Tivoli software

IBM

Backing up Microsoft SQL Server with IBM Tivoli Storage Manager

- Strategic planning and implementation considerations for effective backup
- Tivoli Data Protection for SQL Server V5.5 VSS backups
- SQL Server overview for TSM administrators

Marcia Kubo
Carlos Eduardo Abramo Pinto

Redbooks

ibm.com/redbooks

International Technical Support Organization

Backing up Microsoft SQL Server with IBM Tivoli Storage Manager

June 2008

SG24-6148-01

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

Second Edition (June 2008)

This edition applies to IBM Tivoli Storage Manager, IBM Tivoli Storage Manager for Databases, Data Protection for SQL Server, and IBM Tivoli Storage Manager for Advanced Copy Services.

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

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

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

AIX®
DB2 Universal Database™
DB2®
Domino®
DS6000™
DS8000™
Enterprise Storage Server®
FlashCopy®
General Parallel File System™
IBM®
Informix®
Lotus®
Passport Advantage®
Redbooks®
Redbooks (logo) ®
SysBack™
System p™
System Storage™
System Storage DS™
Tivoli Enterprise Console®
Tivoli®
TotalStorage®
z/OS®

The following terms are trademarks of other companies:

AMD, the AMD Arrow logo, and combinations thereof, are trademarks of Advanced Micro Devices, Inc.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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

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

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

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

Active Directory, Microsoft, SharePoint, SQL Server, Windows NT, Windows Server, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Pentium, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, 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 describes how to plan, install, and implement backup and restore for Microsoft® SQL Server® using Tivoli® Storage Manager products. The book is intended for Tivoli Storage Manager professionals who are responsible for the backup and restore of a Microsoft SQL Server installation using Tivoli Storage Manager.

We discuss the planning, installation, and operation of Tivoli Storage Manager with Microsoft SQL Server. We also give an overview of the Tivoli Storage Manager family of products. We provide essential information regarding Microsoft SQL Server - information intended to assist Tivoli Storage Manager administrators understand the database middleware platform.

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, Austin Center.

Figure 1   Marcia and Carlos

Marcia Kubo is an IT Presales Support Specialist in Brazil. She has more than nine years of experience in the IT field and the Tivoli Storage Manager product portfolio, starting with ADSM V3.1. Her expertise includes AIX®, IBM System p™, and IBM disk and tape. She has been working for IBM since 2004. She is ITIL® Certified, TotalStorage® Productivity Center V3.1 Certified, an IBM Certified Deployment Professional: Tivoli Storage Manager V5.3 and V5.4, and an IBM Certified Advanced Technical Expert for AIX version V4. She has a degree in System Analysis from FATEC-SP, São Paulo. She is an author of *Deployment Guide Series: Tivoli Continuous Data Protection for Files V3.1*, SG24-7423, and *Deployment Guide Series: IBM Tivoli Storage Manager Version 5.4*, SG24-7379.

Carlos Eduardo Abramo Pinto is an IT Specialist for Database Administration in IBM Global Services in Brazil, supporting IBM local and international customers. He is an IBM Certified IT Specialist, with more than 12 years of IT experience in a wide range of client and server platforms, including technical and system support of the Microsoft Windows® operating system, Oracle®, DB2®, and Microsoft SQL Server databases in UNIX®, Linux®, and Windows platforms. He is also specialized in Oracle Real Application Clusters implementation and support. Carlos is an IBM DB2 Certified Database Administrator on DB2 UDB V8.1 for Linux, UNIX, and Windows; an Oracle Certified Professional on Oracle 8i, 9i, and 10g databases; a Microsoft Certified IT Professional Database Administrator and Database Developer for Microsoft SQL Server 2005; a Microsoft Certified Database Administrator for Microsoft SQL Server 7 and 2000; and a Microsoft Certified System Engineer on Windows NT® 4 and 2000. He is an author of *Oracle to DB2 Conversion Guide for Linux, UNIX, and Windows*, SG24-7048.

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

Charlotte Brooks
Budi Darmawan
International Technical Support Organization

Del Hoobler
Mark Yakushev
Tivoli Storage Manager development

Thanks to the authors of the previous editions of this book.

- Authors of the first edition, *Using Tivoli Data Protection for Microsoft SQL Server*, SG24-6148, published in May 2001, were:

  Pat Randall
  Ivanka Kabranova
  Jan Sternberg
  Marcus Thordal

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

Summary of changes

This section describes the technical changes made in this edition of this IBM Redbooks publication and in previous editions. This edition may also include minor corrections and editorial changes that are not identified.

Summary of Changes
for SG24-6148-01
for *Backing up Microsoft SQL Server with IBM Tivoli Storage Manager*
as created or updated on June 27, 2008.

June 2008, Second Edition

This book provides a new description of Tivoli Storage Manager for Databases and Tivoli Data Protection for SQL Server at the current level of these products. It replaces the previous book *Using Tivoli Data Protection for Microsoft SQL Server*, SG24-6148.

1

Introduction

In this chapter we provide an overview of IBM Tivoli Storage Manager for Databases: Data Protection for SQL on Microsoft Windows, as well as associated technologies such as the Volume Shadow Copy Services (VSS), Virtual Disk Service (VDS), and snapshot techniques.

By integrating VSS-based snapshot capabilities with IBM Tivoli Storage Manager and its data-protection component for Microsoft SQL Server, IBM Tivoli Storage Manager for Copy Services provides enhanced backup and recovery features. These features are integrated with existing Microsoft SQL backup and restore capabilities.

The following topics are discussed:

- 1.1, "Tivoli Storage Manager overview" on page 2
- 1.2, "Snapshots" on page 10
- 1.3, "Volume Shadow Copy Services" on page 13
- 1.4, "Microsoft Virtual Disk Service" on page 20
- 1.5, "VSS Service with Tivoli Storage Manager" on page 21
- 1.6, "Integration of Data Protection for SQL Server and SQL Server" on page 22

1.1 Tivoli Storage Manager overview

IBM Tivoli Storage Manager is a powerful storage-management software suite that addresses the challenges of complex storage management in distributed heterogeneous environments. It protects and manages a broad range of data, from workstations, to corporate environments, to heterogeneous platform coverage for 13 different operating system environments. The heterogeneous platform coverage is scalable from PC servers to UNIX and mid-range servers, to z/OS® mainframe servers. It is the premier choice for complete storage management in mixed platform environments.

IBM Tivoli Storage Manager protects an organization's data against failures and other errors by storing backup and archive copies of data in offline storage.

IBM Tivoli Storage Manager provides:

- Centralized Web-based management
- Fully automated data protection
- Efficient automated data protection
- High-speed automated server recovery
- Support for over 500 devices (including disk, tape, and optical)
- Smart data-movement and storage techniques and comprehensive policy-based automation, which work together to minimize data-protection administration costs and the degree of impact on both computers and networks
- Cost and address-compliance management with regulatory data-retention requirements
- Optional modules enabling business-critical applications that must run 24x7x365 to protect their data without interruption

IBM Tivoli Storage Manager enables you to protect your organization's data from failures and other errors by storing backup, archive, space management, and bare-metal restore data, as well as compliance and disaster data in a hierarchy of offline storage. IBM Tivoli Storage Manager is available in three editions; Express, Basic Edition, and Extended Edition, and other optional modules are available that enhance the backup solution.

Appendix A, "Tivoli Storage Manager family of products" on page 245 provides a brief description of the IBM Tivoli Storage Manager family products. Detailed information about Tivoli Storage Manager and other additional products can be found in *IBM Tivoli Storage Management Concepts*, SG24-4877.

Figure 1-1 shows the Tivoli Storage Manager family of products.

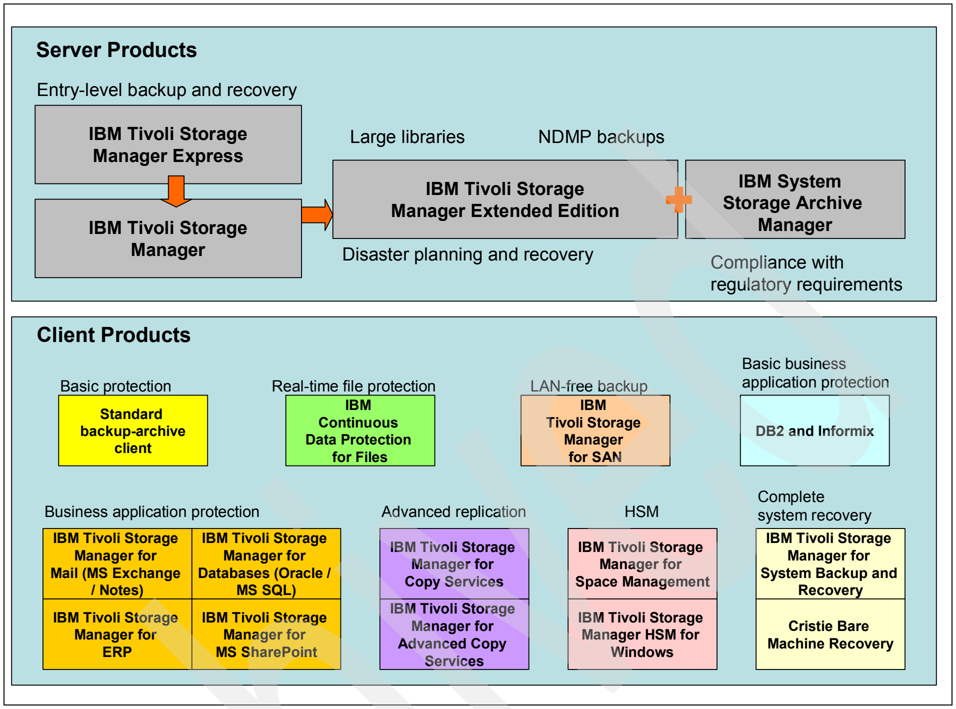

Figure 1-1 IBM Tivoli Storage Manager product family

You can use the IBM Tivoli Storage Manager product family to perform online, consistent, and centralized backups of your Microsoft SQL Server database, avoiding downtime, protecting your vital enterprise data infrastructure, and minimizing operation costs.

Today, in addition to maintaining the availability of applications, it is necessary to meet the requirements of zero-impact backups and instant recovery. To take care of these demands on your Microsoft SQL Server environment, you can integrate IBM Tivoli Data Protection for SQL Server and IBM Tivoli Storage Manager for Copy Services, both products in the IBM Tivoli Storage Manager family.

1.1.1 IBM Tivoli Storage Manager components

The IBM Tivoli Storage Manager server component is installed on the computer that manages storage devices. IBM Tivoli Storage Manager provides the following functions:

- Data management
- Storage device and media management
- Reporting and monitoring functions
- System security

The IBM Tivoli Storage Manager server application is supported by a relational database specifically designed to manage a data-storage environment. The server database operates transparently, requiring minimal administrative oversight. The server relies on the database to maintain an inventory of metadata associated with stored data objects. The database is not used to storage actual client data, which is maintained in server-managed storage. Server operations are configured, controlled, and monitored using graphical or command-line interfaces. Because some tasks can be performed several different ways, the interface you use depends on the type of task and your preferences. Support for SQL SELECT statements and ODBC data transfer is also available for advanced database management and reporting. Figure 1-2, shows the IBM Tivoli Storage Manager components.

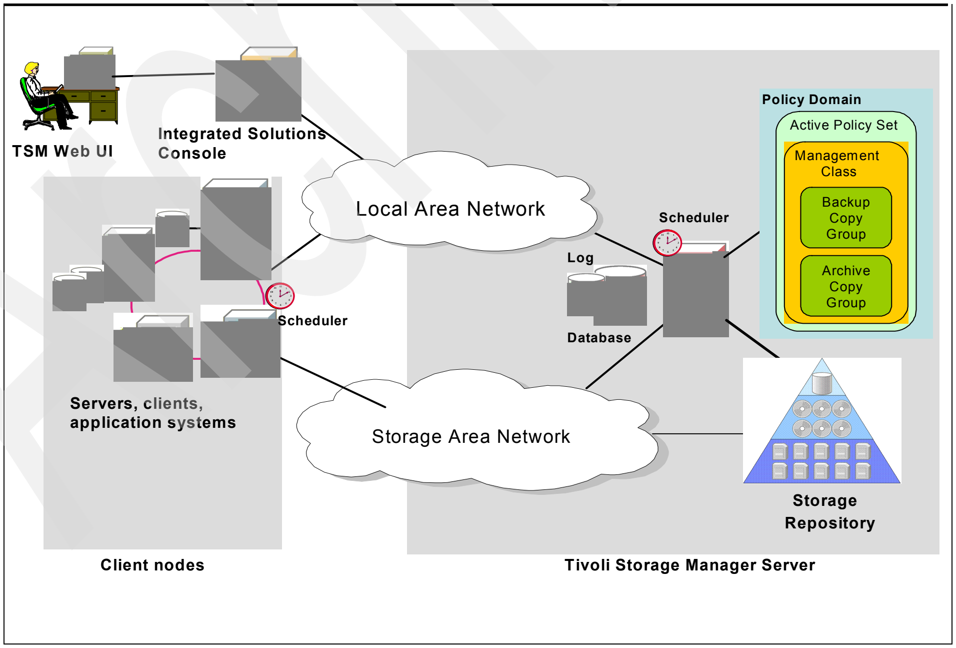

Figure 1-2 IBM Tivoli Storage Manager architecture

IBM Tivoli Storage Manager client overview

The IBM Tivoli Storage Manager client component sends data to, and retrieves data from, an IBM Tivoli Storage Manager server. The IBM Tivoli Storage Manager client must be installed on every machine that transfers data to server-managed storage. The IBM Tivoli Storage Manager server uses a unique node name to identify each IBM Tivoli Storage Manager client instance. A password can be used to authenticate communications between the IBM Tivoli Storage Manager client and server. Data can be recovered to the same client machine that initially transferred it or to another client with a compatible file system format.

The IBM Tivoli Storage Manager client basically consists of a software component and a customization file. The customization file, called the *client options file*, specifies client/server communication parameters and other IBM Tivoli Storage Manager client settings. Client communications parameters must agree with those specified in the server options file. The client options file is located in the client directory and can be modified using a text editor. The client graphical interface also provides a wizard for editing this file. IBM Tivoli Storage Manager provides the following types of clients:

- Backup-archive client

  The backup-archive client provides standard IBM Tivoli Storage Manager client functions, which include four operations: backup, restore, archive, and retrieve. These operations can be performed manually from the client machine or remotely using a Web-based interface. Backup and archive operations can also be scheduled to run automatically.

- Data-protection client

  The data-protection client, also called an *application client*, enables the backup and restoration of data used by various business applications. Data protection receives backup and restore requests from the business application and translates them for IBM Tivoli Storage Manager server processing. Backup and restore processing can be done while the business application is online.

- Space Manager client

  The Tivoli Space Manager client, also called the Hierarchical Storage Manager (HSM), transparently migrates data from the client hard drive to IBM Tivoli Storage Manager server-managed storage. When the migrated data is accessed through the client file system, it is transparently recalled back to the local disk. The migration and management of files is controlled by policy defined by the IBM Tivoli Storage Manager server. Users can also explicitly migrate and recall data. HSM client functions are fully integrated with IBM Tivoli Storage Manager operational backup and client functions.

- Application programming Interface client

  The application programming interface (API) client enables you to create custom IBM Tivoli Storage Manager implementations. The API client can be used to integrate business applications, such as databases or groupware, in an IBM Tivoli Storage Manager environment.

1.1.2 IBM Tivoli Storage Manager for Copy Services overview

IBM Tivoli Storage Manager for Copy Services helps you back up and restore critical data so that it remains available 24x7.

Implement high-efficiency backup and restore processes for your critical business applications with little impact on production performance. IBM Tivoli Storage Manager for Copy Services provides:

- Enhanced backup and recovery features that are integrated with existing Microsoft SQL Server backup and restore capabilities
- Fast backup with minimal impact on your production SQL server with a variety of snapshot providers
- Near instant restoration of Microsoft SQL Server databases from a shadow copy image to the production volumes
- Policy-based management of multiple local backup versions so that recovery for multiple versions is easy
- Improved availability and performance of production database servers with offloaded movement
- Integrated snapshot capabilities with IBM Tivoli Storage Manager and its data-protection component for Microsoft SQL Server
- Support for Microsoft Windows

Two installable modules - Microsoft SQL VSS Integration Module and Hardware Devices Snapshot™ Integration Module - are included in the IBM Tivoli Storage Manager for Copy Services package. Once installed, these modules enable certain menu options in the Tivoli Data Protection for SQL Server GUI, which are otherwise unavailable.

Microsoft SQL Server VSS Integration Module

This component is used with IBM Tivoli Storage Manager for Databases: Data Protection for SQL and enables the use of Microsoft VSS technology to produce an online snapshot of the SQL Server data stored on local shadow volumes or on IBM Tivoli Storage Manager server storage. A license file (ascsql.lic) is installed in the installation directory of Data Protection for SQL Server, which enables you to use IBM Tivoli Storage Manager for Copy Services. This module is required for all VSS operations with Data Protection for SQL Server.

Hardware Devices Snapshot Integration Module

This component is used with IBM Tivoli Storage Manager for Databases: Data Protection for SQL Server. It contains two .dll files (pisnaphdw.dll and pihdw.dll) and two license files (aschdw.lic and acssnp.lic), which are installed in the installation directory of the IBM Tivoli Storage Manager backup-archive client. This module is only required to perform a VSS Instant Restore.

1.1.3 Data Protection for SQL Server

Tivoli Data Protection for SQL Server enables you to perform online backups and restores of Microsoft SQL Server databases to IBM Tivoli Storage Manager Server storage using either command-line or graphical interfaces on Windows 2000 and Windows 2003, in a standalone or clustered environment.

Tivoli Data Protection for SQL Server helps protect and manage Microsoft SQL Server data by making it easy to:

- Back up any SQL Server database to any Tivoli Storage Manager server.
- Perform full and transaction log backups and restores of SQL Server databases.
- Perform backups with an expanded range of options such as differential, file, and group operations.
- Perform operations from multiple Microsoft SQL Server instances on the same machine as Data Protection for SQL Server. You can access only one SQL server per execution of Data Protection for SQL Server from either the command line or GUI.
- Schedule automated backups.
- Perform expanded restore operations on backup objects such as relocating, restoring to named marks, and partially restoring full backups.
- Restore database backups to a different SQL server. Data Protection for SQL Server can restore database backups that were performed on either 32-bit or 64-bit versions of Microsoft SQL Server. Refer to Microsoft documentation on which combinations are supported by Microsoft.
- Retain with a backup the information needed to re-create or move SQL Server databases or files - such as sort order, code page, and Unicode information - and filegroup and logical and physical file names. The meta object information is retained on the IBM Tivoli Storage Manager separately from the backup data objects.

- Inactivate all active Legacy objects, all objects of a particular backup type, or specific objects.Inactivate backup objects older than a specified number of days.
- Set automatic expiration of backup objects based on version limit and retention period.
- Query any local SQL server or any connected Tivoli Storage Manager server for database, status, and configuration information.
- Monitor results through the Data Protection for SQL Server activity log and automatically prune the activity log.
- Set Tivoli Storage Manager client connection configuration to IBM Tivoli Storage Manager servers.
- Set IBM Tivoli Storage Manager security and performance options.
- Participate in Microsoft Cluster Server and fail-over clusters and VCS failover clusters.
- Set Tivoli Storage Manager security and performance options.
- Apply fail-over clustering (for maintenance or for restoring the master database) without unclustering.
- Support globalization efforts.

Tivoli Data Protection for SQL Server operations use the IBM Tivoli Storage Manager API to communicate with the IBM Tivoli Storage Manager server and use the Microsoft SQL Server API to communicate with the SQL server.

When IBM Tivoli Storage Manager for Copy Services is installed together with Tivoli Data Protection for SQL Server, you can also perform online snapshot backups to local shadow volumes, using VSS. These snapshot backups can be retained on local shadow volumes and can be backed up to IBM Tivoli Storage Manager server storage.

To reduce the overhead of backup operations on the SQL server, you can choose to perform the backup to IBM Tivoli Storage Manager using another server with access to the shadow volumes either from local snapshot volumes or from IBM Tivoli Storage Manager server storage.

What’s new in Tivoli Data Protection for SQL Server Version 5.5

The following features and functions have been added to Data Protection for SQL Server Version 5.5:

- VSS backup

  Back up Microsoft SQL Server 2000 and SQL Server 2005 databases (running on Windows Server® 2003) using Microsoft Volume Shadow Copy Services (VSS) technology.

  A VSS backup uses Microsoft VSS technology to produce online snapshot (point-in-time consistent copy) of SQL Server data that can be stored on local shadow volumes or on Tivoli Storage Manager server storage.

- Microsoft SQL version support

  Data Protection for SQL Server supports Microsoft SQL 2000 and 2005 on Windows 32-bit and 64-bit environments.

- Veritas Cluster Server (VCS) support

  Data Protection for SQL Server supports Microsoft SQL Server running in a VCS environment. For Windows 2003, Data Protection for SQL Server uses the Active Directory® to support fail-over clustering.

- Offloaded backup

  Perform a VSS backup to an IBM Tivoli Storage Manager server using an alternate machine instead of a production machine.

- Restore VSS

  Restore VSS backups residing on IBM Tivoli Storage Manager server storage to their original location.

- VSS Fast Restore

  Restore VSS backups residing on local shadow volumes using file-level copy mechanisms.

- VSS Instant Restore

  Restore VSS backups residing on local shadow volumes using hardware-assisted volume-level copy mechanisms.

- Server policy

  Using IBM Tivoli Storage Manager policy-based management, conduct VSS snapshot backups.

1.2 Snapshots

Snapshot is a common industry term that means the ability to record data stored on a storage device at any given moment and preserve that snapshot as a way to perform backup, restore, data mining, and even testing.

1.2.1 Snapshot overview

A snapshot creates a point-in-time copy of data on a disk volume. Typically, a snapshot copy is created instantly and made available for use by other applications such as data protection, data replication, data analysis, and reporting. The original copy of the data continues to be available to the applications without interruption, while the snapshot copy is used to perform other functions on the data.

Snapshots provide an excellent means of data protection, and their use is increasing because of the way the technology addresses many issues that businesses face. Snapshots can do the following:

- Enable better application availability, faster recovery, and easier backup management of large volumes of data
- Reduce exposure to data loss while virtually eliminating backup windows

Snapshots come in many different flavors depending on how a particular vendor chooses to implement the technique. A snapshot method may be hardware specific (that is, implemented for a particular type of storage system), or it may be implemented in software, so that it can be used with different types of storage hardware. In the following sections, we describe principal implementations that are commonly found and provide examples.

1.2.2 Copy-on-write

In the copy-on-write method, a snapshot of a storage volume is created using predesignated space for the snapshot. When the snapshot is first created, only the metadata about where the original data is stored is copied. No physical copy of the data is made at the time the snapshot is created. Therefore, the creation of the snapshot is almost instantaneous.

The snapshot copy then tracks the changing blocks on the original volume as writes to the original volume are performed. The original data being written to is copied to the designated volume that is set aside for the snapshot before original data is overwritten; hence, the name *copy-on-write*.

Before a source block can be written to, the copy-on-write method copies the original data block to the snapshot storage. This keeps the snapshot data consistent with the exact time the snapshot was taken. Read requests to the snapshot volume of unchanged data blocks are redirected to the original volume, while read requests to data blocks that have been changed are directed to the “copied” blocks in the snapshot. The snapshot contains the metadata describing the data blocks that have changed since the snapshot was first created. Original data blocks are copied only once into the snapshot storage, when the first write request is received.

A copy-on-write snapshot may initially impact performance on the original (source) volume while it exists, because write requests to the original volume must wait while the original data is being “copied out” to the snapshot. The read requests to the snapshot are satisfied from the original volumes if data being read has not changed. Additionally, the snapshot requires that the original copy of the data is still valid.

This method is highly space efficient because the storage required to create a snapshot is minimal, holding only the data that is changing.

IBM FlashCopy® (NOCOPY), AIX JFS2 snapshot, IBM General Parallel File System™ snapshot, Linux Logical Volume Manager, and IBM Tivoli Storage Manager Logical Volume Snapshot Agent (LVSA) are all based on copy-on-write.

1.2.3 Redirect-on-write

The redirect-on-write method is quite similar to copy-on-write, without the double write penalty. With redirect-on-write, new writes to the original volume are redirected to another location set aside for snapshot.

The advantage of redirecting the write is that only one write takes place, while with copy-on-write, two writes occur (one to copy the original data to the storage space, and the other to copy the changed data). However, with redirect-on-write, the original copy contains the point-in-time data (that is, snapshot), and the changed data resides on the snapshot storage. When a snapshot is deleted, the data from the snapshot storage must be reconciled back into the original volume.

Furthermore, as multiple snapshots are created, access to the original data, tracking of the data in snapshots and on the original volume, and reconciliation upon snapshot deletion is further complicated. The snapshot relies on the presence of the original copy of the data, and the original data set can quickly become fragmented. IBM N series and the NetApp® Filer snapshot implementation are based on redirect-on-write.

1.2.4 Split mirror

Split mirror creates a physical clone of the storage entity (such as the file system, volume, or logical unit number - LUN - for which the snapshot is being created) on another entity of the same kind and the exact same size. The entire contents of the original volume are copied to a separate volume. Clone copies are highly available because they are exact duplicates of the original volume that reside on a separate storage space. However, due to the data copy, such snapshots cannot be created instantaneously.

Alternatively, a clone can also be made available instantaneously by splitting a pre-existing mirror of the volume in two, with the result that the original volume has one fewer synchronized mirror. This snapshot method requires as much storage space as the original data for each snapshot, and has the performance overhead of writing synchronously to the mirror copy.

1.2.5 Copy-on-write with background copy

Some vendors offer an implementation where a full copy of the snapshot data is created using copy-on-write and a background process that copies data from the original location to snapshot storage space. This approach combines the benefits of the copy-on-write and split mirror methods and is seen in IBM FlashCopy and EMC TimeFinder/Clone.

It uses copy-on-write to create an instant snapshot and then optionally starts a background copy process to perform a block-level copy of the data from the original volume (source volume) to the snapshot storage (target volume) in order to create an additional mirror of the original volume.

1.2.6 IBM FlashCopy

By doing a FlashCopy, a relationship is established between a source and a target. The two form a FlashCopy pair.

As a result of the FlashCopy, either all physical blocks from the source volumes are copied (full copy) or, when using the nocopy option, only those parts that change in the source data since the FlashCopy has been established. Currently, the target volume must be the same size or bigger that the source volume whenever FlashCopy is used to flash a whole volume.

Typically, the data for large applications such as databases is spread across several volumes, and the volumes for large applications should all be FlashCopied at exactly the same point in time. FlashCopy offers Consistency

Groups, which enable multiple volumes to be FlashCopied at exactly the same instance.

Incremental FlashCopy tracks changes made to the source and target volumes when the FlashCopy relationships are established. This provides the capability to refresh a LUN or volume to the source or target's point-in-time content using only the changed data. The refresh can occur in either direction, and it offers improved flexibility and faster FlashCopy completion times.

This incremental FlashCopy option can be used to efficiently create frequent and faster backups and restore without the penalty of having to copy the entire content of the volume (see Figure 1-3).

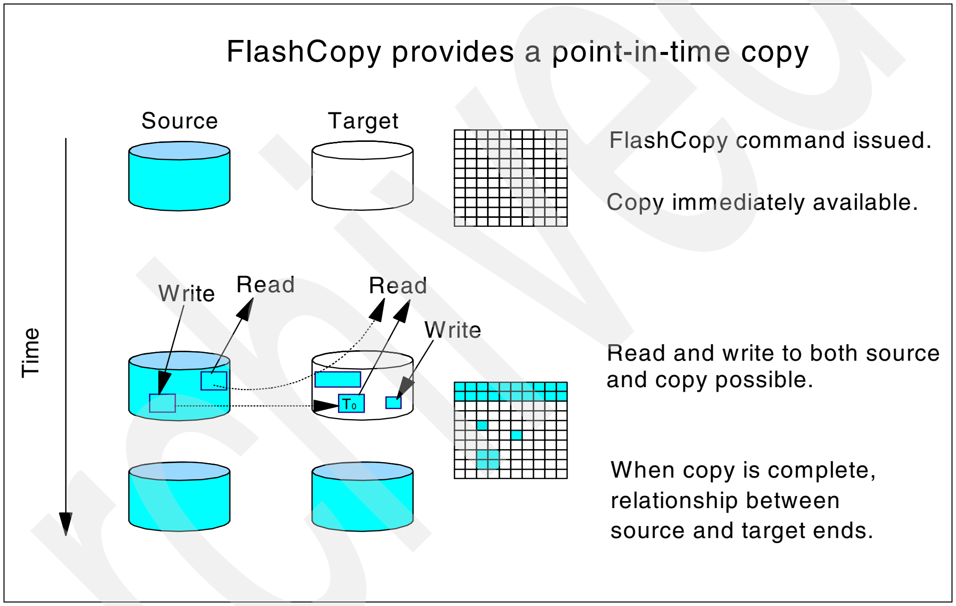

Figure 1-3 FlashCopy concepts

1.3 Volume Shadow Copy Services

The Volume Shadow Copy Services (VSS) provided with Microsoft Windows Server 2003 is an enhanced storage-management feature. VSS provides a framework and an API that enables the creation of consistent point-in-time copies of data known as *shadow copies*. VSS enables the interoperability of third-party storage-management programs, business programs, and hardware providers to create and manage shadow copies.

Several features in Microsoft Windows Server 2003 already use the Volume Shadow Copy Service, such as Shadow Copies for Shared Folders and Backup.

1.3.1 Methods for creating shadow copies

You can create shadow copies using two distinct snapshot methods:

- Full copy
- Differential copy (copy-on-write)

A full copy is usually achieved using a hardware provider (see “Provider” on page 17).

1.3.2 The VSS model

VSS is designed to address problems associated with traditional backup methods (such as inaccessible files and inconsistent file states) and minimize interruptions to production servers during backup, as described in the sections that follow.

Shadow mechanism

The following description provides insight into the mechanism of VSS:

- VSS provides fast volume capture of the state of a disk at a particular point in time (a shadow copy of the volume).
- This volume copy exists side by side with the live volume and contains copies of all files on disk.
- The volume is effectively saved and available as a separate device.
- VSS provides a stable source for backup operations because it is read-only, while allowing ongoing applications to update the original volumes.

Coordination with applications for consistent file state

VSS integrates with participating applications (such as Microsoft SQL Server) by providing COM-based events. This means that the application itself determines the system state for backup, restore, and shadow copy (volume capture) operations, and communicates the state to VSS. An application that is writing to the disk is also responsible for bringing all associated files into a consistent state before creating the shadow copy.

Minimizing application downtime

Creating a shadow copy typically takes approximately several seconds or minutes, depending on the VSS provider. The application is paused only between the so-called Freeze and Thaw VSS events.

Unified interface to VSS

VSS abstracts the shadow copy mechanisms within a common API. This means that any backup application (requestor) and any writer should be able to run on any disk storage system that supports the VSS interface. It also provides the opportunity for individual hardware vendors to add and manage unique features for their own providers.

Multivolume backup

A shadow copy set is a collection of shadow copies. VSS supports these sets across multiple types of disk volumes from different vendors. All shadow copies in a shadow copy set are created with the same time stamp and present the same disk state.

Native shadow copy support

Shadow copy support is available through VSS as a native part of the Microsoft Windows operating system (Windows XP and Windows 2003). Note, however, that Tivoli Storage Manager for Copy Services is supported only on Windows 2003, not Windows XP. VSS shadow copies can be made on any disk attached to the system, as long as at least one NTFS disk is present on the system.

1.3.3 VSS architecture

The VSS framework coordinates communication between VSS requestors, VSS writers, and VSS providers. Figure 1-4 illustrates the VSS architecture.

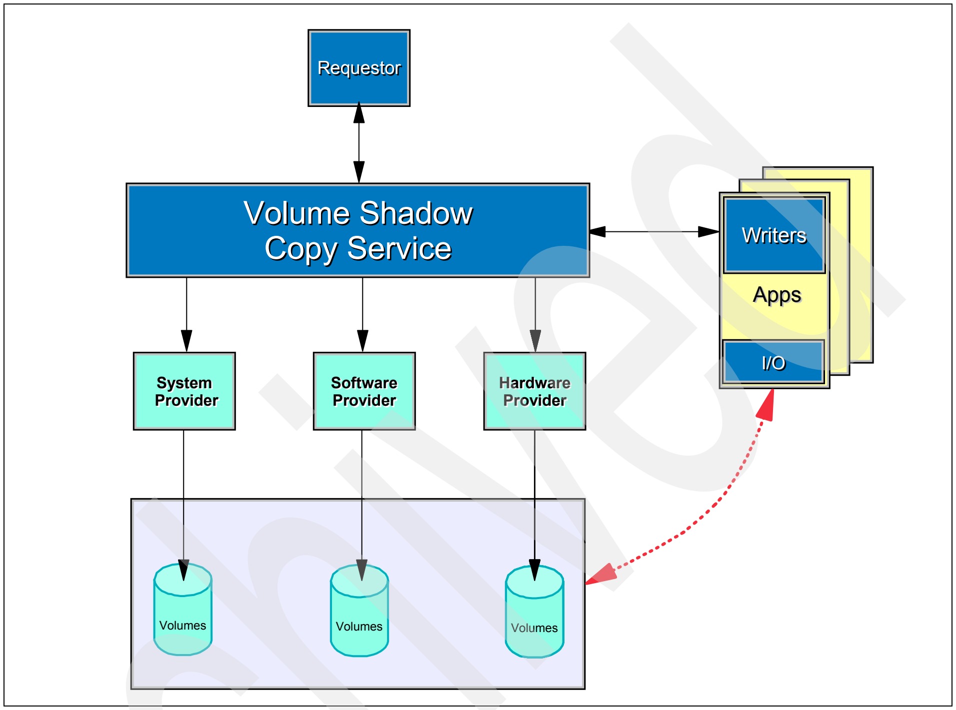

Figure 1-4 VSS architecture

Requestor

The requestor is a management application that invokes VSS to create and manage shadow copy sets of one or more volumes. This role is typically used to implement other functionalities such as backup, restore, and disk mirroring operations. A backup application is an example of a requestor.

Writer

The writer is an application or Windows service that manages its I/O operations with VSS shadow copy and shadow copy-related operations, ensuring the data contained on the shadow copied volume is in a consistent state. Microsoft SQL Server 2005 is an example of a writer.

Provider

The VSS provider is a component that creates and maintains the shadow copies. A VSS provider is provided either by a storage vendor for its particular storage systems (hardware provider) or by a software vendor (software provider). A special case of a software provider is the Microsoft Windows system provider, which is implemented in Windows 2003. This is known as a *system software provider*.

When using a hardware provider, the snapshot is performed at the storage system controller level - for example, using FlashCopy on IBM storage systems such as the DS6000™, DS8000™, SVC, or SnapDrive® on NetApp network-attached storage (NAS) systems. Furthermore, if this provider supports transportable shadow copies, the backup operations can be performed by another machine (offloaded backup).

A software provider, including the Windows native system software provider, can be used with storage systems that do not have their own hardware provider.

If you have a hardware provider available for your disk system, we recommend that you use this, because the work of actually making the snapshot is performed by the disk system itself. A software provider (including the system software provider), by comparison, must do all the work in software on the actual SQL server. The Windows system software provider uses copy-on-write, and therefore, using a software provider requires significant performance overhead.

The Volume Shadow Copy Services selects the provider using the following order:

- Hardware provider
- Software provider
- System software provider

That is, VSS looks first for a hardware provider that supports the disk system and uses it. If no hardware provider is found, a software provider is used, if available. If no other provider is available, the Microsoft system software provider is used.

The requester can override this order if desired.

Source volume

A source volume is a disk volume containing data to be shadow copied.

Storage or target volume

A storage or target volume is a disk volume holding data that has been shadow copied from a source volume. Some VSS provider snapshot implementations require that the target volume be the same size as the source volume, and some do not.

1.3.4 Shadow copy creation

Figure 1-5 illustrates the steps in creating a shadow copy.

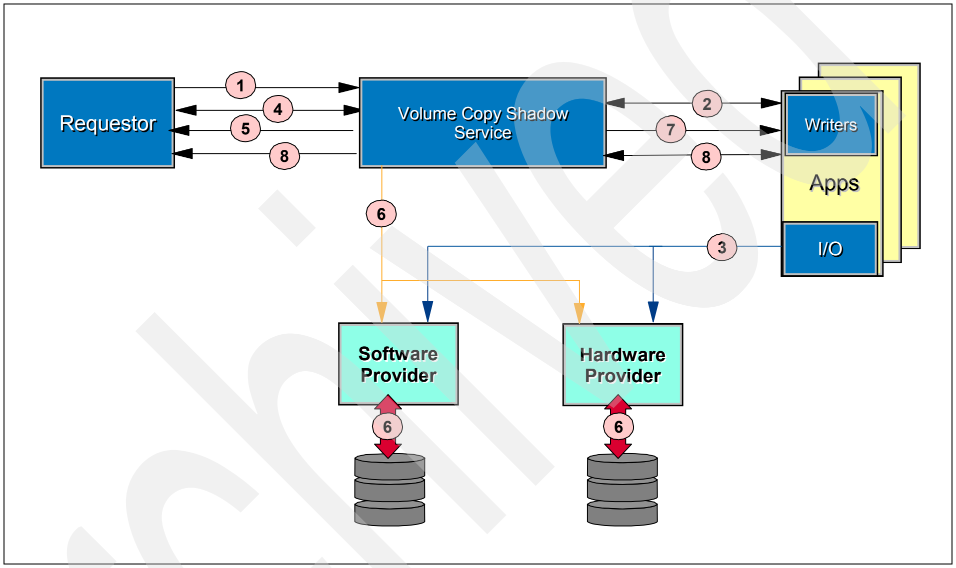

Figure 1-5 Shadow copy creation process

The process is as follows:

1. The requestor asks the VSS to list the writers, gather the writer metadata, and prepare to create the shadow copy.
2. The writer creates an XML description of the backup components to the VSS and defines the restore method. The VSS notifies the application-specific writer to prepare its data for making a shadow copy.
3. The writer prepares the data as appropriate, such as completing all open transactions, rolling transaction logs, and flushing caches. When the data is ready for shadow copy creation, the writer notifies the VSS.
4. The VSS initiates the “commit” shadow copy phase.
5. The VSS tells the writer to quiesce its data and temporarily freeze requestor (application) I/O write requests (I/O read requests are still possible) for the

several seconds required to create the shadow copy of the volume(s). The VSS flushes the file system buffer and then freezes the file system to ensure that file system metadata is written and that the data is written in a consistent order.

6. The VSS tells the provider to create the shadow copy.
7. The VSS thaws the file system. After the shadow copy is created, the VSS signals the writer that it can now complete all queued write I/Os, because the temporary inactive phase is over.
8. The VSS queries the writers to confirm that write I/Os were successfully suspended while the shadow copy was created. If the writes were not successfully suspended (meaning that the shadow copy data is potentially inconsistent), the shadow copy is deleted, and the requestor is notified. The requestor can retry the process (go back to step 1) or notify the administrator to retry at a later time. If the copy is successful, the VSS gives the location information for the shadow copy back to the requestor.

1.3.5 Shadow copy types

Three types of VSS shadow copies can be made:

- Persistent shadow copy

  A persistent shadow copy survives reboots. Persistent shadow copies cannot be auto-released by VSS.

- Non-persistent shadow copy

  A non-persistent shadow copy, also known as an *auto-release shadow copy*, is deleted after the backup operation is complete. The default for shadow copies is non-persistent.

- Transportable shadow copy

  A transportable shadow copy can be moved from one server to another. When a shadow copy is transported, the target volume(s) are dismounted from the server that initiated the shadow copy and mounted on another server. Transportable shadow copies require the use of a VSS hardware provider and enable the offloaded backup function.

1.4 Microsoft Virtual Disk Service

Microsoft Virtual Disk Service (VDS) was introduced in Microsoft Windows Server 2003 to provide a single interface for management and configuration of multivendor direct attached and SAN-based storage.

VDS is a set of APIs that provides a single interface for multivendor storage management. Each hardware vendor develops its own VDS hardware provider to translate the general-purpose VDS APIs into their specific hardware instructions.

VDS is part of Microsoft storage services - the other two components are Remote Storage and Removable Storage.

VDS uses two sets of providers to manage storage devices:

- The built-in VDS software providers that manage disks and volumes at the operating system level.
- Hardware providers supplied by the hardware vendor that manage its specific hardware.

Virtual Disk Service is used for managing LUNs on hardware storage devices, managing disks and volumes, and managing end-to-end storage operations.

Figure 1-6 illustrates the Virtual Disk Service architecture.

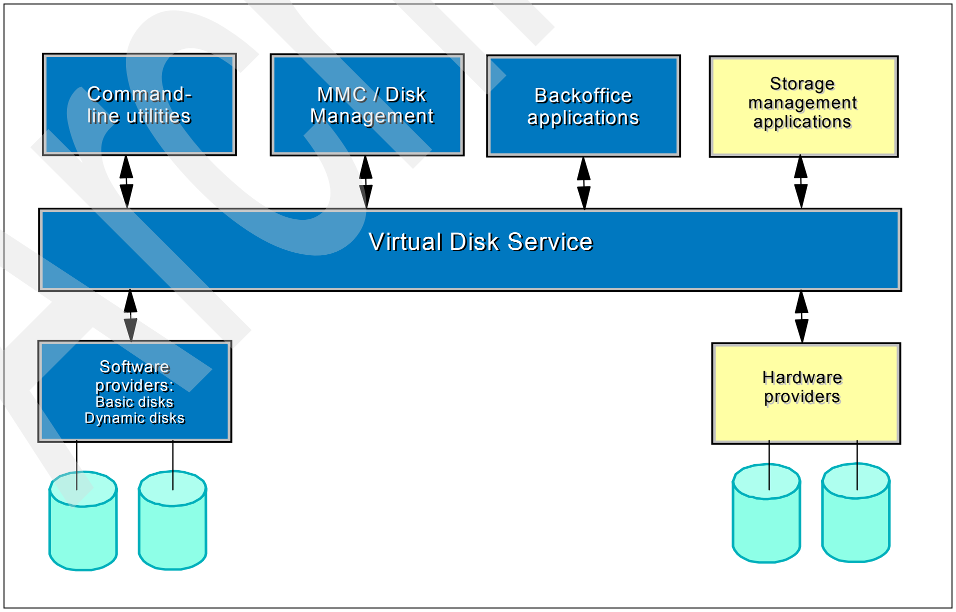

Figure 1-6 VDS architecture

Tivoli Storage Manager for Copy Services integrates with VSS and any supported disk storage system to easily exploit the snapshot on the hardware side and manage the LUN allocation.

1.5 VSS Service with Tivoli Storage Manager

Tivoli Storage Manager can perform VSS backups of Microsoft SQL Server databases using Tivoli Storage Manager for Databases and Tivoli Data Protection for SQL Server together with Tivoli Storage Manager for Copy Services and the Tivoli Storage Manager backup-archive client.We refer to this combined solution generically as Data Protection for SQL, with the understanding that a VSS backup requires the additional module Tivoli Storage Manager for Copy Services.

The VSS service manages and directs three VSS software applications that are used during VSS operations:

- VSS writer

  The VSS writer is the SQL server. It is installed with the Microsoft SQL Server 2005 software and requires no configuration.

- VSS requestor

  The VSS requestor is the IBM Tivoli Storage Manager backup-archive client. The requestor communicates with VSS to access Microsoft SQL Server data. Data Protection for SQL Server is the front end for VSS backups - that is, Data Protection for SQL Server is the user interface for initiating backup and restore operations. However it communicates with the backup-archive client as a VSS requestor to actually perform the backup and restore.

- VSS provider

  The VSS provider manages the volumes where Microsoft SQL Server data resides and performs the actual snapshot copy. You can use either a VSS software provider (including the Windows system provider) or a hardware provider with Data Protection for SQL. You must configure the provider according to the vendor’s specific instructions.

  Configuration requirements are based on the type of VSS provider used. Some VSS providers are more complex to set up initially, but subsequently they provide more powerful functionality and can also decrease the overhead on the SQL server.

Follow these guidelines when choosing which VSS provider meets the needs for a Microsoft SQL Server backup:

- If you are using the standard Windows system provider, little initial configuration is required. This is the quickest and simplest way to set up Data Protection for SQL Server for VSS backups. However, the copy-on-write snapshots are then maintained within the production SQL server, which imposes additional overhead.
- If you are using a VSS software provider, consult the documentation provided with your VSS software provider.
- If your SQL Server databases are configured on a disk storage subsystem and you plan to perform offloaded backups or full-copy snapshot backups, you must install a VSS hardware provider.
- VSS Instant Restores are supported only by IBM System Storage™ SAN Volume Controller, DS6000, and DS8000 storage subsystems, in association with the VSS hardware provider. Therefore, you must install and configure IBM TotalStorage Support for Microsoft Virtual Disk and Volume Shadow Copy Services as your VSS hardware provider to perform VSS Instant Restores.

1.6 Integration of Data Protection for SQL Server and SQL Server

In this section, we discuss how Data Protection for SQL Server integrates with Microsoft SQL Server, and the options offered for backing up and restoring SQL Server databases. Data Protection for SQL Server must be installed on the same server as the SQL server. If you are planning to have zero impact backup and instant restore, consider the installation of IBM Tivoli Storage Manager Copy Services on the same machine.

Data Protection for SQL Server has both GUI and command-line interfaces.

1.6.1 Data Protection for SQL Server backup methods

Two types of backups are available: Legacy backups and VSS backups.

Legacy backup

A Legacy backup is a specialized API backup that functions with the Microsoft SQL Server storage engine, as show in Figure 1-7. This is the type of backup provided by previous releases of Data Protection for SQL Server.

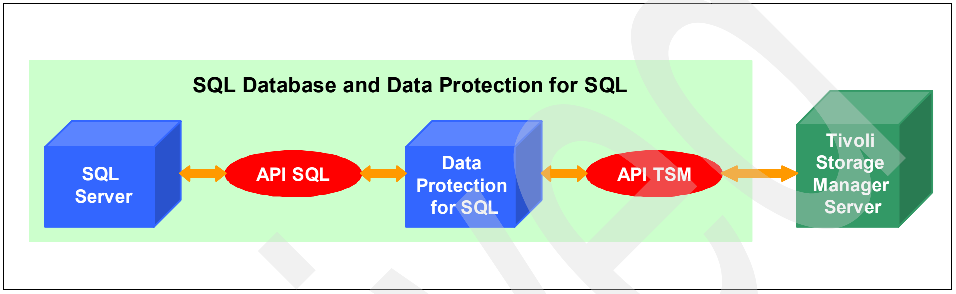

Figure 1-7 Data Protection for SQL Legacy backup communications

A Legacy backup creates a copy of all or part of a SQL Server database on Tivoli Storage Manager storage media. Data Protection for SQL Server provides selection mechanisms and the logic required to back up and restore SQL Server data.

When you initiate a Legacy backup operation, Data Protection for SQL executes the following steps:

1. Starts a session with the server using the IBM Tivoli Storage Manager API and information contained in a client options file.
2. Starts a session with the SQL server using an internal Microsoft interface, known as SQL-DMO (Distributed Management Objects).
3. Instructs the SQL server using the Microsoft SQL-VDI (Virtual Device Interface) to begin a backup of the selected database objects.
4. Receives data from the SQL server and sends it to the Tivoli Storage Manager server.
5. Ends the Tivoli Storage Manager server and Microsoft SQL Server sessions.

Note: When a backup is performed, Data Protection for SQL Server records information about the Microsoft SQL Server and database. This information is available for query and restore operations. The information about the names and sizes of the database filegroups and files is stored along with the database data, as a sub-object. This sub-object is referred to as *metadata*. You need this sub-object when you require information about individual database filegroups and files.

The following characteristics are true of Legacy backups:

- Full, copy, incremental, differential, and database copy types are supported.
- Backup granularity is at the database level.
- Backups are stored on IBM Tivoli Storage Manager server storage.
- Backups are managed through IBM Tivoli Storage Manager server policy.
- Backups can be performed in a Microsoft Cluster Server (MSCS) environment.
- Backups provide Microsoft SQL Server database integrity check functionality.

VSS backups

A VSS backup uses Microsoft Volume Shadow Copy Service technology to produce an online snapshot (point-in-time consistent copy) of SQL Server data that can be stored on local shadow volumes or on Tivoli Storage Manager server storage. During a VSS backup, the SQL server is not in “backup mode” for an extended period of time because the length of time required to perform the snapshot is usually measured in seconds and not hours. In addition, a VSS backup makes it possible to take a snapshot of large amounts of data at the same time because the snapshot works at the volume level. VSS backups require IBM Tivoli Storage Manager for Copy Services to be installed, in addition to Data Protection for SQL and the IBM Tivoli Storage Manager backup-archive client. You can optionally use an alternate machine to move data to the IBM Tivoli Storage Manager server, an offloaded backup.

The VSS architecture is depicted in Figure 1-8.

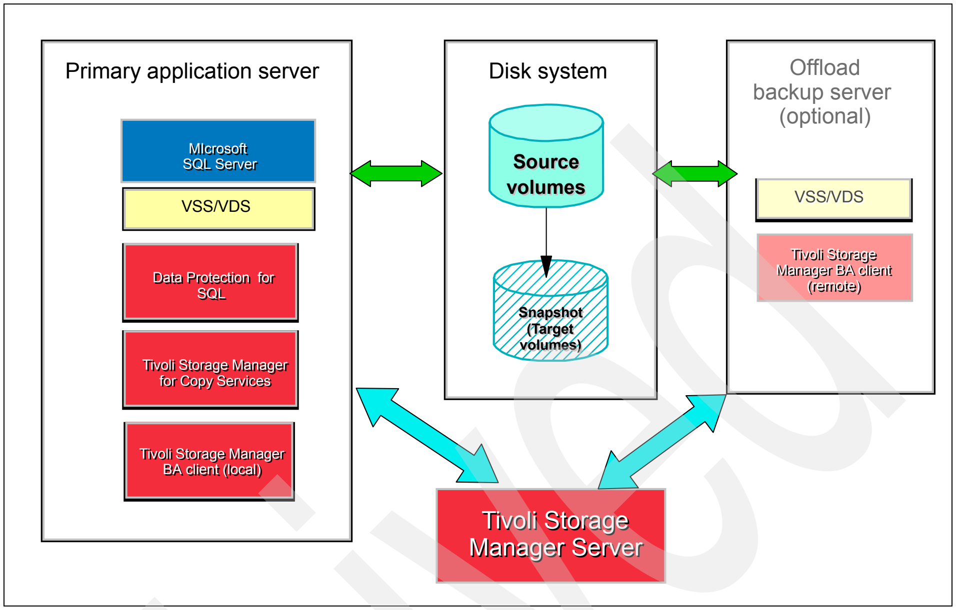

Figure 1-8 General VSS architecture

Optionally, VSS backups can be stored locally on VSS shadow volumes that are directly accessible by the SQL system, as long as sufficient space is available for the snapshot. Local VSS shadow backups are fast because data is not transferred to Tivoli Storage Manager server storage. Restoring these backups is also fast because the SQL Server data is not transferred from Tivoli Storage Manager server storage over the network.

After the snapshot is complete, it can be accessed directly through standard operating system functions or other applications - for example, you can back up and manage the VSS snapshot on an external storage manager (for example, IBM Tivoli Storage Manager). When this function is selected and after the snapshot is made, IBM Tivoli Storage Manager is automatically invoked to store the snapshot.

In this way, we can establish two uses for VSS backup. First, VSS backup is a backup in itself, so that multiple shadow copy generations can potentially be kept online for rapid restore (backup to local). Second, VSS backup is a means for providing extra backups to an external media (backing up to IBM Tivoli Storage Manager), so that the database can be restored even if the disk system containing the original database and the shadow copies fails. When a Data Protection for SQL backup is started, you must specify the backup destination: to local, IBM Tivoli Storage Manager, or both.

Note: VSS backups are available only on Microsoft SQL Server 2005 on Windows Server 2003.

The following characteristics are true of VSS backups:

- Full VSS snapshot backups and full VSS offloaded snapshot backups are supported. Incremental, differential, and transaction log backup types are not supported. (See 1.6.2, “Microsoft SQL Server backup types” on page 26 for definitions of the types of backups.)
- Backup granularity is at the database level only.
- Backups are managed through Tivoli Storage Manager policy.
- Backups can be stored on local shadow volumes, Tivoli Storage Manager server storage, or both locations.
- Different policy settings can be defined for each storage location and backup method.
- Backups to Tivoli Storage Manager server storage can be offloaded to an alternate machine, to reduce the workload on the production servers.
- Backups can be performed in a Microsoft Cluster Server (MSCS) or Veritas Cluster Server (VCS) environment.

1.6.2 Microsoft SQL Server backup types

Microsoft SQL Server supports a number of types of backup. Some of them are supported by the Tivoli Data Protection for SQL Server Legacy backup method; others are supported by the Data Protection for SQL Server Legacy and VSS backup methods, and others are not supported by Data Protection for SQL Server.

Microsoft SQL Server supports the following backup types:

- Full database backup

  A full database backup backs up an entire Microsoft SQL Server database and the portion of the transaction log necessary to provide a consistent database state. With both full and differential backups, the copy includes enough information from any associated transaction logs to make a backup consistent with itself. The portion of the log included contains only the transactions that occurred from the beginning of the backup until its completion. This backup type is supported by the Legacy and VSS backup methods.

Note: You do not have to do an actual full backup to constitute the equivalent of a full backup. Backing up all the groups or files in a database as well as its log is recognized as a full backup by the SQL server. A base backup may be full, group, file, or set backup.

- Differential backup

  A differential backup backs up only those data pages in a Microsoft SQL Server database changed since the last full backup, as well as a portion of the transaction log. This is equivalent to an incremental backup on the Tivoli Storage Manager backup-archive client. This backup type is supported by the Legacy backup method only.

- Log backup

  A log backup backs up only the contents of a Microsoft SQL Server database transaction log since the last successful log backup. Before doing the first log backup, you must have done a full backup or its equivalent first. Log backups normally follow full backups. The portion of the log included in full and differential backups is not equivalent to a log backup. Additionally, in full and differential backups, the log is not truncated as it is during a log backup. However, a log backup following a full or differential backup includes the same transactions as a full or differential. Log backups are not cumulative; they must be applied in turn against a base backup and in the correct order. This backup type is supported by the Legacy backup method only.

Note: A log backup in Microsoft SQL Server terms is not equivalent to an incremental backup in Tivoli Storage Manager terms.

- Tail-log backup

  A tail-log backup is a transaction log backup that includes the portion of the log that has not previously been backed up. The tail-log backup is commonly used when the database is damaged or becomes inaccessible, but the transaction log file is undamaged. This backup type is supported by Data Protection for SQL Server.

- File backup

  A file backup backs up only the contents of a specified Microsoft SQL Server logical file. This can ease the scheduling for backing up very large databases by enabling you to back up different sets of files during different scheduled backups. File, group, and set backups must be followed by a log backup, but a full backup is not required. This backup type is supported by the Legacy backup method only.

- Group backup

  A group backup backs up only the contents of a specified Microsoft SQL Server filegroup. This enables you to back up only the set of database tables and indexes within a specific group of files. This backup type is supported by the Legacy backup method only.

- Set backup

  A set backup backs up the contents of specified Microsoft SQL Server filegroups and files as a unit. This backup type is supported by the Legacy backup method only.

- Copy-only backup

  At times it is necessary to back up a Microsoft SQL Server database without affecting the sequence of conventional Microsoft SQL Server backups - for example, to transfer a database from production to development environments. To address this scenario, Microsoft SQL Server 2005 introduces the copy-only backup. A copy-only backup is a backup that does not affect the overall backup and recovery routines for the database. The two types of copy-only backups are:

  – Copy-only full backups - available in all recovery models

  – Copy-only log backups - available in full recovery and bulk-logged models

  A copy-only full backup cannot be used as a base or differential backup and does not affect differential backups. A copy-only log backup does not change the transaction log sequence; consequently it does not affect the database transaction log chain. A copy-only backup never truncates the transaction log. This backup type is not supported by Data Protection for SQL Server. If you plan to use this feature, you must use Microsoft SQL Server tools to perform the backup.

- Offline backup

  In some situations you may want to perform an offline copy of your Microsoft SQL Server database files. To do this, you can stop the SQL Server instance, and, using operating system tools or backup tools (such as the Tivoli Storage Manager backup-archive client for Windows), copy all the related files to the Microsoft SQL Server database and then restart the SQL Server instance.

  A discussion of this type of backup is beyond the scope of this book. For more information, see the Microsoft SQL Server documentation.

Note: A discussion about backup strategies is included in 2.3.4, “Microsoft SQL Server backup strategies” on page 46.

1.6.3 Data Protection for SQL Server restore methods

Tivoli Data Protection for SQL Server provides several restore methods.

Legacy restore

A Data Protection for SQL Server Legacy restore obtains backup copies of all or part of one or more SQL Server databases and returns them to the SQL server.

A complete restore of a database involves restoring a full backup or the equivalent thereof (from group, file, or set backups) and restoring all transaction logs since the last full backup.

VSS restore

A VSS restore restores VSS backups (SQL Server database files and log files) that reside on Tivoli Storage Manager server storage to their original location.

The following characteristics are true for VSS restores:

- Only full backup types can be restored. Differential, individual filegroups, individual files, and set backups are not supported by VSS and therefore, cannot be restored.
- Restore granularity is at the database level.
- One (or more) databases can be restored from a VSS snapshot backup located on Tivoli Storage Manager storage.
- VSS requires that data must always be restored to the same drive letters and paths as existed during the original backup.
- Restores can be performed in a Microsoft Cluster Server (MSCS) or Veritas Cluster Server (VCS) environment.

VSS Fast Restore

A VSS Fast Restore restores VSS backups that reside on local shadow volumes.

In general, restore processing can conclude within minutes instead of hours in this situation. The following characteristics are true of VSS Fast Restores:

- Only full backup types can be restored. Differential, individual filegroups, individual files, and set backups are not supported by VSS and therefore, cannot be restored.
- Restore granularity is at the database level.
- The key component of completing a VSS Fast Restore is the speed at which the application can become operational with the data that resides on local shadow volumes. Be aware that even though the data is restored relatively

quickly, the transaction logs must still be replayed after the restore and therefore, the time of recovery for the application increases.

VSS Instant Restore

A VSS Instant Restore copies a set of target volumes (that contain a valid snapshot) back to the original source volumes using hardware-assisted volume-level copy mechanisms. The application can return to normal operations as soon as the hardware-assisted volume-level copy has been started and the log replay is complete.

The key component of completing a VSS Instant Restore is the speed with which the application can become operational with the data that resides on local shadow volumes. Be aware that even though the data is restored relatively quickly, the transaction logs must still be replayed after the restore and therefore, the time of recovery for the application can increase.

A VSS Instant Restore requires that all of the source data resides on a supported storage subsystem supported by the VSS Instant Restore. If part of the data being restored (including the log files) resides on a local disk, a VSS Instant Restore of this data is not possible. In this situation, a VSS Fast Restore is performed. At the time of writing, IBM System Storage SAN Volume Controller, DS8000, and DS6000 support VSS Instant Restore.

1.6.4 Data Protection for SQL Server restore types

Tivoli Data Protection for SQL Server provides the same range of object types as for backups:

- Full database restore

  A full database restore restores full database backup objects for specified Microsoft SQL Server databases.

- Differential restore

  A differential restore restores only differential database backup objects for specified SQL Server databases. Restore time is reduced because only the latest differential backup is restored after its associated full backup is restored.

- Log restore

  A log restore restores only log backup objects for specified SQL Server databases.

- File restore

  A file restore restores only the file backup objects needed from a full backup, filegroup backup, a file backup, or a set for specified SQL Server databases.

- Group restore

  A group restore restores only the group backup objects needed from a full backup, filegroup, a file backup, or a set backup for specified SQL Server databases.

- Set restore

  In a set restore, Data Protection for SQL Server restores only set backup objects for specified SQL Server databases.

Depending on the backup strategy you choose, restoring a Microsoft SQL Server database might involve restoring multiple backup objects from the Tivoli Storage Manager server. In support of current Microsoft SQL Server restore capabilities, Data Protection for SQL Server also provides the ability to relocate files during restore and to perform point-in-time restores, named-marks restores, or partial restores:

- Point-in-time

  A point-in-time restore enables you to restore a transaction log backup to a specific SQL transaction date and time.

- Named-marks

  A named-marks restore is a feature of Microsoft SQL Server 2000 and 2005, which enables you to restore a transaction log backup up to or before a named point, possibly after a specified point in time, and to recover multiple related databases to the same named mark.

- Partial

  For Microsoft SQL Server 2000 and 2005, a partial restore enables you to restore just enough of a database into a temporary location to copy a specific table to the active database.

Further Data Protection for SQL Server restore functions include the following:

- Restore a backup using the same number of data stripes used to create the backup, or fewer stripes for Microsoft SQL Server 2000 and 2005.
- Restore with no recovery until the last restore with recovery.
- Restore from any available backup version created by Tivoli Data Protection for SQL Server V5.5.0, V5.2.1, V5.1.5, or V2.2.
- Replace an existing database with the restored database (or replace by relocating the restored database).
- Restore to a different SQL server or to a standby SQL server.
- Automatically restore all backup objects needed to make a restore complete by using *smart selection* in the GUI.

2

Planning considerations

This chapter provides the planning considerations for a successful implementation of Tivoli Storage Manager for Databases: Data Protection for SQL on Microsoft Windows.

