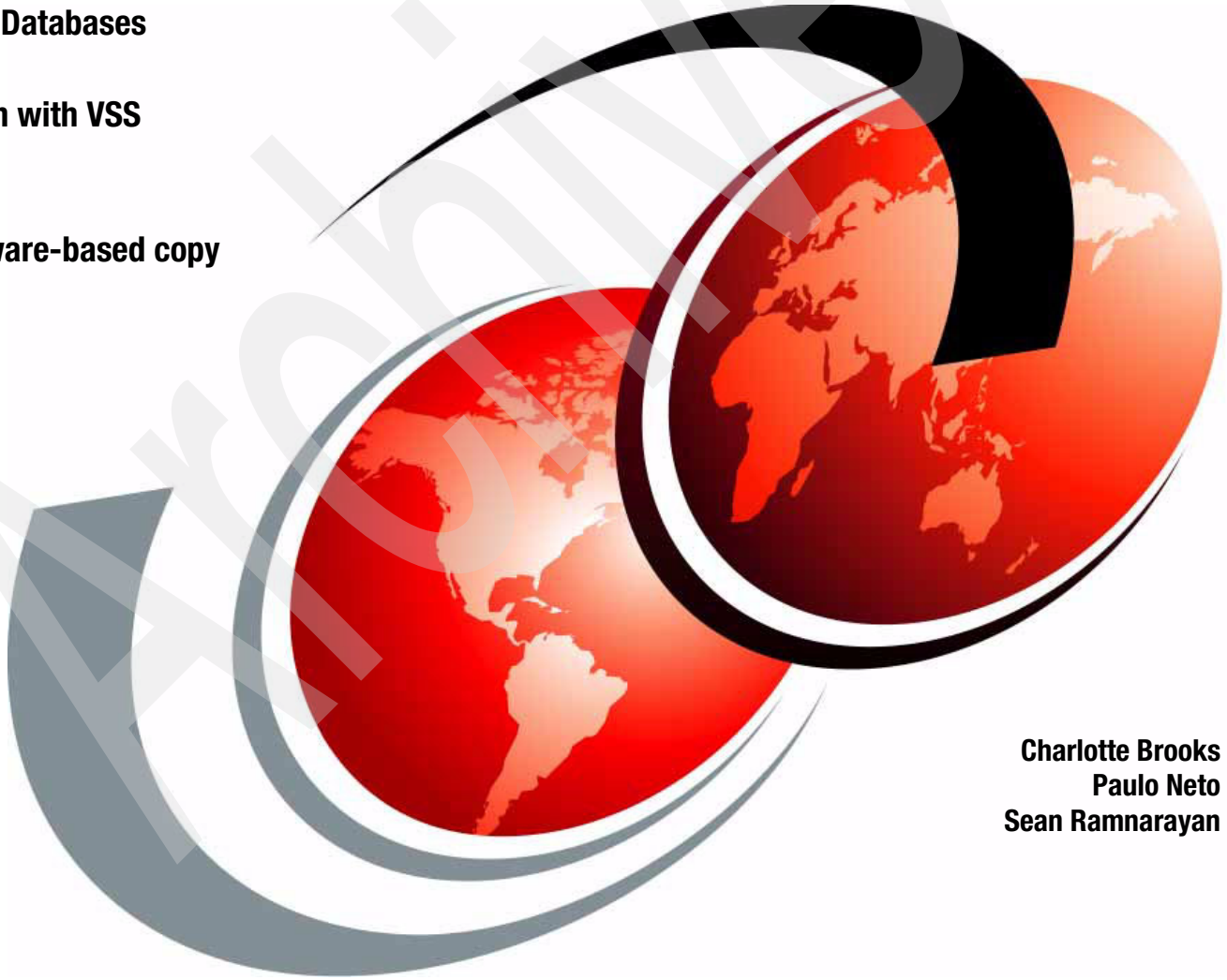
Tivoli software

IBM

Using IBM Tivoli Storage Manager to Back Up Microsoft Exchange with VSS

- Fast backup and restore of Microsoft Exchange Databases
- Integration with VSS
- Use hardware-based copy services



Charlotte Brooks
Paulo Neto
Sean Ramnarayan

Redbooks

ibm.com/redbooks

International Technical Support Organization

Using IBM Tivoli Storage Manager to Back Up Microsoft Exchange with VSS

October 2006

SG24-7373-00

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

First Edition (October 2006)

This edition applies to 5608-CSS IBM Tivoli Storage Manager for 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

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

@server®	DS4000™	Redbooks™
@server®	DS6000™	System p™
Redbooks (logo)  ™	DS8000™	System Storage
eServer™	FlashCopy®	Tivoli®
pSeries®	HACMP™	TotalStorage®
AIX®	IBM®	WebSphere®

The following terms are trademarks of other companies:

Active Directory, Microsoft, 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.

