to get at the contained files. This may involve restoring Gigabytes of data just to get access to one small file. Remember that there is no subfile backup available for the Tivoli Storage Manager Linux client.

For further information about this configuration, see the white paper at:

http://www-1.ibm.com/support/docview.wss?uid=swg27009931

17.2.3 Initial support for VMware Consolidated Backup with Tivoli Storage Manager

VMware Consolidated Backup (VCB) is the preferred approach to back up with VMware for most environments, other than test or trivial ones. It involves off-loading most of the job of backup to a dedicated, non-virtualized system known as the *proxy*.

VCB is a component of VMware Infrastructure, and at the time of writing is exclusively available for guests hosted on VMware ESX servers.

The fundamental idea behind a VCB is to off-load the backup workload from the VMware ESX server to another machine. VCB has two modes: file-level and fullvm.

Fullvm backup

When using fullvm (full virtual machine) backup, a full image of the guest being backed up at that time is *copied* to the proxy, using temporary disk space on the proxy. The image is deleted immediately after backup. The amount of disk space used is directly related to the amount of data stored on the guests' file system, since VMware removes empty disk blocks from the export. It can still be hundreds of GB. In order to achieve file system consistency, the images are not hot during backing up. VMware performs a snapshot operation on the data. For more information snapshot see "VMware VCB snapshot" on page 329.

File-level backup

The file-level backup is somewhat different. The VCB software includes a driver that allows snapshotted file system data from an ESX-hosted Windows guest to be *virtually mounted* across the SAN into a folder on the proxy node's file system. This takes up no space on the proxy node, since the data is not actually *copied* anywhere, only *mounted*. The effect is that it becomes possible to access the files from the snapshotted guest on the proxy's mountpoint. Once the files are mounted in this way, we can back them up with Tivoli Storage Manager from the proxy, as shown in Figure 17-1 on page 234. More information about the VCB software components follows.

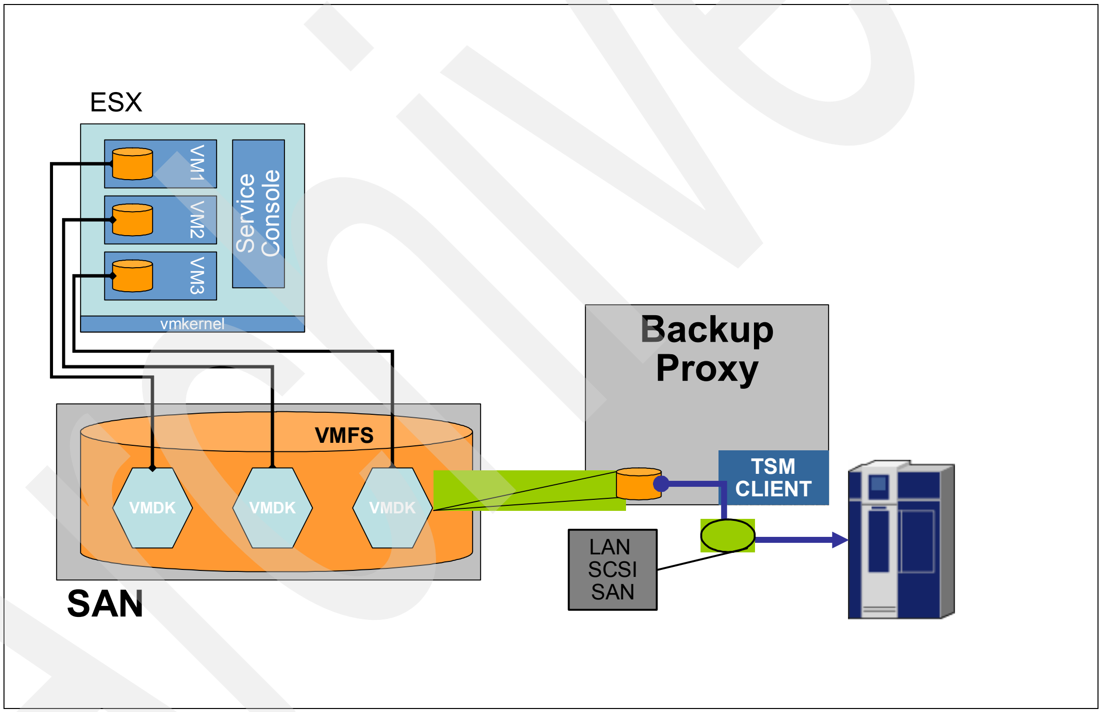


Figure 17-1 VMware consolidated backup in file-level mode

Tivoli Storage Manager has supported VMware Consolidated backup (VCB) through the use of an integration module since the later levels of the Tivoli Storage Manager 5.3 client became available. In order to use Tivoli Storage Manager with VCB, VMware software is required to be installed on the proxy, in order to control the VCB snapshotting/mounting function from the proxy.

- A VMware software component called *VCB Framework* allows the proxy node to initiate snapshots, and to withdraw them after use. In order to do this, it communicates over TCP/IP to the VMware infrastructure, either to a VirtualCenter server or to an ESX server directly. The proxy uses the appropriate credentials for VMware, that is, the ESX Admin ID and password, or VirtualCenter ID and password. VCB Framework is a component of the VMware Infrastructure 3, which requires a VMware license.

- Also required is the Integration Module to Tivoli Storage Manager (TSMIM), which is available at:

  http://www.vmware.com/download/vi/drivers_tools.html

  This is a small archive of scripts that allows the control of the VCB processing on the proxy, and is for use exclusively with pre-V5.5 versions of Tivoli Storage Manager. The archive also includes a readme file containing instructions on how to set up VCB with the TSMIM.

Note: As of Tivoli Storage Manager V5.5, the integration module is no longer required since these functions are integrated into the Tivoli Storage Manager client itself.

Part 5

Tivoli Storage Manager V5.5 server enhancements

This part presents enhancements to Tivoli Storage Manager V5.5 servers. First we detail the supported operating systems and summarize the new features and functions, then subsequent chapters present further details of the most significant new features.

18

Version 5.5 server supported environments

This chapter describes the following Tivoli Storage Manager Version 5.5 functions:

- Server operating system level supported
- New devices supported
- New functionality
  - VTL in SAN device mapping for SAN discovery
  - IPv6 support
- Administration Center support

The major new features of Tivoli Storage Manager V5.5 are described in detail in separate chapters.

For full details, always refer to the announcement letter, and to the installation and user guides and the readme files for the relevant server. Announcement letters can be found using keyword Tivoli Storage Manager at:

`http://www-01.ibm.com/common/ssi/index.wss`

Or directly for V5.5 as:

`http://www-01.ibm.com/common/ssi/index.wss?DocURL=http://www-01.ibm.com/common/ssi/rep_ca/6/877/ENUSZP07-0476/index.html&InfoType=AN&InfoSubType=CA&InfoDesc=Announcement+Letters&panelurl=index.wss%3F&paneltext=Announcement%20letter%20search`

You will find the V5.5 manuals and server readme files by selecting Storage Manager Release notes and readmes at:

`http://publib.boulder.ibm.com/infocenter/tivihelp`

18.1 Server operating systems supported

You will find the readmes for Tivoli Storage Manager V5.5 at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v1r1/topic/com.ibm.itsmreadme.doc_5.5/reln_server.html

An updated list of all the supported operating systems with the corresponding version of Tivoli Storage Manager can be found at:

http://www-1.ibm.com/support/docview.wss?rs=663&context=SSGSG7&uid=swg21243309&loc=en_US&cs=utf-8&lang=en

18.1.1 Technical changes for Version 5.5

The following changes have been made for V5.5.

- Calculating the migration thresholds for storage pools associated with sequential-access disk (FILE) devices is now using a percentage of the storage pool's total data capacity.
- Concurrent access to volumes in storage pools with a device type of FILE.

  The following server processes are allowed shared read access to FILE volumes:

  - BACKUP DB
  - BACKUP STGPOOL
  - COPY ACTIVEDATA
  - EXPORT/IMPORT NODE
  - EXPORT/IMPORT SERVER
  - GENERATE BACKUPSET
  - RESTORE STGPOOL
  - RESTORE VOLUME

  The following server processes are *not* allowed shared read access to FILE volumes:

  - AUDIT VOLUME
  - DELETE VOLUME
  - MIGRATION
  - MOVE DATA
  - MOVE NODEDATA
  - RECLAMATION
- Restartable server-to-server export.
- You can specify the TODATE and TOTIME parameters with an EXPORT NODE or EXPORT SERVER command.
- New support for Plasmon and IBM UDO2 Optical Disk Drives and Media.
- Client and server authentication using Secure Socket Layer (SSL), with two new TCP/IP options SSLTCPPORT land SSLTCPADMINPORT.
- SAN discovery for non-root users (AIX only).
- HP LTO-4 drive support and encryption.

  The IBM RMSS Ultrium device drive is required to be installed to enable drive encryption with IBM LTO-4. IBM LTO-4 SCSI drives do not support encryption.
- 3592 drive encryption enabled for HP-UX.
- Long file-name support, up to 8704 bytes.
- Setting a time zone on the z/OS server.

- z/OS server no longer uses Server Virtual Machine for serialization. Pthreads are used instead, which should improve performance.
- z/OS server is a POSIX-compliant UNX System Services application.

18.1.2 AIX server requirements for Tivoli Storage Manager

The Tivoli Storage Manager V5.5 server on AIX is supported at:

- AIX V5.3 64 bit
- AIX V6.1 64 bit

Note: 32-bit AIX is supported by Tivoli Storage Manager V5.3.

18.1.3 HP-UX server requirements for Tivoli Storage Manager

The requirements are:

- PA-RISC server requirements

  The Tivoli Storage Manager V5.5 server on HP-UX PA-RISC is supported at HP-UX 11i V2 64 bit.

- Itanium server requirements

  The Tivoli Storage Manager server on HP-UX Itanium is supported at HP-UX level 11iV2.

18.1.4 Linux server requirements for Tivoli Storage Manager

In this section we list the Linux server requirements for Tivoli Storage Manager.

Linux x86 server requirements

The Tivoli Storage Manager V5.5 server on Linux x86 is supported at:

- Red Hat Enterprise Linux 4 (AS, WS, ES) and 5
- Red Hat Enterprise Linux 5
- SUSE Linux Enterprise Server 9 and 10
- Asianux 2.0 - Red Flag DC 5.0, Miracle Linux 4.0, and Haansoft Linux 2006 or Asianux 3.0
- V2.3.3 or later of the GNU C libraries installed on the target machine

Linux x86_64server requirements

The Tivoli Storage Manager V5.5 server on Linux x86_64 is supported at:

- Red Hat Enterprise Linux 4 (AS, WS, ES)
- Red Hat Enterprise Linux 5
- SUSE Linux Enterprise Server 9 and 10
- Asianux 2.0 - Red Flag DC 5.0, Miracle Linux 4.0, and Haansoft Linux 2006 or Asianux 3.0
- V2.3.3 or later of the GNU C libraries installed on the target machine

Linux IA64 server requirements

The Tivoli Storage Manager V5.5 server on Linux IA64 is supported at:

- Red Hat Enterprise Linux 4 update 5, and 5
- SUSE Linux Enterprise Server 9 SP3 and 10 SP1
- Asianux 2.0 or Asianux 3.0
- V2.3.3 or later of the GNU C libraries installed on the target machine

Linux System z server requirements

The Tivoli Storage Manager V5.5 server on Linux for System z is supported at these versions (64 bit only):

- Red Hat Enterprise Linux 4 and 5
- SUSE Linux Enterprise Server 9 and 10
- V2.3.3 or later of the GNU C libraries

Linux on POWER server requirements

The Tivoli Storage Manager V5.5 server on Linux IBM System p and IBM System i is supported at:

- Red Hat Enterprise Linux 4 and 5
- SUSE Linux Enterprise Server 9 and 10
- Asianux 2.0 - Red Flag DC 5.0 and Haansoft Linux 2006 or Asianux 3.0
- V2.3.3 or later of the GNU C libraries installed on the target machine

18.1.5 Solaris server requirements for Tivoli Storage Manager

In this section we list the Solaris server requirements for Tivoli Storage Manager.

Solaris SPARC server requirements

The Tivoli Storage Manager V5.5 server on Solaris SPARC is supported at:

- Solaris 9 64 bit
- Solaris 10 64 bit

Solaris x86_64 server requirements

The Tivoli Storage Manager V5.5 server on Solaris x86_64 is supported at Solaris 10 64 bit.

18.1.6 Windows server requirements for Tivoli Storage Manager

The Tivoli Storage Manager V5.5 server on Windows is supported at:

- Windows Server 2003 (Standard, Enterprise, or Datacenter) Edition
- Windows Server 2003 SP1 (Enterprise or Datacenter) Edition 64 bit
- Windows Server 2003 (Standard, Enterprise, or Datacenter) x64 Edition

> **Notes:** Windows Storage Server versions are supported.
>
> All service packs are supported, including R2.
>
> Windows 2000 Server is supported on the Tivoli Storage Manager V5.3 server.

18.1.7 z/OS server requirements for Tivoli Storage Manager

The Tivoli Storage Manager V5.5 server on z/OS is supported at:

- z/OS V1R7
- z/OS V1R8 or later

18.2 Special device considerations

Refer to the following Web site for a list of devices that are currently supported by Tivoli Storage Manager (5608-ISM) and for those that are supported by Tivoli Storage Manager Extended Edition (5608-ISX). Libraries that have more than four drives or more than 48 tape slots require the Extended Edition license. This has been changed since Version 5.3, where the requirements were greater than three drives or 40 slots for Tivoli Storage Manager Extended Edition:

http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliStorageManager.html

In addition, this Web site provides access to a knowledge base of solutions, hints and tips, technical notes, readme files, product fixes and refreshes, product documentation, and more. This knowledge database is located under Self Help.

Specifically, detailed current device support for AIX, HP, Solaris, and Windows can be found at:

http://www.ibm.com/software/sysmgmt/products/support/IBM_TSM_Supported_Devices_for_AIXHPSUNWIN.html

Detailed current device support for Linux can be found at:

http://www.ibm.com/software/sysmgmt/products/support/IBM_TSM_Supported_Devices_for_Linux.html

For a summary of new devices supported as of V5.5, use the announcement letter, or the specific readme files found at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v1r1/topic/com.ibm.itsmreadme.doc_5.5/relnote_devices550.html

Driver recommendations

The driver recommendations are:

- We highly recommend that tape drives and tape libraries are connected to the system on their own Host Bus Adapter, which is not shared with other device types (for example, disk).
- The StorPort driver is supported on Windows 2003. Microsoft Hot Fix 901371 is required.
- On Sun Solaris, disable or configure the Volume Management daemon (vold).
- We recommend Emulex HBA driver Version 6.02f or later for Sun Solaris SPARC.

New device support

Tivoli Storage Manager V5.5 includes HP LTO-4 drive encryption with AIX, HP-UX, Linux, Solaris, and Windows, unless indicated otherwise.

18.3 New functionality

Here is a summary of the new functionality in Tivoli Storage Manager V5.5 that is not expanded on elsewhere in this book.

18.3.1 Virtual Tape Library (VTL) in SAN device mapping for SAN discovery

In a SAN environment, device IDs can change dynamically (for example, device or cabling changes). Tivoli Storage Manager uses a method that dynamically discovers and maps devices in the environment, even when the paths change. Tivoli Storage Manager V5.5 is enhanced to allow for the mapping and discovery of VTL (IBM TS7520) devices in the SAN.

18.3.2 IPv6 support

Tivoli Storage Manager is now able to use TCP/IP Version 6 (IPv6) as its communications protocol for AIX, HP-UX, Linux, Sun Solaris, and Windows systems. The COMMMETHOD option specifies a communication method to be used by the server. You can specify multiple COMMMETHOD options in the server options file.

Internet Protocol V6 is the next generation protocol designed to replace the current version, Internet Protocol V4 (IPv4). IPv6 is interoperable with TCP/IP Version 4. You can specify either IPv4 or both IPv4 and IPv6 in the COMMMETHOD option when you start the server, storage agent, client, or API application. The same port numbers are used by the server, storage agent, client, or API application for both IPv4 and IPv6.

There are some restrictions with the new version. Refer to *IBM Tivoli Storage Manager Administrator's Reference V5.5* and *IBM Tivoli Storage Manager Backup-Archive Clients Installation and User's Guide V5.5*, for further details.

V6TCPIP specifies the TCP/IP communication method option. If TCP/IP Version 4 and Version 6 are both configured, Tivoli Storage Manager uses both protocols simultaneously. If both COMMMETHOD TCPIP and COMMMETHOD V6TCPIP are specified, V6TCPIP overrides the specification of TCPIP. A valid domain name server (DNS) environment must be present to use either TCP/IP Version 4 or TCP/IP Version 6 if this option is specified.

IPv6 address formats are acceptable for all functions that support IPv6. However, if you use IPv6 addresses for functions that do not support IPv6, communications will fail.

- NDMP: backing up and restoring storage pools, copying and moving data (continue to use IPv4)
- ACSLS (Continue to use IPv4.)
- SNMP (Continue to use IPv4.)
- Centera device support (coContinuentinue to use IPv4.)
- Shared Memory Protocol (Continue to use IPv4.)
- Windows Microsoft Management Console functions (Continue to use IPv4.)
- Tivoli Enterprise Console® (TEC) support
- Administration Center (Continue to use IPv4.)

The server and storage agent use COMMMETHOD V6TCPIP to specify support for both IPv4 and IPv6 simultaneously, depending on the protocols configured on the system on which the server or storage agent are running. As in prior releases, COMMMETHOD TCPIP specifies that only IPv4 is used. When configuring the storage agent using the DSMSTA SETSTORAGESERVER command, use addresses that correspond to the communications method used by the backup-archive client. The backup-archive client supports either IPv4 (COMMMETHOD TCPIP) or IPv6 (COMMMETHOD V6TCPIP), but not both at the same time. Other client components (CAD, Web Client) use COMMMETHOD V6TCPIP to support both IPv4 and IPv6 simultaneously.

18.4 Administration Center requirements

For a summary of Administration Center requirements as of V5.5, use the announcement letter and the specific readme file found at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v1r1/topic/com.ibm.itsmreadme.doc_5.5/relnote_adminctr550.html

18.4.1 Administration Center introduction

The Administration Center is a Web-based interface that can be used to centrally configure and manage IBM Tivoli Storage Manager servers. It provides wizards to help guide you through common configuration tasks.

The Administration Center is installed as an IBM Integrated Solutions Console component. The Integrated Solutions Console allows you to install components provided by multiple IBM applications and access them from a single interface.

Backward compatibility

In order to administer Tivoli Storage Manager servers V5.5 and later, you must install or upgrade to the Tivoli Storage Manager Administration Center V5.5.

The Tivoli Storage Manager Administration Center V5.5 is compatible with the Integrated Solutions Console V6.0.1.1. You do not need to reinstall the Integrated Solutions Console if you already have V6.0.1.1 installed.

If you are upgrading from a previous release, consider the following:

- Upgrade from Tivoli Storage Manager V5.3.

  The Integrated Solutions Console needs to be upgraded from V6.0.1.0 to V6.0.1.1 and the Administration Center upgraded from V5.3 to V5.5.

- Upgrade from Tivoli Storage Manager V5.4.

  The Integrated Solutions Console V6.0.1.1 should already be installed. Upgrade the Administration Center to V5.5.

With Tivoli Storage Manager Administration Center, the Integrated Solutions Console is a basic component and will be included with the installation media. For additional information about Integrated Solutions Console see:

http://www.ibm.com/developerworks/autonomic/csa.html?S_TACT=105AGX09&S_CMP=LP

18.4.2 Administration Center system requirements

Detailed hardware and software requirements for the Administration Center can be found in Technote 1195062, at:

http://www-1.ibm.com/support/docview.wss?uid=swg21195062

Web interface

The Tivoli Storage Manager Administration Center Web interface for the server and a Web client interface for client machines require a Java Swing-capable (at JRE 1.4.2) Web browser:

- MS Internet Explorer 6.0 or later with Java Plug-in 1.4.2
- Mozilla 1.6 or later

You must have the 32-bit version of IBM or Sun Java™ Version 1.4.2 or later installed on your system. Do not use a 64-bit Java Runtime Environment. The directory where the Java executable files are installed must be included in your PATH environment variable.

Refer to the backup-archive client requirements section for the specific operating system levels supported for the Web clients. TCP/IP is the only communication protocol supported for this client interface.

For the latest recommendation on the Administration Center installation, use keyword TSMADMINCENTER when you visit:

http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliStorageManager.html

General system requirements

The machine hosting the Administration Center and Integrated Solutions Console requires the following:

- To install the console on a system for the first time, the user needs 982 MB to satisfy the installation program disk space and an additional 300 MB of temporary space.
- To update an installation that already has Integrated Solutions Console (ISC) V6.0.1 installed from previous versions of the Administration Center, the user needs 400 MB of installation program disk space and 225 MB of temporary space.
- 500 MB for the completed installation.
- Virtual memory/swap space: equal to double the system's physical memory. At a minimum, this should be at least equal to the system's physical virtual memory.
- Network connectivity: To use the console across a network, the following items are required for the machine:
  - Network adapter and connection to a physical network that can carry IP packets, for example, Ethernet
  - Static IP address
  - Configured fully qualified host name

    Integrated Solutions Console must be able to resolve an IP address from its fully qualified host name.

System-specific requirements

The Tivoli Storage Manager Administration Center server requires the following hardware and software:

- AIX server
  - AIX V5.1 with ML4, AIX V5.2 with ML1 + APAR IY44183, AIX V5.3 with ML1, or AIX V6.1
  - Processor: Power4 450 MHz at a minimum. Production environments should consider higher speeds.
  - Physical memory: 512 MB or more.

- Windows server
  - Windows 2000 (Professional, Server, or Advanced Server) with SP4, Windows XP, Windows Server 2003 (Standard, Enterprise, or Datacenter) Edition.
  - Processor: CPU speeds of late model. Midrange to high-end servers are recommended. Pentium 800 MHz or equivalent at a minimum. Production environments should consider the Pentium 4 processor at 1.4 GHz or more.
  - Physical memory: 512 MB or more.
  - File system: The NTFS file system is recommended.
- Linux server
  - SUSE Linux Enterprise Server (SLES) 8, SUSE Linux Enterprise Server (SLES) 9, Linux Enterprise Server (SLES) 10, Red Hat Enterprise Linux 3 Update 3, Red Hat Enterprise Linux 4, or Red Hat Linux Enterprise 5.
  - Processor: CPU speeds of late model. Midrange to high-end servers are recommended. Pentium 800 MHz or equivalent at a minimum. Production environments should consider the Pentium 4 processor at 1.4 GHz or more.
  - Processor: Power4 450 MHz at a minimum. production environments should consider higher speeds.
  - Processor: Any IBM System z processor.
  - Physical memory: 512 MB or more.
- Solaris server
  - Solaris 8, 9, or 10.
  - Processor: Ultra 60 at 450 MHz at a minimum. Sun Blade 2000 workstation at 1 GHz or more is recommended.
  - Physical memory: 512 MB or more.

The machine hosting the Tivoli Storage Manager Administration Center server can be the same machine as the Tivoli Storage Manager server if it meets the requirements for both servers. In this case, the physical memory requirements must be added for both servers.

18.5 Servers not migrated to V5.5

The following Tivoli Storage Manager server operating systems, supported in V5.4, were not migrated to V5.5 and are not supported in V5.5:

- z/OS V1R4, V1R5, and V1R6
- HP-UX 11i V1 and HP-UX 32 bit, all versions
- AIX V5.1 and AIX 32 bit, all versions
- Solaris 8
- Red Hat Enterprise Linux Server 3
- SLES 8
- Red Flag 4.1/Asianux 1.0
- Windows 2000

19

IMPORT and EXPORT commands

This chapter provides information about enhancements to the Tivoli Storage Manager server import and export commands in V5.5.

Tivoli Storage Manager can export data, policy settings, and other information to sequential media (for example, tapes or files) or directly to other Tivoli Storage Manager servers over an appropriate network connection.

The main improvements to the import/export functions are:

- Suspend and resume features allow a *server-to-server export* to be suspended and restarted.
- FROMTime and FROMDate / TOTime and TODate functions allow the administrator to specify a window of time from which the exported data will come.

To demonstrate the new functions, we set up server-to-server communication, and we also describe some differences in previewing the export.

For more information about import/export, see the *Tivoli Storage Manager Administration Guide* for your Tivoli Storage Manager Server, available at:

http://publib.boulder.ibm.com/infocenter/tivihelp

19.1 Our example environment

We have two Tivoli Storage Manager servers: one running on AIX called KODIAK and another running on Windows called HAGGIS. As shown in Figure 19-1, HAGGIS has a number of clients that have been backing up to it. We show how to use various export commands, including EXPORT NODE, with this data.

- HAGGIS is located at site A and has IP address 9.43.86.84.
- KODIAK is located at site B and has IP address 9.43.86.50.
- Site B is physically located far enough away from site A to be used as a disaster recovery location.

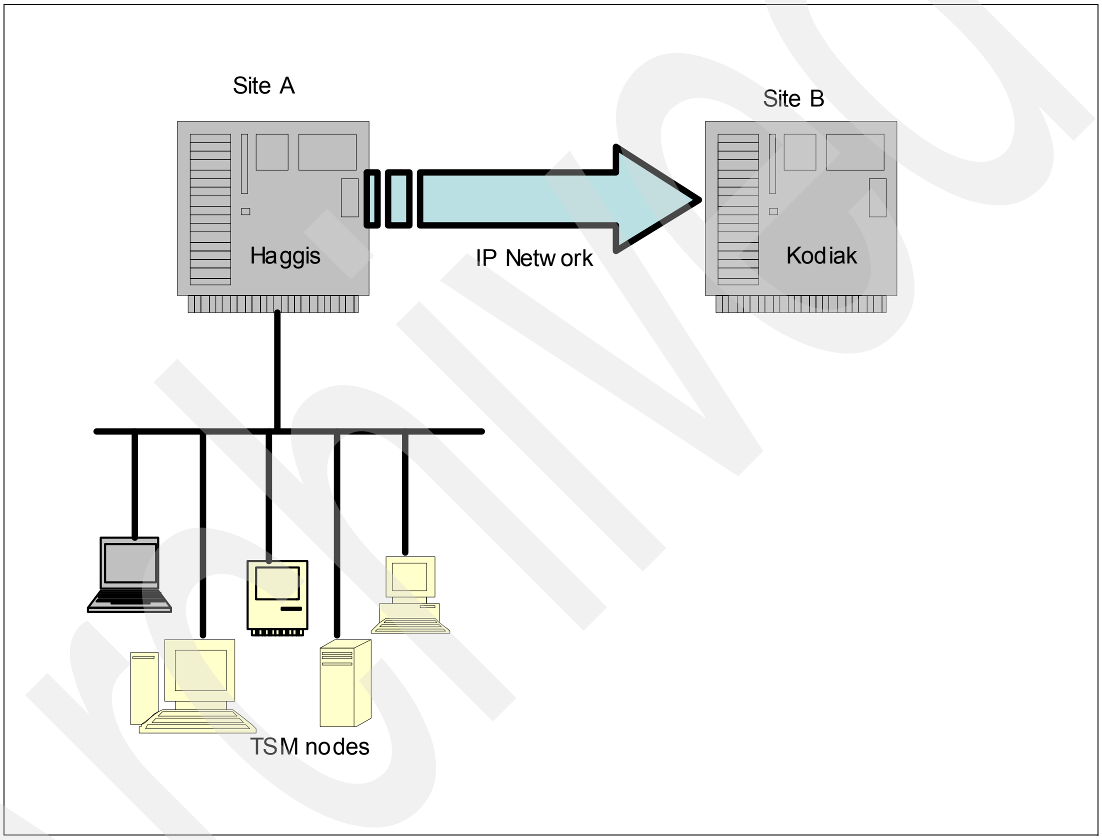


Figure 19-1 ITSO demo environment used to show export operations

Setting up server-to-server communications is a prerequisite to doing direct server-to-server export. We start with this configuration.

19.2 Setting up server-to-server communications

To set up sever-to-server communications:

1. We first need to make sure the internal server configuration is correct using the standard SET SERVER commands. This configuration includes a unique server name, the high and low level addresses (the IP address and port number), and a server password. We also allow cross-definition of servers. Example 19-1 on page 251 and Example 19-2 on page 251 show these commands on HAGGIS and KODIAK, respectively.

Example 19-1 Set up HAGGIS for server-to-server communication

```
set servername haggis
set serverpassword xxxx
set serverhladdress 9.43.86.84
set serverlladdress 1500
set crossdefine on
```

Example 19-2 Set up KODIAK for server-to-server communication

```
set servername kodiak
set serverpassword yyyy
set serverhladdress 9.43.86.50
set serverlladdress 1500
set crossdefine on
```

2. We define each server to each other. By using the CROSSDEFINE option in Example 19-3, when we define the server KODIAK on HAGGIS, an equivalent server object for HAGGIS is automatically created on KODIAK. This is shown in Example 19-4.

Example 19-3 Establishing server definitions on our two servers

```
tsm: HAGGIS>define server kodiak serverpassword=yyyy hladdress=9.43.86.50
lladdress=1500 description="Kodiak AIX TSM Server" crossdefine=yes
tsm: HAGGIS>query server
Server   Comm.  High-level    Low-level   Days Server   Virtual  Allow
Name     Method Address       Address    Since Password Volume   Replacement
                                          Last Set      Password
                                        Access          Set
-------- ------ ------------- --------- ------ -------- -------- -----------
KODIAK   TCPIP  9.43.86.50    1500          <1 Yes      No       No
```

Example 19-4 Server definition for HAGGIS created on KODIAK

```
tsm: KODIAK>query server
Server   Comm.  High-level    Low-level   Days Server   Virtual  Allow
Name     Method Address       Address    Since Password Volume   Replacement
                                          Last Set      Password
                                        Access          Set
-------- ------ ------------- --------- ------ -------- -------- -----------
HAGGIS   TCPIP  9.43.86.84    1500           1 Yes      Yes      No
```

19.3 Exporting a node

In this example we export one of HAGGIS's client nodes, MENSA, to KODIAK. MENSA has stored approximately 6 GB of backup data into storage pools on HAGGIS.

Initially, we use the command EXPORT NODE MENSA FILEDATA=ALL TOSERVER=KODIAK, as shown in Example 19-5 on page 252. In running the export this way, we are accepting a number of defaults. We cover these later in the chapter, along with some alternative settings. The process starts in the background and proceeds to copy MENSA's data to KODIAK. Note the export identifier—EXPORT_NODE_44 in this case.

You can specify your own export identifier using the parameter EXPORTIDentifier=<*name-for-export-process*>.

Example 19-5 Simple export node command

```
tsm: HAGGIS>export node mensa filedata=all toserver=kodiak
ANR0654I Restartable export command with export identifier EXPORT_NODE_44
started as process 44.
ANS8003I Process number 44 started.
tsm: HAGGIS>query process
Process Process Description  Status
  Number
-------- -------------------- -------------------------------------------------
      44 EXPORT NODE          ANR1358I Export Identifier: EXPORT_NODE_44
                               ANR0648I Have copied the following: 1 Nodes  2
                               Filespaces  2804 Backup Files  203659656 Bytes
                               (0 errors have been detected).
```

19.3.1 Suspend and resume an export between servers

An export process between two Tivoli Storage Manager servers at V5.5 can be paused and restarted. This is known as the *restartable export* capability, and is particularly useful for lengthy export jobs that could otherwise interfere with normal server operations. Only server-to-server exports are restartable. Exports to sequential media cannot be suspended.

The Tivoli Storage Manager V5.5 commands that control restartable export features are:

- SUSPEND EXPORT
  - This command is run on the source server (HAGGIS in our example) and takes the export identifier as a parameter. The export identifier is a unique identifier for each export job, which is displayed in the QUERY PROCESS output, as in Example 19-5. We suspend the export that we just started in Example 19-6. Note that the process no longer appears in the QUERY PROCESS output after the suspend.

Example 19-6 Suspend export

```
tsm: HAGGIS>suspend export EXPORT_NODE_44
ANR1372I Suspend export request accepted for export process with export
Identifier EXPORT_NODE_44 ( process 44).
tsm: HAGGIS>query process
ANR0944E QUERY PROCESS: No active processes found.
ANS8001I Return code 11.
tsm: HAGGIS>
```

- – You can suspend an EXPORT NODE or an EXPORT SERVER command where FILEDATA is set to a value other than NONE. EXPORT POLICY and EXPORT ADMIN commands are not restartable, and in any case, would not normally run long enough to have any need to be suspended.
- – A suspended export remains paused until resumed, even if the Tivoli Storage Manager server is restarted or rebooted. To terminate a suspended export, either cancel the export (see CANCEL EXPORT below) or restart the export and cancel the resulting process.

- QUERY EXPORT

  This allows the Tivoli Storage Manager Server administrator to view running and suspended export processes, as shown in Example 19-7 on page 253. Note that the process number is blank, as this export has been suspended. However, we can still identify the export using the export identifier.

Example 19-7 Query export processes

```
tsm: HAGGIS>query export
Export identifier: EXPORT_NODE_44
       Start date: 12/04/2007 10:40:28
           Status: Suspended
   Process number:
          Command: EXPORT NODE mensa filedata=all
                    toserver=kodiak
```

- RESTART EXPORT

  This resumes previously suspended exports. An export could have been explicitly suspended (via the SUSPEND EXPORT command) or suspended because of an error. The QUERY PROCESS output shows all suspended exports that can be restarted.

  You can specify an individual export identifier, as shown in Example 19-8, or you can resume all suspended exports with RESTART EXPORT *. Note that a new process number (46 in this example) is assigned, and that the export now has a status of *running*.

Example 19-8 Restart the export

```
tsm: HAGGIS>restart export EXPORT_NODE_44
ANR0654I Restartable export command with export
identifier EXPORT_NODE_44 started as process 46.
ANS8003I Process number 46 started.
tsm: HAGGIS>query export
Export identifier: EXPORT_NODE_44
       Start date: 12/04/2007 10:40:28
           Status: Running
   Process number: 46
          Command: EXPORT NODE mensa filedata=all
                    toserver=kodiak
```

Note: An export operation is suspended when any of the following occurs:

- A SUSPEND EXPORT command is issued for the running export operation.
- Segment preemption - The file being read for export is deleted by some other process.
- There are communication errors on a server-to-server export.
- There are no available mount points.
- The necessary volumes are unavailable.
- I/O errors are encountered.

- CANCEL EXPORT

  This cancels suspended exports. Specify the export using the export identifier, as shown in Example 19-9.

Example 19-9 Cancel a suspended export

```
tsm: HAGGIS>cancel export EXPORT_NODE_44
ANR1371I CANCEL EXPORT: The export operation with export identifier
EXPORT_NODE_44 has been deleted.>
```

19.3.2 Previewing your exports

When exporting data, it is often helpful to know how much data is going to be exported in order to get a feel for how long it will take or to know how much free space is required on the target server. There are two preview modes available, which may look similar from the command line but actually behave quite differently:

- EXPORT with the PREVIEW parameter when the export is to sequential media.
- EXPORT with the PREVIEWIMPORT parameter when the export is to another Tivoli Storage Manager server, that is, for the EXPORT NODE and EXPORT SERVER commands.

Regardless of the type of preview used, no data is actually imported or written.

PREVIEW=YES

Even if your Tivoli Storage Manager server has no spare tape or disk resources for exporting data because you are planning a direct server-to-server export, you may still wish to use the sequential media version of the preview, since this uses up no bandwidth or data storage space outside the Tivoli Storage Manager database of the source server.

If you have no device class to export your data to, you can set up a dummy device class for the data destination. Since this is only going to be used as a preview, nothing will be written. Example 19-10 shows an example of using a dummy sequential device class defined on the C: drive. Note that no data has been moved.

Example 19-10 Export to sequential media, PREVIEW=YES

```
tsm: HAGGIS>define devclass dummy devtype=file directory=c:
ANR2203I Device class DUMMY defined.
tsm: HAGGIS>export node mensa filedata=all devclass=dummy preview=yes
ANR0609I EXPORT NODE started as process 27.
ANS8003I Process number 27 started.
```

```
tsm: HAGGIS>query actlog begintime=-00:03
ANR2017I Administrator ADMIN issued command: EXPORT NODE mensa filedata=all
devclass=dummy preview=yes
ANR0984I Process 27 for EXPORT NODE started in the BACKGROUND at 11:38:17.
ANR0609I EXPORT NODE started as process 27.
ANR0402I Session 238 started for administrator ADMIN (Server) (Memory IPC).
ANR0610I EXPORT NODE started by ADMIN as process 27.
ANR0635I EXPORT NODE: Processing node MENSA in domain STANDARD.
ANR0637I EXPORT NODE: Processing file space \\mensa\c$ for node MENSA fsId 1 .
ANR0637I EXPORT NODE: Processing file space \\mensa\e$ for node MENSA fsId 2 .
ANR0616I EXPORT NODE: Preview processing completed successfully.
ANR0626I EXPORT NODE: Copied 1 node definitions.
ANR0627I EXPORT NODE: Copied 2 file spaces 0 archive files, 24850 backup files,
and 0 space managed files.
ANR0630I EXPORT NODE: Copied 6143636 kilobytes of data.
ANR0611I EXPORT NODE started by ADMIN as process 27 has ended.
ANR0986I Process 27 for EXPORT NODE running in the BACKGROUND processed 24853
items for a total of 6,291,083,327 bytes with a completion state of SUCCESS at
11:38:20.
```

PREVIEWIMPORT=YES

With a server-to-server export, you can do a similar preview using the parameter PREVIEWIMPORT=YES. This preview does every activity of the export except the actual writing of data on the target node. Accordingly, this sort of preview usually takes much longer, since each byte of data must be read from the source Tivoli Storage Manager server's storage, then written across the network between the Tivoli Storage Manager servers. If bandwidth is not expected to be a problem, it may still be impractical for anything other than small export previews.

Note: Although the server-to-server preview mode PREVIEWIMPORT=YES does not *store* any data on the target server, it *does* write all the data over the network to the target server, and in order to do that it must read all the data from the storage pools of the source server. This can take a long time.

For this reason, we recommend that you test with smaller nodes. If network bandwidth is limited, or if you have a lot of data to move and do not have the time available to transfer all the data, you should avoid using PREVIEWIMPORT=YES.

19.3.3 Exporting shreddable data

For details on shredding see 8.1, "What is data shredding" on page 90.

If some or all of the exported data is stored in a shreddable storagepool, you must use the parameter ALLOWSHREDDABLE=YES to allow the export of these data. The default NO specifies that the server does not allow data to be exported from a storage pool that enforces shredding.

Note: When shreddable data is exported, the data on the export media will not be shredded, and should be protected accordingly. Data shredding is currently only available for random-access media.

19.4 Specifying point-in-time export

The FROMDATE and FROMTIME parameters for the EXPORT SERVER and EXPORT NODE commands have been available since V5.1, to export data based on the date and time that the objects were originally stored in the server. These parameters define a starting point in time for the export, and only apply to client user file data. There is no effect on other exported information such as policy. V5.5 adds TODATE and TOTIME parameters to set an end point and a time interval for an export operation so that you can effectively create a time window for data objects to be exported.

With Tivoli Storage Manager V5.5, the EXPORT NODE and EXPORT SERVER commands selectively allow export data from within a window of time. Incremental exports defining a starting point in time for the export have been available since V5.1, and this is now enhanced to also set the end point, effectively creating a time window for data objects that will be exported.

Suppose that you have a node that has been backing up using normal daily incremental backups. You can choose to only export the objects that were backed up on a given day or set of days.

With these parameters you will export the currently available backup, but not necessarily export the exact state of the exported data at the time of the specified TODATE/TOTIME. Some objects inserted prior to the TODATE/TOTIME may have been deactivated after the TODATE and other objects may have expired or may have been corrupted or deleted after the specified TODATE and no longer exist.

Without the TODATE/TOTIME/FROMDATE/FROMTIME parameters, all objects are eligible for export regardless of the insertion date. Grouped objects (for example, groups of objects related to one file backed up using subfile backup) are also unaffected by these parameters. All grouped objects are exported regardless of the parameter values.

The new parameters TODATE/TOTIME provide the ability to select data for an export operation using a range of time. Some sites may want to isolate a subset of data by time and manage it differently. The data can be exported to another server where it can be accessed and managed by a unique policy to preserve the data for as long as it is needed.

With the capability to export a time range of data the user can also easily split up the data chronologically by performing several export operations with a specified time range. Large export processes that otherwise could take many hours or even days can now be split up into smaller tasks and better scheduled together with other backup processes. The restartable export capability also clearly plays an important role here. See 19.3.1, “Suspend and resume an export between servers” on page 252.

As an example of this functionality, consider node MENSA. It includes a single file system (E drive) included for backup, with 13 files on it. Our Tivoli Storage Manager server (host name LOCHNESE, server name HAGGIS) with NOLIMITS for version retention in the backup copygroup used by MENSA.

1. We do five (selective) backups of this drive, one after another, separated by a minute each, as shown in Example 19-11 (we have reduced the summary to just the relevant information for this example). Each of these backups stores 13 files and the directory they reside in, so a total of 14 objects.