This chapter discusses the following topics:

2.1 Data Protection for SQL Server requirements

This section provides information about Tivoli Data Protection for SQL Server requirements and discusses some of the choices you have to make during installation. Data Protection for SQL Server is available in the following packages:

- Paid in Full

  This package contains a license component and is a complete standalone release of the product.

- Program Temporary Fix (PTF)

  This package does not contain a license component. It is created to install over a previously installed version of Tivoli Data Protection for SQL Server.

2.1.1 Software and operating system requirements

Data Protection for SQL Server requires the following levels of Tivoli Storage Manager software:

- Tivoli Storage Manager backup-archive client Version 5.5.0 (or later).
- Tivoli Storage Manager API Version 5.5.0 (or later).
- Tivoli Storage Manager server Version 5.4.0 (or later)

Legacy backup and restore requirements

Table 2-1 shows the requirements for Legacy backup and restore operations.

Table 2-1 Minimum requirements for Legacy backup and restore

Operating system	Microsoft SQL Server	VSS provider	Tivoli Storage Manager for Copy Services
Windows 2003 x86[a] Windows 2003 x64[b] Windows 2003 ia64	Microsoft SQL Server 2000 or 2005[c]	None	None

a. Windows Server 2003 x86: Standard, Enterprise, or DataCenter Edition. All versions must be at Service Pack 1 (or later). Windows Server 2003 R2: Standard, Enterprise, or DataCenter Edition

b. Windows Server 2003 x64 Standard, Enterprise, or DataCenter x64 Edition. Windows Server 2003 x64 R2: Standard, Enterprise, or DataCenter x64 Edition

c. Microsoft SQL Server 2005 Standard or Enterprise Edition.

Basic VSS software and operating system requirements

Table 2-2 shows the requirements for basic VSS operations.

Table 2-2 Minimum requirements for basic VSS operations

Operating system	Microsoft SQL Server	VSS provider	Tivoli Storage Manager for Copy Services
Windows 2003 x86[a] Windows 2003 x64[b]	Microsoft SQL Server 2005[c]	Any VSS provider supported by Microsoft rules for VSS providers	Microsoft SQL VSS Integration Module V5.5.0

a. Windows Server 2003 x86: Standard, Enterprise, or DataCenter Edition. All versions must be at Service Pack 1 (or later). Windows Server 2003 R2: Standard, Enterprise, or DataCenter Edition.
b. The Microsoft SQL VSS Integration Module is dependent on the base Data Protection for SQL Server product and must be installed to perform any VSS operations.
c. Microsoft SQL Server 2005 Standard or Enterprise Edition.

VSS offloaded backup requirements

Table 2-3 shows the requirements for VSS offloaded backups.

Table 2-3 Minimum software and operating system requirements for VSS offloaded backup

Operating system	Microsoft SQL Server	VSS provider	Tivoli Storage Manager for Copy Services
Windows 2003 x86[a] Windows 2003 x64[b]	Microsoft SQL Server 2005[c]	Any VSS provider that supports transportable shadow copies[d]	Microsoft SQL VSS Integration Module V5.5.0[e]

a. Windows Server 2003 x86: Standard, Enterprise, or DataCenter Edition. All versions must be at Service Pack 1 (or later). Windows Server 2003 R2: Standard, Enterprise, or DataCenter Edition.
b. Windows Server 2003 x64 Standard, Enterprise, or DataCenter x64 Edition. Windows Server 2003 x64 R2: Standard, Enterprise, or DataCenter x64 Edition.
c. Microsoft SQL Server 2005 Standard or Enterprise Edition.
d. The VSS hardware provider must be installed on both machines that are involved in an offloaded backup.
e. The Microsoft SQL VSS Integration Module is dependent on the base Data Protection for SQL Server product and must be installed to perform any VSS operations.

VSS Instant Restore software and operating system requirements

Table 2-4 shows the requirements for VSS Instant Restore operations.

Table 2-4 Minimum software and operating system requirements for VSS Instant Restore operations

Operating system	Microsoft SQL Server	VSS provider	Tivoli Storage Manager for Copy Services
Windows 2003 x86[a] Windows 2003 x64[b]	Microsoft SQL Server 2005[c]	On DS storage subsystems: ► IBM TotalStorage VSS hardware provider V2.4.2 (or later) On SAN Volume Controller storage subsystems: ► IBM TotalStorage SAN Volume Controller V2.1.x (or later) or V3.1.x[d] ► IBM TotalStorage VSS hardware provider V2.4.3 (or later)	On DS storage subsystems: ► Microsoft SQL VSS Integration Module Version 5.5.0 (or later)[e] ► Hardware Devices Snapshot Integration Module V5.5.0 (or later) On SAN Volume Controller storage subsystems: ► Microsoft SQL VSS Integration Module V5.5.0 (or later)[f] ► Hardware Devices Snapshot Integration Module V5.5.0 (or later)[g]

a. Windows Server 2003 x86: Standard, Enterprise, or DataCenter Edition. All versions must be at Service Pack 1 (or later). Windows Server 2003 R2: Standard, Enterprise, or DataCenter Edition.
b. Windows Server 2003 x64 Standard, Enterprise, or DataCenter x64 Edition. Windows Server 2003 x64 R2: Standard, Enterprise, or DataCenter x64 Edition.
c. Microsoft SQL Server 2005 Standard or Enterprise Edition
d. IBM Subsystem Device Driver (SDD) V1.6.0.2 with Host Attachment Scripts V1.1.0.3. or (later) is required.
e. The Microsoft SQL VSS Integration Module is dependent on the base Data Protection for SQL Server product and must be installed to perform any VSS operations.
f. The VSS hardware provider must be installed on both machines that are involved in an offloaded backup.
g. The Hardware Devices Snapshot Integration Module is dependent on the base Tivoli Storage Manager backup-archive client product and must be installed to perform VSS Instant Restore operations.

2.1.2 Hardware requirements

This section explains the hardware requirements for Data Protection for SQL Server.

Note: Data Protection for SQL VSS operations are available on any hardware that supports Microsoft VSS requirements. Refer to your VSS provider documentation for required levels. The following list identifies some hardware storage subsystems that were tested with Data Protection for SQL Server VSS operations:

- IBM TotalStorage DS6000 and a machine with a processor supported by DS6000 with IBM Common Interface Model (CIM) Agent for DS Open API.
- IBM TotalStorage DS8000 and a machine with a processor supported by DS8000 with IBM Common Interface Model (CIM) Agent for DS Open API.
- IBM TotalStorage N3700 with Network Appliance™ (NetApp) SnapDrive Version 3.2 (or later).
- NetApp fabric-attached storage system with NetApp SnapDrive Version 3.2 (or later).
- IBM TotalStorage SAN Volume Controller Version 2.1.x (or later) or Version 3.1.x.

Contact your hardware storage subsystem vendor for exact details about their support of VSS operations.

Legacy or VSS backup and restore hardware requirements

Table 2-5 shows the hardware requirements for Legacy or VSS backup and restore operations.

Table 2-5 Hardware requirements for Legacy or VSS backup and restore operations

Architecture	Hardware description	Disk space	RAM
32-bit	Intel® Pentium® 166 equivalent (or later) processor	20 MB	48 MB (96 MB or greater recommended)
x64	One of the following: ▸ Processor that supports Intel Extended Memory 64 Technology (Intel EM64T) ▸ AMD™ 64-bit processor that supports AMD64 platform		

VSS offloaded backup hardware requirements

Table 2-6 shows the hardware requirements for VSS offloaded backup operations.

Table 2-6 Minimum hardware requirements for VSS offloaded backup operations

Architecture	Hardware description	Disk space	RAM
32-bit or x64	A storage subsystem[a] with a VSS hardware provider	See provider documentation	See provider documentation

a. You must have a hardware storage subsystem that supports transportable shadow copies and delivers a VSS hardware provider for the hardware storage subsystem that adheres to Microsoft VSS provider API standards.

VSS Instant Restore hardware requirements

Table 2-7 shows the requirements for VSS Instant Restore operations.

Table 2-7 Minimum hardware requirements for VSS Instant Restore operations

Architecture	Hardware description	Disk space	RAM
32-bit or x64	One of the following: ► IBM TotalStorage DS6000 disk storage subsystem3[a] ► IBM TotalStorage DS8000 disk storage subsystem3[a] ► IBM TotalStorage SAN Volume Controller V2.1.x (or later) ► IBM TotalStorage SAN Volume Controller V3.1.x	See disk storage subsystem documentation	See disk storage subsystem documentation

a. IBM TotalStorage DS6000 and DS8000 disk storage subsystems require IBM TotalStorage VSS hardware provider V2.4.2 (or later).

For detailed information regarding current hardware product compatibility requirements, see the IBM TotalStorage Web site:

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

2.2 Tivoli Storage Manager backup options

When creating policy for your backups, consider these differences between backing up data to Tivoli Storage Manager storage and backing it up to VSS disks.

Tivoli Storage Manager storage

Backups to Tivoli Storage Manager server storage are usually dictated by time, not versions.

A Tivoli Storage Manager backup operation stores the backed-up data on Tivoli Storage Manager server storage. Although this type of backup typically takes longer to process than a backup to local shadow volumes, a Tivoli Storage Manager backup is necessary when long-term storage is required, such as saving SQL Server data on tape for archival purposes. Tivoli Storage Manager backups are also necessary for disaster recovery situations when disks used for local backups are unavailable. By maintaining multiple backup copies on Tivoli Storage Manager server storage, a point-in-time copy is available should backups on the local shadow volumes become corrupt or deleted.

Local shadow volumes

Backups to local shadow volumes are usually dictated by versions because of space limitations and provisioning of VSS storage.

Sufficient local storage space must be available on local shadow volumes for a VSS backup strategy to be successful. Make sure sufficient storage space is assigned to the volumes to accommodate your Data Protection for SQL Server backup operations. Environment and storage resources also impact how many backup versions are maintained on local shadow volumes (for VSS Fast Restore and VSS Instant Restore) and how many backup versions are maintained on Tivoli Storage Manager server (VSS Restore and longer-term storage). It is recommended that different sets of policies be created for backups to both local shadow volumes and to Tivoli Storage Manager server storage. If you are using a VSS provider other than the Windows VSS system provider, make sure to review the documentation for that specific VSS provider.

VSS in SAN volume controller environments

To determine how much storage space is required for each local backup, be aware that backup LUNs require the same amount of storage space as original LUNs. For example, if you have a 100 GB database residing on a 200 GB LUN, you need a 200 GB LUN for each backup version.

When performing a Data Protection for SQL Server VSS backup (not offloaded) with Tivoli Storage Manager server as the backup destination, the Microsoft SQL Server data residing on SAN Volume Controller (SVC) disks, and using the IBM System Storage VSS hardware provider, in some isolated cases, the SVC LUNs remain mapped to the Windows host even though the VSS backup is complete. To work around this issue, you can use a backup destination other than `TSM` (BOTH or LOCAL). You can also manually unmap the volumes attached to the Windows host to work around this issue.

When performing two back-to-back Data Protection for SQL Server VSS backups and the Microsoft SQL Server data resides on SAN Volume Controller (SVC) disks, if the volumes are large or the SVC background copy rate is set at a low number, it may appear that the second VSS backup is hanging. In fact, it is waiting for the SVC background copy of the first backup to complete before proceeding with the second backup. SVC does not allow two background copies of the same volume to occur at the same time. You do not receive any indication that the second backup is waiting for the first SVC background copy to complete. You may see timeouts errors if the previous SVC background copy takes too long. To work around this issue, schedule your VSS backups far enough apart to accommodate this situation. You can also try increasing the copy rate of the SVC background copy.

VSS operations in IBM N series and NetApp environments

Be aware that in environments that contain IBM N series and NetApp systems, snapshots created using the IBM N series and NetApp snapshot provider are stored on the same volume where the LUN resides. Disk space consumed by a local backup consists only of the blocks that have changed since the last local backup was created. The following formula can be used to help determine how much space is required for each local backup: amount of data changed per hour * number of hours before a local backup expires. In addition, Write Anywhere File Layout (WAFL®) reserves blocks equal to two times the specified size of the LUN to be used. This space reservation ensures writes for virtual disks. Example 2-1 demonstrates how to calculate the size of these volumes.

Example 2-1 IBM N series and Netapp volume size calculation

```
SQL Database size: 100GB
Number of local backups to be kept: 3
Snapshot for TSM backup: 1
duration for TSM backup: 2hr
Backup frequency: 3hrs
The duration before a local backup is expired: 9 hrs
Amount of data changed/added/deleted per hr: 50MB
Space required for each local backup: 50*9= 450 MB
```

```
Space required for 3 local backups + 1 TSM backup: 450*3 + 50*2 = 1450
MB

The volume size required for the database:
100*2 (space reservation) + 1.5 = 201.5 GB
```

VSS limitations for NetApp NAS series or IBM N series

Due to the limitations in SnapDrive V4.0 and supported prior versions, and limitations in the VSS provider for NetApp FAS series and IBM N series, VSS-based operations using Data Protection for SQL Server with the backup destination set to LOCAL must be performed in specific ways. Failure to comply with the following configuration and operational recommendations can lead to serious conditions such as premature deletion of snapshots representing VSS backups to LOCAL, backup failure, and out-of-space conditions on the production volumes. When the limitations in the SnapDrive are addressed by NetApp, Data Protection for SQL Server VSS operations can be fully utilized.

Microsoft SQL Server storage configuration for NetApp NAS series or IBM N series VSS operations

If you plan to perform VSS backups with the backup destination set to LOCAL, check your setup to ensure that following requirements are met.

- The NAS filers LUNs used by a database must be fully dedicated to the database. The Microsoft SQL Server databases cannot share LUNs.
- A NAS filer LUN used by the Microsoft SQL Server databases must be the only LUN on the filer volume. For example, if SQL Server uses four LUNs, there must be four corresponding filer volumes, each volume containing one LUN.

Guidelines for VSS backup operations for NetApp NAS series or IBM N series

If you plan to perform VSS backups with the backup destination set to LOCAL, these backups must adhere to the following guidelines.

- VSS backups with the backup destination set to LOCAL must be bound to a management class that has verExists=1.
- VSS backups with the backup destination set to LOCAL can be either of type full or of type copy. You cannot mix local backups of type full and copy.
- VSS backups with the backup destination set to `TSM` can be full or copy. Tivoli Storage Manager backups have no restrictions.
- When performing VSS backups, you must ensure that a previous backup has finished completely before starting a new backup. Any overlap of backups can

result in undesirable side effects on the Microsoft SQL Server, the VSS service, and the NAS filer.

Sample VSS backup for NetApp FAS (fabric-attached storage) series or IBM N series

This section describes a sample backup procedure that can be used to perform VSS backups utilizing both Tivoli Storage Manager and LOCAL backup destinations in an optimal manner. We recommend you take the previously discussed considerations into account when reading this section.

The following assumptions apply to this sample backup procedure:

- The previously stated configuration requirements are met.
- The VSS backup to Tivoli Storage Manager takes one hour to complete.
- The VSS backup to LOCAL takes five minutes to complete.

Your backup procedure can consist of the following backups:

- Daily VSS full backups to LOCAL every four hours - 12 a.m., 4 a.m., 8 a.m., 12 p.m., 4 p.m., 8 p.m.
- Daily VSS full backups to Tivoli Storage Manager storage by one of the following two methods:
  - Specify backup destination set to BOTH at 12 a.m. Note that this setting creates a 12 a.m. backup to LOCAL. Therefore, no separate 12 a.m. backup to LOCAL is required.
  - Full offloaded backup at 1 a.m. Note that no VSS local backup is available to restore from between 1 a.m. and 4 a.m. when the next VSS backup to local will take place.
- Perform weekly VSS-copy backups to Tivoli Storage Manager (offloaded backup) 5 a.m.
- Perform weekly Legacy full backups (or as needed).

2.3 Microsoft SQL Server backup planning

Implementing a well-planned backup and recovery strategy provides an essential safeguard for protecting Microsoft SQL Server databases and helps to protect databases against failures originating from a variety of causes, such as media failures, hardware failures, human errors, and natural disasters. Several factors must be considered in order to develop a strategy to fulfill business requirements for data protection, such as required resources, work-loss exposure supported for the environment, and the benefits and trade-offs of each scenario.

In this section we discuss technical aspects and considerations for Microsoft SQL Server backups. For a Tivoli Storage Manager administrator working with SQL Server databases, it is crucial to understand the backup options that Microsoft SQL Server offers, the requirements for each one, and how to implement these options to satisfy the business requirements for each environment.

> **Note:** Remember that the prime focus of a backup strategy is to restore data in case of a SQL server failure.

2.3.1 Identify recovery requirements

The most important factor in a backup and recovery strategy is to meet the recovery business requirements. A database can be used for a variety of roles in an organization, from a development database with a few megabytes of information being accessed by a few developers to a non-stop production database with several terabytes of information being accessed by thousands of users around the world. Likewise, the recovery requirements for these particular databases may differ significantly: For a database used in the scenario we first described, maybe a weekly backup will suffice, and, for a database in the latter scenario, a comprehensive strategy should be designed to achieve the recovery requirements.

To identify the recovery requirements, you need to determine:

- How critical are your databases to your business?
- Is it acceptable to lose any database activity? How much time and changes are acceptable to lose?
- What is the maximum acceptable downtime for your database?
- Is it necessary to perform a restore right up to a point-of-failure?
- What is the backup window? How many resources are available for the backup?
- Does your database have to be available only during commercial hours or working days, or does it have to operate on a 24x7x365 basis?
- Are there peak periods of database utilization? How frequently does the data in the database change during peak and nonpeak periods?
- Do you have two or more databases that must maintain a logical consistency?
- What are the legal requirements for your backup routines? Are you required to retain backups for a long period of time, such as 5 or 10 years?

- Are your staff trained in backup and recovery tasks?
- How often will recovery routines be tested?

The answers to these questions can help you determine a backup strategy. For non-critical databases, you may decide to have simple backups that restore data to its state the night before. Or you may have data that you decide not to back up at all, if it can be easily re-created from other sources. You have to arrange more complex backups for critical databases to facilitate a restore to a desired point in time and to minimize the restore period.

In the next sections we discuss backup strategies and the options provided by Microsoft SQL Server and Data Protection for SQL Server to back up a database.

2.3.2 Backup strategy and database recovery model

According to the answers to the questions in 2.3.1, "Identify recovery requirements" on page 43, you must define which database recovery model must be used for your databases.

> **Note:** A further discussion about Microsoft SQL Server database recovery models can be found in Appendix B, "Microsoft SQL Server overview" on page 263.

Simple recovery model

Use the simple recovery model when:

- You do not need to recover a database to a specific point in time.
- You do not want, or you do not have resources available to back up the transaction log.

If the database is lost or damaged, either you can restore the database from a previous backup and lose all updates since the backup, or you can re-create the database from a different source.

> **Note:** By default, the system databases master, msdb, and tempdb use the simple recovery model. You cannot change the recovery model for the tempdb database. You can change the recovery model for the master database to full or bulk-logged for backward compatibility with earlier versions of Microsoft SQL Server; however, you cannot back up the transaction log for the master database. Therefore this change has no practical results.

Full recovery model

Use the full recovery model when:

- Your database contains critical information, and you must be able to recover all the data.
- You must be able to restore a database to a specific point in time in the past.
- You want to be able to restore individual pages.
- You have enough resources to support the administrative costs of transaction log backups.

If your database is lost or damaged, you restore the database from a previous backup and then apply all transaction log backups generated since then up to the point of failure.

Bulk-logged recovery model

Use the bulk-logged recovery model when your database runs in full recovery model and a large-scale bulk operation is performed. During the bulk operation, a point-in-time recovery is not needed.

We recommend you use the bulk-logged recovery model in association with the full recovery model. As soon as the bulk operation finishes, we recommend you switch back to the full recovery model. We also recommend you back up the transaction log before and after switching between full recovery model and bulk-logged recovery model.

2.3.3 Microsoft SQL Server log chains

A log chain is a continuous sequence of Microsoft SQL Server transaction log backups. A log chain starts with a full backup of the database. To perform a database point-in-time recovery or to perform a full database recovery using the transaction logs, it is mandatory that all transaction log backups be available from the beginning of the log chain - the backup full operation - up to the time the database will be recovered.

For databases using the full recovery model or bulk-logged recovery model, you can start backing up the database transaction log immediately after the first full database backup. Then, regularly perform transaction log backups not only to enable truncation of the transaction log files but also to minimize work-loss exposure. The more frequently you back up the transaction log files, the smaller your exposure to work-loss failures and the less vulnerable your transaction log files.

Note: Certain commands in Microsoft SQL Server, such as BACKUP LOG with the TRUNCATE_ONLY option, truncate the log and break the log chain sequence, causing the database to stay vulnerable to media failure until the next execution of a full or differential database backup. We strongly recommend you use these commands only if you fully understand the resulting impact.

2.3.4 Microsoft SQL Server backup strategies

A backup strategy is one of the most import parts of your planning considerations because every environment is unique.

The more simple backup strategy you use, the more simple your restore process. At the same time, using a more simple backup strategy results in more limitations, considering both storage utilization and the restore operation.

The more complex backup strategy you use, the more work you must do when setting up the scheduled backups. At the same time, using a more complex backup strategy gives you more options, considering both storage utilization and the restore operation.

You must balance business recovery requirements and available resources to define the right backup strategy for you. We recommend you clearly identify and document business recovery requirements, your strategy for backing up the environment, the recovery routines for restoring and recovering the environment, and finally the resources involved in the backup and restore procedures.

Different backup strategies are available depending on specific requirements for network traffic, the backup window, and the acceptable restore times.

Commonly used strategies, as well restore steps for each of them, are discussed in the next sections. Practical examples of backup and restore routines can be found in Chapter 4, “Data Protection for SQL Server backup” on page 127 and Chapter 5, “Data Protection for SQL Server restore” on page 179, respectively.

Full backup only (Legacy or VSS backup)

This approach is best for relatively small SQL Server databases because it means that the entire database is backed up each time. Each full backup takes the same amount of time to perform and is directly affected by the resources available in the environment. If you have a large database, you can use VSS snapshot to improve backup and restore times.

The restore process is most efficient because only the most recent full backup has to be restored.

Figure 2-1 illustrates the full backup only strategy.

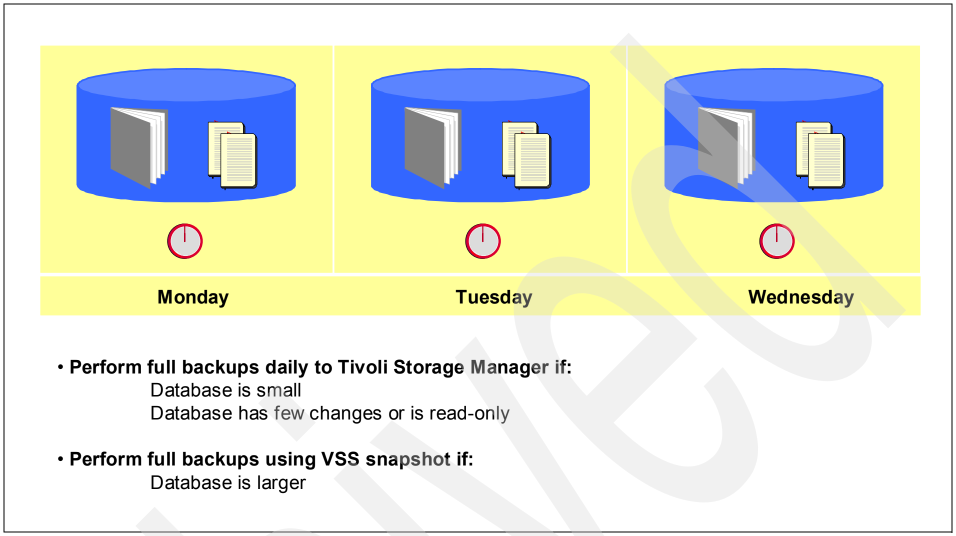

Figure 2-1 Full backup only strategy

Full database backups should be performed periodically - daily, for example. The database is restored in one step from the full backup.

Full plus log backup (Legacy backup only)

A full plus transaction log backup strategy is commonly used when the backup window or network capacity cannot support a full backup each time. In such cases, a periodic full backup followed by a series of log backups minimizes the backup window and network traffic.

The restore operation involves restoring the most recent full backup and the transaction logs since them.

Figure 2-2 illustrates a full plus log backup strategy.

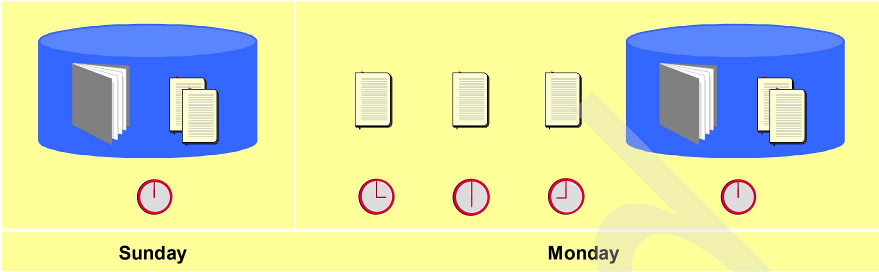

Figure 2-2 Full plus log backup strategy

Full plus log backup of the database:

- Periodically perform full database backups - daily, for example.
- Periodically perform transaction log backups - for example, every hour.

Restoring the database:

- Restore last full backup.
- Restore all transaction logs since the last full backup until the end of the logs or until the desired point in time.

Note: You can do a point-in-time restore to a specific date and time using transaction log backups.

Full plus differential backup (Legacy backup only)

Perform this type of backup between full backups. A differential database backup can save both time and space because it consists of only the changed portions of a database since the last full backup, minimizing resources necessary to back up the database. This strategy also benefits the restore time because instead of applying several transaction log backups, you simply apply the differential backup.

The restore operation involves restoring the most recent full backup and the last differential backup after the full backup.

Figure 2-3 illustrates a full plus differential backup strategy.

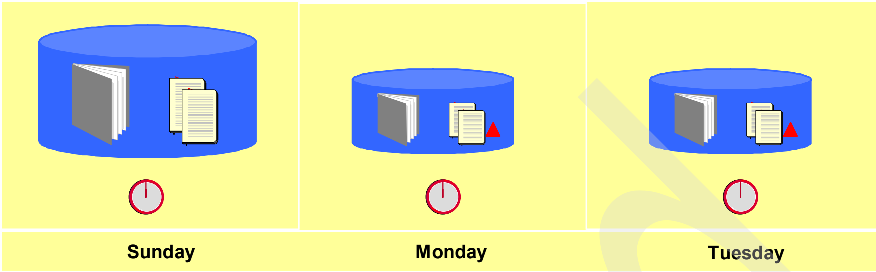

Figure 2-3 Full plus differential backup strategy

Full plus differential backup of the database:

- Periodically perform full database backups - weekly, for example
- Periodically perform differential backups - for example, daily or every 12 hours

Restoring the database:

- Restore last full backup
- Restore last differential backup

Full plus differential plus log backup (Legacy backup only)

This strategy speeds the restore because it reduces the number of transaction logs that may have to be restored and applied. If, for example, a full backup is done weekly, a differential nightly, and a log backup every four hours, the restore involves the full backup, a differential, and, at most, five log backups.

The difference between this strategy and the full plus differential backup is the transaction log files backup. For a database using the simple recovery model, the previous strategy is suitable; however, for production databases using full or bulk-logged recovery models, this strategy is the recommended option.

Figure 2-4 illustrates a full plus differential plus log backup strategy.

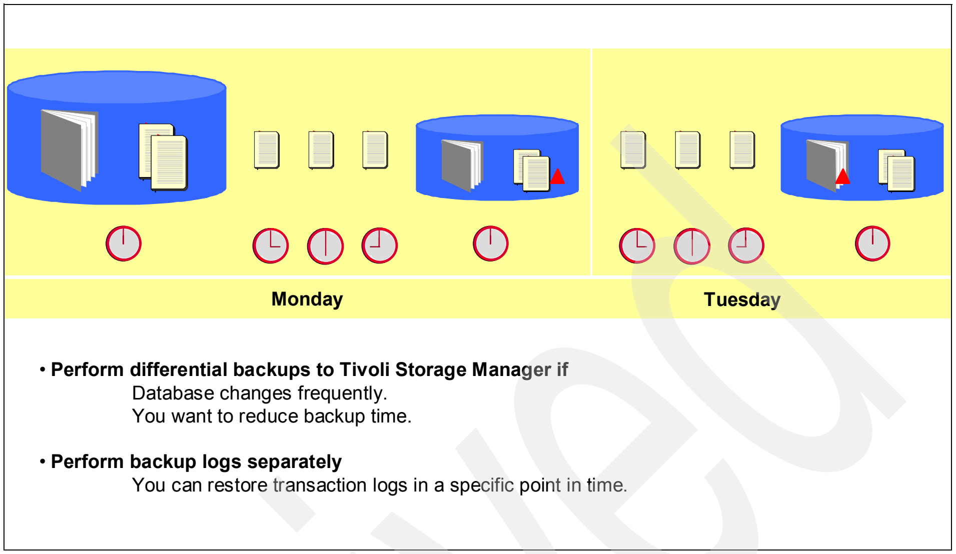

Figure 2-4 Full plus differential plus log backup strategy

Full plus differential plus log backup of the database:

- Periodically perform full database backups - weekly, for example.
- Periodically perform transaction log backups - for example, every 15 minutes or every hour.
- Periodically perform differential backups - for example, daily, or every 12 hours.

Restoring the database:

- Restore the last full backup.
- Restore the last differential backup (before desired restore point in time).
- Restore the following transaction logs until the desired point in time.

File or group backups (Legacy backup only)

Use a file backup strategy when it is impractical to back up an entire database due to its size and accompanying time and performance issues. When performing restores for a file or filegroup, you must perform a separate backup of the transaction log.

Figure 2-5 illustrates a file backup strategy.

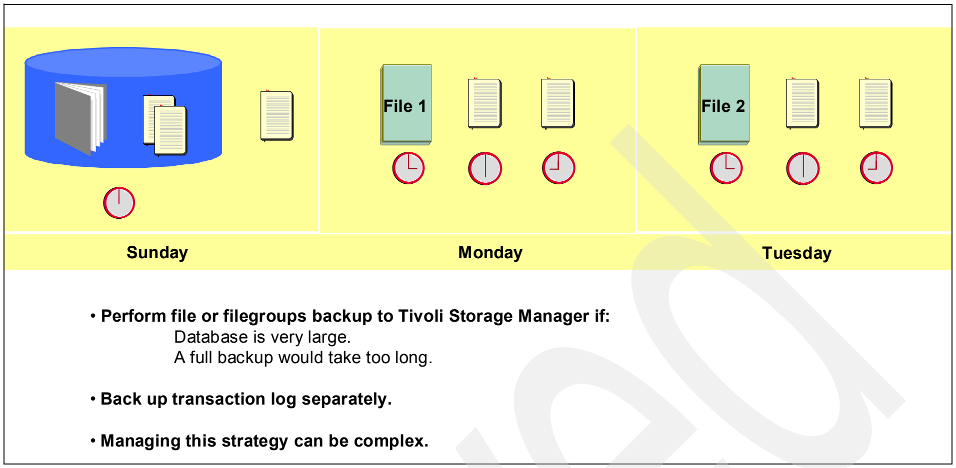

Figure 2-5 File or group backup strategy

File or group backup of the database:

- We recommend you perform an initial full backup of the database.
- Periodically perform transaction log backups - for example, every 15 minutes or every hour.
- Periodically perform file or group backups.

Restoring the database:

- Restore the last file or group backup (before the desired restore point in time).
- Restore the following transaction logs until the desired point in time.

Using VSS and Legacy backups together

Using VSS and Legacy backups together can implement a highly effective backup solution for Tivoli Data Protection for SQL Server data.

Microsoft supports and recommends using both backup methods in your complete backup strategy. However, Microsoft also states that you cannot mix the two types of backups. For example, a Legacy differential backup cannot be applied to a VSS full backup.

Table 2-8 provides details of this strategy.

Table 2-8 Backup strategy characteristics using VSS and Legacy backups together

Strategy characteristics	Legacy backup only	Legacy backup plus VSS backup
Available backup types	Full (one per week) Incremental (four per day)	Legacy full (one per week) VSS full (one per day)

Note: Backups to local shadow volumes are usually dictated by versions because of space limitations and provisioning of VSS storage.

Relationship between database recovery models and backup strategies

Table 2-9 shows which backup strategies are supported for each database recovery model.

Table 2-9 Supported backup strategies for each database recovery model

Backup strategy	Simple recovery model	Bulk-logged recovery model	Full recovery model
Full Legacy backup	Yes	Yes	Yes
Full VSS backup	Yes	Yes	Yes
Full plus log backup	No	Yes	Yes
Full plus differential backup	Yes	Yes	Yes
Full plus differential plus log backup	No	Yes	Yes
File or group backup	Partially - only for read-only filegroups	Yes	Yes

Note: When you implement a full backup only or a full plus differential backup strategy and the database is using either full or bulk-logged database recovery models, the transaction log may grown indefinitely, eventually filling up all available disk space and hanging Microsoft SQL Server.

If you plan to use these backup strategies without using transaction log backups, we recommend you use the simple the database recovery model.

2.4 Additional Microsoft SQL Server backup considerations

In addition to the backup strategies previously described, in this section we discuss additional Microsoft SQL Server characteristics and configurations that affect a successful backup strategy implementation.

2.4.1 System databases

Always back up the system databases (master and msdb) on a regular basis and at times when alterations of system-level information for Microsoft SQL Server are performed. Also back up the model database if it is modified.

We recommend you do backups of the system databases daily because they are unlikely to become large enough to consume a significant amount of resources during the backup operation. The same recommendation applies to the distribution database in replicate Microsoft SQL Server environments.

You cannot back up the tempdb database. It is re-created each time the SQL server is started.

> **Note:** You can consult the overview in Appendix B, "Microsoft SQL Server overview" on page 263.

2.4.2 Backing up checksums and database integrity checks

Regardless of the frequency of database backups, we highly recommend you always run **`dbcc checkdb`** and **`dbcc checkcatalog`** on a database immediately before backing it up to check the logical and physical consistency of the database. See your Microsoft SQL Server documentation for more information about using the Microsoft SQL Server database consistency checker.

2.4.3 Microsoft SQL Server mirrored backup media sets

Microsoft SQL Server 2005 introduces mirrored backup media sets. With this new functionality, you can perform up to four copies (mirrors) of the backup data. You need to use similar devices with the same properties for a successful mirrored backup; in other words, it is not possible to mirror a backup between tape and disk devices.

We recommend you use the option to back up the storage pool in IBM Tivoli Storage Manager. The storage pool can be a group of disk volumes, tape volumes, or optical volumes. IBM Tivoli Storage Manager server has two types of storage pools: the primary storage pool and the copy storage pool. The primary storage pool is used to store backed-up information about your Microsoft SQL Server environment, and the copy storage pool is a copy of your primary storage pool to improve data availability. You can simultaneously write data to a primary storage pool and one or more copy storage pools. You can use this feature in IBM Tivoli Storage Manager, instead of using Microsoft SQL Server mirrored backup media sets.

For more information about Tivoli Storage Manager copy storage pools, refer to the appropriate Tivoli Storage Manager administrator guide for the platform that you are using. See “Related publications” on page 281 for a list of administrator guides.

2.4.4 Backing up a transaction log without truncating the log

When you choose to perform a transaction log backup using Data Protection for SQL Server, you can indicate that you do not want to truncate the log. In general, you do not want to truncate the log when rebuilding a corrupt database. This option enables the server to back up the transaction log but does not try to touch the data in any way. It writes all transaction log entries from the time of the last log backup to the point of database corruption.

An example of transaction log backup without log truncation is shown in 4.2.7, “Tail-log backups using the GUI” on page 150.

2.4.5 Microsoft SQL Server replication

Special attention for backup and restore planning is needed in Microsoft SQL Server replicated environments. In a replicated environment, you must back up:

- The publication database at the publisher.
- The distribution database at the distributor.
- The subscription database at each subscriber.
- The master and msdb system databases in all Microsoft SQL Server instances. To reduce replication inconsistency risks, we recommend you back up these databases at same time as you back up the relevant replication database in the appropriate node - the publication, the distribution, or the subscription.

If regular transaction log backups are made, replication-related changes should be captured in the log backups. If not, we recommend you back up the logs after a relevant change.

Microsoft SQL Server provides three replication topologies:

- Snapshot replication, where all publisher data is always transferred to the subscribers, without allowing partial updates or synchronization.
- Transactional replication, where after an initial snapshot, subsequent changes in the publisher data are applied to the subscribers.
- Merge replication, which is similar to transaction replication except that with transactional replication, the subscriber cannot change the data; whereas merge replication enables both the publisher and the subscribers to change the data. Then the changes are propagated to other replication members.

For each replication type, the backup and restore strategies differ. Data Protection for SQL Server can be used to protect a replicated Microsoft SQL Server environment.

A full discussion of the requirements for each replication strategy type is beyond the scope of this book. For further documentation, refer to Microsoft SQL Server documentation or see:

http://technet.microsoft.com/en-us/library/ms151152.aspx

2.4.6 Microsoft SQL Server log shipping

The Microsoft SQL Server log-shipping feature is used to transfer transaction log backups from a primary database on a primary SQL server instance to one or more secondary databases on separate SQL server instances. This feature can also use an optional monitor server to monitor log-shipping operations and raise alerts when a failure occurs.

This technique is called *warm backup*, or *standby database*. Transaction logs are transferred to the backup database continuously. The changes reflected by the logs are applied to the database backup as they arrive. This significantly reduces the database downtime in case of problems.

When Microsoft SQL Server log shipping is in place, backup jobs are performed by SQL Server. SQL Server log shipping also requires that transaction log file backups are performed only to disk devices, not to tape devices.

If you need the log-shipping (or standby databases) capabilities in your environment, we recommend you use Tivoli Storage Manager tools instead of log shipping. You can achieve log-shipping functionality simply by utilizing Tivoli

Storage Manager Scheduler to periodically restore transaction log backups on secondary databases.

Note: An example of standby implementation can be found in 5.5, “Standby server” on page 207.

If you prefer to use log-shipping tools, you can use Tivoli Storage Manager tools to protect the database in the following way:

- Disable automatic transaction log backups, except the logs that are excluded from the log-shipping task.
- Use Tivoli Storage Manager backup-archive tools to back up the transaction log backup files on the primary database. You can exclude the transaction log backup files from the disk after ensuring they are already applied to all secondary databases and backed up by Tivoli Storage Manager.
- Perform full or differential database backups using Data Protection for SQL Server or Microsoft SQL Server tools. If you use SQL Server tools, also back up the generated files using Tivoli Storage Manager backup-archive tools.

  These backups can be generated from the primary or secondary databases, but keep in mind that if the backups are generated from a secondary database, you cannot include all recent changes in the primary database due to out-of-sync delays between the primary and secondary databases.
- Never use Tivoli Data Protection for SQL Server transaction log backups on a database involved in log shipping.

In a restore operation, you must restore the last full or differential backup and then manually apply the transaction log files backed up by the Tivoli Storage Manager backup-archive tool.

2.4.7 Microsoft SQL Server database mirroring

The Microsoft SQL Server database mirroring feature maintains two copies of a single database on different SQL server instances. One instance acts as the *principal server*, answering to client requests, while the other instance acts as the *mirror server*, also known as the *hot* or *warm standby server*. Unlike log-shipping capabilities where the transaction log backup files are moved to a standby location, Microsoft SQL Server mirroring works directly by applying operations on the principal server to the mirror server, using the transaction log records. Database mirroring can operate in either *synchronous* or *asynchronous* mode. The main difference between them is that in synchronous mode, the transactions must be committed on both nodes at same time before the transaction can return control to the client, while in asynchronous mode the mirror server can do a delayed commit.

The mirror database is created by restoring backups from the principal database on the mirror server. However, after a database-mirroring section is active, the following restrictions apply:

- Backup and restore operations on the mirror database are not allowed.
- Restore of the principal database is not allowed while mirroring is active.
- Backup of the principal database is allowed because you do not use the NORECOVERY option on the transaction log backups.

You can use Data Protection for SQL Server to create the mirror database and to back up the principal database as you would any other user database.

2.4.8 Microsoft SQL Server database snapshot

Microsoft SQL Server database snapshot provides a read-only, static view of a database, which can be used for reporting purposes, at a specific point in time. As the source database is updated, the original pages are copied to the snapshot database, preserving the data records as they were when the database snapshot was created.

You can still back up the source database. However, you cannot restore the source database; to restore the source database, you must drop the database snapshots associated with the source database. In addition, you cannot back up or restore database snapshots.

Data Protection for SQL Server can be used to back up the source database snapshot.

2.4.9 Full-text catalogs

In Microsoft SQL Server 2005 full-text catalogs are included in database backups. Until Microsoft SQL Server 2000, it was necessary to manually back up the operating system files and registry entries for the full-text catalogs.

2.4.10 Backing up Microsoft SQL Server non-database components

Microsoft SQL Server 2005 has several components apart from the database engine. For some components, the configuration data is not stored inside a SQL server database, or a database backup alone is not sufficient to provide the necessary recoverability capabilities for the component.

In this section we discuss these Microsoft SQL Server non-database components, and how can you use Tivoli Storage Manager to protect them.

Analysis Services

While sharing the same nomenclature, Microsoft SQL Server databases and Analysis Services databases have completely different uses and attributes. A Microsoft SQL Server database is used mainly to store relational data, and it is managed by the SQL Server database engine. The Analysis Services database is used to store OLAP metadata, such as cubes and dimensions, and not the transactional data itself. Analysis Services databases are stored in operating system files and are accessed by the Analysis Services application.

To back up the Analysis Services database, you must use Microsoft SQL Server tools, such as SQL Server Management Studio. When you perform a backup operation, the SQL Server Management Studio tool checks all required files that must be backed up and then packages these files into a single file.

> **Note:** In Microsoft SQL Server 2000, it was necessary to back up Analysis Services data directly from the operating system files - also known as a *raw backup*. Although this is possible in Microsoft SQL Server 2005, Microsoft does not recommend it.

You can automate Analysis Services backup execution using scripts, and then use the Tivoli Storage Manager backup-archive client for Windows to back up the packaged file to the Tivoli Storage Manager server. By doing this, you can maintain multiple versions of Analysis Services backups. Data Protection for SQL Server does not back up Analysis Services databases.

A discussion of Analysis Services backup and restore is beyond the scope of this book. For more information about Analysis Services backup and restore strategies, see:

http://www.microsoft.com/technet/prodtechnol/sql/2005/bkupssas.mspx

Reporting Services

A number of Reporting Services components require backing up:

- Reporting Services databases

  Reporting Services stores its application data in two Microsoft SQL Server databases: reportserver, which uses a full recovery model, and reportservertempdb, which uses a simple recovery model. Data Protection for SQL Server can back up these databases, similar to any other Microsoft SQL Server user database.

- Encryption keys

  To back up and restore Reporting Services encryption keys, you must use Microsoft SQL Server tools. After you generate a backup file for the encryption key, you can use the Tivoli Storage Manager backup-archive client for Windows to back up this file.

- Reporting Services Web sites

  Reporting Services uses Internet Information Services (IIS) as the Web server for its pages. You can use IIS backup tools to back up the Reporting Services Web sites.

- Configuration files and data files

  Reporting Services creates several configuration files to store application settings. Reporting Services also creates several operating system files to store its components, such as report definition files, report model files, and shared data source files. You can back up these files using the Tivoli Storage Manager backup-archive client for Windows.

A discussion of Reporting Services backup and restore is beyond the scope of this book. For more information about Reporting Services backup and restore, see:

`http://technet.microsoft.com/en-us/library/ms155814.aspx`

Integration Services

Microsoft SQL Server 2005 Integration Services (SSIS) packages are commonly stored in the msdb database; however, they can also be stored in operating system files. A regular backup of the msdb database protects your packages stored in the database, while you can use the Tivoli Storage Manager backup-archive client for Windows to back up the packages stored outside the database.

Notification Services

Notification Services stores its data and configuration information in databases and operating system files. You can back up the Notification Services databases similar to any other regular user database using Data Protection for SQL Server. To back up the operating system files, you can use the Tivoli Storage Manager backup-archive client for Windows.

> **Note:** We recommend you back up the Notification Services database and operating system files in the same scheduled operation to reduce the likelihood of application errors after recovery.

A discussion of Notification Services backup and restore is beyond the scope of this book. For more information about Notification Services backup and restore, see:

http://technet.microsoft.com/en-us/library/ms166456.aspx

2.5 Data Protection for SQL Server backup strategies

Aside from the main design architecture of Tivoli Storage Manager for backing up Microsoft SQL Server, other considerations are important for a complete backup strategy. While a detailed discussion of these considerations are outside the scope of this book, they are discussed here briefly.

2.5.1 Backup policy considerations

IBM Tivoli Storage Manager policy determines how Tivoli Data Protection for SQL Server backups are managed on IBM Tivoli Storage Manager storage.

The Tivoli Storage Manager server recognizes Data Protection for SQL Server as a node. Data that is backed up to Tivoli Storage Manager storage from this Data Protection for SQL Server node is stored and managed according to settings specified by Tivoli Storage Manager server policy. Tivoli Storage Manager policy can manage the VSS backups that are placed on local shadow volumes as well as in Tivoli Storage Manager server storage pools. The Tivoli Storage Manager server is responsible for managing VSS backups, whether the backup is stored on local shadow volumes or on the Tivoli Storage Manager server. Be aware that while a VSS snapshot (created for backing up to Tivoli Storage Manager server storage) is deleted after the backup completes, a VSS snapshot (created for backing up to local shadow volumes) remains active until the backup version is expired according to the policy settings for VSS backups on local shadow volumes.

Make sure the following policy items are defined with the recommended settings:

- Domain

  Create a policy domain on the Tivoli Storage Manager server to be used exclusively for Data Protection for SQL backups.

- Policy set

  Policy sets contain management classes (which contain copy groups) that determine the rules by which Data Protection for SQL Server backups are performed and managed. Define the policy set to the policy domain to which Data Protection for SQL backups belong. Note that the policy set must be activated. and only one policy set can be active in the policy domain.

- Management class

  Define a management class for backups residing on local shadow volumes and a management class for backups residing on Tivoli Storage Manager server storage. Different management classes provide the opportunity to establish specialized policies for each storage destination.

  Be aware that Legacy backups on IBM Tivoli Storage Manager server storage, VSS backups on IBM Tivoli Storage Manager server storage, and VSS backups on local shadow volumes all have different IBM Tivoli Storage Manager server names. Therefore, each can have its own management class, and it is possible to have three active backups of the same database. Make sure your backup strategy is planned and well defined before defining management classes.

  On Legacy backup only, you need to consider metadata. The management classes for Data Protection for SQL Server metadata should be identical to the corresponding management classes for database data except that metadata management classes should not allow migration to removable media. If any Data Protection for SQL metadata is on removable media, queries may require media mounts, and backups or restores may require additional media mounts.

  Data objects and their associated meta objects should have the same version limits and retention values. However, because meta objects may have to be restored as a result of a Data Protection for SQL Server query, you may want to consider storing meta objects in a disk-only storage pool so that a media mount is not necessary to resolve the query. To do this you can either:

  – Define a separate management class with a copy destination pointing to a disk pool that does not have any removable media in its hierarchy.

  – Bind all meta objects to that management class using an include statement in the Data Protection for SQL Server options file. Alternatively, you can choose to use the same management class (and storage pools) for both meta and data objects if you rarely need the meta objects, or need them only immediately preceding a restore when a volume mount is required anyway. In many cases, you can also obtain the meta object information from Microsoft SQL Server as recorded in its msdb database.

- Copy group

  Define the copy group as a backup copy group and not an archive copy group. Because Data Protection for SQL Server stores all objects as backup objects on Tivoli Storage Manager in backup storage pools, an archive copy group is not required, although an archive copy group can exist. The following backup copy group parameters significantly influence your backup policy:

  VERExists**:** Determines the maximum number of Microsoft SQL Server database backup versions to retain for databases that exist on the Data Protection for SQL Server client system. Therefore, if you want to keep *n* backups on local shadow volumes and also perform VSS backups to Tivoli Storage Manager server storage, make sure you provision enough storage space on local shadow volumes and specify `verexists=n+1`. Make sure to specify a verexists value that accommodates your VSS backup goals.If you have limited storage space for VSS operations and are restricted to a `verexists=1` setting, you can take advantage of the `Backup Destination BOTH` option. This stores the backup on local shadow volumes as well as sending a copy to Tivoli Storage Manager server storage. It is possible for VSS backups (which Data Protection for SQL Server creates and stores on local shadow volumes) to be modified and deleted from outside of Tivoli Storage Manager control.

  For example, the Microsoft VSSADMIN DELETE SHADOWS command can remove a VSS backup managed by Tivoli Storage Manager without Tivoli Storage Manager being able to prevent such a removal. In such a situation, Tivoli Storage Manager recognizes the backup removal and reconciles its index of available backups with what resides on local shadow volumes. It is important to be aware of this potential for removal and establish a strategy that protects VSS backup data stored on local shadow volumes from being compromised.

  – VERDeleted**:** Determines the maximum number of Microsoft SQL Server database backup versions to retain for databases that have been deleted from the Data Protection for SQL Server client system after being backed up by Tivoli Storage Manager.

  – RETExtra**:** Determines the number of days to retain a Microsoft SQL Server database backup version after that version becomes inactive.

  – RETOnly**:** Determines the number of days to retain the last Microsoft SQL Server database backup version of a database that has been deleted from the Data Protection for SQL Server client system. Be aware that log backups do not participate in expirations (due to version limit) because there is never more than one version of log backup object. This is because log backups are always uniquely named. However, all Legacy backup objects for a SQL Server database are inactivated when a new full backup of that SQL Server database is performed.

– MODE, SERialization, FREQuency**:** You can accept default values for these backup copy group parameters because they are not applicable to Data Protection for SQL Server.

– DESTINATION**:** Select the preferred storage pool where you plan to send your backups. Verify performance considerations on “Data Protection for SQL Server performance considerations” on page 68.

See the *IBM Tivoli Storage Manager for Windows Administrator’s Reference Version 5*, SC32-0127, for complete information regarding these parameters.

Additional considerations for VSS backups

The following issues impact your Tivoli Storage Manager policy for managing VSS backups:

- Overall backup strategy.
- Length of time that VSS backups reside on Tivoli Storage Manager server storage.
- Number of VSS backup versions that reside on Tivoli Storage Manager server storage.
- Types of VSS backups that reside on Tivoli Storage Manager server storage.
- Number of VSS backup versions that reside on local shadow volumes.
- Types of VSS backups that reside on local shadow volumes.
- The amount of available target volume storage provisioned for VSS operations.
- Scheduling considerations.

  Schedule VSS and Legacy backups to start at different times because you do not want these backups to overlap. Determine how long each backup will take and adjust their start times, so that one type of backup does not start before another has finished.

2.5.2 Client node name considerations

The machine where Data Protection for SQL Server is installed must be registered to the Tivoli Storage Manager server with a node name. This node name owns and manages all Data Protection for SQL Server data that is backed up to the Tivoli Storage Manager server. Specify this node name with the `nodename` option in the dsm.opt options file located (by default) in the Data Protection for SQL Server installation directory.

Configure the parameter BACKDELete value to YES. This parameter determines whether the Data Protection for SQL Server node can delete its own backup files from the IBM Tivoli Storage Manager server.

To perform VSS operations, you may need to register node names for additional machines.

Proxy node definitions

Because Data Protection for SQL Server VSS backup operations are implemented through the Tivoli Storage Manager backup-archive client, you must use node names specifically for VSS operations in addition to using a node name for where Data Protection for SQL Server is installed. As part of the configuration procedure, a proxy relationship is defined for these various node names. This proxy relationship allows node names to perform operations on behalf of another node name. When registering these nodes to the Tivoli Storage Manager server for VSS operations, do not specify the Tivoli Storage Manager `USerid=NONE` parameter. VSS operations fail when this parameter is specified. Two types of node names are defined in proxy node relationships:

- Target node: A node name that controls backup and restore operations and owns the data on the Tivoli Storage Manager server.
- Agent node: A node name that performs operations on behalf of a target node.

Required node names for basic VSS operations

To perform basic VSS operations, you must have one target node and one agent node (see Table 2-10).

Table 2-10 Required node names for basic VSS operations

Proxy node type	Nodename	Where to specify	Considerations
Target node	Data Protection for SQL Server node name	Use the node name in the Data Protection for SQL Server options file (dsm.opt).	Node name where Data Protection for SQL Server is installed.
Agent node	Local DSMAGENT node	Use the `localdsmagentnode` parameter in the Data Protection for SQL Server configuration file.	Node name where the backup-archive client and VSS provider are installed. The agent node is responsible for performing VSS operations because Data Protection for SQL Server itself does not perform any direct VSS operations.

Note: The agent node and target node are on the same machine for basic VSS operations.

Required node names for VSS offloaded backups

To perform VSS offloaded backups, you must have one target node and two agent nodes (see Table 2-11).

Table 2-11 Required node names for VSS offload backups

Proxy node type	Nodename	Where to specify	Considerations
Target node	Data Protection for SQL Server node name	Use the `nodename` option in the Data Protection for SQL Server options file (dsm.opt).	Node name where Data Protection for SQL Server is installed.
Agent node	Local DSMAGENT node	Use the `localdsmagentnode` parameter in the Data Protection for SQL configuration file.	Node name where the backup-archive client and VSS provider are installed, it is resposible for performing VSS operations because Data Protection for SQL Server itself does not perform any direct VSS operations.

Proxy node type	Nodename	Where to specify	Considerations
Agent node	Remote DSMAGENT node	Use the `remotedsmagentnode` parameter in the Data Protection for SQL Server configuration file.	Node name of a separate machine that must also have the backup-archive client and VSS provider installed. The machine is responsible for performing movement of VSS snapshot data from local shadow volumes to the IBM Tivoli Storage Manager.

Make sure that the `localdsmagentnode` and `remotedsmagentnode` are registered to the same Tivoli Storage Manager server that is specified in the Data Protection for SQL Server options file (dsm.opt) and the backup-archive client options file (also dsm.opt).

2.5.3 Schedule considerations

You schedule Data Protection for SQL Server backups using the Tivoli Storage Manager backup-archive client scheduler.

Consider the following when defining a Tivoli Storage Manager Scheduler:

- If you want to use the Tivoli Storage Manager server-prompted scheduling mode, the Data Protection for SQL option file must contain the `TCPCLIENTADDRESS` and `TCPCLIENTPORT` options. If you want to run more than one scheduler service, use the same `TCPCLIENTADDRESS`. However, you must use different values for `TCPCLIENTPORT` (in addition to different node names). You need multiple scheduler services when you are scheduling Data Protection for SQL as well as the regular Windows backup client. Server-prompted scheduling is supported only in TCP/IP communications. By default, Data Protection for SQL Server uses the client polling schedule mode.
- The Scheduler must be restarted after making any changes to the Data Protection for SQL Server options file that affect the Scheduler.

> **Note:** If you are running the Scheduler Service in a cluster environment, use the Cluster Administrator to stop and restart your Scheduler Service. Do not use the **`net stop`** and **`net start`** commands.

- The default Tivoli Storage Manager Scheduler log file (dsmsched.log) contains status information for the Scheduler. This file is created by default in the installation program directory. To override the files, use the `SCHEDLOGNAME` option in the Data Protection for SQL Server options file.

- Data Protection for SQL Server creates its own log file with statistics about the backed-up database objects when the `/logfile` parameter is specified with the **`tdpsqlc`** command.

> **Note:** Output from scheduled commands are sent to the Scheduler log file (dsmsched.log). After scheduled work is performed, check the log to ensure the work completed successfully.

- If `PASSWORDACCESS GENERATE` is not specified in the dsm.opt file, the Tivoli Storage Manager password must be specified when using the **`tdpsqlc`** command.

2.5.4 Data Protection for SQL Server security considerations

Data Protection for SQL Server must be installed by a user with Windows administrator authority.

Standard Tivoli Storage Manager security requirements apply to Data Protection for SQL Server. Data Protection for SQL Server must be registered to the Tivoli Storage Manager server, and the appropriate node name and password must be used when connecting to the Tivoli Storage Manager server.

Data Protection for SQL Server provides three options when specifying Microsoft SQL Server logon information:

- Accept the default account and blank password used in releases prior to Microsoft SQL Server 2005.
- Use SQL user ID security and specify both the SQL user name and password. With SQL user ID security, the Microsoft SQL Server administrator provides the logon ID and the password that enables access to SQL server.
- Use a trusted connection and let Windows authenticate the logon.

> **Note:** The SQL logon user or Windows user name must be added to the Microsoft SQL Server SYSADMIN fixed server role before it can be used by Data Protection for SQL Server.

For more information about Microsoft SQL Server security, refer to “Microsoft SQL Server security” on page 274.

2.5.5 Data Protection for SQL Server performance considerations

Data Protection for SQL Server provides certain parameters that you can tune for optimum performance.

Buffering

Data Protection for SQL Server is a multithreaded application that uses asynchronous execution threads to transfer data between the SQL and Tivoli Storage Manager servers. To accomplish this, multiple data buffers are used to allow one thread to receive data from one side, while another thread sends data to the other side. For example, one thread can be reading data from Microsoft SQL Server, while another sends data to the Tivoli Storage Manager server. The number of buffers that Data Protection for SQL Server allocates to these threads can be specified in the /BUFFERS and /SQLBUFFERS parameters of the command-line interface. The size of these buffers can be specified in the /BUFFERSIZE and /SQLBUFFERSIZE parameters.

Data striping

In addition to multithreading to maximize throughput on a single session, Data Protection for SQL Server uses separate threads to support SQL Server data striping, which uses multiple parallel sessions to back up and restore a single database. This method is an additional way to maximize data throughput. If a single session cannot fully exploit the available bandwidth, multiple parallel sessions can yield improved data throughput, especially if the database is spread across multiple physical volumes.

If you use one data stripe per physical volume for both the SQL server and the Tivoli Storage Manager server, the performance (measured as the amount of time necessary to back up or restore a particular SQL Server database) should show an improvement over the unstriped case (approximately proportional to the number of data stripes used, given the constraints of the devices and the network used, and striping independent overhead in Microsoft SQL Server, Tivoli Storage Manager server, and Data Protection for SQL Server).

You must use the `MAXNUMMP` parameter on a Tivoli Storage Manager REGISTER NODE or UPDATE NODE command to enable a node to use multiple sessions to store data on removable media such as tape (which requires multiple mount points to be allocated to that node).

> **Note:** Additional striping does not necessarily improve performance and may even decrease performance if system resources such as real and paged memory, CPUs, networkinterface cards, networks, device I/O, and RAID overhead become saturated or exceed capacity.
>
> If you use striping in conjunction with SQL buffers, make sure that the number of SQL buffers specified is equal to or greater than the number of stripes.
>
> The default values that Data Protection for SQL Server assigns to buffers, buffer size, and stripes can be changed in the Data Protection for SQL Server configuration file. Use the **`set`** command or the **Edit** menu on the GUI to modify the configuration file.

LAN-free environment

Running Data Protection for SQL Server in a LAN-free environment, if you are equipped to do so, avoids network constraints. Specify `ENABLELANFREE YES` in the Data Protection for SQL Server options file. For information about setting up a LAN-free environment, see *IBM Tivoli Storage Manager for Windows Storage Agent User's Guide,* SC32-0133.

Collocation

If you use the full plus log backup strategy, you must decide whether to modify Tivoli Storage Manager storage management policies to ensure that all log backups are stored together on the Tivoli Storage Manager server (collocated). This helps improve restore performance by reducing the number of media mounts necessary for restoring a series of log backups. Consult your Tivoli Storage Manager administrator for details on collocation. A single restore can require a full backup, a differential backup, and multiple incremental backups. We recommended you use collocation if these backups are stored on removable media.

Specify collocation by file space: `define stgpool COLlocate=FILespace` if you plan to restore multiple databases in parallel. We make this recommendation because individual data stripes stay on separate removable volumes. If you use data striping, use collocation by file space on sequential storage pools to maintain the stripes on separate storage volumes. This is necessary to enable concurrent parallel access to each of the stripes.

If multiple stripes for the same object end up on the same sequential volume (because sufficient empty volumes are not available), you can issue the Tivoli Storage Manager server **`move data`** command to move the objects to a disk storage pool or to new sequential volumes added to the storage pool so that they can be accessed in parallel. A single, complete restore may require the following:

- A full database backup
- A differential backup
- Multiple log backups
- One or more group files
- Set backups and multiple log backups

We recommend you use collocation if these backups may be stored on removable media.

2.5.6 Clustering considerations

If you use Microsoft Cluster Server clustering for fail-over support, you must install Data Protection for SQL Server on each cluster node and configure them identically. Additional setup is required to complete the fail-over installation. You must identify a clustered SQL server by its virtual server name and use that name in Data Protection for SQL Server to access that SQL server.

Data Protection for SQL Server supports Microsoft SQL Server running in a Microsoft Cluster environment and Veritas cluster environment. The VSS is supported in a Microsoft SQL Server-clustered environment.

For Windows 2003, Data Protection for SQL Server uses the Active Directory to support fail-over clustering. The following list provides information to consider when running Data Protection for SQL Server in a Microsoft Cluster Server environment or in a VCS environment:

- You must install Data Protection for SQL Server on both nodes of the cluster. In addition, when installing Data Protection for SQL Server, you must install it on a disk local to each node (not on a shared cluster disk).
- You must specify `clusternode yes` in the Data Protection for SQL Server options file.
- Use identical configurations in the Data Protection for SQL Server options file when configuring Data Protection for SQL Server on each node of the cluster.
- If you are using the Tivoli Storage Manager Scheduler for automating backups, you must install the Scheduler Service on both nodes of the cluster to enable fail-over support.
- The Tivoli Storage Manager treats backups as coming from a single server (the virtual server) regardless of which node of the cluster a backup was performed on.

Data Protection for SQL supports VSS operations in a clustered Microsoft SQL Server environment. These requirements and limitations must be understood for Data Protection for SQL to successfully perform VSS operations in a clustered SQL Server environment. You need to consider the following limitations that apply to clustering on VSS environments:

- Dynamic disks are not supported.
- VSS Backups that reside on local VSS shadow volumes can be restored only to the physical node that created the VSS backup. For example, if NODE_A of a cluster created a VSS backup and stored it on local shadow volumes, NODE_B of the cluster cannot restore that particular VSS backup. NODE_B can restore only those VSS backups stored on the Tivoli Storage Manager server or those VSS backups stored on local shadow volumes that were created by NODE_B. This is due to a limitation related to VSS cluster support and not to Tivoli Storage Manager.
- VSS backups that reside on local VSS shadow volumes *may be deleted* in the event of a cluster failover. This means that if NODE_A of a cluster created a local VSS backup and afterward the SQL server fails over to NODE_B and if a Data Protection for SQL Server VSS operation is performed on NODE_B of the cluster, the local VSS backup created by NODE_A will be deleted. This is caused by the fact that the Microsoft VSS architecture is not cluster aware.
- The Tivoli Storage Manager Client Acceptor Daemon (CAD) must be installed on each cluster node so that it can continue operations in the event of a failover. Make sure the CAD service name is the same on all cluster nodes so that it can be started by a generic cluster service.
- We recommend that the local DSMAgent client node be a separate node than your normal backup-archive client, because this CAD service must be made a non-cluster option.
- The remote DSMAgent client node does not require you to register a separate node for each server within the cluster because this server only acts as a secondary server.
- Use the Microsoft **`vssadmin`** and **`vshadow`** commands to verify the environment.
- A Data Protection for SQL Server configuration file should be configured for each node in the cluster. These files are almost identical, except that the `localdsmagentnode` parameter points to the corresponding local DSMAgent on each node.

The issues to consider for Data Protection for SQL Server in a cluster environment are covered in “Configuring the Data Protection for SQL Server options file in a clustered environment” on page 106.

2.5.7 Multiple SQL servers on same machine

If multiple instances of Microsoft SQL Server are running, the additional instances are identified by the instance name. You must use that name in Data Protection for SQL Server to access that SQL server.

2.5.8 SQL server listening on a non-default port

If a SQL server is listening on a port different than 1433, you must include the port number in the TDPCFG.sql file. For more information, see 3.2.10, “Specifying Data Protection for SQL Server preferences” on page 107.

3

Installation and configuration

In this chapter we describe how to install and customize IBM Tivoli Storage Manager Data Protection for SQL Server to protect your SQL Server database, and how to install other related components that are necessary to configure your environment.

We provide detailed instructions in this chapter. By following them, you should be able to successfully install IBM Tivoli Storage Manager Data Protection for SQL Server and configure it, meeting your company's requirements.

In addition to basic installation and configuration, we also discuss Data Protection for SQL Server installation with IBM Tivoli Storage Manager for Copy Services. This includes the installation of all components including the backup-archive client.

The following topics are discussed in this chapter:

3.1 Installation and configuration overview

This section provides detailed information about installation and configuration Data Protection for SQL Server and setting IBM Tivoli Storage Manager options, policies, and preferences.

In your planning steps, you must consider whether you are using Legacy or VSS backups. If you use VSS backups, you need to do an additional configuration on your IBM Tivoli Storage Manager server.

You must identify which applications is necessary to install and configure in your environment. Table 3-1 identifies the software applications that you must install and the applications necessary to configure to implement certain features.

Table 3-1 List of applications to install and to configure

To use these features	Application to install (SQL server machine)	Applications to configure
► Legacy backup ► Legacy restore	► Backup-archive client ► Data Protection for SQL Server	► Data Protection for SQL Server ► Tivoli Storage Manager server ► Tivoli Storage Manager backup-archive client scheduler
► VSS backup ► VSS restore	► Backup-archive client ► Data Protection for SQL Server ► IBM Tivoli Storage Manager for Copy Services	► Data Protection for SQL Server ► Tivoli Storage Manager server ► Tivoli Storage Manager backup-archive client scheduler ► Tivoli Storage Manager backup-archive client local Client Acceptor Daemon (CAD) (local DSMAGENT node) ► VSS software provider or VSS hardware provider or both

To use these features	Application to install (SQL server machine)	Applications to configure
► VSS backup ► VSS restore ► Offloaded backup	► Backup-archive client ► Data Protection for SQL Server ► IBM Tivoli Storage Manager for Copy Services	► Data Protection for SQL Server ► Tivoli Storage Manager Server ► Tivoli Storage Manager backup-archive client scheduler ► Tivoli Storage Manager backup-archive client local Client Acceptor Daemon (local DSMAGENT node) ► Tivoli Storage Manager backup-archive client local Client Acceptor Daemon (remote DSMAGENT node) ► VSS software provider or VSS hardware provider or both
► VSS backup ► VSS restore ► VSS Instant Restore ► Offloaded backup	► Backup-archive client ► Data Protection for SQL Server ► IBM Tivoli Storage Manager for Copy Services	► Data Protection for SQL Server ► Tivoli Storage Manager Server ► Tivoli Storage Manager backup-archive client scheduler ► Tivoli Storage Manager backup-archive client local Client Acceptor Daemon (local DSMAGENT node) ► Tivoli Storage Manager backup-archive client local Client Acceptor Daemon (remote DSMAGENT node) ► VSS software provider or VSS hardware provider or both

Note: You can configure Legacy and VSS backups to work together. Consider the features you want to use and install the necessary software to respond to all requests.

3.1.1 IBM Tivoli Storage Manager component requirements

We assume that you have knowledge of IBM Tivoli Storage Manager client and server installation and configuration. For detailed information about IBM Tivoli Storage Manager server, you can consult these IBM Redbooks for reference:

- *IBM Tivoli Storage Management Concepts*, SG24-4877
- *IBM Tivoli Storage Manager Implementation Guide*, SG24-5416

Perform these steps on your IBM Tivoli Storage Manager server:

1. Define the policy domains, policy sets, management classes, copy groups, and storage pools needed to meet your Data Protection for SQL Server backup and restore requirements. For VSS operations, Tivoli Storage Manager server authentication must be on.
2. Register your Data Protection for SQL Server node name and password with the Tivoli Storage Manager REGISTER NODE command. For example, for VSS operations, this node is the Target Node. When registering nodes to the Tivoli Storage Manager server specifically for VSS operations, do *not* specify the Tivoli Storage Manager `USerid=NONE` parameter. VSS operations fail when this parameter is specified.
3. If not already defined, register your Tivoli Storage Manager backup-archive client node name and password for the machine where the SQL server is installed. For example, for VSS operations, this agent node is the local DSMAgent node.
4. (VSS only.) If you plan to perform offloaded backups, register the Tivoli Storage Manager backup-archive client node name and password for the machine that will perform the VSS offloaded backups.
5. (VSS only.) Define the proxy node relationship (for the target node and agent nodes) with the Tivoli Storage Manager **`GRANT PROXYNODE`** command.

3.1.2 Microsoft SQL Server machine configuration

Perform these steps on the machine where the Microsoft SQL Server is installed and running:

1. Specify your Data Protection for SQL Server node name and communication method in the dsm.opt file located (by default) in the Data Protection for SQL installation directory. Additional options are also available. For additional information, see 3.2.9, “Specifying Data Protection for SQL Server options” on page 103.
2. Specify your Data Protection for SQL Server preferences (such as language, date format, and log file) in the tdpsql.cfg file located (by default) in the Data

Protection for SQL installation directory. Use the `set` command or the menu **Edit** → **Configuration** task of the Data Protection for SQL Server GUI. For additional information, see 3.2.10, “Specifying Data Protection for SQL Server preferences” on page 107.

3. Add the Microsoft SQL Server binary path to the PATH statement in the system environment variables.

4. The following additional steps are for VSS only customization:

   a. Specify your VSSPOLICY statement in your Data Protection for SQL Server configuration file. For additional information, see 3.2.10, “Specifying Data Protection for SQL Server preferences” on page 107.

   b. Configure the Tivoli Storage Manager backup-archive client (if it is not already configured). If the backup-archive client is already configured, you can use existing client services. The backup-archive client Setup wizard can guide you through the configuration process (if needed). In the backup-archive client GUI menu, select **Utilities** → **Setup Wizard** → **Help me configure the TSM Backup Archive Client**. Note that the node name for this machine is referred to as the *local DSMAgent node* and is specified with the `localdsmagentnode` parameter in the Data Protection for SQL Server configuration file (tdpsql.cfg by default). For additional information, see “Required node names for VSS offloaded backups” on page 65.

   c. Install and configure the Tivoli Storage Manager Client Acceptor Daemon (CAD) service (if not already installed and configured). You can use an existing client CAD service if one is already installed and configured. The backup-archive client Setup wizard can guide you through the CAD installation process (if needed). In the backup-archive client GUI menu, select **Utilities** → **Setup Wizard** → **Help me configure the TSM Web Client**. Make sure this CAD service is running before proceeding.

   d. Install and configure the Tivoli Storage Manager Remote Client Agent Service (DSMAgent) if it is not already installed and configured. The backup-archive client Setup wizard can guide you through the configuration process. In the backup-archive client GUI menu, select **Utilities** → **Setup Wizard** → **Help me configure the TSM Web Client**. You can use the existing DSMAgent if one is already installed and configured.

   e. Install the Tivoli Storage Manager for Copy Services: Microsoft SQL VSS Integration Module from the product (if it is not already installed).

   f. If you plan to perform VSS Instant Restores, install the Tivoli Storage Manager Copy Services Hardware Devices Snapshot Integration Module from the product (if it is not already installed). Note that a SAN Volume Controller DS6000 or DS8000 storage subsystem is also required to perform VSS Instant Restores.

g. Install and configure a VSS provider. Consult the VSS provider documentation for information regarding configuration of that software. No installation or configuration is required if you are using the default Windows VSS system provider.

h. Define storage space to hold VSS backups that will reside on local shadow volumes. Make sure you define enough space to hold all copies of the VSS backups as designated by your policies. For additional information, see 2.5.1, “Backup policy considerations” on page 60.

3.1.3 VSS offloaded backup configuration

The VSS offloaded backup configuration is necessary when you are working with VSS backups.

Perform these steps on the machine running the offloaded backups:

1. Configure the Tivoli Storage Manager backup-archive client (if it is not already configured). If the backup-archive client is already configured, you can use existing client services. The backup-archive client Setup wizard can guide you through the configuration process (if needed). In the backup-archive client GUI menu, select **Utilities** → **Setup Wizard** → **Help me configure the TSM Backup Archive Client.** Note that the node name for this machine is referred to as the *remote DSMAgent node* and is specified with the `remotedsmagentnode` parameter in the Data Protection for SQL Server configuration file (tdpsql.cfg by default).
2. Install and configure the Tivoli Storage Manager Client Acceptor Daemon (CAD) Service (if not already installed and configured). You can use an existing client CAD service if one is already installed and configured. The backup-archive client Setup wizard can guide you through the CAD installation process (if needed). In the backup-archive client GUI menu, select **Utilities** → **Setup Wizard** → **Help me configure the TSM Web Client**.
3. Install and configure the Tivoli Storage Manager Remote Client Agent Service (DSMAgent). The backup-archive client Setup wizard can guide you through the configuration process. In the backup-archive client GUI menu, select **Utilities** → **Setup Wizard** → **Help me configure the TSM Web Client**.

> **Note:** Microsoft SQL Server does not have to be installed or running on this machine. Only SQL Server management tools are required to be installed on this machine. Check your Microsoft SQL Server documentation for necessary license requirements.

4. Install and configure a VSS provider (if you are not using the default system VSS provider). Consult the VSS provider documentation for information regarding configuration of that software.

3.1.4 Our environment overview

A number of the capabilities of Data Protection for SQL Server are implemented in our lab environment. We can simulate Legacy and VSS backups, as well as fast restore.

Our environment consists of five servers: ZAIRE is our IBM Tivoli Storage Manager server, and COPPER is a standalone SQL server used for Legacy and VSS backups. We also have an Microsoft Cluster Service clustered Microsoft SQL Server environment - consisting of servers LIBRA and LEO. For the VSS offloaded backup server, we have the MOLITO server. We have an IBM System Storage 3582 tape library with two drives.

Figure 3-1 shows our environment.

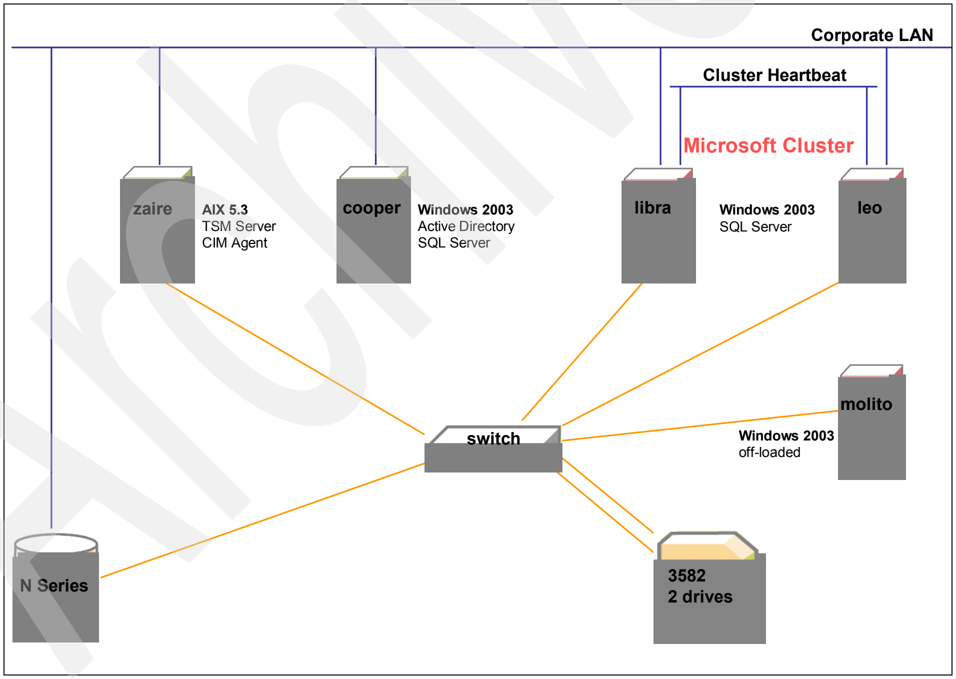

Figure 3-1 LAB environment

In our lab environment we have IBM N series external storage, which hosts the clustered Microsoft SQL Server database environment. This is used as the source for VSS backups. Table 3-2 describes our server's configuration.

Table 3-2 Lab configuration detail

Host name	Purpose	Operating system	IP address	Software installed
ZAIRE	► Tivoli Storage Manager Server	AIX 5.3	9.43.86.22	► IBM Tivoli Storage Manager server
COPPER	► Active Directory ► DNS ► Microsoft SQL Server Legacy backup	Windows 2003	9.43.86.64	► Microsoft SQL Server ► IBM Tivoli Storage Manager client ► Data Protection for SQL Server ► IBM Tivoli Storage Manager for Copy Services
LIBRA	► Microsoft SQL Server node in a cluster environment ► VSS and Legacy backups together	Windows 2003	9.43.86.93	► Microsoft SQL Server ► IBM Tivoli Storage Manager client ► Data Protection for SQL Server ► IBM Tivoli Storage Manager for Copy Services
LEO	► Microsoft SQL Server node in a cluster environment ► VSS and Legacy backup together	Windows 2003	9.43.86.92	► Microsoft SQL Server ► IBM Tivoli Storage Manager client ► Data Protection for SQL Server ► IBM Tivoli Storage Manager for Copy Services
MOLITO	► Offload backup	Windows 2003	9.43.86.95	► IBM Tivoli Storage Manager client ► VSS provider supporting transportable shadow copies ► IBM Tivoli Storage Manager for Copy Services

3.2 Detailed installation and configuration procedure

In the following sections we provide detailed steps to install and configure your environment for Legacy and VSS backups of Microsoft SQL Server.

3.2.1 Verifying name resolution

It is important that all servers in your configuration can correctly perform name resolution, including the IBM Tivoli Storage Manager server. You can check if all machines can connect using both host name and IP address (forward and reverse name resolution).

In our configuration, we have five machines, one AIX and four Windows. COPPER is our DNS server and Active Directory domain controller.

3.2.2 Configuring storage pools

We recommend you set up separate storage pools to back up your Microsoft SQL Server environment. Three storage pools are used in this configuration: one disk storage pool and two tape storage pools. SQLDISKPOOL is the primary storage pool for Microsoft SQL Server backup of transaction logs, and SQLTAPEPOOL is the next storage pool for the SQLDISKPOOL and the primary storage pool for the SQL backup databases. We have another pool, LNGTAPEPOOL, for a long-term retention period. Example 3-1, shows the commands that create these storage pools.

Example 3-1 IBM Tivoli Storage Manager server storage pool definitions

```
tsm: ZAIRE> define stgpool SQLDISKPOOL DISK description=”Backup SQL
Server transaction logs”

tsm: ZAIRE> define stgpool SQLTAPEPOOL LTO2-DC maxscratch=100
reusedelay=1 description=Backup SQL Server Databases”

tsm: ZAIRE>define stgpool lngtapepool LTO2-DC maxscratch=100
reusedelay=1 descri          ption="Backup SQL Server Databases for
Long Term retention"
```

If you are working with VSS backups, we recommend you configure an additional disk storage pool on disk for SQL meta objects. Example 3-2 shows the commands for configuration.

Example 3-2 Additional IBM Tivoli Storage Manager server storage pool definitions

```
tsm: ZAIRE>define stgpool sqlmetapool disk description="Storage Pool
for VSS Bac           kup Metadata"
```

3.2.3 Configuring policy settings

Remember to set up your configuration carefully, considering all requirements for data retention. A policy domain is used in this configuration to back up Microsoft SQL Server databases. We create the following management classes to satisfy our retention requirements:

- SQL_DAILY: This is the management class used for weekly and daily Legacy backups. The retention policy is based on date. If you want to use different backup policies you should create more than one management class.
- SQL_LONG: This is the management class used for Legacy long-term backups. It is enforced by date policy, and in our example, we create this management class to retain monthly backups.
- SQL_LOGS: This is the management class used to back up SQL transaction logs.

If you are working with VSS backups, we recommend you configure additional management classes:

- VSS_LOCAL: This is the management class used for *local* VSS backups. Usually you can perform several local backups per day. The retention policy should be enforced by version instead of time, because you must ensure that you have enough disk space to hold all your required snapshots. In this case we specify `VEREXISTS=3`. The copy group destination points to a small disk storage pool. This is because even though the VSS backup itself does not use the IBM Tivoli Storage Manager space pool, some backup metadata is stored in a storage pool. We recommend you configure a disk pool only, with no migration to tape, to ensure that the metada can be quickly accessed in the event of a restore.
- VSS_FULL_TSM: This is the management class used for daily VSS backups that are sent to IBM Tivoli Storage Manager. This kind of backup uses only one non-persistent (temporary) snapshot to send the data to the IBM Tivoli Storage Manager server. Therefore, you must ensure that you always have the required disk space for this snapshot. If you perform your backup destination with `both`, the target set is used for both backups, local and IBM

Tivoli Storage Manager. The retention policy for backups to IBM Tivoli Storage Manager should be enforced by time period; in this case, we configure 30 days, `VEREXISTS=NOLIMIT` and `RETEXTRA=30`.

Example 3-3 shows the commands that configure these policy requirements.

Example 3-3 Define policy requirements for Microsoft SQL Server backups

```
tsm: ZAIRE>define domain pdsql description="SQL Server Policy Domain"

tsm: ZAIRE>define policyset pdsql pssql description="SQL Server Policy
Set"

tsm: ZAIRE>define mgmtclass pdsql pssql sql_daily description="SQL
Server daily Backups"

tsm: ZAIRE>define mgmtclass pdsql pssql sql_LONG description="SQL
Server Long Tr em backups"

tsm: ZAIRE>define mgmtclass pdsql pssql sql_logs description="SQL
Server transac ation logs"

tsm: ZAIRE>define copygroup pdsql pssql sql_daily type=backup
destination=sqltap epool verexists=nolimit verdeleted=nolimit
retextra=30 retonly=30

tsm: ZAIRE>define copygroup pdsql pssql sql_logs type=backup
destination=sqldisk pool verexists=nolimit verdeleted=nolimit
retextra=30 retonly=30

tsm: ZAIRE>assign defmgmtclass PDSQL PSSQL SQL_DAILY

tsm: ZAIRE>validate policyset PDSQL PSSQL

tsm: ZAIRE>activate policyset PDSQL PSSQL
```

Example 3-4 shows the additional configuration necessary to enable VSS backups.

Example 3-4 Additional policy requirements for Microsoft SQL Server backups

```
tsm: ZAIRE>define mgmtclass pdsql pssql VSS_LOCAl description="VSS
Local Mgmtcla ss"

tsm: ZAIRE>define mgmtclass pdsql pssql VSS_FULL_TSM description="VSS
Full Mgmtc lass"
```

```
tsm: ZAIRE>define mgmtclass pdsql pssql VSS_LONG_TSM description="VSS
Copy Mgmtc lass"

tsm: ZAIRE>define copygroup pdsql pssql vss_local type=backup
destination=sqlmet apool verexists=3 verdeleted=3 retextra=nolimit
retonly=nolimit

tsm: ZAIRE>define copygroup pdsql pssql vss_full_tsm type=backup
destination=sql tapepool verexists=nolimit verdeleted=nolimit
retextra=30 retonly=30

tsm: ZAIRE>define copygroup pdsql pssql vss_copy_tsm type=backup
destination=lng tapepool verexists=nolimit verdeleted=nolimit
retextra=365 retonly=365

tsm: ZAIRE>assign defmgmtclass PDSQL PSSQL VSS_LOCAL

tsm: ZAIRE>validate policyset PDSQL PSSQL

tsm: ZAIRE>activate policyset PDSQL PSSQL
```

3.2.4 Configuring node names

At this time you must register the nodes on the IBM Tivoli Storage Manager server. Example 3-5 shows how to configure a node to use just Legacy backups. We register one node for each of our SQL servers.

Example 3-5 Node configuration for Legacy backups

```
tsm: ZAIRE>register node copper_sql copper domain=pdsql

tsm: ZAIRE>register node clussql01_daily <password> domain=pdsql

tsm: ZAIRE>register node clussql01_long <password> domain=pdsql
```

Example 3-6 shows how to configure a node to work with VSS backups and Legacy backups together.

Example 3-6 Node configuration for VSS and Legacy backups together

```
tsm: ZAIRE>register node copper_vss <password> domain=pdsql

tsm: ZAIRE>register node libra_vss <password> domain=pdsql
```

```
tsm: ZAIRE>register node leo_vss <password> domain=pdsql
```

Example 3-7 shows how to configure a node to perform offloaded VSS backups.

Example 3-7 Node configuration for offloaded backups

```
tsm: ZAIRE>register node molito_offload <password> domain=pdsql
```

3.2.5 Installing the backup-archive client code

Install the IBM Tivoli Storage Manager backup-archive client at V5.5 or later on all machines that will participate in the backup of Microsoft SQL Server. In our environment we have four servers where we install the backup-archive client. The server COPPER is a standalone SQL server and will perform both Legacy and VSS backups. Servers LEO and LIBRA performs both VSS and Legacy backups together in a cluster environment. The server MOLITO will act as a VSS offloaded server.

In a cluster environment, you must install the IBM Tivoli Storage Manager backup-archive client on both machines.

Refer to the client installation documentation for detailed instructions. You may choose Custom installation to select additional components and features, such as Open Files support, Image backup support, and more.

If these features are not required, we recommend you choose Typical installation to ensure that all Tivoli Storage Manager basic client components and prerequisites are installed. You may install the remaining features later, when required.

To install the IBM Tivoli Storage Manager backup-archive client, follow these steps:

1. Insert the product installation CD. Double-click the IBM Tivoli Storage Manager backup-archive client installer icon.

> **Note:** If you do not have the CD and have downloaded the software from the IBM Passport Advantage® Web site, simply double-click the IBM Tivoli Storage Manager backup-archive client executable file (ending with .exe), and you are directed to the windows shown in this section.

2. Select **Install Products** on the Main Menu, as shown in Figure 3-2.

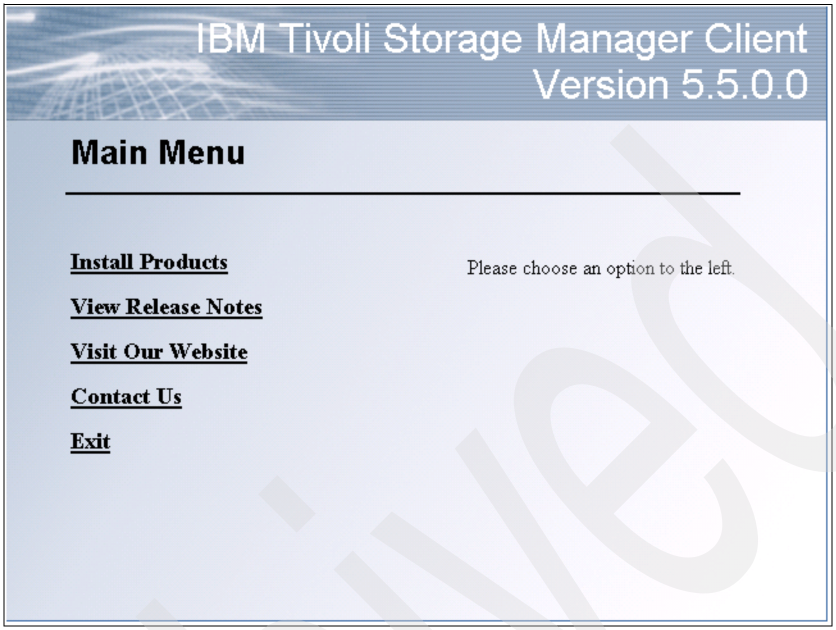

Figure 3-2 IBM Tivoli Storage Manager client Main Menu

3. Select **TSM Backup-archive Client - x32**, as shown in Figure 3-3.

Figure 3-3   Install TSM Backup archive Client

4. Select a language for the installation, as shown in Figure 3-4. We select English language in our installation.

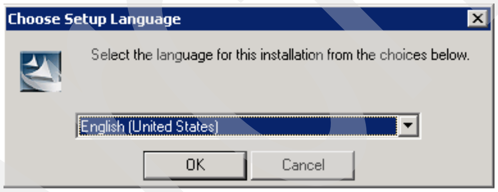

Figure 3-4   Select language for installation

5. Click **Next** in the installation wizard welcome window, as shown in Figure 3-5.

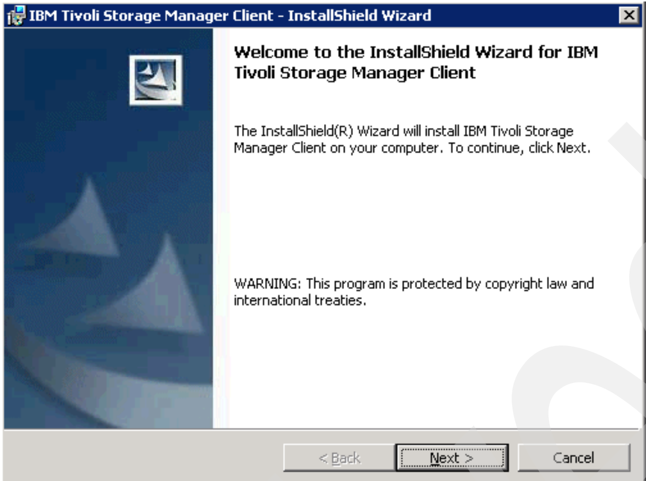

Figure 3-5 InstallShield Wizard welcome

6. Accept the license agreement and click **Next**.
7. Select the destination folder to install the package and click **Next**. We use the default installation directory C:\PROGRAM FILES\TIVOLI\TSM\BACLIENT (see Figure 3-6).

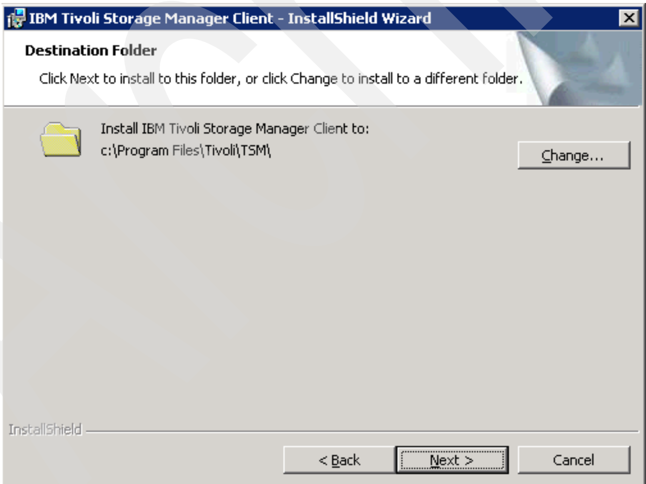

Figure 3-6 IBM Tivoli Storage Manager backup-archive client installation code

8. Select **Setup Type**. We choose Custom setup so that we can also install the Administrative Client command-line files (see Figure 3-7). Click **Next**.

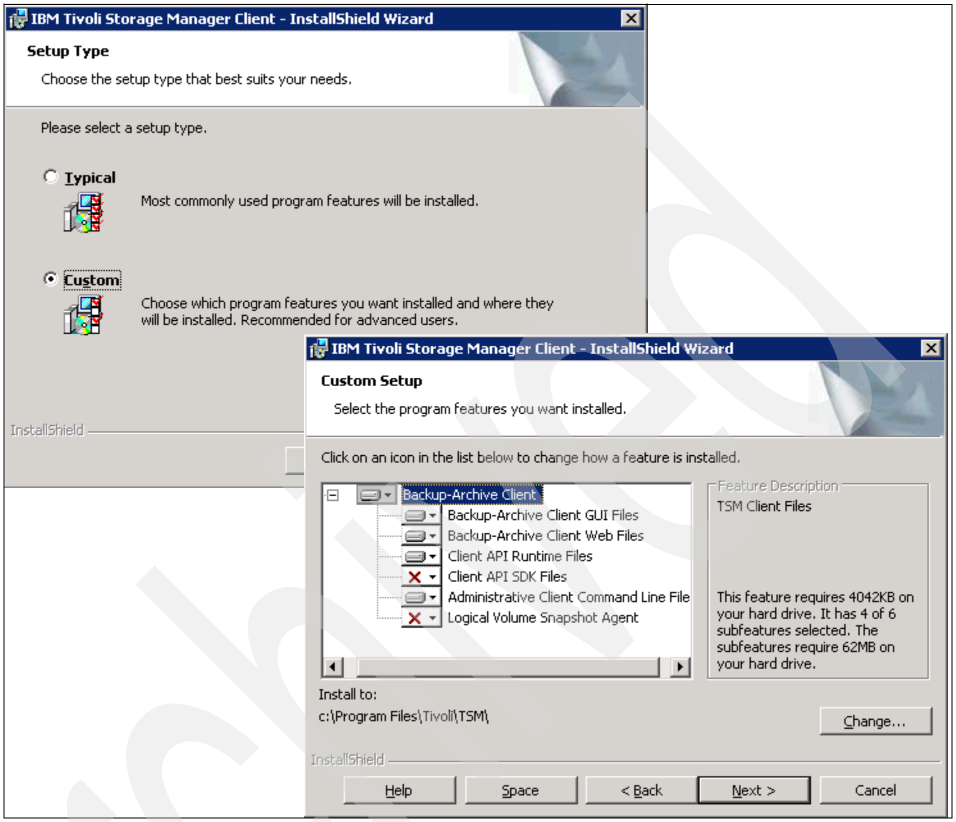

Figure 3-7 Select setup type

9. Click **Install** to start the installation (see Figure 3-8).

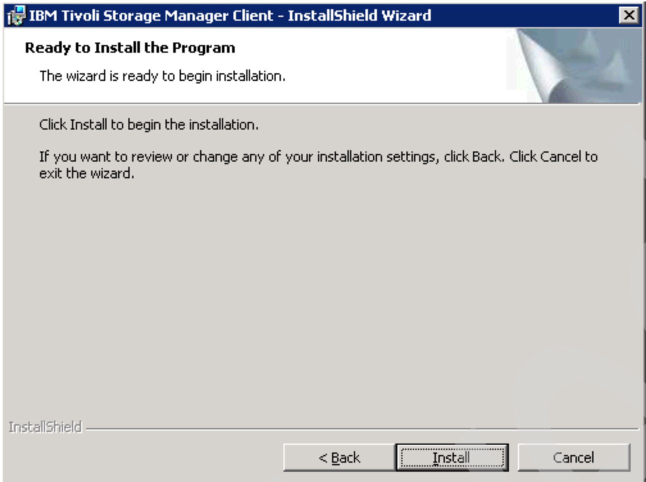

Figure 3-8 Ready to install program

10. If the installation completes successfully, click **Finish** (see Figure 3-9).

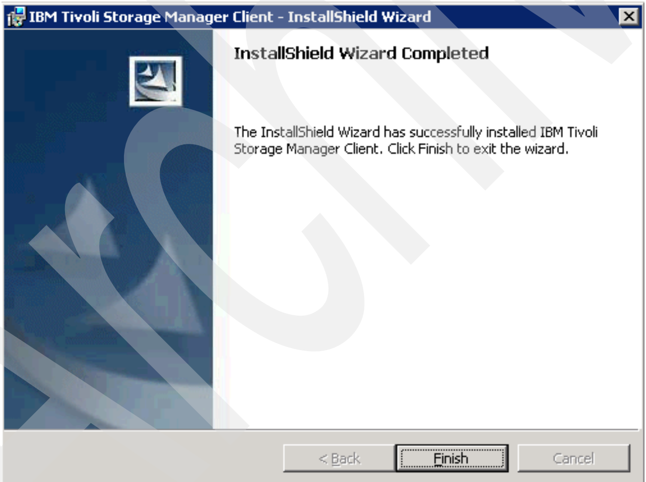

Figure 3-9 IBM Tivoli Storage Manager backup-archive client completed successfully

After the client installs, verify that the VSS Snapshot plug-in pivss.dll exists in the BACLIENT\PLUGINS directory (C:\PROGRAM FILES\TIVOLI\TSM\BACLIENT\PLUGINS).

Installing language packs - X32

You can install additional language packs to provide messages in a language other than English. You can choose the option **Language Packs - X32** (see Figure 3-10), followed by **Main Menu**, to see which languages you can install.

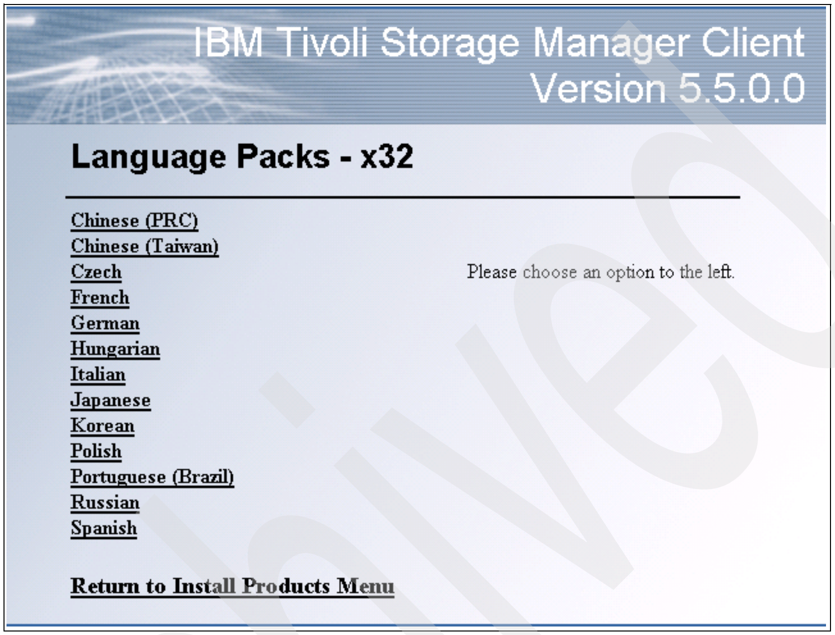

Figure 3-10 Language Packs - X32

3.2.6 Installing the Data Protection for SQL Server code

Install Data Protection for SQL Server at V5.5 or later on all machines that will participate in the Microsoft SQL Server backup. In a cluster environment, you must install Data Protection for SQL Server on both nodes. If you have an Active/Active SQL server cluster environment, you should create a Start Menu shortcut for each virtual SQL server that can run on this machine.

To install Data Protection for SQL Server, follow these steps:

1. Insert the product installation CD. Double-click the Data Protection for SQL Server installer icon.

> **Note:** If you do not have the CD and have downloaded the software from the IBM Passport Advantage Web site, simply double-click the Data Protection for SQL Server client executable file (ending with .exe), and you are directed to the windows that follow.

2. Select a language for the installation, as shown in Figure 3-11. We choose English.

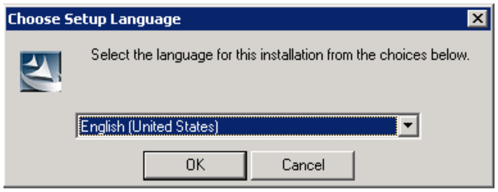

Figure 3-11 Select language for installation

3. Click **Next** in the installation wizard welcome, as shown in Figure 3-12.

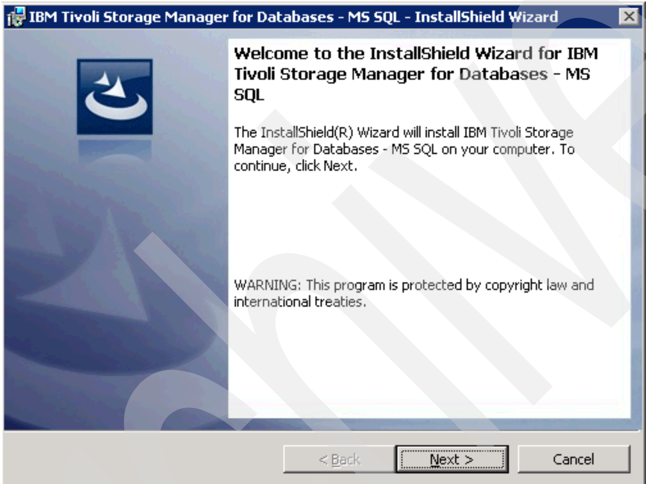

Figure 3-12 InstallShield Wizard welcome

4. Accept the license agreement and click **Next**.

5. Select the destination folder to install the package and click **Next**. We use the default installation directory C:\PROGRAM FILES\TIVOLI\TSM (see Figure 3-13).

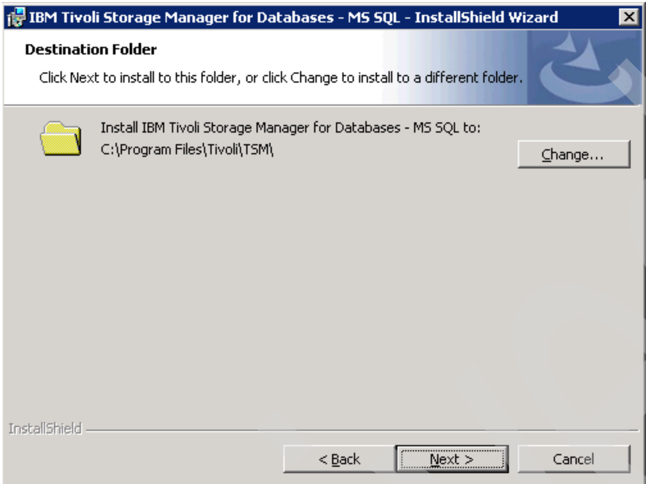

Figure 3-13   Data Protection for SQL Server installation code

6. Click **Install** to start the installation (see Figure 3-14).

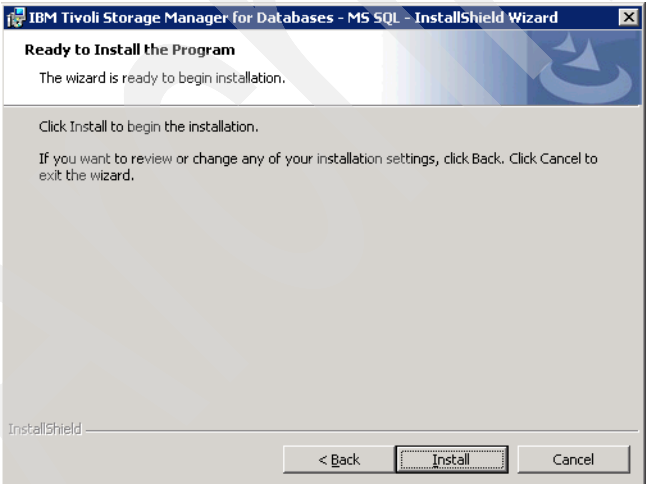

Figure 3-14   Ready to install program

7. If the installation completes successfully, click **Finish** (see Figure 3-15.

Figure 3-15 Data Protection for SQL Server installed successfully

If you want to use the Silent Installation, refer to the *IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server Installation and User's Guide*, SC32-9059, for reference.

Installing Data Protection for SQL Server additional language packs

You can install additional language packs to provide messages in a language other than English. The language packs are additional executable files provided with product CD-ROM. The files are located in the TDPSql\x32\languages directory on the product CD-ROM. You can choose a directory with a three-letter country code associated with the language you want to install. You have the following languages available:

- chs: Chinese Simplified
- cht: Chinese Traditional
- deu: Standard German
- esp: Standard Spanish
- fra: Standard French
- ita: Standard Italian
- jpn: Japanese
- kor: Korean
- ptb: Brazilian Portuguese

3.2.7 Installing Copy Services code and hardware integration module

Install the Copy Services code at V5.5 or later on all machines that will participate in the Microsoft SQL Server VSS backups.

IBM Tivoli Storage Manager for Copy Services actually consists of two modules: Microsoft SQL Server VSS Integration Module and Hardware Devices Snapshot Integration Module. The first module is required in all configurations for VSS backup. The Hardware Devices Snapshot Integration Module is required only if you are using disk storage that supports Instant Restore.

Install Copy Services code

To install Copy Services, follow these steps:

1. In the directory TDPSql\x32\plugin, run setup.exe.

> **Note:** If you do not have the CD and have downloaded the software from the IBM Passport Advantage Web site, simply double-click the Copy Services executable file (ending with .exe), and you are directed to the discussed in this section.

2. Select a language for the installation, as shown in Figure 3-16. We choose the English language in our installation.

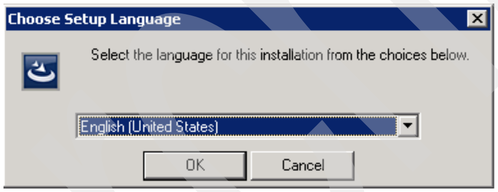

Figure 3-16 Select language for installation

3. Click **Next** in the installation wizard welcome, shown in Figure 3-17.

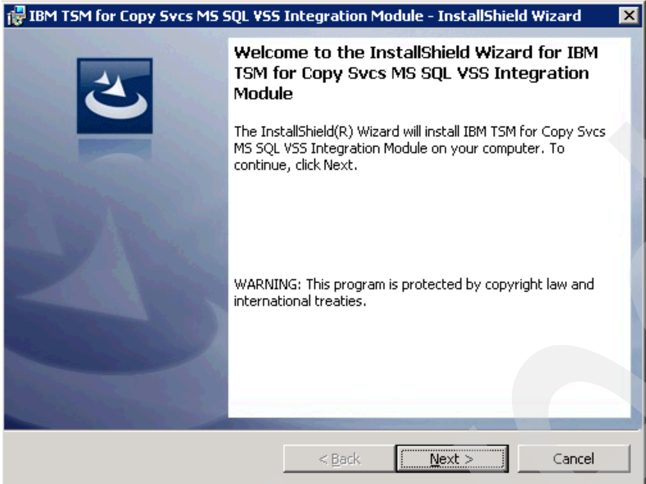

Figure 3-17 InstallShield Wizard welcome

4. Accept the license agreement and click **Next**.
5. Click **Install** to start the installation (see Figure 3-18).

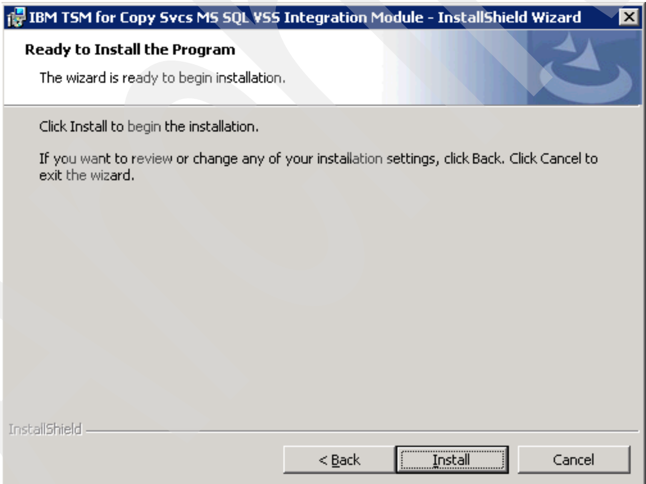

Figure 3-18 Ready to install program

6. If the installation completes successfully, click **Finish** (see Figure 3-19).

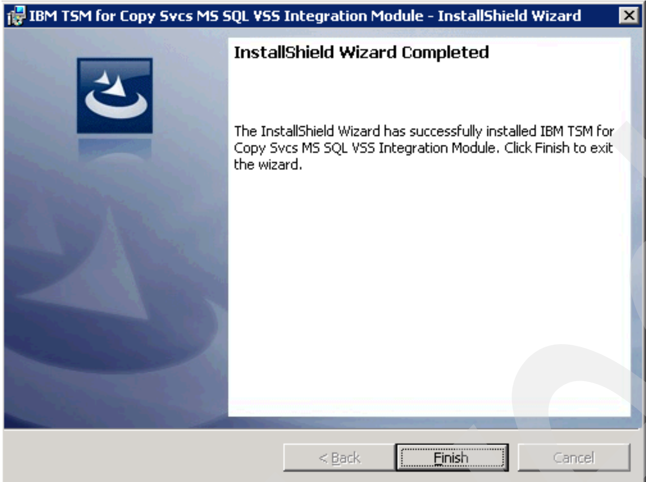

Figure 3-19 Copy Services installed successfully

Install the Hardware Device Snapshot integration module

To install Copy Services, follow these steps:

1. In the directory tsmcli\x32\plugin, run setup.exe.

> **Note:** If you do not have the CD and have downloaded the software from the IBM Passport Advantage Web site, simply double-click the Copy Services executable file (ending with .exe), and you are directed to the windows discussed in this section.

2. Select a language for the installation, as show in Figure 3-20. We choose the English language.

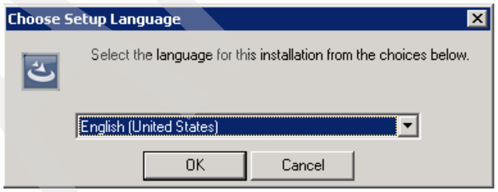

Figure 3-20 Select language for installation

3. Click **Next** in the installation wizard welcome, shown in Figure 3-21.

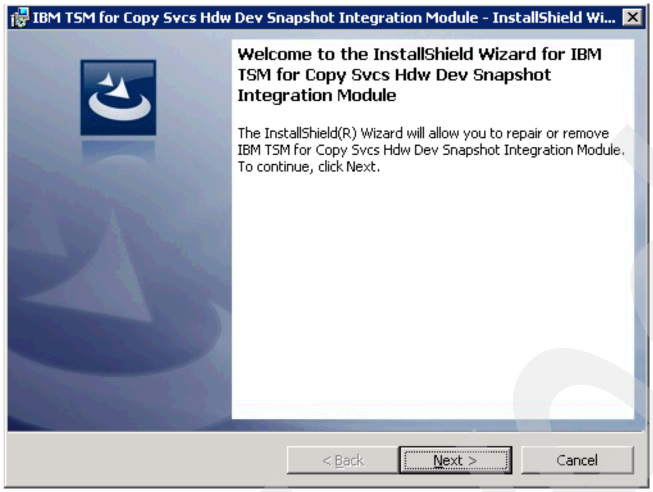

Figure 3-21 InstallShield Wizard welcome

4. Accept the license agreement and click **Next**.
5. Click **Install**, to start the installation (see Figure 3-22).

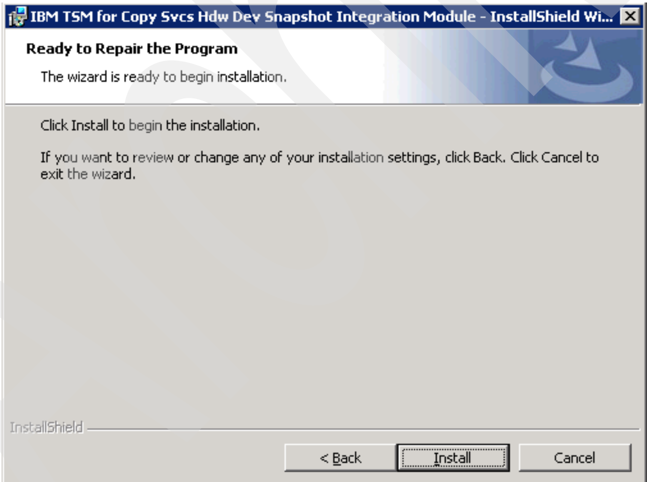

Figure 3-22 Ready to install program

6. If the installation completes successfully, click **Finish** (see Figure 3-23).

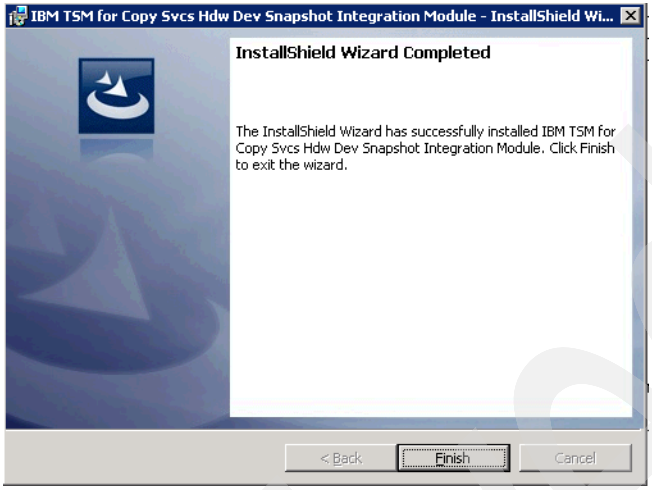

Figure 3-23 Hardware Snapshot Integration Module installed successfully

3.2.8 Specifying backup-archive client options

If you are using VSS backups, the SQL server node requires an IBM Tivoli Storage Manager backup-archive client node (DSMAgent) with an associated options file. The standard options file, dsm.opt, is located in the installation directory (C:\Program files\tivoli\TSM\baclient).

> **Note:** If you are using only Legacy backups, these steps are not necessary.

Configuring the backup-archive options file in a standalone environment

The machine COPPER is a standalone SQL server in our lab configuration. The node copper_vss was created to act as DSMAgent. This node has an associated options file. See Example 3-8.

Example 3-8 Backup-archive options file for a standalone machine configuration

```
NODename          copper_vss
CLUSTERnode       NO
PASSWORDAccess    generate
```

```
COMMMethod        TCPip
TCPServeraddress  9.43.86.45
TCPPort           1500
TCPWindowsize     63
TCPBuffSize       32
TCPCLIENTADDRESS 9.43.86.64
managedservices webclient
```

We created options file dsm_vss.opt in the client installation directory, rather than the default options file dsm.opt. We recommend creating a shortcut for the backup-archive GUI, which points to the actual options file. Follow these steps to create a shortcut:

1. On your Windows desktop, click the right mouse button and select **New** → **Shortcut**. The Create Shortcut window appears (see Figure 3-24).

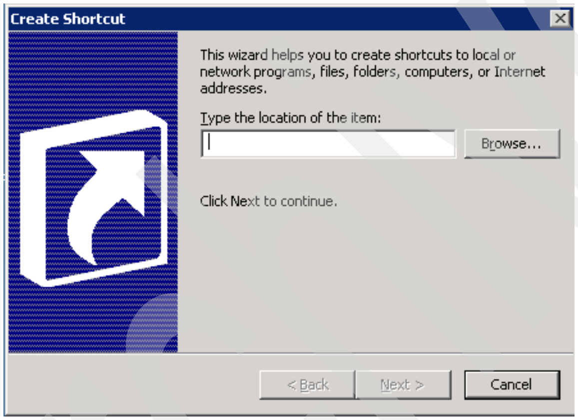

Figure 3-24   Create a shortcut

2. Select the binary files c:\program files\tivoli\tsm\baclient\dsm.exe and include the options file. In our example, the full string is "C:\Program Files\Tivoli\TSM\baclient\dsm.exe" -optfile="C:\Program Files\Tivoli\TSM\baclient\dsm_vss.opt". Click **Next**. See Figure 3-25.

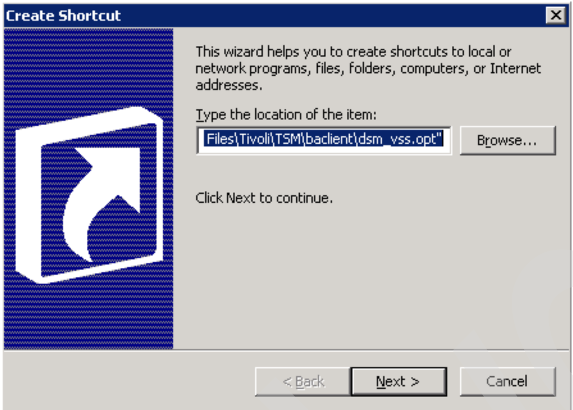

Figure 3-25 Select options file

3. Select a name for the shortcut and click **Finish**. See Figure 3-26:

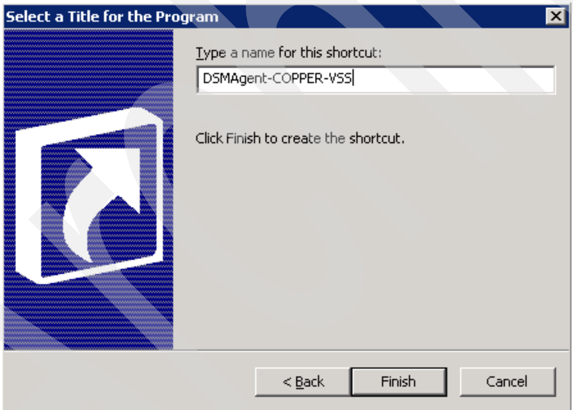

Figure 3-26 Select a name for shortcut

A shortcut is now created in your Windows desktop. It is necessary to launch the backup-archive GUI using the shortcut to store the encrypted password in the registry, because we specified `PASSWORDACCESS GENERATE` in the options file. If you change this password, you need to run the backup-archive GUI again and revalidate the password.

Alternatively, you can use the command-line interface to perform this step, as shown in Example 3-9.

Example 3-9 Using command-line interface to store encrypted password

```
C:\Program Files\Tivoli\TSM\baclient>dsmc -optfile="c:\program
files\tivoli\tsm\
baclient\dsm_vss.opt"
IBM Tivoli Storage Manager
Command Line Backup/Archive Client Interface
  Client Version 5, Release 5, Level 0.0 0827FA
  Client date/time: 10/14/2007 18:02:05
(c) Copyright by IBM Corporation and other(s) 1990, 2007. All Rights
Reserved.

Node Name: COPPER_VSS
Session established with server ZAIRE: AIX-RS/6000
  Server Version 5, Release 4, Level 0.0
  Server date/time: 10/14/2007 16:01:32  Last access: 10/14/2007
16:00:56

tsm>
```

Configuring the backup-archive options file in a clustered environment

The servers LIBRA and LEO are part of our lab cluster environment. We created the nodes libra_vss and leo_vss to act as DSMAgents. Each node has an associated option file. We recommend you store the options file on a shared disk device in a cluster environment. You can maintain the configuration files on each server's local disk, but you need to remember that any modification must be replicated to other cluster machines.

When you have a cluster environment and plan to make local VSS backups, you must configure the parameter `VSSALTSTAGINGIDIR` in the DSMAgent option file. This parameter is used to specify a location to store VSS manager files on a shared volume. It should point to a shared device that does not contain any SQL server objects. See Example 3-10 and Example 3-11 on page 103.

Example 3-10 Backup-archive options file for local DSMAgent node for machine Libra

```
NODename          libra_vss
PASSWORDAccess    generate
vssaltstagingdir f:\tsmvssdir

COMMMethod        TCPip
```

```
TCPServeraddress  9.43.86.45
TCPPort           1500
TCPWindowsize     63
TCPBuffSize       32
TCPCLIENTADDRESS 9.43.86.64
clusternode no
clusterdisksonly no
managedservices webclient
```

Example 3-11 Backup-archive options file for local DSMAgent node for machine Leo

```
NODename          leo_vss
PASSWORDAccess    generate
vssaltstagingdir f:\tsmvssdir

COMMMethod        TCPip
TCPServeraddress  9.43.86.45
TCPPort           1500
TCPWindowsize     63
TCPBuffSize       32
TCPCLIENTADDRESS 9.43.86.64
clusternode no
clusterdisksonly no
managedservices webclient
```

> **Note:** We recommend that the local DSMAgent client node be a separate node from your normal backup-archive client, because this CAD service must be made a non-cluster option. Thus, be sure to specify the following options “clusternode no” and “clusterdiskonly no” in each of the dsm.opt files that are used for the local DSMAgent.

3.2.9 Specifying Data Protection for SQL Server options

Once Data Protection for SQL Server is registered to a Tivoli Storage Manager server, several Data Protection for SQL Server parameters must be configured. The Tivoli Storage Manager administrator should have provided you with the node name, password, and the communications method with the appropriate parameters for connecting to the Tivoli Storage Manager server. These values, together with other parameters, are stored in an options file in the Data Protection for SQL Server directory. The default options file name is dsm.opt; it can be edited with a standard text editor. The options file includes the following parameters, which are required for initial configuration.

Nodename

The Tivoli Storage Manager nodename is the unique name by which Tivoli Storage Manager knows the machine running Data Protection for SQL Server.

Servername

This is the name of the Tivoli Storage Manager server to which you back up SQL Server databases.

Commmethod

The communication protocols link the Data Protection for SQL Server node with the Tivoli Storage Manager server. Data Protection for SQL Server supports the same set of communication protocols supported by other Tivoli Storage Manager clients.

Passwordaccess

When set to the value `GENERATE`, this instructs the Tivoli Storage Manager API to store the current password (encrypted) in the Windows registry and automatically generate a new one when the current one expires. We recommend this method of password management when you are running scheduled, unattended backups because it ensures that the backup never fails because of an expired password. The default value is `PROMPT`. A utility program dsmcutil.exe enables you to manage (update or display) the password as stored in the registry. This utility program is distributed with the Tivoli Storage Manager backup-archive client package. For more information about using the dsmcutil program, see the dsmcutil.hlp file or the dsmcutil.txt file, which are distributed with the Tivoli Storage Manager Backup-Archive Client package.

Compression

A setting of `COMPRESSION ON` instructs the Tivoli Storage Manager API to compress data before sending it to the Tivoli Storage Manager server; this reduces traffic and storage requirements.

Clusternode

A setting of `CLUSTERNODE YES` directs the Tivoli Storage Manager API and Data Protection for SQL Server to be cluster-aware when running in a MSCS or VCS environment. This option *must* be specified for Data Protection for SQL Server to function properly in a MSCS or VCS environment.

Enablelanfree

A setting of `ENABLELANFREE YES` allows Data Protection for SQL Server to run in a LAN-free environment if you are equipped to do so.

> **Note:** If you are running Data Protection for SQL Server in a MSCS environment, the options file on both nodes of the cluster must be identical, including the node name.
>
> You can create additional Data Protection for SQL Server options files to point to other IBM Tivoli Storage Manager servers.

Configuring the Data Protection for SQL Server options file in a standalone environment

In a non-clustered environment, you can use the default standard name and location (C:\Program Files\Tivoli\TSM\TDPSql\dsm.opt). In our case we have two different backup policies configured: one for daily backups and another one for monthly backups. For this scenario, it is necessary to have a different options file for each type of retention policy with an associated node name.

With Data Protection for SQL Server, you can utilize Tivoli Storage Manager automatic expiration and version control by setting policies. Setting automatic policy for backup data is accomplished through the Data Protection for SQL Server options file. Use `include` and `exclude` statements in the options file to define which files are subject to automatic processing and to assign specific management classes to files using object-naming conventions.

See Example 3-12 for Daily Backups and Example 3-13 on page 106 for monthly backups.