Example 19-11 Creating our test environment: performing backups

```
C:\Program Files\Tivoli\TSM\baclient>dsmc sel -subdir=y e:\itsovm1\*
Server date/time: 12/13/2007 13:13:56  Last access: 12/13/2007 13:13:06
Total number of objects backed up:       14
Elapsed processing time:           00:02:25
C:\Program Files\Tivoli\TSM\baclient>dsmc sel -subdir=y e:\itsovm1\*
Server date/time: 12/13/2007 13:18:05  Last access: 12/13/2007 13:13:56
Total number of objects inspected:       14
Elapsed processing time:           00:02:23
C:\Program Files\Tivoli\TSM\baclient>dsmc sel -subdir=y e:\itsovm1\*
Server date/time: 12/13/2007 13:21:35  Last access: 12/13/2007 13:18:05
Total number of objects backed up:       14
Elapsed processing time:           00:02:25
C:\Program Files\Tivoli\TSM\baclient>dsmc sel -subdir=y e:\itsovm1\*
Server date/time: 12/13/2007 13:26:01  Last access: 12/13/2007 13:21:35
Total number of objects backed up:       14
Elapsed processing time:           00:02:23
C:\Program Files\Tivoli\TSM\baclient>dsmc sel -subdir=y e:\itsovm1\*
Server date/time: 12/13/2007 13:29:46  Last access: 12/13/2007 13:26:01
Total number of objects backed up:       14
Elapsed processing time:           00:02:26
```

2. We can now demonstrate the ability to export a subset of MENSA's data to another Tivoli Storage Manager server. We have a target server set up called KODIAK the same policy settings in the standard domain as HAGGIS. We export the node using server to server, being careful to export from a time just before and just after the objects that we want to export were backed up, as shown in Example 19-12. As you can see, we supply times that are relevant to the insert time (that is, the time that the objects were inserted into the Tivoli Storage Manager database during the backup). Our FROMTIME is one second before the backup we are interested in started, and our TOTIME is approximately 34 seconds after it completed.

Example 19-12 Export a subset of a node's data using fromtime and totime

```
tsm: HAGGIS>export node mensa filedata=all toserver=kodiak fromdate=today
fromtime=13:21:34 todate=today totime=13:24:34
ANR0654I Restartable export command with export identifier EXPORT_NODE_28 started
as process 28.
ANS8003I Process number 28 started.
```

3. The process now proceeds to export the relevant data. Example 19-13 shows the activity log for the target server KODIAK.

Example 19-13 Server activity log during EXPORT NODE command from HAGGIS

```
ANR0984I Process 188 for IMPORT (from Server HAGGIS) started in the BACKGROUND at
13:37:00.
ANR4711I IMPORT SERVER (DATES=ABSOLUTE REPLACEDEFS=NO MERGE=NO PREVIEW=NO) by
administrator ADMIN from server HAGGIS (Process 28) starting as process 188.
ANR0402I Session 505 started for administrator ADMIN (Server) (Memory IPC).
ANR0610I IMPORT (from Server HAGGIS) started by ADMIN as process 188.
ANR0615I IMPORT (from Server HAGGIS): Reading EXPORT NODE data from server HAGGIS
exported 12/13/07 13:36:02.
ANR0635I IMPORT (from Server HAGGIS): Processing node MENSA in domain STANDARD.
ANR2147E REGISTER NODE: Node MENSA is already registered.
ANR0636I IMPORT (from Server HAGGIS): Processing file space \\mensa\e$ for node
MENSA as file space \\mensa\e$.
ANR0617I IMPORT (from Server HAGGIS): Processing completed with status SUCCESS.
ANR0620I IMPORT (from Server HAGGIS): Copied 0 domain(s).
ANR0621I IMPORT (from Server HAGGIS): Copied 0 policy sets.
ANR0622I IMPORT (from Server HAGGIS): Copied 0 management classes.
ANR0623I IMPORT (from Server HAGGIS): Copied 0 copy groups.
ANR0624I IMPORT (from Server HAGGIS): Copied 0 schedules.
ANR0625I IMPORT (from Server HAGGIS): Copied 0 administrators.
ANR0891I IMPORT (from Server HAGGIS): Copied 0 optionset definitions.
ANR0626I IMPORT (from Server HAGGIS): Copied 0 node definitions.
ANR0627I IMPORT (from Server HAGGIS): Copied 1 file spaces 0 archive files, 18
backup files, and 0 space managed files.
ANR0629I IMPORT (from Server HAGGIS): Copied 1521761312 bytes of data.
ANR0611I IMPORT (from Server HAGGIS) started by ADMIN as process 188 has ended.
ANR0986I Process 188 for IMPORT (from Server HAGGIS) running in the BACKGROUND
processed 19 items for a total of 1,521,761,312 bytes with a completion state of
SUCCESS at 13:39:09.
```

The number of backup files is listed as 18. This is actually the 13 files and their data and five versions of the directory entry (one active and four inactive, from the five backups).

Note: EXPORT NODE does not respect FROMTIME/FROMDATE and TOTIME/TODATE for group objects such as subfile backups. If you are exporting client data that was backed up using subfile backup, the export may consist of more data than just the particular backup that you want to export. This is so that when an object is not complete without another part of the group, it is exported fully and properly.

20

Other server enhancements

This chapter discusses enhancements made to storage pools using the FILE device type. The changes allow for:

- Efficient use of sequential storage pools on disk
- Parallel volume access for read operations

We also provide a section on an enhancements to the QUERY LIBVOLUME command.

20.1 Migration thresholds for sequential disk

Before Tivoli Storage Manager V5.5, sequential migration thresholds are derived based upon individual volume usage and do not consider the overall utilization of the storage pool. This method works very well for sequential access media such as tapes, but has limitations when using the FILE device class for sequential operations.

A FILE device utilizes random access technology (disk) and has different characteristics than other sequential-access media. Per-volume usage is not as important as overall pool usage. FILE pools are constrained more by overall disk capacity than by the number of volumes available.

The migration threshold mechanism for FILE storage pools now considers overall pool utilization instead of individual volume/file utilization. In other words, this change makes FILE pools more like DISK pools when it comes to migration.

You can see this change by looking at the output of the QUERY STORAGEPOOL command.

To illustrate the changes we run through the following scenario:

1. We define device class CFILECLASS with a maximum capacity value of 100 MB. Primary storage pool CPOOL is configured using this device class, allowing 10 scratch volumes to be used. Client node NODE1 is configured to a domain using the CPOOL as the target destination. We run a backup as shown in Example 20-1.

Example 20-1 500MB backup

```
Total number of objects inspected:      507
Total number of objects backed up:      507
Total number of objects updated:          0
Total number of objects rebound:          0
Total number of objects deleted:          0
Total number of objects expired:          0
Total number of objects failed:           0
Total number of subfile objects:          0
Total number of bytes transferred:   502.20 MB
Data transfer time:                    6.87 sec
Network data transfer rate:        74,823.06 KB/sec
Aggregate data transfer rate:      51,992.61 KB/sec
Objects compressed by:                    0%
Subfile objects reduced by:               0%
Elapsed processing time:           00:00:09
```

2. Example 20-2 shows the volume information output immediately after the backup.

Example 20-2 Q VOLUME output after backup at V5.5

```
tsm: LOCHNESE>Q VOL DEVC=CFILECLASS

Volume Name                Storage      Device      Estimated    Pct   Volume
                           Pool Name    Class Name   Capacity   Util   Status
------------------------   -----------  ----------  ---------  -----  -------
C:\TSMDATA\SERVER1\CFIL-   CPOOL        CFILECLASS       99.1  100.0    Full
 ECLASS\000009CB.BFS
C:\TSMDATA\SERVER1\CFIL-   CPOOL        CFILECLASS       99.1  100.0    Full
 ECLASS\000009CC.BFS
C:\TSMDATA\SERVER1\CFIL-   CPOOL        CFILECLASS       99.1  100.0    Full
```

```
 ECLASS\000009CD.BFS
C:\TSMDATA\SERVER1\CFIL-  CPOOL       CFILECLASS      99.1  100.0    Full
 ECLASS\000009CE.BFS
C:\TSMDATA\SERVER1\CFIL-  CPOOL       CFILECLASS      99.1  100.0    Full
 ECLASS\000009CF.BFS
C:\TSMDATA\SERVER1\CFIL-  CPOOL       CFILECLASS     100.0    7.1  Filling
 ECLASS\000009D0.BFS
```

3. Now let us look at the Pct Migr field from a QUERY STORAGEPOOL command.
    a. On a pre-V5.5 server for a file device type storage pool, we see the percentage of the total number of volumes that have data, as shown in Example 20-3.

Example 20-3 Q STG output based on used volumes, pre 5.5

```
tsm: LOCHNESE>Q STG CPOOL

Storage      Device       Estimated    Pct    Pct  High  Low  Next Stora-
Pool Name    Class Name    Capacity   Util   Migr   Mig  Mig  ge Pool
                                                    Pct  Pct
-----------  ----------  ----------  -----  -----  ----  ---  -----------
CPOOL        CFILECLASS     995.3 M   50.5   60.0    90   70  EPOOL
```

    b. With Tivoli Storage Manager server V5.5, the value in the Pct Migr output field reflects the percentage of migratable data instead. This is shown in Example 20-4.

Example 20-4 Q STG output based on percentage of migratable data

```
tsm: LOCHNESE>Q STG CPOOL

Storage      Device       Estimated    Pct    Pct  High  Low  Next Stora-
Pool Name    Class Name    Capacity   Util   Migr   Mig  Mig  ge Pool
                                                    Pct  Pct
-----------  ----------  ----------  -----  -----  ----  ---  -----------
CPOOL        CFILECLASS     995.3 M   50.5   50.5    90   70  EPOOL
```

The estimated capacity that is displayed for sequential access pools is typically a mean average of volume capacity times the total number of volumes available in the pool. For sequential access pools using TAPE devices this method is the best estimate of obtaining the capacity of the storage pool because the actual capacity of a TAPE is not known to the server until it is defined and has data on it.

With FILE pools, this is not the case. The server determines the capacity of the volumes to the storage pool and gives a more accurate estimate of the storage pool's capacity. If you define the FILE pool with more capacity (that is, using MAXSCRATCH) than resources are available in the file system, the server displays the capacity amount that is available in the file system.

With the example given above, the high-migration threshold is set to the default of 90%. In a pre-V5.5 environment, migration would not start until 90% of the number of volumes are in use. With V5.5, the migration starts when 90% of the occupancy of the storage pool is filled. This may cause unexpected problems if you do not realize that the pool now almost fills to 90% of the capacity before migration starts.

Summary

The new migration method provided for the FILE device storage pool allows you to set your migration thresholds considering overall use of your disk resources instead of the number of volumes being used.

20.2 Concurrent read access for sequential disk

Before Tivoli Storage Manager V5.5, a client session or server process had to wait for a FILE volume if the volume was in use by another session or process. At V5.5, multiple client sessions and server processes can access FILE volumes concurrently, which reduces or eliminates wait times for read access to FILE volumes.

No configuration changes are required to take advantage of the concurrent read access, however we recommend increasing the MAXNUMMP for nodes accessing FILE volumes. This allows for greater concurrency for node read operations, for example, when doing multi-threaded restores. In addition, make sure the MOUNTLIMIT parameter for the device class provides enough mount points for concurrent access.

Concurrent read access is not limited to client read operations but is also available for server internal operations that request volume read access, such as BACKUP STORAGEPOOL, AUDIT VOLUME, and others.

We use the following simple scenario to demonstrate defining NODE1 to NODE4, all belonging to a domain where the backup destination points to a FILE device storage pool, CPOOL. The mount limit for the device class is set to 10.

20.2.1 Behavior before Tivoli Storage Manager V5.5

Figure 20-1 demonstrates the serialized access to a FILE volume. This is the default behavior with a pre-V5.5 Tivoli Storage Manager server.

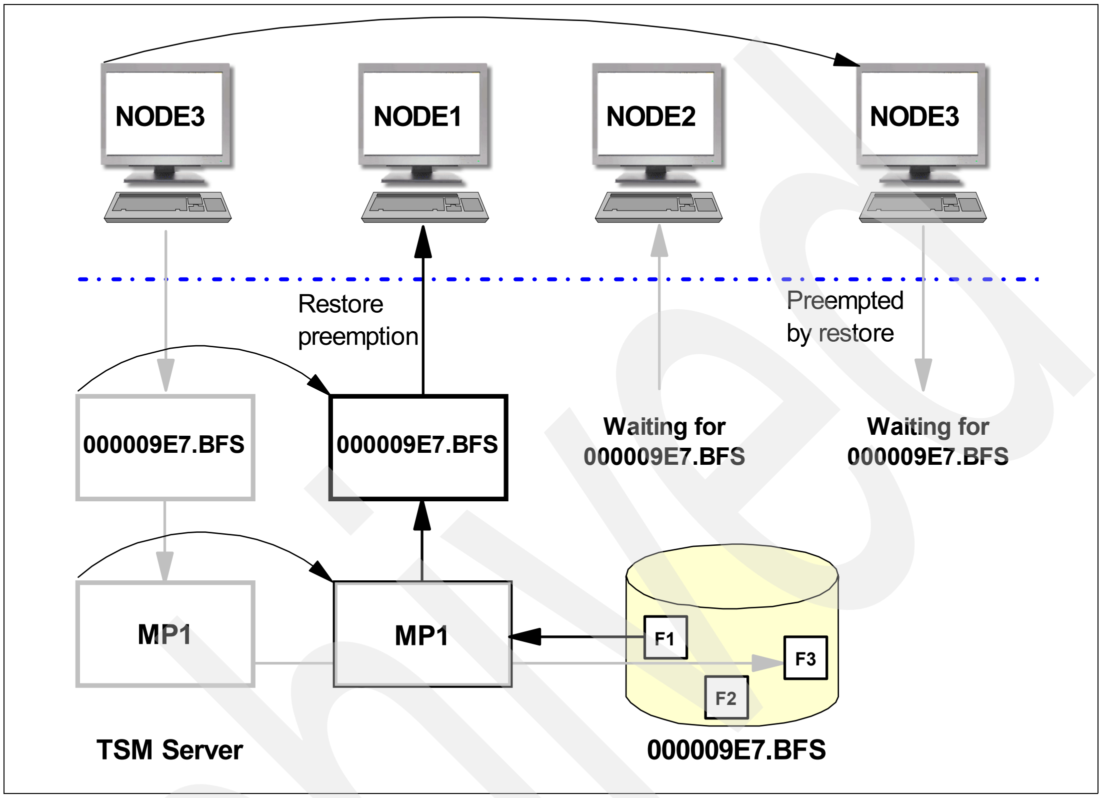


Figure 20-1 Serialized access to FILE volume and mount point preemption

NODE1 and NODE2 request a restore of their data that is backed up to the pool, while NODE3 is doing a backup. Earlier server versions do not allow for parallel access of FILE volumes, therefore the running backup session gets preempted by a restore request. The activity log reports the messages as shown with Example 20-5.

Example 20-5 Mount point preemption for FILE volume, pre-5.5 server

```
11/26/2007 15:46:04  ANR0494I Volume C:\TSMDATA\SERVER1\CFILECLASS\000009E7.BFS
                      in use. Session 7 for node NODE3 (WinNT) being preempted
                      by higher priority operation. (SESSION: 8)
11/26/2007 15:46:04  ANR0490I Canceling session 7 for node NODE3 (WinNT) .
                      (SESSION: 8)
11/26/2007 15:46:04  ANR0524W Transaction failed for session 7 for node NODE3
                      (WinNT) -  data transfer interrupted. (SESSION: 7)
11/26/2007 15:46:04  ANR0514I Session 7 closed volume
                      C:\TSMDATA\SERVER1\CFILECLASS\000009E7.BFS. (SESSION: 7)
11/26/2007 15:46:04  ANR8340I FILE volume C:\TSMDATA\SERVER1\CFILECLASS\000009-
                      E7.BFS mounted. (SESSION: 8)
11/26/2007 15:46:04  ANR0510I Session 8 opened input volume
                      C:\TSMDATA\SERVER1\CFILECLASS\000009E7.BFS. (SESSION: 8)
11/26/2007 15:46:04  ANR0487W Session 7 for node NODE3 (WinNT) terminated -
                      preempted by another operation. (SESSION: 7)
```

Any additional session requesting to read from that volume has to wait until the session closes the volume. So NODE2 in session 10 is waiting for the volume to become available, as shown in the QUERY SESSION F=D output in Example 20-6.

Example 20-6 MEDIAW status for restore sessions, pre-V5.5 server

```
              Sess Number: 8
             Comm. Method: Tcp/Ip
               Sess State: SendW
                Wait Time: 0 S
               Bytes Sent: 29.2 M
              Bytes Recvd: 664
                Sess Type: Node
                 Platform: WinNT
              Client Name: NODE1
      Media Access Status: Current input volumes:  C:\TSMDATA\SERVER1\CFILECLA-
                            SS\000009E7.BFS,(244 Seconds)
                User Name:
Date/Time First Data Sent:
   Proxy By Storage Agent:

              Sess Number: 10
             Comm. Method: Tcp/Ip
               Sess State: MediaW
                Wait Time: 4.0 M
               Bytes Sent: 1.2 K
              Bytes Recvd: 658
                Sess Type: Node
                 Platform: WinNT
              Client Name: NODE2
      Media Access Status: Waiting for input volume(s):
                            C:\TSMDATA\SERVER1\CFILECLASS\000009E7.BFS,(240
                            Seconds)
                User Name:
Date/Time First Data Sent:
   Proxy By Storage Agent:
```

20.2.2 Behavior with Tivoli Storage Manager V5.5

With Tivoli Storage Manager V5.5 and later, the server allows multiple concurrent read access and one write access to the same FILE volume at a time. Figure 20-2 on page 265 illustrates the changed FILE volume access implementation now available.

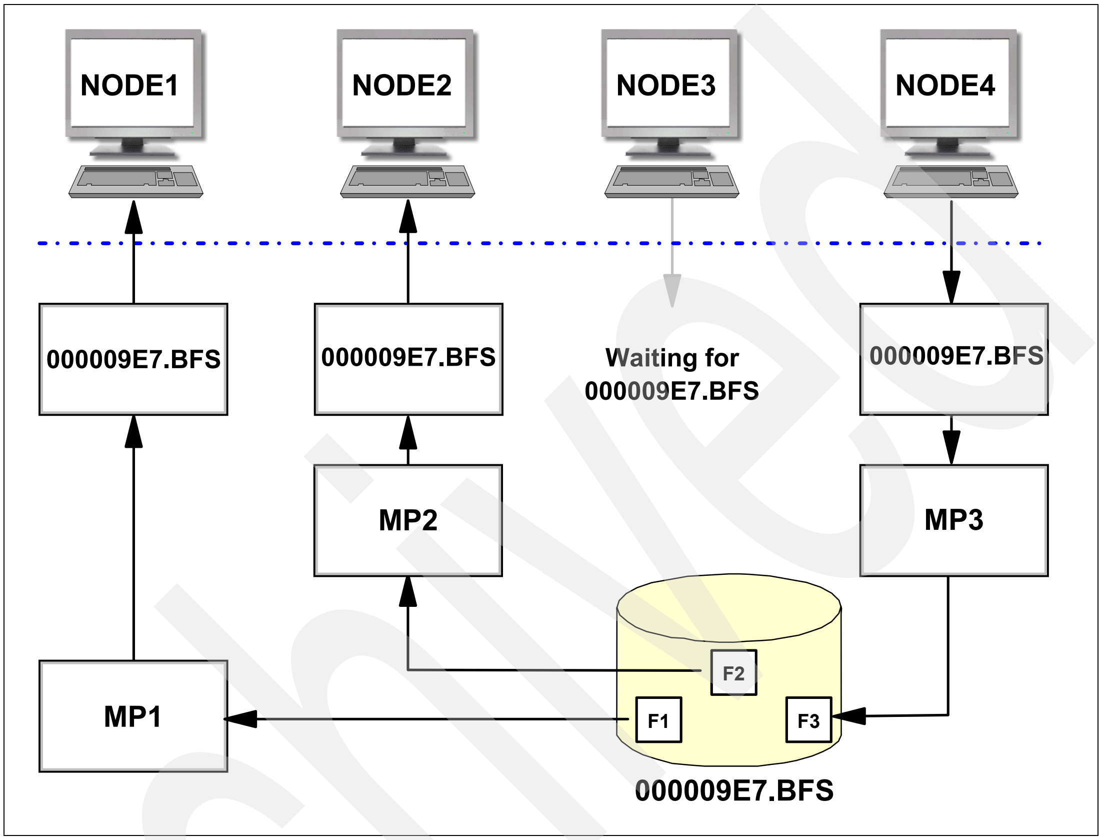


Figure 20-2 Concurrent access to a file volume

You will see the concurrent retrieve access documented with the output for the QUERY SESSION F=D or the QUERY MOUNT command. Example 20-7 shows that the same volume appears to be mounted more than once.

Example 20-7 Concurrent read access, QUERY MOUNT output

```
tsm: LOCHNESE>q mount
ANR8333I FILE volume C:\TSMDATA\SERVER1\CFILECLASS\000009E7.BFS is mounted R/W,
status: IN USE.
ANR8333I FILE volume C:\TSMDATA\SERVER1\CFILECLASS\000009E7.BFS is mounted R/W,
status: IN USE.
ANR8333I FILE volume C:\TSMDATA\SERVER1\CFILECLASS\000009E7.BFS is mounted R/W,
status: IN USE.
```

In addition, suppose that now NODE4 is also doing a backup. In Example 20-8 you see NODE1 and NODE2 accessing volume 000009E7.BFS as the input volume for a restore request. NODE4 is accessing the same volume as the output volume for the backup in parallel. Only NODE3 has to wait for the mount to be satisfied, as parallel write access to the same FILE volume is not supported.

Example 20-8 Concurrent read access, QUERY SESSION F=D output

```
tsm: LOCHNESE>q se f=d
..
              Sess Number: 3
             Comm. Method: Tcp/Ip
               Sess State: SendW
                Wait Time: 0 S
               Bytes Sent: 21.4 M
              Bytes Recvd: 658
                Sess Type: Node
                 Platform: WinNT
              Client Name: NODE2
      Media Access Status: Current input volumes:  C:\TSMDATA\SERVER1\CFILECLA-
                            SS\000009E7.BFS,(173 Seconds)
                User Name:
Date/Time First Data Sent:
   Proxy By Storage Agent:
..
              Sess Number: 13
             Comm. Method: Tcp/Ip
               Sess State: RecvW
                Wait Time: 2 S
               Bytes Sent: 362
              Bytes Recvd: 641.4 K
                Sess Type: Node
                 Platform: WinNT
              Client Name: NODE4
      Media Access Status: Current output volumes:  C:\TSMDATA\SERVER1\CFILECL-
                            ASS\000009E7.BFS,(37 Seconds)
                User Name:
Date/Time First Data Sent: 11/26/2007 16:45:15
   Proxy By Storage Agent:
..
              Sess Number: 14
             Comm. Method: Tcp/Ip
               Sess State: SendW
                Wait Time: 0 S
               Bytes Sent: 1.7 M
              Bytes Recvd: 658
                Sess Type: Node
                 Platform: WinNT
              Client Name: NODE1
      Media Access Status: Current input volumes:  C:\TSMDATA\SERVER1\CFILECLA-
                            SS\000009E7.BFS,(13 Seconds)
                User Name:
Date/Time First Data Sent:
   Proxy By Storage Agent:
..
              Sess Number: 15
             Comm. Method: Tcp/Ip
               Sess State: MediaW
                Wait Time: 10 S
               Bytes Sent: 357
              Bytes Recvd: 651
                Sess Type: Node
                 Platform: WinNT
              Client Name: NODE3
      Media Access Status: Waiting for output volume(s):
                            C:\TSMDATA\SERVER1\CFILECLASS\000009E7.BFS,(10
                            Seconds)
                User Name:
Date/Time First Data Sent: 11/26/2007 16:45:42
   Proxy By Storage Agent:
```

20.2.3 Summary

Concurrent read access support for FILE volumes allows you to more fully exploit I/O capabilities of the underlying disk subsystem. This ability enables storage agents on different systems to concurrently access FILE volumes for READ operations, independent of SANergy® or other file-device sharing software. It can also result in multi-session restores from a single RESTORE command if each of the nodes' restore sessions has data on a single volume and if that volume is associated with a device type of FILE.

While there is no configuration change required, make sure to adjust client MAXNUMMP and storage pool MOUNTLIMIT parameters accordingly.

20.3 QUERY LIBVOLUME command

The mediatype field output has changed in the command QUERY LIBVOLUME FORMAT=DETAIL in Tivoli Storage Manager V5.5. In Tivoli Storage Manager V5.3 and 5.4.0, the mediatype field contains numeric values that represent the type of the media, as shown in Example 20-9.

Example 20-9 Tivoli Storage Manager Server V5.3.5.2

```
tsm: TSMEH1>query libvolume format=detail

  Library Name: LTOLIB01
   Volume Name: VA0000
        Status: Scratch
         Owner:
      Last Use:
  Home Element: 2,132
   Device Type: LTO
Cleanings Left:
    Media Type: 394

tsm: TSMEH1>select * from libvolumes

  LIBRARY_NAME: LTOLIB01
   VOLUME_NAME: VA0000
        STATUS: Scratch
```

```
         OWNER:
      LAST_USE:
  HOME_ELEMENT: 2132
CLEANINGS_LEFT: 0
       DEVTYPE: LTO
     MEDIATYPE: 394
```

In V5.4.1 the UNKNOWN state was set for the mediatype, as shown in Example 20-10.

Example 20-10 Tivoli Storage Manager server V5.4.1

```
tsm: MZAISTSM01>query libvolume format=detail

  Library Name: LIB3584
   Volume Name: 072AEW
        Status: Private
         Owner:
      Last Use: DbBackup
  Home Element: 1,030
   Device Type: LTO
Cleanings Left:
    Media Type: Unknown

tsm: MZAISTSM01>select * from libvolumes

  LIBRARY_NAME: LIB3584
   VOLUME_NAME: 072AEW
        STATUS: Private
         OWNER:
      LAST_USE: DbBackup
  HOME_ELEMENT: 1030
CLEANINGS_LEFT: 0
       DEVTYPE: LTO
     MEDIATYPE: Unknown
```

WIth Tivoli Storage Manager server V5.5 (and also with V5.4.2) the mediatype field reflects a string value such as LTO-2 rather than 394, as shown in Example 20-11. This makes it easier to identify which type of media is used in the library.

Example 20-11 Tivoli Storage Manager Server V5.5.0

```
tsm: PULSE>query libvolume format=detail

  Library Name: LIB3582
   Volume Name: 465AGQ
        Status: Private
         Owner:
      Last Use: DbBackup
  Home Element: 4,100
   Device Type: LTO
Cleanings Left:
    Media Type: LTO-2

tsm: PULSE>select * from libvolumes

  LIBRARY_NAME: LIB3582
```

```
   VOLUME_NAME: 465AGQ
        STATUS: Private
         OWNER:
      LAST_USE: DbBackup
  HOME_ELEMENT: 4100
CLEANINGS_LEFT: 0
       DEVTYPE: LTO
     MEDIATYPE: LTO-2
```

If you are using the mediatype field in server scripts to monitor, for example, how many scratch volumes of a particular type are available, update your scripts and query the new string value instead of using the old numeric values, otherwise the scripts do not work correctly.

Part 6

Tivoli Storage Manager V5.5 client enhancements

This part presents enhancements to Tivoli Storage Manager V5.5 clients. First we detail the supported operating systems and summarize the new features and functions, then subsequent chapters present further details of the most significant new features.

21

Version 5.5 client supported environments

This chapter describes the following Tivoli Storage Manager Version 5.5 client functions:

- Supported client OS levels and currency
- Support for AIX Workload Partitions (AIX 6.1 WPAR)
- Support for AIX Encrypted File System (EFS) backup
- Snapshot image backup of AIX JFS2 file system
- Snapshot-based file-level backup and archive of AIX JFS2 file system
- Windows snapshot function
- Windows IA64, x64 OFS
- Windows IA64, x64 online image backup/restore
- Windows long file name
- IPv6 support

The major new client features of Tivoli Storage Manager V5.5 are described in detail in separate chapters.

For full details, always refer to the announcement letter, and to the installation and user guides for the relevant server. Announcement letters can be found using the keywords Tivoli Storage Manager at:

http://www-01.ibm.com/common/ssi/index.wss

or directly for V5.5 as:

http://www-01.ibm.com/common/ssi/index.wss?DocURL=http://www-01.ibm.com/common/ssi/rep_ca/6/877/ENUSZP07-0476/index.html&InfoType=AN&InfoSubType=CA&InfoDesc=Announcement+Letters&panelurl=index.wss%3F&paneltext=Announcement%20letter%20search

Find the Tivoli Storage Manager documentation at:

http://publib.boulder.ibm.com/infocenter/tivihelp

21.1 Client operating systems supported in V5.5

You will find the backup-archive client readmes and Release Notes for Tivoli Storage Manager V5.5 at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v1r1/topic/com.ibm.itsmreadme.doc_5.5/reln_client.html

Similarly, the client installation and user guides can be found directly at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v1r1/topic/com.ibm.itsmc.doc/clients.html

An overview of all the supported operating systems with the corresponding version of Tivoli Storage Manager client can be found at:

http://www-1.ibm.com/support/docview.wss?rs=663&context=SSGSG7&uid=swg21243309&loc=en_US&cs=utf-8&lang=en

Generally, the migration plan for a Tivoli Storage Manager update allows clients and servers to be upgraded at different times. (Also see 1.3.1, “Client and server version compatibility” on page 6). Although Tivoli Storage Manager is very flexible as to the versions of client code used, always, when possible, upgrade the client code to keep the server and client versions in sync. However, when a certain client is no longer supported, the old and unsupported client code versions will most often continue to work according to their original functionality.

21.1.1 AIX clients for Tivoli Storage Manager V5.5

The Tivoli Storage Manager V5.5 client on AIX is supported at:

- AIX backup-archive client
  - AIX V6.1
  - AIX V5.3 (32 bit or 64 bit)
  - Java JRE 5 or 1.4.1 for the Java GUI
  - Mozilla 1.4 or later browser for the Web client and to access online help and documentation
  - Files systems supported for backup-archive operations
    - JFS
    - JFS2
    - GPFS V2.3 PTF 11 (2.3.0.11) or later PTF, or V3.1 PTF 8 (3.1.0.8) or later PTF
    - VERITAS (VxFS) 4.0
  - Client capabilities
    - Administrative Client Command Line Interface (CLI)
    - Backup-archive CLI
    - Backup-archive Java Graphical User Interface (Java GUI)
    - Backup-archive Web Client Interface
    - Tivoli Storage Manager API (32 bit and 64 bit)
    - X/Open API (32 bit)
- With HACMP
  - AIX V5.3 (32 bit or 64 bit)
  - HACMP 5.3 (with IY80002) or 5.4 (with IY89869

- AIX HSM client
  - AIX V5.3 (32 bit or 64 bit), or AIX 6.1
  - For GPFS HSM: GPFS V3.2
  - Java JRE 5 or 1.4.1 for the Java GUI
  - Client capabilities
    - HSM Client CLI (requires Tivoli Storage Manager for Space Management)
    - HSM Java GUI
- With HACMP
  - AIX V5.3 (32 bit and 64 bit)
  - HACMP 5.3 (with IY80002) or 5.4 (with IY89869)

> **Note:** AIX V5.2 is supported by the Tivoli Storage Manager V5.4 backup-archive client.

21.1.2 Apple Macintosh backup-archive client for Tivoli Storage Manager V5.5

For Apple Macintosh backup-archive client for Tivoli Storage Manager V5.5:

- Macintosh OS X, V10.5
- Client capabilities
  - Administrative Client CLI
  - Backup-archive Web Client Interface
  - Backup-archive Java Graphical User Interface (Java GUI)

21.1.3 Hewlett-Packard HP-UX clients for Tivoli Storage Manager V5.5

The Tivoli Storage Manager V5.5 client on HP-UX is supported at:

- An HP-UX PA-RISC backup-archive client
  - HP-UX 11i V2 (32 bit or 64 bit) or HP-UX 11iV3
  - Java JRE 1.4.1 or JRE 5 for the Java GUI
  - Mozilla 1.4 or later browser for the Web client and to access online help and documentation
  - Client capabilities
    - Administrative Client CLI
    - Backup-archive CLI
    - Backup-archive Java Graphical User Interface (Java GUI)
    - Backup-archive Web Client Interface
    - Tivoli Storage Manager API (32 bit and 64 bit)
    - X/Open API (32 bit)
- Hewlett-Packard HP-UX PA-RISC HSM client
  - HP-UX 11i V2 (32 bit or 64 bit)
  - File system
    - VERITAS file system (VxFS) 4.1
    - VERITAS Volume Manager (VxVM) 3.5 or later, OnlineJFS 3.5
  - Client capabilities
    - HSM Client CLI
    - HSM Java GUI

- Hewlett-Packard HP-UX Itanium 2 backup-archive client
  - HP-UX 11iv2 (32 bit or 64 bit) or HP-UX 11iv3
  - Java JRE 1.4.1 or JRE 5 for the Java GU
  - Mozilla 1.4 or later browser for the Web client and to access online help and documentation
  - Client capabilities
    - Administrative Client CLI
    - Backup-archive CLI
    - Backup-archive Java Graphical User Interface (Java GUI)
    - Backup-archive Web Client Interface
    - Tivoli Storage Manager API
- Hewlett-Packard HP-UX Itanium 2 HSM client
  - HP-UX 11i V2 for Itanium 2
  - File system

    Tivoli Storage Manager-enabled version of VERITAS VxFS 4.1. Contact your IBM Tivoli Storage Manager representative for access to this version of VxFS 4.1.

21.1.4 Linux clients for Tivoli Storage Manager V5.5

The Tivoli Storage Manager V5.5 client with Linux is supported at:

- Linux for x86/86_64 backup-archive client
  - Red Hat Enterprise Linux 4.0 or 5.0
  - SLES 9 and 10
  - Asianux 2.0 or 3.0
  - Novell OES
  - Java JRE 5 or 1.4.1
  - Mozilla 1.4 or later browser for the Web client and to access online help and documentation
  - Client capabilities:
    - Administrative Client CLI
    - Backup-archive CLI
    - Backup-archive Java Graphical User Interface (Java GUI)
    - Backup-archive Web Client Interface
    - Tivoli Storage Manager API
- Linux for x86/86_64 HSM client
  - Red Hat Enterprise Linux 4.0 or 5.0
  - SLES 9 and 10
  - File system - GPFS V3.2
  - Java JRE 5 or 1.4.1
  - Mozilla 1.4 or later browser for the Web client and to access online help and documentation
  - Client capabilities

    - HSM Client CLI
    - HSM Java GUI
- Linux for POWER backup-archive client
  - SLES 9 and 10
  - Red Hat Enterprise Linux 4.0 or 5.0
  - Java JRE 5 or 1.4.1
  - Mozilla 1.4 or later browser for the Web client and to access online help and documentation
  - Client capabilities
    - Administrative Client CLI
    - Backup-archive CLI
    - Backup-archive Java Graphical User Interface (Java GUI)
    - Backup-archive Web Client Interface
    - Tivoli Storage Manager API
- Linux for Itanium 2 backup-archive client
  - SLES 9 and 10
  - Red Hat Enterprise Linux 4.0 or 5.0
  - Java JRE 5 or 1.4.1
  - The Web backup-archive client requires one of:
    - Microsoft Internet Explorer 5.0 or later with JRE 5 or 1.4.1
    - Mozilla 1.4, or later browser for the Web client and to access online help and documentation
- Client capabilities
    - Administrative Client CLI
    - Backup-archive CLI
    - Backup-archive Java Graphical User Interface (Java GUI)
    - Backup-archive Web Client Interface
    - Tivoli Storage Manager API
- Linux for IBM System z backup-archive client
  - SLES 9 and 10 for System z
  - Red Hat Enterprise Linux 4.0 or 5.0 for Linux for System z
  - Java JRE 5 or 1.4.1
  - Mozilla 1.4 or later browser for the Web client and to access online help and documentation
  - Client capabilities
    - Administrative Client CLI
    - Backup-archive CLI
    - Backup-archive Web Client Interface
    - Tivoli Storage Manager API

21.1.5 Novell NetWare backup-archive client for Tivoli Storage Manager V5.5

The Tivoli Storage Manager V5.5 client with Novell NetWare is supported at:

- Novell NetWare 6.5 SP5+ (OES SP2)
- Client capabilities
  - Backup-archive CLI
  - Backup-archive Web Client Interface
  - Tivoli Storage Manager API

21.1.6 OS/400 API client for Tivoli Storage Manager V5.5

The Tivoli Storage Manager V5.5 API client with OS/400 is supported at:

- OS/400 i5/OS V5R3 or i5/OS V5R4
- Client capabilities: Tivoli Storage Manager API

21.1.7 Solaris clients for Tivoli Storage Manager V5.5

The Tivoli Storage Manager V5.5 client on Solaris is supported at:

- A Solaris SPARC backup-archive client
  - Solaris 9 or 10 (32 bit or 64 bit)
  - Java JRE 5 or 1.4.1
  - Mozilla 1.4,or later browser for the Web client and to access online help and documentation
  - Client capabilities
    - Administrative Client CLI
    - Backup-archive CLI
    - Backup-archive Java Graphical User Interface (Java GUI)
    - Backup-archive Web Client Interface
    - Tivoli Storage Manager API
    - X/Open API (32 bit)
- Solaris SPARC HSM client
  - Solaris 9 or 10 (32 bit or 64 bit)
  - VERITAS File System (VxFS) 4.1
  - Java JRE 5 or 1.4.1
  - Client capabilities
    - HSM Client CLI
    - HSM Java GUI
- Solaris X86/X86_64 backup-archive client
  - Solaris 10 (32 bit or 64 bit)
  - Java JRE 5, or 1.4.1
  - Mozilla 1.4 or later browser for the Web client and to access online help and documentation
  - Client capabilities

- Administrative Client CLI
- Backup-archive CLI
- Backup-archive Java Graphical User Interface (Java GUI)
- Backup-archive Web Client Interface
- Tivoli Storage Manager API

21.1.8 Windows backup-archive client for Tivoli Storage Manager V5.5

The Tivoli Storage Manager V5.5 client with Microsoft Windows is supported at:

- Windows XP Professional (32 bit and 64 bit, SP 2 or later)
- Windows Server 2003 Server (all editions, 32 bit and 64 bit)
- Windows Server 2003 Server R2 (all editions, 32-bit and 64-bit support for same features as in Windows Server 2003)
- Windows Vista all editions (except Automated System Recovery (ASR))
- Client capabilities
  - Administrative Client CLI
  - Backup-archive CLI
  - Backup-archive GUI
  - Backup-archive Web Client Interface
  - Tivoli Storage Manager API
  - ODBC (32-bit mode applications only)

> **Note:** Windows 2000 is supported by the Tivoli Storage Manager V5.3 client.
>
> Only 64-bit clients can run on 64-bit machines.

21.1.9 z/OS UNIX System Services, Tivoli Storage Manager V5.5

The Tivoli Storage Manager V5.5 client with z/OS UNIX System Services is supported at (client and API):

- z/OS V1R7, z/OS V1R8, or V1R9
- Java JRE 5 or 1.4.1
- Restrictions - Tivoli Storage Manager server functions not included in this client:
  - SQLDB: Certain SQL select statements using the path for the files backed up by a z/OS UNIX System Services client might not work properly.
  - Server command 'query content'.
  - Cross-client restore.
- Client capabilities
  - Administrative Client CLI
  - Backup-archive CLI
  - Backup-archive Web Client Interface
  - Tivoli Storage Manager API (32 bit)

21.1.10 NDMP requirements

Tivoli Storage Manager Extended Edition includes support for NDMP-controlled backup and restore operations. This is further described in Chapter 10, “NDMP” on page 133.

The requirements are:

- A Tivoli Storage Manager Extended Edition server on Windows Server 2003, AIX 64 bit, Solaris 64 bit, HP 64 bit, or Linux.
- NDMP is supported on all the operating systems that are supported by the Tivoli Storage Manager Extended Edition server except for the z/OS operating system.
- A Tivoli Storage Manager Extended Edition supported backup-archive client on Windows, Solaris SPARC (32 bit or 64 bit) or AIX (32 bit or 64 bit) can be used for initiating backup and restore operations.

21.1.11 IBM Tivoli Storage Manager HSM for Windows V5.5

Tivoli Storage Manager HSM for Windows is further described in Chapter 16, “HSM for Windows V5.4” on page 205:

- Any of the following Windows versions that support NTFS V5:
  - Windows 2003 Server (32 bit)
  - Windows 2003 Server R2 (32 bit)
  - Windows 2003 Server SP2 (32 bit)
  - Windows 2003 Enterprise Server (32 bit)
  - Windows 2003 Enterprise Server R2 (32 bit)
  - Windows 2003 Enterprise Server SP2 (32 bit)
- Tivoli Storage Manager V5.5 Windows backup-archive client
- Tivoli Storage Manager Windows Client API V5.5

21.2 Additional client functionality

In this section we discuss some of the principal new client functions.

21.2.1 VMware consolidated backup integration

Tivoli Storage Manager V5.5 integrates with VMware Consolidated Backup (VCB) to coordinate the movement of virtual machine data from the VCB proxy server to tape devices. This includes LAN-free virtual machine backup. Usability enhancements include better recovery and management of virtual machine data from the Tivoli Storage Manager server. The backup is performed from a VCB backup host and can manage a virtual machine's backup data as if it had been backed up by a Tivoli Storage Manager client running on the virtual machine.

For more information about VCB support with Tivoli Storage Manager, see Chapter 24, “VMware consolidated backup with Tivoli Storage Manager V5.5” on page 325.

21.2.2 AIX V5.5 client additional functionality

There are number of new functions and enhancements specific to the AIX V5.5 client.

Backup, archive, and space management support for AIX WPAR

AIX V6.1 introduces a new, software-based virtualization approach called Workload Partition (WPAR) that complements the existing IBM System Logical Partitions by reducing the number of operating system images that have to be managed when consolidating workloads. WPAR enables the system administrator to consolidate multiple applications inside a single running instance of AIX V6.1. A WPAR configuration typically includes a global partition and one or more local partitions.

Tivoli Storage Manager V5.5 support for WPAR enables:

- Backup and restore of local partition file data within the global partition using the local partition namespace available within the global partition
- Migration and transparent recall of local partition file data within the global partition:
  - Journaled File System (JFS2)
  - General Parallel File System™ (GPFS)
- Storage and retrieval of application data using Tivoli Storage Manager APIs supported from global partition

The /usr file system may be shared (read-only) or not shared (writable) for the local partitions.