Example 3-12 Options file for daily SQL backups in standalone environment

```
NODename          copper_sql
CLUSTERnode       NO
PASSWORDAccess    generate
password copper
COMMMethod        TCPip
TCPServeraddress  9.43.86.45
TCPPort           1500
TCPWindowsize     63
TCPBuffSize       32
COMPRESSIon       NO
SCHEDMODE             Prompt

INCLUDE "\...\meta\...\*"     SQL_DAILY
INCLUDE "\...\data\...\*"     SQL_DAILY

INCLUlDE "\...\meta\...\log*"  SQL_LOGS
INCLUDE "\...\data\...\log*"  SQL_LOGS
```

```
EXCLUDE "\...\master\...\log*"
EXCLUDE "\...\msdb\...\log*"
```

Example 3-13 Options file for monthly SQL backups in standalone environment

```
NODename          copper_lng
CLUSTERnode       NO
PASSWORDAccess    generate
password copper
COMMMethod        TCPip
TCPServeraddress  9.43.86.45
TCPPort           1500
TCPWindowsize     63
TCPBuffSize       32
COMPRESSIon       NO
SCHEDMODE             Prompt

INCLUDE "\...\meta\...\*"     SQL_LONG
INCLUDE "\...\data\...\*"     SQL_LONG

EXCLUDE "\...\master\...\log*"
EXCLUDE "\...\msdb\...\log*"
```

Configuring the Data Protection for SQL Server options file in a clustered environment

In a clustered environment, the Data Protection for SQL Server options file must be accessible from both nodes. You can use a directory in an external disk to store this file. This directory must be in the cluster configuration to fail over with the SQL server instance. You can use automatic expiration in a clustered environment, the same as you can in a standalone configuration. So, if you have different backup policies for Legacy backups, you need to create a different options file. We must specify that we are in a cluster environment, so we specify the parameter `CLUSTERNODE yes`.

See Example 3-14 for a daily backup example and Example 3-15 on page 107 for a monthly backup example.

Example 3-14 Options file for daily SQL backups in clustered environment

```
NODename          clussql01_daily
CLUSTERnode       Yes
PASSWORDAccess    generate
password mssqldb
COMMMethod        TCPip
```

```
TCPServeraddress  9.43.86.45
TCPPort           1500
TCPWindowsize     63
TCPBuffSize       32
COMPRESSIon       NO
SCHEDMODE             Prompt

INCLUDE "\...\meta\...\*"     SQL_DAILY
INCLUDE "\...\data\...\*"     SQL_DAILY

INCLUDE "\...\meta\...\log*"  SQL_LOGS
INCLUDE "\...\data\...\log*"  SQL_LOGS

EXCLUDE "\...\master\...\log*"
EXCLUDE "\...\msdb\...\log*"
```

Example 3-15 Options file for monthly SQL backups in clustered environment

```
NODename          clussql01_lng
CLUSTERnode       Yes
PASSWORDAccess    generate
password copper
COMMMethod        TCPip
TCPServeraddress  9.43.86.45
TCPPort           1500
TCPWindowsize     63
TCPBuffSize       32
COMPRESSIon       NO
SCHEDMODE             Prompt

INCLUDE "\...\meta\...\*"     SQL_LONG
INCLUDE "\...\data\...\*"     SQL_LONG

EXCLUDE "\...\master\...\log*"

EXCLUDE "\...\msdb\...\log*"
```

3.2.10 Specifying Data Protection for SQL Server preferences

You define Data Protection for SQL Server configuration parameters in the Data Protection for SQL Server configuration file (tdpsql.cfg by default). These configuration parameters determine such preferences as the location of your log file, how date and time stamps display, and the number of buffers to use. You can set the values of the Data Protection for SQL Server configuration parameters in two ways:

- Using the menu **Edit** → **Configuration** of the Data Protection for SQL Server GUI.
- Using the `tdpsqlc set` command in the Data Protection for SQL Server command-line interface.

Note the following characteristics of Data Protection for SQL Server configuration parameters:

- The value of a configuration parameter specified on a command-line invocation overrides (but does not change) the value of the configuration parameter specified in the Data Protection for SQL Server configuration file.
- During a command-line invocation that does not specify an overriding value for a configuration file parameter, the values in the default Data Protection for SQL Server configuration file (tdpsql.cfg) are used.

Set the policy for VSS backups by specifying the VSSPOLICY statement in your Data Protection for SQL Server configuration file. You set this parameter only in the configuration file - it cannot be specified using the `tdpsqlc set` command or the menu **Edit** → **Configuration** task of the Data Protection for SQL Server GUI.

VSSPOLICY statements are processed from the bottom up and processing stops at the first match. To ensure that more specific specifications are processed at all, the more general specification should be listed before the more specific ones, so as to be processed after the more specific specifications. Otherwise, the more general specification matches the target before the more specific specifications are seen.

By default, Microsoft SQL Server accepts connections on TCP/IP port 1433. If SQL Server is configured to listen on a TCP/IP port different than 1433, you must specify the TCP/IP port for the parameters `SQLSERVer` and `FROMSQLserver`. Example 3-16 shows how to configure Tivoli Data Protection for SQL Server to access the instance SQL_STDBY on server COPPER using port 5555.

Example 3-16 TDPSQL.cfg parameter file for Microsoft SQL Server with non-default port

```
SQLSERVer        COPPER\SQL_STDBY,5555
FROMSQLserver    COPPER\SQL_STDBY,5555
```

If you do not specify the TCP/IP port when accessing a Microsoft SQL Server instance listening on a non-default port, you receive an error message similar to Figure 3-27.

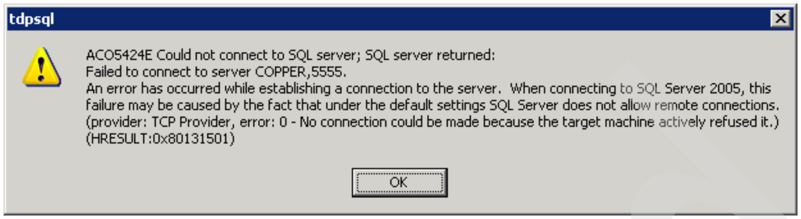

Figure 3-27 Tivoli Data Protection for SQL Server connection error

> **Note:** This error can occur when you install Microsoft SQL Server 2000 and 2005 on the same machine. In our tests, we installed Microsoft SQL Server 2000 first and then SQL Server 2005. Although SQL Server tools were able to connect to both SQL Server installations, Tivoli Data Protection for SQL Server was able to connect only to the SQL server listening on port 1433. To resolve this issue, it was necessary to include in the TDPSQL.cfg configuration file the port that SQL server was listening on.
>
> You can verify the port that the SQL server is listening on, using Microsoft SQL Server tools, such as the Server Network utility for SQL Server 2000 or SQL Server Configuration Manager for SQL Server 2005. Another way to verify this information is to check the SQL server error log.

Configuring Data Protection preferences in a standalone environment

In a non-clustered environment, you can configure the preferences in the default preferences files located on C:\Program Files\Tivoli\TSM\TDPSQL\tdpsql.cfg. If you have more than one backup policy, you can create different preferences files. See Example 3-17 and Example 3-18 on page 110.

Example 3-17 Data Protection for SQL Server configuration file for daily backups (tdpsql_daily.cfg)

```
SQLSERVer     COPPER
FROMSQLserver     COPPER
SQLAUTHentication     INTegrated
nodename copper_sql
MOUNTWaitfordata     Yes
BACKUPMethod     LEGACY
DIFFESTimate     20
```

```
BUFFers     3
BUFFERSIze     1024
STRIPes     1
SQLBUFFers     0
SQLBUFFERSIze     1024
LOGPrune     60
LANGuage     ENU
BACKUPDestination     Both
LOCALDSMAgentnode     copper_vss
REMOTEDSMAgentnode
********** Server Storage Group Name BU Type BU Dest. Mgmt Class
********** ------ ------------------ ------- -------- ----------
VSSPOLICY  *      *                  FULL    TSM      VSS_FULL_TSM
VSSPOLICY  *      *                  LOCAL   LOCAL    VSS_LOCAL
```

Example 3-18 Data Protection for SQL Server configuration file for monthly backups (tdpsql_long.cfg)

```
SQLSERVer     COPPER
FROMSQLserver     COPPER
SQLAUTHentication     INTegrated
nodename copper_lng
MOUNTWaitfordata     Yes
BACKUPMethod     LEGACY
DIFFESTimate     20
BUFFers     3
BUFFERSIze     1024
STRIPes     1
SQLBUFFers     0
SQLBUFFERSIze     1024
LOGPrune     60
LANGuage     ENU
BACKUPDestination     TSM
LOCALDSMAgentnode     copper_vss
REMOTEDSMAgentnode
********** Server Storage Group Name BU Type BU Dest. Mgmt Class
********** ------ ------------------ ------- -------- ----------
VSSPOLICY  *      *                  FULL    TSM      VSS_LONG_TSM
```

We recommend creating a shortcut for the Data Protection for SQL Server GUI pointing to each options file. You can follow the steps 1 on page 100 through 3 on page 101 described starting on page 100 to create the shortcuts.

To create shortcuts for daily and monthly backups, you must specify the options file and configuration file. See Example 3-19 and Example 3-20.

Example 3-19 Shortcut definition for daily SQL backup

```
"C:\Program Files\Tivoli\TSM\TDPSql\tdpsql.exe" /tsmoptfile="C:\Program
Files\Tivoli\TSM\TDPSql\dsm_daily.opt" /configfile="C:\Program
Files\Tivoli\TSM\TDPSql\tdpsql_daily.cfg"
```

Example 3-20 Shortcut definition for monthly SQL backup

```
"C:\Program Files\Tivoli\TSM\TDPSql\tdpsql.exe" /tsmoptfile="C:\Program
Files\Tivoli\TSM\TDPSql\dsm_long.opt" /configfile="C:\Program
Files\Tivoli\TSM\TDPSql\tdpsql_long.cfg"
```

Configuring Data Protection for SQL Server preferences in a clustered environment

In a clustered environment, we created the DSMAgent options file for each node in a cluster was created. At this point, it is necessary to configure Data Protection for SQL Server preferences for each node in the cluster. You can use a directory in an external disk and configure both files, one for each node in the cluster. You need to match the corresponding local DSMAgent node according to the specific machine in the cluster.

If you are using an offloaded backup server, it is necessary to configure the remote DSMAgent node pointing to your offloaded node. This parameter is required only if you are using an offloaded backup server.

This configuration also contains the VSSPOLICY statements, so if you have more than one backup policy, it is necessary to specify more than one configuration. See Example 3-21, Example 3-22 on page 112, Example 3-23 on page 112, and Example 3-24 on page 113.

Example 3-21 Data Protection for SQL Server configuration file for daily backups (tdpsql_libra_daily.cfg)

```
SQLSERVer     CLUSQL01\SQL01
FROMSQLserver CLUSQL01\SQL01
SQLAUTHentication     INTegrated
nodename CLUSQL01_Daily
MOUNTWaitfordata     Yes
BACKUPMethod     LEGACY
DIFFESTimate     20
BUFFers     3
BUFFERSIze     1024
```

```
STRIPes     1
SQLBUFFers     0
SQLBUFFERSIze     1024
LOGPrune     60
LANGuage     ENU
BACKUPDestination     Both
LOCALDSMAgentnode     libra_vss
REMOTEDSMAgentnode leo_offload
********** Server Storage Group Name BU Type BU Dest. Mgmt Class
********** ------ ------------------ ------- -------- ----------
********** ------ ------------------ ------- -------- ----------
VSSPOLICY  *      *                  FULL    TSM      VSS_FULL_TSM
VSSPOLICY  *      *                  LOCAL   LOCAL    VSS_LOCAL
```

Example 3-22 Data Protection for SQL Server configuration file for monthly backups (tdpsql_libra_long.cfg)

```
SQLSERVer     CLUSQL01\SQL01
FROMSQLserver     CLUSQL01\SQL01
SQLAUTHentication     INTegrated
nodename clusql01_lng
MOUNTWaitfordata     Yes
BACKUPMethod     LEGACY
DIFFESTimate     20
BUFFers     3
BUFFERSIze     1024
STRIPes     1
SQLBUFFers     0
SQLBUFFERSIze     1024
LOGPrune     60
LANGuage     ENU
BACKUPDestination     TSM
LOCALDSMAgentnode     libra_vss
REMOTEDSMAgentnode leo_offload
********** Server Storage Group Name BU Type BU Dest. Mgmt Class
********** ------ ------------------ ------- -------- ----------
VSSPOLICY  *      *                  FULL    TSM      VSS_LONG_TSM
```

Example 3-23 Data Protection for SQL Server configuration file for daily backups (tdpsql_leo_daily.cfg)

```
SQLSERVer     CLUSQL01\SQL01
FROMSQLserver CLUSQL01\SQL01
SQLAUTHentication     INTegrated
nodename CLUSQL01_Daily
```

```
MOUNTWaitfordata     Yes
BACKUPMethod     LEGACY
DIFFESTimate     20
BUFFers     3
BUFFERSIze     1024
STRIPes     1
SQLBUFFers     0
SQLBUFFERSIze     1024
LOGPrune     60
LANGuage     ENU
BACKUPDestination     Both
LOCALDSMAgentnode     leo_vss
REMOTEDSMAgentnode libra_offload
********** Server Storage Group Name BU Type BU Dest. Mgmt Class
********** ------ ------------------ ------- -------- ----------
********** ------ ------------------ ------- -------- ----------
VSSPOLICY  *      *                  FULL    TSM      VSS_FULL_TSM
VSSPOLICY  *      *                  LOCAL   LOCAL    VSS_LOCAL
```

Example 3-24 Data Protection for SQL Server configuration file for monthly backups (tdpsql_leo_long.cfg)

```
SQLSERVer     CLUSQL01\SQL01
FROMSQLserver     CLUSQL01\SQL01
SQLAUTHentication     INTegrated
nodename clusql01_lng
MOUNTWaitfordata     Yes
BACKUPMethod     LEGACY
DIFFESTimate     20
BUFFers     3
BUFFERSIze     1024
STRIPes     1
SQLBUFFers     0
SQLBUFFERSIze     1024
LOGPrune     60
LANGuage     ENU
BACKUPDestination     TSM
LOCALDSMAgentnode     leo_vss
REMOTEDSMAgentnode libra_offload
********** Server Storage Group Name BU Type BU Dest. Mgmt Class
********** ------ ------------------ ------- -------- ----------
VSSPOLICY  *      *                  FULL    TSM      VSS_LONG_TSM
```

We recommend creating a shortcut for the Data Protection for SQL Server GUI pointing to each options file. You can follow steps 1 on page 100 through 3 on page 101, which are described starting on page 100, to create the shortcuts.

To create shortcuts for daily and monthly backups, you must specify the options and configuration file. See Example 3-25, Example 3-26, Example 3-27, and Example 3-28.

Example 3-25 Shortcut definition for daily SQL backup for server Libra

```
"C:\Program Files\Tivoli\TSM\TDPSql\tdpsql.exe"
/tsmoptfile="E:\tsmdata\dsm_mssqldb_daily.opt"
/configfile="E:\tsmdata\tdpsql_libra\tdpsql_libra_daily.cfg"
```

Example 3-26 Shortcut definition for daily SQL backup for server Leo

```
"C:\Program Files\Tivoli\TSM\TDPSql\tdpsql.exe"
/tsmoptfile="E:\tsmdata\dsm_mssqldb_daily.opt"
/configfile="E:\tsmdata\tdpsql_libra\tdpsql_leo_daily.cfg"
```

Example 3-27 Shortcut definition for monthly SQL backup for server Libra

```
"C:\Program Files\Tivoli\TSM\TDPSql\tdpsql.exe"
/tsmoptfile="E:\tsmdata\dsm_mssqldb_long.opt"
/configfile="E:\tsmdata\tdpsql_libra\tdpsql_libra_long.cfg"
```

Example 3-28 Shortcut definition for monthly SQL backup for server Leo

```
"C:\Program Files\Tivoli\TSM\TDPSql\tdpsql.exe"
/tsmoptfile="E:\tsmdata\dsm_mssqldb_daily.opt"
/configfile="E:\tsmdata\tdpsql_libra\tdpsql_leo_long.cfg"
```

3.2.11 Configuring machine running offloaded backups (VSS only)

Perform these steps on the machine running the offloaded backups. In our configuration, this is MOLITO:

1. Install IBM Tivoli Storage Manager backup-archive client as described in 3.2.5, “Installing the backup-archive client code” on page 85.
2. Configure the IBM Tivoli Storage Manager backup-archive client, as shown in Example 3-29.

Example 3-29 Backup-archive client options file for offloaded machine

```
NODename          molito_offload
PASSWORDAccess    generate

COMMMethod        TCPip
TCPServeraddress  9.43.86.45
TCPPort           1500
TCPWindowsize     63
TCPBuffSize       32
TCPCLIENTADDRESS 9.43.86.64
clusternode no
clusterdisksonly no
managedservices webclient
```

3. Install and configure both the IBM Tivoli Storage Manager Client Acceptor Daemon (CAD) service and Remote Client Agent service (DSMAgent). Remember, that you can use the backup-archive GUI, select **Utilities** → **Setup Wizard** → **Help me configure the TSM Web Client**. See the steps on “Configuring the CAD and remote agent services” on page 117.
4. In your environment if you have a VSS provider (that is not the default system VSS provider), you must configure it. Consult the VSS provider documentation for information regarding the configuration of that software.
5. Verify on your Windows services panel whether the CAD and remote agent are started.

3.2.12 Summary of configuration files

As described in earlier chapters, we have to configure numerous files before starting to back up SQL Server databases. The following examples show the files that must be configured in a non-clustered and in a clustered environment. See Figure 3-28 and Figure 3-29 on page 117.

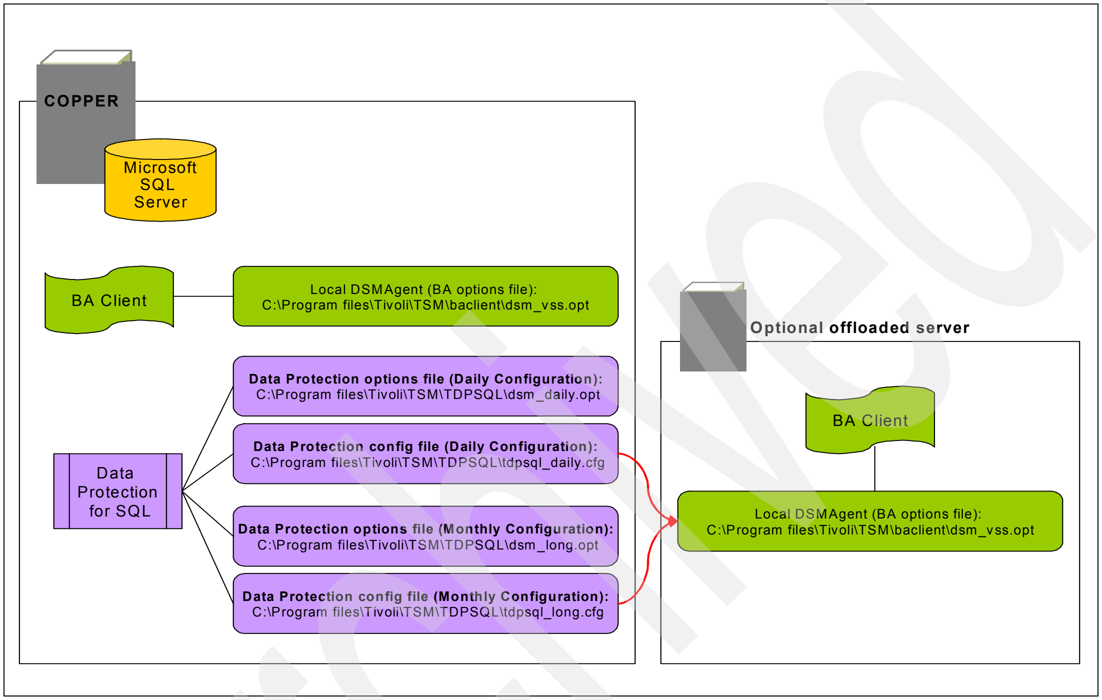

Figure 3-28 Summary configuration files in a standalone environment

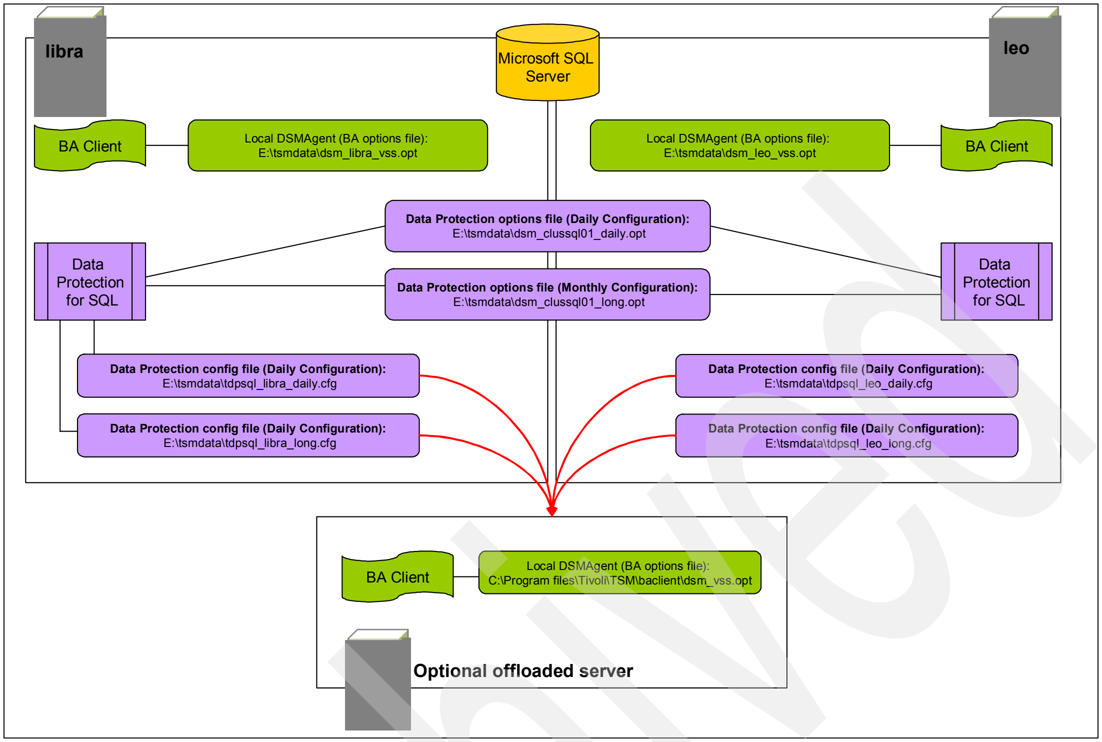

Figure 3-29 Summary configuration files in a clustered environment

3.2.13 Configuring the CAD and remote agent services

It is necessary to configure the Client Acceptor Daemon (CAD) and remote agent services for the local DSMAgent node to permit communication among Data Protection for SQL Server, the backup-archive client, and IBM Tivoli Storage Manager.

You can use either IBM Tivoli Storage Manager backup-archive setup wizard or **dsmcutil** to perform these tasks.

1. From the backup-archive GUI, select **Utilities** → **Setup Wizard**.
2. The window TSM Client Configuration Wizard is displayed. Select the option **Help me to configure the TSM Web Client**. See Figure 3-30.

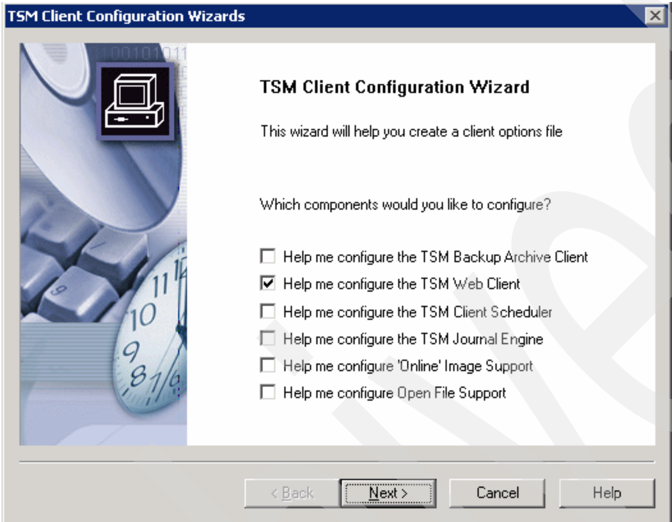

Figure 3-30 TSM Client Configuration wizard

3. Select the option **Install a new Web client agent** and click **Next**. See Figure 3-31.

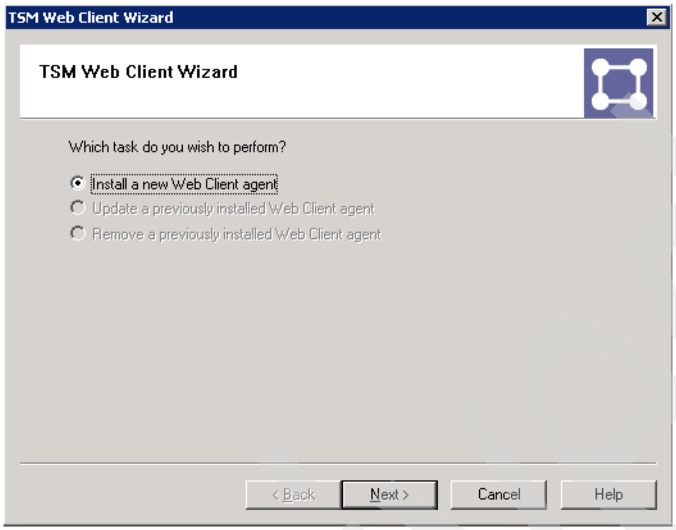

Figure 3-31 Select Install a new Web Client agent

4. Select the name of the TSM acceptor and click **Next**. Figure 3-32.

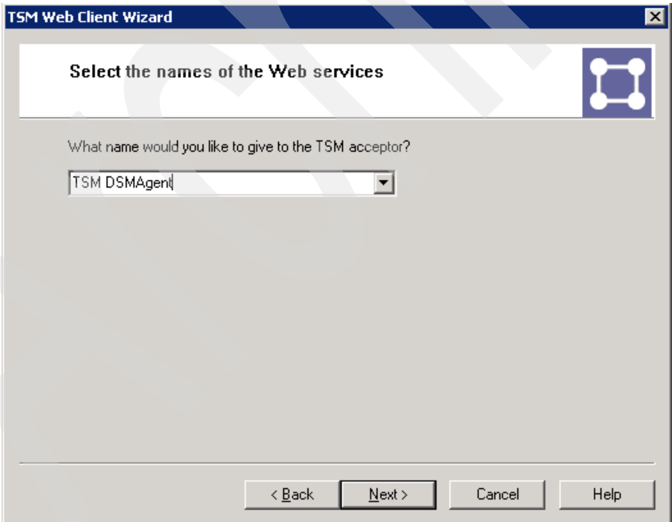

Figure 3-32 Select the name of the TSM acceptor

5. Select the options file and its location and click **Next**. See Figure 3-33.

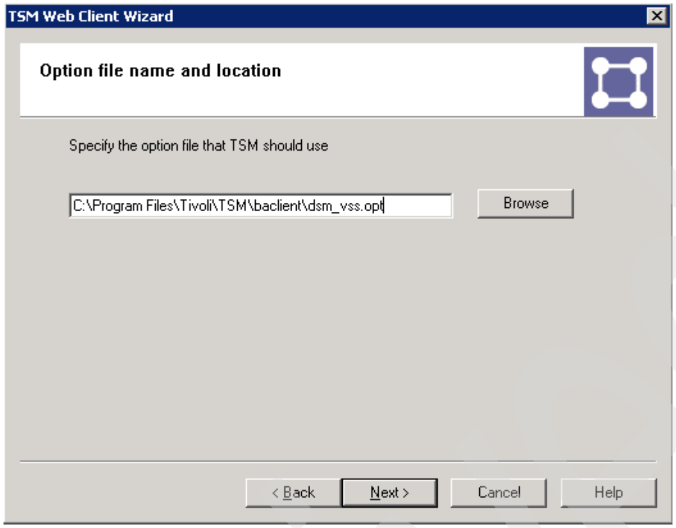

Figure 3-33 Select options file

6. Choose the HTTP port and click **Next**. See Figure 3-34.

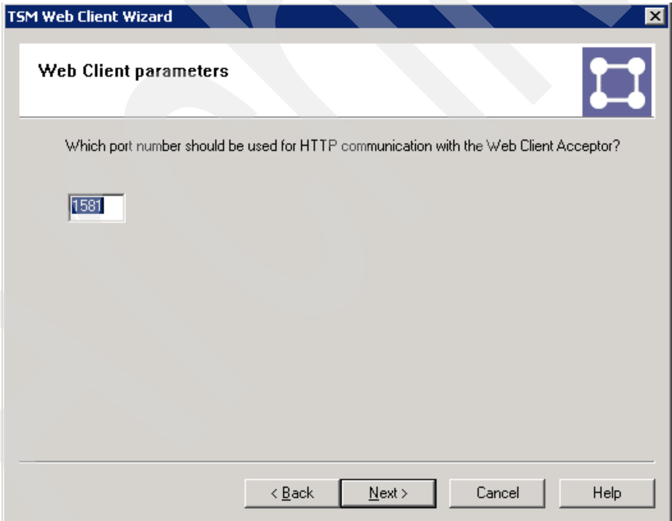

Figure 3-34 HTTP port

7. Fill in the node name and password information for the backup-archive node. See Figure 3-35.

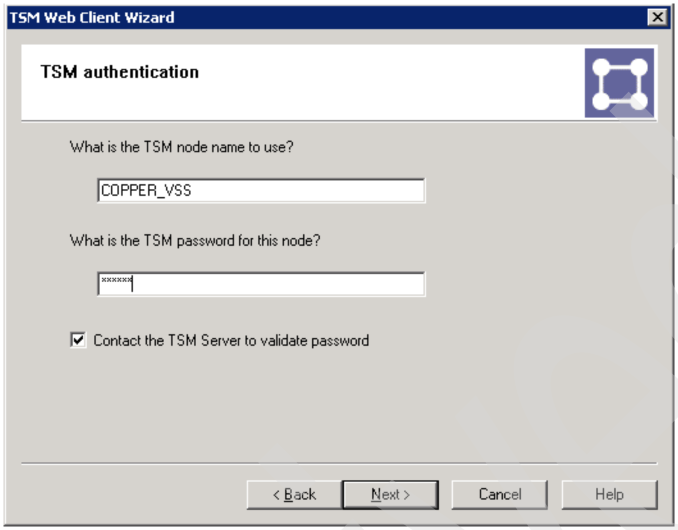

Figure 3-35 TSM authentication

8. Select **The System Account**; if you want to use a specific user, you can provide the user name and the password. Configure the service to start automatically. See Figure 3-36.

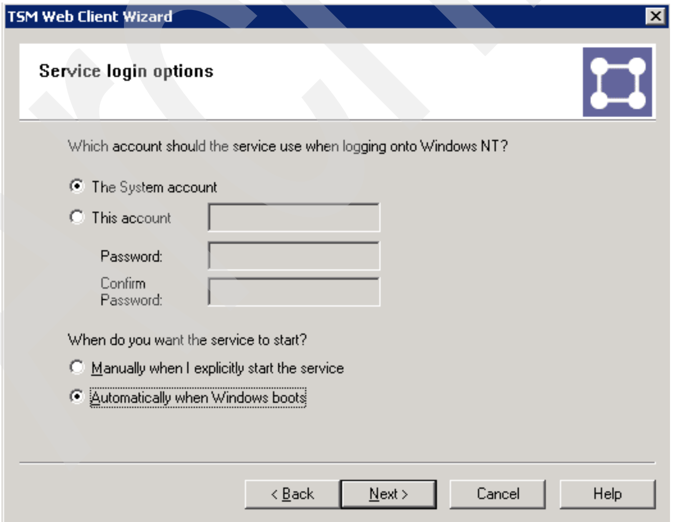

Figure 3-36 Service log on options

9. Choose the name of the Remote Agent service name. See Figure 3-37.

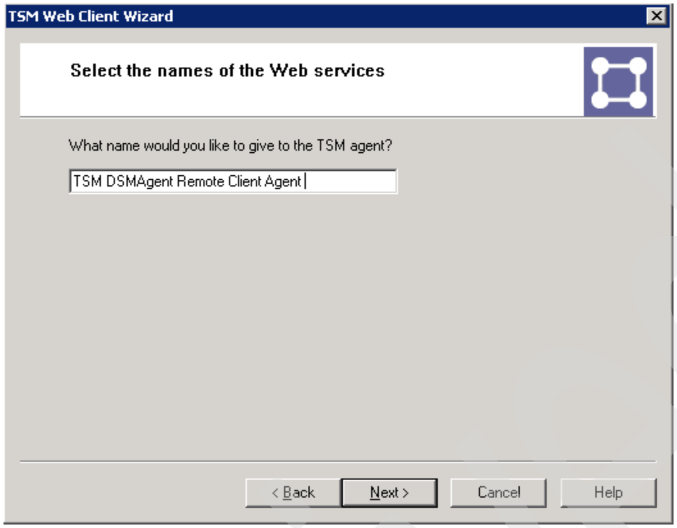

Figure 3-37 Choose Web services name

10. Select **No** to revoke the remote access privileges to the Web Client. See Figure 3-38.

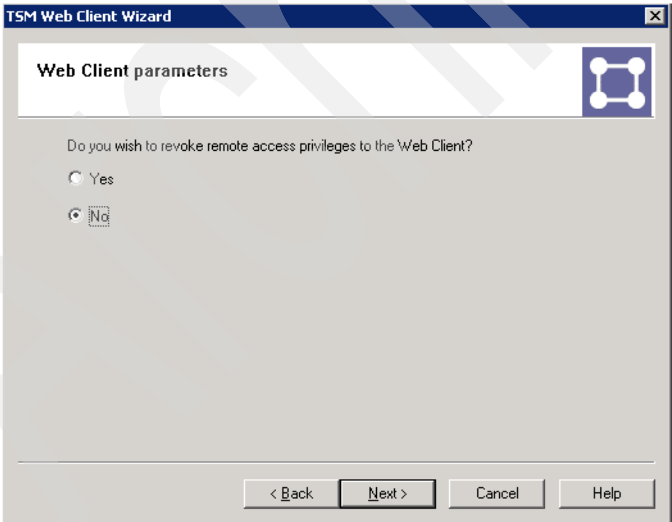

Figure 3-38 Web Client parameters

11.Select **Yes** to start this service now. See Figure 3-39.

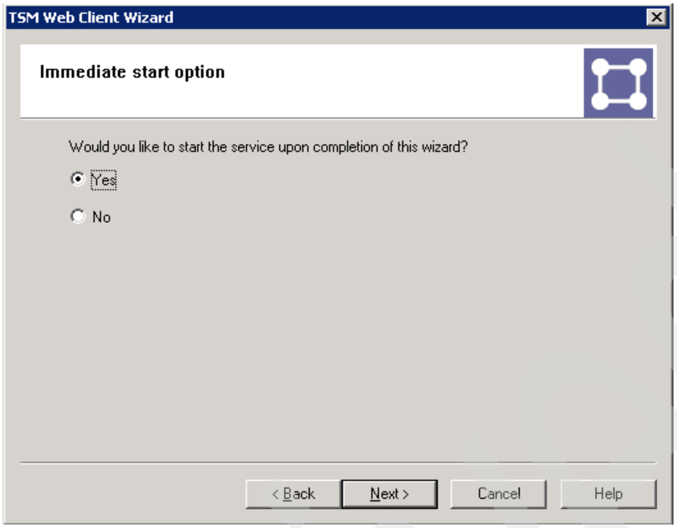

Figure 3-39 Immediate start option

12.In the completion window, click **Finish**. See Figure 3-40.

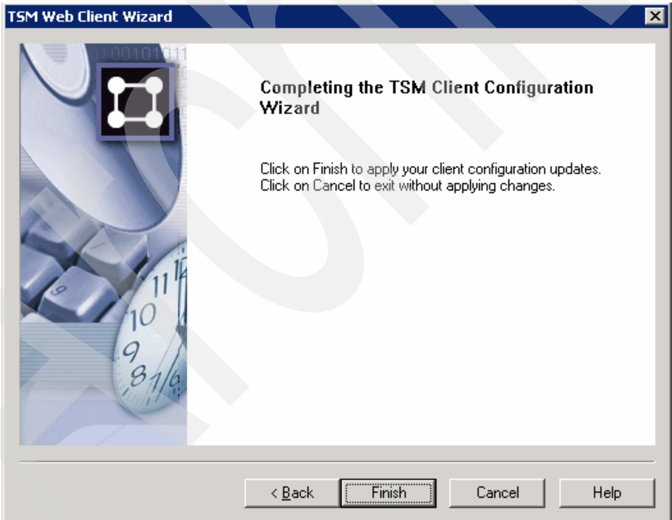

Figure 3-40 Completing TSM Client Configuration Wizard

> **Note:** In a clustered environment you can create a service to manage the CAD service as a cluster resource. To do so, in step 8 select **Manually when I explicitly start the service**, and in step 11 select **No** so that the service does not start immediately.

3.2.14 Configuring the proxy node definitions

You must configure proxy node definitions when you intend to perform VSS backups. Configuring proxy authority enables you to grant proxy authority to a client node on the IBM Tivoli Storage Manager server. Target client nodes own the data, and agent nodes act on behalf of the target nodes. When granted proxy authority to a target client node, an agent node can perform backup and restore operations for the target node. Data that the agent node stores on behalf of the target node is stored under the target node's name in server storage.

The DSMAgent is used as an agent node. The options file (dsm.opt) created for the backup-archive client is used as the DSMAgent, and the target node is the owner of the backups. In Example 3-30, we can see a GRANT PROXY command for two nodes because we have two different backup policies for this SQL server node in a standalone configuration.

Example 3-30 Proxy authority

```
tsm: ZAIRE>GRANT PROXYNODE target=copper_sql agent=copper_vss

tsm: ZAIRE>GRANT PROXYNODE target=copper_lng agent=copper_vss
```

Example 3-31 shows the GRANT PROXY commands required in the clustered environment, with two different backup policies.

Example 3-31 Proxy authority in a clustered environment

```
tsm: ZAIRE>GRANT PROXYNODE target=clusql01_daily agent=libra_vss

tsm: ZAIRE>GRANT PROXYNODE target=clusql01_lng agent=libra_vss

tsm: ZAIRE>GRANT PROXYNODE target=clusql01_daily agent=leo_vss

tsm: ZAIRE>GRANT PROXYNODE target=clusql01_lng agent=leo_vss

tsm: ZAIRE>GRANT PROXYNODE target=clusql01_daily agent=libra_vss

tsm: ZAIRE>GRANT PROXYNODE target=clusql01_lng agent=libra_vss
```

```
tsm: ZAIRE>GRANT PROXYNODE target=clusql01_daily agent=leo_vss

tsm: ZAIRE>GRANT PROXYNODE target=clusql01_lng agent=leo_vss

tsm: ZAIRE>GRANT PROXYNODE target=clusql01_daily agent=molito_offload

tsm: ZAIRE>GRANT PROXYNODE target=clusql01_lng agent=molito_offload
```

3.2.15 The hardware provider

To support VSS Instant Restore, you must configure the hardware provider. You need to check whether the hardware is supported by IBM Tivoli Storage Manager for Copy Services at this web site:

http://www-1.ibm.com/support/docview.wss?&uid=swg21269169.

Your hardware provider process installation depends on your disk hardware type.

The following steps are performed by Microsoft VSS in conjunction with FlashCopy when a backup application initiates a request for a backup on an IBM disk system (SVC, DS6000, or DS8000):

1. VSS retrieves a list of volumes from the storage system and selects appropriate target volumes from the free pool (VSS_FREE).
2. VSS moves the target volumes to the reserved pool (VSS_RESERVED), and the Microsoft SQL Server database suspends writes.
3. VSS issues a FlashCopy from the source volumes to the target volumes. The FlashCopy is performed on the hardware under the direction of the VSS hardware provider. The FlashCopy is made as a transportable nonpersistent snapshot.
4. The database resumes writes after the FlashCopy is complete. At this point, the SQL server has no further involvement in the operation.
5. VSS assigns the target volumes to the offloaded server's HBAs. Microsoft Windows mounts the volumes on the offloaded server.
6. The VSS requestor reads the data from the target volumes and copies it to IBM Tivoli Storage Manager server storage.
7. Once the backup to IBM Tivoli Storage Manager is complete, Microsoft VSS unmounts the volumes, and VSS unassigns the target volumes from the backup server's HBAs.
8. VSS assigns the target volumes back to the free pool (VSS_FREE).

9. The target volumes are made available for use in other VSS operations.

For more information refer to Chapter 9 in *IBM System Storage DS Open Application Programming Interface Reference*, GC35-0516. You can find this manual at the following Web site:

http://www-1.ibm.com/support/docview.wss?uid=ssg1S7001160&aid=1

4

Data Protection for SQL Server backup

In this chapter we discuss how to use the Data Protection for SQL Server graphical user interface (GUI) and command-line interface (CLI) to back up Microsoft SQL Server databases.

This chapter covers the following:

4.1 GUI overview

The Data Protection for SQL Server GUI consists of a main window with the following elements:

- Common menu bar
- Toolbar
- Backup Databases tab
- Backup Groups/Files tab
- Restore Database tab
- Restore Groups/Files tab
- Inactivate tab

> **Note:** By default, the Inactivate tab is not displayed in the main window. To display the Inactivate tab, you must check the option **Inactivate** tab in the View menu bar option.

The backup and restore windows contain a directory tree and operation controls.

Figure 4-1 shows the Data Protection for SQL Server GUI. We describe how to launch the GUI in 4.1.3, “Launching the GUI” on page 139. Because we have installed Tivoli Storage Manager for Copy Services, the VSS backup option is available for selection. If Tivoli Storage Manager for Copy Services is not installed, the option is grayed out.

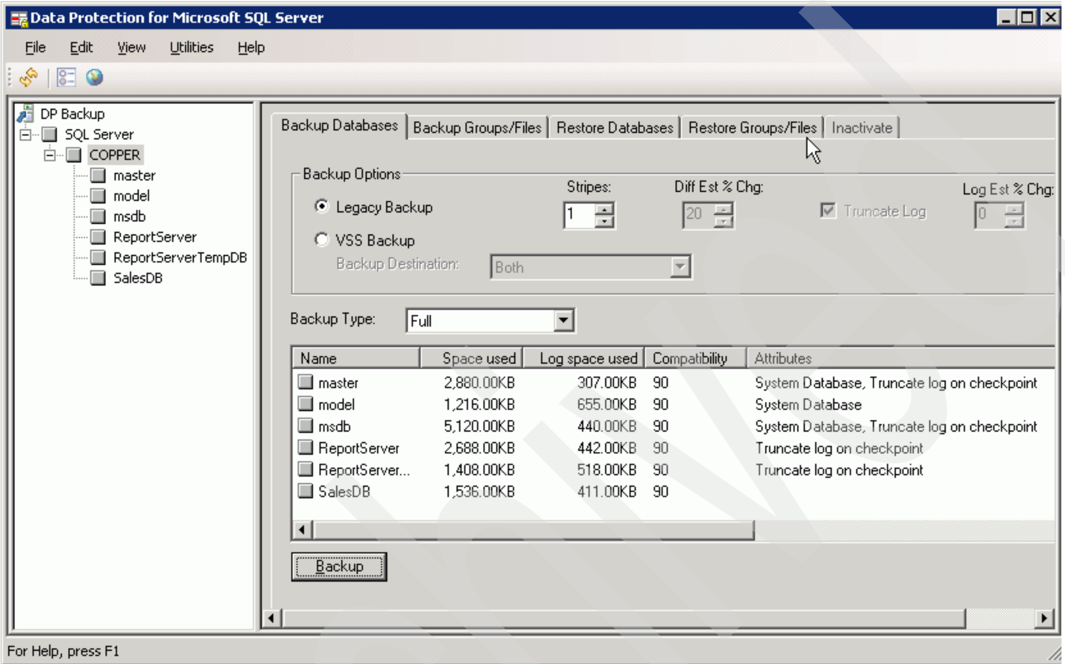

Figure 4-1 Data Protection for SQL Server GUI

4.1.1 Menu bar

The Data Protection for SQL Server menu bar includes these items and menu list functions:

- File

  Exit Data Protection for SQL Server GUI tool

- Edit

  Edit Data Protection for SQL Server configurations. The default configuration settings are contained in the tdpsql.cfg file.

- View

  Refresh the tree window and display the Inactivate tab.

- Utilities

  Change the Tivoli Storage Manager password, set the SQL server logon information, or show server information for both the Tivoli Storage Manager server and the SQL server.

- Help

  Obtain Data Protection for SQL help to assist with GUI tasks, Tivoli Storage Manager Web access, and information about Data Protection for SQL.

Edit menu

Use the Edit menu to change Data Protection for SQL Server configuration settings.

You can modify the Data Protection for SQL Server configuration file. If a configuration file is not specified when launching the GUI tool, the file tdpsql.cfg is used. If no configuration file is found, a default file is created that contains all the default settings for the parameters, except for the LASTPRUNEDATE value. To specify a different configuration file, start the GUI from the command line with the /configfile parameter.

Click **Configure** under Edit to display the Data Protection for SQL Server Settings dialog with the following five tabs and their parameters:

General tab

This tab displays the preferences page for general configuration parameters.

The General tab is shown in Figure 4-2.

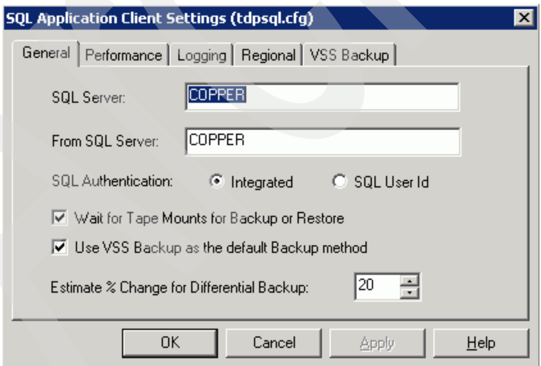

Figure 4-2 General tab

In this tab you can modify the following settings:

- SQL Server

  Specifies the SQL server that Data Protection for SQL Server logs on to.

- From SQL Server

  Specifies the SQL server that backup objects were backed up from. This parameter is necessary only when the name of the SQL server to restore to, as determined by the SQL Server parameter, is different from the name of the SQL server that the backup objects were created from.

> **Note:** By default, Microsoft SQL Server listens on TCP/IP port 1433. If the SQL server is listening on a TCP/IP port other than 1433, you must explicitly configure the SQL Server and From SQL Server parameters shown in Figure 4-2 on page 130. For more information, see 3.2.10, “Specifying Data Protection for SQL Server preferences” on page 107.

- SQL Authentication

  Specifies the authorization mode used when logging on to the SQL server.

  – Integrated (default)

    Specifies using a trusted connection and enables Windows to authenticate the logon.

  – SQL User ID

    Specifies using SQL User ID security. With this type of security, the administrator provides the logon ID and the password to log on to Data Protection for SQL Server.

- Wait for Tape Mounts for Backup or Restore

  Check this box if you want Data Protection for SQL Server to wait for tape media (if used) to be mounted for backup and restore operations. When backups are stored on tape, it is likely that backup and restore operations will have to wait until the required tape volume mounts.

  This setting specifies whether Data Protection for SQL Server should wait for the media mount or stop the current operation. Waiting for tape mounts is the default, which is usually appropriate in an environment with an automated tape library. This option is only used on Legacy operations.

- Use VSS Backup as the default Backup method

  Check this box to set VSS Backups as the default backup method. This parameter is grayed out if the IBM Tivoli Storage Manager for Copy Services: Microsoft SQL VSS Integration Module is not installed. Remember that VSS backups can only be restored using VSS. If you use VSS as the default, the local DSMAgent node name parameter must be specified (as shown in Figure 4-6 on page 135).

- Estimate % Change for Differential Backup

  Specifies the value for the estimated change to database pages for differential backups. This estimate is used by Data Protection for SQL Server to determine whether sufficient storage space is available for the backup. The value specified here becomes the default value for all differential backups.

Performance tab

This tab displays the preferences page for performance configuration parameters. The Performance tab is shown in Figure 4-3.

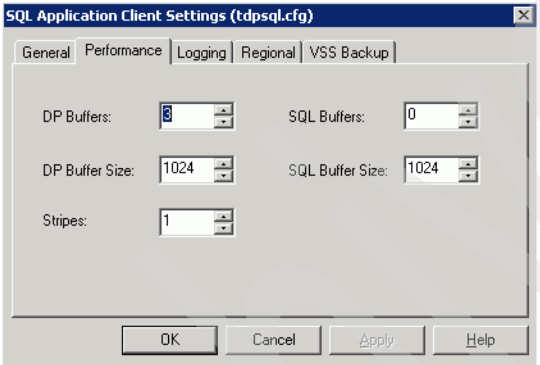

Figure 4-3 Performance tab

In this tab you can configure the following settings:

- DP Buffers (3 by default)

  Specifies the number of communication data buffers Data Protection for SQL Server uses when transferring data between Data Protection for SQL Server and the Tivoli Storage Manager server. Each buffer is the size specified by the TDP Buffer Size option. Note that this option applies to Legacy backups only.

- DP Buffer Size (1024 by default)

  Specifies the size of the buffers used by Data Protection for SQL Server to transfer data to the Tivoli Storage Manager server. Note that this option applies to Legacy backups only.

- Stripes (1 by default)

  Specifies the number of data stripes (1 to 64) to use in a Legacy backup or Legacy restore operation. The default value is 1. Note that VSS operations do not support multiple stripes. As a result, the default value for VSS operations is 1.

- SQL Buffers (0 by default)

  Select a number (0 to 999) that specifies the number of communication data buffers Data Protection for SQL Server uses when transferring data between the Microsoft SQL Server and Tivoli Storage Manager server. Each buffer is the size specified in the TDP Buffer Size option.

- SQL Buffer Size (1024 by default)

  Select a number (64 to 4096) that specifies the size of the buffers used by Data Protection for SQL Server to transfer data from the Microsoft SQL Server to Data Protection for SQL.

Logging

This tab displays the preferences page for logging configuration parameters. The Logging tab is shown in Figure 4-4.

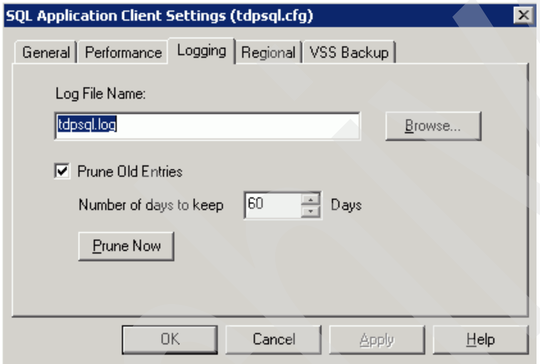

Figure 4-4 Logging tab

In this tab you can configure the following settings:

- Log File Name (tdpsql.log by default)

  Specifies the name of the file where you want Data Protection for SQL Server to write activity log information.

- Prune Old Entries (selected by default)

  Check this box to enable pruning of the activity log.

  – Number of days to keep (60 by default)

    Use this field to specify the number of days (0 to 9999) worth of entries to keep in the activity log. Data Protection for SQL Server prunes entries greater than this number when you initialize this application.

  – Prune Now

    Click **Prune Now** to prune the activity log immediately.

Regional

This tab displays the preferences page for regional configuration parameters. The Regional tab is shown in Figure 4-5.

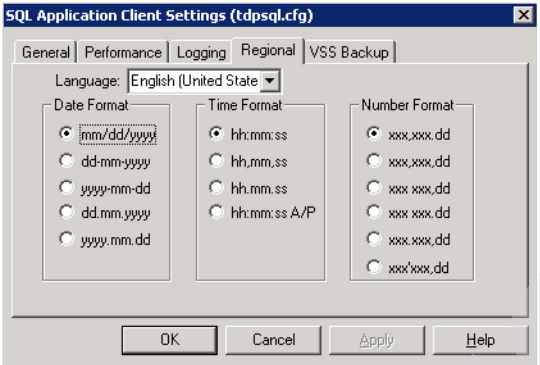

Figure 4-5 Regional tab

In this tab you can configure the following settings:

- Language (American English by default)

  Specify the language you want to use for displaying GUI and Data Protection for SQL Server messages. You can select from the following:

  – English (United States - the default)
  – Brazilian Portuguese
  – Chinese (Simplified)
  – Chinese (Traditional)
  – French
  – German
  – Italian
  – Japanese
  – Korean
  – Spanish

  The language you specify does not become effective until you exit and restart the GUI.

> **Note:** To use a non-default language you must install the corresponding language pack. See “Installing Data Protection for SQL Server additional language packs” on page 94 for the installation procedure.

- Date Format (mm/dd/yyyy by default)

  Click one of the following buttons for the date format of your choice.

  – **dd**: day of the month
  – **mm**: month of the year
  – **yyyy**: year time format (hh:mm:ss by default)

- Time Format (hh:mm:ss by default)

  Click one of the Time Format buttons to select a format for displaying time.

  – **hh**: hours (24-hour day)
  – **mm**: minutes in an hour
  – **ss**: seconds in a minute

- Number Format (xxx,xxx.dd by default)

  Click one of the Number Format buttons to select a format for displaying numbers. The choices on the display represent several ways to place the decimal, comma, and spaces.

VSS Backup

This tab displays the preferences page for VSS Backup configuration parameters. The VSS Backup tab is shown in Figure 4-6.

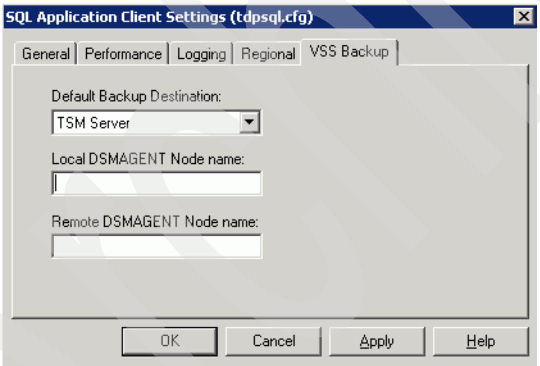

Figure 4-6 VSS Backup tab

In this tab you can configure the following settings:

- Default Backup Destination (Tivoli Storage Manager server by default)

  Select the default storage location for your backups. You can select from the following storage locations:

  – TSM Server

    The data is stored on Tivoli Storage Manager server storage only. This is the default.

– Local

The backup is stored on local VSS disk only.

– Both

The backup is stored on both Tivoli Storage Manager server storage and local VSS disk.Note that this parameter is only valid when using the VSS backup method.

- Local DSMAgent node name (blank by default)

  Specify the Tivoli Storage Manager node name (agent node) of the local client machine that performs VSS operations and moves the VSS data from local shadow volumes to Tivoli Storage Manager server storage during Tivoli Storage Manager server backups. This parameter must be specified for VSS operations to be performed. See Chapter 5, “Data Protection for SQL Server restore” on page 179 for instructions on how to configure this node.

- Remote DSMAgent node name (blank by default)

  Specify the Tivoli Storage Manager node name (agent node) of the remote client machine that moves the VSS data from local VSS disks to Tivoli Storage Manager server storage during offloaded backups. This option is required only if you are using an offloaded backup server. See Chapter 3, “Installation and configuration” on page 73 for instructions on how to configure this node.

View menu

The view menu gives you the following options:

- Refresh tree view

  By refreshing the GUI, you can:

  – Clear any selections.

  – Collapse the tree to the level you have highlighted.

  – Collapse corresponding tab trees even if they are not currently displayed (for example, refreshing the Backup Databases tree also refreshes the Backup Groups/Files tree).

  – Display new backup operations in the restore trees.

> **Note:** If you simply move back and forth between tabs without refreshing, the current selections or tree view are maintained.

- Inactivate tab

  Click this item to add the tab control to the backup and restore windows, enabling you to inactivate SQL Server databases in Tivoli Storage Manager storage.

Utilities menu

The Utilities menu provides the following options:

- Change TSM Password

  This dialog prompts you to enter the old password and then to enter the new password twice to verify the new password.

- SQL Server Login settings

  You can select the following in the SQL Server Login Information dialog:

  – Use Windows Authentication (selected by default).

  – Use SQL Authentication; if you select this option, you have to fill in a user ID (sa by default) and password (blank by default).

  Figure 4-7 shows the SQL Server Login Information dialog.

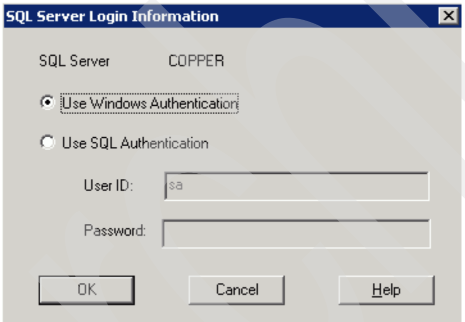

Figure 4-7 SQL Server Login Information

Note: Microsoft SQL Server logon permission requirements for Data Protection for SQL Server are discussed in 2.5.4, "Data Protection for SQL Server security considerations" on page 67.

- Show TSM server information

  This window displays the following connection information:

  – Nodename
  – Server Network Host Name
  – Tivoli Storage Manager API Version

- Server Name
- Server Type
- Server Version
- Compression Mode
- Domain Name
- Active Policy Set
- Default Management Class

Figure 4-8 shows the Tivoli Storage Manager Server information window.

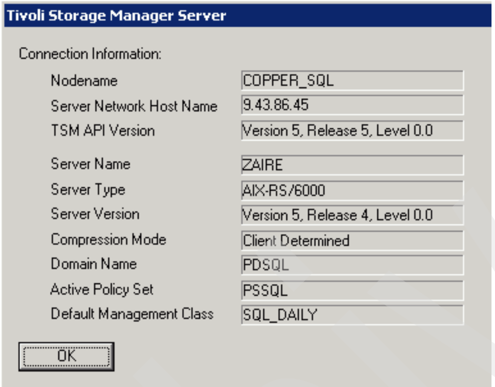

Figure 4-8 Tivoli Storage Manager Server information

- Show MS SQL Server information

  This window displays the following information:

  - SQL Server Name
  - Version
  - Cluster

Help menu

The Help menu provides the following options:

- Data Protection for SQL Help

  This dialog launches online help.

- TSM Web Access

  This dialog launches a Web browser to view Tivoli Storage Manager information online.

- About Data Protection for SQL

  This dialog launches version, release, and modification level information about Data Protection for SQL Server.

4.1.2 Toolbar

The toolbar provides shortcuts to frequently used items, such as:

- Refresh tree view
- Edit Data Protection for SQL configuration
- Access Tivoli Storage Manager Web links

4.1.3 Launching the GUI

To launch the GUI, choose **Start** → **Programs** → **Tivoli Storage Manager** → **Data Protection For Microsoft SQL Server** → **SQL Client GUI**.

Alternatively, you can use the **`tdpsql`** command from the installation directory, which can take the following parameters:

- configfile

  If specified, this parameter overrides the default Data Protection for SQL Server configuration file - tdpsql.cfg in the installation directory. Otherwise, the default configuration file is used.

  For example, to specify a configuration file, file.cfg, located in the \temp\test directory when invoking the GUI, enter:

  ```
  tdpsql /CONFIGfile=c:\temp\test\file.cfg
  ```

- sqlserver

  If specified, this parameter overrides the default SQL server, which is the local SQL server. You must use this switch to access SQL server named instances and SQL server clustered instances.

  For example, to access a SQL server named instance SQLNAMED1 on server Copper, invoke the Data Protection for SQL Server GUI as:

  ```
  tdpsql /sqlserver=Copper\SQLNAMED1
  ```

- tsmoptfile

  If specified, this parameter overrides the default Tivoli Storage Manager API option file (dsm.opt). For example, to specify the file.opt option file located in the \temp\test directory, enter:

  ```
  tdpsql /TSMOPTFile=c:\temp\test\file.opt
  ```

If you want to specify non-default options - for example, if you are in a clustered environment, we recommend customizing a shortcut for launching the GUI, as shown in “Configuring the Data Protection for SQL Server options file in a clustered environment” on page 106.

4.1.4 Backup and restore windows

Data Protection for SQL Server offers separate windows for backup and restore operations, each with its own tree, list, and tab controls.

Considerations

Take into account the following considerations:

- Both Legacy and VSS operations are performed from the same tab.
- When the GUI starts, the backup window is the initial display.
- Different types of backup and restores are available in different tabs.
- VSS-related features are grayed out unless the Tivoli Storage Manager for Copy Services MS SQL VSS Integration Module is installed.
- After you install Tivoli Storage Manager for Copy Services, the VSS backup becomes the default type for SQL backups. You can modify it changing the check box **Use VSS Backup as the default Backup method**, as discussed in “General tab” on page 130.
- You cannot close, minimize, or move the backup or restore windows independently of the main window.

Expanded backup options

You must use different Data Protection for SQL Server tabs to perform different types of backup operations. For each tab, a different view of the backup and restore window is displayed in the right pane. According to the selected tab, you can use different selectable units to perform the operations. For example, in the **Backup Databases** tab, the lowest level of Microsoft SQL Server structure you can choose is the database, while in the **Backup Groups/Files** tab, you can choose to back up a specific file or filegroup.

Table 4-1 describes the available tabs and the type of backup and restore available in each tab.

Table 4-1 Data Protection Backup and Restore tabs

Tab selection	Function	Lowest selectable unit
Backup Databases	Perform full, differential, and log backups	Database
Backup Groups/Files	Perform group, file, and set backups	Filegroup or file
Restore Databases	Restore from full, differential, and log backups	Database, differential, and log
Restore Groups/Files	Restore from full, group, file, set, and log backups.	Filegroup, file, or set backup

Tab selection	Function	Lowest selectable unit
Inactivate tab	Manually inactivate selected objects as opposed to automated inactivation	Tivoli Storage Manager backup object

Highlighting and selecting

When an item is highlighted in the tree, information about all the items one level under the highlighted item are displayed in the List view; for example:

- If a database is highlighted in Backup Groups/Files, the filegroups and transaction log for that database are displayed in the List view.
- If a database is highlighted in the Restore tree, all full and differential database and log backups for that database are displayed in the List view.
- If a database is highlighted in Restore File/Groups, all full, differential, group, file, and set backups for that database are displayed in the List view.