Shared (read-only) /usr file system

The Tivoli Storage Manager client can be installed in the global WPAR and each local WPAR user can use the same client installation. In this environment:

- The global administrator needs to update the Tivoli Storage Manager client only once and the changes will be applied to all the local WPARs.
- Every local and global WPAR has to use the same version of the Tivoli Storage Manager client.
- Each WPAR can have its own set of configuration files by setting DSM_CONFIG and DSM_DIR environment variables. Alternatively, the dsm.sys can be stored in the default location by specifying one or more server stanzas per WPAR in the dsm.sys file. Each WPAR will have to set its DSM_CONFIG.

Non-shared (writable) /usr file system

In an environment where /usr is non-shared:

- If the Tivoli Storage Manager client is already installed at the global WPAR before the local WPAR with a non-sharing /usr file system is created, all the files from the global /usr file system will be copied over to the local /usr file system. The local WPAR will then have its own Tivoli Storage Manager client installation when the local WPAR is created, as a separate client install instance.
- If the Tivoli Storage Manager client is not installed at the global WPAR before the local WPAR with the non-sharing /usr file system is created, then the Tivoli Storage Manager client can be installed either at the global WPAR or the local WPAR (after creating the local WPAR). These clients will be separate instances of Tivoli Storage Manager clients.
- The Tivoli Storage Manager client can also be installed at a non-default location if desired.

Support for AIX Encrypted File System (EFS) backup

EFS is integrated into JFS2 beginning with AIX V6.1. Tivoli Storage Manager V5.5 backs up files in either clear text or in raw (encrypted) format. In raw (encrypted) format, the data is not decrypted on backup, and the keys must be available to use the data after restore. In clear text format, the data is decrypted (by EFS) as it is being read on backup and can optionally be encrypted by Tivoli Storage Manager using encryption options available within Tivoli Storage

Manager. Using the option to decrypt and back up with Tivoli Storage Manager, encryption can make it easier to manage keys for long-term data archival using Tivoli Storage Manager key managed encryption.

Snapshot image backup of AIX JFS2 file system

Snapshot image backup support is available for the AIX JFS2 file system for AIX 5.3 or later. This support is based on an AIX JFS2 snapshot. Snapshot image backup can significantly reduce application downtime due to backup operations.

Snapshot-based file level backup and archive of AIX JFS2 file system

Snapshot-based file backup and archive support using AIX JFS2 snapshot is available for AIX JFS2 files system for AIX V5.3 or later. This support provides consistent file-level backup and archive of the data while helping to reduce application downtime.

NFSV4 ACL support for AIX and AIX JFS2 file system

Support for backup-restore, archive-retrieve, and migration-recall of NFSV4 ACL for JFS2 file system and NFS mounted file systems is available on AIX V5.3 or later. This additional support allows non-AIX NFSV4 ACL data to be backed up from an AIX NFS client.

AIX JFS2 EAV2 support

Support for backup-restore, archive-retrieve, and migration-recall of AIX JFS2 extended attributes (EA) support is available on AIX V5.3 or later.

Used block-only image backup of AIX JFS2 file system

Used block-only image backup allows backup only of the in-use blocks of the AIX JFS2 file system. This support can reduce the backup time for file systems that are not fully occupied.

21.2.3 Windows client V5.5 additional functionality

There are number of new enhancements specific to the Windows V5.5 client.

Snapshot provider for online image and open file support

The Windows V5.5 client includes two new options for snapshot support. These are:

- SNAPSHOTPROVIDERFS: enables snapshot-based file backup/archive operations and specifies a snapshot provider. This parameter can be set to either VSS, LVSA, or NONE. However, note that VSS is available only on Windows 2003 Server and Vista. VSS backup is not supported on Windows XP. The provider selected will provide the open file support (OFS) during file backup and archive operations. If no provider is specified, then no OFS is available. The default is SNAPSHOTPROVIDERFS NONE.
- SNAPSHOTPROVIDERIMAGE: enables snapshot-based online image backup/archive operations and specifies a snapshot provider. This parameter can be set to VSS or LVSA, or NONE. However, note that VSS is available only on Windows 2003 Server and Vista. VSS backup is not supported on Windows XP. The provider selected will provide the online image support during image backup operations. If no provider is specified, then no online image support is available. The default is SNAPSHOTPROVIDERIMAGE NONE.

You can set these two options in the client options file or at the command line. You can also use the GUI (**Edit ∅ Preferences ∅ Image-Snapshot**), as shown in Figure 21-1.

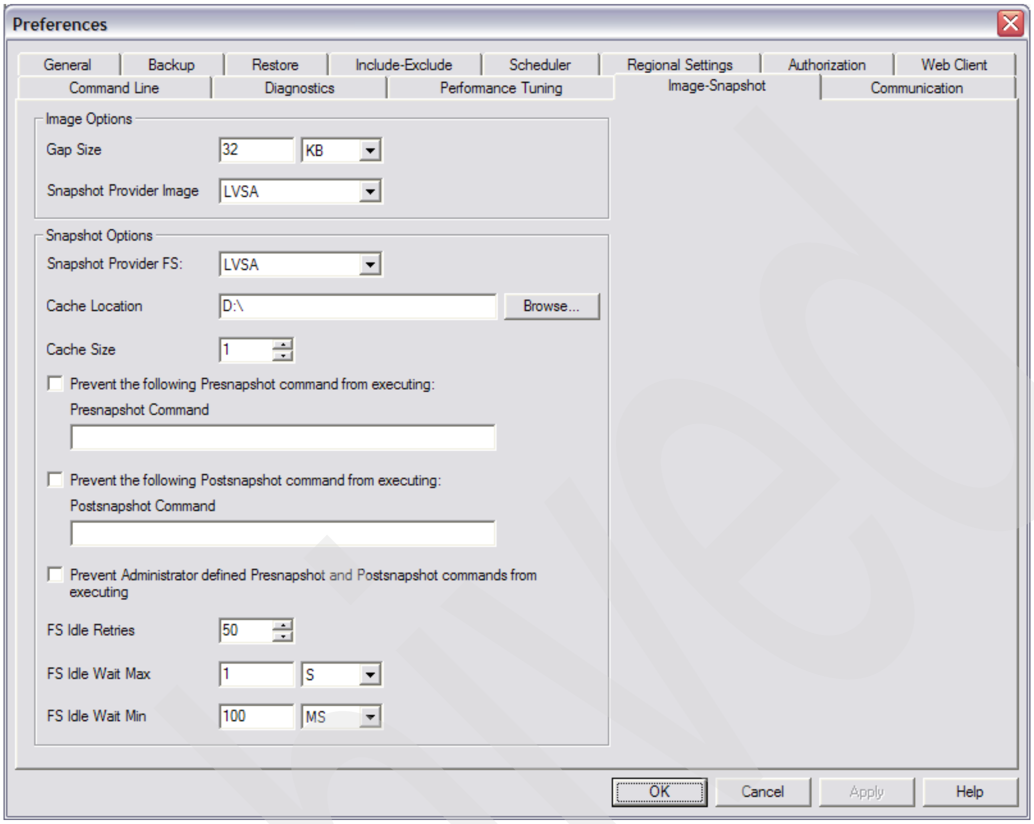


Image Options

Gap Size: 32 KB

Snapshot Provider Image: LVSA

Snapshot Options

Snapshot Provider FS: LVSA

Cache Location: D:\

Cache Size: 1

☐ Prevent the following Presnapshot command from executing:

Presnapshot Command

☐ Prevent the following Postsnapshot command from executing:

Postsnapshot Command

☐ Prevent Administrator defined Presnapshot and Postsnapshot commands from executing

FS Idle Retries: 50

FS Idle Wait Max: 1 S

FS Idle Wait Min: 100 MS

Figure 21-1 Set snapshot provider options

Alternatively, you can use the setup wizard (**Utilities ∅ Setup Wizard**) in the GUI to configure the online image and open file support. During the wizard you will be asked to choose a snapshot provider.

Note that the Microsoft Volume Shadowcopy Service (VSS) can now be used on Windows 2003 and Vista to provide online backup, as an alternative to the Logical Volume Snapshot supported 2003, Vista, and XP. If you use VSS for online backup, you do not need to install the LVSA.

Attention: If you upgrade a pre-V5.5 client to V5.5 and are using online image and open file support, you must configure the appropriate snapshot provider options in the client options file. If SNAPSHOTPROVIDERFS and SNAPSHOTPROVIDERIMAGE are not set, they default to NONE, and any online image and open file operations fail.

Online image backup on Windows 64-bit operating systems

On Windows client platforms, Tivoli Storage Manager can take snapshots of a volume while it is online to enable online point-in-time volume image copies to be backed up to Tivoli Storage Manager. Tivoli Storage Manager V5.5 adds support of 64-bit Windows platforms to the previously available 32-bit support.

Open file support for Windows 64-bit operating systems

The Tivoli Storage Manager client Open File Support (OFS) enables files that are locked by other applications to be backed up. Tivoli Storage Manager V5.5 adds support of 64-bit Windows platforms to the previously available 32-bit support.

Files with up to 8184-character directory names

The Tivoli Storage Manager Windows V5.5 client can back up files with directory names up to 8184 characters in length.

21.2.4 Server-managed encryption keys for backup-archive client

To help improve the security of stored data, the backup-archive client implements an optional encryption function, which allows for encrypting data *before* it is sent to the Tivoli Storage Manager server. This helps secure backup or archive data during transmission, and it means that the data stored on the Tivoli Storage Manager server is encrypted.

Previously, using this encryption method, the user had to remember the encryption key password during restore or keep the password stored locally on the client system. With V5.5, Tivoli Storage Manager generates, encrypts, stores, and manages the encryption key in the Tivoli Storage Manager database, freeing the user from these tasks. For more details, see 22.1, “Transparent client encryption” on page 288.

Tivoli Storage Manager server-managed encryption keys have been available in releases prior to Tivoli Storage Manager V5.5 for data backed up via the Tivoli Storage Manager API and for Tivoli Storage Manager data protection modules.

Application-managed encryption, however, is a tape hardware encryption available for IBM System Storage TS1120 (available since V5.4.0) and LTO-4 tape drives (available since V5.4.1). The hardware encryption supports three different encryption management methods: application, system, and library managed. For application-managed encryption, Tivoli Storage Manager generates, stores, and communicates encryption keys to the tape drives. Tivoli Storage Manager's policy management capabilities automatically determine whether tape drive encryption is to be used, and if so, which of the TS1120 or LTO-4 encryption management methods to employ. For details see Chapter 9, “Tape data encryption” on page 101.

21.2.5 IPv6 support

The IBM Tivoli Storage Manager client now supports the TCP/IP Version 6 (IPv6) protocol and can be used in a dedicated IPv6, IPv4, or intermixed IP environment. This protocol is supported for AIX, HP-UX, Linux, Sun Solaris, and Windows systems. Refer also to 18.3.2, “IPv6 support” on page 244.

The parameter COMMMETHOD V6TCPIP indicates that either TCP/IP Version 4 or Version 6 should be used, depending on the system configuration and the results of a domain name service lookup. A valid DNS environment must be available.

Internet Protocol V6 is the next-generation protocol designed to replace the current version, Internet Protocol V4 (IPv4). IPv6 is interoperable with TCP/IP Version 4. You can specify either IPv4 or IPv6 in the COMMMETHOD option when you start the client application. The same port numbers are used for both IPv4 and IPv6.

There are some restrictions with the IPv6 version, specifically that the dsmc schedule command cannot be used when both SCHEDMODE PROMPT and COMMMETHOD

V6TCPIP are specified. Refer to *IBM Tivoli Storage Manager Administrator's Reference V5.5* and *IBM Tivoli Storage Manager Backup-Archive Clients Installation and User's Guide V5.5* for further details.

21.2.6 Clients not migrated to V5.5

The following operating system versions, supported in V5.4, do not have a V5.5 client available. The V5.4 clients for these operating systems can be used with V5.5 Tivoli Storage Manager servers for as long as V5.4 is in support.

- Macintosh 10.4
- AIX V5.2

22

Client security enhancements

Data security is always a big concern for most companies, and Tivoli Storage Manager V5.5 addresses some security-related requirements with the introduction of:

- Transparent encryption for the data transferred between client and server
- Secured communication between client and server using SSL encryption

This chapter provides details of the changes made to the client and server to provide the security enhancements and provides example implementation details.

22.1 Transparent client encryption

Tivoli Storage Manager V5.5 provides backup-archive client transparent data encryption for Archive and retrieve and backup and restore, including no query restore (NQR), with all key management (generation, retrieval) done by Tivoli Storage Manager.

Before V5.5, the Tivoli Storage Manager backup-archive client could already encrypt client data with key management done by the client user. Files to be encrypted were selected via the include.encrypt and exclude.encrypt options. The backup-archive client supported two options, ENCRYPTKEY=PROMPT (default) and ENCRYPTKEY=SAVE.

When ENCRYPTKEY=PROMPT, you are prompted to specify the key upon every invocation of the backup-archive client. You therefore have to remember each client key used.

When ENCRYPTKEY=SAVE, your specified encryption key is saved to the local password file (TSM.PWD in UNIX, Linux, Macintosh, and Netware, and the registry on Windows) for use on subsequent invocations. All files backed up or archived by that node then have the same encryption key.

The API supported these same two options, as well as a third option, ENABLECLIENTENCRYPTKEY (default no), for transparent encryption. With this option set, the API internally generates an encryption key and saves the key to the Tivoli Storage Manager server. The option ENABLECLIENTENCRYPTKEY is not applicable to the backup-archive client, it is an API-only option and is ignored by the client during backup or archive.

In Tivoli Storage Manager V5.5, the ENCRYPTKEY option now applies to both the backup-archive client and the API. Use the option ENCRYPTKEY=GENERATE to enable transparent (server-managed) encryption. The ENCRYPTKEY option is the preferred way to specify the type of encryption to be used. Table 22-1 provides an overview of the supported option settings.

Note that the ENABLECLIENTENCRYPTKEY option is still supported and usable by the API client. However, this may be removed in the future. Therefore, we recommend using ENCRYPTKEY=GENERATE.

Table 22-1 Encryption option settings

Option setting		**Action**	
ENABLECLIENTENCRYPTKEY	**ENCRYPTKEY**	**API**	**Backup-archive client**
NO	GENERATE	Transparent encryption	Transparent encryption
NO	PROMPT	Key prompted encryption	Key prompted encryption
NO	SAVE	Encryption key saved locally	Encryption key saved locally
YES	GENERATE	Transparent encryption	Transparent encryption
YES	PROMPT	API error	Key prompted encryption
YES	SAVE	API error	Encryption key saved locally

When ENCRYPTKEY=GENERATE, the backup-archive client generates an internal encryption key during session initialization with the server. This key is used to encrypt all files backed up or archived on that session.

The option is only applicable during backup and archive processing. Files that are encrypted on the Tivoli Storage Manager server are properly decrypted and restored/retrieved with or without the specification of these options.

> **Note:** Encryption processing is used to ensure that data moving from the client to the server (and the data on the server) cannot be read by an unauthorized person. Authorization to restore the data is not changed by using this option.

One of the advantages of this support is that the encryption key is saved on the server. If the original machine is rebuilt, or you are trying to recover on another machine, the data will be transparently unencrypted and restored on the target machine because the key is part of the server data. There is no need to access an encryption key on the original machine.

The ENCRYPTKEY=GENERATE option is only supported if backup-archive client and server are at V5.5 or later.

22.1.1 Implementation

To implement:

1. For our implementation example we add the option parameters shown in Example 22-1 to an option file called node3.opt on a Windows client.

   Example 22-1 Encryption option configuration

   ```
   include.encrypt e:\demodata\...\*.gz
   encryptkey generate
   ```

   The INCLUDE.ENCRYPT command instructs the client to encrypt all files with the .gz extension in the demodata directory of volume E: during backup processing.

2. We back up a single object for our tests, as shown in Example 22-2.

Example 22-2 Back up with ENCRYPTKEY=GENERATE

```
C:\Tivoli\TSM\baclient>dsmc -optfile=node3.opt -testflag=instrument:detail
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 5, Level 0.0
  Client date/time: 12/06/2007 16:32:00
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.

Node Name: NODE3
Session established with server HAGGIS: Windows
  Server Version 5, Release 5, Level 0.0
  Server date/time: 12/06/2007 16:32:00  Last access: 12/06/2007 16:29:03

tsm> sel e:\demodata\demodata.tar.gz
Selective Backup function invoked.

Normal File-->         7,618,412 \\lochnese\e$\demodata\demodata.tar.gz [Sent]

Selective Backup processing of '\\lochnese\e$\demodata\demodata.tar.gz' finished
without failure.

Total number of objects inspected:        1
Total number of objects backed up:        1
```

```
Total number of objects updated:          0
Total number of objects rebound:          0
Total number of objects deleted:          0
Total number of objects expired:          0
Total number of objects failed:           0
Total number of subfile objects:          0
Total number of bytes transferred:    7.26 MB
Data transfer time:                    0.07 sec
Network data transfer rate:        94,189.50 KB/sec
Aggregate data transfer rate:      7,006.56 KB/sec
Objects compressed by:                    0%
Subfile objects reduced by:               0%
Elapsed processing time:           00:00:01
```

3. Note that during backup there is no message indicating the use of encryption (similarly to a restore operation). However, we collected the trace information using the flag -testflag=instrument:detail. The instrumentation trace proves that the encryption module has been invoked, since there is a line item for encryption, as shown in the extract in Example 22-3.

Example 22-3 Encryption processing time

```
Section                  Actual(sec)Average(msec)Frequency used
------------------------------------------------------------------
..
Compute                      0.000      0.0        234
BeginTxn Verb                0.000      0.0          1
Transaction                  0.000      0.0          1
File I/O                     0.016      0.1        235
..
Encryption                   0.046      0.2        234
..
Data Verb                    0.079      0.3        234
Confirm Verb                 0.000      0.0          1
EndTxn Verb                  0.047     47.0          1
..
Thread Wait                  0.859    214.8          4
Other                        0.015      0.0          0
```

> **Note:** It should be obvious that client encryption requires CPU cycles and increases processing time. You must consider this when configuring your INCLUDE.ENCRYPT option so that you only encrypt data that is worth the overhead.

4. After you have backed up an object with transparent encryption enabled, you can no longer restore that object with a pre-V5.5 client, as shown in Example 22-4. An ANS1461E error is reported, as those clients are not capable of dealing with the object's encryption key.

Example 22-4 ANS1461E: unsupported encryption type

```
C:\Tivoli\TSM\baclient>dsmc res \\lochnese\e$\demodata\demodata.tar.gz
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 4, Level 1.2
  Client date/time: 12/06/2007 16:39:42
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.
```

```
Node Name: NODE3
Session established with server HAGGIS: Windows
  Server Version 5, Release 5, Level 0.0
  Server date/time: 12/06/2007 16:39:49  Last access: 12/06/2007 16:39:18

Restore function invoked.

 ** Unsuccessful **
ANS1461E Error processing '\\lochnese\e$\demodata\test.gz': unsupported encryption
type.

<       0  B> [ - ]
Restore processing finished.

Total number of objects restored:        0
Total number of objects failed:          1
Total number of bytes transferred:       0  B
Data transfer time:                   0.00 sec
Network data transfer rate:           0.00 KB/sec
Aggregate data transfer rate:         0.00 KB/sec
Elapsed processing time:          00:00:06
```

5. The ENCRYPTKEY=GENERATE option is also not supported when contacting a pre-V5.5 server. Objects matching the encryption specification are skipped during the backup process with message ANS1228E and message ANS1978E explaining the reason. Example 22-5 shows what happens when we try to back up the file with transparent encryption enabled to a 5.4 server.

Example 22-5 ANS1978E: down-level server with ENCRYPTKEY=GENERATE

```
C:\Tivoli\TSM\baclient>dsmc -optfile=node3.opt
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 5, Level 0.0
  Client date/time: 12/07/2007 15:12:37
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.

Node Name: NODE3
Session established with server ZAIRE: AIX-RS/6000
  Server Version 5, Release 4, Level 0.0
  Server date/time: 12/07/2007 13:14:11  Last access: 12/07/2007 13:12:31

tsm> sel e:\demodata\*
Selective Backup function invoked.

ANS1228E Sending of object '\\lochnese\e$\demodata\demodata.tar.gz' failed
ANS1978E The TSM server is downlevel and does not support the requested function
. See error log for version information.
Directory-->                    0 \\lochnese\e$\demodata [Sent]
Normal File-->          7,618,412 \\lochnese\e$\demodata\demodata.file  [Sent]
ANS1804E Selective Backup processing of '\\lochnese\e$\demodata\*' finished with
failures.

Total number of objects inspected:       3
Total number of objects backed up:       2
Total number of objects updated:         0
Total number of objects rebound:         0
Total number of objects deleted:         0
Total number of objects expired:         0
Total number of objects failed:          1
Total number of subfile objects:         0
Total number of bytes transferred:   10.36 MB
Data transfer time:                   40.82 sec
Network data transfer rate:          259.86 KB/sec
Aggregate data transfer rate:        249.72 KB/sec
Objects compressed by:                   0%
Subfile objects reduced by:              0%
Elapsed processing time:           00:00:42
```

Access data from another node

When using transparent encryption, you can still grant access to your data for another node without the need to exchange encryption keys. In Example 22-6, we allow NODE4 to access an encrypted NODE3 object (remember that E:\demodata\*.gz is set to be encrypted) (Example 22-6).

Example 22-6 Grant access to NODE4

```
C:\Tivoli\TSM\baclient>dsmc -optfile=node3.opt
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 5, Level 0.0
  Client date/time: 01/04/2008 01:56:03
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.

Node Name: NODE3
Session established with server HAGGIS: Windows
  Server Version 5, Release 5, Level 0.0
  Server date/time: 01/04/2008 01:56:03  Last access: 01/04/2008 01:51:27

tsm> set access backup * node4
ANS1148I 'Set Access' command successfully completed
tsm> q access
Type     Node        User        Path
----     ----------------------------
Backup   NODE4       *           *

ANS1148I 'Query Access' command successfully completed
```

Even though NODE4 does not have the ENCRYPTKEY set in its option file, it can access the data, as shown in Example 22-7, since the server supplies the encryption key.

Example 22-7 Transparent encryption works to another node with access

```
C:\Tivoli\TSM\baclient>dsmc -optfile=node4.opt
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 5, Level 0.0
  Client date/time: 01/04/2008 02:02:27
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.
```

```
Node Name: NODE4
Session established with server HAGGIS: Windows
  Server Version 5, Release 5, Level 0.0
  Server date/time: 01/04/2008 02:02:27  Last access: 01/04/2008 01:50:14

tsm> restore -fromnode=node3 \\lochnese\e$\demodata\*gz .\
Restore function invoked.

Restoring               0 \\lochnese\e$\demodata --> \\lochnese\c$\Tivoli\TSM\ba
client\demodata [Done]
Restoring       7,618,412 \\lochnese\e$\demodata\demodata.tar.gz --> \\lochnese\
c$\Tivoli\TSM\baclient\demodata\demodata.tar.gz [Done]

Restore processing finished.

Total number of objects restored:         2
Total number of objects failed:           0
Total number of bytes transferred:    7.26 MB
Data transfer time:                    0.00 sec
Network data transfer rate:            0.00 KB/sec
Aggregate data transfer rate:      2,381.19 KB/sec
Elapsed processing time:           00:00:03
```

If you enable client tracing, you will see messages similar to those shown in Example 22-8, which indicate that the data has been decrypted. Use traceflags verbdetail incr fileops verbdetail encrypt.

Example 22-8 Extracts from client trace to show data is decrypted

```
...
Contents of verb (0x50100) BeginObjDataEnhanced, length: 104:
version             : 0x1
versIdHi            : 0
versIdLo            : 10820739
clientEncrKey       :
67F61C63 02D62074 91589C43 9EEE90CD 5E5227D6 4F26CC51 D58358FB DBF11F6A
924BB88B 890312A8 7E9EECEE D565186C 81E6E12C 403384E3 E12BD0FD 27E1E5
...
01/04/2008 02:02:27.592 : restcore.cpp        (3261): Process transparent
encryption key
...

01/04/2008 02:02:27.592 : restcore.cpp        (3521): CheckKeyValidity: for
transparent encryption
```

22.1.2 Server operations

Once client data is encrypted, there is an effect on some Tivoli Storage Manager server commands.

Backup sets

The GENERATE BACKUPSET command is not supported for file systems that contain any transparently encrypted data. The file system will not be included in the backup set. Example 22-9 shows that you will receive an ANR0952W for the related filespace. The command, however, will complete with a completion state of success if other filespaces are to be processed.

Example 22-9 ANR0952W upon GENERATE BACKUPSET

```
tsm: HAGGIS>generate backupset node3 071207node3 *  devc=cfileclass wait=yes
ANR0984I Process 43 for GENERATE BACKUPSET started in the FOREGROUND at 10:47:29.
ANR0952W The filespace \\lochnese\e$ cannot be included in the backup set because
it contains encrypted data.
ANR3500I Backup set for node NODE3 as 071207NODE3.27432773 (data type File) being
generated.
ANR3501I Backup set for NODE3 as 071207NODE3.27432773 (data type File) completed
successfully - processed 1678 files.
ANR3547I Backup set 071207NODE3.27432773 used volume
C:\TSMDATA\SERVER1\CFILECLASS\97053249.ost.
ANR1779I GENERATE BACKUPSET process completed: 1 backupset(s) were generated or
defined out of 1 backupset(s) requested by the command's specifications.
ANR0986I Process 43 for GENERATE BACKUPSET running in the FOREGROUND processed
1678 items for a total of 785,324,955 bytes with a completion state of SUCCESS at
10:47:55.
```

If your GENERATE BACKUPSET command only specifies filespaces that cannot be processed because of the ANR0952W condition, the entire command fails, as shown in Example 22-10.

Example 22-10 ANR3508W upon GENERATE BACKUPSET

```
tsm: HAGGIS>generate backupset node3 071207node3 9 namet=fsid devc=cfileclass
wait=yes
ANR0984I Process 44 for GENERATE BACKUPSET started in the FOREGROUND at 10:55:23.
ANR0952W The filespace \\lochnese\e$ cannot be included in the backup set because
it contains encrypted data.
ANR3508W Generation of backup set for NODE3 as 071207NODE3.27432776 (data type
File) failed - no filespaces to process.
ANR0985I Process 44 for GENERATE BACKUPSET running in the FOREGROUND completed
with completion state FAILURE at 10:55:23.
ANR2034E GENERATE BACKUPSET: No match found using this criteria.
ANS8001I Return code 11.
```

Export

For server data movement operations the encryption of the file is transparent, and you can also export the data to another server. In this case, the encryption key is exported along with the data. We demonstrate this by exporting NODE3 data from LOCHNESE to KODIAK. The LOCHNESE activity log messages are shown in Example 22-11. The EXPORT NODE command is restricted to V5.5 or later level servers, since a pre-V5.5 server cannot receive the exported encryption key information.

Example 22-11 EXPORT NODE NODE3 to server KODIAK

```
ANR2017I Administrator ADMIN issued command: EXPORT NODE node3 filedata=all
toserver=kodiak
```

```
ANR0984I Process 45 for EXPORT NODE started in the BACKGROUND at 11:42:04.
ANR0654I Restartable export command with export identifier EXPORT_NODE_45 started
as process 45.
..
ANR0515I Process 45 closed volume C:\TSMDATA\SERVER1\CFILECLASS\00000A42.BFS.
ANR0617I EXPORT NODE: Processing completed with status SUCCESS.
ANR0626I EXPORT NODE: Copied 1 node definitions.
ANR0627I EXPORT NODE: Copied 2 file spaces 0 archive files, 22030 backup files,
and 0 space managed files.
ANR0629I EXPORT NODE: Copied 842016697 bytes of data.
ANR0611I EXPORT NODE started by ADMIN as process 45 has ended.
ANR0986I Process 45 for EXPORT NODE running in the BACKGROUND processed 22033
items for a total of 842,016,697 bytes with a completion state of SUCCESS at
 11:43:42.
```

On the importing side, server KODIAK logs the messages in Example 22-12 on page 295.

Example 22-12 IMPORT NODE NODE3 from server LOCHNESE

```
ANR0984I Process 141 for IMPORT (from Server HAGGIS) started in the BACKGROUND at
11:43:13.
ANR4711I IMPORT SERVER (DATES=ABSOLUTE REPLACEDEFS=NO MERGE=NO PREVIEW=NO) by
administrator ADMIN from server HAGGIS (Process 45) starting as process 141.
ANR0610I IMPORT (from Server HAGGIS) started by ADMIN as process 141.
ANR0615I IMPORT (from Server HAGGIS): Reading EXPORT NODE data from server HAGGIS
exported 12/07/07 11:42:04.
ANR0635I IMPORT (from Server HAGGIS): Processing node NODE3 in domain
ACTIVEDOMAIN.
ANR2060I Node NODE3 registered in policy domain ACTIVEDOMAIN.
ANR2099I Administrative userid NODE3 defined for OWNER access to node NODE3.
ANR0636I IMPORT (from Server HAGGIS): Processing file space \\lochnese\e$ for node
NODE3 as file space \\lochnese\e$.
ANR0636I IMPORT (from Server HAGGIS): Processing file space \\lochnese\c$ for node
NODE3 as file space \\lochnese\c$.
ANR0617I IMPORT (from Server HAGGIS): Processing completed with status SUCCESS.
ANR0620I IMPORT (from Server HAGGIS): Copied 0 domain(s).
ANR0621I IMPORT (from Server HAGGIS): Copied 0 policy sets.
ANR0622I IMPORT (from Server HAGGIS): Copied 0 management classes.
ANR0623I IMPORT (from Server HAGGIS): Copied 0 copy groups.
ANR0624I IMPORT (from Server HAGGIS): Copied 0 schedules.
ANR0625I IMPORT (from Server HAGGIS): Copied 0 administrators.
ANR0891I IMPORT (from Server HAGGIS): Copied 0 optionset definitions.
ANR0626I IMPORT (from Server HAGGIS): Copied 1 node definitions.
ANR0627I IMPORT (from Server HAGGIS): Copied 2 file spaces 0 archive files, 22030
backup files, and 0 space managed files.
ANR0629I IMPORT (from Server HAGGIS): Copied 842016697 bytes of data.
ANR0611I IMPORT (from Server HAGGIS) started by ADMIN as process 141 has ended.
ANR0986I Process 141 for IMPORT (from Server HAGGIS) running in the BACKGROUND
processed 22033 items for a total of 842,016,697 bytes with a completion state of
SUCCESS at 11:44:52.
```

Once the data is exported, we can then transparently restore the data from the new server. To prove that the data has been exported encrypted, we try to access the encrypted object again from a down-level client. The operation fails with the ANS1461E message, as shown in Example 22-13.

Example 22-13 ANS1461E during restore from server KODIAK

```
C:\Program Files\Tivoli\TSM\baclient>dsmc -node=node3
-tcps=kodiak.itsosj.sanjose.ibm.com -tcpp=1500
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 4, Level 1.2
  Client date/time: 12/07/2007 13:18:06
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.

Node Name: NODE3
Session established with server KODIAK: AIX-RS/6000
  Server Version 5, Release 5, Level 0.0
  Server date/time: 12/07/2007 13:19:23  Last access: 12/07/2007 13:18:05

tsm> res \\lochnese\e$\demodata\demodata.tar.gz
Restore function invoked.

 ** Unsuccessful **
ANS1461E Error processing '\\lochnese\e$\demodata\demodata.tar.gz': unsupported
encryption type.

Restore processing finished.

Total number of objects restored:         0
Total number of objects failed:           1
Total number of bytes transferred:        0  B
Data transfer time:                    0.00 sec
Network data transfer rate:            0.00 KB/sec
Aggregate data transfer rate:          0.00 KB/sec
Elapsed processing time:           00:00:04
```

22.1.3 Summary

Transparent encryption allows you to easily add a level of security to the data that you back up. Configuration is easy, and once set you can forget about the setting. The main limitation is that the file systems containing any transparently encrypted data cannot be added to a backup set. Also, be aware that encryption of any kind comes with a price, as it adds to the overall time it takes to complete your backups.

22.2 Securing client and server communication

Starting with Tivoli Storage Manager V5.5 you can add another level of data protection by using Secure Sockets Layer (SSL) for communication between the server and the backup-archive client, API, and administrative command-line client (**dsmadmc**). SSL, developed by Netscape, is the standard technology for creating encrypted links between servers and clients. SSL provides a secure channel for servers and clients to communicate over open communications paths. With SSL, the identities of the parties are verified using digital certificates.

The IBM Global Security Kit (GSKit) is a required component for the Secure Socket Layer. Tivoli Storage Manager server and client installation procedures automatically silently install the GSKit.

SSL communication encryption is available for AIX and Windows platforms.

22.2.1 Server setup for SSL communication

To set up the server for SSL communication:

1. Configure the new SSLTCPPORT option in the server's dsmserv.opt as shown with Example 22-14. There is no default port. Choose a suitable free port (1503 in our example).

Example 22-14 Server SSLTCPPORT option - dsmserv.opt

```
*  =====================================================================
*
*  TCPIP
*
*   ********************************************************************
*   TCPPort
*
*   Specifies the TCP/IP port used to connect to the server.
*
*   Syntax
*   +------------------+-----------------------------------------------+
*   | TCPPort          | port_addr                                     |
*   +------------------+-----------------------------------------------+
*
COMMmethod TCPIP
TCPPort 1500
SSLTCPPORT 1503
```

   If your ADMINONCLIENTPORT option is set to NO, you also need to configure the SSLTCPADMINPORT option to point to the desired port number. The SSLTCPPORT and SSLTCPADMINPORT options are only honored if the COMMETHOD is set to either TCPIP or V6TCPIP.

2. After you set the option and re-start the server, if a key ring database (cert.kdb) does not exist and there is no password for it in the database, the key ring database is created. Then the following actions take place:

   a. The key ring database access password is automatically generated and stored in the Tivoli Storage Manager server database (encrypted). This allows the server to open the key ring database and access the certificate information.

   b. The Tivoli Storage Manager server generates a self-signed certificate and stores it in the key ring database in the server instance directory. This is the directory where the Tivoli Storage Manager server was started and that stores the dsmserv.dsk file.

   c. The public certificate, which can be used by the Tivoli Storage Manager client, is extracted and put in the cert.arm file.

> **Note:** This implementation of SSL requires only a server certification. There is no client certificate.

3. When the server is restarted and the SSL communication is correctly configured, message ANR8195I informs you that the server is ready for SSL communication, as shown in Example 22-15.

Example 22-15 ANR8195I, server configured for SSL communication

```
ANR8195I The SSL TCP/IP Version 4 driver is ready for connection with clients
on port 1503.
```

4. You can find the certification database (cert.kdb) and the certificate file (cert.arm) in your servers directory (in our example server1 on LOCHNESE). Example 22-16 on page 298 shows all the cert files in that directory.

Example 22-16 Server directory: cert files

```
C:\Tivoli\TSM\server1>dir cert*
 Volume in drive C has no label.
 Volume Serial Number is DCDC-8C9E

 Directory of C:\Tivoli\TSM\server1

12/10/2007  10:53 AM               824 cert.arm
12/10/2007  10:53 AM                80 cert.crl
12/10/2007  10:53 AM           125,080 cert.kdb
12/10/2007  10:53 AM                80 cert.rdb
               4 File(s)        126,064 bytes
               0 Dir(s)  89,068,150,784 bytes free
```

You will later (in step 3 on page 300) manually copy the cert.arm file to the client machines, where it is added to the local certificate database as a signed certificate. You must ensure that the transfer method is secure so that the original server certificate cannot be tampered with or replaced.

> **Important:** The cert.crl and cert.rdb files are used by GSKit. Do not delete those files.
>
> Make sure to take backup copies of your cert.arm and cert.kdb file in case you need to restore a Tivoli Storage Manager server.

We now describe the steps to complete on the client side once the cert.arm file is available for distribution.

22.2.2 Client setup for SSL communication

The following client components support SSL:

- Command-line client
- Administrative command-line client
- Backup-archive client GUI
- Client API

Only outgoing client-server connections support SSL. Incoming connections (for example, CAD, server-initiated schedule connections) do not support SSL. Client-to-client communications and the Web GUI also do not support SSL.

In order to enable SSL communication, you need to perform the following actions:

1. Make sure that the Tivoli Storage Manager server certificate, as described in step 4 on page 298, is available. Each Tivoli Storage Manager server generates its own certificate. To set up SSL communication you need to obtain a copy of the server’s cert.arm file. Do not actually copy it yet. We do that in step 3 on page 300.
2. Create the local key database. If a local key database already exists you can skip this step. If not, you need to create the key database. Perform the appropriate following section for Windows or AIX, then continue at step 3 on page 300. The **`gsk7capicmd`** command is provided by Global Security Kit (GSKit). On a Windows client, Tivoli Storage Manager automatically installs GSKit in c:\Program Files\IBM\gsk7. On AIX the default installation path is /usr/opt/ibm/gskta/bin/.

   If the GSKit has been installed before the Tivoli Storage Manager installation, it is possible that it is in some other location. On a Windows system you might have to obtain the GSKit location from the registry key HKLM\SOFTWARE\IBM\GSK7\CurrentVersion\InstallPath. On AIX, you usually find a link to the **`gsk7cap1cmd`** similar to /usr/bin/gsk7capicmd -> /usr/opt/ibm/gskta/bin/gsk7capicmd.

   > **Note:** On 64-bit Windows, the GSKit, by default, is installed in C:\Program Files\IBM\gsk7_64. Again, this can vary, so you should check the registry key. For a 64-bit platform, use the **`gsk7capicmd_64`** command.

   To create the key database on a Windows client:

   a. In a command window, change to your Tivoli Storage Manager client directory (DSM_DIR), for example:

      `cd “c:\Program Files\Tivoli\TSM\baclient”`

   b. Add the GSKit binary and library paths to the PATH environment variable, for example:

      `set PATH=C:\Program Files\IBM\gsk7\bin;C:\Pogram Files\IBM\gsk7\lib;%PATH%`

   c. Create the local key database, if it does not exist by using the command **`gsk7capicmd -keydb -create -db dsmcert.kdb -pw <password> -stash`**, as shown in Example 22-17. The password is used to access the database file using the **`gsk7capicmd`**. If you lose the password you no longer can make changes to the database. The Tivoli Storage Manager client, however, still can use the database file. In case you need to apply changes to the database you now have to delete the old database and create a new one.

Example 22-17 Windows: Create client key database

```
C:\Documents and Settings\Administrator>cd \Tivoli\tsm\baclient

C:\Tivoli\TSM\baclient>set PATH=C:\Program Files\IBM\gsk7\bin;C:\Pogram
Files\IBM\gsk7\lib;%PATH%

C:\Tivoli\TSM\baclient>gsk7capicmd -keydb -create -db dsmcert.kdb -pw
passphrase4gsk -stash

C:\Tivoli\TSM\baclient>dir dsmcert.*
 Volume in drive C has no label.
 Volume Serial Number is DCDC-8C9E
 Directory of C:\Tivoli\TSM\baclient

12/10/2007  01:29 PM                80 dsmcert.crl
12/10/2007  01:29 PM           120,080 dsmcert.kdb
12/10/2007  01:29 PM                80 dsmcert.rdb
12/10/2007  01:29 PM               129 dsmcert.sth
               4 File(s)        120,369 bytes
               0 Dir(s)  89,068,023,808 bytes free
```

The dsmcert.kdb is the key database and the dsmcert.sth is the stash file to hold the stored password. The password is used to encrypt the key database and the stash file is used later by the Tivoli Storage Manager client to retrieve the key database password.

To create the key database on an AIX client:

a. In a shell, change to your Tivoli Storage Manager client directory (DSM_DIR), for example:

```
cd /usr/tivoli/client/ba/bin
```

b. Make sure that the **gsk7capicmd** is found in your PATH statement. On our system a link is available to /usr/bin. See Example 22-18 for details.

c. Create the local key database if it does not exist:

```
gsk7capicmd -keydb -create -db dsmcert.kdb -pw <password> -stash
```

Example 22-18 shows the commands that we used on our AIX system.

Example 22-18 AIX: Create client key database

```
[root@Kodiak:]/ # cd /usr/tivoli/tsm/client/ba/bin
[root@Kodiak:]/usr/tivoli/tsm/client/ba/bin # which gsk7capicmd
/usr/bin/gsk7capicmd
[root@Kodiak:]/usr/tivoli/tsm/client/ba/bin # ls -al /usr/bin/gsk7capicmd
lrwxrwxrwx   1 root     system           34 Nov 13 12:54 /usr/bin/gsk7capicmd
-> /usr/opt/ibm/gskta/bin/gsk7capicmd
[root@Kodiak:]/usr/tivoli/tsm/client/ba/bin # gsk7capicmd -keydb -create -db
dsmcert.kdb -pw passphrase4gsk -stash
[root@Kodiak:]/usr/tivoli/tsm/client/ba/bin # ls -al dsmcert*
-rw-------   1 root     system           80 Dec 10 13:49 dsmcert.crl
-rw-------   1 root     system       120080 Dec 10 13:49 dsmcert.kdb
-rw-------   1 root     system           80 Dec 10 13:49 dsmcert.rdb
-rw-------   1 root     system          129 Dec 10 13:49 dsmcert.sth
```

Again, the dsmcert.kdb is the key database and the dsmcert.sth is the stash file to hold the stored password. The password is used to encrypt the key database, and the stash file is used later by the Tivoli Storage Manager client to retrieve the key database password.

3. Import the server certificate file cert.arm.

Now that you have created the key database you can import the certificate provided by your Tivoli Storage Manager administrator. Make sure that the transfer of the cert.arm file is secure. Copy the file to the DSM_DIR directory and use this command to import the certificate. It is the same on AIX or Windows. Specify a password and a label:

```
gsk7capicmd -cert -add -db dsmcert.kdb -pw <password> -label “TSM server
<servername> self-signed key” -file cert.arm -format ascii -trust enable
```

Example 22-19 shows the command that we submitted.

Example 22-19 Add the server key to the client database

```
gsk7capicmd -cert -add -db dsmcert.kdb -pw passphrase4gsk -label "TSM server
lochnese self-signed key" -file cert.arm -format ascii -trust enable
```

You can add more than one server certificate to the client key database. This allows the client to connect to different servers. Each different certificate must have a unique label. The label names are not important, but meaningful names should be used.

Once the certificate has been loaded to the client's database you can delete the local copy of the cert.arm file, as it is no longer needed to access the server.

4. Check that your dsmcert.kdb and dsmcert.sth exist in the Tivoli Storage Manager client directory -(DSM_DIR). If you followed the instructions in 2 on page 299, they will be. However, if you had a previous client key database installation, the files may be in another directory. In that case, copy the files dsmcert.kdb and dsmcert.sth into the Tivoli Storage Manager client directory.

   Now you are ready to enable SSL communication between Tivoli Storage Manager client and server.

5. Configure backup-archive client SSL options.

   Once the server certificate is added to the client key database, add the SSL YES option to the client options file and update the value of the TCPPORT to match the server's SSLTCPPORT (Example 22-14 on page 297), as shown in Example 22-20. The options are the same for AIX and Windows systems.

   Example 22-20 Client SSL option configuration

```
commmethod       TCPIP
ssl              yes
tcpport          1503
tcpserveraddress lochnese.itsosj.sanjose.ibm.com
```

6. From this point the communication between client and server is encrypted. See Example 22-21 for the client output of the client's QUERY SESSION command.

   Example 22-21 Client QUERY SESSION output

```
tsm> q session
TSM Server Connection Information

Server Name.............: HAGGIS
Server Type.............: Windows
Archive Retain Protect..: "No"
Server Version..........: Ver. 5, Rel. 5, Lev. 0.0
Last Access Date........: 12/10/2007 14:49:58
Delete Backup Files.....: "No"
Delete Archive Files....: "Yes"

Node Name...............: NODE5
User Name...............:

SSL Information.........: SSLv3 AES-256
```

7. As a Tivoli Storage Manager administrator, you can also use the QUERY SESSION command to verify the COMMMETHOD used between client and server, as shown in

Example 22-22. For an administrative command session, the Comm. Method also shows SSL.

Example 22-22 Server QUERY SESSION output

```
tsm: HAGGIS>q session 22 f=d

              Sess Number: 22
             Comm. Method: SSL
               Sess State: IdleW
                Wait Time: 7.8 M
               Bytes Sent: 911
              Bytes Recvd: 340
                Sess Type: Node
                 Platform: WinNT
              Client Name: NODE5
      Media Access Status:
                User Name:
Date/Time First Data Sent:
   Proxy By Storage Agent:
```

8. You now can also SSL encrypt your API sessions. To demonstrate, we use the sample API dapismp.exe. You can find the executable in the api\SAMPRUN directory for your installation. We contacted the server with the SSL YES option and the TCPPORT configured to point to the server's SSLTCPPORT. Again, we use the administrator's QUERY SESSION command to verify the COMMETHOD between the client and server, as shown in example Example 22-23.

Example 22-23 QUERY SESSION for API session

```
tsm: HAGGIS>q se 67 f=d

              Sess Number: 67
             Comm. Method: SSL
               Sess State: IdleW
                Wait Time: 33 S
               Bytes Sent: 744
              Bytes Recvd: 384
                Sess Type: Node
                 Platform: Sample-API
              Client Name: NODE5
      Media Access Status:
                User Name: node5
Date/Time First Data Sent:
   Proxy By Storage Agent:
```

However, to the API application, the SSL encryption is transparent. The Session Info Query, as shown with Example 22-24, returned by the sample API shows the client using the port configured for SSL communication, 1503.

Example 22-24 API: session info query

```
Server Information:
    Server name: HAGGIS
    Server Host: LOCHNESE.ITSOSJ.SANJOSE.IBM.COM
    Server port: 1503
    Server date: 2007/12/11  14:21:19
    Server type: Windows
    Server version: 5.5.0.0
    Server Archive Retention Protection : NO
  Client Information:
    Client node type: Sample-API
    Client filespace delimiter: :
    Client hl & ll   delimiter: \
    Client compression: Client determined (3u)
    Client archive delete: Client can delete archived objects
    Client backup delete: Client CANNOT delete backup objects
    Maximum objects in multiple object transactions: 2560
  General session info:
    Node:  NODE5
    Owner: node5
    API Config file:
  Policy Information:
    Domain name: ACTIVEDOMAIN
    Policyset name: ACTIVEPOLICY
    Policy activation date: 0/0/0  0:0:0
    Default management class: ACTIVEMGMT
    Backup retention grace period: 30 days
    Archive retention grace period: 365 days
```

The Session Options Query, as shown with Example 22-25, reports commMethod 1, which translates to TCPIP. So, from this information you cannot tell that SSL communication is used.

Example 22-25   API: session option query

```
DSMI_DIR                >C:\Program Files\Common Files\Tivoli\TSM\api<
DSMI_CONFIG             >.\node5.opt<
serverName              >DSMSERV<
commMethod               1
serverAddress           >LOCHNESE.ITSOSJ.SANJOSE.IBM.COM<
nodeName                >NODE5<
compress                 0
compressalways           1
passwordAccess           0
```

22.2.3 Recovery from a lost server key database

If you lose the server's key database, the server informs you during startup. Example 22-26 shows the related ANR8579E message. ANR8199I informs the Tivoli Storage Administrator that SSL communication could not be initialized.

Example 22-26   ANR8579E, SSL key database lost

```
ANR8579E The SSL key ring file does not exist, but the Tivoli Storage Manager
database contains a password for it.
ANR8199I The SSL TCP/IP driver could not be initialized on port 1503.
```

Example 22-27 shows the ANS1017E received upon a client's subsequent attempt to contact the server.

Example 22-27 ANS1017E, TCP/P failure

```
C:\Tivoli\TSM\baclient>dsmc
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 5, Level 0.0
  Client date/time: 12/10/2007 15:09:36
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.

Node Name: NODE5
ANS1017E Session rejected: TCP/IP connection failure
```

This is a fairly generic client message for TCP/IP connection failure. It is not specific to the SSL communication that the client tried to initiate here. If a client node owner contacts you with this problem, you might find it confusing until you determine that non-SSL clients can communicate and clients using SSL cannot. Check your activity log and make sure all communication ports initialized correctly.

At this point, if you do not have a backup copy of your keyring database, you need to delete the password stored in the Tivoli Storage Manager database using the administrative DELETE KEYRING command. Example 22-28 shows the server deleting the SSL-related information from its database.

Example 22-28 DELETE KEYRING command

```
ANR2017I Administrator ADMIN issued command: DELETE KEYRING
ANR4749I Key ring filename and password have been deleted from the server
database.
```

Once completed, you need to restart the server so that a new key database and a new cert.arm file will be created. You then need to redistribute the server certificate as described in 22.2.2, "Client setup for SSL communication" on page 298. Once completed, you can use SSL-encrypted communication again.

If you execute the DELETE KEYRING command and then later try to apply a previously saved keyring database copy, this is not possible, as the server no longer has the required password. Example 22-29 shows that the server still cannot initialze the SSL communication.

Example 22-29 SSL key database without valid server password

```
ANR8578E The Tivoli Storage Manager database does not have a password for the SSL
key ring file.
ANR8199I The SSL TCP/IP driver could not be initialized on port 1503.
```

The server does not try to overwrite the cert.kdb file found. You need to manually delete it and then you need to restart the server so a new key database and a new cert.arm file will be created. Redistribute the server certificate then as described in 22.2.2, "Client setup for SSL communication" on page 298.

At this point, if you did not activate the new cert.arm file on the client you still cannot access the server. Example 22-30 shows the session initialization failing with a bad certificate being submitted to the server.

Example 22-30 ANS1595E after replace of the server key database

```
C:\Tivoli\TSM\baclient>dsmc
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 5, Level 0.0
  Client date/time: 12/10/2007 15:48:37
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.

Node Name: NODE5
ANS1595E Bad server certificate.
```

To activate the cert.arm file, if you try to use the **gsk7capicmd -cert -add**, the command fails with GSKKM_ERR_DATABASE_DUPLICATE_KEY_LABEL. Instead, first delete the old instance and then re-add, as shown in Example 22-31.

Example 22-31 Activate a new server certificate on the client

```
C:\Tivoli\TSM\baclient>gsk7capicmd -cert -delete -db dsmcert.kdb -pw
passphrase4gsk -label "TSM server lochnese self-signed key"

C:\Tivoli\TSM\baclient>gsk7capicmd -cert -add -db dsmcert.kdb -pw passphrase4gsk
-label "TSM server lochnese self-signed key" -file cert.arm -format ascii
-trust enable
```

22.2.4 Key database management

You can administer the key database using either a command-line or GUI applet provided with GSKit.

Command line - gsk7capicmd

The **gsk7capicmd** command has other options. See the help, as shown in Example 22-32.

Example 22-32 Help for gsk7capicmd

```
C:\Tivoli\TSM\bin>gsk7capicmd -help
Object   Action       Description
----     ------       --------------------------------------------------------
-keydb   -changepw    Change the password for a key database
         -convert     Convert the format of a key database
         -create      Create a key database
         -delete      Delete a key database
         -expiry      Display password expiry
         -stashpw     Stash the password of a key database into a file
         -list        Currently supported types of key database.
-cert    -add         Add a CA Certificate
         -create      Create a self-signed certificate
         -delete      Delete a certificate
         -details     Show the details of a specific certificate
         -export      Export a personal certificate and associated private key
                      into a PKCS12 file or a key database
         -extract     Extract a certificate from a key database
         -getdefault  Show the default personal certificate
         -import      Import a certificate from a key database or a PKCS12 file
         -list        List certificates in a key database
         -modify      Modify a certificate (NOTE: the only field that my be
                      modified is the trust field)
         -receive     Receive a certificate
         -setdefault  Set the default personal certificate
         -sign        Sign a certificate
-certreq -create      Create a certificate request
         -delete      Delete a certificate request from a certificate request
                      database
         -details     Show the details of a specific certificate request
         -extract     Extract a certificate from a certificate request database
         -list        List all certificate requests in a certificate request
                      database
         -recreate    Recreate a certificate request
-version              Display ikeycmd version information
-help                 Display this help text
```

As a sample of the commands available, we list the contents of the key database in Example 22-33. It is useful to list the certificates, in case you forget the exact name.

Example 22-33 List certificates in database

```
C:\Tivoli\TSM\baclient>gsk7capicmd -cert -list -db dsmcert.kdb -pw
passphrase4server

Certificates in database: dsmcert.kdb
   TSM server lochnese self-signed key
   Thawte Personal Premium CA
   Thawte Personal Freemail CA
   Thawte Personal Basic CA
   Thawte Premium Server CA
   Thawte Server CA
   RSA Secure Server Certification Authority
   VeriSign Class 3 Secure Server CA
   VeriSign International Server CA - Class 3
   VeriSign Class 4 Public Primary Certification Authority - G3
   VeriSign Class 3 Public Primary Certification Authority - G3
   VeriSign Class 2 Public Primary Certification Authority - G3
   VeriSign Class 1 Public Primary Certification Authority - G3
   VeriSign Class 4 Public Primary Certification Authority - G2
   VeriSign Class 3 Public Primary Certification Authority - G2
   VeriSign Class 2 Public Primary Certification Authority - G2
   VeriSign Class 1 Public Primary Certification Authority - G2
   VeriSign Class 3 Public Primary Certification Authority
   VeriSign Class 2 Public Primary Certification Authority
   VeriSign Class 1 Public Primary Certification Authority
   Entrust.net Global Secure Server Certification Authority
   Entrust.net Global Client Certification Authority
   Entrust.net Client Certification Authority
   Entrust.net Certification Authority (2048)
   Entrust.net Secure Server Certification Authority
```

You can display full details of an individual certificate, as shown in Example 22-34.

Example 22-34 Display certificate details

```
C:\Tivoli\TSM\baclient>gsk7capicmd -cert -details -label "TSM server lochnese
self-signed key" -db dsmcert.kdb -pw passphrase4server

Label: TSM server lochnese self-signed key
Key Size: 1024
Version: X509 V3
Serial Number: 87 C3 88 A9 6F F9 3A 36
Issued By: TSM Self-Signed Certificate
TSM Network
TSM
US
Subject: TSM Self-Signed Certificate
TSM Network
TSM
US
Valid From: Sunday, December 9, 2007 3:48:07 PM PST To: Thursday, December 7, 20
17 3:48:07 PM PST
Fingerprint: 10:89:DE:34:E3:6D:BE:22:31:77:69:E9:E0:02:1C:20:19:3B:99:58
Signature Algorithm: 1.2.840.113549.1.1.4
Trust Status: enabled
```

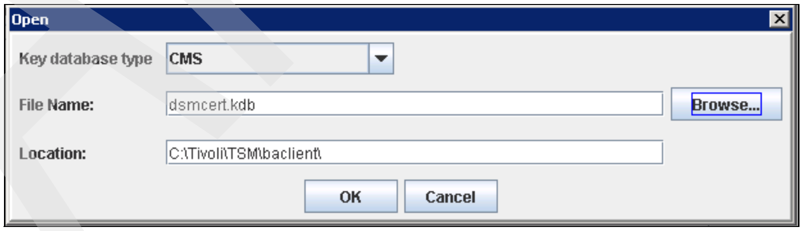
GUI

A GUI is available for the GSKit. Start it as shown in Example 22-35. Note that this applet requires the Java Cryptography Extension (JCE), so check whether your Java run time includes this. IBM JVM™ does include this.

Example 22-35 Start GSKit GUI

```
C:\>cd \Program Files\ibm\gsk7\bin
C:\Program Files\ibm\gsk7\bin>set JAVA_HOME=c:\Program Files\ibm\java50\jre
C:\Program Files\ibm\gsk7\bin>gsk7ikm
```

Open the CMS key database that you created in Example 22-17 on page 299 (ours is dsmcert.kdb in C:\Tivoli\TSM\baclient), as shown in Figure 22-1. Enter the password that you specified.



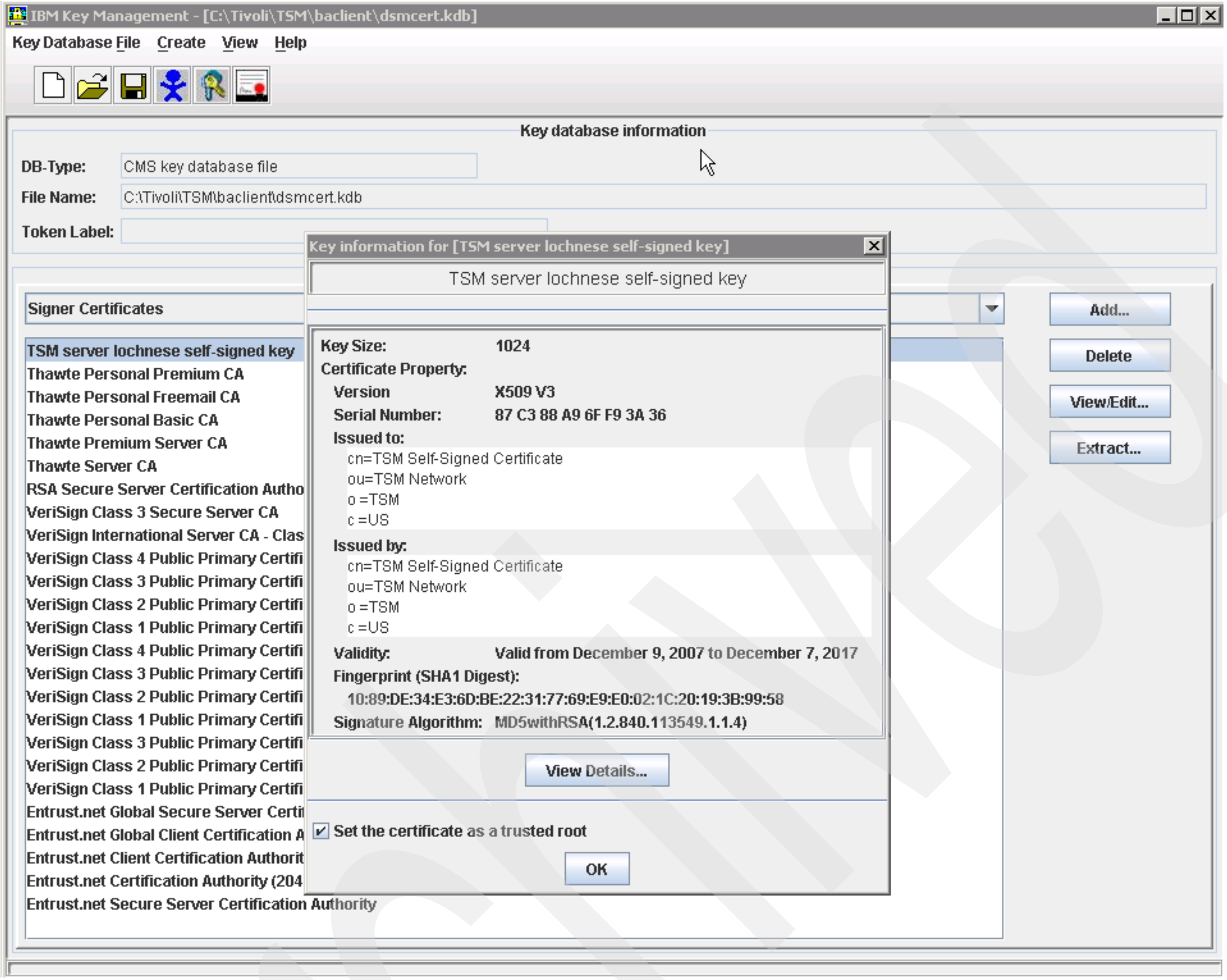
Key database type: CMS

File Name: dsmcert.kdb

Location: C:\Tivoli\TSM\baclient\

Figure 22-1 Open key database

You can now browse the database. Figure 22-2 on page 308 shows how you can display the details of the SSL certificate.



DB-Type: CMS key database file

File Name: C:\Tivoli\TSM\baclient\dsmcert.kdb

Token Label:

Signer Certificates

TSM server lochnese self-signed key
Thawte Personal Premium CA
Thawte Personal Freemail CA
Thawte Personal Basic CA
Thawte Premium Server CA
Thawte Server CA
RSA Secure Server Certification Autho
VeriSign Class 3 Secure Server CA
VeriSign International Server CA - Clas
VeriSign Class 4 Public Primary Certifi
VeriSign Class 3 Public Primary Certifi
VeriSign Class 2 Public Primary Certifi
VeriSign Class 1 Public Primary Certifi
VeriSign Class 4 Public Primary Certifi
VeriSign Class 3 Public Primary Certifi
VeriSign Class 2 Public Primary Certifi
VeriSign Class 1 Public Primary Certifi
VeriSign Class 3 Public Primary Certifi
VeriSign Class 2 Public Primary Certifi
VeriSign Class 1 Public Primary Certifi
Entrust.net Global Secure Server Certi
Entrust.net Global Client Certification A
Entrust.net Client Certification Authorit
Entrust.net Certification Authority (204
Entrust.net Secure Server Certification Authority

Key information for [TSM server lochnese self-signed key]

TSM server lochnese self-signed key

Key Size: 1024
Certificate Property:
Version X509 V3
Serial Number: 87 C3 88 A9 6F F9 3A 36
Issued to:
cn=TSM Self-Signed Certificate
ou=TSM Network
o =TSM
c =US
Issued by:
cn=TSM Self-Signed Certificate
ou=TSM Network
o =TSM
c =US
Validity: Valid from December 9, 2007 to December 7, 2017
Fingerprint (SHA1 Digest):
10:89:DE:34:E3:6D:BE:22:31:77:69:E9:E0:02:1C:20:19:3B:99:58
Signature Algorithm: MD5withRSA(1.2.840.113549.1.1.4)

☑ Set the certificate as a trusted root

Figure 22-2 Show details of a self-signed key

22.2.5 Common client configuration problems

In this section we describe some common mistakes that can be made in configuring SSL after setting up the client's server certificate database.

SSL set Yes, TCPPORT does not match SSLTCPPORT

One scenario is that you configure the SSL YES option and forget to match the TCPPORT to the servers SSLTCPPORT. Then if you try to connect to the server you immediately see the error message s shown in Example 22-36.

Example 22-36 ANS1592E: SSL YES, trying to communicate with server TCPPORT

```
C:\Tivoli\TSM\baclient>dsmc
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 5, Level 0.0
  Client date/time: 12/10/2007 16:24:15
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.

Node Name: NODE5
ANS1592E Failed to initialize SSL protocol.
```

For this session, the server reports a protocol error. Example 22-37 shows the related ANR0440W message.

Example 22-37 ANR0440W with wrong client configuration.

```
ANR0440W Protocol error on session 22 for node  () - invalid verb header
received.
```

Note that the nodename is not reported with the message, since the server listening on the TCPPORT is not able to extract the nodename from the SSL encrypted communication buffer passed in.

SSL set No, TCPPORT points to SSLTCPPORT

In the next scenario, let us say that you configure the default SSL NO option, but accidentally specify the client TCPPORT to point to the server's SSLTCPPORT. In this case, if you start the client session you see the session hanging until it eventually times out or you stop the session. Example 22-38 shows the client message for a failed connection attempt.

Example 22-38 SSL NO, trying to communicate with server SSLTCPPORT

```
C:\Tivoli\TSM\baclient>dsmc
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 5, Level 0.0
  Client date/time: 12/10/2007 15:54:07
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.

Node Name: NODE4
ANS1017E Session rejected: TCP/IP connection failure
```

The server's activity log will help you analyze this situation with the messages reported in Example 22-39.

Example 22-39 SSL socket initialization error

```
ANR8583E An SSL socket initialization error occurred on session 23.  The GSKit
return code is 410.
ANR8581E An SSL read error occurred on session 23.  The GSKit return code is 406.
```

Lost or inaccessible client key database

If you lose your client key database, dsmcert.kdb, or the user does not have the rights to access the database file, the Tivoli Storage Manager client terminates the **dsmc** process after message ANS1593E is reported (Example 22-40). In this case you need to either recreate the database (as described in 22.2.2, "Client setup for SSL communication" on page 298) or make sure that the user has sufficient rights to access it.

Example 22-40 ANR1593E: lost client key database

```
C:\Tivoli\TSM\baclient>dsmc
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 5, Level 0.0
  Client date/time: 12/11/2007 11:39:24
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.

Node Name: NODE5
ANS1593E Cannot open the key database.
```

GSKit not found

Example 22-41 shows the error message if the GSKit installation is corrupted or uninstalled. On AIX, you can re-install GSKit since it is shipped as a separate fileset. On Windows, you probably have to re-install the Tivoli Storage Manager client package.

Example 22-41 Error when GSKit is not found

```
C:\Tivoli\TSM\baclient>dsmc
ANS1464S Cannot load ICC encryption library.
```

22.2.6 Summary

Tivoli Storage Manager V5.5 now allows for industry-standard SSL-based secure communications between the Tivoli Storage Manager client and server. The support is available for AIX and Windows clients and servers. As shown in this section, it is easy to configure and adds another level of security to your installation. It effectively secures the client/server authentication and provides encryption for the rest of the session.

23

HSM for Windows V5.5

This chapter describes the following enhancements for the IBM Tivoli Storage Manager Hierarchical Storage Management client (HSM client) for Windows V5.5:

- Backup integration - Enhanced integration with the backup-archive client ensures there is a current copy of the file content in a Tivoli Storage Manager server backup for each backed up stub file.
- Reconciliation - After migrated files have been modified or deleted, obsolete objects exist on the Tivoli Storage Manager server in the HSM archive. Reconciliation removes these objects from the Tivoli Storage Manager server and also detects orphans in the local file system.
- Scalability and performance enhancements for data movement.
- HSM GUI enhancements.

Additional enhancements in the IBM Tivoli Storage Manager Hierarchical Storage Management client were released in V5.4. These are discussed in Chapter 16, “HSM for Windows V5.4” on page 205. That chapter also includes an introduction to Hierarchical Storage Management functionality in 16.1, “Hierarchical Storage Management” on page 206 and a hints and tips section in 16.6, “Hints and tips for using HSM” on page 228.

For more details about the installation and configuration of the HSM client see *Tivoli Storage Manager HSM for Windows Administration Guide*, SC32-1733, and *Using the Tivoli Storage Manager HSM Client for Windows*, REDP-4126.

23.1 Backup integration

The enhanced integration between the HSM for Windows client and the Tivoli Storage Manager backup-archive client ensures that the backup-archive client, independently of the HSM client, always maintains a copy of the complete file in the backup pool, whether this file is migrated or not.

In other words, for migrated files there will exist two identical versions of the file on the Tivoli Storage Manager server. One is in the HSM archive, created by the HSM client, and one is the backup copy in the backup pool, created by the backup-archive client. This ensures that each stub file always has an associated current copy of the complete file in the backup pool. The stub file and the complete file version are associated with each other and managed as a single version of the file in the Tivoli Storage Manager server, as shown in Figure 23-1. The copy of the complete file will not be expired until the copy of the stub expires.

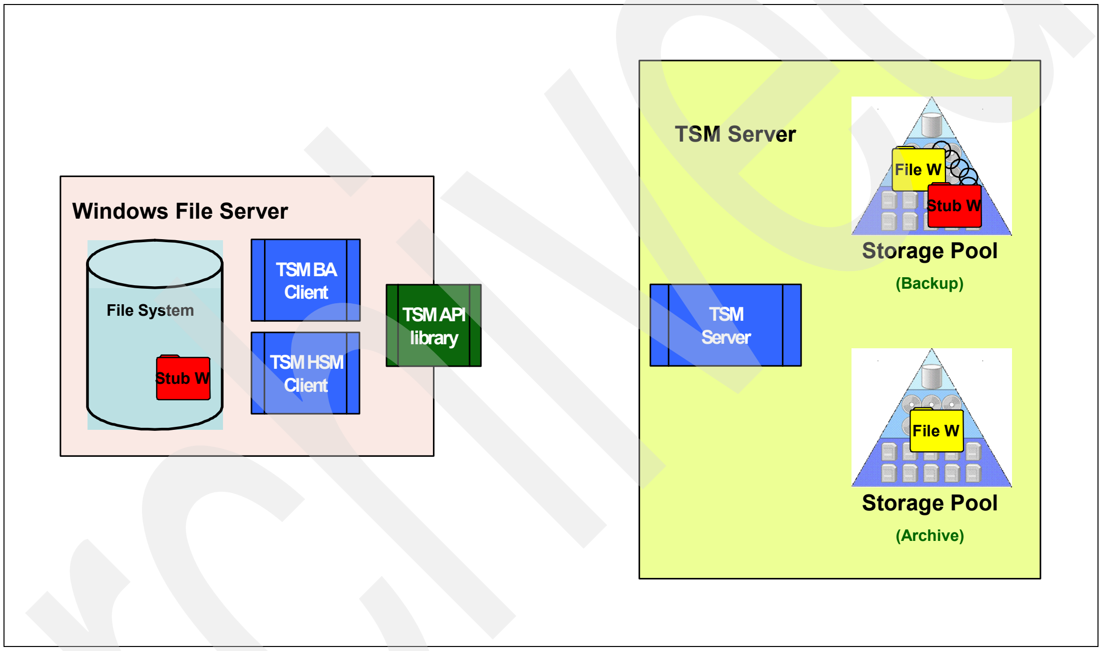


Figure 23-1 Backup integration: stub file and complete file are tied together in the backup pool

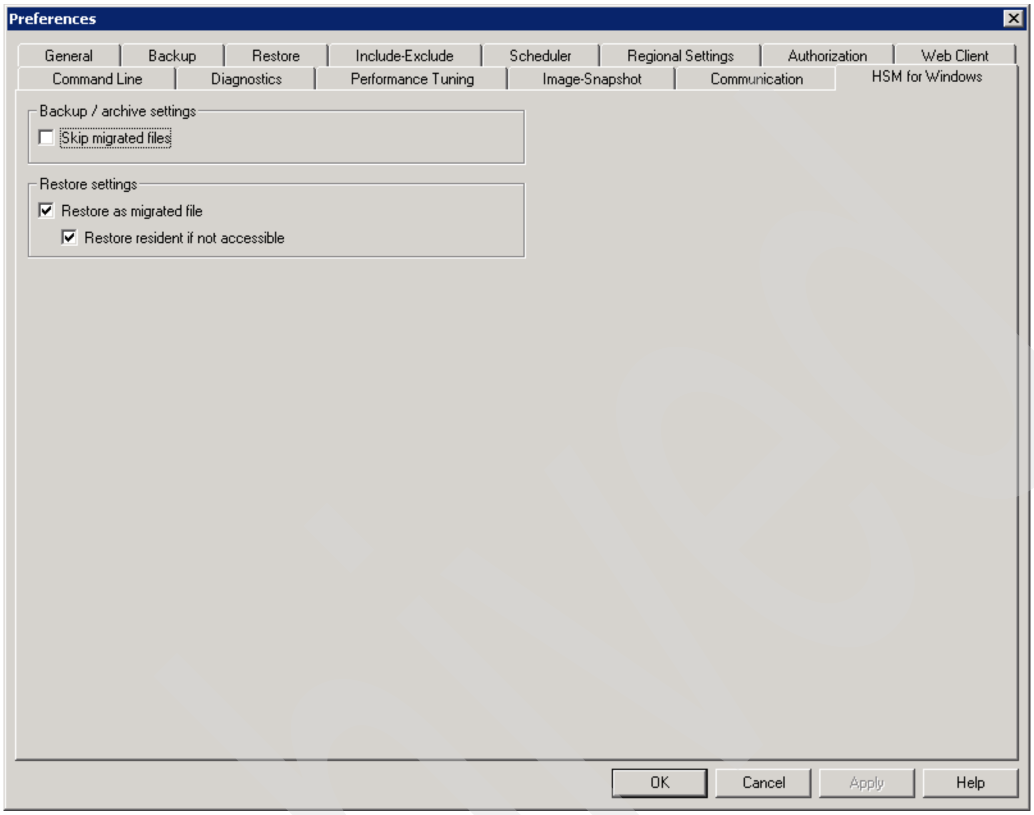
Because of this, when restoring files, the backup-archive client can always recreate the complete file from the backup only, even in the case of a HSM client problem (for example, if the copy in the HSM archive has been erroneously deleted). Therefore, when restoring, either the complete file or the stub file can be recreated.

Attention: For the full support of the backup integration you are required to use at least the V5.5.0 for the Tivoli Storage Manager server, backup-archive client, and the HSM for Windows client.

Even with the enhanced backup integration, it is still possible to use different Tivoli Storage Manager servers for HSM and backup-archive client functions.

Three new backup-archive client options control how the HSM client data is handled by the Tivoli Storage Manager backup-archive client. The **S**kip migrated files option regulates backup and archive operations on stubs. The two restore options, Restore as migrated file and Restore resident if not accessible, define how stubs are restored.

These options can be configured in the backup-archive GUI by selecting **Edit** ∅ **Preferences** ∅ **HSM for Windows**, as shown in Figure 23-2 on page 313, as well in the backup-archive client options file (dsm.opt).



Backup / archive settings

☐ Skip migrated files

Restore settings

☑ Restore as migrated file

☑ Restore resident if not accessible

Figure 23-2 HSM for Windows plug-In in the backup-archive client

> **Note:** The HSM for Windows tab is only available if the HSM for Windows client is installed on the system.

Table 23-1 relates the name of the check box in the GUI client tab with the short option name used in the backup-archive client option file.

Table 23-1 Backup-archive HSM for Windows option names

HSM for Windows preferences tab check box name	**Short option name (dsm.opt)**	**Default**
Skip migrated files	SKIPMIGRATED	Unchecked (no)
Restore as migrated file	RESTOREMIGSTATE	Checked (yes)
Restore resident if not accessible	RESTORECHECKSTUBACCESS	Checked (yes)

We now describe these options in more detail.

23.1.1 Backup and archive of migrated files

The *skip migrated files* option affects how the backup and archive operations handle migrated files (stub files). If the default SKIPMIGRATED NO is used, the behavior is different if you use an incremental backup operation compared to a selective backup or archive operation.

A selective backup or an archive operation with the default setting will always recall the files and then perform the specific operation (selective backup or archiving the files). After the selective backup or archiving operation is finished the files are not automatically remigrated. This could be done as a separate activity with the HSM client. The behavior has changed compared with pre-V5.5 backup-archive clients. A pre-V5.5 backup-archive client would always back up or archive the stub file.

> **Attention:** A selective backup or an archiving operation could cause mass recalls if the default setting SKIPMIGRATED NO is used.

An incremental backup with the default SKIPMIGRATED NO recalls the files if an appropriate copy of the complete files does not exist in the backup and backs up then the complete files. The files could then be remigrated with the HSM client. If a copy of the files already exists in the backup, the stub files will be backed up and linked with the last complete file in the backup. The stub file and the complete file version are always associated with each other and managed as a single version of the file in the Tivoli Storage Manager server. Therefore, the copy of the complete file will not be expired until the copy of the stub expires.

If you use the option SKIPMIGRATED YES (which is *not* the default) for any incremental, selective, or archive operation, the stub files will be ignored by the Tivoli Storage Manager backup-archive client.

Updating from a pre-V5.5 HSM environment to V5.5

If files have been backed up and migrated with a client older then HSM client V5.5, then the initial backup with the V5.5 client forces recalls of all migrated files. If no additional action is taken, then the file system could potentially run out of space. With the client option SKIPMIGRATED, you have the option to avoid such a situation after the upgrade.

You can run your normal backup with SKIPMIGRATED YES to avoid massive recalls and to back up the resident files only. With this option set, the backup-archive client still backs up the active (not-migrated) data in the file system. In parallel, you can back up the directories that contain the stub files directory by directory with the option SKIPMIGRATED NO to control the amount of recalls. After the backup of these directories is done, files can be re-migrated with the HSM for Windows client.

Impact of changing file encryption

Take special care when applying encryption to or removing encryption from resident files or stub files. When you change the encryption of a file, the backup and resident file content is no longer the same.

When the encryption of a file has changed, the backup-archive client treats this as a content change. If this applies to a migrated file, a recall is triggered at the next incremental backup. Thus, if you change the encryption status of many stubs, a massive recall might be triggered at the next incremental backup, which might cause an out-of-space condition. To avoid this situation, set the encryption status of files before backing up the resident files.

Note: Recall quotas could also protect you from uncontrolled mass-recall situations. They are discussed in 16.5, “Recall quotas” on page 226.

23.1.2 Restore of migrated files

In case of a restore, the two options *restore as migrated file* and *restore resident if not accessible* define how stubs are restored. The options do not affect an archive retrieve, because no stub files are stored in an archive. By default (RESTOREMIGSTATE YES), the stub is restored, but only if the stub is accessible (RESTORECHECKSTUBACCESS YES).

- RESTOREMIGSTATE defines whether the stub file or the complete file is restored.
  - YES: The stub is restored.
  - NO: The resident file is restored.

  The option RESTORECHECKSTUBACCESS is applicable only if the value of RESTOREMIGSTATE is YES.
- RESTORECHECKSTUBACCESS verifies the readability of a stub file before restoring the corresponding migrated file as a stub. If the stub file is not readable, the file will be restored completely (in the resident state) and not as a stub. When the default RESTORECHECKSTUBACCESS YES is used the following conditions must be met for a file to only be restored as stub:
  - The file was migrated on the last backup.
  - The HSM for Windows client is installed.
  - The restored object is the active version.
  - The original file system and the target file system are of the same type (NTFS).
  - The file system, high- level name, and low-level name are identical (source and destination).

It is preferable to restore only the stub if possible, since this will reduce the restore time, since a smaller amount of data is transmitted, and also saves space on the client, since the entire file will only be required to be restored if and when it is recalled.

23.1.3 Backup before migrate in V5.5

If the backup before migrate option is selected, the HSM client invokes the backup-archive client for all files to migrate and will then migrate only those files that have been successfully backed up. More details about backup before migrate are in 16.3, “Backup integration - backup before migrate” on page 210.

In order to verify whether a file has been backed up, the HSM client now uses a new AUDIT log. As this AUDIT log creates exactly one failure or success message for each file, the HSM client is now able to do a much more detailed analysis, and prevent situations where files are not migrated, although they were backed up. The AUDIT log is stored by default in C:\Program Files\Tivoli\TSM\hsmclient\tmp. This change (moving from trace to AUDIT log) is transparent to the user. Therefore, there is no change in the behavior of the HSM client. Example 23-1 shows some sample entries in the AUDIT file.

Example 23-1 Sample audit entries

```
12/07/2007 16:58:01 TSM Backup-Archive Client Version 5, Release 5, Level 0.0
12/07/2007 16:58:04 ANS1650I Command: incremental -filelist="C:\Program
Files\Tivoli\TSM\hsmclient\tmp\dsmgui-backup.lst" -errorlogname="C:\Program
Files\Tivoli\TSM\hsmclient\logs\dsmgui-backup.log" -filesonly -auditlogging=full
-auditlogname="C:\Program Files\Tivoli\TSM\hsmclient\tmp\dsmgui-backup.audit"
12/07/2007 16:58:05 ANS1651I Backed Up: \\kcwc09b\e$\HSMData9
12/07/2007 16:58:05 ANS1651I Backed Up: \\kcwc09b\e$\HSMData9\itso.files1.txt
12/07/2007 16:58:05 ANS1651I Backed Up: \\kcwc09b\e$\HSMData9\itso.files2.txt
12/07/2007 16:58:05 ANS1651I Backed Up: \\kcwc09b\e$\HSMData9\itso.files3.txt
12/07/2007 16:58:05 ANS1651I Backed Up: \\kcwc09b\e$\HSMData9\itso.files4.txt
12/07/2007 16:58:05 ANS1651I Backed Up: \\kcwc09b\e$\HSMData9\itso.files5.txt
```

23.2 Reconciliation

The reconciliation process in the HSM client V5.5 is the process of synchronizing a volume, which you have configured for reconciliation, with the Tivoli Storage Manager server that you are using as the destination for the migrated files.

With a pre-V5.5 HSM client, files were migrated to the Tivoli Storage Manager server, but they were never deleted on the Tivoli Storage Manager server. Therefore, if a stub file is deleted, or if it has been modified and migrated again, the obsolete copies of the file will remain on the Tivoli Storage Manager server. Each obsolete copy of a file increases the storage resources required, as well as the software costs, since HSM for Windows is priced based on the capacity used on the Tivoli Storage Manager server for migrated files.

Figure 23-3 illustrates the high-level reconciliation process.

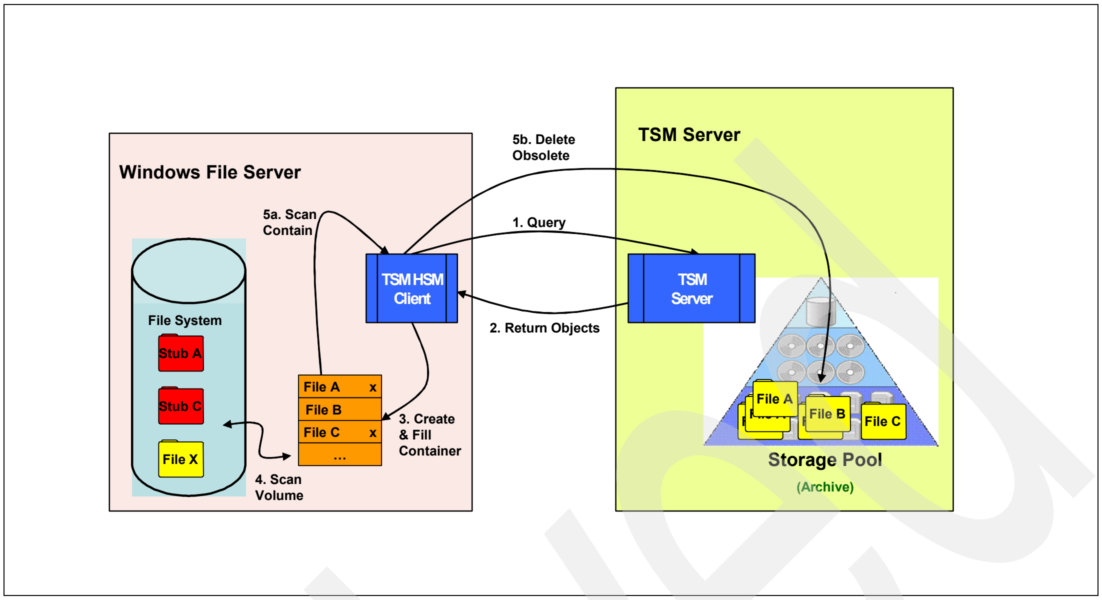


Figure 23-3 Reconciliation process

When reconciliation starts for a specific volume, it first obtains a list of all migrated files for that volume from the Tivoli Storage Manager server (1). The returned objects from the Tivoli Storage Manager server (2) are filled in a container, a temporary hidden file dsmrecon.bin in the root of the volume (3).

Note: Reconciliation stores about 100 bytes for each object in a preallocated table. This means that for 1 million migrated files, reconciliation needs 100 MB of temporary space on the volume.

Afterwards, the local file system will be traversed and the corresponding objects in the list will be marked as found (4). If an orphan is found (a stub on the volume, which has no corresponding object on the Tivoli Storage Manager), the name of the file is put in the file hsmmonitor-orphan.log (see “Orphan files” on page 321). The reconciliation process then scans the container (5a) to delete any objects that were not found on the Tivoli Storage Manager server (5b).