To select an item for backup or restore, check the square selection box to the left of the item name. Checking a selection box in the tree also highlights the item and displays associated information in the List view.

Double-click a selection box in the tree to select that item and collapse or expand the tree at that point. An item can be selected from both the tree and the List view.

4.2 Legacy backups using the GUI

In this section we discuss how to perform Microsoft SQL Server backups using the Data Protection for SQL Server GUI tool. In the following examples, we assume you have already installed and configured Data Protection for SQL Server, launched the Data Protection for SQL Server GUI as explained in 4.1.3, "Launching the GUI" on page 139, and expanded the SQL Server tree in the left pane. All backup scenarios are performed starting at this point.

4.2.1 Full database backups using the GUI

To perform a full backup of a database, execute the following steps:

1. Select the **Backup Databases** tab.
2. In the left pane, choose the databases to back up. If you want to back up all databases for the Microsoft SQL Server instance, choose the SQL server instance name, and automatically all databases under this instance are selected.

3. In the Backup Options section, choose the **Legacy Backup** radio button and the number of stripes for this backup.
4. In the Backup Type drop-down menu, choose **Full**.
5. Click **Backup** to start the backup.

Figure 4-9 shows how to select all databases in a SQL server instance for a full backup.

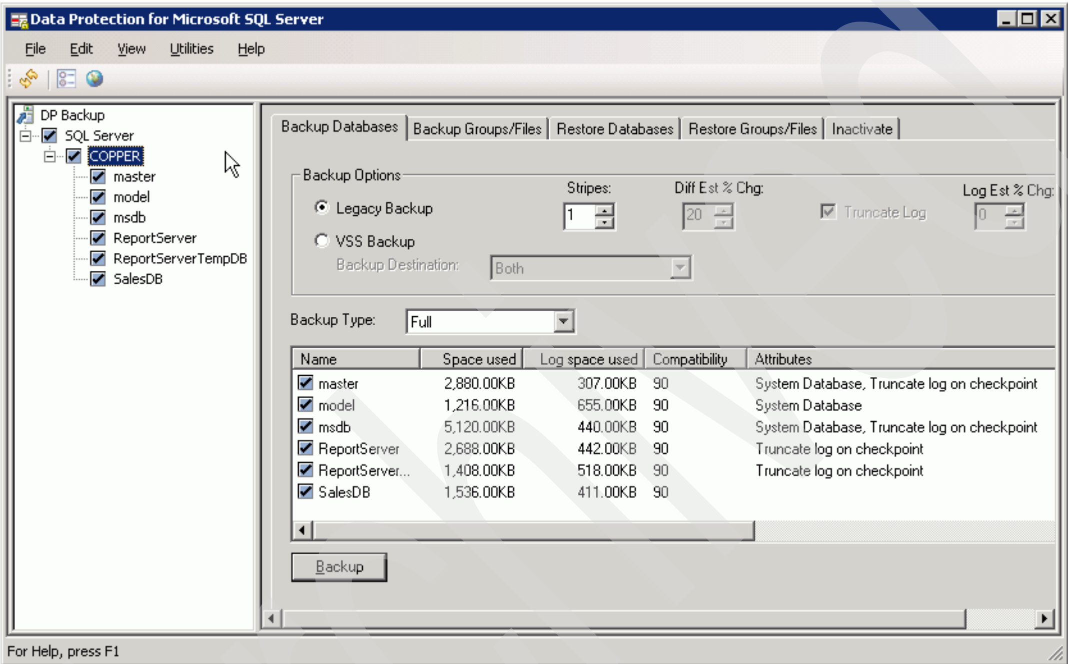

Figure 4-9 Legacy full backup

The backup progress is displayed as shown in Figure 4-10.

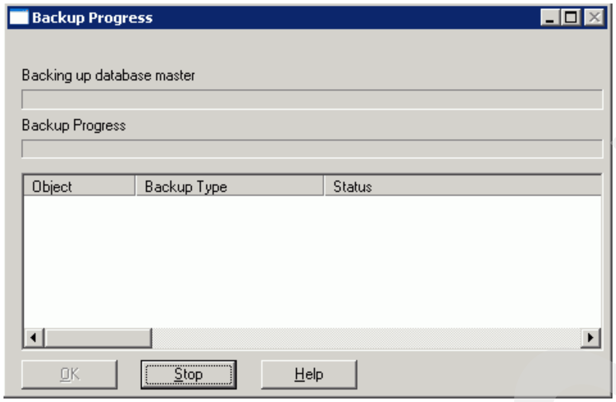

Figure 4-10 Database operation progress

After the backup is complete, the Backup Progress window indicating whether or not the operation completed successfully and the object(s) backed up with detailed status information is displayed, as shown in Figure 4-11. Click **OK** to finish. If an error message is displayed, the backup has failed.

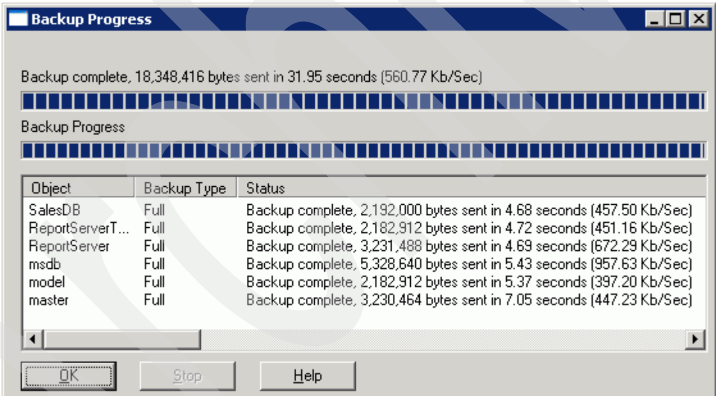

Figure 4-11 Backup complete message

4.2.2 Transaction log backups using the GUI

Performing a transaction log backup is very similar to performing a full database backup. The difference is that you must choose **Log** instead of **Full** in the Backup Type drop-down menu. When you choose **Log** in the Backup Options section, you are enabled to change the configuration of the options Truncate Log and Log Est % Chg. Unless you are performing a tail-log backup, we recommend that you do not uncheck Truncate Log; otherwise, the transaction log file is not truncated when the transaction log backup finishes, which enables the transaction log to consume all disk space available.

> **Note:** An example of tail-log backup is shown in 4.2.7, "Tail-log backups using the GUI" on page 150.

The Log Est % Chg spin box enables you to estimate the percentage of database pages that have changed due to non-logged operations since the last log backup. The default is 0.

When the simple recovery model or truncate log on checkpoint options are displayed with an "X" in the left panel, you cannot choose these databases to perform a log backup.

Figure 4-12 shows an example of how to select a database for log backups. In our example, we select the SalesDB database to perform the transaction log backup. Note that several databases on the left pane, such as master and msdb databases, are marked with an "X". You cannot perform transaction log backups of these databases.

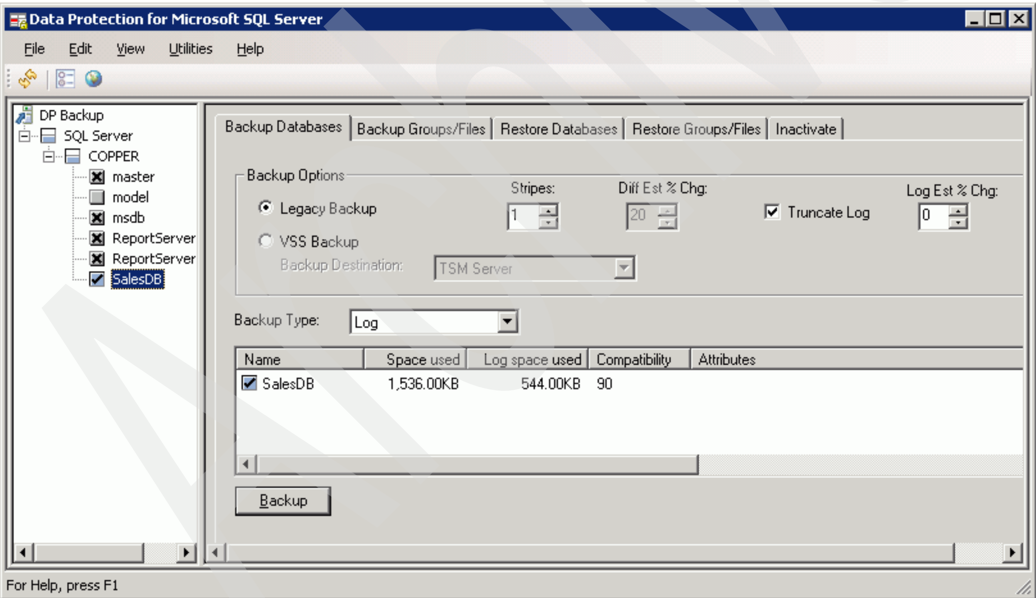

Figure 4-12 Legacy transaction log backup

Click **Backup** to start the backup operation. The Backup Progress window is displayed to inform you whether or not the operation completed successfully, and it lists the objects backed up with detailed status information.

4.2.3 Differential backups using the GUI

Performing a full differential backup is similar to performing full and transaction log backups. You must click the **Backup Databases** tab, and select **Differential** in the Backup Type drop-down menu. The parameters Stripes and Diff Est % Chg become available for you to customize your backup operation. The parameter Diff Est % Chg assumes the value specified in Estimate % Change for Differential Backup, as discussed in "General tab" on page 130. It is used to estimate the percentage of database pages that have changed since the last full backup.

Figure 4-13 shows an example of a differential backup.

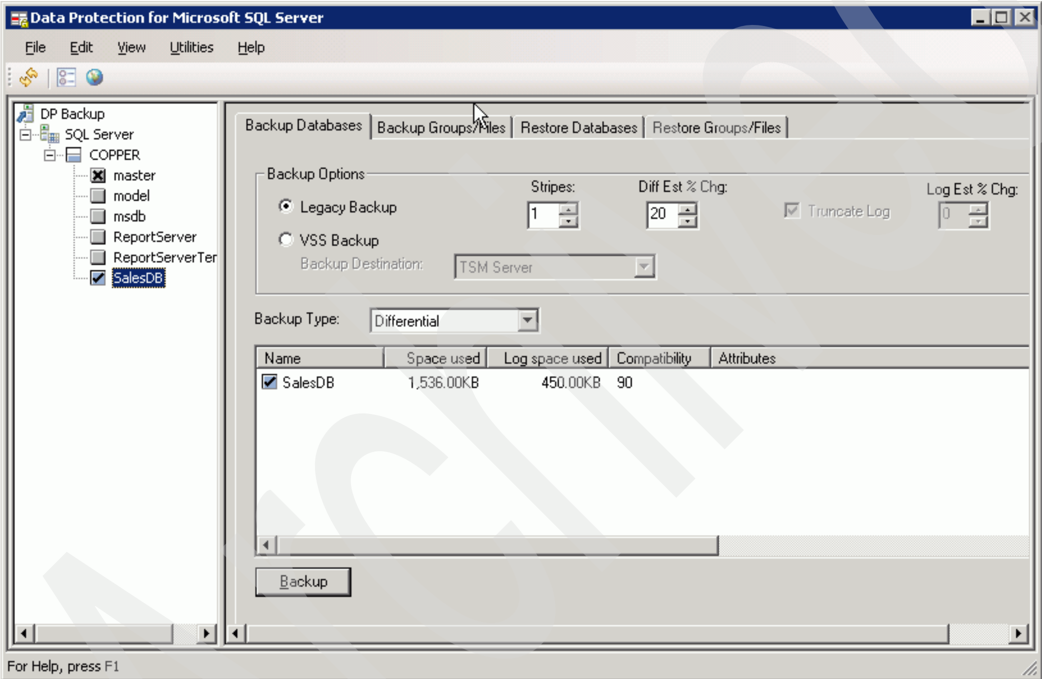

Figure 4-13 Legacy differential backup

Click **Backup** to start the backup operation. The Backup Progress window is displayed to inform you whether or not the operation completed successfully and list the objects backed up with detailed status information.

4.2.4 Group backups using the GUI

While for full, log, and differential backups, you use the Backup Databases tab, for filegroup, file, and set backups, you use the Backup Groups/Files tab. To perform a group backup, follow these steps:

1. Select the **Backup Groups/Files** tab.
2. Select the **Group** radio button in the Backup Type section.
3. Select the number of stripes in the Backup Options section.
4. On the left pane, expand the SQL Server tree to display the list of databases. Note that, as for transaction log backups, the database does not use the simple recovery model, and truncate log on checkpoint active is not available for selection. You can identify those databases not available for group backups by the “X” in the check box.
5. On the left pane, click the database you want to back up. The existing filegroups for the database appears under the database name and also in the right pane.
6. Select the filegroups you want to back up. Note that when you highlight the filegroup. the files belonging to this filegroup are listed in the List view in the right pane. However, you cannot select the file individually; when you select a file, all files in the filegroup are selected.

   You can select several filegroups in the same database or filegroups in different databases.

Figure 4-14 shows an example of group backup. In this example, we are backing up the SalesDB_LA filegroup in the SalesDB database.

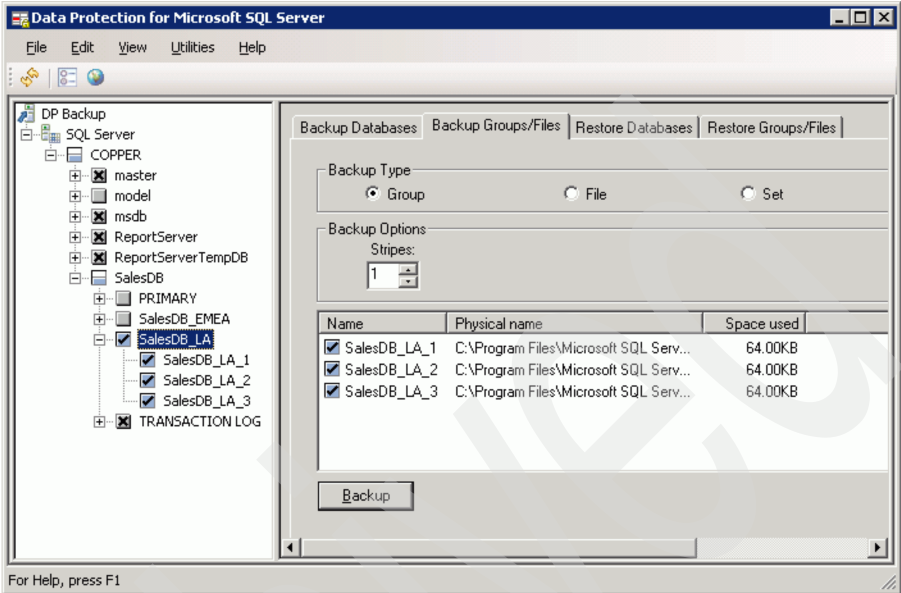

Figure 4-14 Legacy group backup

7. Click **Backup** to start the backup operation. The Backup Progress window is displayed to inform you whether or not the operation completed successfully, and it lists the objects backed up with detailed status information.

Note: We recommend you follow group backups with transaction log backups for all SQL Server databases you back up.

4.2.5 File backups using the GUI

Performing a file backup is similar to performing a group backup.

1. On the right pane, click the **Backup Groups/Files** tab, select the **File** radio button in the Backup Type section, and choose the number of stripes.
2. On the left pane, expand the tree to select the files you want to back up.

   In contrast with a group backup, in a file backup you can individually choose the files you want to back up in the left pane, while in the group backup, you choose the filegroup itself and back up all files belonging to the filegroup. Note that when you highlight the filegroup on the left pane, the files belonging to this filegroup are listed in the List view in the right pane. You can individually select any file belonging to the filegroup.

Figure 4-15 shows an example of file backup. In this example, only the file SalesDB_LA_1 is backed up. No other files from the SalesDB_LA filegroup are included in this backup.

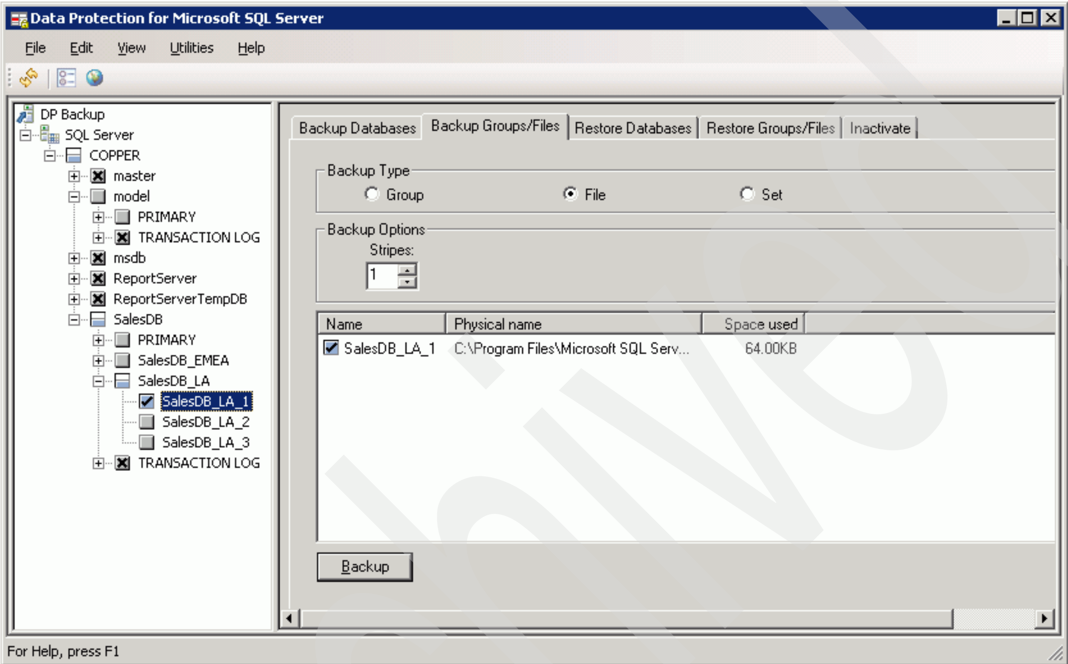

Figure 4-15 File backup

3. Click **Backup** to start the backup operation. The Backup Progress window is displayed to inform you whether or not the operation completed successfully, and it lists the objects backed up with detailed status information.

> **Note:** We recommend you follow file backups with transaction log backups for all SQL Server databases you back up.

4.2.6 Set backups using the GUI

Performing a set backup is similar to performing group or file backups.

1. On the right pane, click the **Backup Groups/Files** tab, select the **Set** check box in the Backup Type section and, choose the number of stripes in the Backup Options section,
2. On the left pane, choose the SQL server files and filegroups you want to back up.

   Figure 4-16 shows an example of a set backup. In this example the filegroup SalesDB_EMEA and the file SALESDB_LA_2 from the filegroup SalesDB_LA are backed up.

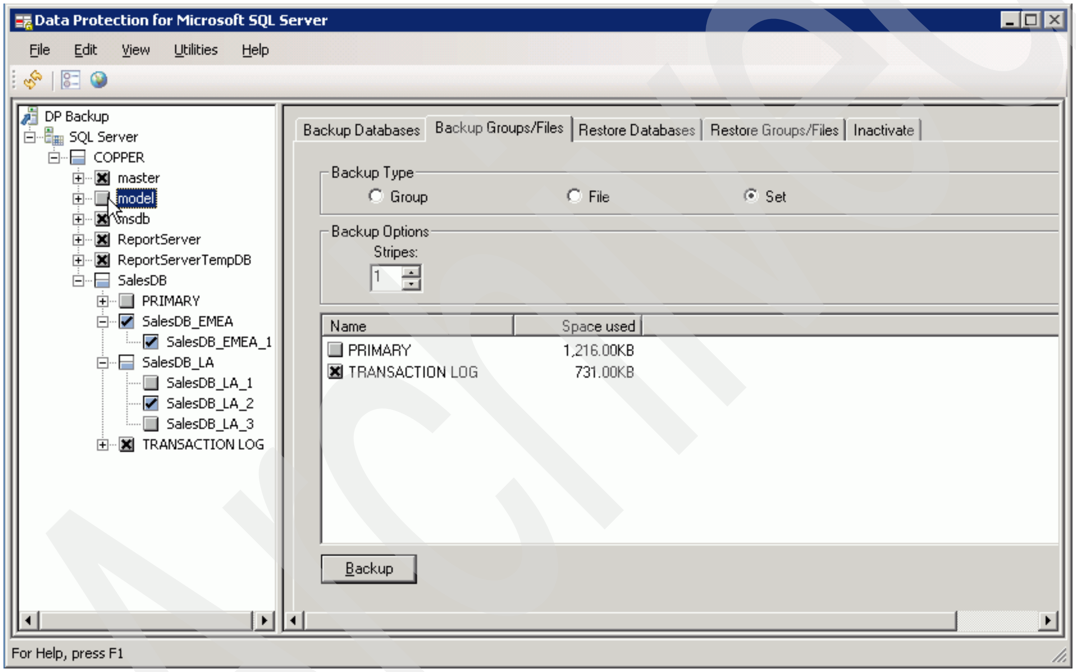

Figure 4-16 Legacy set backup

3. Click **Backup** to start the backup operation. The Backup Progress window is displayed to inform you whether or not the operation completed successfully and lists the object(s) backed up with detailed status information.

Note: We recommend you to follow set backups with transaction log backups for all SQL Server databases you back up.

4.2.7 Tail-log backups using the GUI

A tail-log backup is similar to a transaction log backup. The only difference is that you must remove the check in the **Truncate Log** check box in the Backup Options section.

Figure 4-17 shows an example of tail-log backup. Note that the **Truncate Log** check box is unchecked.

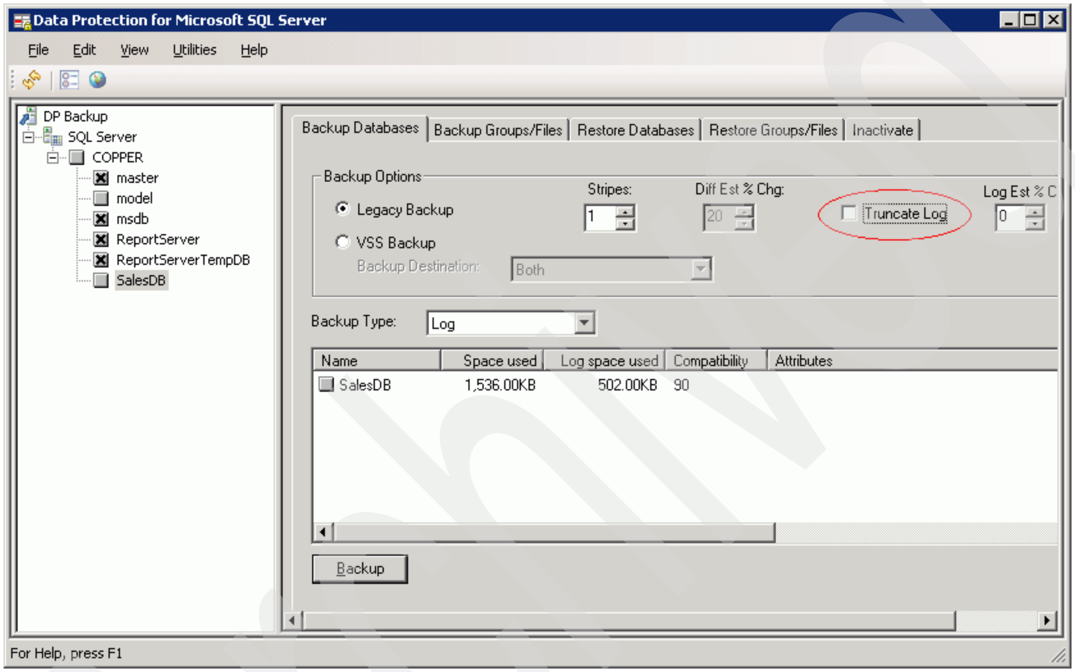

Figure 4-17 Legacy tail-log backup

Click **Backup** to start the backup operation. The Backup Progress window is displayed to inform you whether or not the operation completed successfully, and it lists the objects backed up with detailed status information.

> **Note:** Tail-log backups are intended only for special situations. Refer to 2.4.4, “Backing up a transaction log without truncating the log” on page 54 for more information.

4.3 VSS backups using the GUI

With Data Protection for SQL Server you can perform only full VSS backups:

- VSS full backup
- VSS offloaded full backup

In the following sections, we discuss how to perform GUI backups using both VSS backup types.

4.3.1 Full VSS backup using the GUI

To perform a full VSS backup:

1. Make sure a local DSMAgent node name is specified and correctly configured. See “VSS Backup” on page 135 for more information.
2. In the Data Protection for SQL Server GUI, click the **Backup Databases** tab.
3. In the left pane, choose the databases to back up. If you want to back up all databases for the Microsoft SQL Server instance, choose the name of the Microsoft SQL Server instance, and all databases under this instance automatically are selected.
4. In the right pane, select the **VSS Backup** check box in the Backup Options section, and choose the VSS backup destination. The VSS backup destination can be:
   - Both: The backup is performed on the local disk and the Tivoli Storage Manager server.
   - Local: The backup is performed only on local disks.
   - TSM Server: The backup is performed only on the Tivoli Storage Manager server.

5. Click **Backup** to start the backup.

   Figure 4-18 shows an example of the VSS full backup selection for all databases in a Microsoft SQL Server instance. Note that only the full backup option is available.

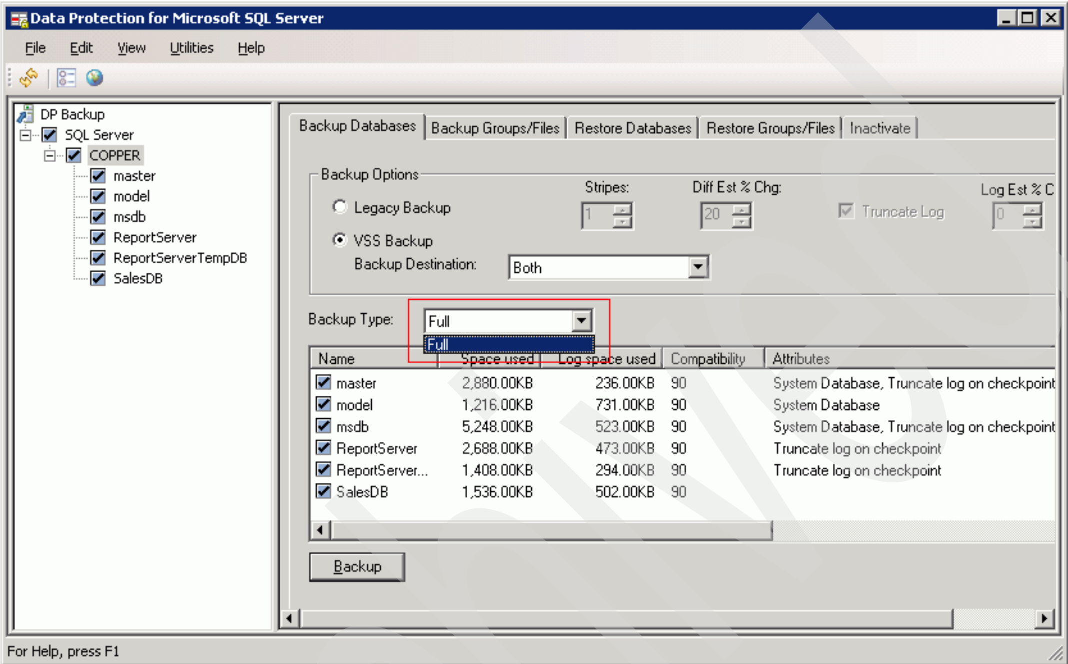

Figure 4-18 VSS full backup

After you click **Backup**, the following activities are performed by Data Protection for SQL Server:

1. A connection to the local DSM agent is established, as shown in Figure 4-19.

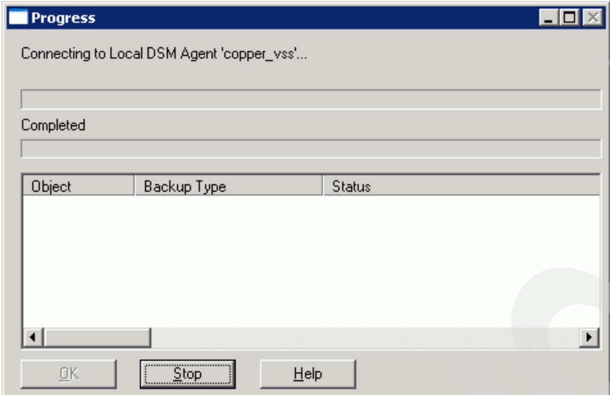

Figure 4-19 Connection to local DSM agent for VSS backup

2. After a connection to the local DSM agent is established, Data Protection for SQL Server queries the local DSM agent to gather information about the VSS configuration, as shown in Figure 4-20.

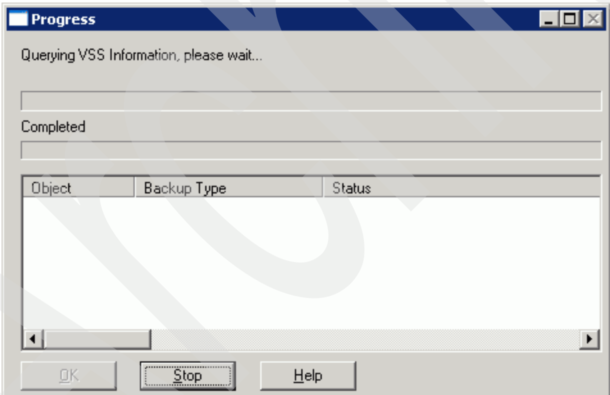

Figure 4-20 Querying VSS information about local DSM agent node

Then the VSS backup of the selected databases is started, as shown in Figure 4-21.

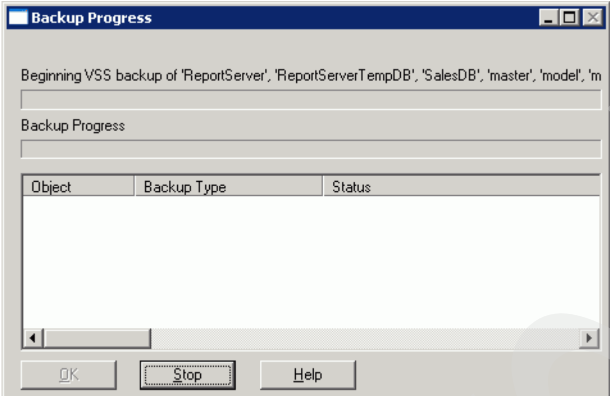

Figure 4-21 Start of VSS backup operation

3. The progress of the VSS backup operation is reported in the Backup Progress window. When the backup finishes, a report providing the VSS backup results is displayed, as shown in Figure 4-22.

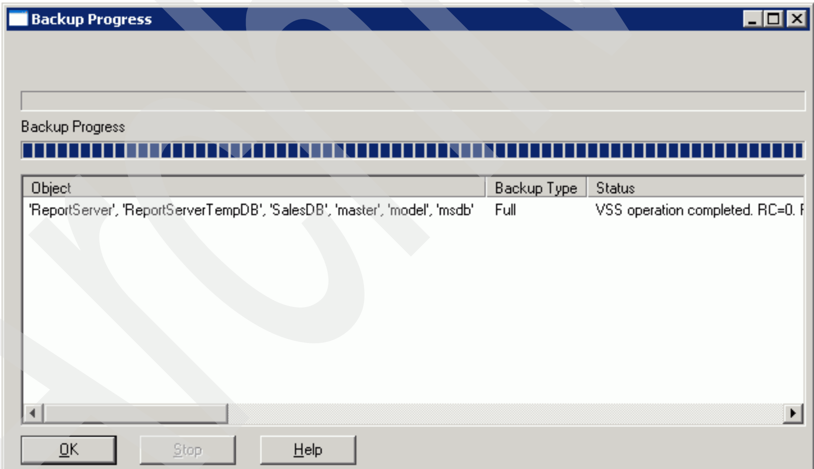

Figure 4-22 VSS backup report

4.3.2 VSS offloaded backup using the GUI

An offloaded backup uses an alternate machine to move SQL Server data to Tivoli Storage Manager server storage. This may reduce the impact on network, I/O, and CPU resources during backup processing.

Performing a VSS GUI offloaded backup is very similar to a performing a normal VSS GUI backup. The differences are that you must configure the `remotedsmagentnode` parameter in the Data Protection for SQL Server configuration file (tdpsql.cfg by default), using either the Configuration task in the Edit menu of the GUI or the **`tdpsqlc set`** command. Then, in the **Backup Databases** tab, choose **TSM Server (Offloaded)** in the Backup Destination list box, as shown in Figure 4-23.

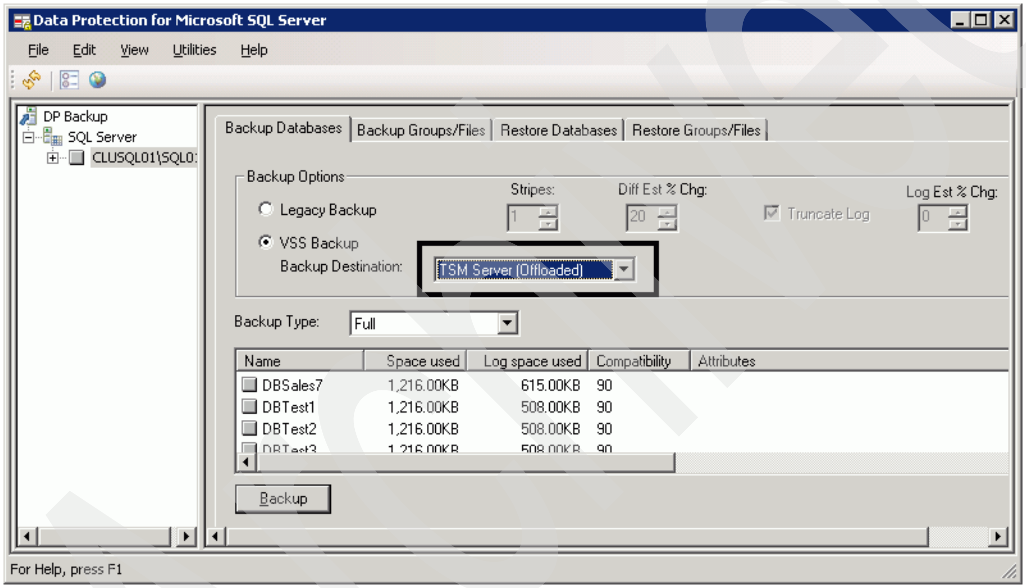

Figure 4-23 VSS offloaded backup selection

4.4 Working with existing backups using the GUI

With the Data Protection for SQL Server GUI, you can display information about existing backups, and manually inactivate backups.

This section covers:

- Displaying existing backups
- Inactivating Legacy backups

4.4.1 Displaying existing backups using the GUI

You can use the **Restore Databases** tab and the **Restore Groups/Files** tab to list the existing Legacy and VSS backups for a Microsoft SQL Server instance, The **Restore Databases** tab displays full, differential, and log backups, and the **Restore Groups/Files** tab displays full, log, groups, file, and set backups.

Figure 4-24 shows an example of backups displayed in the **Restore Databases** tab for the SalesDB database.

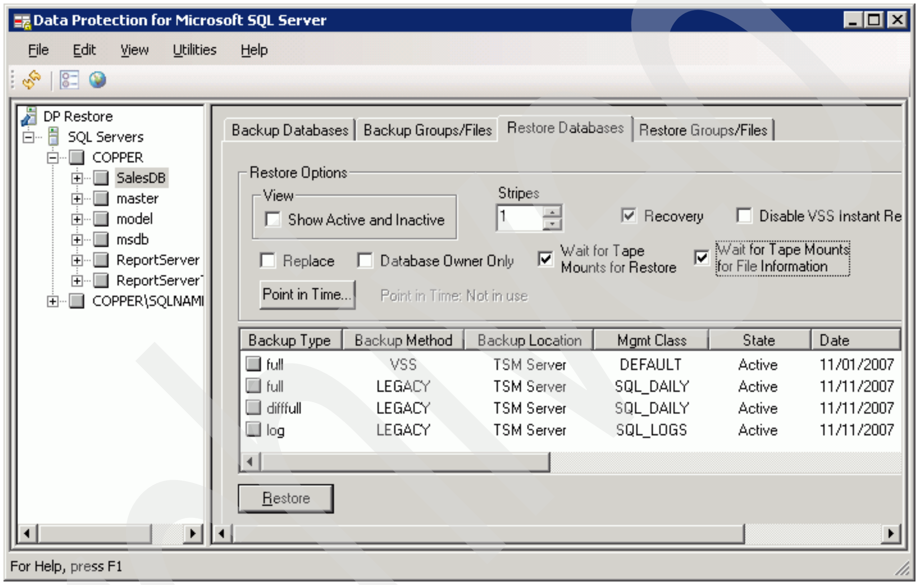

Figure 4-24 List database backups in the Restore Databases tab

Figure 4-25 shows an example of the backups displayed in the **Restore Groups/File** tab for the SalesDB database.

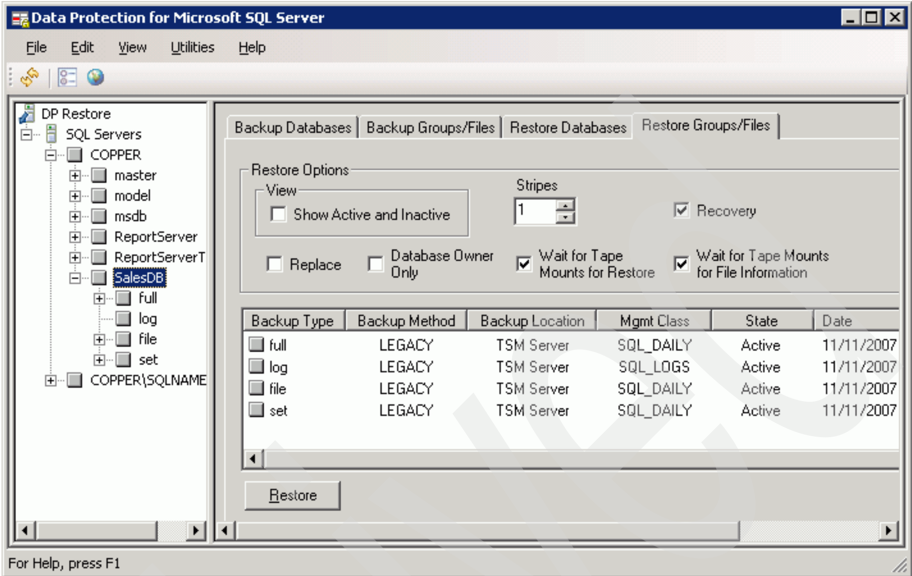

Figure 4-25 List database backups in the Restore Groups/Files tab

By default, only active backups are displayed. To display both active and inactive backups, check the **Show Active and Inactive** check box.

Figure 4-26 shows both active and inactive backups for the SalesDB database.

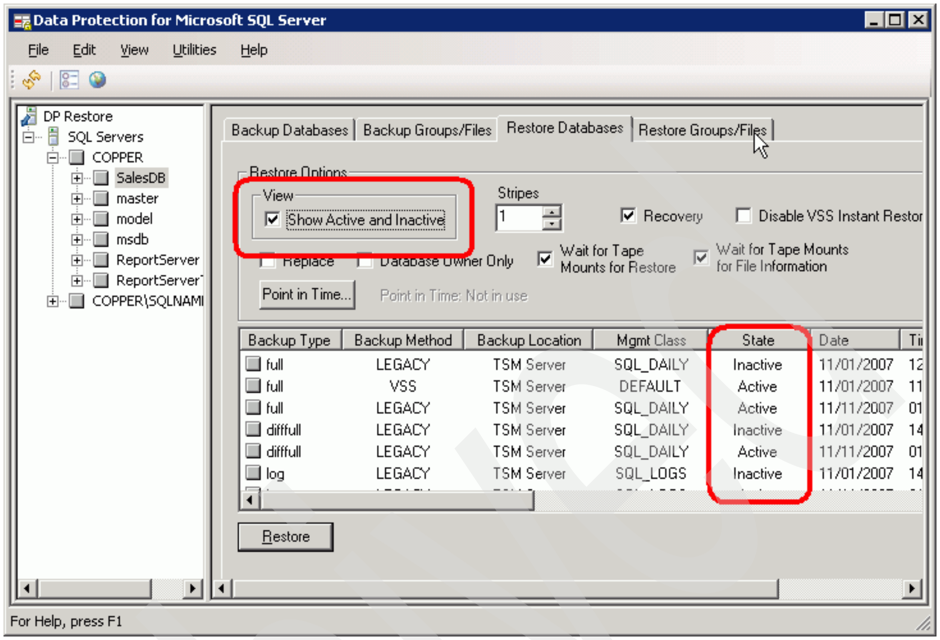

Figure 4-26 Displaying inactive backups

4.4.2 Inactivating backups using the GUI (Legacy only)

The Data Protection for SQL Server GUI tool enables you to inactivate all active objects, all objects of a particular backup type, or specific objects.

Only those backups performed since the last full backup are considered to be active. When you perform a Legacy full database backup, all backups taken since the previous full backup are automatically inactivated. However, this does not mean they cannot be used anymore to restore your databases. You can still use an inactive backup as long as it is not expired from the Tivoli Storage Manager inventory. Once a backup has been expired from the Tivoli Storage Manager inventory, it can no longer be used in a restore operation. Other backup types also inactivate previous backups, as can be seen in Table 4-2.

Table 4-2 Automatic inactivation by backups

Backup type	Backup inactivated
Legacy full backup	All prior active backup objects for the same SQL Server database

Backup type	Backup inactivated
Legacy differential backup	All differential backups taken since the last full backup for the same SQL Server database
Legacy log backup	Does not inactivate any backup
Legacy group backup	All group backups taken since the last full backup for the same filegroup for the same SQL Server database
Legacy file backup	All file backups taken since the last full backup for the same file for the same SQL Server database
Legacy set backup	Does not inactivate any backup

Tivoli Storage Manager never expires the active backup. If you drop a Microsoft SQL Server database, its active backup remains in the Tivoli Storage Manager server inventory until it is manually inactivated, and then it is expired. The space allocated for this backup is deallocated from Tivoli Storage Manager server.

In fact, when you inactivate a backup, you select it to participate in Tivoli Storage Manager expiration processing. Typical backups do not require this command because Data Protection for SQL Server performs inactivation as a part of Tivoli Storage Manager policy management. As a result, backup objects are typically inactivated as part of the scheduled backup processing.

Note: You must manually enable the **Inactivate** tab. See “View menu” on page 136 for more information.

Figure 4-27 shows the **Inactivate** tab. In the next example, we selected all backups on SalesDB to be inactivated.

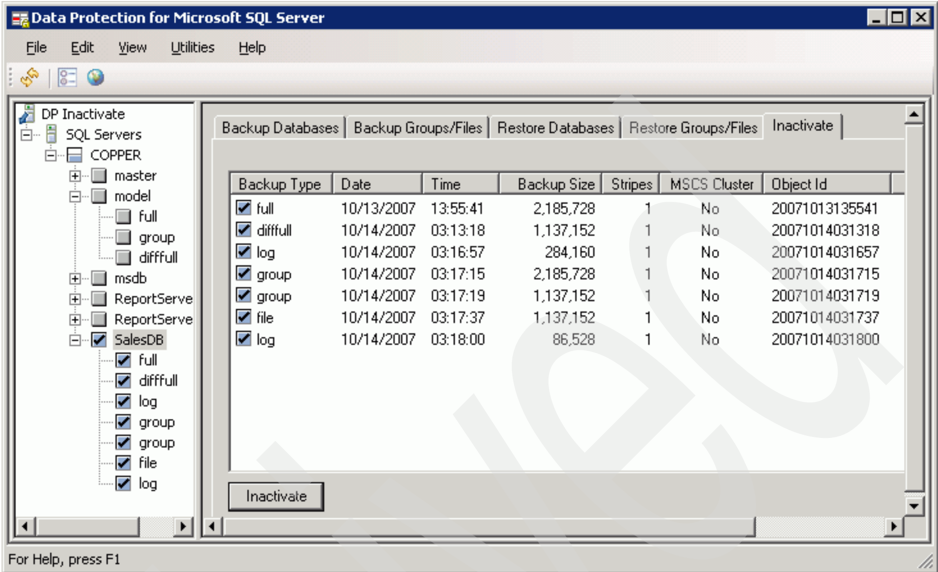

Figure 4-27 Inactivate tab

To inactivate the backups, click **Inactivate**. Figure 4-28 displays the backups that were inactivated in our example.

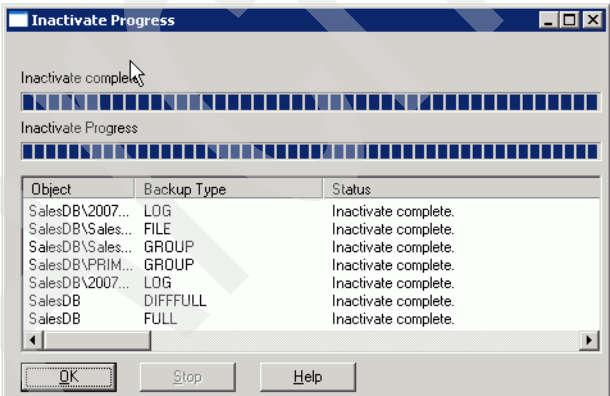

Figure 4-28 Backups inactivated

Figure 4-29 shows an example of a full backup automatically inactivating previous backups for a database. You do not need to worry about the inactivation messages.

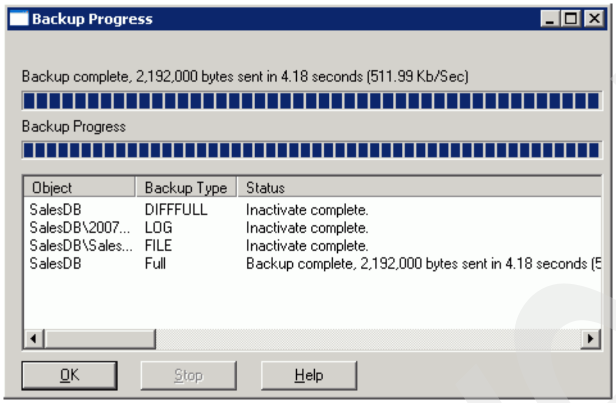

Figure 4-29 Automatic inactivation by Legacy full backup

4.5 CLI overview

The Data Protection for SQL Server CLI is **`tdpsqlc.exe`**. It is located in the directory where Data Protection for SQL Server is installed; \Program Files\Tivoli\TSM\TDPSql is the default directory. Issue the **`tdpsqlc ?`** or **`tdpsqlc help`** command to display help for the command-line interface. The Data Protection for SQL Server CLI provides the commands listed on Table 4-3.

Table 4-3 Data Protection for SQL Server CLI commands

Command	Description
`Backup`	Backs up all or part of one or more SQL Server databases to the Tivoli Storage Manager server
`Query`	Displays information about servers, databases, backup objects, and Data Protection for SQL configuration
`Restore`	Restores all or part of one or more SQL Server databases to SQL server
`INACTIVate`	Inactivates one or more active backup objects on the Tivoli Storage Manager server
`Help`	Displays the syntax of Data Protection for SQL Server commands.

Command	Description
`Set`	Changes the values of configuration parameters
`CHANGETSMPassword`	Changes the Tivoli Storage Manager password used by Data Protection for SQL Server

By default, **`tdpsqlc`** uses the parameters stored in the tdpsql.opt configuration file. To specify a different configuration file, you can use the parameter `/CONFIGfile =` *`configfilename`*, where *configfilename* is the name of Data Protection for SQL Server configuration file. Other useful parameters are `/sqlserver` and `/tsmoptfile`. When you specify the `/sqlserver` parameter, Data Protection for SQL Server overrides the default SQL server, which is the local SQL server. You must use this switch to access Microsoft SQL Server named instances and SQL Server clustered instances. When you specify `/tsmoptfile`, it overrides the default Tivoli Storage Manager API option file (dsm.opt).

You can also use **tdpsqlc** parameters to specify customized settings for your operations. One example is the parameter `/BACKUPMethod`, that you can specify to choose the type of backup you want to perform: Legacy or VSS. If you omit this parameter, the value specified for the `BACKUPMethod` parameter in the configuration file is used.

> **Note:** Data Protection for SQL Server CLI parameters are not case sensitive; however, all SQL names of databases or parts of databases are case sensitive.

For a detailed explanation of the command-line **tdpsql** tool, refer to *IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server Installation and User's Guide*, SC32-9059.

4.5.1 Data Protection for SQL Server V5.5 CLI new features

In Data Protection for SQL Server releases prior to V5.5, to control which databases are included and excluded from backup operations, you use INCLUDE and EXCLUDE statements. The INCLUDE and EXCLUDE statements are stored, by default, in the dsm.opt configuration file. You have the flexibility to include or exclude individual databases from a specific backup type - for example, excluding offline databases from backup operations or excluding databases using simple recovery models from transaction log backups.

This option is still available in Data Protection for SQL Server V5.5; however, the Data Protection for SQL Server V5.5 CLI introduces a new parameter to the backup command and provides two built-in features to provide greater flexibility and control over backup operations.

The new CLI parameter introduced in the backup command is the `/EXCLUDEDB` parameter. With this parameter, available for all Legacy and VSS backup types, you can exclude databases from being backed up directly in the Data Protection for SQL Server CLI backup command, instead of having to change the EXCLUDE statements in the dsm.opt file. Example 4-2 on page 165 shows an example of a full Legacy backup with the /EXCLUDEDB parameter.

The two built-in features introduced in Data Protection for SQL Server V5.5 are:

- Automatic exclusion of simple recovery model databases from CLI log backups. An example of this built-in functionality is shown in Example 4-4 on page 167.
- Automatic exclusion of master databases from CLI log and differential backups. An example of this built-in functionality is shown in Example 4-6 on page 169.

For more information about new features in Data Protection for SQL Server V5.5, refer to *IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server Installation and User's Guide*, SC32-9059.

4.6 Legacy backups using the CLI

In this section we discuss how to perform Microsoft SQL Server backups using the Data Protection for SQL Server CLI tool. In the examples in the following sections, we assume that you already have installed and configured Data Protection for SQL Server.

The following sections show how to perform similar backups to those performed in 4.2, "Legacy backups using the GUI" on page 141 using the Data Protection for SQL Server CLI tool.

> **Note:** For the examples in the following sections, we use the default configuration parameters stored in the tdpsql.cfg file. The parameter `BACKUPMethod` is configured as Legacy.

4.6.1 Full database backups using the CLI

Example 4-1 shows a full database backup and its output. Example 4-2 on page 165 backs up all databases and produces the same result as the GUI example shown in 4.2.1, "Full database backups using the GUI" on page 141.

Example 4-1 CLI Legacy full database backup

```
C:\>tdpsqlc backup * full

IBM Tivoli Storage Manager for Databases:
Data Protection for Microsoft SQL Server
Version 5, Release 5, Level 0.0
(C) Copyright IBM Corporation 1997, 2007. All rights reserved.

Connecting to SQL Server, please wait...

Starting SQL database backup...

Connecting to TSM Server as node 'COPPER_SQL'...

Beginning full backup for database master, 1 of 6.
Full: 0   Read: 3230464  Written: 3230464  Rate: 278.47 Kb/Sec
Backup of master completed successfully.

Beginning full backup for database model, 2 of 6.
Full: 0   Read: 2184960  Written: 2184960  Rate: 534.51 Kb/Sec
Backup of model completed successfully.

Beginning full backup for database msdb, 3 of 6.
Full: 0   Read: 6377216  Written: 6377216  Rate: 1,262.72 Kb/Sec
Backup of msdb completed successfully.

Beginning full backup for database ReportServer, 4 of 6.
Full: 0   Read: 3231488  Written: 3231488  Rate: 646.80 Kb/Sec
Backup of ReportServer completed successfully.

Beginning full backup for database ReportServerTempDB, 5 of 6.
Full: 0   Read: 2182912  Written: 2182912  Rate: 426.69 Kb/Sec
Backup of ReportServerTempDB completed successfully.

Beginning full backup for database SalesDB, 6 of 6.
Full: 0   Read: 2192000  Written: 2192000  Rate: 433.15 Kb/Sec
Backup of SalesDB completed successfully.
```

```
Total SQL backups selected:             6
Total SQL backups attempted:            6
Total SQL backups completed:            6
Total SQL backups excluded:             0
Total SQL backups inactivated:          0

Throughput rate:                        539.79 Kb/Sec
Total bytes transferred:                19,399,040
Elapsed processing time:                35.10 Secs
```

As discussed in 4.5.1, “Data Protection for SQL Server V5.5 CLI new features” on page 162, it is possible to exclude a database from a backup operation using the `/excludedb` parameter, as shown in Example 4-2. In this example, we exclude the databases ReportServer and ReportServerTempDB from the backup operation.

Example 4-2 Exclusion of a database in a full database backup operation

```
C:\>tdpsqlc backup * full /excludedb=ReportServer,ReportServerTempDB

IBM Tivoli Storage Manager for Databases:
Data Protection for Microsoft SQL Server
Version 5, Release 5, Level 0.0
(C) Copyright IBM Corporation 1997, 2007. All rights reserved.

Connecting to SQL Server, please wait...

Starting SQL database backup...

Connecting to TSM Server as node 'COPPER_SQL'...

Beginning full backup for database master, 1 of 4.
Full: 0   Read: 3231488  Written: 3231488  Rate: 353.31 Kb/Sec
Backup of master completed successfully.

Beginning full backup for database model, 2 of 4.
Full: 0   Read: 2187008  Written: 2187008  Rate: 398.16 Kb/Sec
Backup of model completed successfully.

Beginning full backup for database msdb, 3 of 4.
Full: 0   Read: 7425792  Written: 7425792  Rate: 1,335.74 Kb/Sec
Backup of msdb completed successfully.

Beginning full backup for database SalesDB, 4 of 4.
```

```
Full: 0   Read: 2192000  Written: 2192000  Rate: 468.92 Kb/Sec
Backup of SalesDB completed successfully.


Total SQL backups selected:             6
Total SQL backups attempted:            4
Total SQL backups completed:            4
Total SQL backups excluded:             2
Total SQL backups inactivated:          0

Throughput rate:                        604.05 Kb/Sec
Total bytes transferred:                15,036,288
Elapsed processing time:                24.31 Secs
```

4.6.2 Transaction log backups using the CLI

Example 4-3 shows transaction log backup and its output. We back up the SalesDB transaction log, similar to the process we described for the GUI example shown in 4.2.2, "Transaction log backups using the GUI" on page 143.

Example 4-3 CLI Legacy transaction log backup

```
C:\>tdpsqlc backup SalesDB log

IBM Tivoli Storage Manager for Databases:
Data Protection for Microsoft SQL Server
Version 5, Release 5, Level 0.0
(C) Copyright IBM Corporation 1997, 2007. All rights reserved.

Connecting to SQL Server, please wait...


Starting SQL database backup...

Connecting to TSM Server as node 'COPPER_SQL'...

Beginning log backup for database SalesDB, 1 of 1.
Full: 0   Read: 26240  Written: 26240  Rate: 37.08 Kb/Sec
Backup of SalesDB completed successfully.


Total SQL backups selected:             1
Total SQL backups attempted:            1
Total SQL backups completed:            1
```

```
Total SQL backups excluded:             0

Throughput rate:                        36.71 Kb/Sec
Total bytes transferred:                26,240
Elapsed processing time:                0.70 Secs
```

A new Data Protection for SQL Server feature is useful when performing transaction log backups: the ability to automatically exclude databases using the simple recovery model (or truncate log on checkpoint option) from log backups. With this new feature, you can simply ask Data Protection for SQL Server to perform transaction log backups for all databases from a SQL server, and Data Protection for SQL detects the databases using the simple recovery model and automatically excludes them from the backup operation.

Example 4-4 shows an example of this new feature.

Example 4-4 Automatic exclusion of simple recovery model databases from transaction log backup

```
C:\>tdpsqlc backup * log

IBM Tivoli Storage Manager for Databases:
Data Protection for Microsoft SQL Server
Version 5, Release 5, Level 0.0
(C) Copyright IBM Corporation 1997, 2007. All rights reserved.

Connecting to SQL Server, please wait...


Starting SQL database backup...

Connecting to TSM Server as node 'COPPER_SQL'...

Beginning log backup for database model, 1 of 2.
Full: 0   Read: 1535744  Written: 1535744  Rate: 1,315.57 Kb/Sec
Backup of model completed successfully.

Beginning log backup for database SalesDB, 2 of 2.
Full: 0   Read: 223872  Written: 223872  Rate: 193.99 Kb/Sec
Backup of SalesDB completed successfully.


Total SQL backups selected:             6
Total SQL backups attempted:            2
Total SQL backups completed:            2
```

```
Total SQL backups excluded:              4

Throughput rate:                         754.33 Kb/Sec
Total bytes transferred:                 1,759,616
Elapsed processing time:                 2.28 Secs
```

4.6.3 Differential backups using the CLI

Example 4-5 shows a differential backup and its output. We back up the SalesDB database, similar to the process described for the GUI example shown in 4.2.3, "Differential backups using the GUI" on page 145.

Example 4-5 CLI Legacy differential backup

```
C:\>tdpsqlc backup SalesDB diff

IBM Tivoli Storage Manager for Databases:
Data Protection for Microsoft SQL Server
Version 5, Release 5, Level 0.0
(C) Copyright IBM Corporation 1997, 2007. All rights reserved.

Connecting to SQL Server, please wait...


Starting SQL database backup...

Connecting to TSM Server as node 'COPPER_SQL'...

Beginning difffull backup for database SalesDB, 1 of 1.
Full: 0   Read: 1143424  Written: 1143424  Rate: 270.37 Kb/Sec
Backup of SalesDB completed successfully.


Total SQL backups selected:              1
Total SQL backups attempted:             1
Total SQL backups completed:             1
Total SQL backups excluded:              0

Throughput rate:                         269.91 Kb/Sec
Total bytes transferred:                 1,143,424
Elapsed processing time:                 4.14 Secs
```

A new Data Protection for SQL Server feature is useful when performing differential backups: the ability to automatically exclude the master database from differential backups. With this new feature, you can simply ask Data Protection for SQL Server to perform differential backup for all databases from a Microsoft SQL Server, and Data Protection for SQL automatically excludes the master database from the backup operation.

Example 4-6 shows the automatic exclusion of a master database in differential backups.

Example 4-6 Automatic exclusion of master database from differential backups

```
C:\>tdpsqlc backup * diff

IBM Tivoli Storage Manager for Databases:
Data Protection for Microsoft SQL Server
Version 5, Release 5, Level 0.0
(C) Copyright IBM Corporation 1997, 2007. All rights reserved.

Connecting to SQL Server, please wait...

Starting SQL database backup...

Connecting to TSM Server as node 'COPPER_SQL'...

Beginning difffull backup for database model, 1 of 5.
Full: 0   Read: 1138432  Written: 1138432  Rate: 285.94 Kb/Sec
Backup of model completed successfully.

Beginning difffull backup for database msdb, 2 of 5.
Full: 0   Read: 2182912  Written: 2182912  Rate: 403.21 Kb/Sec
Backup of msdb completed successfully.

Beginning difffull backup for database ReportServer, 3 of 5.
Full: 0   Read: 1134336  Written: 1134336  Rate: 243.19 Kb/Sec
Backup of ReportServer completed successfully.

Beginning difffull backup for database ReportServerTempDB, 4 of 5.
Full: 0   Read: 1134336  Written: 1134336  Rate: 246.77 Kb/Sec
Backup of ReportServerTempDB completed successfully.

Beginning difffull backup for database SalesDB, 5 of 5.
Full: 0   Read: 1143424  Written: 1143424  Rate: 245.36 Kb/Sec
Backup of SalesDB completed successfully.


Total SQL backups selected:             6
Total SQL backups attempted:            5
```

```
Total SQL backups completed:            5
Total SQL backups excluded:             1

Throughput rate:                        288.53 Kb/Sec
Total bytes transferred:                6,733,440
Elapsed processing time:                22.79 Secs
```

4.6.4 Group backups using the CLI

Example 4-7 shows a group backup and its output. We back up the SalesDB_LA filegroup of the SalesDB database, similar to the process described in the GUI example shown in 4.2.4, “Group backups using the GUI” on page 146.

Example 4-7 CLI Legacy group backup

```
C:\>tdpsqlc backup SalesDB group=SalesDB_LA

IBM Tivoli Storage Manager for Databases:
Data Protection for Microsoft SQL Server
Version 5, Release 5, Level 0.0
(C) Copyright IBM Corporation 1997, 2007. All rights reserved.

Connecting to SQL Server, please wait...


Starting SQL database backup...

Connecting to TSM Server as node 'COPPER_SQL'...

Beginning group backup for database SalesDB, 1 of 1.
Full: 0   Read: 1139968  Written: 1139968  Rate: 266.33 Kb/Sec
Backup of SalesDB completed successfully.

Total SQL backups selected:             1
Total SQL backups attempted:            1
Total SQL backups completed:            1
Total SQL backups excluded:             0

Throughput rate:                        265.95 Kb/Sec
Total bytes transferred:                1,139,968
Elapsed processing time:                4.19 Secs
```

Note: We recommend you follow group backups with transaction log backups for all SQL Server databases you back up.