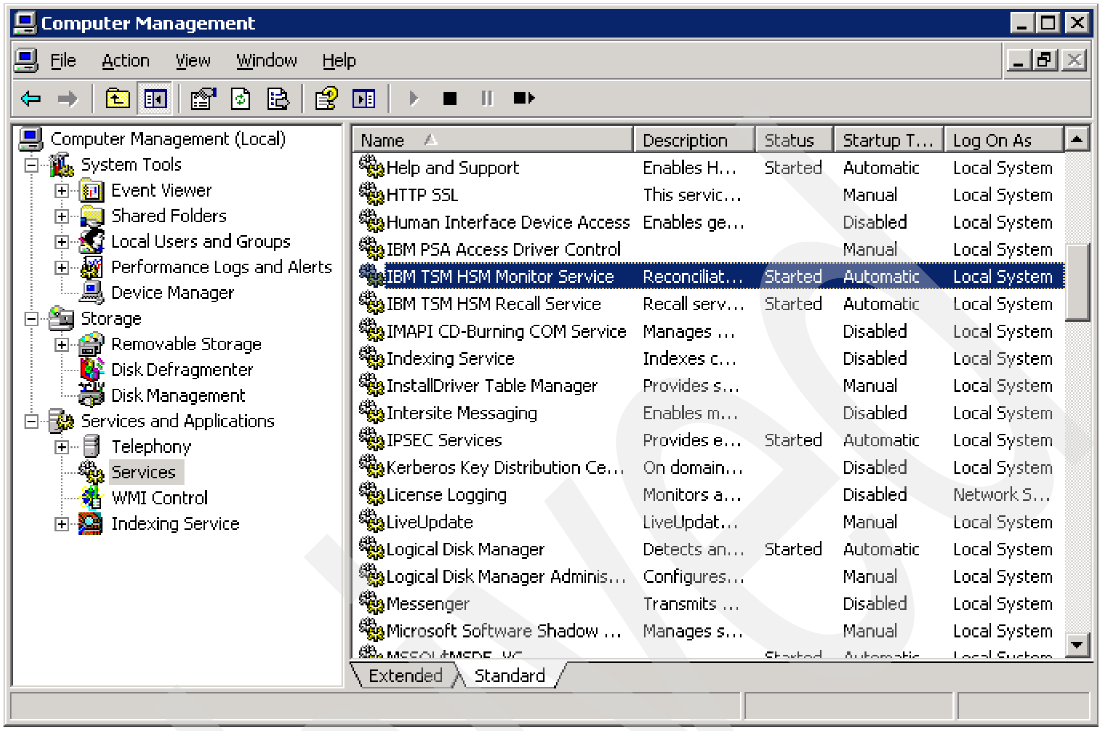
After running reconciliation, exactly one migrated object exists on the Tivoli Storage Manager server for each migrated file. So, by removing old and obsolete objects from the Tivoli Storage Manager server storage, reconciliation helps you to reduce your storage and license expenses.

Note that reconcile only marks the object for deletion on the Tivoli Storage Manager server. The Tivoli Storage Manager EXPIRE INVENTORY process deletes the objects.

Attention: As reconciliation deletes objects on the Tivoli Storage Manager server, we highly recommend backing up the file system before a reconciliation is started.

Reconcile configuration

The reconcile implementation runs as a Windows service called IBM TSM HSM Monitor Service (hsmmonitor.exe). This service is new in V5.5. The service runs reconcile threads and provides the traditional Windows interface for start/stop/restart. Figure 23-4 shows the service.

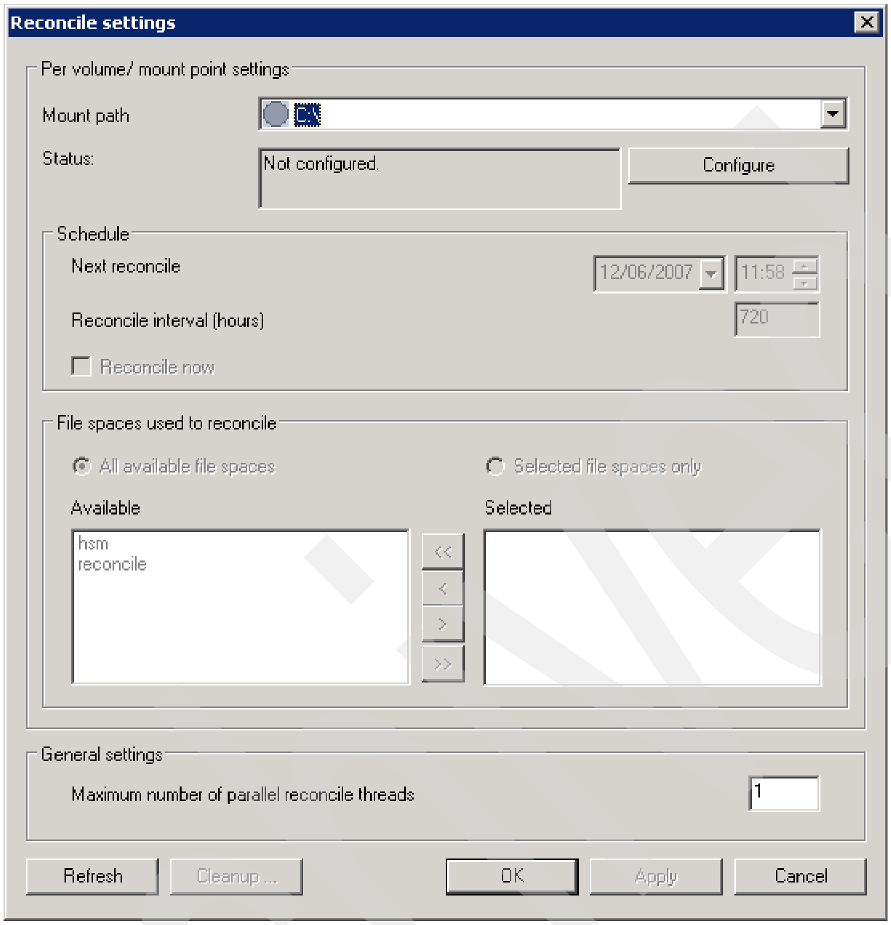


Name	Description	Status	Startup T...	Log On As
Help and Support	Enables H...	Started	Automatic	Local System
HTTP SSL	This servic...		Manual	Local System
Human Interface Device Access	Enables ge...		Disabled	Local System
IBM PSA Access Driver Control			Manual	Local System
IBM TSM HSM Monitor Service	Reconciliat...	Started	Automatic	Local System
IBM TSM HSM Recall Service	Recall serv...	Started	Automatic	Local System
IMAPI CD-Burning COM Service	Manages ...		Disabled	Local System
Indexing Service	Indexes c...		Disabled	Local System
InstallDriver Table Manager	Provides s...		Manual	Local System
Intersite Messaging	Enables m...		Disabled	Local System
IPSEC Services	Provides e...	Started	Automatic	Local System
Kerberos Key Distribution Ce...	On domain...		Disabled	Local System
License Logging	Monitors a...		Disabled	Network S...
LiveUpdate	LiveUpdat...		Manual	Local System
Logical Disk Manager	Detects an...	Started	Automatic	Local System
Logical Disk Manager Adminis...	Configures...		Manual	Local System
Messenger	Transmits ...		Disabled	Local System
Microsoft Software Shadow ...	Manages s...		Manual	Local System
MSSQL$MSDE_VC		Started	Automatic	Local System

Figure 23-4 WIndows services including the HSM Monitor service

Reconciliation is turned off by default. This means that the Windows service is running, but it must be explicitly enabled, or configured for each volume required in the system using the HSM client GUI (**Tools ∅ Reconciliation**) or with the command-line tool **`dsmhsmclc`**.

Figure 23-5 shows the Reconciliation settings window with an unconfigured drive and Figure 23-6 on page 320 shows a drive for which reconciliation is configured.



Reconcile settings

Per volume/ mount point settings

Mount path: C:\

Status: Not configured.

Schedule

Next reconcile: 12/06/2007 11:58

Reconcile interval (hours): 720

□ Reconcile now

File spaces used to reconcile

● All available file spaces ○ Selected file spaces only

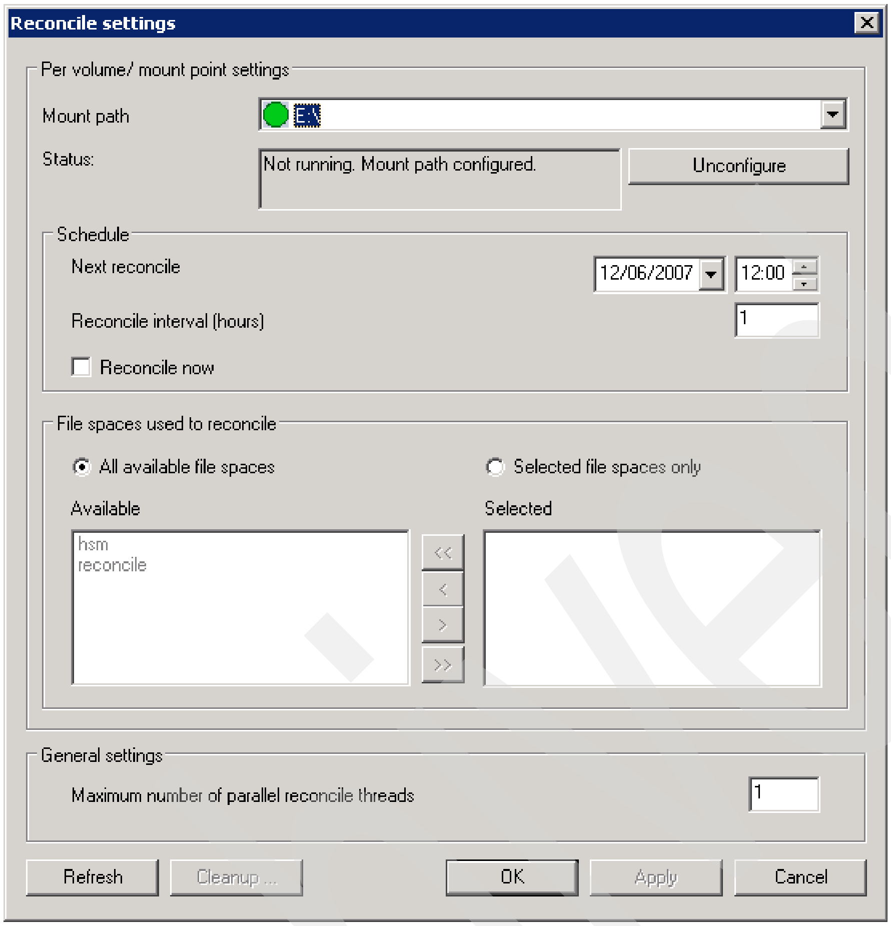
Available: hsm, reconcile

Selected:

General settings

Maximum number of parallel reconcile threads: 1

Figure 23-5 Reconcile settings window for an unconfigured drive



Reconcile settings

Per volume/ mount point settings

Mount path: E:\

Status: Not running. Mount path configured.

Schedule

Next reconcile: 12/06/2007 12:00

Reconcile interval (hours): 1

☐ Reconcile now

File spaces used to reconcile

● All available file spaces ○ Selected file spaces only

Available: hsm, reconcile

Selected:

General settings

Maximum number of parallel reconcile threads: 1

Figure 23-6 Reconcile settings window for a configured drive

As shown, there are several configurable options for the reconciliation process. These include:

- Mount path - for the volume for which reconciliation should be performed
- Next reconcile - when reconcile should start
- Reconcile interval (hours) - the interval between two subsequent reconcile runs
- Reconcile now - starts a reconcile process immediately after clicking Apply or OK
- File spaces used to reconcile - which file spaces should be included in the reconcile
- Maximum number of parallel reconcile threads - how many reconciliations can run in parallel

  If this number is exceeded, any further reconcile is delayed until a running reconcile has finished.

You can configure each of these settings for each volume individually (for example, drive e: could be reconciled once a week on Monday at 3 a.m., while drive f: might only be reconciled every fourth weekend on Sunday at 11 a.m.

The HSM client performs reconciliation automatically at intervals specified with the RECONCILEINTERVAL option that you define using the HSM client GUI or with the command-line tool **`dsmhsmclc`**. An administrative user can also start reconciliation manually at any time using the GUI (reconcile now) or the command line **`dsmhsmclc <vol_mount_path> -reconcilenow yes`**.

Note: Reconciliation should not be used with filespaces or volumes with migration jobs that have the action *keep the original file* or *delete the file* configured.

Orphan files

Reconciliation also checks whether there are stub files without a corresponding copy on the Tivoli Storage Manager server on the volume. These files are called *orphan* files, and when detected, they are listed in the hsmmonitor-orphan.log file, located by default in the HSM client log directory (default C:\Program Files\Tivoli\TSM\hsmclient\logs). If the reconciliation process finds orphan files on your volume, the process completes processing the volume, but does not delete any objects on the Tivoli Storage Manager server. You should check the hsmmonitor-orphan.log file carefully for any orphans and decide whether you could delete the orphan stub file or whether you need to restore the consistent copy from your backup (which is available because of the HSM client backup integration). When the reconciliation process completes without finding any orphan files, it deletes obsolete copies of migrated files on the Tivoli Storage Manager server.

Filespace considerations when using reconcile

Remember that within an HSM migration job, you can configure which filespace on the Tivoli Storage Manager server is used for the migrated files. Therefore, different files from one file system can be migrated to different filespaces on the Tivoli Storage Manager server, or even different versions of one file can be migrated to different filespaces on the Tivoli Storage Manager server.

The reconcile process is specific to each volume, and must query all filespaces on the Tivoli Storage Manager server that are associated with the HSM client node to obtain the information about all migrated files for this volume. This increases the time required for reconciliation of a single file system exponentially. To mitigate this you could restrict the Tivoli Storage Manager server queries to certain filespaces using the option FILESPACELIST in the HSM client GUI (file spaces used to reconcile) or with the command-line tool **`dsmhsmclc`**.

If files from several local file systems (volumes) are migrated to the same filespace, then the Tivoli Storage Manager server eventually (depending on the names of the files) returns not only the files from the volume, which is currently being reconciled, but also other files from other volumes.

Therefore, to improve reconciliation performance and avoid having to use the backup-archive client to restore files (which were erroneously deleted by the reconciliation), we recommend using separate filespaces for each local volume.

Changing drive letter or volume mount paths

We recommend that you do not change a drive letter or volume mount path after files are migrated if you plan to use reconciliation for this volume.

If it is necessary to change the drive letter or the volume mount path when reconciliation is activated, you could restore the consistent files from the backup-archive client and migrate them then again with HSM client.

Stub files with pre-V5.4 format

Reconcile ignores all files and their objects on Tivoli Storage Manager server that have been migrated with an old client (pre-V5.4) because the stub files in each version have a different format that is not compatible if reconciliation is used. To change the format of these pre-V5.4 stub files, a tool called **`dsmreconconverter`** is provided.

The **dsmreconconverter** command converts pre-V5.4 stubs to a format compatible with reconciliation. The command also checks all stub files and their Tivoli Storage Manager server objects for inconsistencies and tries to resolve them.

Further considerations when using reconcile

Do not plan to use reconcile for a local volume that contains a paging file (pagefile.sys). Because of the structure of the paging file, pagefile.sys is detected as an orphan file, and this causes reconcile to not delete any objects on the Tivoli Storage Manager server as long as the pagefile.sys exists on this volume. A fix is anticipated for this situation. Check for APAR number IC54660.

When you restore from a file-system image backup and plan to run reconciliation, you must restore the files that have been migrated after the image backup using the backup-archive client. Otherwise, migrated files, which have been created after the image backup, are deleted by the reconciliation process from the Tivoli Storage Manager server because stub files from the image are not readable and must be restored from the file backup.

23.3 Scalability and performance enhancements

The HSM client for Windows V5.5 includes enhancements to the scalability and performance of data movement. These are transparent. There is nothing required to be configured.

Migrating files

When migrating files:

- During the file system scan, memory handling reduces the amount of RAM required to build candidate lists.
- The file scanning, backup before migration (if used), and file migration processes occur in parallel to speed up migration.
- The migration processing splits the file reading processes to allow parallel buffer read and writes.

Retrieving files

When retrieving files:

- To reduce the Tivoli Storage Manager server retrieval time, the HSM console sorts file retrieval by tape order.
- The HSM console eliminates a re-query step to the Tivoli Storage Manager server by storing a key for each file.
- Files can now be retrieved when the IBM TSM HSM recall service is not running. A Tivoli Storage Manager HSM administrator can use the **dsmclc** command or the HSM for Windows client GUI.

Recalling files

You are no longer required to restart the HSM for Windows client to apply service configuration changes, such as changing the number of recall threads.

Filter driver

The improved memory usage of the HSM file system filter driver allows a quicker file recall and reduces uses of Windows non-paged pool memory.

23.4 HSM GUI enhancements

You can now use the HSM GUI to configure all settings required for the HSM client. Previously, for some settings it was necessary to edit the registry. This includes the following settings:

- Log settings for all applications: **Tools ∅ Trace Preferences**
- Trace file and listings file settings: **Tools ∅ Trace Preferences**
- File recall settings: **Tools ∅ Preferences ∅ Recall Service**
- Reconciliation settings: **Tools ∅ Reconciliation**

24

VMware consolidated backup with Tivoli Storage Manager V5.5

Beginning with Tivoli Storage Manager V5.5, support for VMware Consolidated Backup (VCB) environments is enhanced with a tighter integration between Tivoli Storage Manager and VMware. Previously, VMware's Integration Module to Tivoli Storage Manager was required. This is no longer true.

The Tivoli Storage Manager V5.5 client includes features that allow easier setup and management of VCB-based infrastructures, and that allow it to initiate backups in a VCB environment.

We provided some overview information of VCB in 17.2.3, "Initial support for VMware Consolidated Backup with Tivoli Storage Manager" on page 233. In this chapter we cover Tivoli Storage Manager V5.5 features for VCB backup of VMware images.

There are a number of types of VMware server available. In the rest of this chapter we discuss the VMware ESX server since that is the enterprise version and will most likely be used for production services.

For more information about VMware see:

http://www.vmware.com

24.1 Overview of VMware backup approaches with Tivoli Storage Manager V5.5

First we consider a few architectures for Tivoli Storage Manager environments.

24.1.1 Non-VMware environment

In a non-VMware Tivoli Storage Manager environment, it is typical to install Tivoli Storage Manager backup-archive client software on each client node. The clients send backup data to a Tivoli Storage Manager server that stores and tracks the stored objects (files, directories, databases, and so on). Figure 24-1 shows an example of such a traditional Tivoli Storage Manager setup.

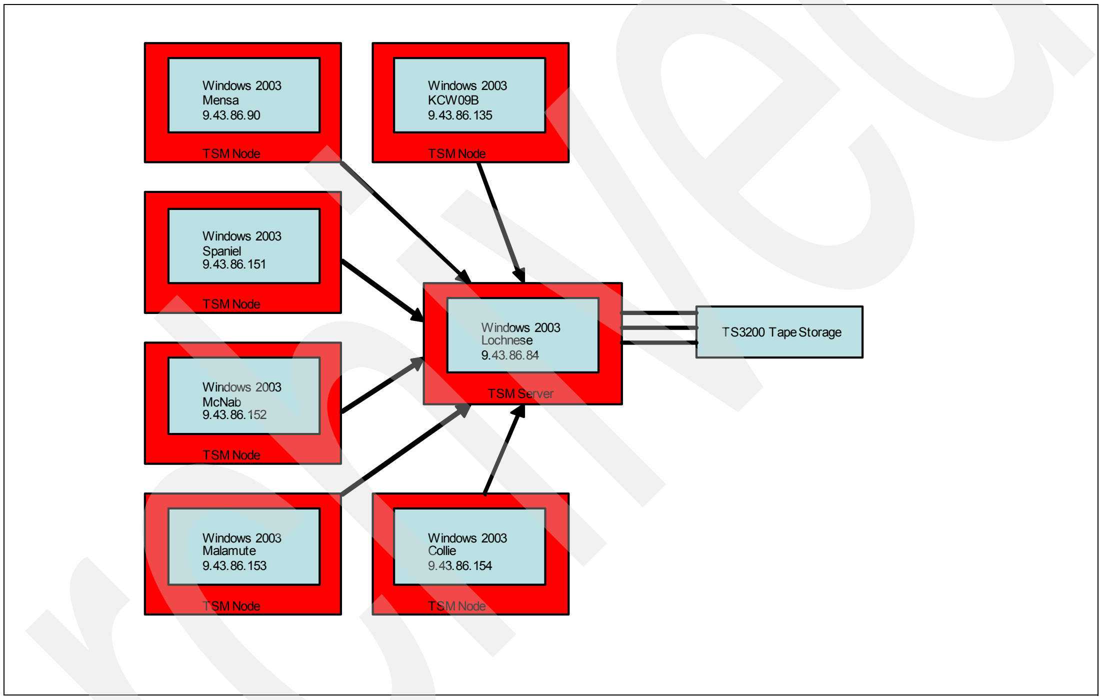


Figure 24-1 Traditional Tivoli Storage Manager setup

24.1.2 Install client on each VMware host

We could take exactly the same approach in a VMware environment (that is, install a Tivoli Storage Manager client on each hosted image). Figure 24-2 on page 327 shows a traditional Tivoli Storage Manager setup running on VMware ESX.

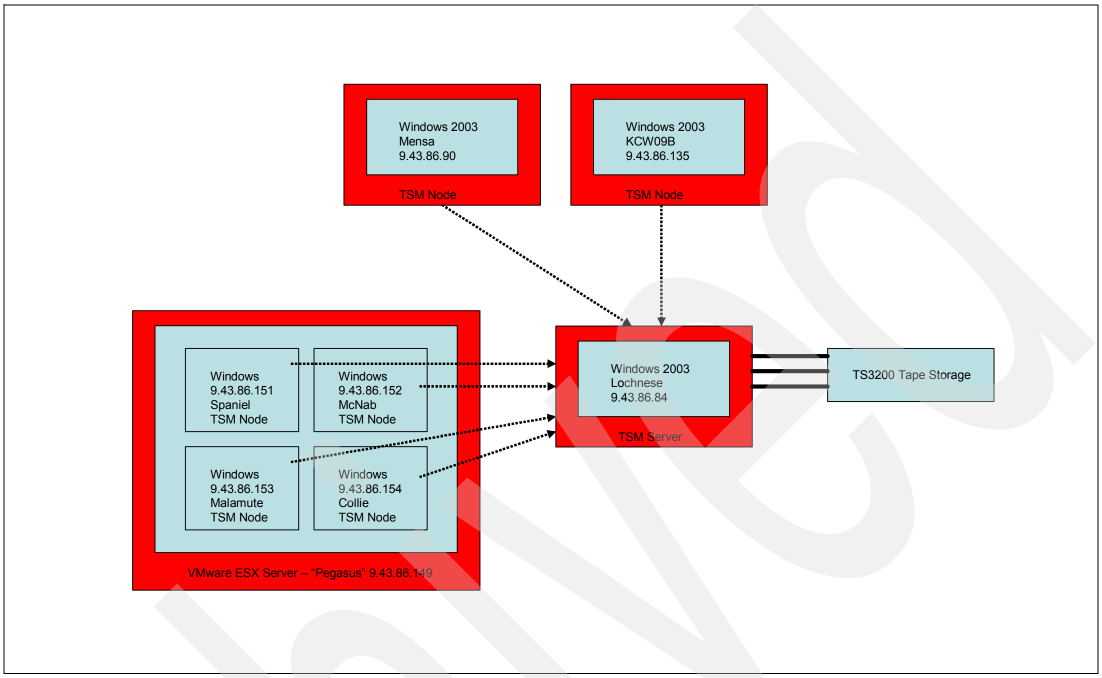


Figure 24-2 Traditional Tivoli Storage Manager setup on VMware ESX

Installing a Tivoli Storage Manager client on each of potentially many hosted images is not necessarily the ideal or most efficient configuration because of the virtualized environment. For the sake of clarity, we refer to a hosted operating system image as a *guest* in the rest of this document.

By definition and design, VMware ESX servers share physical hardware resources between the guests in order to make more effective use of those resources. If each guest installs and runs a Tivoli Storage Manager client, it is possible that many of the guests will attempt backup or restore at the same time, which may put an unacceptably high load onto the ESX server as a whole. This could impact performance of the actual production applications. Even if measures are put into place to prevent this scenario from occurring (for example, by careful scheduling of backup operations), there can be good reasons to isolate the backup processes from the live production environment. These reasons include:

- Running multiple Tivoli Storage Manager clients simultaneously on the same physical hardware (in different guests) may use up too much of the following finite resources to keep the live-running services performing as required on both the guest doing the backup and possibly on other guests:
  - CPU
  - Disk I/O
  - PCI bus bandwidth
  - Storage area network bandwidth
  - Memory
  - Network bandwidth

- Configuring scheduling to avoid concurrent backups from the same ESX server may prove complex and hard to maintain or scale.
- Installing and customizing a large number of Tivoli Storage Manager clients requires some administrative effort, both initially and whenever software upgrades are required. Of course, this affects non-virtualized environments too, but the difference may be more apparent in an automated VMware environment, where builds are otherwise relatively fast and simple.
- Keeping as much of the backup workload away from the live system as possible may help with performance diagnostics issues.
- It may be that the production VMware services are hosted on a type of system where the processing and memory characteristics of the hardware are more important than the storage I/O capability of the machine (an example here could be Blades, which sometimes give up some I/O ability and expandability in favor of a smaller form factor).
- Virtualized environments tend to be dynamic. Guests can be frequently added, deleted, or migrated between VMware hosts. Traditional backup methods do not have the tools to handle this sort of change very easily.

A further reason to offload backup from the virtualized environment is that for a VMware guest, Tivoli Storage Manager LAN-free backup is not supported. Therefore, all the backup data travels via the IP network to the Tivoli Storage Manager server. The IP network could become a point of contention here, along with the processing overhead of TCP on the guest and ESX server. With a Tivoli Storage Manager client running on a guest, there is no supported way to achieve LAN-free backup of that guest directly.

24.1.3 VMware proxied backup with VCB

A principal characteristic of VCB is that it allows backup activity to be *proxied* to a separate, non-virtualized system with suitable access and configuration. With proxying, another system performs the backup operations on behalf of the guests, therefore off-loading the workload. Proxying also allows LAN-free backup of data from VMware guests.

Figure 24-3 shows an overview of a VCB proxied environment in the sample configuration that we will use to demonstrate VCB features with Tivoli Storage Manager.

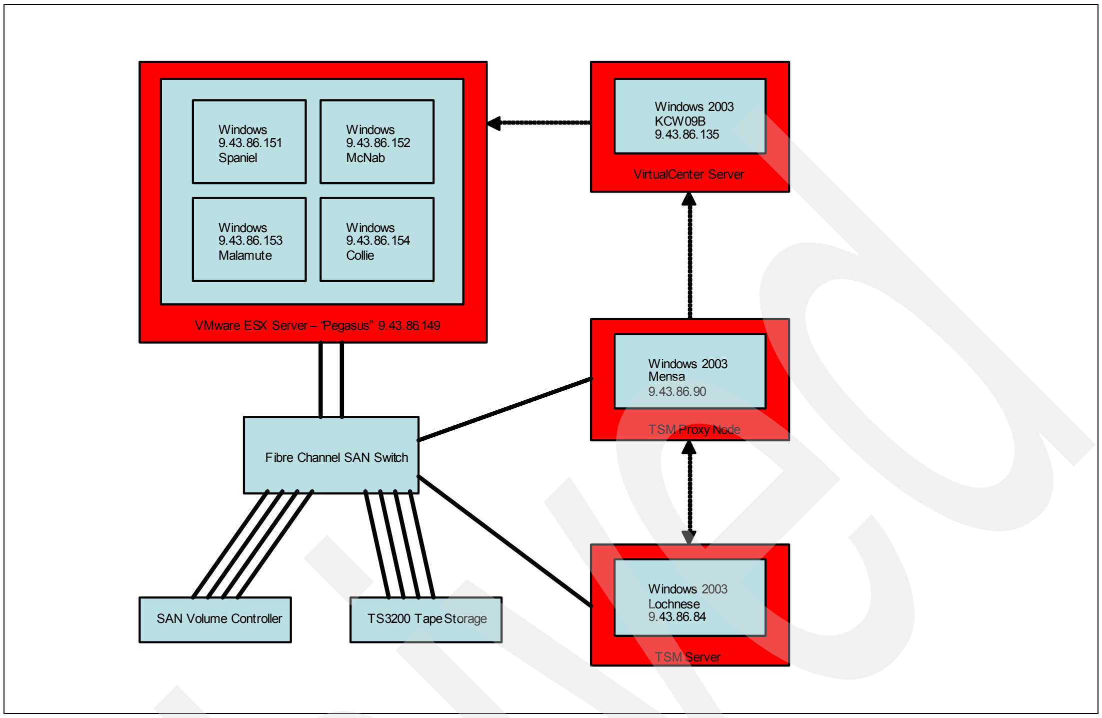


Figure 24-3 Overview of VCB test environment

In this environment:

- VMware ESX server (PEGASUS) hosts four guest images (SPANIEL, MCNAB, MALAMUTE, and COLLIE) installed on SAN-attached disk (an IBM System Storage SAN Volume Controller, in our example).
- The proxy node (MENSA) will run the VCB backup of the guests, since it has access to the same SAN-storage on the SVC. The backup may be initiated using a scheduler tool (for example, the **`dsmsched`**).
- The proxy node communicates with the VirtualCenter server, KCW09B.
- The backups are sent to the Tivoli Storage Manager server, LOCHNESE.

VCB offloads much of the backup activity from a production VMware environment (usually one or more ESX servers). Fundamentally, VCB has two modes: full backup (which is similar to an image backup of a virtual machine's disk) and file-level backup. At the time of writing, Tivoli Storage Manager can be used for VCB file-level backup of Windows guests only or full backup. In order for the backups (either file-level or full backup) generated by VCB to be consistent, VMware performs an operation called a *snapshot*.

VMware VCB snapshot

A VCB snapshot is created as follows:

1. The ESX server temporarily freezes (pauses) a running VMware guest, then redirects all future writes to that guest's disk to a separate cache instead, for the duration of the snapshot.
2. If VMware Tools is installed on the guest, it also flushes any Windows disk buffers so that the Windows file system is consistent before the backup takes place.

3. Once the write cache is in place, the guest is thawed (resumed) and continues running as normal. The time taken to establish the cache is typically in the order of a few seconds or less.
4. A backup of the snapshot can now be taken.
5. When the snapshot backup is completed, the ESX server tidies up the cached writes by writing them to the guest's disk. This happens transparently (and in the background) to the guest. In this way, VMware temporarily creates a read-only version of the guest's disk, which can be backed with minimal impact to production operations.

> **Note:** VMware snapshots should not be made to persist for longer than necessary. While a snapshot is in place, any changed data on the guest will use up extra space on the ESX server as it is written to the cache, and may slow down operations on that server. Another reason to ensure that snapshots are withdrawn promptly is that only one snapshot is allowed at a time for a given guest. You cannot establish multiple snapshots of a guest.

Without snapshotting, we would either have to stop the guest in order to back it up, or we would have a fuzzy backup of many of the files on the guest, which are both inferior to using snapshotted data.

Once a snapshot is created, it is possible to make it available across a SAN (or other shared storage, like a NAS or iSCSI) to another system.

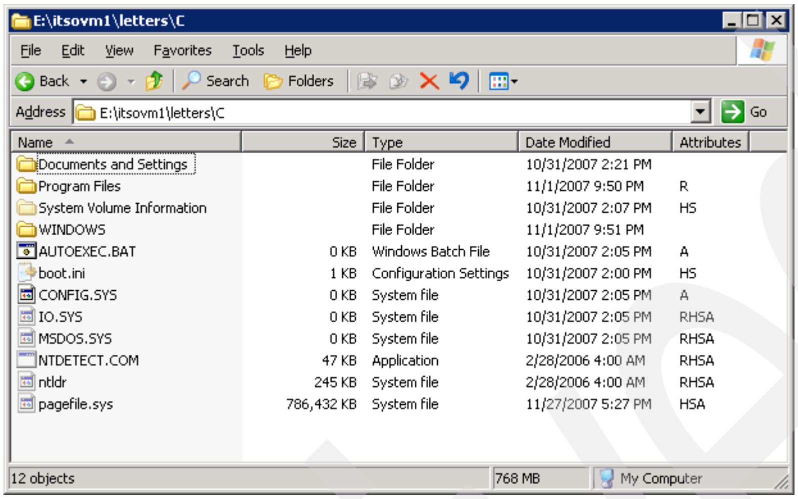
While it is possible to run more than one snapshot at the same time, this is only possible if the snapshots are for different guests. There are limits to the total number of snapshots an ESX server can handle, and there are limits to the number of snapshots a VirtualCenter server can handle without specific tuning. For additional information about these limits, refer to the VMware support documentation at:

http://vmware.com

File-level backup of VMware guests

File-level backup allows the file systems of Windows (only, at the time of writing) guests in a VMware ESX server to be presented across the storage network to another physical (non-virtualized) Windows 2003 system used specifically for backup. This system is referred to as the proxy node. We show how to perform file-level backup in 24.7, "Full backup of VMware hosted systems" on page 351.

Figure 24-4 on page 331 shows the root of a guest's C: drive, which is mounted on the proxy node during a snapshot operation. Here we have performed a test mount using the native VCB **`vcbmounter`** command (as shown in step b on page 339). When doing this, we can specify the mountpoint (E:\ in this case). However, during a Tivoli Storage Manager file-level VCB backup, the drives will be always mounted at location C:\mnt\tsmvmbackup\filelevel\.



Name	Size	Type	Date Modified	Attributes
Documents and Settings		File Folder	10/31/2007 2:21 PM	
Program Files		File Folder	11/1/2007 9:50 PM	R
System Volume Information		File Folder	10/31/2007 2:07 PM	HS
WINDOWS		File Folder	11/1/2007 9:51 PM	
AUTOEXEC.BAT	0 KB	Windows Batch File	10/31/2007 2:05 PM	A
boot.ini	1 KB	Configuration Settings	10/31/2007 2:00 PM	HS
CONFIG.SYS	0 KB	System file	10/31/2007 2:05 PM	A
IO.SYS	0 KB	System file	10/31/2007 2:05 PM	RHSA
MSDOS.SYS	0 KB	System file	10/31/2007 2:05 PM	RHSA
NTDETECT.COM	47 KB	Application	2/28/2006 4:00 AM	RHSA
ntldr	245 KB	System file	2/28/2006 4:00 AM	RHSA
pagefile.sys	786,432 KB	System file	11/27/2007 5:27 PM	HSA

12 objects | 768 MB | My Computer

Figure 24-4 VCB file-level snapshot, mounted at the root of proxy machine's E:\ drive

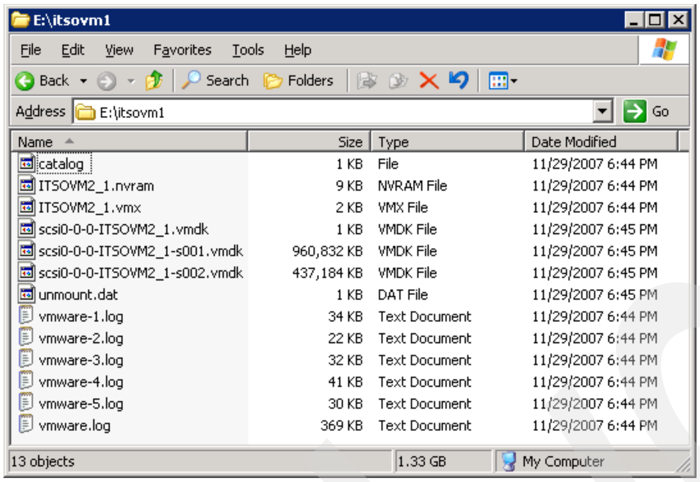
Although from this view of Windows Explorer these folders look like local files, they are actually mounted as a virtual mount point on the proxy. This means that they are not copied and do not occupy any disk space on the proxy.

After backup to Tivoli Storage Manager, the filespaces created are associated with the actual guest's nodename (not the proxy nodename), and the Tivoli Storage Manager database therefore records and expires these files individually. Files and other objects appear as belonging to the Tivoli Storage Manager node registered for that guest (not to the proxy), so from the Tivoli Storage Manager server perspective, the guests each look like they have been backed up from a locally installed client on the guest. A corollary is that individual files from a particular guest can, if desired, be restored by a backup-archive client on that guest. We describe this in 24.6.1, "Restore files directly to the guest" on page 349.

Full backup of VMware guests

Full backup of VMware guests means that the guest's disk files are backed up as a single entity. Similarly, the entire image can then be restored to VMware.

Even though it is an image-type backup, full backup creates a small number of large objects, rather than one enormous object. It also presents the various log files and settings files that accompany the guest. The images are sliced into manageable sized chunks of (by default) approximately 2 GB. The files so created from a small VMware guest are shown in Figure 24-5 on page 332.



Name	Size	Type	Date Modified
catalog	1 KB	File	11/29/2007 6:44 PM
ITSOVM2_1.nvram	9 KB	NVRAM File	11/29/2007 6:44 PM
ITSOVM2_1.vmx	2 KB	VMX File	11/29/2007 6:44 PM
scsi0-0-0-ITSOVM2_1.vmdk	1 KB	VMDK File	11/29/2007 6:45 PM
scsi0-0-0-ITSOVM2_1-s001.vmdk	960,832 KB	VMDK File	11/29/2007 6:45 PM
scsi0-0-0-ITSOVM2_1-s002.vmdk	437,184 KB	VMDK File	11/29/2007 6:45 PM
unmount.dat	1 KB	DAT File	11/29/2007 6:45 PM
vmware-1.log	34 KB	Text Document	11/29/2007 6:44 PM
vmware-2.log	22 KB	Text Document	11/29/2007 6:44 PM
vmware-3.log	32 KB	Text Document	11/29/2007 6:44 PM
vmware-4.log	41 KB	Text Document	11/29/2007 6:44 PM
vmware-5.log	30 KB	Text Document	11/29/2007 6:44 PM
vmware.log	369 KB	Text Document	11/29/2007 6:44 PM

Figure 24-5 Showing the files created during a fullvm backup with VCB

Full backup works well with Tivoli Storage Manager adaptive differencing (subfile backup) technology, which eliminates much of the backup overhead of taking full images at the client side, before they ever make it to the Tivoli Storage Manager server. This makes the backup very efficient both from the client processing required, as well as overall storage utilization on the Tivoli Storage Manager server.

We show how to perform a full backup in 24.7, “Full backup of VMware hosted systems” on page 351. This section also shows the benefits of subfile backup.

24.2 Planning for VCB with Tivoli Storage Manager V5.5

As always, there are a number of important planning considerations for VCB. The principal items to consider are:

- Is there a VirtualCenter (VC) server, or will the Tivoli Storage Manager client connect (via the VCB framework) to the ESX servers individually?

  Typically, for a VMware farm of more than a few instances of ESX server, having a VC server makes the solution easier to manage. It is also a useful tool for problem diagnosis. Our example uses a VC server called KCW09B.

- Is LAN-free backup required and, if so, will it be effective?

  LAN-free backup involves backing up objects straight to tape. When dealing with many thousands of small files (in a file-level backup), it may be more appropriate to back these up to a Tivoli Storage Manager diskpool, which is then migrated to tape.

- The storage network infrastructure should be sufficient to provide the speeds required.

  As we have said, the proxy node must have visibility to the external disks containing the VMware guest images. However, it is not supported to use a multipath driver such as SDD or RDAC to load-balance across multiple HBAs. It may therefore be useful to invest in a single, faster HBA than multiple slower ones. This depends on the speed of the disk being backed up and the backup window available. The storage network design itself will have to be up to the job (for example, non-blocked and where fanout is applied, it should have enough bandwidth to accomplish the job).

- Security controls of the backup proxy machine are important.

  Since VCB file-level backup presents the NTFS file systems of the guests from the ESX server to the proxy node, this effectively bypasses the security controls on each guest operating system. Therefore, the proxy node should be appropriately secured according to enterprise policy and practice from unauthorized access.

Hardware infrastructure guidance

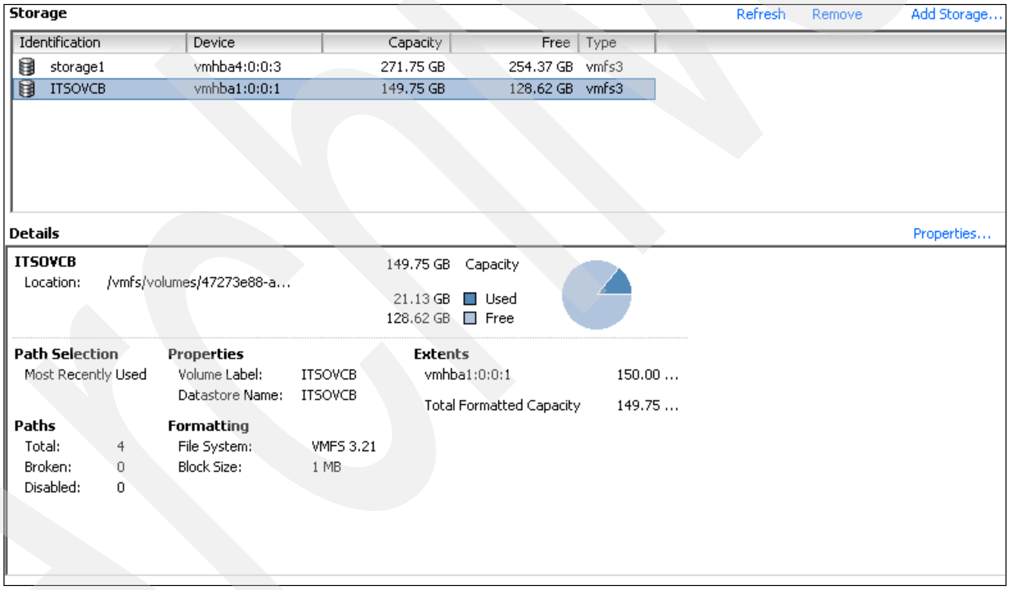
In this section we discuss some general guidelines for planning the hardware infrastructure.

For the guest images on the ESX server

The guest images must be installed on shared storage (for example, SAN, NAS, iSCSI.) Carefully check the VMware Storage/SAN Compatibility Guide for supported storage and HBA configurations, available at:

http://www.vmware.com/pdf/vi3_san_guide.pdf

We have configured a 150 GB virtual disk on a SAN Volume Controller. All the guests to be backed up via VCB are using this datastore. The disk used is shown in Figure 24-6 on page 333.



Identification	Device	Capacity	Free	Type
storage1	vmhba4:0:0:3	271.75 GB	254.37 GB	vmfs3
ITSOVCB	vmhba1:0:0:1	149.75 GB	128.62 GB	vmfs3

ITSOVCB
Location: /vmfs/volumes/47273e88-a...

149.75 GB Capacity
21.13 GB ■ Used
128.62 GB □ Free

Path Selection
Most Recently Used

Properties
Volume Label: ITSOVCB
Datastore Name: ITSOVCB

Extents
vmhba1:0:0:1 150.00 ...
Total Formatted Capacity 149.75 ...

Paths
Total: 4
Broken: 0
Disabled: 0

Formatting
File System: VMFS 3.21
Block Size: 1 MB

Figure 24-6 SVC disk on ESX server

For the VirtualCenter server

The VirtualCenter (VC) server is optional, however most enterprise VMware environments will already be deploying this, since it simplifies and centralizes the administration of a large number of ESX servers. The workload imposed by VCB upon the VC server is likely to be minimal since its only job is to control the running of snapshot jobs. The VC server does not actually move any backup data around. For this reason, a desktop or small Blade is sufficient in most cases. Consult the VMware documentation for formal hardware and platform requirements.

For the proxy node

The proxy node will move all the backup data either out onto the network, or via the SAN straight to tape. The proxy node must be running Windows 2003 SP1 with an HBA that is supported for access to the SAN disk where the guest images are installed. The proxy node must have visibility to the SAN disk. In our case we created a mapping on the SVC between the proxy node and the virtual disk. The proxy node then sees the disk, as shown in Figure 24-7 on page 334.

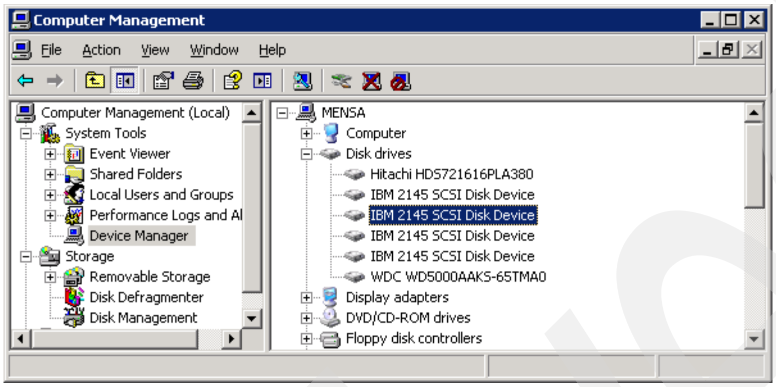


Figure 24-7 Proxy node has visibility to the same SAN disk as the ESX server

We strongly recommend separating SAN disk and tape traffic on the proxy node to dedicated HBAs. It should also be a powerful enough system to cope with the performance requirements required, often hundreds of MB per second. A presentation from VMware is available at:

http://communities.vmware.com/docs/DOC-1793.pdf;jsessionid=DCF8C8B0E0B4BE25B13F3938E9FF0015

This includes excellent recommendations for designing a VCB solution. A typical minimum configuration would be a dual core CPU and 2 GB memory.

Performing full VM backups and restores requires actual disk space on the proxy node. The actual amount required varies according to the number of simultaneous full VM backups to be performed and the size of the images generated. You should plan on having storage space sufficient to keep the largest guest, plus some extra, and to increase this if you will make multiple simultaneous full snapshots. If you will only perform file-level backup, disk space is not required on the proxy node, since the guest file systems are attached as virtual mount points. We strongly recommend pre-production prototyping of VCB solutions in order to more accurately predict resource requirements for your particular environment.

Note that at the time of writing, there is not support for using any multipathing software on the proxy node, such as RDAC or SDD. The proxy node must also *not* be allowed to write a disk label on the SAN disk, as this could corrupt the VM images. We show how to disable the proxy node's built-in Windows automounter in step 1 on page 335.

24.3 Install and configure VCB with Tivoli Storage Manager V5.5

There are some important steps to take before using VMware Consolidated Backup with any third-party backup product, including Tivoli Storage Manager configuration. This section explains the steps required to install VCB with Tivoli Storage Manager V5.5. Read through the steps and then follow them in order, particularly if this is your first time using VCB or the first VCB set up in your enterprise. Where steps are specified as optional, we recommend that you do them anyway, particularly for a first installation, since they provide more diagnostic steps than the minimum, and may help work out what is going wrong if problems are encountered.

As a reminder, our environment, shown in Figure 24-3 on page 329, is:

- VMware ESX server: PEGASUS IP address 9.43.86.149
- VC server on Windows 2003: KCW09B, IP address 9.43.86.135
- VCB proxy node on Windows 2003: MENSA, IP address 9.43.86.90

  If you wish to use LAN-free backup from the proxy node to the Tivoli Storage Manager storage, you should install the Tivoli Storage Manager Storage Agent on the proxy and configure it as a LAN-free client of the Tivoli Storage Manager server.
- VMware guests running Windows XP:
  - Host names are SPANIEL, MCNAB, MALAMUTE, and COLLIE, IP addresses 9.43.86.151 to 9.43.86.154
  - VM names are ITSOVM1, ITSOVM2, ITSOVM3, ITSOVM4, respectively
- Tivoli Storage Manager V5.5 server, LOCHNESE, IP address 9.43.86.84

24.3.1 Prerequisites for VMware and operating system settings

In order to allow VCB to function, we have to configure a number of settings on our proxy server.

1. Prevent the Windows 2003 proxy node, MENSA, from assigning drive letters to new disks automatically whenever it mounts disks from the ESX server on Windows via the SAN. We use the Windows **diskpart** command for this, as shown in Example 24-1.

   Example 24-1 Disable automatic disk drive letter assignment

   ```
   C:\Documents and Settings\Administrator>diskpart
   Microsoft DiskPart version 5.2.3790.3959
   Copyright (C) 1999-2001 Microsoft Corporation.
   On computer: MENSA
   DISKPART> automount disable
   Automatic mounting of new volumes disabled.
   DISKPART> automount scrub
   DiskPart successfully scrubbed the mount point settings in the system.
   Automatic mounting of new volumes disabled.
   DISKPART> exit
   Leaving DiskPart...
   C:\Documents and Settings\Administrator>shutdown /r
   ```

   Important: You must reboot Windows in order for the **diskpart** change to take effect. This must be done before attempting to use or test VCB. The setting persists over reboots. It only needs to be done once.

2. Install VCB Framework on the proxy node.

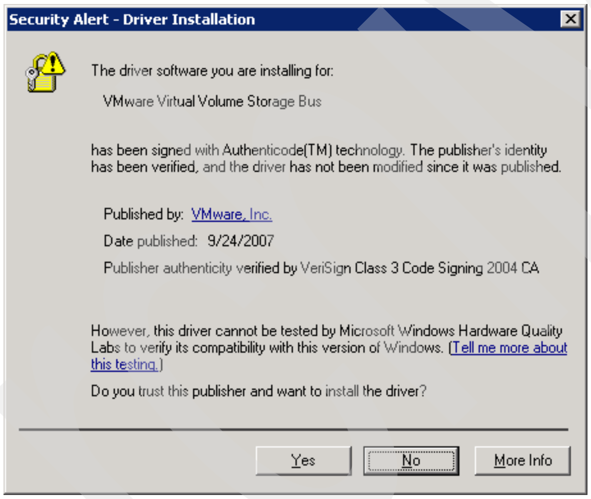
   VCB Framework is a component of the VMware Infrastructure 3 package, which can be downloaded from:

   http://www.vmware.com/download/vi/

A valid license is required. See your VMware administrator for licensing information.

> **Note:** At the time of writing, some VCB Framework versions available from VMware did not automatically create the directory where the guest's snapshotted file system will be mounted. If you have a version with this issue, the backup operation will fail if the directory does not exist, with the error:
>
> ```
> 007-11-28 14:28:59.265 'vcbMounter' 1960 error] Error: <directory-name>: Is
> not a writeable directory.
> ```
>
> A fix is expected to be available. Check for the availability of APAR IC54709. A workaround for this is to manually create the mountpoint and make it read-only before running the backup. This ensures that the mountpoint will persist. You can use commands similar to:
>
> ```
> mkdir     c:\mnt\tsmvmbackup\filelevel
> attrib +r c:\mnt\tsmvmbackup\filelevel
> ```

Installing VCB Framework is straightforward. You are only prompted for the installation directory. Figure 24-8 on page 336 shows a Windows dialog that asks whether you want to install the VMware driver since it has not been through MS-WHQL testing. You must accept and install this for VCB to work.



Security Alert - Driver Installation

The driver software you are installing for:

VMware Virtual Volume Storage Bus

has been signed with Authenticode(TM) technology. The publisher's identity has been verified, and the driver has not been modified since it was published.

Published by: VMware, Inc.

Date published: 9/24/2007

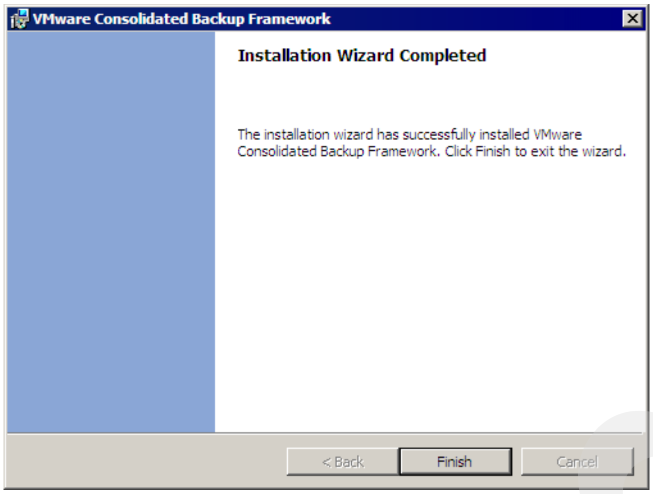
Publisher authenticity verified by VeriSign Class 3 Code Signing 2004 CA

However, this driver cannot be tested by Microsoft Windows Hardware Quality Labs to verify its compatibility with this version of Windows. (Tell me more about this testing.)

Do you trust this publisher and want to install the driver?

Figure 24-8   Driver installation dialog for VMware Consolidated Backup Framework

Figure 24-9 on page 337 displays after the installation successfully completes.



Installation Wizard Completed

The installation wizard has successfully installed VMware Consolidated Backup Framework. Click Finish to exit the wizard.

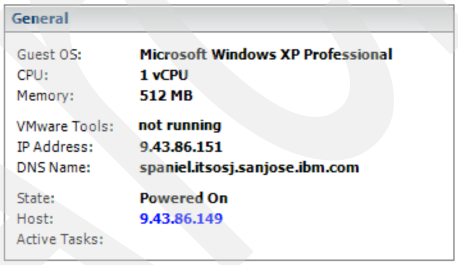
Figure 24-9 VCB Framework installed

Once VCB Framework is installed, there is no further configuration required.; Tivoli Storage Manager will automatically call VCB Framework with any required parameters.

3. Install VMware Tools on each virtual machine guest.

   VMware Tools allows VMware to force a sync of the file systems before the snapshot occurs, thus assuring file system integrity. The file system sync does not by itself ensure that all files backed up in this manner will be consistent for the applications that use them (for example, many applications such as databases will hold transactions in flight, which will not be flushed using this sync). Rather, the sync ensures that the snapshot of the file system itself is not rendered dirty or corrupted by the snapshot processing.

   a. To check whether the VMware Tools are installed, look at the field VMware Tools for each guest in the Virtual Infrastructure Client, as shown in Figure 24-10. If the field displays `not running`, as here, you must install the VMWare tools.



General

Guest OS: Microsoft Windows XP Professional
CPU: 1 vCPU
Memory: 512 MB

VMware Tools: not running
IP Address: 9.43.86.151
DNS Name: spaniel.itsosj.sanjose.ibm.com

State: Powered On
Host: 9.43.86.149
Active Tasks:

Figure 24-10 VMware Tools not installed

b. Right-click each guest and select **Install VMware Tools** from the menu, as shown in Figure 24-11. The install has been initiated from the Virtual Infrastructure Client. The installation is straightforward.

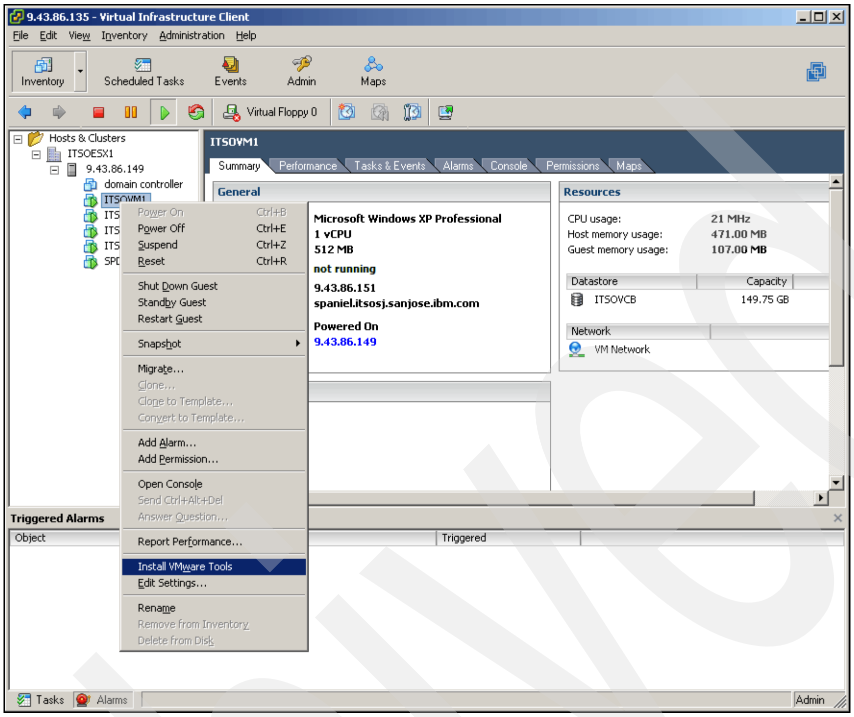
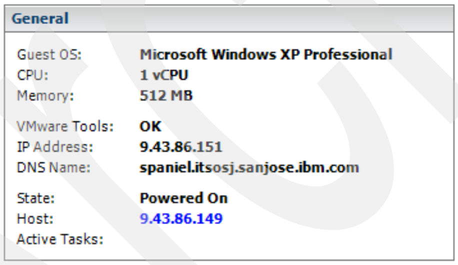


Figure 24-11 Start installation of VMware Tools

c. After the install is complete, the field VMware Tools will change to OK, as shown in Figure 24-12.



General

Guest OS: **Microsoft Windows XP Professional**
CPU: **1 vCPU**
Memory: **512 MB**

VMware Tools: **OK**
IP Address: **9.43.86.151**
DNS Name: **spaniel.itsosj.sanjose.ibm.com**

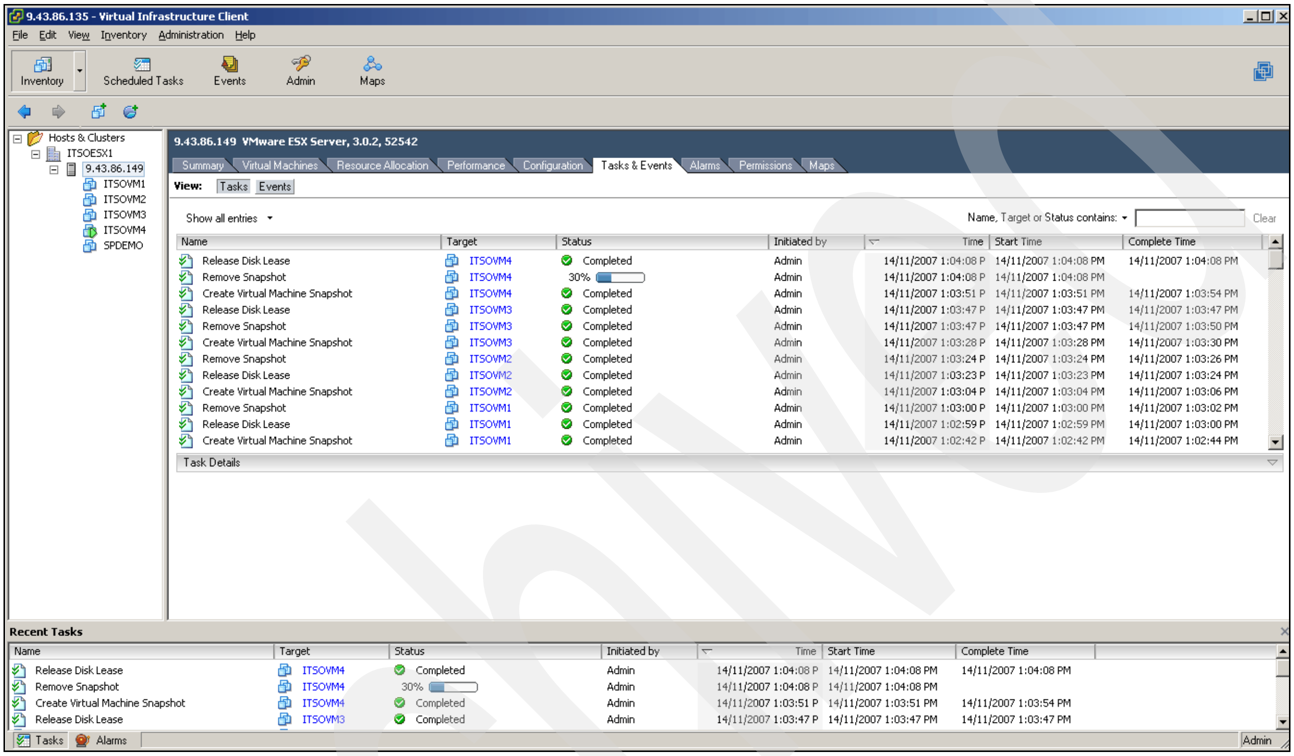
State: **Powered On**
Host: **9.43.86.149**
Active Tasks:

Figure 24-12 VMware Tools installed

4. The following steps are optional, but highly recommended:

   a. Install VMware Infrastructure Client on a system accessible by the Tivoli Storage Manager administrator, for example, on your workstation.

      This gives the ability to view the operations performed by the ESX server as they happen. It is therefore a useful problem diagnosis tool. You can also install VMware Tools onto your guests from here. An image of VIC is shown in Figure 24-13 on page 339.



Name	Target	Status	Initiated by	Time	Start Time	Complete Time
Release Disk Lease	ITSOVM4	Completed	Admin	14/11/2007 1:04:08 P	14/11/2007 1:04:08 PM	14/11/2007 1:04:08 PM
Remove Snapshot	ITSOVM4	30%	Admin	14/11/2007 1:04:08 P	14/11/2007 1:04:08 PM	
Create Virtual Machine Snapshot	ITSOVM4	Completed	Admin	14/11/2007 1:03:51 P	14/11/2007 1:03:51 PM	14/11/2007 1:03:54 PM
Release Disk Lease	ITSOVM3	Completed	Admin	14/11/2007 1:03:47 P	14/11/2007 1:03:47 PM	14/11/2007 1:03:47 PM
Remove Snapshot	ITSOVM3	Completed	Admin	14/11/2007 1:03:47 P	14/11/2007 1:03:47 PM	14/11/2007 1:03:50 PM
Create Virtual Machine Snapshot	ITSOVM3	Completed	Admin	14/11/2007 1:03:28 P	14/11/2007 1:03:28 PM	14/11/2007 1:03:30 PM
Remove Snapshot	ITSOVM2	Completed	Admin	14/11/2007 1:03:24 P	14/11/2007 1:03:24 PM	14/11/2007 1:03:26 PM
Release Disk Lease	ITSOVM2	Completed	Admin	14/11/2007 1:03:23 P	14/11/2007 1:03:23 PM	14/11/2007 1:03:24 PM
Create Virtual Machine Snapshot	ITSOVM2	Completed	Admin	14/11/2007 1:03:04 P	14/11/2007 1:03:04 PM	14/11/2007 1:03:06 PM
Remove Snapshot	ITSOVM1	Completed	Admin	14/11/2007 1:03:00 P	14/11/2007 1:03:00 PM	14/11/2007 1:03:02 PM
Release Disk Lease	ITSOVM1	Completed	Admin	14/11/2007 1:02:59 P	14/11/2007 1:02:59 PM	14/11/2007 1:03:00 PM
Create Virtual Machine Snapshot	ITSOVM1	Completed	Admin	14/11/2007 1:02:42 P	14/11/2007 1:02:42 PM	14/11/2007 1:02:44 PM

Recent Tasks

Name	Target	Status	Initiated by	Time	Start Time	Complete Time
Release Disk Lease	ITSOVM4	Completed	Admin	14/11/2007 1:04:08 P	14/11/2007 1:04:08 PM	14/11/2007 1:04:08 PM
Remove Snapshot	ITSOVM4	30%	Admin	14/11/2007 1:04:08 P	14/11/2007 1:04:08 PM	
Create Virtual Machine Snapshot	ITSOVM4	Completed	Admin	14/11/2007 1:03:51 P	14/11/2007 1:03:51 PM	14/11/2007 1:03:54 PM
Release Disk Lease	ITSOVM3	Completed	Admin	14/11/2007 1:03:47 P	14/11/2007 1:03:47 PM	14/11/2007 1:03:47 PM

Figure 24-13 VIC graphic showing VCB during snapshot operations

   b. Test a mount of a guest file system to the proxy node. This procedure is a useful pre-test of the configuration, before Tivoli Storage Manager is in the picture, and ensures that the proxy node can correctly access the SAN disk hosting the guest images. Use the VMware **`vcbmounter`** command, as shown in Example 24-2. You can display the complete syntax by running the command without parameters, and we also give more **`vcbmounter`** examples elsewhere in this chapter. In this test, we use the following parameters:

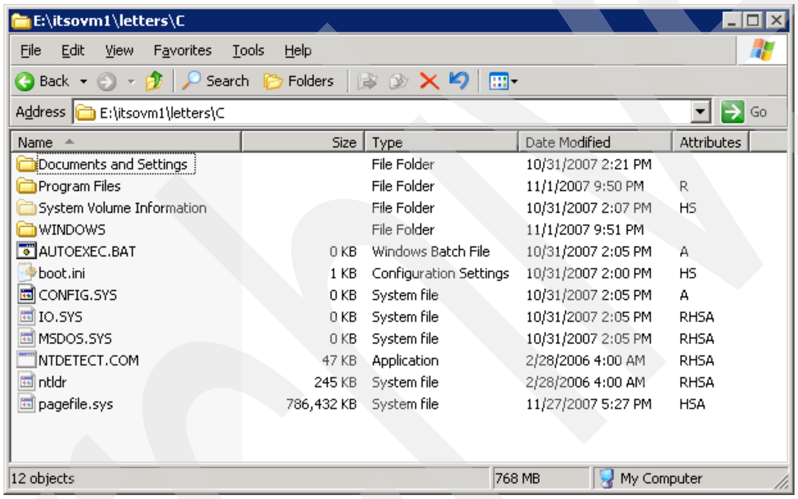
      -h <*ESX/VC host*> 9.43.85.135
      -u <*username of administrator on ESX/VC host*>
      -p <password of administrator>
      -a ipaddr:<*guest to mount*> 9.43.86.151
      -r <*directory on proxy where file system is mounted*> e:\itsovm1
      -t <*type of backup - fullvm or file*> *file*

Example 24-2 Test mount of a guest file system on the proxy

```
C:\Program Files\VMware\VMware Consolidated Backup Framework>vcbmounter -h
9.43.86.135 -u Admin -p xxxxx -a ipaddr:9.43.86.151 -r e:\itsovm1 -t file
[2007-11-29 13:23:41.312 'App' 3964 info] Current working directory: C:\Program
Files\VMware\VMware Consolidated Backup Framework
```

```
[2007-11-29 13:23:41.312 'BaseLibs' 3964 info] HOSTINFO: Seeing Intel CPU,
numCoresPerCPU 2 numThreadsPerCore 1.
[2007-11-29 13:23:41.312 'BaseLibs' 3964 info] HOSTINFO: This machine has 1
physical CPUS, 2 total cores, and 2 logical CPUs.
[2007-11-29 13:23:41.312 'BaseLibs' 3964 info] Using system libcrypto, version
90703F
[2007-11-29 13:23:41.718 'BaseLibs' 3972 warning] [Vmdb_Unset] Unsetting
unknown path: /vmomi/
Opened disk: blklst://snapshot-154[ITSOVCB]
ITSOVM2_1/ITSOVM2_1.vmdk@9.43.86.135?xxxx/xxxx
Proceeding to analyze volumes
Done mounting
Volume 1 mounted at e:\itsovm1\digits\1 (mbSize=3059 fsType=NTFS )
Volume 1 also mounted on e:\itsovm1\letters\C
C:\Program Files\VMware\VMware Consolidated Backup Framework>
```

Figure 24-14 shows the directory created on the proxy node. All the files of the guest SPANIEL are available in this directory tree.



Name	Size	Type	Date Modified	Attributes
Documents and Settings		File Folder	10/31/2007 2:21 PM	
Program Files		File Folder	11/1/2007 9:50 PM	R
System Volume Information		File Folder	10/31/2007 2:07 PM	HS
WINDOWS		File Folder	11/1/2007 9:51 PM	
AUTOEXEC.BAT	0 KB	Windows Batch File	10/31/2007 2:05 PM	A
boot.ini	1 KB	Configuration Settings	10/31/2007 2:00 PM	HS
CONFIG.SYS	0 KB	System file	10/31/2007 2:05 PM	A
IO.SYS	0 KB	System file	10/31/2007 2:05 PM	RHSA
MSDOS.SYS	0 KB	System file	10/31/2007 2:05 PM	RHSA
NTDETECT.COM	47 KB	Application	2/28/2006 4:00 AM	RHSA
ntldr	245 KB	System file	2/28/2006 4:00 AM	RHSA
pagefile.sys	786,432 KB	System file	11/27/2007 5:27 PM	HSA

12 objects 768 MB My Computer

Figure 24-14 vcbmounter file level test: resulting mounted directory

Since the test executed correctly, we dismount the snapshotted file system, as shown in Example 24-3. Remember to unmount your test snapshot once you have successfully completed the test, or unexpected errors could occur. The -U option is used in **vcbmounter** to unmount.

Example 24-3 Use vcbmounter to remove a previously mounted snapshot

```
C:\Program Files\VMware\VMware Consolidated Backup Framework>vcbmounter -h
9.43.86.135 -u Admin -p xxxxx -U e:\itsovm1
[2007-11-29 17:06:27.453 'App' 2548 info] Current working directory: C:\Program
Files\VMware\VMware Consolidated Backup Framework
[2007-11-29 17:06:27.468 'BaseLibs' 2548 info] HOSTINFO: Seeing Intel CPU,
numCoresPerCPU 2 numThreadsPerCore 1.
[2007-11-29 17:06:27.468 'BaseLibs' 2548 info] HOSTINFO: This machine has 1
physical CPUS, 2 total cores, and 2 logical CPUs.
[2007-11-29 17:06:27.468 'BaseLibs' 2548 info] Using system libcrypto, version
90703F
[2007-11-29 17:06:27.859 'BaseLibs' 1968 warning] [Vmdb_Unset] Unsetting unknown
path: /vmomi/
```

```
Unmounted e:\itsovm1\digits\1\ (formatted)
Deleted directory e:\itsovm1\digits\1\
Deleted directory e:\itsovm1\digits\
Deleted directory e:\itsovm1\letters\C\
Deleted directory e:\itsovm1\letters\
Deleted directory e:\itsovm1
C:\Program Files\VMware\VMware Consolidated Backup Framework>
```

24.3.2 Prerequisite configuration for the Tivoli Storage Manager server

When using VCB, the Tivoli Storage Manager administrator must create a Tivoli Storage Manager node for each guest to be backed up. In addition, the proxy node itself requires a nodename, even if it is not being backed up itself. This is because when the proxy node connects to Tivoli Storage Manager it will do so as itself *on behalf* of a given VMware guest.

1. We start by registering all the nodes, including the proxy node, in the usual way, as shown in Example 24-4. In the example, we are not registering administrative users for each node, but you can do this if you want. We have registered the node names to match the VM names (ITSOVM1, ITSOVM2, and so on), not the TCP/IP host names, which are different (SPANIEL, MCNAB, and so on).

> **Note:** In most configurations, we recommend using the TCP/IP host name for the Tivoli Storage Manager nodename. This simplifies the configuration. Our configuration used the VM name rather than the host name for the Tivoli Storage Manager nodename, since this requires a slightly more complex parameter setting in the proxy node's options file (dsm.opt). This is shown in 24.3.3, "Configure the proxy node's options file (dsm.opt)" on page 342, under the VMLIST item.

Example 24-4 Register proxy node and nodes for each guest

```
tsm: LOCHNESE>register node mensa itsoproxy1passwd domain=standard user=none
contact='Craig'
ANR2060I Node MENSA registered in policy domain STANDARD.
tsm: LOCHNESE>register node itsovm1 itsovm1passwd domain=standard user=none
contact='Claire'
ANR2060I Node ITSOVM1 registered in policy domain STANDARD.
tsm: LOCHNESE>register node itsovm2 itsovm2passwd domain=standard user=none
contact='Minnie'
ANR2060I Node ITSOVM2 registered in policy domain STANDARD.
tsm: LOCHNESE>register node itsovm3 itsovm3passwd domain=standard user=none
contact='Shasta'
ANR2060I Node ITSOVM3 registered in policy domain STANDARD.
tsm: LOCHNESE>register node itsovm4 itsovm4passwd domain=standard user=none
contact='Flyer'
ANR2060I Node ITSOVM4 registered in policy domain STANDARD.
tsm: LOCHNESE>query node
Node Name                 Platform Policy Domain  Days Since Days Since Locked?
                                   Name           Last Acce-   Password
                                                          ss        Set
------------------------- -------- -------------- ---------- ---------- -------
ITSOVM1                   (?)      STANDARD               <1         <1   No
ITSOVM2                   (?)      STANDARD               <1         <1   No
```

```
ITSOVM3                   (?)      STANDARD               <1         <1   No
ITSOVM4                   (?)      STANDARD               <1         <1   No
MENSA                     (?)      STANDARD               <1         <1   No
```

2. Grant authority to the proxy node to access and add to the node data for each of the VMware guests. Use the GRANT PROXYNODE command, as shown in Example 24-5.

Example 24-5 Grant authority to the proxy for each guest node

```
tsm: LOCHNESE>grant proxy agent=mensa target=itsovm1
ANR0140I GRANT PROXYNODE: success.  Node MENSA is granted proxy authority to node
ITSOVM1.
tsm: LOCHNESE>grant proxy agent=mensa target=itsovm2
ANR0140I GRANT PROXYNODE: success.  Node MENSA is granted proxy authority to node
ITSOVM2.
tsm: LOCHNESE>grant proxy agent=mensa target=itsovm3
ANR0140I GRANT PROXYNODE: success.  Node MENSA is granted proxy authority to node
ITSOVM3.
tsm: LOCHNESE>grant proxy agent=mensa target=itsovm4
ANR0140I GRANT PROXYNODE: success.  Node MENSA is granted proxy authority to node
ITSOVM4.
tsm: LOCHNESE>query proxy
Target Node         Agent Node
---------------     ---------------------------------------------
ITSOVM1             MENSA
ITSOVM2             MENSA
ITSOVM3             MENSA
ITSOVM4             MENSA
```

24.3.3 Configure the proxy node's options file (dsm.opt)

We need to modify the proxy node's client options file (dsm.opt) to enable it for VCB. The new VCB-specific parameters are as follows:

- VMCHOST

  IP address or DNS host name of the VMware VirtualCenter server, or ESX server. Our VirtualCenter server is KCW09B, at 9.43.86.135.

- VMCUSER

  VMware Administrative user ID for the VirtualCenter, which is the same user ID that one would use to log onto VirtualCenter using the Virtual Infrastructure Client. In our example, we have a user ID of Admin.

- VMCPW

  This is the password for the VMware VirtualCenter Administrative user ID specified in VMCUser. We indicate our password with ‘xxxxx’. However, obviously you put in the real string here.

- VMLIST

  This is a list of nodes to be processed by the VCB proxy node. The nodes are separated by commas.

  The order of this list determines the order in which VCB will process the nodes during a **`backup VM`** command if called without any specific operators.

  Where a host name for a node is different from the virtual machine host name, use the format *hostname*[*nodename*], where *hostname* is the virtual machine's host name and *nodename* is the Tivoli Storage Manager nodename. All of our examples below are specified in this way (for example, hostname SPANIEL refers to Tivoli Storage Manager nodename ITSOVM1 in our example).

Where the host name and nodename are the same (which is the more common configuration), only the host name is required, so in our example that would look like "SPANIEL,MCNAB,MALAMUTE,COLLIE".

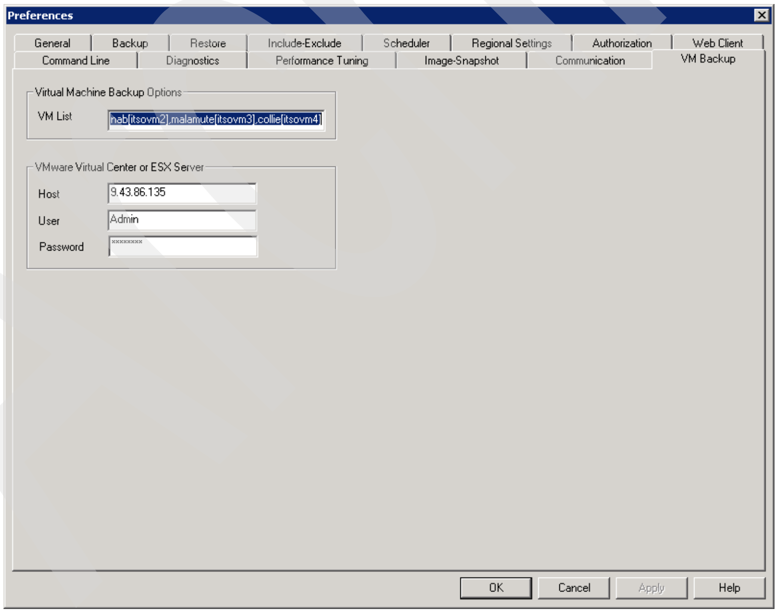
You can also override these options by specifying them in a backup command, for example, **`dsmc backup vm -vmlist=spaniel[itsovm1]`**. This command would back up only the node specified (without the vmlist parameter, the value defaults to the vmlist specified in dsm.opt)—all four guests in our case.

Our lab proxy node's dsm.opt file is shown in Example 24-6 on page 343. We have four guests that will be backed up using VCB. The PASSWORDACCESS and TCPSERVERADDRESS fields are specified as usual.

Example 24-6 The dsm.opt file on our example proxy node MENSA

```
NODENAME            MENSA
PASSWORDACCESS      GENERATE
TCPSERVERADDRESS    9.43.86.84
VMCHOST             9.43.86.135
VMCUSER             Admin
VMCPW               xxxxx
VMLIST        spaniel[itsovm1],mcnab[itsovm2],malamute[itsovm3],collie[itsovm4]
```

You can also use the VM Backup tab in the client GUI Preferences editor, as shown in Figure 24-15 on page 343. Whichever method you use, you must restart the Tivoli Storage Manager client to pick up the changes in the options file.



Virtual Machine Backup Options

VM List: nab[itsovm2],malamute[itsovm3],collie[itsovm4]

VMware Virtual Center or ESX Server

Host: 9.43.86.135

User: Admin

Password: *********

Figure 24-15 Client GUI Preferences editor for VCB options

24.4 File-level backup of VMware-hosted Windows systems

We have completed the configuration and can now start testing the VCB integration with Tivoli Storage Manager. As we know, the actual VCB operations will be performed by the VCB proxy node.

1. We run the **dsmc backup vm** command from the VCB proxy, MENSA, giving output similar to Example 24-7. This will create a full backup of all of the nodes listed in the VMLIST parameter. We specified the -quiet client option to reduce the amount of output, and have also removed three of the four nodes' output for brevity. The remaining nodes produce similar output.

Example 24-7 File-level backup of VMware guests with VCB

```
C:\Program Files\Tivoli\TSM\baclient>dsmc backup vm -quiet
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 5, Level 0.0
  Client date/time: 11/14/2007 11:17:28
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.
Node Name: MENSA
Session established with server LOCHNESE: Windows
  Server Version 5, Release 5, Level 0.0
  Server date/time: 11/14/2007 11:26:22  Last access: 11/14/2007 11:26:12
Backup VM command started.  Total number of virtual machines to process: 4
Backup of Virtual Machine 'spaniel'
Mount virtual machine disk on backup proxy for VM 'spaniel'
Executing Operating System command or script:
   vcbMounter -h 9.43.86.135 -u Admin -p **** -a ipaddr:spaniel -r
C:\mnt\tsmvmbackup\filelevel\spaniel -t file
[2007-11-14 11:17:28.250 'App' 3460 info] Current working directory: C:\Program
Files\Tivoli\TSM\baclient
[2007-11-14 11:17:28.250 'BaseLibs' 3460 info] HOSTINFO: Seeing Intel CPU,
numCoresPerCPU 2 numThreadsPerCore 1.
[2007-11-14 11:17:28.250 'BaseLibs' 3460 info] HOSTINFO: This machine has 1
physical CPUS, 2 total cores, and 2 logical CPUs.
[2007-11-14 11:17:28.250 'BaseLibs' 3460 info] Using system libcrypto, version
90703F
[2007-11-14 11:17:28.656 'BaseLibs' 3348 warning] [Vmdb_Unset] Unsetting unknown
path: /vmomi/
Opened disk: blklst://snapshot-85[ITSOVCB]
ITSOVM2_1/ITSOVM2_1.vmdk@9.43.86.135?xxxx/xxxx
Proceeding to analyze volumes
Done mounting
Volume 1 mounted at C:\mnt\tsmvmbackup\filelevel\spaniel\digits\1 (mbSize=3059
fsType=NTFS )
Volume 1 also mounted on C:\mnt\tsmvmbackup\filelevel\spaniel\letters\C
Finished command.  Return code is: 0
Incremental backup of Virtual Machine 'spaniel'
Querying all_local drives for VM 'spaniel'
Searching for VM 'spaniel' volumes for backup at location:
   C:\mnt\tsmvmbackup\filelevel\spaniel\letters
Accessing as node: itsovm1
Incremental backup of volume '\\itsovm1\c$'
Successful incremental backup of '\\itsovm1\c$'
Total number of objects inspected:    8,254
Total number of objects backed up:    8,187
Total number of objects updated:          0
Total number of objects rebound:          0
Total number of objects deleted:          0
Total number of objects expired:          0
Total number of objects failed:           0
Total number of subfile objects:          0
Total number of bytes transferred:    1.53 GB
Data transfer time:                  122.69 sec
Network data transfer rate:        13,144.79 KB/sec
Aggregate data transfer rate:      6,714.98 KB/sec
Objects compressed by:                    0%
Subfile objects reduced by:               0%
Elapsed processing time:           00:04:00
Successful incremental backup of Virtual Machine 'spaniel'
Unmount virtual machine disk on backup proxy for VM 'spaniel'
Executing Operating System command or script:
   vcbMounter -h 9.43.86.135 -u Admin -p **** -U
C:\mnt\tsmvmbackup\filelevel\spaniel
[2007-11-14 11:21:35.328 'App' 3784 info] Current working directory: C:\Program
Files\Tivoli\TSM\baclient
[2007-11-14 11:21:35.328 'BaseLibs' 3784 info] HOSTINFO: Seeing Intel CPU,
numCoresPerCPU 2 numThreadsPerCore 1.
[2007-11-14 11:21:35.328 'BaseLibs' 3784 info] HOSTINFO: This machine has 1
physical CPUS, 2 total cores, and 2 logical CPUs.
[2007-11-14 11:21:35.328 'BaseLibs' 3784 info] Using system libcrypto, version
90703F
[2007-11-14 11:21:35.718 'BaseLibs' 3228 warning] [Vmdb_Unset] Unsetting unknown
path: /vmomi/
Unmounted C:\mnt\tsmvmbackup\filelevel\spaniel\digits\1\ (formatted)
Deleted directory C:\mnt\tsmvmbackup\filelevel\spaniel\digits\1\
Deleted directory C:\mnt\tsmvmbackup\filelevel\spaniel\digits\
Deleted directory C:\mnt\tsmvmbackup\filelevel\spaniel\letters\C\
Deleted directory C:\mnt\tsmvmbackup\filelevel\spaniel\letters\
Deleted directory C:\mnt\tsmvmbackup\filelevel\spaniel
Finished command.  Return code is: 0
.
.
.
... Deleted output for three other nodes which produce similar listing ...
.
Backup VM command complete
Total number of virtual machines backed up successfully: 4
  virtual machine spaniel backed up to nodename itsovm1
  virtual machine mcnab backed up to nodename itsovm2
  virtual machine malamute backed up to nodename itsovm3
  virtual machine collie backed up to nodename itsovm4
Total number of virtual machines failed: 0
Total number of virtual machines processed: 4
```

2. We can see how the backed up data is stored in the Tivoli Storage Manager server, using a V5.5 administrative command, QUERY VM, as shown in Example 24-8. Note that this is a backup-archive client command, so we run it from MENSA. The four full backups are shown.