4.6.5 File backups using the CLI

Example 4-8 shows an example of a file backup and its output. In this example, only the file SalesDB_LA_1 is backed up. All other files from the SalesDB_LA filegroup are not included in this backup. It produces the same result as the process described for the GUI example shown in 4.2.5, “File backups using the GUI” on page 147.

Example 4-8 CLI Legacy file backup

```
C:\>tdpsqlc backup SalesDB file=SalesDB_LA_1

IBM Tivoli Storage Manager for Databases:
Data Protection for Microsoft SQL Server
Version 5, Release 5, Level 0.0
(C) Copyright IBM Corporation 1997, 2007. All rights reserved.

Connecting to SQL Server, please wait...


Starting SQL database backup...

Connecting to TSM Server as node 'COPPER_SQL'...

Beginning file backup for database SalesDB, 1 of 1.
Full: 0   Read: 1138304  Written: 1138304  Rate: 264.55 Kb/Sec
Backup of SalesDB completed successfully.


Total SQL backups selected:               1
Total SQL backups attempted:              1
Total SQL backups completed:              1
Total SQL backups excluded:               0

Throughput rate:                          264.17 Kb/Sec
Total bytes transferred:                  1,138,304
Elapsed processing time:                  4.21 Secs
```

Note: We recommend you follow file backups with transaction log backups for all SQL Server databases you back up.

4.6.6 Set backups using the CLI

Example 4-9 shows a file backup and its output. In this example, the filegroup SalesDB_EMEA and the file SALESDB_LA_2 from the filegroup SalesDB_LA are backed up. It produces the same result as the process we described for the GUI example shown in 4.2.6, “Set backups using the GUI” on page 149.

Example 4-9 CLI Legacy set backups

```
C:\>tdpsqlc backup SalesDB set /group=SalesDB_EMEA /file=SalesDB_LA_2

IBM Tivoli Storage Manager for Databases:
Data Protection for Microsoft SQL Server
Version 5, Release 5, Level 0.0
(C) Copyright IBM Corporation 1997, 2007. All rights reserved.

Connecting to SQL Server, please wait...


Starting SQL database backup...

Connecting to TSM Server as node 'COPPER_SQL'...

Beginning set backup for database SalesDB, 1 of 1.
Full: 0   Read: 1139456  Written: 1139456  Rate: 281.71 Kb/Sec
Backup of SalesDB completed successfully.

Total SQL backups selected:               1
Total SQL backups attempted:              1
Total SQL backups completed:              1
Total SQL backups excluded:               0

Throughput rate:                          281.28 Kb/Sec
Total bytes transferred:                  1,139,456
Elapsed processing time:                  3.96 Secs
```

Note: We recommend you follow set backups with transaction log backups for all SQL Server databases you back up.

4.6.7 Tail-log backups using the CLI

Example 4-10 shows a transaction log backup and its output. We back up the SalesDB transaction tail log, similar to the process we described for the GUI example shown in 4.2.7, “Tail-log backups using the GUI” on page 150.

Example 4-10 CLI Legacy tail-log backup

```
C:\>tdpsqlc backup SalesDB log /trunc=no

IBM Tivoli Storage Manager for Databases:
Data Protection for Microsoft SQL Server
Version 5, Release 5, Level 0.0
(C) Copyright IBM Corporation 1997, 2007. All rights reserved.

Connecting to SQL Server, please wait...


Starting SQL database backup...

Connecting to TSM Server as node 'COPPER_SQL'...

Beginning log backup for database SalesDB, 1 of 1.
Full: 0   Read: 223872  Written: 223872  Rate: 171.74 Kb/Sec
Backup of SalesDB completed successfully.


Total SQL backups selected:               1
Total SQL backups attempted:              1
Total SQL backups completed:              1
Total SQL backups excluded:               0

Throughput rate:                          170.93 Kb/Sec
Total bytes transferred:                  223,872
Elapsed processing time:                  1.28 Secs
```

Note: Tail-log backups are intended only for special situations. Refer to 2.4.4, “Backing up a transaction log without truncating the log” on page 54 for more information.

4.7 VSS backups using the CLI

With Data Protection for SQL Server, you can only perform full VSS backups. Two types of VSS backups are available with Data Protection for SQL Server:

- VSS full backup
- VSS offloaded full backup

In the following sections, we discuss how to perform both VSS backup types using the CLI.

4.7.1 VSS full backup using the CLI

Example 4-11 shows a VSS full database backup and its output. We back up all databases, similar to the process we described for the GUI example shown in 4.3.1, “Full VSS backup using the GUI” on page 151.

Example 4-11 CLI VSS full backup

```
C:\>tdpsqlc backup * full /backupmethod=VSS

IBM Tivoli Storage Manager for Databases:
Data Protection for Microsoft SQL Server
Version 5, Release 5, Level 0.0
(C) Copyright IBM Corporation 1997, 2007. All rights reserved.

Connecting to SQL Server, please wait...

Connecting to TSM Server as node 'COPPER_SQL'...
Connecting to Local DSM Agent 'copper_vss'...

Starting SQL database backup...


Beginning VSS backup of 'ReportServer', 'ReportServerTempDB',
'SalesDB', 'master', 'model', 'msdb'...


Preparing to backup using snapshot.
   Files Examined/Completed/Failed: [ 64 / 64 / 0 ]   Total Bytes:
6183635

VSS Backup operation completed with rc = 0
   Files Examined   : 64
   Files Completed  : 64
```

```
Files Failed     : 0
Total Bytes      : 6183635
```

4.7.2 VSS offloaded backup using the CLI

An offloaded backup uses an alternate machine to move SQL Server data to Tivoli Storage Manager server storage. This may reduce the impact on network, I/O, and CPU resources during backup processing.

A VSS offloaded backup using the CLI is similar to performing a normal VSS CLI backup. The differences are that you must configure the `remotedsmagentnode` parameter in the Data Protection for SQL Server configuration file (tdpsql.cfg by default) using either the **Configuration** task in the Edit menu of the GUI or the **`tdpsqlc set`** command with the `/offload` parameter for the Data Protection for SQL Server CLI command, as shown in Example 4-12.

Example 4-12 CLI VSS offloaded backup

```
C:\>tdpsqlc backup * full /backupmethod=VSS /backupdestination=TSM
/offload
```

4.8 Working with existing backups using the CLI

With the Data Protection for SQL Server GUI, you can display information about existing backups and manually inactivate backups.

This section covers:

- Displaying existing backups
- Inactivating Legacy backups

4.8.1 Displaying existing backups using the CLI

You use the QUERY command to display information about the Microsoft SQL Server and its databases, about the Tivoli Storage Manager server and its backup objects, and about Data Protection for SQL Server. Table 4-4 on page 176 shows useful query commands.

Table 4-4 Useful query commands

To display information about . . .	Use the command
Microsoft SQL Server instance	`tdpsqlc query sql /compat`
All SQL server databases	`tdpsqlc query sql * /compat`
A specific SQL server database	`tdpsqlc query sql SalesDB /compat`[a]
Data Protection for SQL Server configuration file information	`tdpsqlc query tdp`
All active Legacy backup types for all databases	`tdpsqlc query tsm * types /active`
All active and inactive Legacy backup types for all databases	`tdpsqlc query tsm * types /all`
All active and inactive Legacy backup types for a specific database	`tdpsqlc query tsm SalesDB types /all`[a]
Active backups for all databases[b]	`tdpsqlc query tsm *`
Active backups for a specific database	`tdpsqlc query tsm SalesDB`[a]
Active full backups for a specific database including compatibility information[b]	`tdpsqlc query tsm SalesDB full /compat`[a]
Active full backups for a specific database including compatibility information[b]	`tdpsqlc query tsm SalesDB full /compat /active`[a]
Active and inactive full backups for a specific database including file information	`tdpsqlc query tsm SalesDB full /fileinfo /mountwait=yes /all`[a]

a. Change SalesDB to the database name you want to display information.
b. VSS and Legacy backups.

For a detailed discussion about the query command, refer to *IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server Installation and User's Guide*, SC32-9059.

4.8.2 Inactivating backups using the CLI (Legacy only)

You use the INACTIVATE command to inactivate one or more active backup objects on the Tivoli Storage Manager server.

Inactivating backups through the Data Protection for SQL Server CLI gives you more flexibility in contrast with the Data Protection for SQL Server GUI. Using the CLI, you can inactivate backups older than a specified number of days, while when using the GUI, you must individually select the desired objects to inactivate.

You can use the parameter `/olderthan` to specify how old a backup object must be before the command can inactivate it. The number of days can range from 0 to 9999, and if you select 0 you inactivate all selected objects. This parameter has no default value.

Example 4-13 shows an example of how to inactivate all backups for a SQL server. It is similar to the GUI example shown in 4.4.2, “Inactivating backups using the GUI (Legacy only)” on page 158.

Example 4-13 Inactivating all backups

```
C:\>tdpsqlc inactiv * *

IBM Tivoli Storage Manager for Databases:
Data Protection for Microsoft SQL Server
Version 5, Release 5, Level 0.0
(C) Copyright IBM Corporation 1997, 2007. All rights reserved.

Connecting to TSM Server as node 'COPPER_SQL'...

Starting Sql database backup inactivation...
Querying Tivoli Storage Manager server for a list of database backups,
please wait...


Inactivating full backup master
Inactivating full backup model
Inactivating full backup msdb
Inactivating full backup ReportServer
Inactivating full backup ReportServerTempDB
Inactivating full backup SalesDB
Inactivating set backup SalesDB\20071020024434\00001774
Inactivating set backup SalesDB\20071020024714\000017A0
Inactivating set backup SalesDB\20071020024845\00000774
Inactivating log backup SalesDB\20071020025936\00001420

Total database backups inspected:                    10
Total database backups requested for inactivation:   10
Total database backups inactivated:                  10
Total database skipped:                              0

Elapsed processing time:                             0.30 Secs
```

5

Data Protection for SQL Server restore

In this chapter we discuss how to use the Data Protection for SQL Server graphical user interface (GUI) and command-line interface (CLI) to restore Microsoft SQL Server databases. An introduction to the Data Protection for SQL Server GUI and CLI is provided in 4.1, “GUI overview” on page 128 and 4.5, “CLI overview” on page 161, respectively. In this chapter we assume that you are familiar with the Data Protection for SQL Server GUI and CLI tools.

In this chapter, we also provide several examples to demonstrate how to perform restores for some common situations. We also discuss how to use Data Protection for SQL Server to implement a standby database.

This chapter covers the following:

5.1 Considerations for restore operations

Before you restore a database, you must consider several factors for a successful restore operation. For each specific restore scenario, a different level of complexity is required for the restore operation. Data Protection for SQL Server provides various options for restoring a simple database from a full backup on the same server to restoring all databases on a different server - in a disaster recovery scenario, for example.

It is important to understand that the restore capabilities for a Microsoft SQL Server are directly related to the backup operations performed for the databases. A well-planned and implemented set of backup routines are crucial for a successful restore operation; in other words, you cannot restore what has not been backed up. See 2.3, "Microsoft SQL Server backup planning" on page 42 for a discussion of Microsoft SQL Server backup planning.

Another important point is that you may experience unexpected hardware or software failures during a restore operation. You can minimize this risk by regularly testing your restore routines to make sure they are working as expected.

When you restore a database, keep in mind that the data that exists in the database is overwritten and is no longer available after the restore is complete. The Data Protection for SQL Server Restore Databases feature enables you to restore databases or parts of databases only from full, differential, and log backups. Although only VSS full backups are supported, Legacy differential and Legacy log backups can be applied after a full VSS backup has been restored.

A master database restore requires special attention. See 5.4.3, "Restoring Microsoft SQL Server system databases" on page 190 for step-by-step instructions.

5.1.1 Displaying list of backups

Before you start a restore process, you must check which backups are available for the database you want to restore.

Using the Data Protection for SQL Server GUI, you can use the **Restore Databases** tab to display full, differential, and log backups, and the **Restore Groups/Files** tab to display full, log, group, set, and file backups. Legacy and VSS backups are displayed together. For more information, refer to 4.4.1, "Displaying existing backups using the GUI" on page 156.

From the Data Protection for SQL Server CLI, you can issue the `query` command. For more information about the `query` command, see 4.8.1, “Displaying existing backups using the CLI” on page 175. or refer to *IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server Installation and User’s Guide*, SC32-9059.

5.1.2 VSS considerations

Be aware of the following considerations when performing VSS restores. Unless otherwise specified, “VSS restores” refers to all restore types that use VSS (VSS Restore, VSS Fast Restore, and VSS Instant Restore):

- If you plan to perform a VSS Restore of the master database, see 5.4.3, “Restoring Microsoft SQL Server system databases” on page 190.
- A VSS Instant Restore overwrites the entire contents of the source volumes. However, you can avoid overwriting the source volumes by selecting the Disable VSS Instant Restore option. This option bypasses volume-level copy and uses file-level copy instead to restore the files from a VSS backup that resides on local shadow volumes. We recommend that the source volume contain only the SQL Server database.
- Be aware that when a VSS restore from local shadow volumes is performed, the bytes transferred will display “0”, which occurs because no data (“0”) is restored from the Tivoli Storage Manager server.
- To perform a VSS Instant Restore, the IBM Tivoli Storage Manager for Copy Services Hardware Devices Snapshot Integration Module must be installed.
- When performing VSS Instant Restores, you must make sure that any previous background copies (that involve the volumes being restored) are completed prior to initiating the VSS Instant Restore.

5.2 Performing restores using the GUI

Using the Data Protection for SQL Server GUI, you can perform full and partial restores of your databases. In a full restore, you restore all files belonging to the database, while in a partial restore, you choose to restore only individual files from the database.

If you plan to fully restore your database using full, log, and differential backups, click the **Restore Database** tab in the Data Protection for SQL Server GUI. If you plan to restore only parts of your database using full, file, group, set, or log backups select the **Restore Groups/Files** tabs in the Data Protection for SQL Server GUI.

Note: You can use both the **Restore Database** and **Restore Groups/Files** tabs to fully restore your database from a full backup and to apply the subsequent transaction log files. The difference between these two tabs is that in the **Restore Groups/Files** tab, you can choose individual files from the database full backup to be restored, while in the **Restore Database** tab, you restore all files from your database.

In next sections we discuss how to restore Microsoft SQL Server databases using the Data Protection for SQL Server GUI.

5.2.1 Performing a full database restore

Complete the following steps to restore a Microsoft SQL Server database using full, differential, and log backups.

1. Start the Data Protection for SQL Server GUI.
2. Click the **Restore Database** tab.
3. Check **Show Active and Inactive** if you want to display inactive backup objects in addition to active backup objects.
4. Click the plus sign (+) in the tree view to the left of the SQL server that you want to work with. All Microsoft SQL Servers backed up under the Tivoli Storage Manager node name are displayed.
5. Click the plus sign in the tree view to show the names of databases backed up on the Tivoli Storage Manager server. All databases backed up under the Tivoli Storage Manager node name are displayed, even those databases that were already dropped from the SQL server but were not expired from the Tivoli Storage Manager server inventory.
6. Click the plus sign in the tree view to the left of the SQL server that you want to restore from. The tree expands again and shows the databases available for restore processing.
7. Click the plus sign in the tree view to the left of the database that you want to restore. The database expands to show the types of backups available for restore.
8. Click the selection box in the tree view to the left of the full, differential, or transaction log backup that you want to restore.
9. Select the desired restore options for your backup.
10. Click **Restore**. The Restore Progress dialog appears.
11. Click **OK**. The restore is complete.

5.2.2 Performing a partial restore

The steps required to restore a Microsoft SQL Server file or filegroup using the Data Protection for SQL Server GUI are similar to those required for fully restoring a Microsoft SQL Server database:

1. Start the Data Protection for SQL Server GUI.
2. Click the **Restore Groups/Files** tab.
3. Check **Show Active and Inactive** if you want to display inactive backup objects in addition to active backup objects.
4. Click the plus sign in the tree view to the left of the Microsoft SQL Server that you want to work with. All Microsoft SQL Servers backed up under the Tivoli Storage Manager node name are displayed.
5. Click the plus sign in the tree view to show the names of databases backed up on the Tivoli Storage Manager server. All databases backed up under the Tivoli Storage Manager node name are displayed, even those databases that were already dropped from Microsoft SQL Server but were not expired from the Tivoli Storage Manager server inventory.
6. Click the plus sign in the tree view to the left of the SQL server that you want to restore from. The tree expands again and shows the databases available for restore processing.
7. Click the plus sign in the tree view to the left of the database that you want to restore. The database expands to show the types of backups available for restore.
8. Select the desired restore options for your backup.
9. If you want to replace the existing database object with the file or filegroup you are about to restore, check the **Replace** box.
10. If you want only the database owner to access the database after it has been restored, check the **Database Owner Only** box.
11. Click **Restore**. The Restore Progress dialog appears.
12. Click **OK**. The restore is complete.

5.2.3 Restore options

You can specify how the restore operation is performed using the **Restore Options** tab. From either the **Restore Databases** tab or the **Restore Groups/Files** tab, you can select the following options.

- Show Active and Inactive

  By checking this option, you can include inactive backup objects in the tree and list. This enables you to easily specify inactive objects for restore purposes. The default is to display only active objects.

- Stripes

  You can specify the number of data stripes to use in a restore operation. A maximum of 64 data stripes is allowed. The default value is 1. Make sure that this value matches the value set for SQL buffers. Note that this option is always enabled for Legacy operations. However, stripes are not available for VSS operations.

- Replace

  You can replace a database during a restore by selecting this check box. The default is not to replace databases. This option is always enabled and applies to Legacy restores only.

- Recovery

  If you select several objects for restore in the GUI (for example, full, differential, full log, and log) and leave this option selected, Data Protection for SQL Server ensures that SQL administers the recovery option only on the last backup object for each database being restored. This option is selected by default, but you can clear this check box when needed.

- Database Owner Only

  You can mark a database for owner use only after a restore by selecting this check box. The default is not to mark a database for owner use. This option is always enabled and applies to Legacy restores only.

- Wait for Tape Mounts for Restore

  You can specify whether or not the Data Protection for SQL Server restore operation waits for the Tivoli Storage Manager server to mount removable media such as tapes or CDs. This information is retrieved from Tivoli Storage Manager when you press the plus icon next to the backup object to expand the tree.

- Wait for Tape Mounts for File Information

  When querying Tivoli Storage Manager for file information, you can specify whether or not Data Protection for SQL Server waits for the Tivoli Storage

Manager server to mount removable media. This option is not selected by default and applies to Legacy restores only.

From the **Restore Databases** tab only, the following additional options are available:

- Point in Time

  You can specify a point in time to which to restore a database by clicking the **Point in Time** button. This button is enabled only when you select to restore a full backup object and at least one log backup.

  – Point in Time dialog

    Clicking the **Point in Time** button displays a dialog box with the following options:

    - No point in time
    - Stop at
    - Stop at mark
    - Stop before mark

    The stop radio buttons enable you to specify a date and time. The **Stop at** mark and **Stop before mark** buttons enable you to name a mark for the restore and include the date and time to help locate the mark. To clear a set point in time, select the **No point in time** radio button. When point in time is in use, a static field is enabled to display the results of the action.

- Disable VSS Instant Restore

  Selecting **Disable VSS Instant Restore** bypasses volume-level copy and uses file-level copy to restore the files from a local VSS backup. If this option is not selected, volume-level snapshot restore is used for local VSS backups if the backup exists on volumes that support it. The default value is to use volume-level snapshot restore if supported. This option is available for VSS operations only. When performing VSS Instant restores, you must make sure that any previous background copies (that involve the volumes being restored) are completed prior to initiating the VSS Instant restore.

Shortcut menu

You can display additional restore options by right-clicking a selected item in the list control. This menu is available only when you highlight a database in the tree. All of its backup objects are displayed in the list control, and the menu is available for any selected objects. The right-click pop-up menu contains the following items:

- Restore Into

  Use this option to specify the database to restore a backup object to. Click **Restore Into** to display an edit box. If you have selected several databases to be restored, the restore into name you specify applies only to the selected backup object that you right-clicked. If other selected backups require the **Restore Into** option, you have to specify them one at a time, but you can do so in one restore operation.

- Relocate

  Use the Relocate dialogs to specify new destination locations in which to restore backed-up SQL Server databases, logs, and Microsoft SQL Server full-text index files:

  – Relocate All Files Into a Directory

    Select this option to restore the SQL Server data files, logs, and other related files into a location different from where the data was originally backed up.

    • Relocate Log Files Into

      Check this box to restore the log files into a location different from where the SQL Server database and other related files are being restored.

    • Relocate Other Files Into

      Check this box to restore Microsoft SQL Server full-text index files into a location different from where the SQL Server database and logs are being restored.

  – Relocate Files Individually

    Select this option to restore each SQL Server database, log, and Microsoft SQL Server full-text index file individually. This is available for Legacy backups only.

- Standby Server Undo File

  Use this option to specify the undo file for a Legacy restore to a standby SQL Server database. If the target SQL Server database is not already in standby mode, it is placed in standby mode. This menu item appears only in the **Restore Databases** window and is available for full, differential, and log backup types, but only for one database at a time. Click this option to display an edit box for the undo file name. Once you specify this for a database, it applies to all backup objects for that database. Likewise, once you remove this option for a backup object, it is removed for all.

5.3 Performing restores using the CLI

Use the command RESTORE to perform Legacy and VSS restores. You can perform full and partial restores, using full, differential, log, group, file, and set backups.

When using Data Protection for SQL Server commands, keep in mind that all SQL names of databases or parts of databases are case sensitive:

- SQL Server database names are case sensitive.
- The logicalfilename variable is case sensitive.
- The groupname variable is case sensitive

Almost all restore operations can be performed using either the Data Protection for SQL Server GUI or the CLI tool. In this chapter we mostly cover Data Protection for SQL Server GUI routines.

For a complete discussion about the parameters for the RESTORE command, refer to *IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server Installation and User's Guide*, SC32-9059.

5.4 Restore examples

Restores performed on your Microsoft SQL Server can cover a wide range of complexity, from simply restoring databases on a running server to accomplishing a complete disaster recovery.

In the following sections we show complete examples of how a disaster recovery is performed and how to restore from different backup types in various situations.

5.4.1 Considerations for restore operations

Before we discuss our restore examples, a brief reminder about important topics for restore operations is necessary.

Recovery option

When the check box **Recovery** is checked (the default), the database is ready for use as soon as the restore is completed, and no subsequent logs can be applied. If you accidentally check this option before you apply the last transaction log, you must restore your database again.

When **Recovery** is unchecked, the database is restored with no recovery, leaving it in an unusable intermediate state, and further transaction logs can be applied. The last backup to restore must be with the Recovery option enabled to make the database ready for use.

Additional information can be found in Microsoft SQL Server documentation.

Backing up the tail of the log before the restore

If you are restoring a database over an existing database, and the database is using bulk-logged or full recovery models, you must first perform a tail-log backup, or choose the **Replace** check box in the **Restore Options** panel. Tail-log backups are discussed in 4.2.7, “Tail-log backups using the GUI” on page 150.

If you try to restore a database without enabling the previously described options, you receive errors similar to those shown in Figure 5-1.

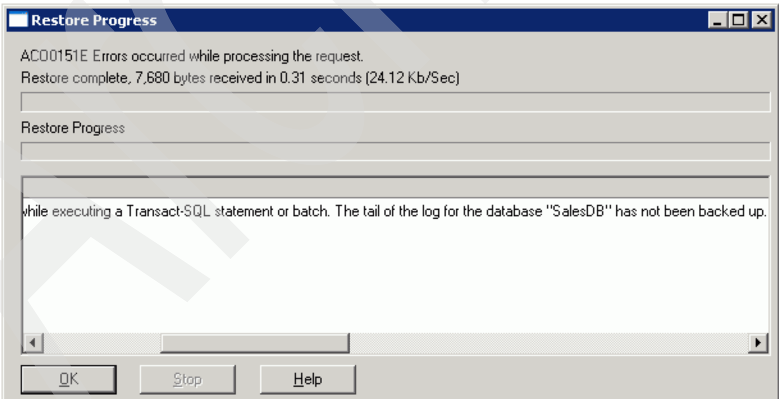

Figure 5-1 Error message related to tail-log backup

5.4.2 Disaster recovery

In a disaster recovery situation, the most likely scenario may involve a reinstalled SQL server, or you may have to rebuild the master database on your existing SQL server.

Generally, according to the recovery required, you may have to perform the following tasks:

1. Install Microsoft SQL Server and apply the required patch sets. Remember to use the same sort order and code page as used on the SQL server you recover.
2. Install Data Protection for SQL Server according to the description in “Chapter 3, “Installation and configuration” on page 73 and then restore the dsm.opt and tdpsql.opt files with the Tivoli Storage Manager backup-archive client. You can also re-create the dsm.opt and tdpsql.opt files yourself, using instructions contained in previously cited chapter.
3. Start Microsoft SQL Server in single-mode using the **`sqlservr.exe`** command with the `-m` parameter.
4. Use Data Protection for SQL Server to restore the master database using either Legacy or VSS backups. At the end of the restore operation, SQL Server is shut down.
5. Start Microsoft SQL Server normally, as a service.
6. Manually reapply any changes that were made to the master database after the date of the database backup used to do the restore operation.
7. Use Data Protection for SQL Server to restore all other system and user databases.

Note: Because the tempdb database is re-created every time Microsoft SQL Server is restarted, there is no need to back up this database.

In some disaster recovery situations, only database files are damaged, while all Microsoft SQL Server binary files and Windows registry entries are intact. For example, this occurs when you do not have a valid backup for the system databases, only for the user databases.

For these situations, instead of reinstalling Microsoft SQL Server, you can rebuild the SQL server master database and then perform the previously listed steps 3 through 6. When you rebuild the master database, the msdb and model databases are re-created as well, so you must also restore those databases after the rebuild operation.

Note: In Microsoft SQL Server 7 and Microsoft SQL Server 2000, to rebuild the master database use the Rebuildm.exe utility in \. .\mssql7\binn\ or \. .\Microsoft SQL server\80\Tools\Binn\ for SQL 2000.

In Microsoft SQL Server 2005, use the Setup command to rebuild the master database.

For all Microsoft SQL Server versions, the compact disc or shared network directory containing the SQL Server installation software is required to rebuild the master database, as well any service pack applied after the Microsoft SQL Server installation.

For more information, refer to Microsoft SQL Server documentation.

5.4.3 Restoring Microsoft SQL Server system databases

As discussed in 5.4.2, “Disaster recovery” on page 189, in a disaster recovery scenario, after installing Microsoft SQL Server and Data Protection for SQL Server, you must restore the system databases, starting with the master database and then restoring the msdb and model databases.

In this section we show you how to restore Microsoft SQL Server databases.

1. Stop all Microsoft SQL Server-related services to the instance you will restore the system databases - services such as SQL Server Integration Services and SQL Server Analysis Services.
2. At this point, you must start Microsoft SQL Server in a single-user mode.

   Open a command prompt window, go to the Binn directory located inside the Microsoft SQL Server installation path, and start SQL Server in single-user mode using the following command:

   ```
   sqlservr.exe -m
   ```

3. Launch the Data Protection for SQL Server GUI, select the **Restore Databases** tab, and select the master database to restore, as shown in Figure 5-2.

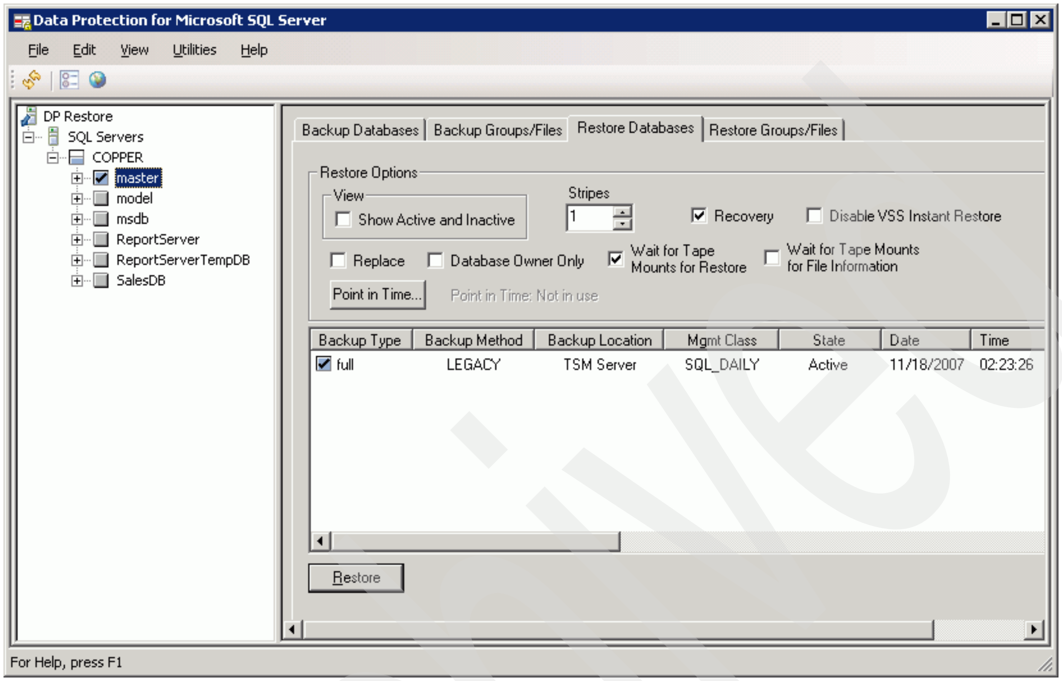

Figure 5-2   Selecting master database to restore

Regardless of the previous file path of the master database file, which is stored with the backup object of the database, the master database file is restored where the reinstalled and rebuilt master database is present.

After the restore is completed, a confirmation window is displayed with the restore results, as shown in Figure 5-3.

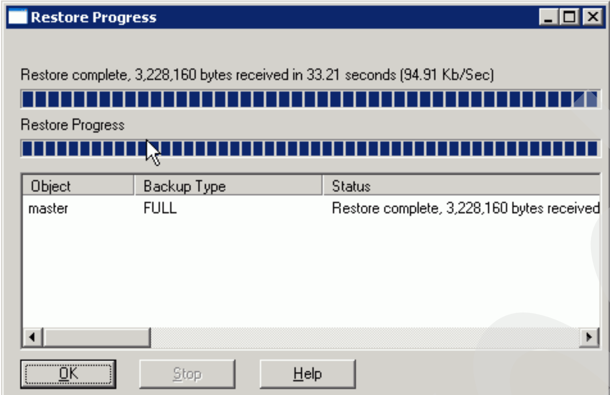

Figure 5-3 Restore of master database complete

At the end of the restore operation, Microsoft SQL Server is automatically shut down. In previous Data Protection for SQL Server releases, this causes an error message to be displayed at the end of restore operation.You can safely ignore this error message.

4. Start Microsoft SQL Server as a service, using the Windows Control Panel.

> **Note:** When the file path settings (in the restored master database) are different from the current file path of the model database (obtained by rebuilding the master database or from reinstalling Microsoft SQL Server), the SQL server fails to start.
>
> Here’s a workaround: Move the model database files model.mdf and modellog.ldf to the file path defined in the restored master database.

5. Restore the model and msdb databases using Data Protection for SQL Server. In the **Restore Databases** tab, select the model and msdb databases. If needed, you can relocate the file space destination for the database, as shown in Figure 5-4.

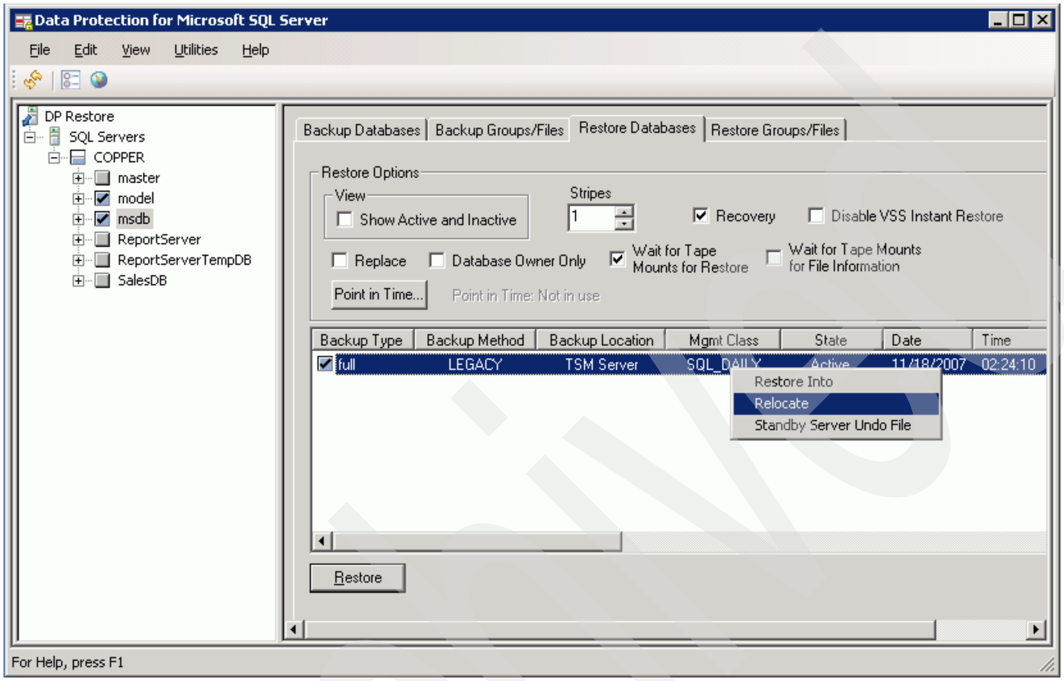

Figure 5-4 Relocating system databases

6. In the Relocate window, choose the location where you want to restore the files, as shown in Figure 5-5.

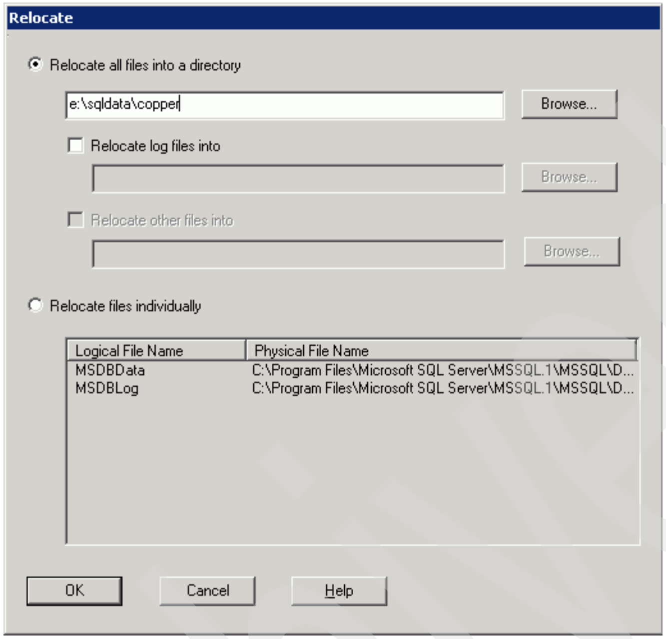

Figure 5-5 Choosing the location where model and msdb will be restored

> **Note:** If the Logical File Names and Physical File Names columns do not contain information about the database files (which occurs because your metadata was migrated to removable media), you must check the **Wait for Tape Mounts for File Information** box and refresh the tree view.

7. Start the restore process by clicking **Restore**. At the end of the operation, you receive a confirmation window with the restore results.

   At this point, you have restored all your system databases, and then you can start restoring your user databases, as shown in the next section.

5.4.4 Performing a complete restore

After you restore your system databases in a disaster recovery scenario, you must restore your user databases. In several other situations - for example, a database corruption or when data is truncated - you may want to restore a database.

Performing a complete restore of the database means applying the last full backup taken, the last differential backup, if any, and all transaction log backups since the last full backup was taken.

You can choose to restore multiple databases at the same time. If you want to relocate, you must specify this for each database to be restored.

To perform a complete restore of a database, click the **Restore Databases** tab, and on the left pane, select on the databases to be restored, as shown in Figure 5-6.

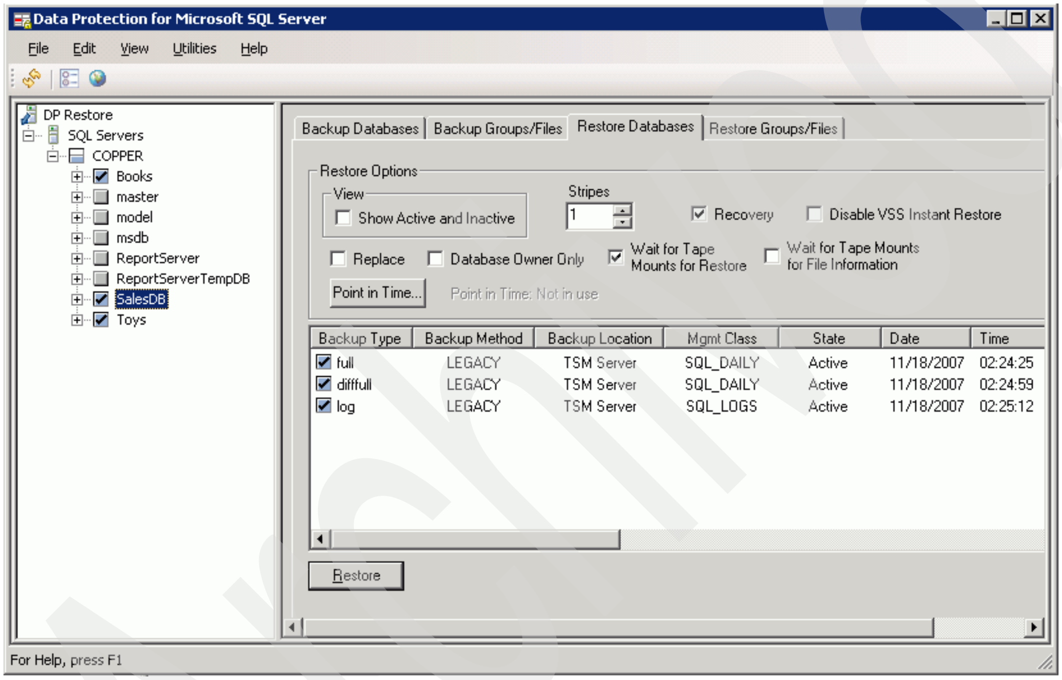

Figure 5-6 Complete restore

5.4.5 Performing transaction log and differential restores

Transaction log backups and differential backups are worthwhile only when restored together with a full database backup. You cannot start a restore operation using either a transaction log backup or a differential backup; you must first restore the last full backup taken before the backup you want to restore. Then you restore the desired backup.

In the Data Protection for SQL Server GUI, the necessary logs for performing a restore are automatically selected according to the backup object you select.

However, you also have the option to manually select and restore individual backup objects for your databases. Enabling the Data Protection for SQL Server GUI to choose the required backup objects to be restored (for example, not restoring unnecessary transaction logs due to the existence of differential backups) can help you avoid wasting time and resources during a backup operation.

For more information about selection propagation rules in the Data Protection for SQL Server GUI, refer to Chapter 4, "Using the graphical user interface" in *IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server Installation and User's Guide*, SC32-9059.

If you want to manually restore a transaction log or differential backup, you can:

1. Restore a full database backup taken before the transaction log or differential backup you want to restore with the **Recovery** option unchecked.
2. In the case of differential backups, directly restore the desired differential backup with the **Recovery** option checked.
3. In case of transaction log files, you can either apply the last differential backup taken before the transaction log backup, if available, and then all transaction log backups since the last differential backup until the desired transaction log backup, or apply all transaction log backups since the full backup. For these two scenarios, restore only the last transaction log with the **Recovery** option checked.

5.4.6 Performing a point-in-time restore

To restore a database to a specific point in time using Data Protection for SQL Server, you must first restore the latest full backup prior to the desired point in time. Then restore all transaction logs taken between the last full backup until after the desired point in time.

For the example in this section, we restore the database SalesDB to the time stamp of Feb 16, 2007, 07:40.

1. We select the last full backup and all subsequent transaction log backups. Because the time of the last transaction log backup is 07:57:13, it must be included in this restore operation. Figure 5-7 shows our selections.

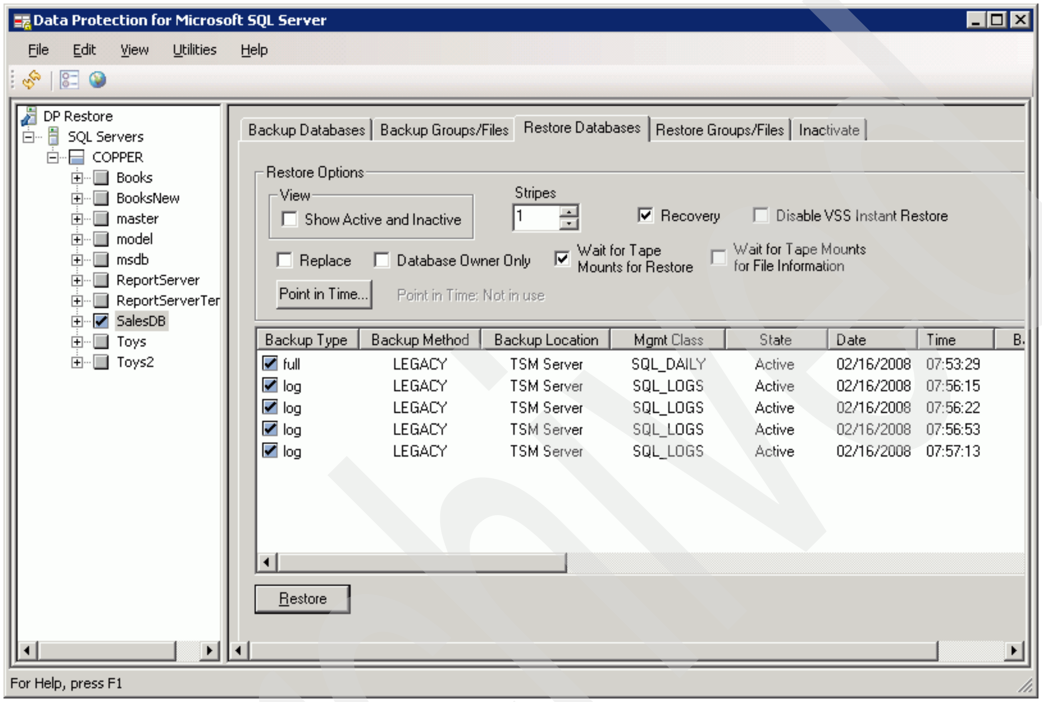

Figure 5-7 Selecting backups for the point-in-time restore

2. Click the **Point in Time** button and choose the desired time to restore the database (see Figure 5-8).

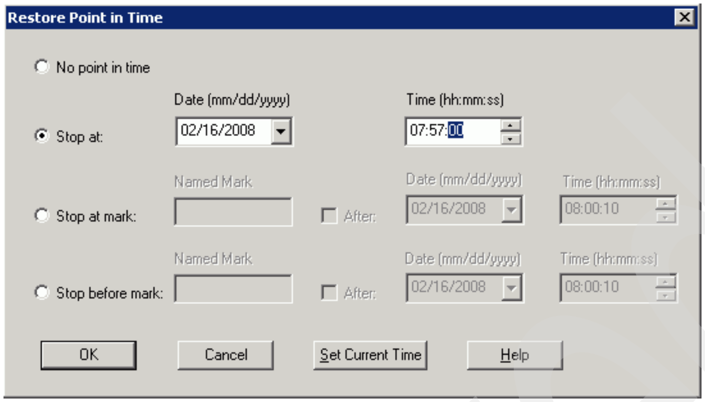

Figure 5-8 Selecting time for point-in-time restore

After you choose the date and time desired for the point-in-time restore operation, it is shown in the main window (see Figure 5-9).

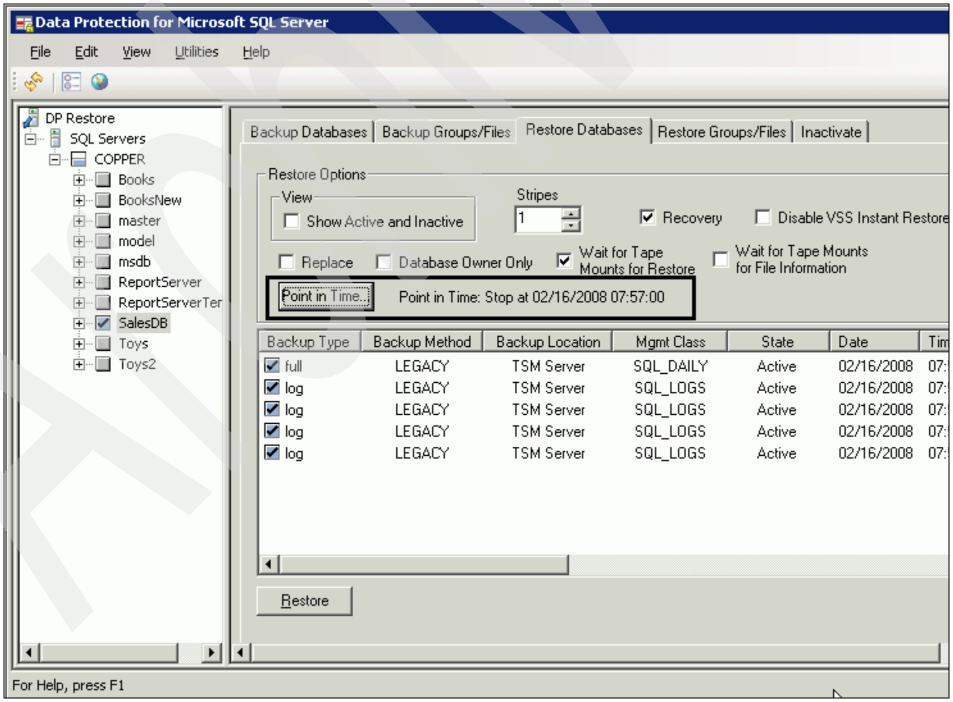

Figure 5-9 Point-in-time restore

> **Note:** Point-in-time restores are available only from the **Restore Databases** tab

If you want to include file, groups, or set backups in your point-in-time restore operation, you can:

1. From the **Restore Databases** tab, restore a full backup taken before the point you want to restore you database with the **Recovery** option in the Restore options panel unchecked.
2. If a differential backup is taken after the full backup is restored and before the time you want for your point-in-time recovery, restore it using the **Restore Databases** tab with the **Recovery** option in the Restore options panel unchecked.
3. Switch to the **Restore File/Groups** tab and apply the subsequent transaction log, file, group, and set backups with the **Recovery** option in the Restore options panel unchecked. Do not restore the last transaction log backup taken before the time you want for your point-in-time recovery.
4. Return to the **Restore Databases** tab and choose the last transaction log to be applied. Click the **Point in Time** button to specify when the database will be restored. Before clicking on the **Restore** button, check the **Recovery** option in the Restore options panel.

5.4.7 Performing a named mark restore

When you have to maintain consistency among two or more databases, you may implement named mark transactions. Microsoft SQL Server 2000 and 2005 support named mark transactions, which means you can mark transactions across related databases and use these marked transactions to recover related databases to the same transaction point. This way, you do not have to perform synchronized backups.

Data Protection for SQL Server supports restoring to a named mark. To restore to a named mark, you must select the **Restore Databases** tab, and click the **Point in Time** option in the Restore Options panel. Then specify the mark name and perform the restore before or after the mark. Because the mark is bound to the transaction, it is most likely repeated in the log; therefore, you must specify a time prior to the desired mark in time.

Figure 5-10 shows how to select a named point restore. In this example, the database is restored to a mark called batch_start that occurred after 05:00 a.m. from November 18, 2007.

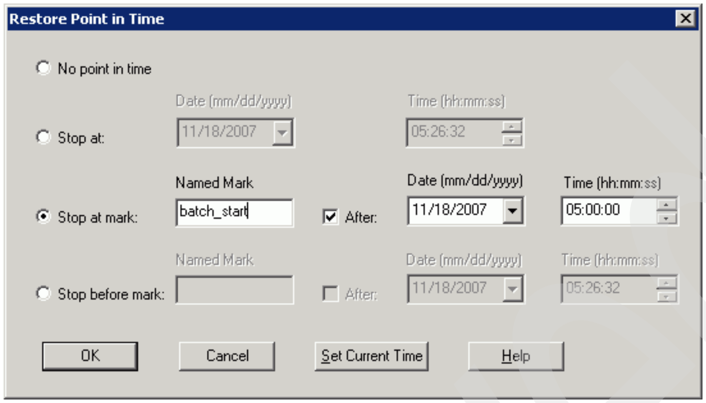

Figure 5-10 Restore to a named mark in time

5.4.8 Relocating files during a restore

The backup object of a database file contains the file name and file path location from where it was backed up. Therefore, when restoring to another file name or file path, you must specify the additional relocation option.

To relocate the database files using the Data Protection for SQL Server GUI, right-click the database object and select **Relocate**, as shown in Figure 5-11.

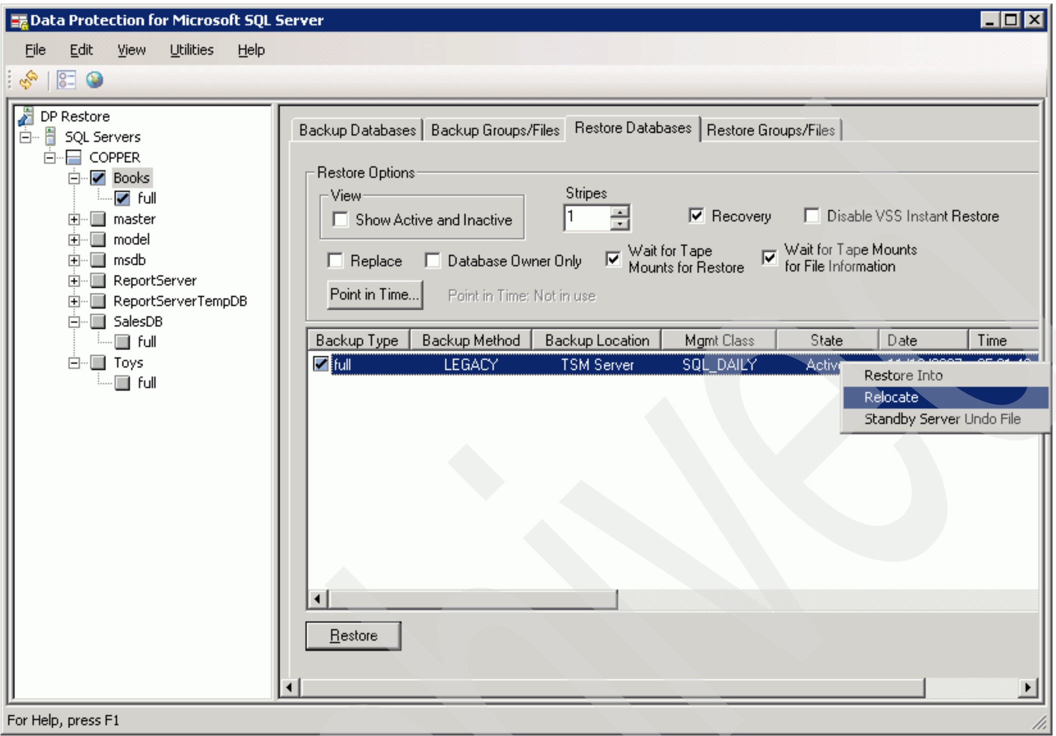

Figure 5-11 Choosing Relocate from Data Protection for SQL Server GUI

Then the relocate box pops up, where you can specify the new location and physical file name. In the relocate box you have two options:

- Relocate all files into a directory

  With this option you can choose to restore all files into a single location or choose to restore data files in one location, log files in a different location, and other files, such as full-text index files, in another location. If you do not specify a location for log files or full-text index files, they are restored to the same location as the SQL server data files.

- Relocate files individually

  Using this option you can specify a different location for each physical file.

Figure 5-12 shows how to specify a different location for each physical file from a database with a full-text catalog.

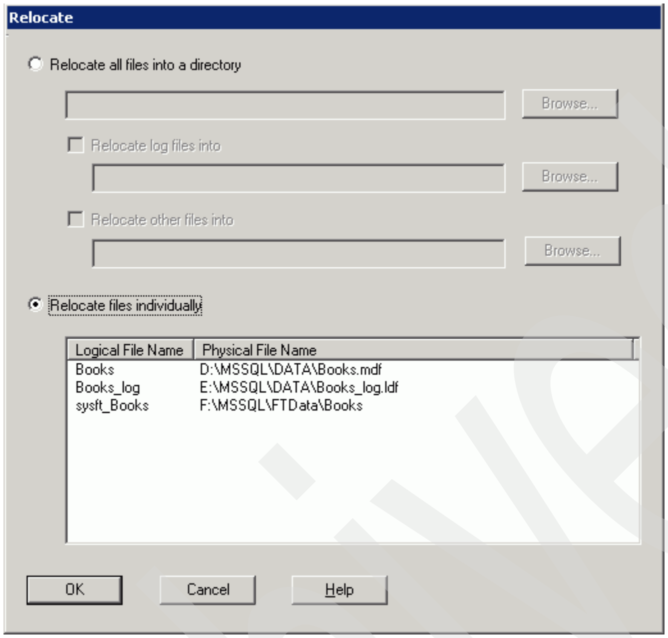

Figure 5-12 Choosing a different location for each file

> **Note:** If the Logical File Names and Physical File Names columns do not contain information about the database files, you must check the **Wait for Tape Mounts for File Information** box and refresh the tree view.

After you choose the new locations for the physical files, perform the restore operation clicking the **Restore** button on the Data Protection for SQL Server GUI.

5.4.9 Performing a partial restore

In certain situations, such as when a disk is corrupted, it may be necessary to partially restore the databases, only restoring those files damaged or lost. You can perform partial restores only on full database backup objects. You can also use partial restores to create a subset of the SQL Server database.

After the partial restore, you can restore differential and transaction log backups on the restored file.

When performing a partial restore, you must always restore the primary filegroup together with the other files you specify.

Note: When performing a partial restore on a new server, you must perform it from the Data Protection for SQL Server CLI because the relocation option is not valid for a partial restore using the Data Protection for SQL Server GUI.

5.4.10 Performing group and file restores

Filegroup backups should be followed by a transaction log backup. You cannot restore a filegroup (or multiple groups) without performing a current transaction log backup following the group backup.

When restoring a filegroup only, you cannot perform a restore with recovery. Even though it is possible to check the **Recovery** check box from the Data Protection for SQL Server GUI, the database is in a loading state after the restore.

Figure 5-13 shows how to select a group backup together with a transaction log backup.

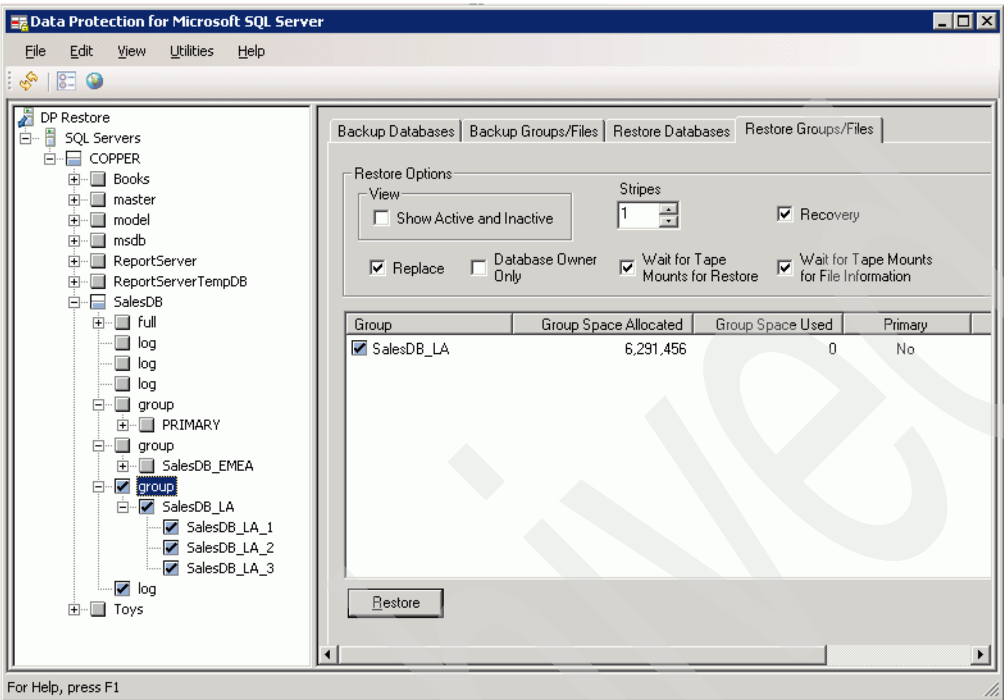

Figure 5-13 Group restore selection

5.4.11 Restoring to another database

At times you want to restore to a database with a different name on the same server. For this situation, you must specify the name of the database to restore to. If the database already exists on the SQL server, check the **Replace** check box. Also, if the file path is different than the one specified in the backup object, it must be relocated. In addition, if the files already exist but are in use by another database, you must change the physical file names.

To restore a database backup to another database, you must first select the database objects to be restored. From the Data Protection for SQL Server GUI, first select the required objects. Then, right-click the backup objects in the right panel and choose the **Restore Into** option. A pop-up window is displayed, where you enter the name of the new database, as shown in Figure 5-14.

In Figure 5-14 and for our example in this section, we restore the database Books to BooksNew. Because the database BooksNew does not yet exist, it is not necessary to check the **Replace** check box.

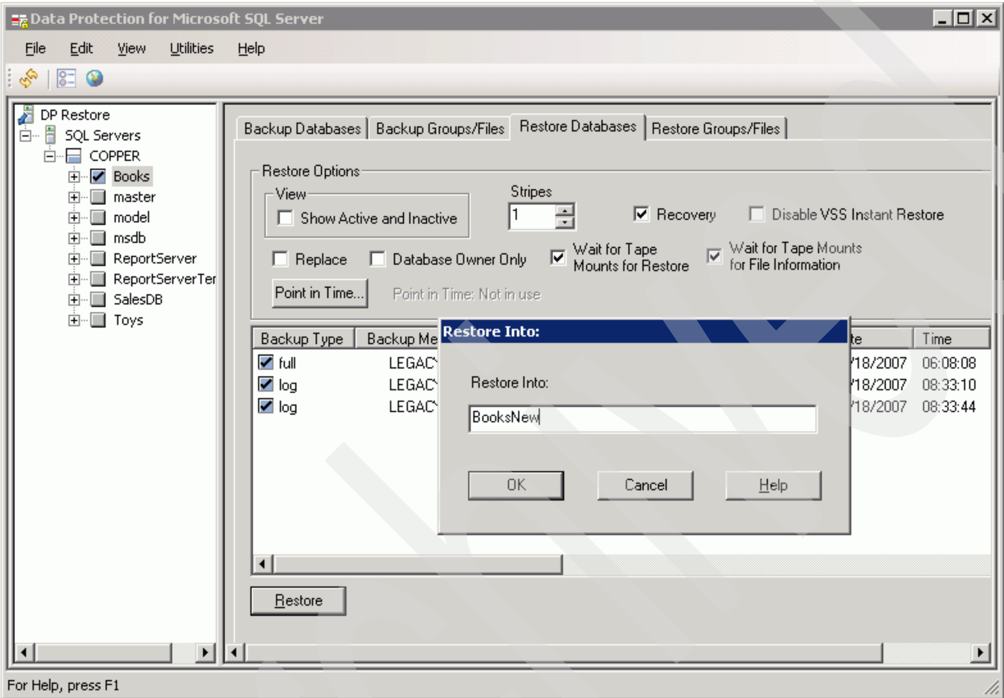

Figure 5-14 Restoring Books to BooksNew

Because the database Books exists, you must relocate the BooksNew files. To do so, right-click one backup object and choose **Relocate**. Then, in the Relocate pop-up, choose where the data files will be restored. We recommend changing not only the location of the files but also the names of the physical files. Doing so makes it easier to identify them as data files from the new database. Figure 5-15 shows an example of relocated physical files.

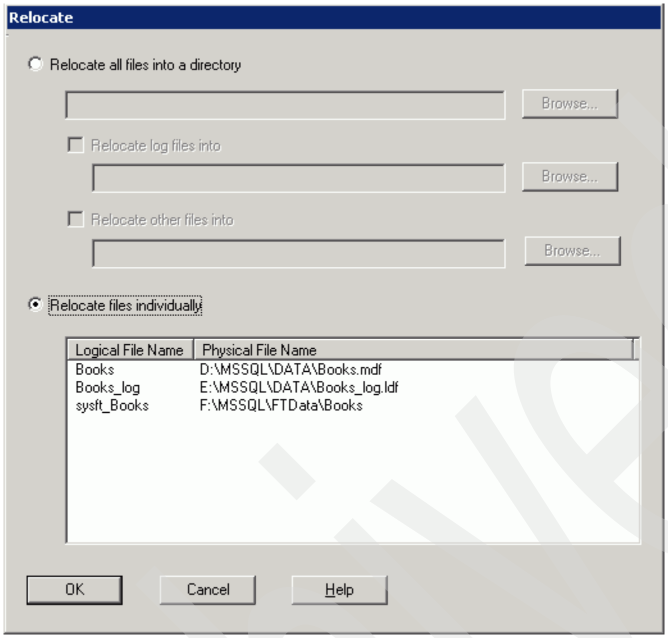

Figure 5-15 BooksNew relocated files

Click **Restore** to restore the Books database into the new BooksNew database.