Example 24-8 Query VM, from dsmc MENSA, our proxy node

```
tsm> query vm
Filespace Query for Virtual Machine 'spaniel'
Accessing as node: itsovm1
  #     Last Incr Date      Type    File Space Name
---     --------------      ----    ---------------
  1   11/14/2007 13:10:55   NTFS    \\itsovm1\c$
Filespace Query for Virtual Machine 'mcnab'
Accessing as node: itsovm2
  #     Last Incr Date      Type    File Space Name
---     --------------      ----    ---------------
  1   11/14/2007 13:11:19   NTFS    \\itsovm2\c$
Filespace Query for Virtual Machine 'malamute'
Accessing as node: itsovm3
  #     Last Incr Date      Type    File Space Name
---     --------------      ----    ---------------
  1   11/14/2007 13:11:43   NTFS    \\itsovm3\c$
Filespace Query for Virtual Machine 'collie'
Accessing as node: itsovm4
  #     Last Incr Date      Type    File Space Name
---     --------------      ----    ---------------
  1   11/14/2007 13:12:04   NTFS    \\itsovm4\c$
tsm>
```

3. Similarly, we can display the filespaces on the server using QUERY FILESPACE from an administrative command-line session, as shown in Example 24-9.

Example 24-9 Filespaces for VM file-level backups as queried from the server

```
tsm: LOCHNESE>q fi

Node Name   Filespace     FSID   Platform   Filespace Capacity     Pct
            Name                            Type      (MB)         Util
---------   -----------   ----   --------   ---------  ---------  -----------
ITSOVM1     \\itsovm1\c$  1      ??         NTFS       3,059.2    57.8
ITSOVM2     \\itsovm2\c$  1      ??         NTFS       3,059.2    54.2
ITSOVM3     \\itsovm3\c$  1      ??         NTFS       3,059.2    51.4
ITSOVM4     \\itsovm4\c$  1      ??         NTFS       3,059.2    61.5
```

There are some significant differences between VCB backups of file systems when compared with regular Tivoli Storage Manager file-level backup:

- File-level VCB backup can back up some additional objects as files successfully (unlike regular file-level Tivoli Storage Manager backup, where they would be constantly changing). It handles backup of the Windows system objects (registry, and so on) as *files*, and can back these up consistently. These files, which are normally excluded from a typical incremental backup, are not excluded when being processed by **`backup vm`**. This is a fundamental difference between file-level VMware backup and a normal incremental backup.

- It is important that the Tivoli Storage Manager include/exclude settings between the proxy node and the guest do not conflict or unpredictable results can occur, should you decide to back up incrementally from both the guest and using VCB. This may also cause other problems (for example, if the filespace names do not match up).
- Pre-snapshot and post-snapshot commands can be used on the guest, which are invoked by the VCB Framework. These commands can be used to quiesce applications before the VCB snapshot takes place, and resume them after the snapshot is in effect, in order to allow consistent backup of applications that hold transactions in memory.

  These files are hosted on the guest, and are called C:\WINDOWS\PRE-FREEZE-SCRIPT.BAT and C:\WINDOWS\POST-THAW-SCRIPT.BAT, respectively. If these files exist, the commands contained will be executed automatically before and after the snapshot.

24.5 Scheduling VCB operations with the client scheduler

Our example has shown a basic manual VCB test. In a production environment, you will likely want to schedule your backups. The recommended way to do this is using a client macro schedule as follows:

1. Set up a schedule on the Tivoli Storage Manager server. The target will be a macro file to be run by our proxy node, as shown in Example 24-10.

   Example 24-10 Setting up the client schedule

   ```
   tsm: LOCHNESE>define schedule standard vcb action=macro object="vcb.macro"
   starttime=01:00:00
   ANR2500I Schedule VCB defined in policy domain STANDARD.
   tsm: LOCHNESE>
   ```

2. Associate the proxy node with the schedule as shown in Example 24-11.

   Example 24-11 Associate MENSA with the schedule

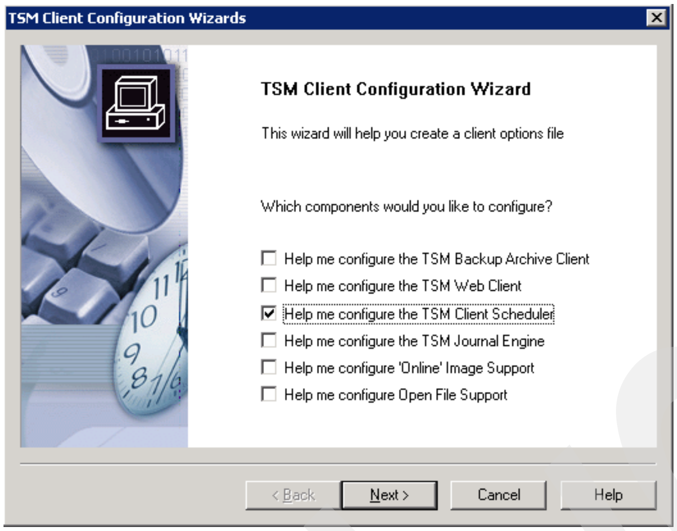
   ```
   tsm: LOCHNESE>def assoc standard vcb mensa
   ANR2510I Node MENSA associated with schedule VCB in policy domain STANDARD.
   tsm: LOCHNESE>
   ```

3. Set up the macro file of Tivoli Storage Manager commands on our proxy node as shown in Example 24-12. This is a very simple example to back up all the guests. You can specify a subset of guests here and run another schedule to back up another set of guests at a different time, for example.

   Example 24-12 Contents of MENSA's C:\Program Files\Tivoli\TSM\baclient\vcb.macro file

   ```
   backup vm
   ```

4. Set up the scheduler service on the proxy node as shown in Figure 24-16. If there is already a scheduler service on MENSA for backing it up as a client node, you might use the existing schedule or define a separate schedule for VCB operations.



TSM Client Configuration Wizard

This wizard will help you create a client options file

Which components would you like to configure?

☐ Help me configure the TSM Backup Archive Client
☐ Help me configure the TSM Web Client
☑ Help me configure the TSM Client Scheduler
☐ Help me configure the TSM Journal Engine
☐ Help me configure 'Online' Image Support
☐ Help me configure Open File Support

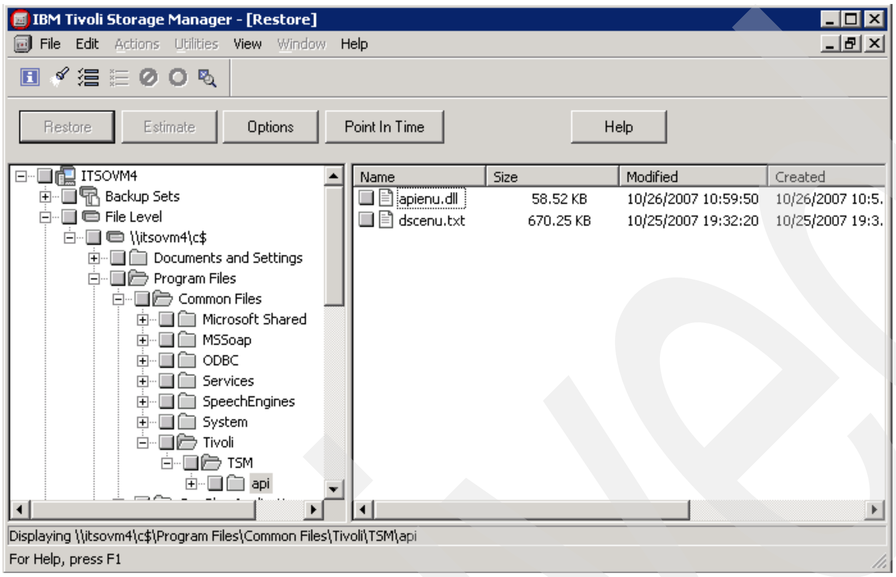
Figure 24-16 Set up the scheduler service for VCB on Mensa

24.6 Restore file data in a VCB environment

When restoring data backed up to Tivoli Storage Manager using the file-level method, there are four main possibilities, depending on both the destination for the restored files and which client node actually performs the restore.

24.6.1 Restore files directly to the guest

This requires the Tivoli Storage Manager client to be installed on the guest in order to initiate the restore. You can then browse and restore files as usual, as shown in Figure 24-17 on page 349.



Name	Size	Modified	Created
apienu.dll	58.52 KB	10/26/2007 10:59:50	10/26/2007 10:5.
dscenu.txt	670.25 KB	10/25/2007 19:32:20	10/25/2007 19:3.

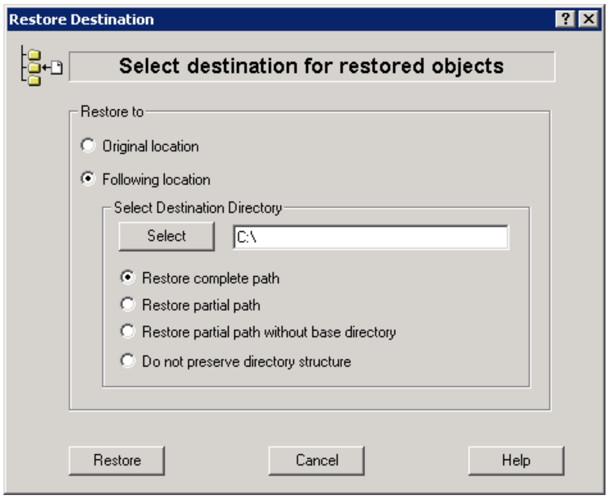
Displaying \\itsovm4\c$\Program Files\Common Files\Tivoli\TSM\api

For Help, press F1

Figure 24-17 Restore files directly to VM guest

If the client has not been previously installed (since VCB does not require the guest to have any Tivoli Storage Manager code for backup operations), then the client/server password access will probably have to be re-established between the guest node and the Tivoli Storage Manager server, since this node would never have connected to the server before. Therefore, when the client imitates for the first time, you will be prompted for the password, which will then be stored locally if PASSWORDACCESS GENERATE is specified.

There is an interesting issue with this if your guest's nodename is not the same as its host name, as is true in our configuration. When we perform a backup using VCB, the Tivoli Storage Manager client must put the file data into a filespace on Tivoli Storage Manager in a UNC form, like \\hostname\c$\. When using VCB with an alternate name, Tivoli Storage Manager in fact backs up the data into a filespace called \\nodename\c$\. When you try to restore to the default original path, it will fail with the error `ANS1410 Unable to access the network path`. Instead, when prompted to select a destination for restore objects, select **Following location** and the destination directory, as shown in Figure 24-18 on page 350. In our case, as shown in Figure 24-17, the filespace is called \\itsovm4\c$, rather than \\collie\c$. Therefore a restore without the alternate destination parameter would fail.



Restore Destination

Select destination for restored objects

Restore to

○ Original location

● Following location

Select Destination Directory

C:\

● Restore complete path

○ Restore partial path

○ Restore partial path without base directory

○ Do not preserve directory structure

Figure 24-18 Restore data to an alternate location so that data is restored to the original location

24.6.2 Restore back to the proxy node's local disk

If you do not want to install the Tivoli Storage Manager client on a guest, you can restore files to the proxy node's local disk using the existing Tivoli Storage Manager client. This is expected to be a commonly used method of recovery for small amounts of data or numbers of files. Once the files are on the proxy node, they can be accessed there or copied to the guest.

To restore to the proxy node, use the Tivoli Storage Manager -ASNODENAME parameter. Remember that the proxy node already has authority to do this from the GRANT PROXYNODE command shown in Example 24-5 on page 342, and also does not need any additional password authentication. Example 24-13 shows how to start the Tivoli Storage Manager GUI from the command line with the -ASNODENAME parameter. Once you start the GUI, the restore display will look similar to Figure 24-17 on page 349. That is, it specified the file space of \\itsovm4\c$. However, restores go to MENSA's local disk. In this case, you would almost certainly want to restore to an alternate location.

Example 24-13 Restore file from ITSOVM4 to the proxy node's local disk

```
C:\Documents and Settings\Administrator>cd "\Program Files\Tivoli\TSM\baclient"
C:\Program Files\Tivoli\TSM\baclient>dsm -asnodename=itsovm4
```

Note: This is not the same as simply opening the GUI and selecting **Utilities ∅ Access another node** (which is the GUI's way of using the -VIRTUALNODENAME parameter).

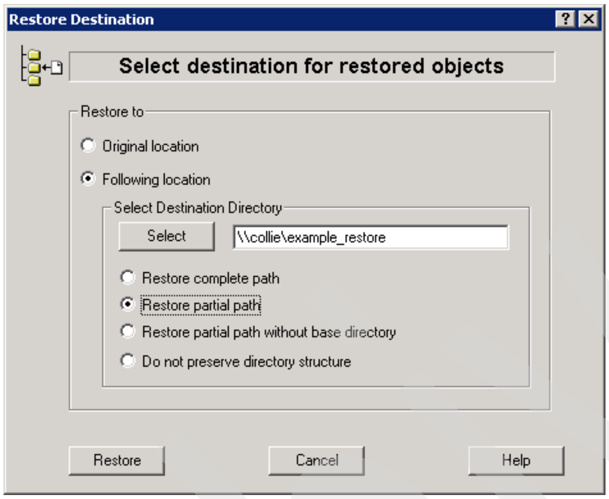
24.6.3 Restore to an alternative server than the proxy or the guest

You can also restore to a computer other than the original guest or the proxy node. To do this, use the -VIRTUALNODENAME parameter in the CLI, or via the GUI select **Utilities ∅ Access another node**. In order to do this, you need to have granted access on the guest's backup-archive client to the server where the files are to be restored, using the SET ACCESS command, and you also need to know the node's password.

24.6.4 Restore to the guest via the proxy node and a CIFS share

The proxy node can restore files directly onto the guest by mounting the guest's file system (with appropriate permissions) as a CIFS share. A benefit of this is that there is no need to install Tivoli Storage Manager on the guest itself, thus saving disk space and administration costs.

In our example, we run the client on MENSA, specifying ASNODENAME=ITSOVM4, but specify to restore to a share accessed from the guest node, as shown in Figure 24-19 on page 351.



Restore Destination

Select destination for restored objects

Restore to

○ Original location

● Following location

Select Destination Directory

Select: \\collie\example_restore

○ Restore complete path

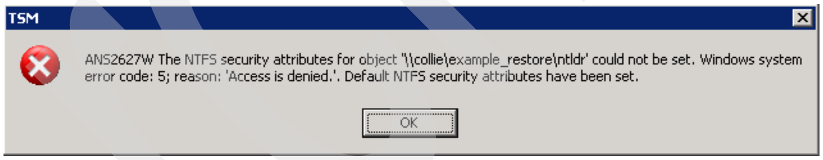
● Restore partial path

○ Restore partial path without base directory

○ Do not preserve directory structure

Figure 24-19 Restore to a CIFS share from a VMware guest

You may lose some of the NTFS security ACLs using this method, depending on the configuration of your file sharing system. We demonstrate this in our test lab environment in Figure 24-20.



TSM

ANS2627W The NTFS security attributes for object '\\collie\example_restore\ntldr' could not be set. Windows system error code: 5; reason: 'Access is denied.'. Default NTFS security attributes have been set.

Figure 24-20 Losing NTFS security information when restoring back via a CIFS share

24.7 Full backup of VMware hosted systems

This section describes how to use Tivoli Storage Manager to back up a full VM (that is, not the individual files inside the guest as we showed in 24.4, "File-level backup of VMware-hosted Windows systems" on page 344, but something more similar to an image backup of the entire guest system). We use the term *fullvm* for this style of backup from now on. Fullvm backup is particularly applicable to DR-type environments, since it is quite simple and fast to recover full VM's using this technique.

A significant difference between VCB fullvm backup and file-level backup is that the fullvm backup requires and uses a large amount of temporary disk space to be available on the proxy node. By comparison, a file-level VCB backup uses no space locally on the proxy node at all since it simply mounts the same volumes used for the running guests on the proxy node and caches all changes on the ESX server. With fullvm, the data is physically *copied* to the proxy node, not just mounted on the proxy node.

The fullvm temporary space needs to be at least as large as the disk image being backed up (in other words, it must be large enough to store all the disks from the largest guest within its temporary space). This space will be occupied by the fullvm disk slices while the backup is in progress, and will be deleted after each backup. We recommend that, for the stability of the proxy node, use temporary space on a drive other than the proxy's system drive. In fact, we recommend using fast, reliable disk for the process since it will be very I/O intensive.

The fullvm backup process copies the disk image from the ESX server to the proxy node's temporary space via the SAN and produces manageable-sized files (2 GB per image slice by default, though this is tunable). These files, which include the VMware VMDK files, can then be backed up or archived by the proxy node to the Tivoli Storage Manager server using normal selective backup, as if they were the proxy node's own files. Incidentally, we use selective backup as opposed to incremental backup with fullvm images. This is so that when we use subfile backup, all the subfile chunks will be retained for the same amount of time.

Since these are just regular files from the Tivoli Storage Manager's perspective, you can back them up to them to alternative nodenames using the -ASNODENAME in the Tivoli Storage Manager client if you wish (for example, so that you may selectively do EXPORT NODE once the data is on the server). Documentation of this is beyond the scope of this book, but the procedure is fairly straightforward for experienced Tivoli Storage Manager administrators.

In theory, any supported guest operating system running under ESX could be backed up using this method, not just the Windows guests where file-level backup is available. It should be pointed out that VMware Tools, which controls the sync of the file system, is only available on Windows. Therefore, other methods would be required to sync in non-Windows environments.

Procedure to create and mount backup images

You can mount VMware full backup images independently of Tivoli Storage Manager using the VMware **vcbmounter** command. The summary procedure is:

1. Take a full image backup of the VMware guest 9.43.86.151 to a specified folder on our proxy node's E drive.
2. Back up the files with Tivoli Storage Manager, with subfile backup enabled.
3. Unmount the fullvm files and make changes to the guest's file system.
4. Rerun the fullvm backup. We take two backups in order to show the benefit of using subfile backup with fullvm images.

It is beyond the scope of this book to show the many parameters for the **vcbmounter** command. The operands used here are:

```
C:\Program Files\VMware\VMware Consolidated Backup Framework>vcbmounter -h
9.43.86.135 -u Admin -p itsoVirtualCenterPassword -a ipaddr:9.43.86.151 -r
e:\itsovm1 -t fullvm
```

- -h 9.43.86.135

  VC server IP address.

- -u Admin

  VC server User ID.

- -p xxxxx

  VC server password for the UserID specified

- -a ipaddr:9.43.86.151.

  Identifier that tells VCB what the IP address of the guest to be backed up is.

- -r e:\itsovm1

  Path where the VMDK and other files will be created. In our environment, we have over 400 GB of free space on this drive.

- -t fullvm

  Specify to use a fullvm backup (as opposed to file-level)

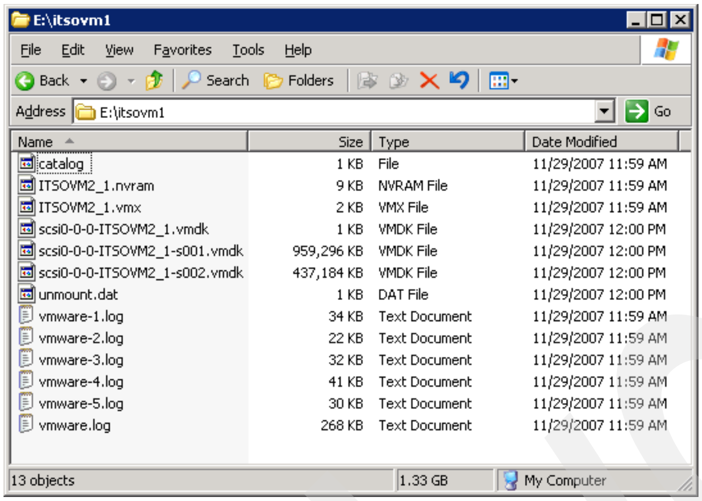
1. We create and mount the snapshot (Example 24-14).

Example 24-14 Use vcbmounter to produce a fullvm snapshot

```
C:\Program Files\VMware\VMware Consolidated Backup Framework>vcbmounter -h
9.43.86.135 -u Admin -p itsoVirtualCenterPassword -a ipaddr:9.43.86.151 -r
e:\itsovm1 -t fullvm
[2007-11-29 11:59:30.562 'App' 3336 info] Current working directory: C:\Program
Files\VMware\VMware Consolidated Backup Framework
[2007-11-29 11:59:30.562 'BaseLibs' 3336 info] HOSTINFO: Seeing Intel CPU,
numCoresPerCPU 2 numThreadsPerCore 1.
[2007-11-29 11:59:30.562 'BaseLibs' 3336 info] HOSTINFO: This machine has 1
physical CPUS, 2 total cores, and 2 logical CPUs.
[2007-11-29 11:59:30.593 'BaseLibs' 3336 info] Using system libcrypto, version
90703F
[2007-11-29 11:59:31.031 'BaseLibs' 3344 warning] [Vmdb_Unset] Unsetting unknown
path: /vmomi/
Copying "[ITSOVCB] ITSOVM2_1/ITSOVM2_1.vmx":
        0%=====================50%=====================100%
        **************************************************
Copying "[ITSOVCB] ITSOVM2_1/ITSOVM2_1.nvram":
        0%=====================50%=====================100%
        **************************************************
Copying "[ITSOVCB] ITSOVM2_1//vmware-1.log":
        0%=====================50%=====================100%
        **************************************************
Copying "[ITSOVCB] ITSOVM2_1//vmware-2.log":
        0%=====================50%=====================100%
        **************************************************
Copying "[ITSOVCB] ITSOVM2_1//vmware-3.log":
        0%=====================50%=====================100%
        **************************************************
Copying "[ITSOVCB] ITSOVM2_1//vmware-4.log":
        0%=====================50%=====================100%
        **************************************************
Copying "[ITSOVCB] ITSOVM2_1//vmware-5.log":
        0%=====================50%=====================100%
        **************************************************
Copying "[ITSOVCB] ITSOVM2_1//vmware.log":
        0%=====================50%=====================100%
        *************************************************
[2007-11-29 11:59:41.687 'BaseLibs' 3348 warning] [Vmdb_Unset] Unsetting unknown
path: /vmomi/
Converting "e:\itsovm1\scsi0-0-0-ITSOVM2_1.vmdk" (compact file):
        0%=====================50%=====================100%
        **************************************************
```

```
C:\Program Files\VMware\VMware Consolidated Backup Framework>
```

2. The snapshot files of the fullvm are created on the proxy, MENSA. They are visible in Windows Explorer, as shown in Figure 24-21 on page 354.



Name	Size	Type	Date Modified
catalog	1 KB	File	11/29/2007 11:59 AM
ITSOVM2_1.nvram	9 KB	NVRAM File	11/29/2007 11:59 AM
ITSOVM2_1.vmx	2 KB	VMX File	11/29/2007 11:59 AM
scsi0-0-0-ITSOVM2_1.vmdk	1 KB	VMDK File	11/29/2007 12:00 PM
scsi0-0-0-ITSOVM2_1-s001.vmdk	959,296 KB	VMDK File	11/29/2007 12:00 PM
scsi0-0-0-ITSOVM2_1-s002.vmdk	437,184 KB	VMDK File	11/29/2007 12:00 PM
unmount.dat	1 KB	DAT File	11/29/2007 12:00 PM
vmware-1.log	34 KB	Text Document	11/29/2007 11:59 AM
vmware-2.log	22 KB	Text Document	11/29/2007 11:59 AM
vmware-3.log	32 KB	Text Document	11/29/2007 11:59 AM
vmware-4.log	41 KB	Text Document	11/29/2007 11:59 AM
vmware-5.log	30 KB	Text Document	11/29/2007 11:59 AM
vmware.log	268 KB	Text Document	11/29/2007 11:59 AM

Figure 24-21 An example of the files created during a fullvm backup

3. Before performing the Tivoli Storage Manager backup, we enable subfile backup. Subfile backup is optional. However, the fullvm operation is an ideal application for this function.

   Modify the client options file dsm.opt to include the lines shown in Example 24-15. Specify a different location for the subfile cache than is used for any other subfile activities on the proxy node, and make sure to exclude the directory from any local backups of the proxy node. You could consider configuring a separate backup-archive node on the proxy specifically for fullvm backups.

   Example 24-15 Enable subfile backup

   ```
   SUBFILEBACKUP      YES
   SUBFILECACHEPATH   c:\tsmsubfile
   SUBFILECACHESIZE   100
   ```

4. Back up the snapshot files with the Tivoli Storage Manager client on MENSA, as shown in Example 24-16.

Example 24-16 Tivoli Storage Manager client backup of guest's snapshot files

```
C:\Program Files\Tivoli\TSM\baclient>dsmc sel -subdir=y e:\itsovm1\*
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 5, Level 0.0
  Client date/time: 12/11/2007 15:55:47
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.
Node Name: MENSA
Session established with server LOCHNESE: Windows
  Server Version 5, Release 5, Level 0.0
  Server date/time: 12/11/2007 15:56:13  Last access: 12/11/2007 15:51:05
Total number of objects inspected:      14
Total number of objects backed up:      14
Total number of objects updated:         0
Total number of objects rebound:         0
```

```
Total number of objects deleted:          0
Total number of objects expired:          0
Total number of objects failed:           0
Total number of subfile objects:          0
Total number of bytes transferred:    1.41 GB
Data transfer time:                  144.13 sec
Network data transfer rate:        10,291.31 KB/sec
Aggregate data transfer rate:      9,659.34 KB/sec
Objects compressed by:                    0%
Subfile objects reduced by:               0%
Elapsed processing time:           00:02:33
```

5. After the first backup run, we unmount the fullvm image as shown in Example 24-17. This deletes the files and the attached directory. In fact, we could just use an operating system DELETE command here, but the unmount is shown in the example because it produces meaningful output that could be used to diagnose problems, should any occur.

Example 24-17 Unmount first fullvm image

```
   C:\Program Files\VMware\VMware Consolidated Backup Framework>vcbmounter -h
   9.43.86.135 -u Admin -p itsoVirtualCenterPassword -U e:\itsovm1
   [2007-11-29 16:59:11.546 'App' 2376 info] Current working directory: C:\Program
   Files\VMware\VMware Consolidated Backup Framework
   [2007-11-29 16:59:11.546 'BaseLibs' 2376 info] HOSTINFO: Seeing Intel CPU,
   numCoresPerCPU 2 numThreadsPerCore 1.
   [2007-11-29 16:59:11.546 'BaseLibs' 2376 info] HOSTINFO: This machine has 1
   physical CPUS, 2 total cores, and 2 logical CPUs.
   [2007-11-29 16:59:11.546 'BaseLibs' 2376 info] Using system libcrypto, version
   90703F
   [2007-11-29 16:59:11.953 'BaseLibs' 2304 warning] [Vmdb_Unset] Unsetting
   unknown path: /vmomi/
   Deleted directory e:\itsovm1
C:\Program Files\VMware\VMware Consolidated Backup Framework>
```

6. We made a small change to the guest's file system. We created a small test file on the C drive and repeated the fullvm backup operation to see how using subfile backup would perform.
7. The results are shown in Example 24-18. Compared to Example 24-16 on page 354, we can see that the original 1.33 GB backup is reduced to 155 MB with subfile backup enabled. The total time elapsed is less than 10 seconds, compared to the original 2 minutes 33 seconds.

   It is likely that the 11 MB of changed data that was picked up by subfile backup includes things like parts of the paging file, as well as the files touched when we logged into ITSOVM1 to create our small file (for example, NTUSER.DAT).

Example 24-18 Second backup with subfile enabled

```
C:\Program Files\Tivoli\TSM\baclient>dsmc sel -subdir=y e:\itsovm1\*
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 5, Level 0.0
  Client date/time: 12/11/2007 16:06:34
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights Reserved.
Node Name: MENSA
Session established with server LOCHNESE: Windows
  Server Version 5, Release 5, Level 0.0
  Server date/time: 12/11/2007 16:07:00  Last access: 12/11/2007 16:04:26
Total number of objects inspected:       14
Total number of objects backed up:       14
Total number of objects updated:          0
Total number of objects rebound:          0
Total number of objects deleted:          0
Total number of objects expired:          0
Total number of objects failed:           0
Total number of subfile objects:         10
Total number of bytes transferred:   10.64 MB
Data transfer time:                    1.14 sec
Network data transfer rate:        9,548.90 KB/sec
Aggregate data transfer rate:      1,127.46 KB/sec
Objects compressed by:                    0%
Subfile objects reduced by:             100%
Elapsed processing time:           00:00:09
C:\Program Files\Tivoli\TSM\baclient>
```

For your information and interest, we provide a sample script to perform these operations in Appendix A, “Sample script for fullvm backup with Tivoli Storage Manager” on page 373.

> **Note:** You could *archive* the generated files rather than *selective backup*. In this case, a single fullvm image would be archived or retrieved as a single operation. You can specify a package description to the archive for easier identification on retrieve. The downside of archive versus backup is that you cannot exploit subfile backup in an archive operation. Therefore, you will always transmit and store all the data.
>
> You might also consider storing the generated fullvm backups locally and managing them via HSM, using HSM for Windows. This is beyond the scope of this book.

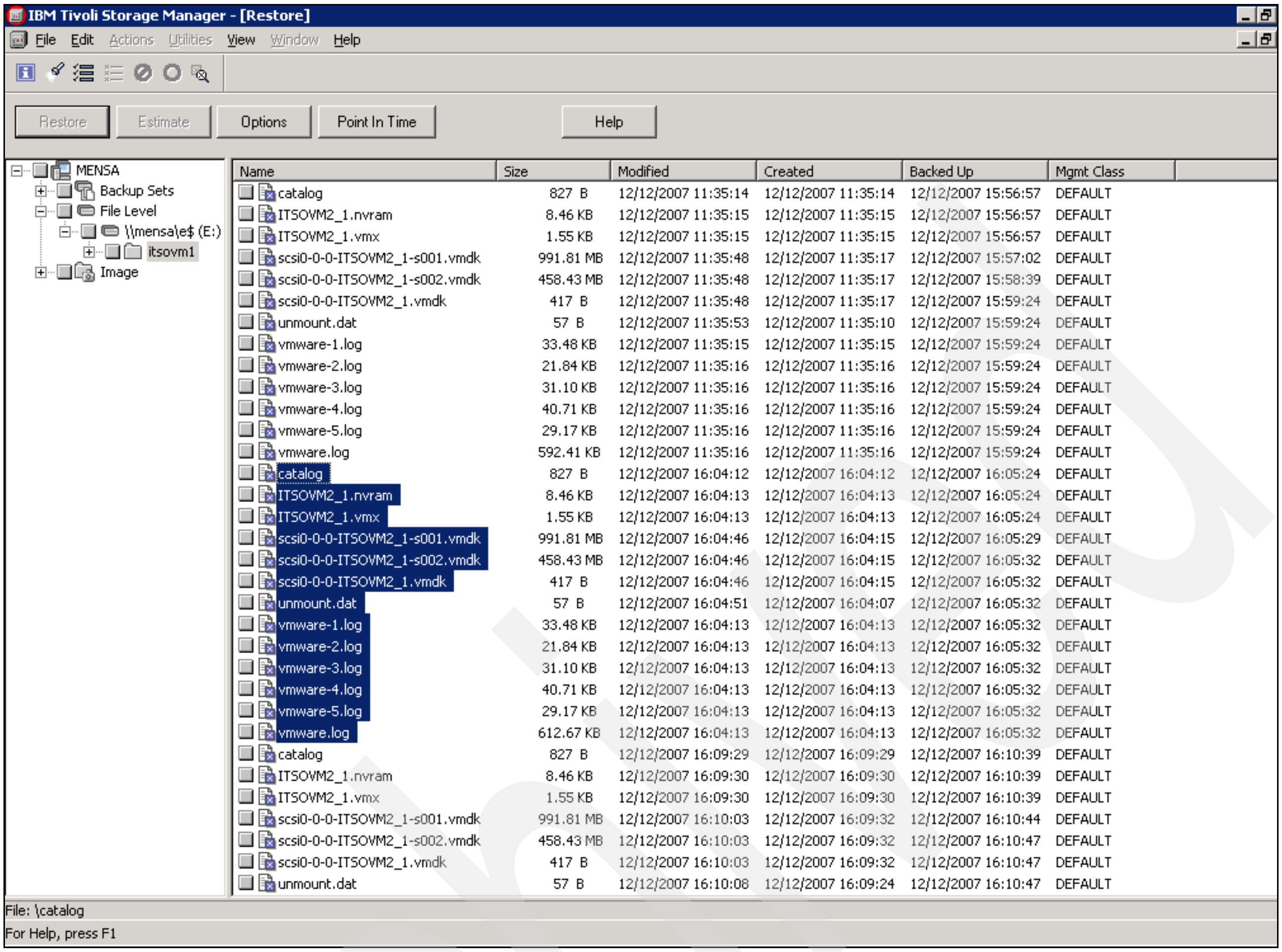
24.8 Restore a full virtual machine in a VCB environment

Now that you have backed up the fullvm image files, what if you want to restore? You can only do a full restore in this type of backup. Direct file-level restore is not possible.

> **Note:** It is possible to restore individual files using **mountvm**, a VMWare command-line utility. The **mountvm** command takes a VMDK disk file and mounts it as a virtual disk on top of an existing hard drive's file system. Once it is mounted, you can browse the VMware virtual disk and copy files from it as required. Documentation of the use of **mountvm** is beyond the scope of this book. For more information see:
>
> http://vmblog.com/archive/2007/09/05/3-vmware-consolidated-backup-vcb-utilities-you-should-know.aspx.

As a first step, restore (or retrieve, if you archived the files to Tivoli Storage Manager) all the image files to a directory, for example, on the proxy node. Make sure to restore all the files backed up in Example 24-16.

You must restore all the files from the same backup, since mixing the files from different fullvm snapshots causes unexpected behavior. You can choose to restore the files based on the date they were backed up, as shown in Figure 24-22 on page 357.



Name	Size	Modified	Created	Backed Up	Mgmt Class
□ catalog	827 B	12/12/2007 11:35:14	12/12/2007 11:35:14	12/12/2007 15:56:57	DEFAULT
□ ITSOVM2_1.nvram	8.46 KB	12/12/2007 11:35:15	12/12/2007 11:35:15	12/12/2007 15:56:57	DEFAULT
□ ITSOVM2_1.vmx	1.55 KB	12/12/2007 11:35:15	12/12/2007 11:35:15	12/12/2007 15:56:57	DEFAULT
□ scsi0-0-0-ITSOVM2_1-s001.vmdk	991.81 MB	12/12/2007 11:35:48	12/12/2007 11:35:17	12/12/2007 15:57:02	DEFAULT
□ scsi0-0-0-ITSOVM2_1-s002.vmdk	458.43 MB	12/12/2007 11:35:48	12/12/2007 11:35:17	12/12/2007 15:58:39	DEFAULT
□ scsi0-0-0-ITSOVM2_1.vmdk	417 B	12/12/2007 11:35:48	12/12/2007 11:35:17	12/12/2007 15:59:24	DEFAULT
□ unmount.dat	57 B	12/12/2007 11:35:53	12/12/2007 11:35:10	12/12/2007 15:59:24	DEFAULT
□ vmware-1.log	33.48 KB	12/12/2007 11:35:15	12/12/2007 11:35:15	12/12/2007 15:59:24	DEFAULT
□ vmware-2.log	21.84 KB	12/12/2007 11:35:16	12/12/2007 11:35:16	12/12/2007 15:59:24	DEFAULT
□ vmware-3.log	31.10 KB	12/12/2007 11:35:16	12/12/2007 11:35:16	12/12/2007 15:59:24	DEFAULT
□ vmware-4.log	40.71 KB	12/12/2007 11:35:16	12/12/2007 11:35:16	12/12/2007 15:59:24	DEFAULT
□ vmware-5.log	29.17 KB	12/12/2007 11:35:16	12/12/2007 11:35:16	12/12/2007 15:59:24	DEFAULT
□ vmware.log	592.41 KB	12/12/2007 11:35:16	12/12/2007 11:35:16	12/12/2007 15:59:24	DEFAULT
□ catalog	827 B	12/12/2007 16:04:12	12/12/2007 16:04:12	12/12/2007 16:05:24	DEFAULT
□ ITSOVM2_1.nvram	8.46 KB	12/12/2007 16:04:13	12/12/2007 16:04:13	12/12/2007 16:05:24	DEFAULT
□ ITSOVM2_1.vmx	1.55 KB	12/12/2007 16:04:13	12/12/2007 16:04:13	12/12/2007 16:05:24	DEFAULT
□ scsi0-0-0-ITSOVM2_1-s001.vmdk	991.81 MB	12/12/2007 16:04:46	12/12/2007 16:04:15	12/12/2007 16:05:29	DEFAULT
□ scsi0-0-0-ITSOVM2_1-s002.vmdk	458.43 MB	12/12/2007 16:04:46	12/12/2007 16:04:15	12/12/2007 16:05:32	DEFAULT
□ scsi0-0-0-ITSOVM2_1.vmdk	417 B	12/12/2007 16:04:46	12/12/2007 16:04:15	12/12/2007 16:05:32	DEFAULT
□ unmount.dat	57 B	12/12/2007 16:04:51	12/12/2007 16:04:07	12/12/2007 16:05:32	DEFAULT
□ vmware-1.log	33.48 KB	12/12/2007 16:04:13	12/12/2007 16:04:13	12/12/2007 16:05:32	DEFAULT
□ vmware-2.log	21.84 KB	12/12/2007 16:04:13	12/12/2007 16:04:13	12/12/2007 16:05:32	DEFAULT
□ vmware-3.log	31.10 KB	12/12/2007 16:04:13	12/12/2007 16:04:13	12/12/2007 16:05:32	DEFAULT
□ vmware-4.log	40.71 KB	12/12/2007 16:04:13	12/12/2007 16:04:13	12/12/2007 16:05:32	DEFAULT
□ vmware-5.log	29.17 KB	12/12/2007 16:04:13	12/12/2007 16:04:13	12/12/2007 16:05:32	DEFAULT
□ vmware.log	612.67 KB	12/12/2007 16:04:13	12/12/2007 16:04:13	12/12/2007 16:05:32	DEFAULT
□ catalog	827 B	12/12/2007 16:09:29	12/12/2007 16:09:29	12/12/2007 16:10:39	DEFAULT
□ ITSOVM2_1.nvram	8.46 KB	12/12/2007 16:09:30	12/12/2007 16:09:30	12/12/2007 16:10:39	DEFAULT
□ ITSOVM2_1.vmx	1.55 KB	12/12/2007 16:09:30	12/12/2007 16:09:30	12/12/2007 16:10:39	DEFAULT
□ scsi0-0-0-ITSOVM2_1-s001.vmdk	991.81 MB	12/12/2007 16:10:03	12/12/2007 16:09:32	12/12/2007 16:10:44	DEFAULT
□ scsi0-0-0-ITSOVM2_1-s002.vmdk	458.43 MB	12/12/2007 16:10:03	12/12/2007 16:09:32	12/12/2007 16:10:47	DEFAULT
□ scsi0-0-0-ITSOVM2_1.vmdk	417 B	12/12/2007 16:10:03	12/12/2007 16:09:32	12/12/2007 16:10:47	DEFAULT
□ unmount.dat	57 B	12/12/2007 16:10:08	12/12/2007 16:09:24	12/12/2007 16:10:47	DEFAULT

File: \catalog

For Help, press F1

Figure 24-22 Showing the files we want to use for this particular restore

If you have archived your fullvm files instead of backing them up, you will simply retrieve all of them from the appropriate archive.

Once you have restored the files, you can then use the VMware Converter utility on a system of your choice to import the restored set of image files back onto an ESX Server. You may choose to put the VMware Converter on the proxy so that you backup and restore from the same system. If you choose to do this, make sure to restore the image files to an alternate location from the backup mountpoint directory so that you do not interfere with scheduled backup operations.

VMware Converter can be downloaded from:

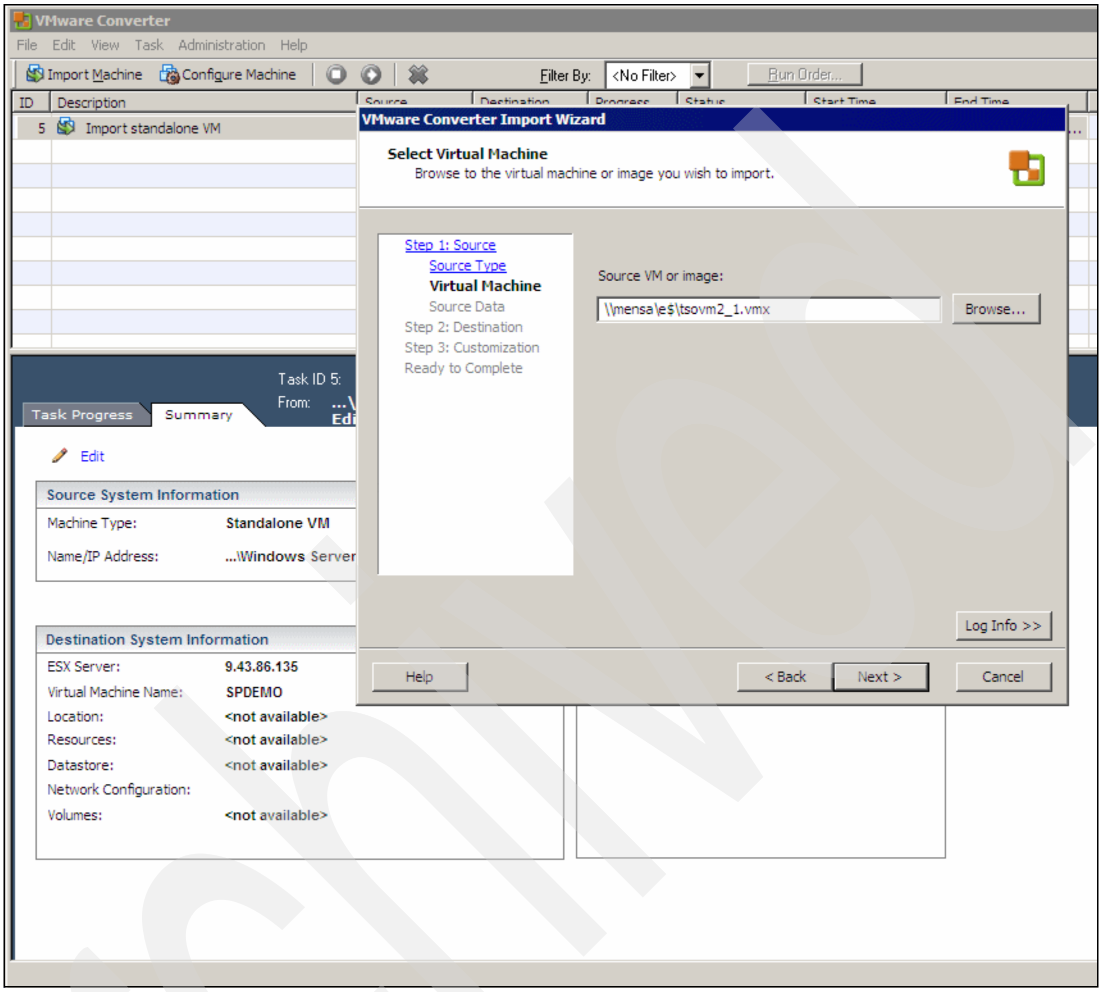
`http://www.vmware.com/products/converter/`

This is the same tool used to convert a physical system into a guest on an ESX server. In our case it takes an existing set of VMware files and imports them into a production ESX environment.