5.4.12 Restoring to another machine - Legacy only

When using the Tivoli Data Protection for SQL Server GUI, the procedure for restoring a Microsoft SQL Server database to a different machine is exactly the same as the procedure for restoring the database to the server where the backup was taken. Microsoft SQL Server and Data Protection for SQL Server must be installed and configured on both machines.

> **Note:** Unlike Legacy backups, VSS backups cannot be restored to a SQL server with a different name.

When restoring a database to another server, you must log on to the Tivoli Storage Manager server with the correct node name to retrieve the backup.

You must specify the Tivoli Storage Manager node name of the SQL server from which you backed up the database in the dsm.opt file to provide the correct logon to the Tivoli Storage Manager server. and the tdpsql.cfg file must specify the server you want to restore to.

For more information, refer to Appendix F, “Restoring to an alternate machine” in *IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server Installation and User’s Guide*, SC32-9059.

5.4.13 Restoring SQL 2000 backup to SQL Server 2005 database

In some situations, you may want to restore a database taken from a Microsoft SQL Server 2000 backup to a Microsoft SQL Server 2005 instance. Data Protection for SQL Server enables you to restore this type of backup in the same way that you restore backups taken from the same database version.

While a Data Protection for SQL Server restore operation creates a Microsoft SQL Server 2005 database, it does not guarantee that your applications can run in Microsoft SQL Server 2005 in the same way they ran in Microsoft SQL Server 2000. We recommend that you check the Microsoft SQL Server documentation for all required steps, recommendations, restrictions, and pitfalls associated with the Microsoft SQL Server version upgrade process and that you spend the necessary time to test your application against the new database version.

5.5 Standby server

The concept of a standby (or warm backup) server is quite simple: After restoring a full backup taken from the primary server to a standby server, all transaction log files generated in the primary server are transferred and restored to the standby server. This method does not guarantee no loss of data in your Microsoft SQL Server environment; it can protect only changes until the last transaction log was backed up. Thus it is important to periodically back up the primary transaction log file. Also, you must periodically check whether all transaction log files backups are being correctly restored in the standby server to avoid any unpleasant surprise when you need to use the standby server.

Standby servers are commonly used to protect user databases; thus keep in mind that you might have to create routines to propagate changes in system databases, such as Microsoft SQL Server log ons, for example. Refer to the Microsoft SQL Server documentation for additional information.

In the example in this section, we set up a standby server, step by step, from our virtual Microsoft SQL Server cluster CLUSQL01\SQL01 to our standalone SQL server COPPER, using the Tivoli Storage Manager Scheduler.

Note: When implementing a standby solution, all transaction log backups must be restored into the standby server. To simplify the operation, and avoid transaction log backup gaps during the restore operation, we recommend you use a common node name for all transaction log backups.

The following steps are necessary:

1. Register the node name SQL01_logship on the Tivoli Storage Manager server and create the client options file logship.dsm, containing parameters for this node's communication with the Tivoli Storage Manager server.

   Perform a full backup of the database LogShippingDB on SQL01, specifying the /tsmoptfile=logship.dsm file. In this case, LogShippingDB uses the full recovery model to ensure that Microsoft SQL Server logs all data changes.
2. Restore LogShippingDB to the server COPPER with the **Recovery** option unchecked. You can perform this operation using either the Data Protection for SQL Server GUI or the CLI interface, but you must leave the database in Recovery mode regardless of which interface you use.
3. Transaction log backups of the LogShippingDB on SQL01 are performed regularly. To determine the interval of the transaction log backups, you must balance the overhead of the transaction log backups against your production servers and the amount of changes in the database you can afford to lose in case of primary server failure. In our case, we use 10 minutes. The script used for SQL01\LogShippingDB backup is shown in Example 5-1.

Example 5-1 Transaction log backup script

```
REM This command file is placed on the primary Server
REM C:\TSM_jobs\BackupLogShip.cmd
REM----------------------------------------------------

set sql_dir=C:\Progra~1\Tivoli\TSM\TDPSql

C:
cd %sql_dir%
date < NUL >> %sql_dir%\sqlsched.log
time < NUL >> %sql_dir%\sqlsched.log

%sql_dir%\tdpsqlc backup LogShippingDB log /sqlserver=CLUSQL01\SQL01
/tsmoptfile=logshipdsm.opt
```

4. Use the Tivoli Storage Manager Scheduler to run the cmd file shown in Example 5-2 every 10 minutes. This restores the transaction logs on the standby server COPPER with NORECOVERY. The cmd file first restores all active log backups for the database LogShippingDB from SQL server CLUSQL01\SQL01. Then all log backups are inactivated. This must be done; otherwise, every log from the beginning (since the full backup) is restored every time the restore job runs.

Example 5-2 Standby transaction log restore script

```
REM This command file is placed on the standby server
REM C:\TSM_jobs\RestoreLogShip.cmd
REM----------------------------------------------------
set sql_dir=C:\Progra~1\Tivoli\TSM\TDPSql
C:
cd %sql_dir%
date < NUL >> %sql_dir%\sqlsched.log
time < NUL >> %sql_dir%\sqlsched.log
%sql_dir%\tdpsqlc restore LogShippingDB log=* /standby=”e:\temp\file2”
/fromsqlserver=CLUSQL01\SQL01 /tsmoptfile=logshipdsm.opt

%sql_dir%\tdpsqlc inactivate LogShippingDB log=*
/fromsqlserver=CLUSQL01\SQL01
```

If the file path for the database files is different on the standby server, use /relocate=logicalfilename /to=physicalfilename.

> **Note:** Both cmd files specify using /tsmoptfile=logshipdsm.opt. The client options file, logshipdsm.opt, defines a different node name than the one defined in dsm.opt. This is done so that the periodic full backup on the primary server does not interfere with log shipping. If the full backup is performed with the same node name as the log backups for shipping, the log backups that are active at the time the full backup is completed are inactivated.
>
> This situation requires more complicated scripting because you then have to check that the latest log backup is already restored on the standby server prior to performing the full backup, which inactivates all the prior backups.

Define the management class for the log objects so they are always available on disk. You can do so by issuing the command **`define stgpool LOG_SHIP_DISK disk description='Disk for Log Shipping'`**.

The schedules for the two jobs are defined on the Tivoli Storage Manager server. Example 5-3 shows the schedule for the backup job.

Example 5-3 Scheduling log backup

```
DEFine SCHedule tdpsql2_domain log_ship_backup
DESCription=”Log Ship every 10 minutes”
ACTion=command
OBJects=”C:\TSM_jobs\BackupLogShip.cmd”
STARTDate=TODAY
STARTTime=18:00
DURAtion=5
DURUnits=minutes
PERIods=600
PERUnits=seconds (seconds is not documented but it works)
DAYofweek=any
```

Example 5-4 shows the schedule for the restore job.

Example 5-4 Scheduling log restore

```
DEFine SCHedule tdpsql2_domain log_ship_restore
DESCription=”Log Ship every 10 minutes”
ACTion=command
OBJects=”C:\TSM_jobs\RestoreLogShip.cmd”
STARTDate=TODAY
STARTTime=18:05
DURAtion=5
DURUnits=minutes
PERIods=600
PERUnits=seconds (seconds is not documented but it works)
DAYofweek=any
```

6

Daily operations

This chapter describes the automation mechanisms IBM Tivoli Storage Manager provides to initiate certain actions such as regular backup and housekeeping activities. The following topics are covered:

6.1 Automating backups

After you have installed and configured Tivoli Data Protection for SQL Server, you have to configure schedules to automate your backup strategy. You can schedule Legacy and VSS backups using the IBM Tivoli Storage Manager Scheduler, or another scheduler tool - for example, Tivoli Workload Scheduler to automate your backups.

This section covers how to configure the IBM Tivoli Storage Manager Scheduler to automate your backups.

6.1.1 Tivoli Storage Manager Scheduler considerations

IBM Tivoli Storage Manager includes a central scheduling component that enables the automatic initiation of administrative and client operations at predefined times. An administrator creates and maintains the schedules in each policy domain. Two types of scheduling are available: administrative and client scheduling. Microsoft SQL Server backups are scheduled using client schedules.

For client schedules, you can specify whether the client will poll the server regularly to receive information about scheduled actions, or whether it must wait to be contacted by the server to start a scheduled action. This option is called the *scheduling mode* on the client and is set in the client options file. Another type of client schedule called *clientaction*, which is for actions that you want to run only once as opposed to recurring scheduled actions.

Many factors influence the actual start time and duration of the various operations, including the client backup window, storage pool sizes, and amount of data. Remember: It is important to consider the timing and sequencing of scheduled operations; otherwise, the jobs can overlap and not complete properly.

Consider the following issues when defining a IBM Tivoli Storage Manager schedule:

- If you are planning to schedule VSS and Legacy backups, do not overlap these schedules in time; otherwise, the second one will fail. Microsoft SQL Server does not allow Legacy and VSS backups to be performed at the same time.
- If you are using server-prompted scheduling mode, make sure that the TCPCLIENTADDRESS and TCPCLIENTPORT options are specified in the Data Protection for SQL Server options file.
- If you change the Data Protection for SQL Server options file, you must restart the service.

Attention: If you are running the Scheduler Service in a cluster environment, use the Cluster Administrator to stop and restart your Scheduler Service.

- Data Protection for SQL Server creates its own log file with statistics for the backed-up database objects when the `/logfile` parameter is specified during the **`tdpsqlc`** command. Output from scheduled commands is sent to the scheduler log file (dsmsched.log). After scheduled work is performed, check the log to ensure the work completed successfully.
- The preferred method of password management for scheduler operations is to specify PASSWORDACCESS GENERATE in the dsm.opt file. If PASSWORDACCESS GENERATE is not specified in dsm.opt, the node password must to be specified in the **`tdpsqlc`** command. To specify the password, use the /tsmpassword parameter in the command file.

After the Data Protection for SQL Server node name has been registered to a IBM Tivoli Storage Manager server and Microsoft SQL Server is installed and configured, you need to perform the following steps:

1. On the IBM Tivoli Storage Manager server:
   a. Define a schedule to execute a Windows command file. This schedule must be defined in the policy domain to which the Data Protection for SQL Server node name is registered.
   b. Associate the Data Protection for SQL Server node with the defined schedule.
2. On the machine where Microsoft SQL Server and Data Protection for SQL Server are installed:
   a. Install the IBM Tivoli Storage Manager Scheduler client as a Windows service for Data Protection for SQL Server. If a scheduler already exists for the regular IBM Tivoli Storage Manager backup client, install another one for Data Protection for SQL Server.
   b. Define a command file that contains the Data Protection for SQL Server commands you plan to use to perform the desired backup.
   c. If you are running in a cluster server environment, install the IBM Tivoli Storage Manager Scheduler client as a Windows service on both cluster nodes.

If you are running in a cluster server environment, create a new cluster resource that represents the IBM Tivoli Storage Manager Scheduler. Verify that the cluster resource is started.

6.1.2 Installing the IBM Tivoli Storage Manager Scheduler client

In the environment we used when writing this book, we have the following setup:

- IBM Tivoli Storage Manager backup-archive installed on the SQL server in the directory C:\Program Files\Tivoli\TSM\baclient.
- Data Protection for SQL Server installed on the SQL server in the directory C:\Program files\Tivoli\TSM\TDPSql.
- The communication options in the dsm.opt option files point to the IBM Tivoli Storage Manager server to which the SQL Server data is to backed up. The options file that is defined for Data Protection for SQL Server is used by the scheduler when validating the node and password. The options file is also used when contacting the IBM Tivoli Storage Manager for schedule information.

Perform the following on the SQL server to set up the IBM Tivoli Storage Manager Scheduler client:

1. Log on using a Windows account with administrative privileges.
2. Install a new IBM Tivoli Storage Manager service to back up the Microsoft SQL Server databases. See Example 6-1.

Example 6-1 Installing IBM Tivoli Storage Manager Scheduler service

```
C:\Program Files\Tivoli\TSM\baclient>dsmcutil inst /name:"TSM SQL
Scheduler serv
ice" /node:CLUSQL01_DAILY /password:clusql01 /autostart:no
/clientdir:"c:\progra
m files\tivoli\tsm\baclient"
/optfile:"F:\tsmdata\dsm_sql_daily_sql01.opt" /star
tnow:no
```

> **Note:** In a cluster environment, you have to run this command on both machines. Remember to configure the following settings:
>
> a. Change the /autostart option to NO; in a standalone environment configure this option to YES.
>
> b. Move the SQL virtual server to the secondary node of the cluster to create the Scheduler Service. Make sure the secondary node of the cluster has ownership of the SQL virtual server.
>
> c. The primary node of the cluster must contain the command file on the file share used to create the Scheduler Service.
>
> d. Copy the options file to a shared drive associated with the virtual server.

3. You can see the log information about the standard output. See Example 6-2.

Example 6-2 Check standard output

```
TSM Windows NT Client Service Configuration Utility
Command Line Interface - Version 5, Release 5, Level 0.0
(C) Copyright IBM Corporation, 1990, 2007, All Rights Reserved.
Last Updated Oct 25 2007
TSM Api Verison 5.5.0

Command: Install TSM Client Service
Machine: LIBRA(Local Machine)

Installing TSM Client Service:

       Machine          : LIBRA
       Service Name     : TSM SQL Scheduler service
       Client Directory : c:\program files\tivoli\tsm\baclient
       Automatic Start  : no
       Logon Account    : LocalSystem
The service was successfully installed.

Creating Registry Keys ...

Updated registry value 'ImagePath' .
Updated registry value 'EventMessageFile' .
Updated registry value 'TypesSupported' .
Updated registry value 'TSM SQL Scheduler service' .
Updated registry value 'ADSMClientKey' .
Updated registry value 'OptionsFile' .
Updated registry value 'ClientNodeName' .
Updated registry value 'EventLogging' .

Generating registry password ...
Authenticating TSM password for node CLUSQL01_DAILY ...

Connecting to TSM Server via client options file
'F:\tsmdata\dsm_sql_daily_sql01
.opt' ...

Password authentication successful.

The registry password for TSM node CLUSQL01_DAILY has been updated.
```

Note: If you have to make corrections after installing a service:

1. Issue the following command to remove the service:
   `dsmcutil remove /name:'TSM SQL Scheduler service'`
2. Install a new IBM Tivoli Storage Manager service to back up the Microsoft SQL Server databases.

3. If you are in a cluster environment, you must start the Scheduler Service:
   a. Start the Cluster Administrator. Select the Microsoft SQL Server cluster group and create a new resource to represent the Microsoft SQL Server scheduler (choose **File** → **New** → **Resource**). See Figure 6-1.

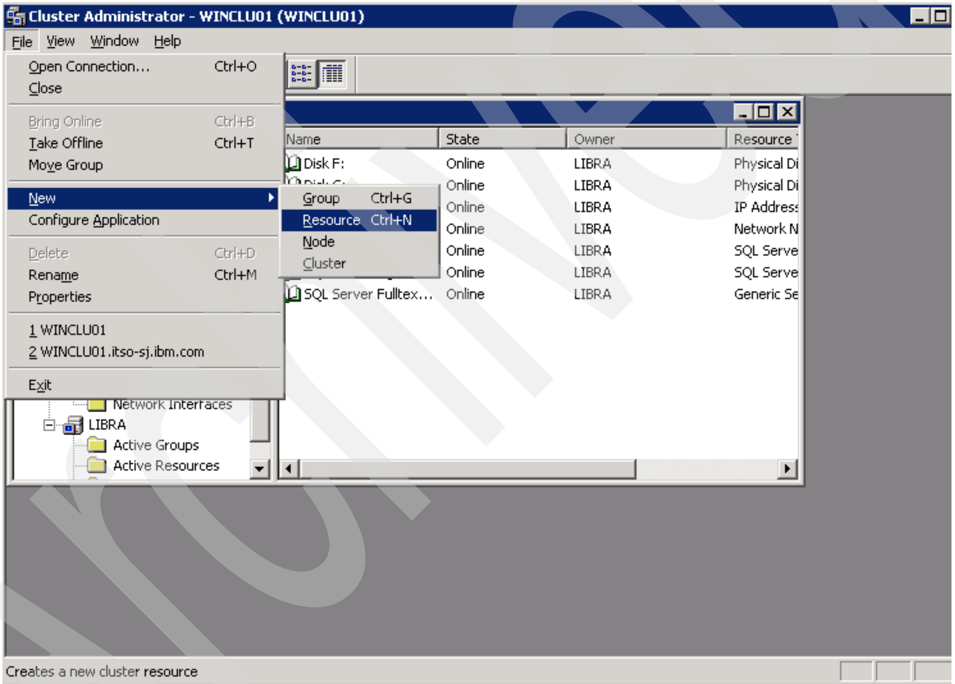

Figure 6-1 Creating a new cluster resource

b. Set the Resource type to **Generic Service** and select your cluster group in the Group drop-down menu. See Figure 6-2.

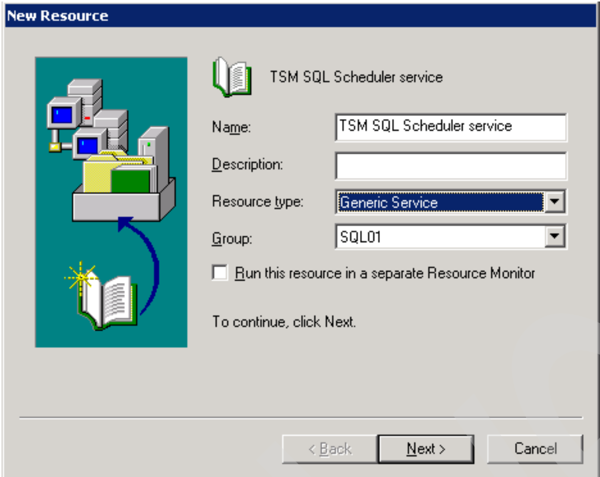

Figure 6-2 Creating a generic service

c. Select the servers that this resource will handle. See Figure 6-3.

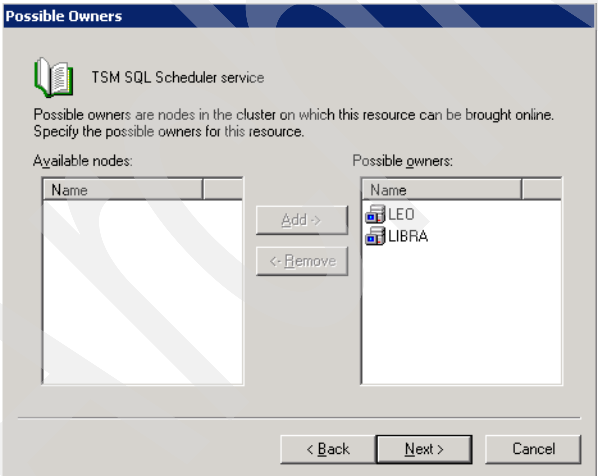

Figure 6-3 Possible owners

d. Select the Resource dependencies to start the Scheduler Service. We select to start only the database, as shown in Figure 6-4.

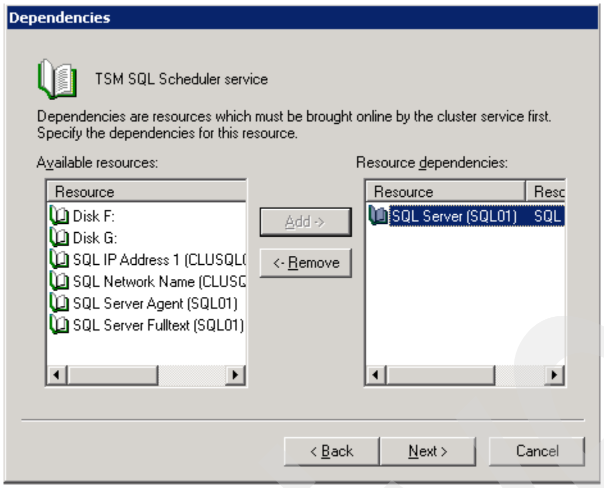

Figure 6-4 Selecting resource dependencies

e. Set the parameters in the Generic Service Parameters window. See Figure 6-5.

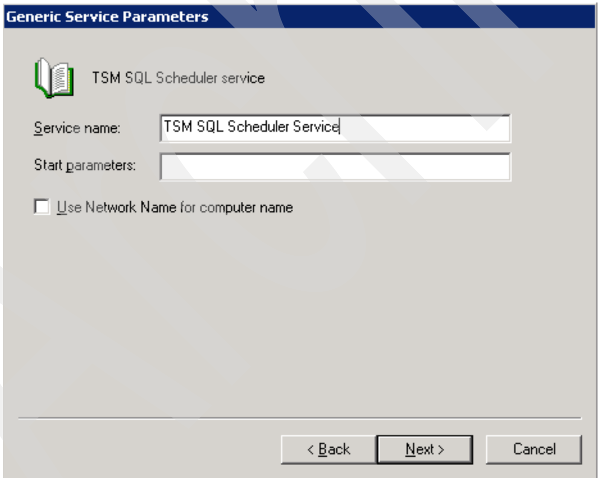

Figure 6-5 Generic service parameter

f. You must add Registry Replication. Click **Add**. When the window is displayed, specify the root registry key. The root registry key must be the exact key where the Data Protection for SQL Server node name is listed.

The registry key is of the format SOFTWARE\IBM\ADSM\CurrentVersion\BackupClient\NODES\<*nodename*>\,<*servername*>. Specify <*nodename*> as your cluster TSM SQL node and <*servername*> as the name of the server you are adding the service. See Figure 6-6.

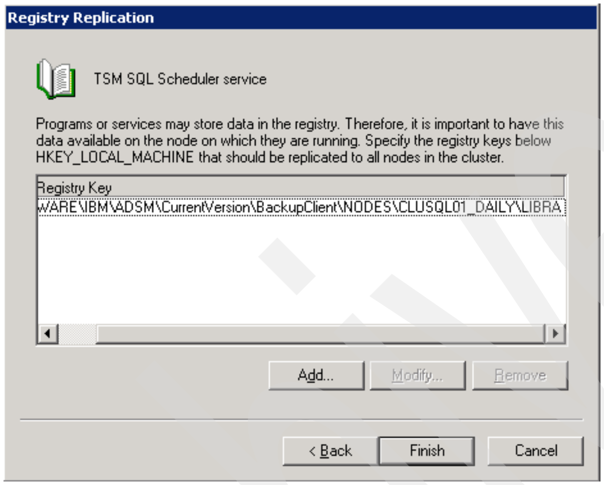

Figure 6-6 Registry replication

A message confirms that the service was created successfully (see Figure 6-7).

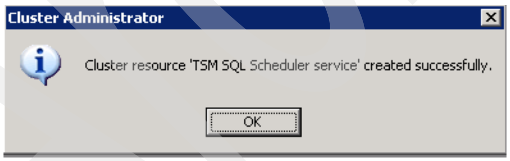

Figure 6-7 Scheduler created successfully

g. To start the service, select the service and choose **File** → **Bring online**. See Figure 6-8.

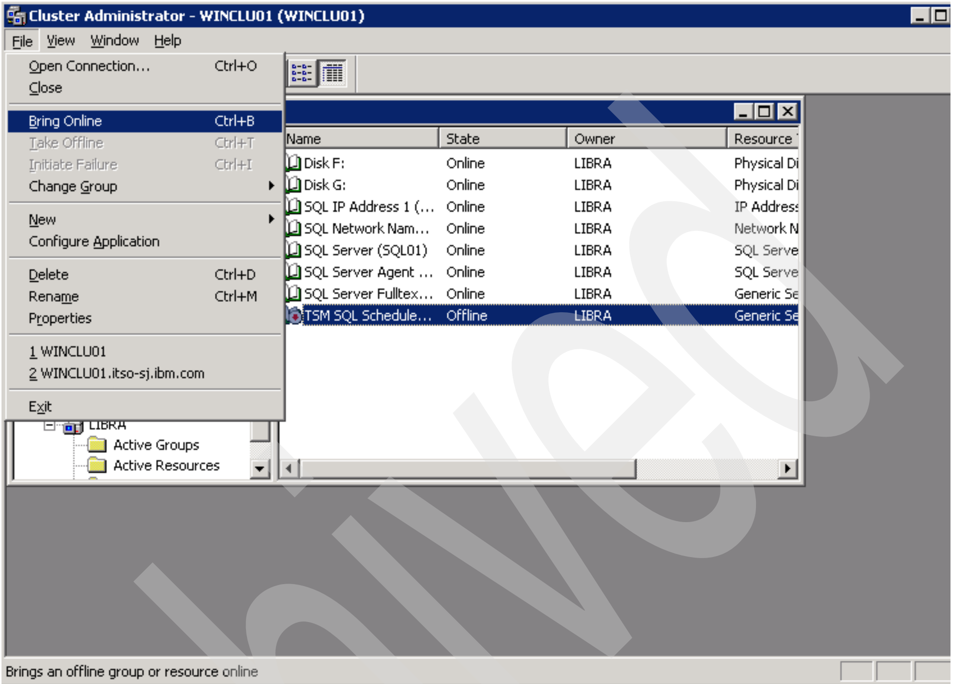

Figure 6-8 Starting the Scheduler Service

6.1.3 Configuring scripts to back up a Microsoft SQL Server

You have to create the scripts on your Microsoft SQL Server machine. The Data Protection for SQL Server installation directory includes a sample command file (sqlfull.smp, as shown in Example 6-3 on page 221) to perform a scheduled full Legacy backup of all the SQL Server databases to the IBM Tivoli Storage Manager server. You simply customize it with the appropriate value for your environment and for the types of backups that you want to perform.

Note: You must specify COMPLETE PATHNAMES in the command file for all file names and non-system commands.

If you are in a cluster environment, your command file can reside on local drives, but you need to remember to replicate the same command file to all machines in the cluster. Alternatively, you can create the command file on a shared drive. The TSMOPTFILE and LOGFILE options specified in your command file must reflect the location of the options file and log file on the Microsoft SQL Server File Share.

Example 6-3 C:\Program files\tivoli\tsm\tdpsql\sqlfull.smp

```
@ECHO OFF
rem ==================================================================
rem   sqlfull.smp sample command file
rem
rem   Sample command file containing commands to do a scheduled full
rem   backup of all SQL databases to an IBM Tivoli Storage Manager
rem   server.
rem
rem   This file is meant to be executed by the IBM Tivoli Storage
rem   Manager central scheduler in response to a defined schedule on
rem   the IBM Tivoli Storage Manager server.
rem
rem ==================================================================

rem ==================================================================
rem   Replace "C:" with the drive where Data Protection for SQL
rem   is installed. Update the directory to match the installation
rem   directory that you chose when you installed the product.
rem ==================================================================

set sql_dir=C:\Progra~1\Tivoli\TSM\TDPSql

C:

cd %sql_dir%

rem ==================================================================
rem   The two lines below put a date/time stamp in a log file for you.
rem   Note: You can change "sqlsched.log" to whatever you prefer in
rem   lines below.
rem ==================================================================
```

```
date < NUL >> %sql_dir%\sqlsched.log
time < NUL >> %sql_dir%\sqlsched.log

rem  ======================================================================
rem   Now call the command-line interface to do the backup:
rem
rem   Replace "srvrname" with the name of the options file name you
rem   plan to use.
rem
rem   If SQL authentication is being used and the SQL login settings
have
rem   not been stored via the GUI, you must also specify the /sqluser
and
rem   /sqlpassword options on the command below.
rem
rem   In this example, we use the '*' to back up all of the databases
rem   on the SQL server. Note that database 'tempdb' will not
rem   be backed up.
rem
rem   Note: You can change "sqlsched.log" and "sqlfull.log"  to
rem         whatever you prefer.
rem  ======================================================================

%sql_dir%\tdpsqlc backup * full /tsmoptfile=%sql_dir%\srvrname.opt
/logfile=%sql_dir%\sqlfull.log >> %sql_dir%\sqlsched.log
```

Based on the script in Example 6-3 on page 221, you can create another script (see Example 6-4) to back up all databases on your server.

Example 6-4 Script sql_backupfull.bat

```
@ECHO OFF
rem  ======================================================================
rem   Script to backup the database all databases
rem  ======================================================================

rem  ======================================================================
rem   Set the installation directory
rem  ======================================================================

set sql_dir=C:\Progra~1\Tivoli\TSM\TDPSql

C:

cd %sql_dir%
```

```
rem  ==================================================================
rem   The two lines below put a date/time stamp in a log file for you.
rem   Note: You can change "sqlsched.log" to whatever you prefer in
rem   lines below.
rem  ==================================================================

date < NUL >> %sql_dir%\sqlsched.log
time < NUL >> %sql_dir%\sqlsched.log

rem  ==================================================================
rem   Backup command
rem  ==================================================================

%sql_dir%\tdpsqlc backup * full /SQLSERVER=CLUSQL01\SQL01
/backupdestination=TSM /tsmoptfile=%sql_dir%\dsm_sql_daily_sql01.opt
/configfile=%sql_dir%\tdpsql_daily_sql01.cfg
/logfile=%sql_dir%\sqlfull_full_daily.log >> %sql_dir%\sqlsched.log
```

You can create another script to back up only one database. For example, the script sql_backupdb.bat was created to back up dbsales7. If you intend to back up more than one database, you can separate the databases using commas. See Example 6-5.

Example 6-5 Script sql_backupdb.bat

```
@ECHO OFF
rem  ==================================================================
rem   Script to backup the database DBSales7
rem  ==================================================================

rem  ==================================================================
rem   Set the installation directory
rem  ==================================================================

set sql_dir=C:\Progra~1\Tivoli\TSM\TDPSql

C:

cd %sql_dir%

rem  ==================================================================
rem   The two lines below put a date/time stamp in a log file for you.
rem   Note: You can change "sqlsched.log" to whatever you prefer in
rem   lines below.
```

```
rem ==================================================================

date < NUL >> %sql_dir%\sqlsched.log
time < NUL >> %sql_dir%\sqlsched.log

rem ==================================================================
rem  Backup command
rem ==================================================================

%sql_dir%\tdpsqlc backup DBSales7 full /SQLSERVER=CLUSQL01\SQL01
/backupdestination=TSM /tsmoptfile=%sql_dir%\dsm_sql_daily_sql01.opt
/configfile=%sql_dir%\tdpsql_daily_sql01.cfg
/logfile=%sql_dir%\sqlfull_db_daily.log >> %sql_dir%\sqlsched.log
```

You can create another script to perform VSS backups. For example, we created the script sql_vss.bat (see Example 6-6) to back up all database files.

Example 6-6 Script sql_vss.bat

```
@ECHO OFF
rem ==================================================================
rem  Script to backup all SQL databases using VSS
rem ==================================================================

rem ==================================================================
rem  Set the installation directory
rem ==================================================================

set sql_dir=C:\Progra~1\Tivoli\TSM\TDPSql

C:

cd %sql_dir%

rem ==================================================================
rem  The two lines below put a date/time stamp in a log file for you.
rem  Note: You can change "sqlsched.log" to whatever you prefer in
rem  lines below.
rem ==================================================================

date < NUL >> %sql_dir%\sqlsched.log
time < NUL >> %sql_dir%\sqlsched.log

rem ==================================================================
rem  Backup command
```

```
rem ==================================================================

%sql_dir%\tdpsqlc backup * full /SQLSERVER=CLUSQL01\SQL01
/backupdestination=LOCAL /backupmethod=VSS
/tsmoptfile=%sql_dir%\dsm_sql_daily_sql01_vss.opt
/configfile=%sql_dir%\tdpsql_daily_sql01.cfg
/logfile=%sql_dir%\sqlfull_db_daily.log >> %sql_dir%\sqlsched_vss.log
```

You can create another script to back up only the database logs - for example, the script sql_backuplog.bat in Example 6-7.

Example 6-7 Script backup_sql_logs.bat

```
@ECHO OFF
rem ==================================================================
rem  Script to backup the database SQL Logs
rem ==================================================================

rem ==================================================================
rem  Set the installation directory
rem ==================================================================

set sql_dir=C:\Progra~1\Tivoli\TSM\TDPSql

C:

cd %sql_dir%

rem ==================================================================
rem  The two lines below put a date/time stamp in a log file for you.
rem  Note: You can change "sqlsched.log" to whatever you prefer in
rem  lines below.
rem ==================================================================

date < NUL >> %sql_dir%\sqlsched.log
time < NUL >> %sql_dir%\sqlsched.log

rem ==================================================================
rem  Backup command
rem ==================================================================

%sql_dir%\tdpsqlc backup * full /SQLSERVER=CLUSQL01\SQL01
/backupdestination=TSM /tsmoptfile=%sql_dir%\dsm_sql_daily_sql01.opt
```

```
/configfile=%sql_dir%\tdpsql_daily_sql01.cfg
/logfile=%sql_dir%\sqlfull_log_daily.log >> %sql_dir%\sqlsched.log
```

6.1.4 Configuring schedules on a Tivoli Storage Manager server

After creating the Scheduler Service and the script files on your SQL server, you have to create schedules on the IBM Tivoli Storage Manager server.

Perform the following steps on the IBM Tivoli Storage Manager server to create schedules to back up your SQL Server database:

1. Enter the command shown in Example 6-8 to define the schedule. You can enter this command on the server console or from an administrative client.

Example 6-8 Defining schedule to back up database daily

```
tsm: ZAIRE>define schedule PDSQL backup_daily description="SQL Daily
Full Backup" action=command objects="c:\program
files\tivoli\tsm\tdpsql\sql_backupfull.bat" priority=2 starttime=20:00
duration=30 durunits=minutes period=1 perunits=days dayofweek=any

Session established with server ZAIRE: AIX-RS/6000
  Server Version 5, Release 4, Level 0.0
  Server date/time: 02/08/08   09:50:46  Last access: 02/08/08
05:34:08

ANR2500I Schedule BACKUP_DAILY defined in policy domain PDSQL.
```

2. Associate this schedule with a node name. See Example 6-9.

Example 6-9 Associating schedule with a node name

```
tsm: ZAIRE>define association pdsql backup_daily clusql01_daily
ANR2510I Node CLUSQL01_DAILY associated with schedule BACKUP_DAILY in
policy
domain PDSQL.
```

You can use the same examples to create additional schedules for your environment, it is important to create a schedule to back up the SQL log files. If your backup policy does not specify daily backups, you must schedule them.

6.2 Verifying and monitoring backups

You must monitor your backups to check whether they completed successfully. This task is as important as performing the backup itself; otherwise, you cannot guarantee a restore when it is necessary. In this section we discuss verifying and monitoring backups.

6.2.1 Managing logs

If errors are reported in a backup operation, review the logs for errors or inconsistencies. You must check a number of logs, which are described in the sections that follow.

IBM Tivoli Storage Manager activity log

The IBM Tivoli Storage Manager activity log contains all messages normally sent to the server console during a server operation. You can monitor the activity log using either the administrative client command line or the IBM Tivoli Storage Manager Integrated Solutions Console Web interface. Example 6-10, shows the contents of the activity log for a Data Protection for SQL Server backup. You can see the start session for the node to back up, the start session for the proxy agent (in this case, we are using VSS), and the completion status of the backup, including statistics.

Example 6-10 IBM Tivoli Storage Manager activity log

```
tsm: ZAIRE>q actlog begint=07:19:19

02/19/08   07:19:19      ANR0406I Session 335 started for node
CLUSQL01_DAILY (TDP
                          MSSQL Win32) (Tcp/Ip
libra.itso-sj.ibm.com(1266)).
                          (SESSION: 335)
02/19/08   07:19:20      ANR0406I Session 336 started for node
LIBRA_VSS (WinNT)
                          (Tcp/Ip libra.itso-sj.ibm.com(1293)).
(SESSION: 336)
02/19/08   07:19:20      ANR0397I Session 336 for node LIBRA_VSS has
begun a proxy
                          session for node CLUSQL01_DAILY.  (SESSION:
336)
02/19/08   07:19:21     ANE4940I (Session: 336, Node: CLUSQL01_DAILY)
Performing
                          a full, TSM backup of object
'SqlServerWriter' component
```

```
                         'DBSales7' using shadow copy.(SESSION: 336)
02/19/08   07:19:21     ANE4940I (Session: 336, Node: CLUSQL01_DAILY)
Performing
                         a full, TSM backup of object
'SqlServerWriter' component
                         'DBTest1' using shadow copy.(SESSION: 336)
02/19/08   07:19:21     ANE4940I (Session: 336, Node: CLUSQL01_DAILY)
Performing
                         a full, TSM backup of object
'SqlServerWriter' component
                         'DBTest2' using shadow copy.(SESSION: 336)
02/19/08   07:19:21     ANE4940I (Session: 336, Node: CLUSQL01_DAILY)
Performing
                         a full, TSM backup of object
'SqlServerWriter' component
                         'DBTest3' using shadow copy.(SESSION: 336)
02/19/08   07:19:21     ANE4940I (Session: 336, Node: CLUSQL01_DAILY)
Performing
                         a full, TSM backup of object
'SqlServerWriter' component
                         'DBTest6' using shadow copy.(SESSION: 336)
02/19/08   07:19:22     ANE4940I (Session: 336, Node: CLUSQL01_DAILY)
Performing
                         a full, TSM backup of object
'SqlServerWriter' component
                         'LogShippingDB' using shadow copy.(SESSION:
336)
02/19/08   07:19:22     ANE4940I (Session: 336, Node: CLUSQL01_DAILY)
Performing
                         a full, TSM backup of object
'SqlServerWriter' component
                         'TEst4' using shadow copy.(SESSION: 336)
02/19/08   07:19:22     ANE4940I (Session: 336, Node: CLUSQL01_DAILY)
Performing
                         a full, TSM backup of object
'SqlServerWriter' component
                         'master' using shadow copy.(SESSION: 336)
02/19/08   07:19:22     ANE4940I (Session: 336, Node: CLUSQL01_DAILY)
Performing
                         a full, TSM backup of object
'SqlServerWriter' component
                         'model' using shadow copy.(SESSION: 336)
02/19/08   07:19:23     ANE4940I (Session: 336, Node: CLUSQL01_DAILY)
Performing
```

```
                          a full, TSM backup of object
'SqlServerWriter' component
                          'msdb' using shadow copy.(SESSION: 336)
02/19/08   07:19:23      ANR0406I Session 337 started for node
LIBRA_VSS (WinNT)
                          (Tcp/Ip libra.itso-sj.ibm.com(1324)).
(SESSION: 337)
02/19/08   07:19:23      ANR0397I Session 337 for node LIBRA_VSS has
begun a proxy
                          session for node CLUSQL01_DAILY.  (SESSION:
337)
02/19/08   07:19:36      ANR0406I Session 338 started for node
LIBRA_VSS (WinNT)
                          (Tcp/Ip libra.itso-sj.ibm.com(1345)).
(SESSION: 338)
02/19/08   07:19:36      ANR0397I Session 338 for node LIBRA_VSS has
begun a proxy
                          session for node CLUSQL01_DAILY.  (SESSION:
338)
02/19/08   07:20:08      ANR8337I LTO volume 027AKK mounted in drive
3580_1
                          (/dev/rmt0). (SESSION: 338)
02/19/08   07:20:08      ANR0511I Session 338 opened output volume
027AKK.
                          (SESSION: 338)
02/19/08   07:20:24     ANE4941I (Session: 338, Node: CLUSQL01_DAILY)
Backup of
                          object 'SqlServerWriter' component 'DBTest1'
finished
                          successfully.(SESSION: 338)
02/19/08   07:20:39     ANE4941I (Session: 338, Node: CLUSQL01_DAILY)
Backup of
                          object 'SqlServerWriter' component 'DBTest2'
finished
                          successfully.(SESSION: 338)
02/19/08   07:20:53     ANE4941I (Session: 338, Node: CLUSQL01_DAILY)
Backup of
                          object 'SqlServerWriter' component 'DBTest3'
finished
                          successfully.(SESSION: 338)
02/19/08   07:21:08     ANE4941I (Session: 338, Node: CLUSQL01_DAILY)
Backup of
                          object 'SqlServerWriter' component 'DBTest6'
finished
                          successfully.(SESSION: 338)
```

```
02/19/08   07:21:22      ANE4941I (Session: 338, Node: CLUSQL01_DAILY)
Backup of
object 'SqlServerWriter' component 'DBSales7' finished
                          successfully.(SESSION: 338)
02/19/08   07:21:37      ANE4941I (Session: 338, Node: CLUSQL01_DAILY)
Backup of
                          object 'SqlServerWriter' component
'LogShippingDB'
                          finished successfully.(SESSION: 338)
02/19/08   07:21:52      ANE4941I (Session: 338, Node: CLUSQL01_DAILY)
Backup of
                          object 'SqlServerWriter' component 'TEst4'
finished
                          successfully.(SESSION: 338)
02/19/08   07:22:06      ANE4941I (Session: 338, Node: CLUSQL01_DAILY)
Backup of
                          object 'SqlServerWriter' component 'master'
finished
                          successfully.(SESSION: 338)
02/19/08   07:22:16      ANE4941I (Session: 338, Node: CLUSQL01_DAILY)
Backup of
                          object 'SqlServerWriter' component 'model'
finished
                          successfully.(SESSION: 338)
02/19/08   07:22:22      ANE4941I (Session: 338, Node: CLUSQL01_DAILY)
Backup of
                          object 'SqlServerWriter' component 'msdb'
finished
                          successfully.(SESSION: 338)
02/19/08   07:22:22      ANR0514I Session 338 closed volume 027AKK.
(SESSION: 338)
02/19/08   07:22:27      ANR0399I Session 337 for node LIBRA_VSS has
ended a proxy
                          session for node CLUSQL01_DAILY.  (SESSION:
337)
02/19/08   07:22:27      ANE4952I (Session: 336, Node: CLUSQL01_DAILY)
Total
                          number of objects inspected:      140
(SESSION: 336)
02/19/08   07:22:27      ANR0403I Session 337 ended for node LIBRA_VSS
(WinNT).
                          (SESSION: 337)
02/19/08   07:22:27      ANE4954I (Session: 336, Node: CLUSQL01_DAILY)
Total
```

```
                          number of objects backed up:      140
(SESSION: 336)
02/19/08   07:22:27      ANE4958I (Session: 336, Node: CLUSQL01_DAILY)
Total
                          number of objects updated:          0
(SESSION: 336)
02/19/08   07:22:27      ANE4960I (Session: 336, Node: CLUSQL01_DAILY)
Total
                          number of objects rebound:          0
(SESSION: 336)
02/19/08   07:22:27      ANE4957I (Session: 336, Node: CLUSQL01_DAILY)
Total
                          number of objects deleted:          0
(SESSION: 336)
02/19/08   07:22:27      ANE4970I (Session: 336, Node: CLUSQL01_DAILY)
Total
                          number of objects expired:          0
(SESSION: 336)
02/19/08   07:22:27      ANE4959I (Session: 336, Node: CLUSQL01_DAILY)
Total
                          number of objects failed:           0
(SESSION: 336)
02/19/08   07:22:27      ANE4961I (Session: 336, Node: CLUSQL01_DAILY)
Total
                          number of bytes transferred: 40.02 MB
(SESSION: 336)
02/19/08   07:22:27      ANE4963I (Session: 336, Node: CLUSQL01_DAILY)
Data
                          transfer time:                   55.50 sec
(SESSION: 336)
02/19/08   07:22:27      ANE4966I (Session: 336, Node: CLUSQL01_DAILY)
Network
                          data transfer rate:          738.47 KB/sec
(SESSION: 336)
02/19/08   07:22:27      ANE4967I (Session: 336, Node: CLUSQL01_DAILY)
Aggregate
                          data transfer rate:        219.11 KB/sec
(SESSION: 336)
02/19/08   07:22:27      ANE4968I (Session: 336, Node: CLUSQL01_DAILY)
Objects
                          compressed by:                    0%
(SESSION: 336)
02/19/08   07:22:27      ANE4964I (Session: 336, Node: CLUSQL01_DAILY)
Elapsed
```

```
                          processing time:            00:03:07
(SESSION: 336)
02/19/08   07:22:27      ANR0399I Session 336 for node LIBRA_VSS has
ended a proxy
                          session for node CLUSQL01_DAILY.  (SESSION:
336)
02/19/08   07:22:27      ANR0403I Session 336 ended for node LIBRA_VSS
(WinNT).
                          (SESSION: 336)
02/19/08   07:22:27      ANR0399I Session 338 for node LIBRA_VSS has
ended a proxy
                          session for node CLUSQL01_DAILY.  (SESSION:
338)
02/19/08   07:22:27      ANR0403I Session 338 ended for node LIBRA_VSS
(WinNT).
                          (SESSION: 338)
02/19/08   07:22:27      ANR0403I Session 335 ended for node
CLUSQL01_DAILY (TDP
                          MSSQL Win32). (SESSION: 335)
```

For more information about the IBM Tivoli Storage Manager server activity log, consult a Tivoli Storage Manager administrator guide (see the list of guides in "Related publications" on page 281).

Data Protection for SQL Server log

Data Protection for SQL Server logs output to the file tdpsql.log in the Data Protection for SQL Server installation directory; by default, this directory is C:\Program Files\tivoli\tsm\TDPSQL. To change this location, use the parameter `/logfile=e:\tsmlogs\sqlfull_db_daily.log`. Example 6-11 shows sample output.

Example 6-11 Log SQL sqlfull_db_daily.log

```
======================================================================
==
02/19/2008 08:48:08 Request                       : FULL BACKUP
02/19/2008 08:48:08 Database Input List           :
DBSales7,DBTest1,DBTest2,DBTest3,DBTest6,LogShippingDB,master,model,msd
b,TEst4
02/19/2008 08:48:08 Group Input List              :
02/19/2008 08:48:08 File Input List               :
02/19/2008 08:48:08 Number of Buffers             : 3
02/19/2008 08:48:08 Buffer Size                   : 1024
02/19/2008 08:48:08 Number of SQL Buffers         : 0
```

```
02/19/2008 08:48:08 SQL Buffer Size                 : 1024
02/19/2008 08:48:08 Number of Stripes specified     : 1
02/19/2008 08:48:08 Estimate                        : -
02/19/2008 08:48:08 Truncate Log?                   : -
02/19/2008 08:48:08 Wait for Tape Mounts?           : Yes
02/19/2008 08:48:08 TSM Options File                : C:\Program
Files\Tivoli\TSM\TDPSql\dsm_sql_daily_sql01.opt
02/19/2008 08:48:08 TSM Nodename Override           : -
02/19/2008 08:48:08 Sqlserver                       : CLUSQL01\SQL01
02/19/2008 08:48:08
02/19/2008 08:49:59 Total SQL backups selected:               10
02/19/2008 08:49:59 Total SQL backups attempted:              10
02/19/2008 08:49:59 Total SQL backups completed:              10
02/19/2008 08:49:59 Total SQL backups excluded:               0
02/19/2008 08:49:59 Total SQL backups inactivated:            0
02/19/2008 08:49:59 Throughput rate:                          289.37
Kb/Sec
02/19/2008 08:49:59 Total bytes transferred:
26,030,592
02/19/2008 08:49:59 Elapsed processing time:                  87.85
Secs
02/19/2008 09:15:48
============================================================
02/19/2008 09:15:48 Request                             : VSS Backup
02/19/2008 09:15:48 Component List                      : 'DBSales7',
'DBTest1', 'DBTest2', 'DBTest3', 'DBTest6', 'LogShippingDB', 'TEst4',
'master', 'model', 'msdb'
02/19/2008 09:15:48 Backup Type                         : full
02/19/2008 09:15:48 Backup Destination                  : TSM
02/19/2008 09:15:48 Local DSMAGENT Node                 : libra_vss
02/19/2008 09:15:48 Offload to Remote DSMAGENT Node     :
02/19/2008 09:15:48 Mount Wait                          : Yes
02/19/2008 09:15:48
------------------------------------------------------------
02/19/2008 09:18:55 VSS Backup operation completed with rc = 0
02/19/2008 09:18:55    Files Examined   : 140
02/19/2008 09:18:55    Files Completed  : 140
02/19/2008 09:18:55    Files Failed     : 0
02/19/2008 09:18:55    Total Bytes      : 41970349
```

IBM Tivoli Storage Manager API log

The IBM Tivoli Storage Manager API log, dsierror.log, is located in the Data Protection for SQL Server installation directory. For example, messages dealing with authentication problems are logged in this file, as shown in Example 6-12.

Example 6-12 TSM dsierror.log

```
02/19/2008 08:44:54 ANS1025E Session rejected: Authentication failure
02/19/2008 08:46:21 ANS1025E Session rejected: Authentication failure
02/19/2008 08:46:30 ANS1025E Session rejected: Authentication failure
02/19/2008 08:47:07 ANS1025E Session rejected: Authentication failure
02/19/2008 08:47:19 ANS1025E Session rejected: Authentication failure
02/19/2008 08:47:33 ANS1025E Session rejected: Authentication failure
```

Windows Event log

Using Event Viewer and event logs, you can gather information about hardware, software, and system problems. VSS snapshot operations write detailed information to the Application log.

The SQL server writes event information to the Windows Event log. For example, you can find backup messages in the Event log. See Figure 6-9.

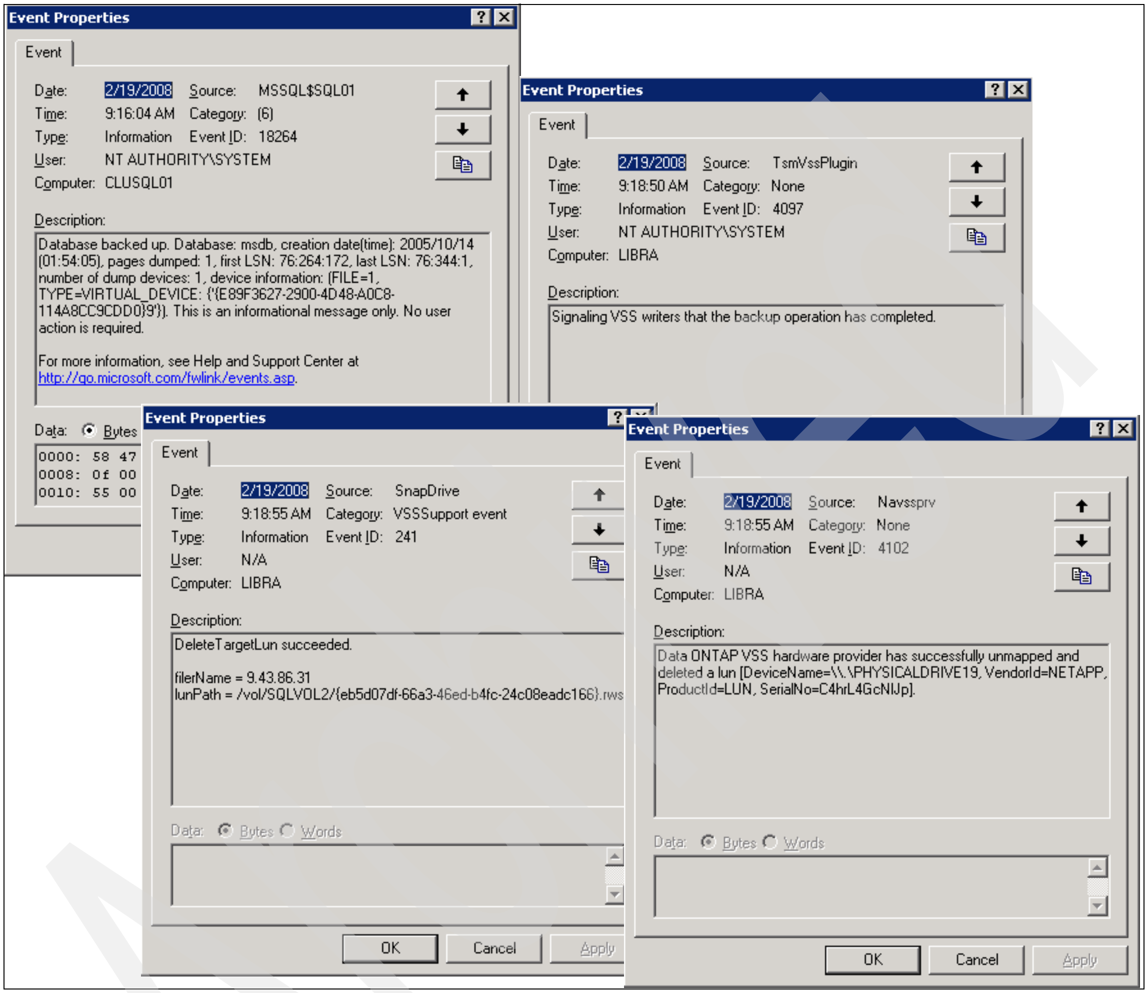

Figure 6-9 Backup events

Staging directory log files

Staging directory log files are generated when a VSS backup is initiated. For every VSS operation that is run, a new subdirectory is created with the current date and time stamp.

In our scenario, this subdirectory is the following:

```
F:\adsm.sys\vss_staging\CLUSQL01_DAILY\9.43.86.45
```

where:

- You configure drive F:\ in the dsm.opt file for your local DSMAgent.
- CLUSQL01_DAILY is the node name.
- Tivoli Storage Manager TCP/IP address is 9.43.86.45.

Within this directory, you can find audit log files, which are created for each SQL Server database. These files check the VSS volumes for any errors before the volumes are used.

Additional log files

You need to check the backup-archive client log files, which also contain output from VSS backups:

- dsmsched.log: Provides schedule results.
- dsmerror.log: Lists VSS errors.
- agtsverr.log: Provides VSS backup information. This file is located in the backup-archive installation directory.
- dsmwebcl.log: Contains information about the DSMAgent. This file is located in the backup-archive installation directory.

If your storage supports VSS Instant Restore, and you are using this function, you should also check the file IBMVSS.log.

6.2.2 Configuring monitoring on an Tivoli Storage Manager server

You can use the server and client messages, which provide a record of IBM Tivoli Storage Manager activity, to monitor the server. You can log server messages and most client messages as events to one or more repositories called *receivers*. You can log the events to any combination of the following receivers:

- Tivoli Storage Manager server console and activity log
- FIle and user exits
- Tivoli Enterprise Console®
- Simple Network Management Protocol (SNMP)
- Event server receiver (enterprise event logging)

You can filter the types of events to enable for logging. For example, you can enable some messages for one receiver and other messages to other receivers.

To configure event logging, you have to enable or disable logging for one or more event types and for one or more receivers, and you have to begin or end logging to one or more receivers.

When you enable or disable events, you can specify the following:

- Message number or event severity (ALL, INFO, WARNING, ERROR, or SEVERE)
- Events for one or more client nodes (NODENAME) or for one or more servers (SERVERNAME).

For example, to send Data Protection for SQL Server messages to a Tivoli Enterprise Console, assuming that you already have a Tivoli Enterprise Console server in your environment, follow these steps:

1. In the server options file (dsmserv.opt), specify the location of the host on which the Tivoli server is running. In Example 6-13, we specify a Tivoli Enterprise Console server at the IP address 9.43.86.50:155.

Example 6-13 dsmserv.opt TEC configuration

```
techost 9.114.22.345
tecport 1555
```

2. Begin event logging for the Tivoli receiver using the BEGIN EVENTLOGGING Tivoli Storage Manager administrative command. See Example 6-14.

Example 6-14 Executing a command at the Tivoli Storage Manager server prompt

```
begin eventlogging tivoli
```

3. On the IBM Tivoli Storage Manager server, configure the Tivoli Data Protection for SQL Server events. See Example 6-15.

Example 6-15 Enabling events to send to Tivoli Enterprise Console

```
enable events tivoli <event id> Nodename=<node>
```

The events for Data Protection for SQL Server have the string “ACO” followed by four-digit numbers. Remember that the application client must have enhanced Tivoli Enterprise Console support enabled to route messages to the Tivoli Enterprise Console.

6.2.3 Troubleshooting tips

If you experience problems, it is important to look for error messages in the log files that we have described in the previous section. The first step to solving a problem is reaching a diagnosis. Here are some hints for analyzing and isolating the problem:

- Can you connect to the SQL server and the Tivoli Storage Manager server using their native client tools? Can you remotely connect to each server?
- Are the firewall and network connections between the Tivoli Storage Manager server and the SQL server correctly configured?
- Is Tivoli Data Protection for SQL Server configured to access the Microsoft SQL Server on its current listening port? If not, refer to 3.2.10, "Specifying Data Protection for SQL Server preferences" on page 107, for information about how to configure Tivoli Data Protection for SQL Server to access the SQL Server when the SQL Server is configured to listen on a non default port - that is, a port other than 1433.
- Analyze whether the problem concerns all or individual servers. If only one server is affected, check the individual configuration.
- Are all databases affected or only one database? If only one database is affected, ask your database administrator to check whether an individual error exists on that database.
- Check whether the problem is constant or intermittent. What other things are happening that could affect the operation?
- If the problem occurs when performing a scheduled backup, try running the same backup operation manually; it could be an error on your script.
- Is it a Legacy or a VSS backup?
- Try to reproduce the error on both interfaces, the GUI and CLI.

Tracing Data Protection for SQL Server

The Data Protection for SQL Server client uses the Tivoli Storage Manager API to communicate with the Tivoli Storage Manager server and provide data management functions. You can run a trace to determine where the problem exists. The trace provides detailed trace information about the actions you perform. If you use this parameter, trace information is written to the trace file or sent to the console. If you want this information to be sent to a file, specify:

- `/TraceFile=x:\testtrace.log`

  You can place this option in the dsm.opt file of the Microsoft SQL Server for Legacy backups or in your local or remote DSMAgent dsm.opt file. If this file does not exist, a new one is created. If the file exists, the new events are appended to the file.

- `/TraceFlag=ALL`

  This is the default. You can trace only specific events, and this option may not give you the required information to determine your problem. For 90% of the cases, using `/traceflag=all` is fine. You can place this option in your dsm.opt file for Legacy backups.

- `TraceFlag ALL_VSS`

  This option you can use in your dsm.opt file for your local and remote DSMAgent for VSS backups.

Data Protection for SQL Server with VSS backup-restore support

Data Protection for SQL Server provides support for protecting Microsoft SQL databases by two different methods. The most commonly used method is by using Microsoft Server Managed Objects (SMO) API. Data Protection for SQL Server uses the Microsoft VSS method.

If you encounter a problem during Data Protection for SQL Server processing using VSS for backup and restore, follow these steps to resolve the problem:

1. Retry the operation that failed.
2. If the problem persists, close other applications, especially those applications that interact with SQL. Retry the operation that failed.
3. If the problem persists:
   a. Shut down the SQL server.
   b. Restart the SQL server.
   c. Run the operation that failed.
4. If the problem persists:
   a. Shut down the entire machine.
   b. Restart the machine.
   c. Run the operation that failed.
5. If the problem persists, open a ticket on IBM Support.

Determining whether a problem is a Data Protection for SQL issue or a VSS issue

The Data Protection for SQL Server client interacts closely with the backup-archive client (DSMAgent), which performs all of VSS operations. Determine first whether the problem is with the Microsoft VSS service or with the Tivoli Storage Manager.

Perform the following steps to isolate the source of the error:

1. Test the connectivity between the Data Protection for SQL Server client and the Tivoli Storage Manager DSMAgent. Issue the TDPSQLC QUERY SQL command on the machine where the SQL server is installed to verify that your installation and configuration are correct. The command in Example 6-16 returns information about SQL server status and VSS components.

Example 6-16 TDPSQLC QUERY SQL command output

```
C:\Program Files\Tivoli\TSM\TDPSql>tdpsqlc query sql
/tsmoptfile="C:\Program Fil
es\Tivoli\TSM\TDPSql\dsm_sql_daily_sql01.opt" /configfile="C:\Program
Files\Tivo
li\TSM\TDPSql\tdpsql_daily_sql01.cfg

IBM Tivoli Storage Manager for Databases:
Data Protection for Microsoft SQL Server
Version 5, Release 5, Level 0.0
(C) Copyright IBM Corporation 1997, 2007. All rights reserved.

Connecting to SQL Server, please wait...

SQL Server Information
----------------------

SQL Server Name   ........................ CLUSQL01\SQL01
SQL Server Version ....................... 9.0.3042 (SQL Server 2005)


Volume Shadow Copy Service (VSS) Information
--------------------------------------------

Writer Name             : SqlServerWriter
Local DSMAgent Node     : libra_vss
Remote DSMAgent Node    : leo_vss
Writer Status           : Online
Selectable Components   : 10
```

   If the TDPSQLC QUERY SQL command does not return all this information, you might have a proxy configuration problem.

2. Use the vssadmin or vshadow utility to re-create the VSS operation standalone - that is, without any Tivoli Storage Manager involvement. When VSS operations are failing, use these programs to re-create the error to

determine whether the problem is a general VSS problem or a problem within Tivoli Storage Manager code.

– vssadmin

The vssadmin utility is pre-installed with your operating system. It displays current volume shadow copy backups and all installed shadow copy writers and providers in the command window. The following are example vssadmin commands:

– **`vssadmin list writers`**

– **`vssadmin list providers`**

– **`vssadmin list shadows`**

– **`vshadow`**

The vshadow utility is included with the Microsoft VSS SDK. You can use this utility to exercise most of the VSS infrastructure, such as creating, querying, and deleting shadow copies. You can also use vshadow to create both persistent and nonpersistent shadow copies and transportable snapshots, and you can use vshadow to assign a drive letter or mount point to a shadow copy. Using the vssadmin or vshadow utility, you can:

– Verify VSS provider configurations and setup.

– Rule out any possible VSS problems before running the Tivoli Storage Manager VSS functions.

– Determine whether you might have a VSS configuration problem or a hardware problem.

– Determine whether you have a Tivoli Storage Manager problem. If an operation works with vshadow or vssadmin but not with the Tivoli Storage Manager, this may be the case.

Perform the following tests to ensure that VSS is working correctly:

– Test nonpersistent shadow copy creation and deletion

  i. Run **`vshadow -p d: e:`** (where d:\ and e:\ are the SQL server database and log volumes.)

  ii. Repeat the previous step four times.

  iii. Inspect the Windows Event log to ensure that its entries are appropriate.

– Test persistent shadow copy creation and deletion

  i. Run **`vshadow -p d: e:`** (where d:\ and e:\ are the Microsoft SQL Server database and log volumes). You may have to run **`vshadow -da`** to remove the persistent shadow if you do not have enough space.

  ii. Repeat the previous step four times.

iii. Inspect the Windows Event log to ensure that its entries are appropriate.

– Test nonpersistent transportable shadow copy creation and deletion (VSS Hardware provider environments only).

  i. Run **`vshadow -p -t=export.xml d: e:`** (where d:\ and e:\ are the Microsoft SQL Server database and log volumes).

  ii. Copy the resultant export.xml file from machine 1 to machine 2 before performing the next step.

  iii. In the machine you have set aside offload, run **`vshadow -i=export.xml`**.

  iv. Inspect the Windows Event log to ensure that its entries are appropriate.

If any of these tests fail repeatedly, a hardware configuration problem or a VSS problem exists. Consult your hardware documentation for known problems or search the Microsoft Knowledge Database for information. If all tests pass, continue to next text.

– Re-create your specific problem by issuing **`vshadow`**. If you can re-create your problem only by performing a series of steps (for example: a backup fails only when you perform two consecutive local backups), try performing those same tests using **`vshadow`**.

  - SQL VSS backups to the local disk are simulated by running a **`vshadow`** persistent snapshot.
  - SQL VSS backups to the Tivoli Storage Manager server are simulated by running a **`vshadow`** nonpersistent snapshot.
  - SQL VSS backups to the local disk and to the Tivoli Storage Manager server are simulated by running a **`vshadow`** persistent snapshot.
  - Offloaded SQL VSS backups to the Tivoli Storage Manager are simulated by running a **`vshadow`** non-persistent, transportable snapshot.

Refer to the **`vshadow`** documentation for the specific commands for performing backups:

http://msdn.microsoft.com/en-us/library/bb530725.aspx

If you can re-create the problem, it most likely is a general VSS issue. Refer to the Microsoft Knowledge Database for information. If your operation passes successfully with **`vshadow`**, it most likely is a Tivoli Storage Manager or Data Protection for SQL Server client problem.

Gathering files before calling IBM

You must collect several log files and other data to diagnose Data Protection for SQL Server problems.

Gather as many of the following files as possible before contacting IBM Support:

- The Data Protection for SQL Server configuration file. The default configuration file is tdpsql.cfg.
- The Data Protection for SQL Server Tivoli Storage Manager API options file. The default options file is dsm.opt.
- The Tivoli Storage Manager registry hive export.
- The Microsoft SQL Server registry hive export.
- The Tivoli Storage Manager server activity log. The Data Protection client logs information to the server activity log. A Tivoli Storage Manager administrator can view this log for you if you do not have a Tivoli Storage Manager administrator user ID and password.
- If the Data Protection for SQL Server client is configured for LAN-free data movement, you also collect the options file for the Tivoli Storage Manager storage agent. The default name for this file is dsmsta.opt.
- Screen shots or command-line output of failures or problems.

Log files can indicate the date and time of a backup, the data that is backed up, and error messages or completion codes that can help determine the nature of your problem. Gather the following Tivoli Storage Manager log files:

- Data Protection for SQL Server log file. The default location of this file is C:\Program Files\Tivoli\TSM\TDPSql\tdpsql.log.
- Tivoli Storage Manager API error log file. The default location of this file is C:\Program Files\Tivoli\TSM\TDPSql\dsierror.log.
- DSMAgent error log file. The default location of this file is C:\Program Files\Tivoli\TSM\baclient\dsmerror.log.

The Windows event log receives information from the Microsoft SQL Server and many different components involved during a VSS operation.

The following VSS provider log files can also be helpful:

- System provider - (Windows Event log)
- IBM System Storage SAN Volume Controller, DS6000, DS8000 - D:\Program Files\IBM\Hardware Provider for VSS\IBMVss.log
- NetApp or N series- D:\Program Files\SnapDrive*.log

A

Tivoli Storage Manager family of products

This appendix provides a product overview of the Tivoli Storage Manager family of products that may be used with the solutions in this IBM Redbook. The products include:

- Tivoli Storage Manager
- Tivoli Storage Manager Express
- Tivoli Storage Manager Basic Edition
- Tivoli Storage Manager Extended Edition
- Tivoli Storage Manager Space Management
- Tivoli Storage Manager for Space Management
- Tivoli Storage Manager for HSM for Windows
- Tivoli Storage Manager for Storage Area Networks
- Tivoli Continuous Data Protection for Files
- Tivoli Storage Manager for System Backup and Recovery
- Tivoli Storage Manager for Databases
- Tivoli Storage Manager for Enterprise Resource Planning
- Tivoli Storage Manager for Mail
- Tivoli Storage Manager for Microsoft SharePoint®
- Tivoli Storage Manager for Advanced Copy Services
- Tivoli Storage Manager for Copy Services

Tivoli Storage Manager

IBM Tivoli Storage Manager enables you to protect your organization's data from failures and other errors by storing backup, archive, space management, and bare-metal restore data, as well as compliance and disaster recovery data in a hierarchy of offline storage. Because it is highly scalable, Tivoli Storage Manager can help protect computers running a variety of different operating systems, on hardware ranging from notebooks to mainframe computers, and connected through the Internet, a wide area network (WAN), a local area network (LAN), or a storage area network (SAN).

Tivoli Storage Manager uses Web-based management, intelligent data move-and-store techniques, and comprehensive policy-based automation, which work together to help increase data protection and potentially decrease time and administration costs. Because it is highly scalable, Tivoli Storage Manager can also help protect computers running a variety of different operating systems.

IBM Tivoli Storage Manager core functions include:

- Backup and recovery management
- Archive management

IBM Tivoli Storage Manager Extended Edition adds additional support through:

- Disaster preparation planning and recovery (Tivoli Disaster Recovery Manager)
- Network Data Management Protocol (NDMP) backup for network-attached storage
- Small and large tape libraries

Attributes that set Tivoli Storage Manager apart include:

- Easy management of multiple types of inactive data in a hierarchical repository
- Lower storage cost through intelligent hierarchy of storage
- Centralized, comprehensive management
- Reduced network bandwidth through intelligent data movement
- Policy-based automation

IBM Tivoli Storage Manager family of offerings include:

- IBM Tivoli Storage Manager for Application Servers
- IBM Tivoli Storage Manager for Databases
- IBM Tivoli Storage Manager for Enterprise Resource Planning
- IBM Tivoli Storage Manager for Copy Services
- IBM Tivoli Storage Manager for Advanced Copy Services
- IBM Tivoli Storage Manager for Mail

- IBM Tivoli Storage Manager for System Backup and Recovery
- IBM Tivoli Storage Manager for Data Retention

Optional additions to Tivoli Storage Manager include:

- IBM Tivoli Storage Manager for Storage Area Networks
- IBM Tivoli Storage Manager for Space Management

For more product information, see the following Web site:

http://www.ibm.com/software/tivoli/products/storage-mgr/

IBM Tivoli Storage Manager Express

IBM Tivoli Storage Manager Express is suitable for small and medium businesses with a comparatively simple IT environment, or for departments within an enterprise that do not require the full suite of IBM Tivoli Storage Manager features. It provides a subset of IBM Tivoli Storage Manager features, focusing on backup and recovery for Windows operating system environments between 5 and 20 client machines. The features of IBM Tivoli Storage Manager Express are:

- Easy installation

  IBM Tivoli Storage Manager Express takes less than one hour to install, configure, and start running backups.

- Simplified administration GUI

  A new GUI simplifies administration, and operational reporting is integrated. Client software deployment is also included. The GUI is an intuitive Web-based interface.

- Fully upgradable

  It can be easily upgraded to IBM Tivoli Storage Manager Extended Edition.

- Simplified tape management

  Uses traditional methods - such as grandfather/father/son backup sets - that simplify tape rotation. All tape management is fully automated.

- Automatic configuration

  Clients are automatically configured with scheduled backups using industry best practices.

IBM Tivoli Storage Manager Express supports:

- Windows 2003 as the platform for the IBM Tivoli Storage Manager Express server
- From 5 to 20 client systems
- A database size up to 20 GB
- LAN-based systems and devices
- Optional backup for Microsoft Exchange and Microsoft SQL Server

For more information, see

- *Deployment Guide Series: IBM Tivoli Storage Manager Express*, SG24-7033

  http://www.ibm.com/software/tivoli/products/storage-mgr-express/

IBM Tivoli Storage Manager Basic Edition

IBM Tivoli Storage Manager Basic Edition contains a rich set of features and provides the core functions of backup, recovery, and archive management.

Backup and restore methodology

Tivoli Storage Manager keeps track of each backed-up file in its own internal relational database, maintaining an individual record of each version of each file that is backed up so that it can be accurately restored in one step. Using the progressive backup methodology means that only changed files are backed up - periodic full backups are not necessary after the first initial operation. This saves time and storage space. Version control allows user-defined policies to dictate the number of versions kept of each file, and the amount of time they are kept. Backups can be automatically scheduled to make sure they are reliably executed. Tivoli Storage Manager Basic Edition tracks data wherever it is stored, delivering direct one-step file restore.

Policy management

Tivoli Storage Manager policies enable you to specify:

- What data is backed up? You can reduce backup times if unneeded files are not backed up.
- How many versions to keep? What about deleted files?
- How long to keep extra file versions, or the last remaining version of a deleted file?
- Where to initially store the backup? Backups can go to disk first or direct to tape - for example, for large database backups.

These policies can be set for all client nodes, for a group of client nodes, for individual client nodes, for certain files on a client node, down to individual policies for each individual file - enabling you to precisely control how much storage space is required for backups.

Archive

Tivoli Storage Manager archive enables you to archive particular files or groups of files for a designated period of time. Archived files are separate from the normal backup cycle and are therefore not managed by version. You simply specify which files to archive and a retention period. You can create a description of each archive package so you can search these descriptions when you have to retrieve files.

Efficient use of storage space

You can define tiered levels of backup storage, so that backups can be directed first to a disk pool - for fast backup and restore. Data can be later automatically migrated to tape or optical media, for the most cost-effective storage.

This sequential media is automatically managed through the process of reclamation. Space on a sequential volume becomes reclaimable as files expire or are deleted from the volume. For example, files become obsolete because of aging or limits on the number of versions of a file. In reclamation processing, the server rewrites files on the volume being reclaimed to other volumes in the storage pool, making the reclaimed volume available for reuse. This helps to utilize the sequential volumes more efficiently - again, to speed up the restore process.

With collocation enabled, the server attempts to keep files belonging to a group of client nodes, a single client node, client file space or the last active data for a client node, on a minimal number of sequential access storage volumes. You can set collocation for each sequential access storage pool when you define or update the pool. By using collocation, you can reduce the number of volumes required when users restore, retrieve, or recall a large number of files from the storage pool. Collocation thus reduces the amount of time required for these operations.

Library and device support

Tivoli Storage Manager Basic Edition supports libraries with up to 3 tape drives and with 40-cartridge capacity. Larger libraries can be accommodated but with only 3 devices and 40 slots enabled.

You can find more information about IBM Tivoli Storage Manager Basic Edition at the Web site:

http://www.ibm.com/software/tivoli/products/storage-mgr/

IBM Tivoli Storage Manager Extended Edition

The Extended Edition of IBM Tivoli Storage Manager expands on the features and possibilities of the Basic Edition described in the previous section.

IBM Tivoli Storage Manager Extended Edition adds disaster recovery planning capability for the server, Network Data Management Protocol (NDMP) control for network-attached storage (NAS) filers, and support for larger capacity tape libraries and more tape drives.

You can find more information at:

http://www.ibm.com/software/tivoli/products/storage-mgr-extended/

Disaster Recovery Manager

The Disaster Recovery Manager (DRM) component of IBM Tivoli Storage Manager Extended Edition offers various options to configure, control, and automatically generate a disaster recovery plan to reconstruct the original environment. The plan contains the information, scripts, and procedures needed to automate restoration and help ensure quick recovery of data after a disaster. The scripts contain the commands necessary to rebuild the IBM Tivoli Storage Manager server.

One of the key features of IBM Tivoli Storage Manager and Disaster Recovery Manager is the ability to track media in all possible states, such as on site, in transit, or in a vault. The media movement features assist greatly with the daily tasks of sending disaster recovery media off site and receiving expired media on site for reuse. With these features, the system administrator can quickly locate all available copies of data.

Disaster Recovery Manager functions help maintain business continuity by:

- Establishing and helping to automate a thorough server disaster recovery plan — clients can then subsequently restore their data from the server if required, and they can continue their daily backup procedures.
- Ensuring that vital site-specific information is available in the same plan.
- Automating vital recovery steps to return the IBM Tivoli Storage Manager server and backup environment to normal operation.
- Managing and identifying offset media needed for recovery.
- Tracking and reporting destroyed systems in the event of a disaster.
- Storing client configuration information and assigning client recovery priorities.

With Disaster Recovery Manager you can recover at an alternate site, on a replacement computer hardware with a different hardware configuration and with people who are not familiar with the applications. The disaster recovery plan can be periodically tested to certify the recoverability of the server. The disaster recovery plan can be (and should be) re-created easily every day so that the plan stays up to date.

NDMP backup for Network Attached Storage

For NAS devices, Tivoli Storage Manager Extended Edition uses Network Data Management Protocol (NDMP) to perform high-performance, scalable backups and restores. NDMP-based backups and restores minimize network traffic and transfer data out of the Tivoli Storage Manager client and server. NDMP enables a full and differential file system image backup and restore of Network Appliance file servers with operating system Data ONTAP® V6.1.1 or higher and EMC Celerra systems. Multiple backup and restore operations can be performed simultaneously.

The NDMP backup and restore features are fully integrated with Tivoli Storage Manager Extended Edition server and client. No extra software is required on the server, client, or NAS appliance.

Extended library and device support

Tivoli Storage Manager Extended Edition supports larger tape libraries, thus removing the 40-cartridge limit for library capacity and allowing more than 3 tape drives within a single library.

Optional additional products

IBM Tivoli Storage Manager can be integrated with a number of optional applications that together form a powerful integrated storage management solution. These include:

- IBM Tivoli Storage Manager for Space Management
- IBM Tivoli Storage Manager for HSM for Windows
- IBM Tivoli Storage Manager for Storage Area Networks
- IBM Tivoli Continuous Data Protection for Files
- IBM Tivoli Storage Manager for System Backup and Recovery
- IBM System Storage Archive Manager

For a full product listing, visit:

`http://www.ibm.com/software/tivoli/products/`

IBM Tivoli Storage Manager for Space Management

IBM Tivoli Storage Manager for Space Management provides hierarchical storage management (HSM) to automatically migrate rarely accessed files to alternative storage, without disrupting the most frequently used files in local storage. Migrated files are automatically and transparently recalled to primary storage when needed by applications or users. Administrators and users are freed from manual file system maintenance tasks, and more online disk space is available for more important active data. IBM Tivoli Storage Manager for Space Management can also help defer the need to purchase additional disk storage for clients, by making optimal use of available client storage.

IBM Tivoli Storage Manager for Space Management is supported on AIX, HP-UX, Solaris™, and Linux.

IBM Tivoli Storage Manager for HSM for Microsoft Windows

IBM Tivoli Storage Manager for HSM for Windows provides hierarchical storage management functionality to the Windows platform. As with IBM Tivoli Storage Manager for Space Management, HSM for Windows automatically migrates rarely accessed files to alternative storage, without disrupting the most frequently used files in local Microsoft Windows file systems. Similarly, migrated files are automatically and transparently recalled to their original location when needed by applications or users.

HSM for Windows allows various levels of granularity for migration of files. Files can be migrated individually, and file systems can be partially or fully migrated, based on a comprehensive set of policy options.

IBM Tivoli Storage Manager for Storage Area Networks

IBM Tivoli Storage Manager for Storage Area Networks software enables SAN-connected IBM Tivoli Storage Manager servers and client computers to make maximum use of their SAN connection to storage. Both servers and client computers are able to perform the majority of their backup and restore and their archive and retrieve data transfers over the SAN instead of the LAN. Data transfers over the SAN can be either directly to tape or disk storage pools. The impact of data protection on the LAN is greatly reduced, as is CPU utilization on both client and server. For computers running Windows, some SAN configurations allow specific SAN devices to perform data movements directly to and from some tape devices, further reducing client and server CPU utilization.

IBM Tivoli Continuous Data Protection for Files

According to industry surveys, almost 70% of corporate data exists on mobile computers or desktop machines, and less than 8% of it is backed up regularly. For mobile, desktop, and file server machines that contain important, critical, or sensitive data that is constantly being updated, a typical 24-hour backup cycle may not be sufficient to provide adequate data protection. The addition of Tivoli Continuous Data Protection for Files provides a client machine with the capability of being able - transparently, in real time - to back up a file to a IBM Tivoli Storage Manager server as soon as the file is saved. Files that are backed up by this method are managed in the same ways as other corporate data by the IBM Tivoli Storage Manager server.

Tivoli Continuous Data Protection for Files was developed with mobile computer and desktop users in mind, but it can be applied to any client with a high rate of changing data on its file systems.

Tivoli Continuous Data Protection for Files, which is supported on Windows platforms, provides clients with true point-in-time recoverability. For more information, see:

http://www.ibm.com/software/tivoli/products/continuous-data-protection/

IBM Tivoli Storage Manager for System Backup and Recovery

IBM Tivoli Storage Manager for System Backup and Recovery (SysBack™) provides a flexible backup tool for AIX systems (System p) to help protect data and provide bare machine recovery capabilities. It offers comprehensive system backup, restore, and reinstallation methods.

V5.6 and higher of SysBack are integrated with IBM Tivoli Storage Manager, allowing backups to be stored on a IBM Tivoli Storage Manager server.

SysBack provides the following features and benefits:

- Backup and recovery options allow:
  - A full system installation image, known to AIX administrators as a mksysb.
  - Volume group backup.
  - File system backup.
  - File or directory backup.
  - Raw logical volume backup.
  - Recovery of all or part of the system.

   - A system installation image (mksysb) from one system to be installed on another system with either identical or different hardware configurations (also known as *cloning*).
- Central management and automation tools:
   - Provide utilities for creating backup scripts and schedules for easier task automation.
   - Quickly assessed backup, list, and verify operations by means of a completion status-tracking log.
   - Managing backup operations centrally from a single server (remote or local). This is achieved with a “pull” client backup feature.
- Network boot and install features include:
   - Network boot using remote SysBack functions (Classic boot).
   - Network Installation Management (NIM) resources (NIM Resource boot).
- Offline mirror backup options:
   - Split specified AIX mirrors to enable access to inactive (offline) copies of data, allowing simultaneous user and system access to the active copies.

IBM System Storage Archive Manager

IBM System Storage Archive Manager (SSAM) facilitates compliance with regulatory requirements. It helps manage and simplify the retrieval of the ever-increasing amount of data that organizations must retain for strict record retention regulations. Many of the regulations demand the archiving of records, e-mails, design documents, and other data for many years, in addition to requiring that the data is not changed or deleted.

SSAM existing policy-based data management capabilities help organizations meet many of the regulatory requirements of various government and industry agencies, but some new regulations require additional safeguards on data retention. IBM System Storage Archive Manager provides data retention policies that help meet these new regulations.

SSAM makes the deletion of data before its scheduled expiration extremely difficult. Short of physical destruction to storage media or servers, deliberate corruption of data, or deletion of the Archive Manager database, Archive Manager does not allow data on the storage managed by the SSAM server to be deleted before its scheduled expiration date. Content management and archive applications can apply business policy management for ultimate expiration of archived data at the appropriate time.

SSAM hierarchical storage capabilities provide policies that enable storing data on the type of media that best meets that data's longevity, access speed, and cost needs.

Movement of the data from one media type to another (as media needs change or as new types of media become available) is achieved by *migration*. Migration automates moving data to help ensure data longevity and allows data to be stored on the type of media that best meets its speed-of-access and cost needs.

Other SSAM features include:

- Expiration policies

  Expire the data when it is no longer needed, thus freeing up the storage media and providing cost effectiveness.

- Off-site data protection

  This feature is standard. Off-site copies can be created on any of the hundreds of types of media supported and, like the primary copy, is policy managed to allow for expiration.

- Archive client program

  Permits users to archive files from their workstations or file servers to archive retention-protected storage and also to retrieve archived copies of files to their local workstations.

- Expiration and deletion suspension

  Allows you to place an unconditional hold on data. This feature means that data cannot be deleted or modified until the deletion hold is released.

- Event-based retention management

  Data is retained subject to a time interval that is calculated after a retention-initiating event occurs. The data then cannot be deleted until the time limit has expired. For example you can specify keeping records for a particular employee for one year after the employee leaves the organization.

- Data-retention protection

  Data is not deleted until the retention criteria for the object is satisfied.

For more information, visit the Web page:

http://www.ibm.com/software/tivoli/products/storage-mgr-data-reten/

Data Protection product family

Using its data-protection components, IBM Tivoli Storage Manager provides data protection for a wide variety of applications, databases, mail, and hardware. IBM Tivoli Storage Manager data-protection components ensure that data is safe and secure no matter where it is located or how it is stored. These products interface directly with applications using their backup-certified utilities and interfaces, simplifying online backup and restore procedures. These products are now called:

- IBM Tivoli Storage Manager for Databases
- IBM Tivoli Storage Manager for Enterprise Resource Planning
- IBM Tivoli Storage Manager for Mail
- IBM Tivoli Storage Manager for Microsoft SharePoint
- IBM Tivoli Storage Manager for Copy Services
- IBM Tivoli Storage Manager for Advanced Copy Services

IBM Tivoli Storage Manager for Databases

IBM Tivoli Storage Manager for Databases is an optional software module that works with Tivoli Storage Manager to protect a wide range of application data by protecting the underlying database management systems holding that data. Tivoli Storage Manager for Databases exploits the backup-certified utilities and interfaces provided for Oracle, Microsoft SQL Server, and Informix®. In conjunction with IBM Tivoli Storage Manager, IBM Tivoli Storage Manager for Databases automates data-protection tasks and enables database servers to continue running their primary applications while they back up and restore data to and from offline storage.

IBM DB2 Universal Database™ includes the same functionality, enabling it to work directly with Tivoli Storage Manager without the need to buy any additional modules. Regardless of which database is used, Tivoli Storage Manager for Databases allows the centralized and automated data-protection capabilities of Tivoli Storage Manager to be applied to up-and-running database servers.

Data Protection for Informix

Informix-certified Data Protection for Informix provides centralized, online, incremental backup capabilities for restoring and managing Informix server databases and logical logs. It provides both parallel backup and restore and automatic backup of logical logs with the Informix ON-Bar utility. ON-Bar uses the X/Open Backup Services Application Program Interface (XBSA) to communicate with the Tivoli Storage Manager, where backups are stored.

Data Protection for Informix is supported on AIX, HP/UX, and Solaris up to V5.2 of IBM Tivoli Storage Manager for Databases. Beginning with Informix V10, the Tivoli Storage Manager backup interface is included with the Informix database product itself - no add-on is required. This is similar to the situation with IBM DB2 UDB.

Data Protection for Oracle

Data Protection for Oracle provides an interface between IBM Tivoli Storage Manager and Oracle Recovery Manager (RMAN) for Oracle 8i, Oracle 9i, and Oracle Database 10g databases. The data may be stored on the wide variety of storage devices supported by IBM Tivoli Storage Manager. Particular version support varies according to the underlying operating system of the Oracle server. For specific supported versions, see:

http://www.ibm.com/software/tivoli/products/storage-mgr-db/platforms.html

RMAN functions and features include:

- Full or table space backup of a database while it is online or offline.
- Full database restore while a database is online or offline.
- Table space restore while database is offline.
- Backups of archive log files.
- Block-level incremental backup of changed database pages.
- A “duplex copy” feature of RMAN V2.0 makes it possible to send a backup to two separate storage tapes simultaneously.
- Optimized performance with tunable multi-buffer caching during backups.
- Synchronization utility to reconcile inventory between the Tivoli Storage Manager server and the RMAN catalog.

Data Protection for SQL Server

Data Protection for SQL Server enables online backups of SQL Server databases to Tivoli Storage Manager storage. Data Protection for SQL Server features include:

- Full and transaction-log backup support
- The ability to maintain multiple versions of SQL Server database and transaction logs
- GUI and command-line interfaces to simplify usage
- Support for Tivoli Storage Manager automatic expiration and version control by policy, which frees users from having to explicitly delete Microsoft SQL Server backup objects in the Tivoli Storage Manager server

- Support for Microsoft SQL Server V7.0, Microsoft SQL Server 2000, and Microsoft SQL Server 2005
- MSCS support for failover
- Differential backup and restore of SQL Server databases
- Backup and restore of individual filegroups and individual database files
- SQL Server data striping for high performance
- The ability to restore to a standby SQL server
- The ability to restore to a different SQL server or to different physical file names

IBM Tivoli Storage Manager for Enterprise Resource Planning

IBM Tivoli Storage Manager for Enterprise Resource Planning (ERP) is an optional software module that integrates with Tivoli Storage Manager to protect infrastructure and application data and improve the availability of SAP® servers.

Tivoli Storage Manager for ERP offers the following features:

- It is specifically designed and optimized for SAP environments.
- It is SAP certified for heterogeneous environments.
- It reduces the performance impact of backup and restore operations on mySAP™ servers.
- It allows multiple mySAP servers to utilize a single IBM Tivoli Storage Manager server.
- It can handle large-volume backups and restores, and data cloning.
- Multiple path and session support provides one path or session per tape device, thus maximizing backup and restore performance.
- Multiple server operations enable multiple Tivoli Storage Manager servers to be used in parallel for backup and restore, thus eliminating capacity bottlenecks.
- Multiplexing merges multiple data streams into one data stream, thereby leveraging the full write bandwidth of storage devices and minimizing backup window times.
- Multiple log files store log files in two management classes, thus providing additional security through redundancy of log files.
- SAN support and integration allows the use of SAN fiber channels with high bandwidth for LAN-free backups and restores.

- Support for FlashCopy and split mirror technology creates an additional disk for backup purposes, leaving mySAP applications and performance unaffected during the backup.
- Adaptive file sequencing sorts and sequences files to be backed up according to the overall status of the path and session load, thereby optimizing resource usage and decreasing total backup and restore times.

IBM Tivoli Storage Manager for Mail

IBM Tivoli Storage Manager for Mail is an optional software module for IBM Tivoli Storage Manager that automates the data protection of e-mail servers running either Lotus® Domino® or Microsoft Exchange. IBM Tivoli Storage Manager for Mail utilizes the APIs provided by Lotus and Microsoft to perform online hot backups without shutting down the e-mail server. Tivoli Storage Manager for Mail enables 24x7x365 operation of e-mail servers while performing data backups and restores.

For Lotus Domino databases, IBM Tivoli Storage Manager for Mail exploits the Lotus Domino “transaction logging” feature, enabling the capture of just the database changes for logged databases. Thus, full database backups are not required as frequently as in previous Domino releases.

For Microsoft Exchange, Tivoli Storage Manager for Mail supports Microsoft Exchange Server V5.5, Microsoft Exchange Server 2000, and Microsoft Exchange Server 2003. It uses the Microsoft backup APIs to create a copy of the Exchange server storage group databases along with the associated transaction logs. Tivoli Storage Manager for Mail can produce the different types of backups specified by Microsoft backup APIs: full backups, incremental backups, differential backups, copy backups, and database copy backups.

Data Protection for Lotus Domino

Data Protection for Lotus Domino helps protect and manage Lotus Domino V6.5, 7, and 8 servers. Data Protection for Lotus Domino:

- Performs centralized, online, incremental backup of Lotus Domino databases
- Integrates with the Tivoli Storage Manager Web client
- Maintains multiple versions of Domino databases
- Archives Domino transaction log files, when archival logging is in effect
- Restores backup versions of a Domino database and applies changes made since the backup from the transaction log
- Restores Domino databases to a specific point in time
- Recovers to the same or different Domino server

- Performs expiration database backups automatically based on version limit and retention period
- Expires archived transaction logs when they are no longer needed
- Provides online documentation: context-sensitive, task, and conceptual help
- Performs automated scheduled backups
- Recovers one or more archived transaction logs independent of a database recovery
- Recovers from the loss of the transaction log
- Archives the currently filling transaction log file
- Supports Domino Individual Mailbox restore

Data Protection for Lotus Domino provides two types of database backups, incremental and selective, and a log archive function. Incremental backup provides a conditional backup function that creates a full online backup of Domino databases when necessary. The specific conditions that determine when a new backup is necessary vary depending on whether or not the database is logged. Selective backup unconditionally backs up the specified databases, unless they are excluded from backup through exclude statements. When archival logging is in effect, changes to logged databases can be captured between full backups by archiving the transaction log.

Data Protection for Microsoft Exchange Server

Data Protection for Microsoft Exchange Server provides complete integration with Microsoft Exchange APIs, featuring:

- Centralized online backups (full, copy, incremental, and differential) of Exchange Directory and Information stores to Tivoli Storage Manager server storage
- Auto-detection of the Recovery Storage Group facility of Exchange 2003 to provide restoration of mailbox databases without dismounting or affecting the existing mailboxes
- Automatic expiration and version control by policy
- Failover for MSCS
- Parallel backup sessions for high performance
- Automated transaction log file management
- LAN-free backup
- Windows GUI
- The ability to restore objects to a specified directory

Data Protection for Exchange Server supports Microsoft Exchange individual Mailbox restore in conjunction with the Tivoli Storage Manager backup-archive client and the Microsoft ExMerge tool.

IBM Tivoli Storage Manager for Microsoft SharePoint

IBM Tivoli Storage Manager for Microsoft SharePoint enables you to quickly and confidently restore your Microsoft SharePoint business data and content due to a business interruption of almost any kind.

IBM Tivoli Storage Manager for Microsoft SharePoint is a policy-based backup and recovery solution that provides full, incremental, or differential backup at the site level, subsite level, and item level for Microsoft SharePoint Portal 2003, Microsoft Office SharePoint Server 2007, and Windows SharePoint Services V2.0 and V3.0 environments.

For more information, visit the Web page:

`http://www-306.ibm.com/software/tivoli/products/storage-mgr-sharepoint/`

IBM Tivoli Storage Manager for Advanced Copy Services

IBM Tivoli Storage Manager for Advanced Copy Services (formerly known as IBM Tivoli Storage Manager for Hardware) is an optional software module for AIX that integrates with IBM Tivoli Storage Manager Extended Edition. Tivoli Storage Manager for Advanced Copy Services protects mission-critical data that must be available 24x7 and integrates hardware- and software-based snapshot capabilities with IBM Tivoli Storage Manager and its data-protection components for DB2 UDB, Oracle, and mySAP.

Tivoli Storage Manager for Advanced Copy Services supports a wide range of hardware:

- IBM DS6000
- IBM DS8000
- SAN Volume Controller (SVC) and all IBM and non-IBM devices supported by the SVC
- IBM Enterprise Storage Server® (ESS)

For a complete list, see:

http://www.ibm.com/servers/storage/software/virtualization/svc/interop.html

Tivoli Storage Manager for Advanced Copy Services also provides the following functionality:

- FlashCopy support for ESS for Oracle

- FlashCopy support for ESS for DB2
- FlashCopy support for ESS for mySAP on DB2 UDB
- FlashCopy support for ESS for mySAP on Oracle
- Snapshot support for DS8000, DS6000, and SVC for DB2 UDB
- Snapshot support for DS8000, DS6000, and SVC for Oracle
- Snapshot support for DS8000, DS6000, and SVC for mySAP on DB2 UDB
- Snapshot support for DS8000, DS6000, and SVC for mySAP on Oracle
- Multiple snapshot versions managed by Tivoli Storage Manager policy
- Coordinated FlashCopy backup of multi-partition DB2 UDB databases distributed across multiple host systems.

Support of FlashCopy and snapshot functionality allows for “zero impact” backups and instant recovery. Data transfer to the Tivoli Storage Manager server is handled from a separate storage server, allowing the primary production data to remain online and undisturbed.

IBM Tivoli Storage Manager for Copy Services

IBM Tivoli Storage Manager for Copy Services is a optional module for Windows that integrates with IBM Tivoli Storage Manager and IBM Tivoli Storage Manager Extended Edition. It is designed to leverage the Microsoft Volume Shadow Copy Services (VSS) on Windows 2003. Tivoli Storage Manager for Copy Services provides similar functionality to Tivoli Storage Manager for Advanced Copy Services, supporting Windows VSS with Microsoft Exchange Server 2003 and Microsoft SQL Server 2005.

Tivoli Storage Manager for Copy Services features:

- Single command-line interface for performing Legacy and VSS snapshot backup, restore, and query operations
- Single GUI for performing Legacy and VSS snapshot backup, restore, and query operations
- Support for both hardware and software VSS providers that strictly adhere to Microsoft VSS provider requirements
- Support for a clustered Exchange environment
- Support for a clustered Microsoft SQL Server environment

As with Tivoli Storage Manager for Advanced Copy Services, zero impact backups and instant recovery allow the primary production data to remain online and undisturbed. Data movement to IBM Tivoli Storage Manager storage can be offloaded to a secondary machine by a VSS Hardware provider that supports transportable shadow copy volumes.

B

Microsoft SQL Server overview

A successful implementation of Tivoli Storage Management products that protect a Microsoft SQL Server environment requires that both Microsoft SQL Server and Tivoli Storage Management administrators have a certain level of knowledge of each environment. This appendix is meant to facilitate the understanding of SQL Server for Tivoli Storage Manager administrators.

Microsoft SQL Server is a relational database management system (RDBMS) platform from Microsoft, used for online transaction processing (OLTP), data warehousing, and e-commerce applications. It also provides functionality for data integration, analytical processing, and reporting solutions.

It uses Transact SQL and XML to send requests between the client and the SQL server. Transact SQL is a programming and query language that enables data to be accessed, queried, updated, and managed. Microsoft SQL Server runs only on Windows platforms and has 32-bit and 64-bit editions.

Microsoft SQL Server 2005 components

Microsoft SQL Server 2005 consists of the following components:

- Database Engine

  The Microsoft SQL Server Database Engine is the core component of the Microsoft SQL Server platform. It is a service used to store, manage and secure data. It is also known as the SQL server itself, or the SQL server RDBMS.

- Analysis Services

  Analysis Services is the component used to support online analytical processing (OLAP) and data mining functionality in business intelligence applications.

- Integration Services

  Integration Services is the component used to integrate different sources of information to provide extract, transform, and load (ETL) capabilities to Microsoft SQL Server. Integration Services is a replacement for Data Transformation Services (DTS, that was available in Microsoft SQL Server releases 7 and 2000.

- Reporting Services

  Reporting Services is the component used to create reports from several data sources, allowing to publish Web-based reports in several formats.

- Notification Services

  Notification Services is the component to develop and deliver notifications.

- Full Text Search

  Full Text Search is the component used to submit full-text queries against plain text documents stored in Microsoft SQL Server tables.

- Replication

  Replication is the component used to distribute and replicate data from one database to another.

- Service Broker

  Service Broker is a component used to implement message queuing in Microsoft SQL Server.

Several Microsoft SQL Server components store their information in Microsoft SQL Server databases, while others use operating system files. From the point of view of backup needs for a Microsoft SQL Server platform, it is necessary to implement a solution containing both Microsoft SQL Server databases and operating system files backup. Refer to 2.3, “Microsoft SQL Server backup planning” on page 42 for a detailed discussion of the requirements for protecting all Microsoft SQL Server components.

Microsoft SQL Server Database Engine (RDBMS)

The Microsoft SQL Server Database Engine is the component used to manage data. It is commonly known as the SQL Server itself.

Similar to IBM DB2, the Microsoft SQL Server relational database management system (RDBMS) uses the concepts of *instance* and *database*, as shown in Figure B-1.

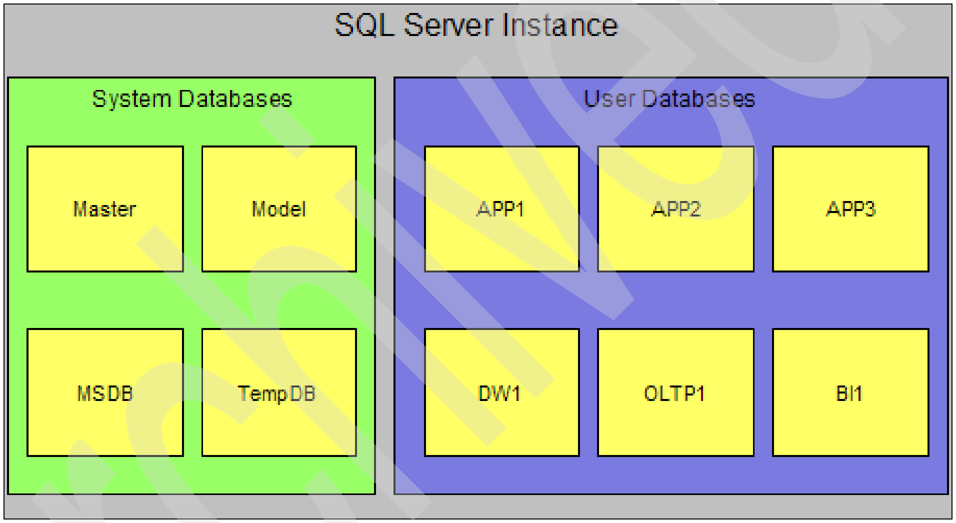

Figure B-1 Microsoft SQL Server instance and database concepts

Microsoft SQL Server instance

A Microsoft SQL Server instance is a set of operating system processes. It can be started either as a Windows service or, for certain maintenance operations, by using a command-line interface using the SQL server binaries. The SQL Server instance configuration parameters are stored in Windows registry files and in some Microsoft SQL Server databases.

Until Microsoft SQL Server release 7, it was possible to have only one SQL server instance per machine; since the release of Microsoft SQL Server 2000, it is possible to have several instances per machine.

Microsoft SQL Server database

A Microsoft SQL Server database is a physical structure stored on disk, which is accessed by a SQL server instance. It is made up of a collection of tables and objects that store data in a structured way.

Microsoft SQL Server databases are either system databases and user databases:

System databases

A system database stores information about the system - about Microsoft SQL Server itself, about all other databases, and about SQL Server components other than the Database Engine component.

Microsoft SQL Server has five system databases:

- Master

  The master database manages the SQL server and user databases and contains information about all databases residing on the SQL server. The master database is important, and it must be backed up every time you perform certain operations or system stored procedures that modify it automatically. Without a current backup of the master database, and in the case of failure, you must completely rebuild all of the system databases. The master database can be backed up only as a full database backup operation.

- Model

  The model database is a template for new user databases. All modifications made to the model database are applied to any database created afterward. If the model database is modified, it must be backed up. When rebuilding the master database, subsequent changes to the model databases are lost and must be restored from the backup.

- msdb

  The msdb database is used as storage area for scheduling information and job history. If you do not have a backup for this database, you must rebuild all of the system databases and then re-create each job, alert, and operator.

- tempdb

  The tempdb table is used for temporary tables and other temporary working storage needs. You cannot back up this database - it is re-created each time the SQL server is restarted.

- Resource

  The resource database is a new system database for Microsoft SQL Server 2005 and contains system objects that are included with Microsoft SQL Server 2005. The system objects logically appear in the sys schema of every database but are physically stored in the resource database. The resource database is read-only and cannot be modified without support from a Microsoft Customer Support Services (CSS) specialist. The resource database cannot be backed up by Data Protection for SQL Server; instead, use the Tivoli Storage Manager backup-archive client to back up the file as an operating system file, similar to the SQL server binaries. The resource database data files are located in the same place as the data files for the master database, and if you move or restore the master database to a different location, you must also move or restore the resource data files to the same location as the master database data files. The resource database data file and log file are mssqlsystemresource.mdf and mssqlsystemresource.ldf, respectively.

  For more information about the resource database, refer to Microsoft Books Online:

  `http://msdn2.microsoft.com/en-us/library/ms190940.aspx`

Microsoft SQL Server does not support directly updating the information stored in the system databases. To manage and modify the information stored in the system databases, you must use one of the Microsoft SQL Server administrative tools provided within the Microsoft SQL Server installation.

User databases

A user database stores user information. You create and store tables, indexes, procedures, triggers, and other objects in user databases.They must be backed up regularly, especially after an index has been created after a load operation. It is good practice to create different user databases for different applications.

Each database, including the master database, contains a database catalog, which is a collection of system tables containing metadata about the database. System tables store metadata, which is information about the data. The master database contains a collection of system tables that store information about the entire system and all other databases.

Database files

Microsoft SQL Server databases have three types of files:

- Primary data file

  This file contains the database catalog tables. It can also contain user data and objects. The recommended file name extension for primary files is .mdf.

- Secondary data file

  This optional file contains user data and objects only and is used to spread data across different files and drives. The recommended file name extension for secondary files is .ndf.

- Transaction log file

  This file records all database transactions, and it is used to recover the database in case of failures. The recommended file name extension for transaction log files is .ldf.

Each Microsoft SQL Server database has at least two operating system files: a primary data file and a transaction log file. By default, the data and transaction log files are stored in the same location; however, for production environments, we recommend, whenever possible, that you put data files and transaction log files on different disks. You can have up to 32,767 files in a database.

The location of all data files in a database is recorded in the master database and also in the database primary data file. Most of the time, Microsoft SQL Server uses the information stored in the master database to identify the data files, but, in some situations - such as a recover from the master database - SQL Server uses the information stored in the primary data file to initialize the database.

All files have a logical name and a physical name. The logical name is the name that references the file inside Microsoft SQL Server, and the physical name is the operating system file name. SQL Server data files can be stored in either FAT or NTFS file systems.

Database filegroups

For administrative and allocation purposes, you can group database objects and files in filegroups, the two types of which are:

- Primary filegroups

  The primary filegroup contains the primary data file and any other data files that are not specifically assigned to a user-defined filegroup. The primary filegroup is created automatically during database creation.

- User-defined filegroups

  All other filegroups are user-defined filegroups.

> **Note:** Transaction log files are not part of a filegroup.

Each data file is member of only one filegroup, and a database object can be stored in only one filegroup. For each database, one filegroup is designated as the default filegroup. When a database object is created without the filegroup specification, the object is stored in the default filegroup. If no default filegroup is specified, the primary filegroup becomes the default filegroup.

Example B-1 shows how to create a database with several files and filegroups.

Example: B-1 Database creation with filegroups

```
USE master;
GO

CREATE DATABASE OLTP
ON PRIMARY
  ( NAME='OLTP_PRI_Dat',
    FILENAME=
       'd:\MSSQL\OLTP\data\OLTP_Primary.mdf',
    SIZE=100MB,
    MAXSIZE=200MB,
    FILEGROWTH=20MB),
FILEGROUP OLTP_FG1
  ( NAME = 'OLTP_FG1_Dat1',
    FILENAME =
       'E:\MSSQL\OLTP\data\OLTP_FG1_DF1.ndf',
    SIZE = 1000MB,
    MAXSIZE=2000MB,
    FILEGROWTH=100MB),
```

```
  ( NAME = 'OLTP_FG1_Dat2',
    FILENAME =
       'F:\MSSQL\OLTP\data\OLTP_FG1_DF2.ndf',
    SIZE = 1000MB,
    MAXSIZE=2000MB,
    FILEGROWTH=100MB)
LOG ON
  ( NAME='OLTP_log',
    FILENAME =
       'G:\MSSQL\OLTP\log\OLTP_LOG_DF1.ldf',
    SIZE=400MB,
    MAXSIZE=1000MB,
    FILEGROWTH=100MB);
GO
```

The command executed in Example B-1 on page 269 creates a database with a structure similar to the database depicted in Figure B-2.

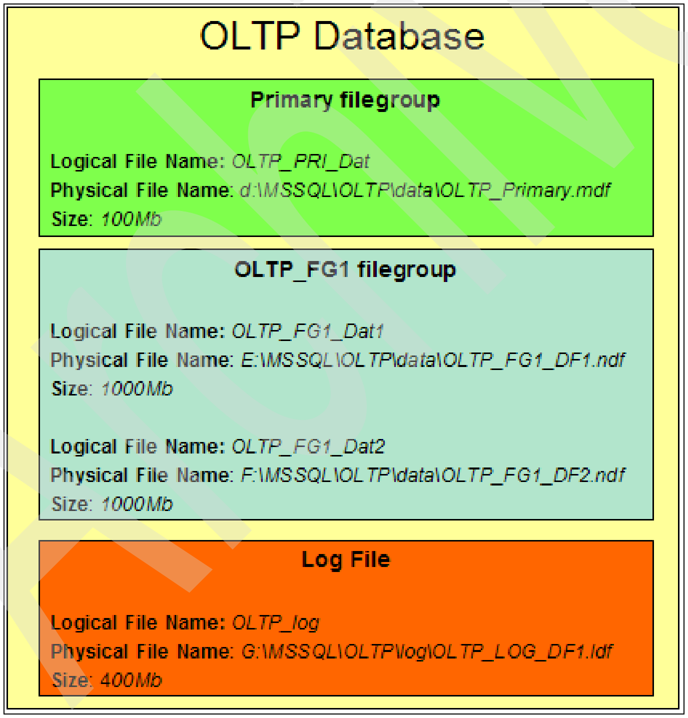

Figure B-2 OLTP database structure example

Database recovery model

Before we discuss database recovery models, we provide a brief introduction to how transactions are handled by Microsoft SQL Server.

The Microsoft SQL Server recovery model relies on a transaction log to record all transaction activities in the database. When data is modified, this modification is first written to the log cache and to the transaction log file. The information recorded for the transaction contains the modification being executed by the transaction, the necessary information to undo (or roll back) the transaction and restore the data to the state before the operation (the before image), and the value of the data after the transaction (the after image). Some transactions record the entire row, while others record only the bytes that have changed during the transaction.

Transactions from the transaction log are periodically committed to the database data files and written to the disk. At this point, the transaction log records for these transactions become inactive - all such transaction information is already written in the database data files and the transaction log records are used only if a database restore from a backup taken prior to this moment is performed.

The transaction log architecture enables Microsoft SQL Server to perform three operations:

- Recover from a single transaction

  When an application submits a ROLLBACK command, or when a connection failure occurs between the client and the server, the log records stored in the transaction log are used to roll back the modifications made by the incomplete transactions.

- Recover all transactions when a database is started

  When a database is restarted after a failure, the transaction log records are used to roll forward committed transactions that are not written in the database data files and to roll back any uncommitted transactions, ensuring database integrity.

- Rolling forward a database in a recovery scenario

  After a database restore, Microsoft SQL Server uses the transaction log records to reapply all recorded transactions performed in the database and to roll back any uncommitted transactions.

The Microsoft SQL Server transaction log architecture also allows standby-server solutions, database mirroring, and log shipping. A discussion of these SQL Server capabilities is not within the scope of this book. For more information, see the Microsoft SQL Server documentation.

Multiple log files are treated as though they were concatenated into a single file.

As more transactions are performed against a database, more information is recorded in the transaction log file. This can lead to a scenario where a transaction log can grow indefinitely, filling all available space on the disks holding the physical log files. However, older transactions recorded in the transaction log may have become inactive - becoming transactions that do not have to be recovered or restored to the database - and can be deleted. The process of deleting the old records and reusing the space is called *truncating the log*. The active portion of the transaction log can never be truncated because it contains information required to recover the database at any time, allowing the database to roll back the transactions.

> **Note:** Truncating the transaction log does not reduce the size of a physical log file; it reduces only the size of the logical log file. To reduce the size of a physical log file, it is necessary to shrink the file, using, for example, the DBCC SHRINKFILE command.

When a log truncation occurs, all inactive transactions are deleted from the transaction log. However, this information is still required to roll forward a database during a recovery process. To address this situation, Microsoft SQL Server enables you to perform transaction log backups. A transaction log backup copies all information recorded in the transaction log to a backup file and then performs a truncate log to liberate space for new transactions.

> **Note:** Backup database strategies are discussed in 2.3, "Microsoft SQL Server backup planning" on page 42.

Another important aspect is that recording all database transactions can severely impact performance in the environment - specially for operations that demand a high degree of data manipulation, such as an index creation or a data warehouse load process. In addition, recording all database transactions can consume a large amount of disk space.

In this situation, Microsoft SQL Server enables you to reduce the amount of information that is recorded in the transaction log files. Because not all information is recorded in the transaction log file, the trade-off is that you may not be able to fully restore a database because not all required information is recorded.

To give administrators the flexibility of choosing the right option for their specific needs, Microsoft SQL Server implements three database recovery models that are mutually exclusive and, with some limitations, can be changed when needed. We discuss the three database recovery models in the sections that follow.

Simple recovery model

If the database is lost in simple recovery model databases, you lose all modifications performed since the last full backup or last differential backup and the point of failure.

With the simple recovery model, you cannot perform transaction log backups. Log space is automatically reclaimed, limiting the size of the transaction log file space. This model permits high-performance bulk-copy operations because only page allocations are logged instead of row insertions, increasing performance and reducing log space consumption.

> **Note:** The simple recovery model is similar to setting the `trunc. log on chkpt.` database option in Microsoft SQL Server V7.0 or earlier.

Generally, the simple recovery model is not used for read-write user databases in production environments.

Full recovery model

The full recovery model enables you to recover a database to a specific point in time, provided the backups are complete up to that point in time.

This recovery model requires more disk space for the transaction log files than other recovery models. Under this model, transaction log backups are essential and must be executed periodically to ensure database recovery and to keep transaction log disk usage at normal levels.

> **Note:** Even the full recovery model does not guarantee that you will not lose data. In an event of complete hardware crash, information that was stored in the tail of the log file may not have been backed up before the failure. In this case, you must redo all changes after the last transaction log backup.

Recovering a database in a full recovery model usually requires a combination of database backups and transaction log backups. Refer to 2.3, "Microsoft SQL Server backup planning" on page 42 for a detailed discussion of different strategies for backing up databases.

Generally, the full recovery model is the recommended recovery model for user databases in a production environment.

Bulk-logged recovery model

The bulk-logged recovery model is an adjunct to the full recovery model. It should be used only during large-scale bulk processes, such as index creation or a batch load. The bulk-logged recovery model permits high-performance bulk-copy operations because only page allocations are logged instead of row insertions. This increases performance and reduces log space consumption.

For databases using the bulk-logged recovery model, you still must back up the transaction log.

As is the case with full recovery model databases, it is possible to recover a bulk-logged database to the end of the transaction logs; however, point-in-time recovery is not supported for bulk-logged databases.

Microsoft SQL Server security

Securing a Microsoft SQL Server involves three areas:

- Platform and network, including the physical hardware, the operating system and the remote systems communicating with the SQL server
- Security of principals and database objects, which includes user authentication and authorization
- Application security, which is related to the security of applications accessing Microsoft SQL Server databases

Discussions of platform and network security considerations, as well application security considerations, are beyond the scope of this book. We provide an introduction to principal and database object security in the sections that follow.

Microsoft SQL Server 2000 and earlier

Until Microsoft SQL Server 2000, two levels of security were used to control access to SQL Server:

Authentication

The user must have an account to connect to a SQL server. The two authentication modes are:

- Windows authentication mode

  Microsoft SQL Server relies on Windows authentication to verify user name and password credentials. Microsoft SQL Server logons are not allowed to connect to the SQL server when Windows authentication mode is configured.

- Mixed mode authentication

  Provided for backward compatibility, mixed mode authentication enables users to connect to Microsoft SQL Server using either their Windows logon accounts or a SQL server logon account. When a SQL server logon account is used, the user name and password data are verified against the SQL server.

The users connected to Microsoft SQL Server using their logon accounts are called *trusted connections*. The Microsoft SQL Server administrator specifies which kind of authentication is used, and the default and recommended setting is Windows authentication only.

Authorization

After a user has been authenticated, the user must have proper permissions in order to perform any activity in the SQL server. Permissions determine the kinds of activities the user can perform. The two authorization levels are:

- Logon permissions

  The logon permissions are related to activities the user can perform at the Microsoft SQL Server instance level, such as create a database, modify a Microsoft SQL Server instance parameter, or create a Microsoft SQL Server logon. Logon permissions are granted through the use of fixed server roles, and each role has a predefined set of permissions. Examples of fixed server roles are the sysadmin role, which can perform any activity in the Microsoft SQL Server, or the serveradmin role, which can set serverwide configuration options and shut down the server.

- Database permissions

  Database permissions are related to activities the user can perform at the database level, such as create a table, read any table in the database, manage object permissions, and back up the database. Database permissions are configured through the use of fixed database roles or directly to users using the GRANT, REVOKE, and DENY commands. As fixed server roles, each fixed database role has a predefined set of permissions. Examples of fixed database roles are the role, which can perform any activity in the database; the db_backupoperator, which has permission to back up the database; and the db_datareader, which can access data from all user tables in the database.

Microsoft SQL Server 2005

To provide more granular control over security components, Microsoft SQL Server 2005 introduces a new concept for security, based on principals. securables, and permissions. This concept can be understood as an extension to the previous authentication and authorization concepts.

Principals

Principals are users, groups, and applications granted access to Microsoft SQL Server. The three different types of principals are:

- Windows-based principals

  Examples of Windows-based principals are Windows domain logons and Windows user logons.

- SQL Server-level principal

  An example of a SQL Server-level principal is the sa SQL Server account.

- Database-level principal

  Examples of database-level principals are database users, database roles, and application roles.

The principals connect to the Microsoft SQL Server database using Microsoft SQL Server authentication or Windows authentication methods.

Securables

Securables are resources that have authorization access controlled either by Microsoft SQL Server or by the Windows operating system. At the Windows level, the securables include files and registry keys used by Microsoft SQL Server. At the SQL server level, securables are resources, such as the server itself, the databases, and the objects stored within a database, that have authorization access controlled by Microsoft SQL Server.

The three scope levels for the SQL Server securables are:

- Server

  Examples of server securables are SQL Server endpoints, logons, and databases.

- Database

  Examples of database securables are database users, database roles, full text catalogs, and certificates.

- Schema

  Examples of schema securables are types, objects (such as tables, views, and procedures), and XML schema collections.

Permissions

Permissions are the rights granted to principals to perform an activity against the securables. At the Windows securable level, permissions are controlled through Windows access control lists (ACL). The GRANT, REVOKE, and DENY statements are used to control the permissions that principals can perform on SQL Server securables. Each SQL Server securable has an associated set of permissions. Examples of permissions are the SELECT, INSERT, UPDATE, and DELETE permissions applicable to TABLE objects, the EXECUTE permission related to PROCEDURE objects, and the BACKUP permission related to the DATABASE securable.

For a detailed description of principals, securables, and permissions, refer to the Microsoft SQL Server documentation.

Microsoft SQL Server services

A Microsoft SQL Server installation creates several Microsoft Windows services. Some of them are instance-aware, meaning that the service is associated with a specific Microsoft SQL Server instance, while other services are instance-unaware, when the service is shared among all Microsoft SQL Server instances installed on the machine. The instance-unaware services are installed only once and cannot be installed side by side, while an instance-aware service can be installed multiple times, each one using its own Microsoft SQL Server binaries.

In a default Microsoft SQL Server installation, the instance-aware services are:

- SQL Server (MSSQLSERVER) - service name: MSSQLSERVER

  The service for the SQL Server Database Engine (RDBMS) component.

- SQL Server agent (MSSQLSERVER) - service name: SQLSERVERAGENT

  The service for the SQL Server agent process, responsible for execute jobs, monitors SQL Server, fires alerts, and allows administrative tasks. The SQL Server agent is dependent on the SQL Server service.

- SQL Server Analysis Services (MSSQLSERVER) - service name: MSSQLServerOLAPService

  The service responsible for the Analysis Server component.

- SQL Server FullText Search (MSSQLSERVER) - service name: msftesql

  The service responsible for the FullText Search component.

- SQL Server Reporting Services (MSSQLSERVER) - service name: ReportServer

  The service responsible for the Reporting Services component.

In the Windows Services utility display names, the string MSSQLSERVER between parentheses identifies the instance of the SQL server. For the default instance, it is MSSQLSERVER. For named instances, it is replaced by the named instance name. Moreover, for named instances, the service name itself also receives the instance identifier. For a named instance called SQLNAMED1, for example, the instance-aware services are:

- SQL Server (SQLNAMED1) - service name: MSSQL$SQLNAMED1
- SQL Server agent (SQLNAMED1) - service name: SQLAgent$SQLNAMED1
- SQL Server Analysis Services (SQLNAMED1) - service name: MSOLAP$SQLNAMED1
- SQL Server FullText Seach (SQLNAMED1) - service name: msftesql$SQLNAMED1
- SQL Server Reporting Services (SQLNAMED1) - service name: ReportServer$SQLNAMED1

The instance-unaware services are:

- SQL Server Active Directory Helper - service name: MSSQLServerADHelper

  The SQL Server Active Directory Helper is responsible for publishing and managing SQL Server services in the Active Directory.

- SQL Server Browser - service name: SQLBrowser

  The SQL Server Browser Service allows name resolution that provides SQL Server connect information for client computers.

- SQL Server Integration Services - service name: MsDTSServer

  This service is responsible for the Integration Services component. It provides management support for SSIS packages storage and execution.
- SQL Server VSS Writer - service name: SQLWriter

  The SQL Server VSS Writer service is responsible for integrating backup and restore applications to operate in the VSS framework.

Each Microsoft SQL Server account has its own registry, file system, and operating system security requirements to operate properly. These requirements are configured by the Microsoft SQL Server installer during Microsoft SQL Server installation.

Microsoft SQL Server administrative tools

Microsoft SQL Server provides several management tools to help administrators to minimize and automate daily tasks. Table B-1 lists some Microsoft SQL Server 2000 and Microsoft SQL Server 2005 tools and their functionality.

Table B-1 Microsoft SQL Server administrative tools

SQL Server 2000	SQL Server 2005	Functionality
Enterprise Manager	SQL Server Management Studio	Execute most administrative tasks for Microsoft SQL Server databases
Query Analyzer	Code editor in SQL Server Management Studio	Execute ad hoc queries - GUI tool
Server Network Utility	SQL Server Configuration Manager	Configure server network protocols and parameters
Client Network Utility	SQL Server Configuration Manager	Configure client network protocols and parameters
Service Manager	SQL Server Configuration Manager	Start and stop Microsoft SQL Server databases
osql command prompt tool	osql is still supported sqlcmd	Start and stop Microsoft SQL Server databases
Books on Line	Books on Line	Microsoft SQL Server documentation

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 282. Note that some of the documents referenced here may be available in softcopy only.

- *IBM Tivoli Storage Manager Implementation Guide*, SG24-5416
- *IBM Tivoli Storage Management Concepts*, SG24-4877
- *Using IBM Tivoli Storage Manager to Back Up Microsoft Exchange with VSS*, SG24-7373

Other publications

These publications are also relevant as further information sources:

- *IBM Tivoli Storage Manager for Databases Data Protection for Microsoft SQL Installation and User’s Guide*, SC32-9059
- *IBM Tivoli Storage Manager for Windows: Backup-Archive Clients Installation*, SC32-0146
- *IBM Tivoli Storage Manager for AIX Administrator’s Guide Version 5.5,* SC32-0117
- *IBM Tivoli Storage Manager for AIX Administrator's Reference Version 5.5,* SC32-0123
- *IBM Tivoli Storage Manager for HP-UX Administrator’s Guide Version 5.5,* SC32-0118
- *IBM Tivoli Storage Manager for HP-UX Administrator’s Reference,* SC32-0773
- *IBM Tivoli Storage Manager for Linux Administrator’s Guide Version 5.5*, SC32-0119

- *IBM Tivoli Storage Manager for Linux Administrator's Reference Version 5.5*, SC32-0125
- *IBM Tivoli Storage Manager for Sun Solaris Administrator’s Guide Version 5*, SC32-0120
- *IBM Tivoli Storage Manager for Sun Solaris Administrator’s Reference Version 5.5*, SC32-0126
- *IBM Tivoli Storage Manager for Windows Administrator’s Guide Version 5.5*, SC32-0121
- *IBM Tivoli Storage Manager for Windows Administrator’s Reference Version 5*, SC32-0127
- *IBM Tivoli Storage Manager for z/OS Administrator’s Guide Version 5.5*, SC32-0122
- *IBM Tivoli Storage Manager for z/OS Administrator’s Reference Version 5.5*, SC32-0128

Online resources

These Web sites are also relevant as further information sources:

- IBM Tivoli Storage Manager publications site:

  `http://publib.boulder.ibm.com/infocenter/tivihelp/v1r1/index.jsp`

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

Backing up Microsoft SQL Server with IBM Tivoli Storage Manager

(0.5” spine)
0.475”<->0.875”
250 <-> 459 pages

Backing up Microsoft SQL Server with IBM Tivoli Storage Manager

Strategic planning and implementation considerations for effective backup

Tivoli Data Protection for SQL Server V5.5 VSS backups

SQL Server overview for TSM administrators

This IBM Redbooks publication describes how to plan, install, and implement backup and restore for Microsoft SQL Server using Tivoli Storage Manager products. The book is intended for Tivoli Storage Manager professionals who are responsible for the backup and restore of a Microsoft SQL Server installation using Tivoli Storage Manager.

We discuss the planning, installation, and operation of Tivoli Storage Manager with Microsoft SQL Server. We also give an overview of the Tivoli Storage Manager family of products. We provide essential information regarding Microsoft SQL Server - information intended to assist Tivoli Storage Manager administrators understand the database middleware platform.

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

SG24-6148-01 ISBN 073848542X