VMware Converter GUI

The VMware Converter GUI is shown in Figure 24-23 on page 358.

Select **Import Machine** to start the import wizard. In the window labelled Source, select **Standalone virtual machine, backup or disk image**. You will be prompted for the location of the .vmx file that you restored (with the other files) from the Tivoli Storage Manager server, as shown in Figure 24-23 on page 358.



Select Virtual Machine

Browse to the virtual machine or image you wish to import.

Source VM or image: \\mensa\e$\tsovm2_1.vmx

Source System Information

Machine Type:	Standalone VM
Name/IP Address:	...\Windows Server

Destination System Information

ESX Server:	9.43.86.135
Virtual Machine Name:	SPDEMO
Location:	<not available>
Resources:	<not available>
Datastore:	<not available>
Network Configuration:	
Volumes:	<not available>

Figure 24-23 VMware Converter

VMware Converter command line

If you want to script or automate a guest restore, you can use the VMware Converter command line. This requires the use of a customized XML file. An example XML file is shown in Example 24-19, with the modified parameters in **bold**.

Example 24-19 C:\Program Files\VMware\VMware Converter\vcb_rest.xml

```
<?xml version="1.0" encoding="UTF-8" ?>
<!-- Restore a VCB image to an ESX 3.x machine directly -->
<p2v version="1.0" xmlns="http://www.vmware.com/v2/sysimage/p2v"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.vmware.com/v2/sysimage/p2v p2v.xsd">
    <source>
      <!-- the "password" attribute is only used for encrypted sources such as the
SV2I format and can be omitted or other types of sources -->
      <hostedSpec password="" path="E:\ITSOVM1\ITSOVM2_1.vmx" />
    </source>
    <dest>
```

```
      <managedSpec datastore="ITSOVCB" folder="" host="" resourcePool=""
vmName="ITSOVM1">
       <creds host="9.43.86.135" password="xxxx" port="" username="Admin" />
      </managedSpec>
    </dest>
      <importParams clonePagefile="false" diskType="VMFS" keepIdentity="true"
       preserveDeviceBackingInfo="false" targetProductVersion="PRODUCT_MANAGED">
      <nicMappings preserveNicsInfo="true" />
    </importParams>
    <postProcessingParams installTools="false" powerOnVM="false" />
</p2v>
```

Save the XML file in the VMware Converter installation directory, and run the **p2vtool** command, specifying the XML file as a parameter, as shown in Example 24-20.

Example 24-20 Run VMware Converter command line

```
C:\Program Files\VMware\VMware Converter>p2vtool -i -s vcb_rest.xml
Using system libcrypto, version 90709F
p2vTool version 3.0.1 build-44840
Reading P2V input from file vcb_rest.xml...
...done
Connecting to UFAD in progress...
...done
Import in progress...
...done
C:\Program Files\VMware\VMware Converter>
```

25

System state and system service

This chapter describes the change of the system state and system service operation in the Tivoli Storage Manager client V5.5 for Windows 2003 and Windows Vista. The system state consists of all bootable system state and system services components. Tivoli Storage Manager uses the Microsoft Volume Shadow Service (VSS) on Windows 2003 and Windows Vista to back up and restore all system state components.

The list of bootable system state and system services components is dynamic and can change depending on the service pack and operating system features installed. Tivoli Storage Manager allows for the dynamic discovery and back up of these components. For a list of components that could be included in the system state see the *Windows Backup-Archive Clients Installation and User’s Guide,* SC32-0146.

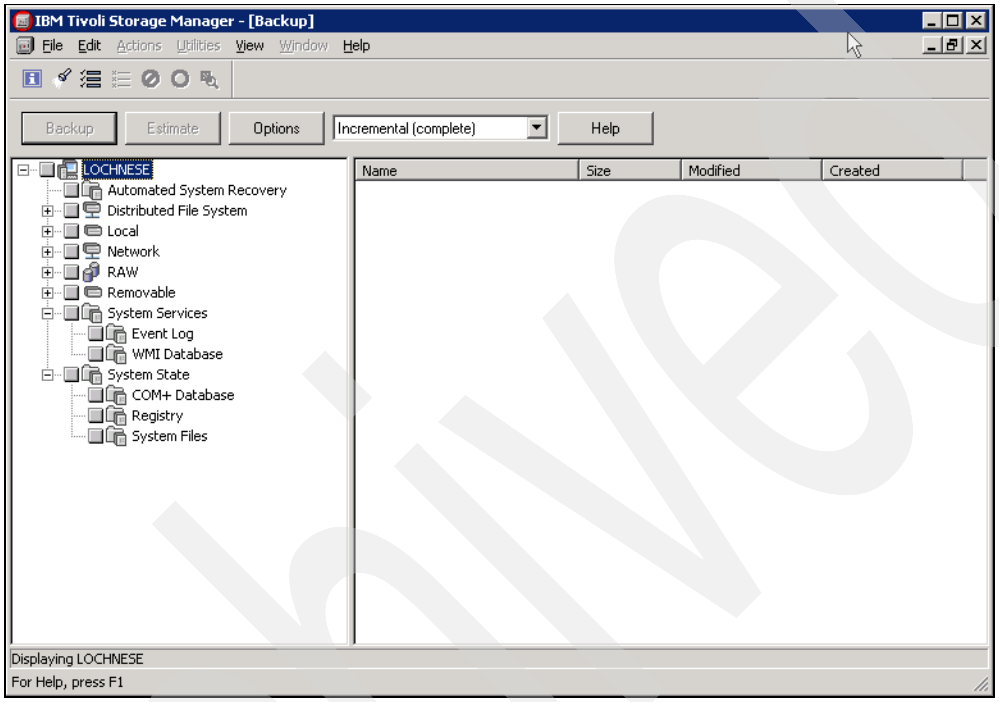
Windows Vista: Allow additional time to back up system state components on a Windows Vista operating system because of the number of files involved.

Windows XP: In Windows XP, the system state and system service backup operation is known as the system object operation. For details about the system object backup operation, see the *Windows Backup-Archive Clients Installation and User’s Guide,* SC32-0146.

25.1 Change between Versions 5.4 and 5.5

In V5.5, system service and system state are now considered as one component, called system state.

In V5.4, you could see the system service and the system state in the backup-archive client GUI Backup window. See Figure 25-1 on page 362.

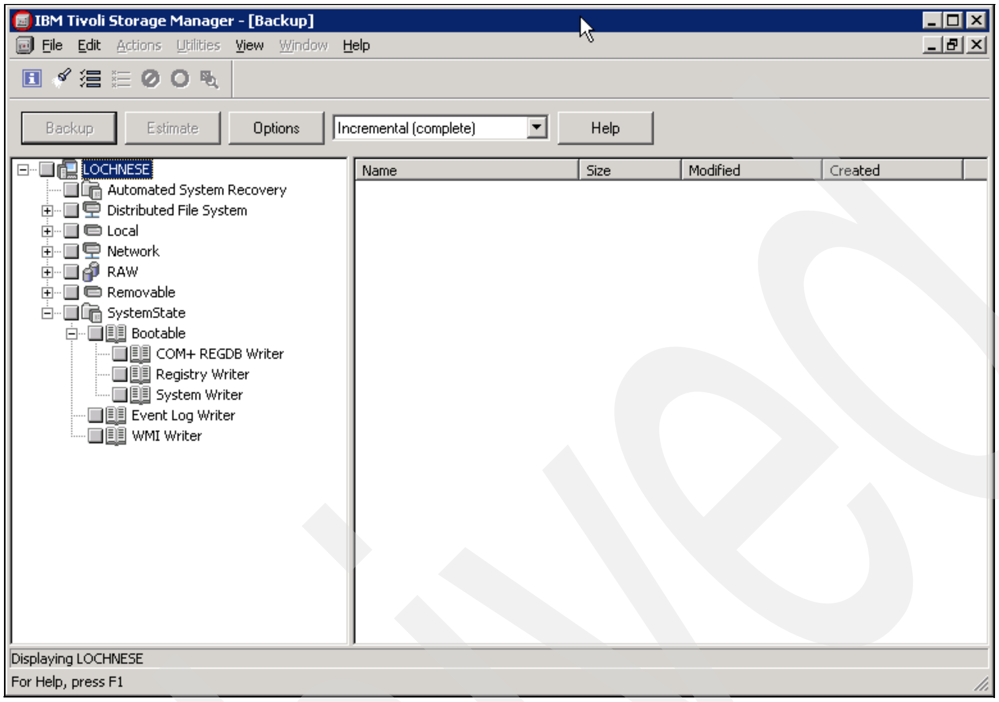


Displaying LOCHNESE

For Help, press F1

Figure 25-1 System state and system service: Tivoli Storage Manager V5.4 Windows 2003 client

In V5.5, the behavior has changed. You will see only SystemState in the backup-archive client GUI Backup window. The system state consists of all bootable system state and system services components, as shown in Figure 25-2 on page 363.



Displaying LOCHNESE

For Help, press F1

Figure 25-2 System state in Tivoli Storage Manager V5.5 Windows 2003 client

This behavior is also reflected in the equivalent restore panels.

In the command line interface (CLI) only the command BACKUP SYSTEMSTATE is still available. The BACKUP SYSTEMSERVICES command is not valid anymore. For the CLI restore, similarly, only the RESTORE SYSTEMSTATE is available, and the RESTORE SYSTEMSERVICES is no longer valid.

The naming convention for the filespace name of the system state on the Tivoli Storage Manager server has also changed. System state is stored as a single file space on the server. For details see 25.2, “Back up the system state” on page 363, and 25.4, “Updating from client V5.4 to V5.5” on page 370.

25.2 Back up the system state

You can back up the system state using either the Tivoli Storage Manager client GUI or CLI. The Microsoft Volume Shadow Service (VSS) is used to back up all system state components as a single object, to provide a consistent point-in-time snapshot of the system state. Administrative authority is required to back up system state information. The system state is always backed up as a single entity. You cannot back up individual components.

For a Windows Server 2003 machine the system and boot files component of the system state are backed up only if a member (file) of that component has changed since the last backup. If any member changes, the entire group of files that comprise that component are backed up. For Windows Vista the complete system state is backed up always.

The backup of the system state for Windows Server 2003 always includes a backup of the Automated System Recovery (ASR). For more details about backing up Automated System Recovery (ASR) see the *Windows Backup-Archive Clients Installation and User's Guide,* SC32-0146.

Note: Backup of Automated System Recovery is not available for Windows Vista.

To back up the Windows system state, your client must be connected to a Tivoli Storage Manager with the Version V5.2.0 or later.

If you use backup sets that include the back up of the system state, your Tivoli Storage Manager server must have one of the following versions:

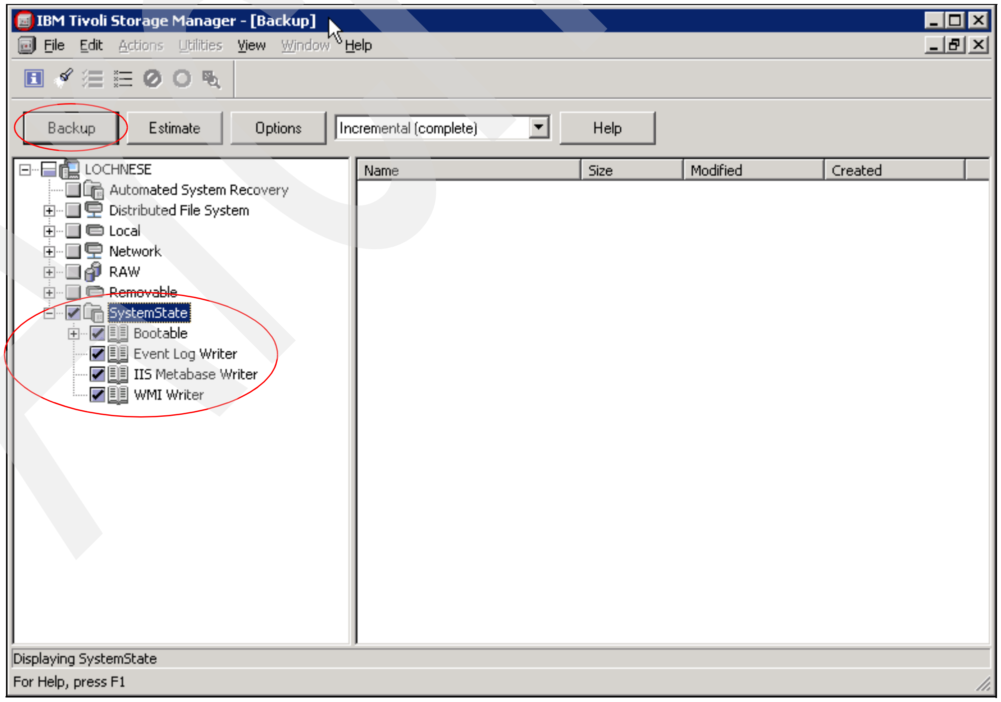
- V5.3.6 and later
- V5.4.1 and later
- V5.5.0

Use the include.systemstate option in your client options file (dsm.opt) to assign management classes for back up of the system state. By default, the system state object is bound to the default management class. The option exclude.systemservice could be used to exclude individual system services.

Include/exclude: For more options for including and excluding the system state operation see the *Windows Backup-Archive Clients Installation and User's Guide,* SC32-0146.

25.2.1 Back up using the GUI

In the GUI, click **Backup** in the main window, check the **SystemState** box, and click **Backup**, as shown in Figure 25-3.



Displaying SystemState

For Help, press F1

Figure 25-3 Back up the system state with GUI

25.2.2 Back up using the CLI

Use the BACKUP SYSTEMSTATE command, as shown in Example 25-1.

Example 25-1 Back up the system state with CLI

```
tsm> backup systemstate
Session established with server LOCHNESE: Windows
  Server Version 5, Release 5, Level 0.0
  Server date/time: 11/12/2007 13:37:14  Last access: 11/12/2007 13:34:44

Backup System State using shadow copy...
Preparing to backup using snapshot.

...

Total number of objects inspected:    2,968
Total number of objects backed up:    2,968
Total number of objects updated:          0
Total number of objects rebound:          0
Total number of objects deleted:          0
Total number of objects expired:          0
Total number of objects failed:           0
Total number of bytes transferred:   558.60 MB
Data transfer time:                    2.40 sec
Network data transfer rate:        237,448.80 KB/sec
Aggregate data transfer rate:      8,724.64 KB/sec
Objects compressed by:                    0%
Elapsed processing time:           00:01:05

SystemState Backup finished successfully.

tsm>
```

Use the QUERY SYSTEMSTATE command to display information about backups of the system state on the Tivoli Storage Manager server or inside a backup set when a backup set is specified (option -backupsetname must be specified). Sample output is shown in Example 25-2.

Example 25-2 QUERY SYSTEMSTATE command

```
tsm> query systemstate
           Size        Backup Date      Mgmt Class   A/I File
           ----        -----------      ----------   --- ----
    19,287,020  B  11/14/2007 22:00:06    DEFAULT     A  FULL LOCHNESE\SystemSt
ate\NULL\System State\SystemState\TSM\FULL\20071114220006\Top\SystemState\WMI\W
indows Managment Instrumentation\1\WMI Writer
       300,176  B  11/14/2007 22:00:06    DEFAULT     A  FULL LOCHNESE\SystemSt
ate\NULL\System State\SystemState\TSM\FULL\20071114220006\Top\SystemState\IISME
TABASE\null\1\IIS Metabase Writer
       182,332  B  11/14/2007 22:00:06    DEFAULT     A  FULL LOCHNESE\SystemSt
ate\NULL\System State\SystemState\TSM\FULL\20071114220006\Top\SystemState\Event
 Logs\Event Logs\1\Event Log Writer
    18,544,560  B  11/14/2007 22:00:06    DEFAULT     A  FULL LOCHNESE\SystemSt
ate\NULL\System State\SystemState\TSM\FULL\00000000000000\Top\SystemState\Boota
ble\Bootable System State\0\Bootable
```

```
    18,522,112  B  11/14/2007 22:00:06    DEFAULT     A  FULL LOCHNESE\SystemSt
ate\NULL\System State\SystemState\TSM\FULL\20071114220006\Top\SystemState\Boota
ble\Registry\Registry\1\Registry Writer
        22,448  B  11/14/2007 22:00:06    DEFAULT     A  FULL LOCHNESE\SystemSt
ate\NULL\System State\SystemState\TSM\FULL\20071114220006\Top\SystemState\Boota
ble\COM+ REGDB\COM+ REGDB\1\COM+ REGDB Writer
   580,247,944  B  11/14/2007 22:00:06    DEFAULT     A  FULL LOCHNESE\SystemSt
ate\NULL\System State\SystemState\TSM\FULL\20071114114351\Top\SystemState\Boota
ble\System Files\System Files\1\System Writer
```

25.2.3 System state filespaces

When viewing backups on the Tivoli Storage Manager server, filespaces for the ASR and system state are created, as shown in Example 25-3.

Example 25-3 Output from query filespace on the Tivoli Storage Manager Server

```
tsm: LOCHNESE>query filespace lochnese format=detail

Node Name: LOCHNESE
                                 Filespace Name: LOCHNESE\SystemState\NULL\Sys-
                                                  tem State\SystemState
                     Hexadecimal Filespace Name: 4c4f43484e4553455c53797374656-
                                                  d53746174655c4e554c4c5c53797-
                                                  374656d2053746174655c5379737-
                                                  4656d5374617465
                                           FSID: 1
                                       Platform: WinNT
                                 Filespace Type: VSS
                          Is Filespace Unicode?: Yes
                                  Capacity (MB): 0.0
                                       Pct Util: 0.0
                    Last Backup Start Date/Time: 11/12/2007 15:32:15
                 Days Since Last Backup Started: <1
               Last Backup Completion Date/Time: 11/12/2007 15:33:10
               Days Since Last Backup Completed: <1
Last Full NAS Image Backup Completion Date/Time:
Days Since Last Full NAS Image Backup Completed:

                                      Node Name: LOCHNESE
                                 Filespace Name: ASR
                     Hexadecimal Filespace Name: 415352
                                           FSID: 2
                                       Platform: WinNT
                                 Filespace Type: NTFS
                          Is Filespace Unicode?: Yes
                                  Capacity (MB): 0.0
                                       Pct Util: 0.0
                    Last Backup Start Date/Time: 11/12/2007 15:33:15
                 Days Since Last Backup Started: <1
               Last Backup Completion Date/Time: 11/12/2007 15:33:15
               Days Since Last Backup Completed: <1
Last Full NAS Image Backup Completion Date/Time:
Days Since Last Full NAS Image Backup Completed:
```

This example shows that there is a new naming convention for the system state filespace name compared with previous Tivoli Storage Manager Windows client versions. The filespace name has the format <*hostname*>\SystemState\NULL\System State\SystemState, where *hostname* indicates the system from where the system state was backed up.

For more information about the filespace name when migrating from a previous Tivoli Storage Manager client version, see 25.4, “Updating from client V5.4 to V5.5” on page 370, later in this chapter.

25.3 Restore the system state

You can restore the system state with either the GUI or CLI. The Microsoft Volume Shadow Service (VSS) is used to restore the system state. Administrative authority is required to restore system state information.

> **Attention:** Restoring system state in a situation other than system recovery is not recommended.

By default, all system state components are restored together. However, you can restore just the bootable system state components or individual system services components, as shown in Figure 25-4.

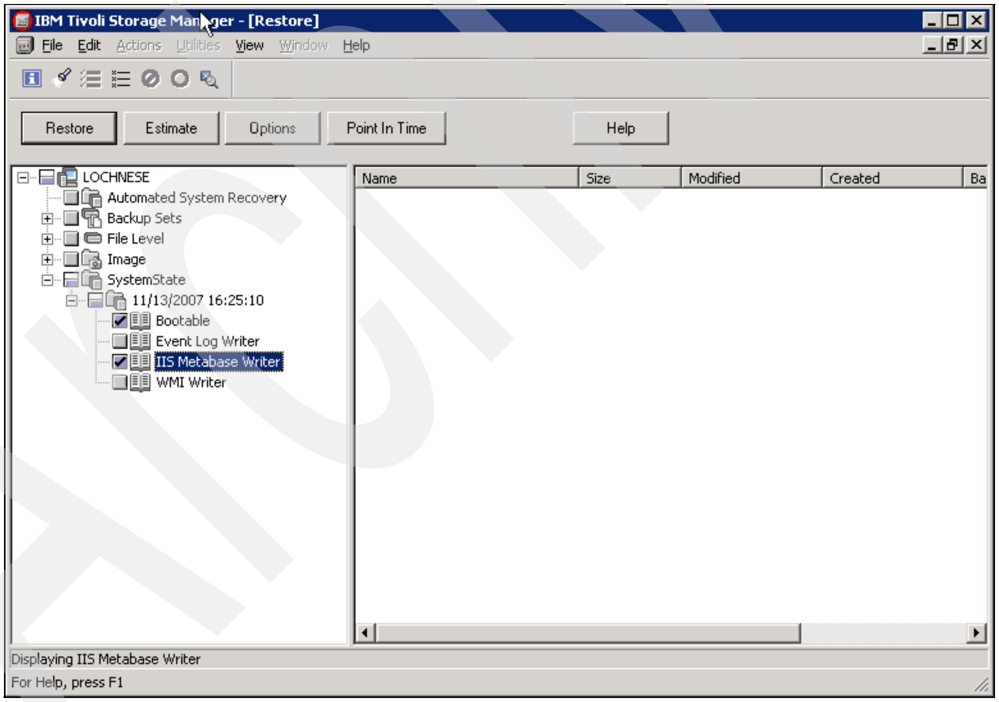


Figure 25-4 Restoring individual components from SystemState

Restoring an individual system services component will restore only a specific system service and not necessarily your Windows operating system.

If the system state was not previously backed up with the Tivoli Storage Manager client V5.5, it is not displayed in the restore GUI. System state backups with pre-V5.5 clients can also not be selected for restores, and they are not displayed in the V5.5 GUI. For more details on pre-V5.5 clients, see 25.4, “Updating from client V5.4 to V5.5” on page 370.

During system state restore, all data is restored to their original locations except for files that are protected by System File Protection (SFP). SFP files are restored to a temporary location. You must then reboot. After the reboot, the original SFP files are deleted, and the restored SFP files are renamed to the original file names.

Extra disk space is required to restore SFP files because they are restored to a temporary location on disk. On Windows Server 2003, most of the system state data are SFP files, so approximately 1 GB of free disk space is required. Because more files are involved in the system state for Windows Vista approximately 7 GB of free disk space is needed.

25.3.1 Restore using the GUI

To restore using the GUI, click **Restore** in the main window, check the **SystemState** box, and click **Restore**, as shown in Figure 25-5.

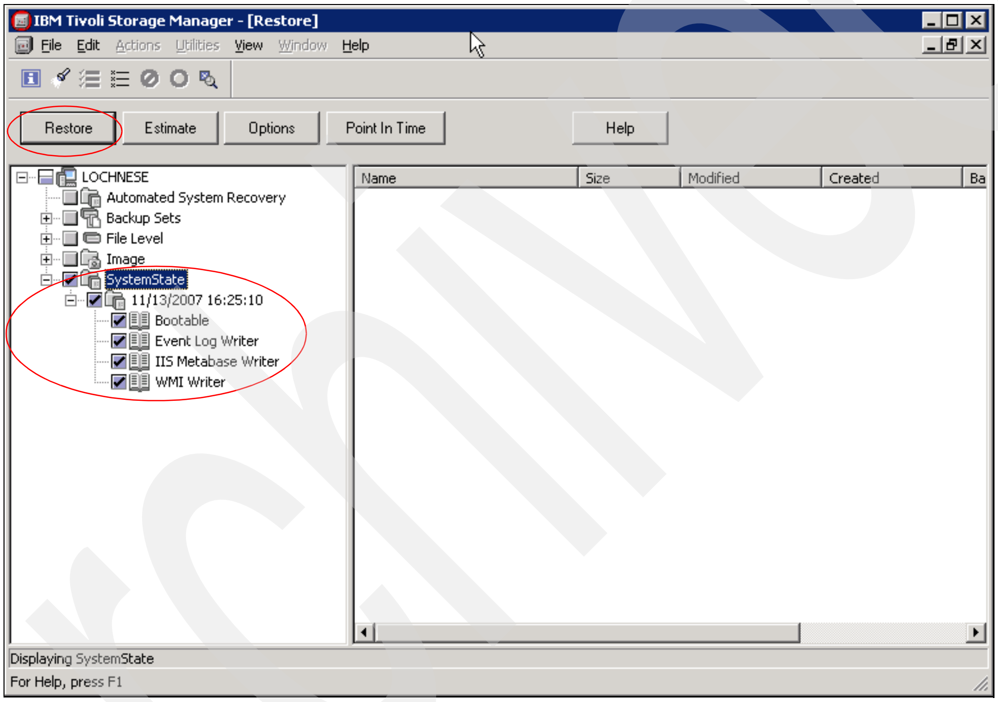


Figure 25-5 Restore SystemState using the B/A client GUI on Windows 2003

As seen in the figure, as of the V5.5 backup-archive client, the date of the SystemState backup is displayed under the SystemState category. This helps to quickly identify whether the selected SystemState for the restore is from a valid date. To display older SystemState backups for the restore, select **View ∅ Display active/inactive files**, but restore components from different available backups is not possible. The components that you like to restore must belong to the same backup.

25.3.2 Restore using the CLI

Use the RESTORE SYSTEMSTATE command, as shown in Example 25-4.

Example 25-4 Restore the system state using the CLI on a Windows Server 2003

```
tsm> restore systemstate
Restore System State using shadow copy...
Preparing for restore of 'System State' from TSM backup.
ANS1899I ***** Examined     1,000 files *****
ANS1899I ***** Examined     2,000 files *****
Restoring         927,504 \\lochnese\c$\WINDOWS\system32\mfc40u.dll [Done]
Restoring       1,160,704 \\lochnese\c$\WINDOWS\system32\mfc42.dll [Done]
Restoring       1,163,776 \\lochnese\c$\WINDOWS\system32\mfc42u.dll [Done]
Restoring          23,040 \\lochnese\c$\WINDOWS\system32\mfcsubs.dll [Done]
Restoring         461,672 \\lochnese\c$\WINDOWS\Fonts\micross.ttf [Done]
Restoring           8,704 \\lochnese\c$\WINDOWS\Fonts\modern.fon [Done]
Restoring         668,460 \\lochnese\c$\WINDOWS\AppPatch\msimain.sdb [Done]

...<output deleted>

ANS1139W '\\lochnese\c$\WINDOWS\system32\wbem\Repository\FS\MAPPING2.MAP' was re
stored as '$TSMInUse.1195065777.78.f5.MAPPING2.MAP'. A reboot is required to com
plete the restore.
Restoring       7,749,632 \\lochnese\c$\WINDOWS\system32\wbem\Repository\FS\OBJE
CTS.DATA [Done]
ANS1139W '\\lochnese\c$\WINDOWS\system32\wbem\Repository\FS\OBJECTS.DATA' was re
stored as '$TSMInUse.1195065777.93.f6.OBJECTS.DATA'. A reboot is required to com
plete the restore.

Total number of objects restored:     2,889
Total number of objects failed:           0
Total number of bytes transferred:   556.94 MB
Data transfer time:                    2.96 sec
Network data transfer rate:        192,153.50 KB/sec
Aggregate data transfer rate:      11,223.73 KB/sec
Elapsed processing time:           00:00:50
ANS1430W The machine must be rebooted for the changes to take effect.
tsm>
```

With the RESTORE SYSTEMSTATE command, all system state components are restored together. To restore just the bootable system state components, use RESTORE SYSTEMSTATE BOOTABLE. For individual system services components you can enter, for example, RESTORE SYSTEMSTATE WMI, to restore the WMI, for example. For a list of the individual system state services see the *Windows Backup-Archive Clients Installation and User's Guide*.

25.4 Updating from client V5.4 to V5.5

If you have used a pre-V5.5 Tivoli Storage Manager client to back up a node, you will see different filespace names for the system state and the system service, as shown in Example 25-5.

Example 25-5 Query filespace from a client with pre-V5.5 B/A client

```
tsm: LOCHNESE>query filespace lochnese

Node Name       Filespace   FSID Platform Filespace Is Files-    Capacity   Pct
                Name                      Type        pace           (MB)  Util
                                                    Unicode?
--------------- ----------- ---- -------- --------- --------- ----------- -----
LOCHNESE        SYSTEM         1 WinNT    SYSTEM       Yes              0.0   0.0
                 SERVICES
LOCHNESE        SYSTEM         2 WinNT    SYSTEM       Yes              0.0   0.0
                 STATE
LOCHNESE        ASR            3 WinNT    NTFS         Yes              0.0   0.0
```

After you update the client to V5.5 and run a system state backup, a new filespace is added as explained in 25.2.3, “System state filespaces” on page 366. The filespaces will be displayed similar to Example 25-6.

Example 25-6 Query filespace from a client with V5.5 B/A client

```
tsm: LOCHNESE>query filespace lochnese

Node Name       Filespace   FSID Platform Filespace Is Files-    Capacity   Pct
                Name                      Type        pace           (MB)  Util
                                                    Unicode?
--------------- ----------- ---- -------- --------- --------- ----------- -----
LOCHNESE        SYSTEM         1 WinNT    SYSTEM       Yes              0.0   0.0
                 SERVICES
LOCHNESE        SYSTEM         2 WinNT    SYSTEM       Yes              0.0   0.0
                 STATE
LOCHNESE        ASR            3 WinNT    NTFS         Yes              0.0   0.0
LOCHNESE        LOCHNESE\S-    4 WinNT    VSS          Yes              0.0   0.0
                 ystemStat-
                 e\NULL\Sy-
                 stem Stat-
                 e\SystemS-
                 tate
```

Any previously backed up system state and system services filespaces (with a pre-V5.5 client) will be expired according to the management class policy, but the active version will not expire automatically. If you need to restore information from the old filespaces (the pre-V5.5 system state backups) you must install an older (pre-V5.5) B/A client. If you generate a backup set that includes these filespaces and perform a restore from this backup set, the filespaces are skipped and the message `ANS1753E: File space 'filespace name' was backed up by an older client version, and cannot be restored with this client version. The file space will be skipped` is displayed.

If the old filespaces are not needed anymore (for example, when the system state has been backed up several times successful with the Version 5.5) you should consider deleting the old filespaces, because they will not be deleted automatically (active versions will not expire). This could be performed with the commands, as shown in Example 25-7.

Example 25-7 Deleting pre-V5.5 system state backups

```
tsm: LOCHNESE>delete filespace lochnese "SYSTEM SERVICES" nametype=unicode
ANR2238W This command will result in the deletion of all inventory references
to the data on filespaces that match the pattern SYSTEM SERVICES (fsId=1) for
node LOCHNESE , whereby rendering the data unrecoverable.

Do you wish to proceed? (Yes (Y)/No (N)) y
ANS8003I Process number 8 started.

tsm: LOCHNESE>delete filespace lochnese "SYSTEM STATE" nametype=unicode
ANR2238W This command will result in the deletion of all inventory references
to the data on filespaces that match the pattern SYSTEM STATE (fsId=4) for node
LOCHNESE , whereby rendering the data unrecoverable.

Do you wish to proceed? (Yes (Y)/No (N)) y
ANS8003I Process number 9 started.

tsm: LOCHNESE>
```

A

Sample script for fullvm backup with Tivoli Storage Manager

This appendix provides a sample perl script that you can use to automate a fullvm VCB backup with Tivoli Storage Manager. The script is provide as is and should be customized and carefully tested before using.

Example: A-1 Perl script for full VMware VCB backups from a backup proxy

```
#############################################################################
#  name:  vcbfull.pl
#  desc:  Perform full VMware VCB backups from a backup proxy
#         utilizing vcbMounter.exe and dsmc.exe
#
# notes:  You will need to customize the variables $VCBPATH and $TSMPATH
#         below to match your environment
#         This script is provided “AS-IS” -
#         No support is given or implied by IBM
#############################################################################

my $vcbpath = "O:\\Program Files\\VMware\\VMware Consolidated Backup Framework";
my $tsmpath = "O:\\Program Files\\Tivoli\\TSM\\baclient";

use Cwd;
use File::Path;


# Validate and process command arguments
if (@ARGV < 5)
{
  usage();
  die;
}
```

```
# Process optional arguments
my $vmchost = "";
my $vmcuser = "";
my $vmcpw = "";
my $vmlist = "";
my $vcbmnt = "";

foreach $arg (@ARGV)
{
  if ($arg =~ m/-vmchost=(\S+)/i)
  {
    $vmchost = $1;
  }
  elsif ($arg =~ m/-vmcuser=(\S+)/i)
  {
    $vmcuser = $1;
  }
  elsif ($arg =~ m/-vmcpw=(\S+)/i)
  {
    $vmcpw = $1;
  }
  elsif ($arg =~ m/-vmlist=(\S+)/i)
  {
    $vmlist = $1;
  }
  elsif ($arg =~ m/-vcbmnt=(\S+)/i)
  {
    $vcbmnt = $1;
  }
  else
  {
    print "\nERROR: unexpected argument $arg\n";
    usage();
    die;
  }
}

if ($vmchost eq "" || $vmcuser eq "" || $vmcpw eq "" || $vmlist eq "" || $vcbmnt
eq "")
{
  print "\nERROR: Missing one or more required parameters\n";
  usage();
  die;
}

print
"\n=========================================================================\n";
$curtime = localtime();
print "\n$curtime: Command vcbfull invoked with the following arguments:\n";
print (" vmchost =\t$vmchost\n vmcuser =\t$vmcuser\n vmcpw =\t$vmcpw\n vmlist
=\t$vmlist\n vcbmnt =\t$vcbmnt\n");

# Parse the machine specified in vmlist
my @vmList = split (',', $vmlist);
```

```
# Build the complete VCB local storage path
my $vcbstore = $vcbmnt."\\tsmvmbackup\\fullVM";
my $buildpath = "";
foreach $dir (split('\\\\', $vcbstore))
{
  $buildpath = $buildpath.$dir."\\";
if (! -d $buildpath)
  {
    mkdir ($buildpath, 0777);
  }
  chdir ($buildpath);
}

if (-d $vcbstore)
{
  print "\n$curtime: The following path will be used:\n";
  print (" vcbstore =\t$vcbstore\n");
}
else
{
  print "\nERROR: Unable to create full path for VCB store in this path:\n";
  print (" vcbstore =\t$vcbstore\n");
  die;
}


# Validate required programs are available
if (! -f $vcbpath."\\vcbMounter.exe")
{
  print "\nERROR: Unable to locate required VCB program:\n";
  print ("\t$vcbpath\\vcbMounter.exe\n");
  die;
}
if (! -f $tsmpath."\\dsmc.exe")
{
  print "\nERROR: Unable to locate required TSM program:\n";
  print ("\t$tsmpath\\dsmc.exe\n");
  die;
}
else
{
  $curtime = localtime();
  print "\n$curtime: Located required program files:\n";
  print ("\t$vcbpath\\vcbMounter.exe\n");
  print ("\t$tsmpath\\dsmc.exe");
  print "\n";
}


# Perform the requested backups
my @succList = qw();
my @failList = qw();

$curtime = localtime();
```

```
print "$curtime: Starting backup processing.\n";

foreach $vm (@vmList)
{
  # create the full snapshot export
  chdir ($vcbpath);
  $curtime = localtime();
  print "\n------------------------------------------------------\n";
  print "$curtime:  Creating export of $vm with the following command:\n";
  my $cmd = "vcbMounter -h $vmchost -u $vmcuser -p $vmcpw -a ipaddr:$vm -r 
${vcbstore}\\$vm -t fullvm";
  print "\t$cmd\n";
  @out = `$cmd`;
  if ($? != 0)
  {
    print "ERROR:  failed to take snapshot:\n@out\n";
    push (@failList, $vm);
  }
  else
  {
    print "@out\n";
    chdir ($tsmpath);
    $curtime = localtime();
    print "$curtime = Performing backup of $vm using the command:\n";
    $cmd = "dsmc sel ${vcbstore}\\$vm\\* -optfile=dsm.opt3";
    print "\t$cmd\n";
    @out = `$cmd`;
    if ($? != 0)
    {
      print "ERROR: failure during backup.\n@out\n";
      push (@failList, $vm);
    }
    else
    {
      print "@out\n";
      rmtree ($vcbstore."\\".$vm, 0, 0);
      push (@succList, $vm);
    }
  }
}


$curtime = localtime();
print "$curtime: Processing finished.\n";
print "Machines processed successfully: @succList\n";
print "Machines which failed: @failList\n";

sub usage
{
  print "\nUSAGE: perl vcbfull.pl\n\t-vmchost=<VMware ESX or VC 
host>\n\t-vmcuser=<user>\n\t-vmcpw=<secret>\n\t-vmlist=<vm1,vm2,..,vmN>\n\t-vcbmnt
=<mnt pnt>\n";
  print "\n";
}
```

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

IBM Redbooks

For information about ordering these publications, see "How to get Redbooks" on page 378. Note that some of the documents referenced here may be available in softcopy only.

- *IBM Tivoli Storage Management Concepts*, SG24-4877
- *IBM Tivoli Storage Manager Implementation Guide*, SG24-5416
- *IBM System Storage Tape Encryption Solutions*, SG24-7320
- *IBM System Storage Tape Encryption Solutions*, SG24-7320
- *IBM Tivoli Storage Manager: Building a Secure Environment*, SG24-7505
- *Using the Tivoli Storage Manager HSM Client for Windows*, REDP-4126
- *IBM Tivoli Storage Manager Version 5.3 Technical Guide*, SG24-6638
- *Using the IBM System Storage N Series with IBM Tivoli Storage Manager*, SG24-7243

Other publications

These publications are also relevant as further information sources:

- *IBM Tivoli Storage Manager for AIX Administrator's Guide,* SC32-0117
- *IBM Tivoli Storage Manager for AIX Administrator's Reference,* SC32-0123
- *IBM Tivoli Storage Manager for HP-UX Administrator's Guide,* SC32-0118
- *IBM Tivoli Storage Manager for HP-UX Administrator's Reference,* SC32-0773
- *IBM Tivoli Storage Manager for Linux Administrator's Guide*, SC32-0119
- *IBM Tivoli Storage Manager for Linux Administrator's Reference*, SC32-0125
- *IBM Tivoli Storage Manager for Sun Solaris Administrator's Guide*, SC32-0120
- *IBM Tivoli Storage Manager for Sun Solaris Administrator's Reference*, SC32-0126
- *IBM Tivoli Storage Manager for Windows Administrator's Guide*, SC32-0121
- *IBM Tivoli Storage Manager for Windows Administrator's Reference*, SC32-0127
- *IBM Tivoli Storage Manager for z/OS Administrator's Guide*, SC32-0122
- *IBM Tivoli Storage Manager for z/OS Administrator's Reference*, SC32-0128
- *IBM Tivoli Storage Manager for UNIX Backup-Archive Clients Installation and User's Guide*, SC32-0145
- *IBM Tivoli Storage Manager for Windows Backup-Archive Clients Installation and User's Guide*, SC32-0146
- *IBM Tivoli Storage Manager for Windows Backup-Archive Clients Installation and User's Guide*, SC32-0144

- *IBM Tivoli Storage Manager Using the Application Program Interface*, SC32-0147
- *IBM Encryption Key Manager - Introduction, Planning and User's Guide*,GA76-0418
- *IBM Tape Device Drivers - Encryption Support*, GA32-0565
- *IBM System Storage TS1120 Tape Drive and Controller Operator Guide 3592 Models J1A, E05, J70 and C06*, GA32-0556
- *IBM System Storage TS3500 Tape Library Operator Guide*, GA32-0560-01
- *IBM Encryption Key Manager component for the Java platform Introduction, Planning, and User's Guide*, GA76-0418

How to get Redbooks

You can search for, view, or download Redbooks, Redpapers, Technotes, draft publications and Additional materials, as well as order hardcopy Redbooks, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

IBM

Redbooks

IBM Tivoli Storage Manager Versions 5.4 and 5.5 Technical Guide

IBM Tivoli Storage Manager Versions 5.4 and 5.5 Technical Guide

The new functions in V5.4 and V5.5

Techniques for VMware backup

NDMP backup enhancements and much more

This IBM Redbooks publication gives you details of changes, updates, and new functions provided in IBM Tivoli Storage Manager Version 5.4 and Version 5.5. We cover all the new functions of Tivoli Storage Manager that have been available since the publication of *IBM Tivoli Storage Manager Version 5.3 Technical Guide*, SG24-6638.

This book is intended for customers, consultants, IBM Business Partners, and IBM and Tivoli staff who are familiar with earlier releases of Tivoli Storage Manager and who want to understand what is new in Version 5.4 and Version 5.5. Hence, since we target an experienced audience, we use certain shortcuts to commands and concepts of Tivoli Storage Manager. If you want to learn more about Tivoli Storage Manager functionality, see *IBM Tivoli Storage Management Concepts*, SG24-4877 and *IBM Tivoli Storage Manager Implementation Guide*, SG24-5416.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-7447-00 ISBN 0738485926