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

Typical Microsoft® Exchange environments are growing larger and increasingly are managing data and applications critical to a business. This makes backup and restore a greater challenge. Microsoft Volume Shadow Copy Service (VSS) is a way to use instant copy capabilities of disk storage hardware for faster backup, thereby reducing the time taken for backup as well as reducing the impact which the backup operation has on the Exchange server.

IBM® Tivoli® Storage Manager for Copy Services, together with Tivoli Storage Manager for Mail Data Protection for Exchange, leverages VSS functionality in an integrated, easy-to-use way, to back up and restore Exchange databases. It supports a wide variety of disk hardware and uses the same interface as traditional Data Protection for Exchange operations.

This IBM Redbook will help you plan, configure and run IBM Tivoli Storage Manager for Copy Services in your Microsoft Exchange environments.

The team that wrote this redbook

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

Left to right: Charlotte, Paulo, Sean

Charlotte Brooks is an IBM Certified IT Specialist and Project Leader for Storage Solutions at the International Technical Support Organization, San Jose Center. She has 15 years of experience with IBM in storage hardware and software support, deployment, and management. She has written many IBM Redbooks™, and has developed and taught IBM classes in all areas of storage and storage management. Before joining the ITSO in 2000, she was the Technical Support Manager for Tivoli Storage Manager in the Asia Pacific Region.

Paulo Neto is a Senior IT Specialist in IBM Global Services, Portugal. He has been with IBM for more than 17 years, and has seven years of experience in Tivoli Storage Manager. His areas of expertise include storage implementation, storage management, SANs, Disaster Recovery, System p™, and HACMP™. He is an IBM Certified Advanced Deployment Professional - Tivoli Storage Management Solutions and an IBM eServer™ Certified Systems Expert - pSeries® HACMP for AIX® 5L. He also holds several professional certifications in

pSeries, AIX, TotalStorage®, Tivoli Workload Scheduler, SNIA and ITIL. Paolo has a degree in Electronics and Computer Engineering from I.S.E. do Porto and is pursuing a Master's degree in Computer Science at Faculdade de Ciências da Universidade do Porto. He is a Certified Tivoli Instructor for Tivoli Storage Manager.

Sean Ramnarayan is a Senior IT Specialist with IBM in Cape Town, South Africa. He has 18 years of experience in the IT field. He has worked at IBM for the last 14 months as a Tivoli Storage Manager Specialist, and is IBM Certified in Tivoli Storage Manager V5.2 Implementation. Sean's areas of expertise include AIX, disaster recovery solutions, several Data Protection products and Tivoli Storage Manager solution implementation.

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

Deanna Polm, Sangam Racherla
International Technical Support Organization, San Jose Center

Del Hoobler
IBM Endicott

Danny Cao, Bruce Fong, Neeta Garimella, Jie Liang
IBM San Jose

David West
IBM Seattle

Lu Nguyen
IBM Tampa

Michel Baus
SVA, Germany

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll 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'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Obtain more information about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

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

- Use the online **Contact us** review redbook 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

1

Introduction

In this chapter we provide you with an overview of IBM Tivoli Storage Manager for Copy Services, as well as the associated technologies such as the Volume Shadow Copy Service (VSS), Virtual Disk Services (VDS), and snapshot techniques.

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

The following topics are discussed:

- Data Protection for Exchange and IBM Tivoli Storage Manager for Copy Services overview
- Snapshots overview
- Volume Shadow Copy Service
- Virtual Disk Services
- VSS integration with Data Protection for Microsoft Exchange

1.1 Tivoli Storage Manager for Copy Services - Data Protection for Exchange overview

Today, e-mail systems play a key role in making an enterprise successful. Businesses are often severely impacted when e-mail service is down, even if other production services are running. Consequently, ensuring e-mail server availability has become a critical business concern.

In the face of such constraints, there are requirements to be addressed, such as:

- Fast recovery
- Fast backups
- "Zero impact", high performance backups
- Intelligent management of these backups

Addressing these demands, IBM Tivoli Storage Manager for Copy Services provides an enhanced backup and recovery solution integrating VSS-based snapshot capabilities (see 1.3, "Volume Shadow Copy Service" on page 6) with Tivoli Storage Manager for Mail - specifically the Data Protection for Microsoft Exchange component.

Tivoli Storage Manager for Copy Services offers new options to implement highly efficient backup, while minimizing the backup-related impact on the performance of the Exchange production server.

Definition: In this publication, we refer to the previously available backup capabilities (without VSS) of Data Protection for Exchange (that is, without Tivoli Storage Manager for Copy Services) as *legacy backups*. See Legacy backup and "VSS backup" on page 14 for further details about this topic.

1.1.1 Data Protection for Exchange

Data Protection for Exchange performs online backups and restores of Microsoft Exchange Server databases to Tivoli Storage Manager storage. You can perform backups and restores using a command line or GUI on a Windows® 2000 or Windows 2003 system, in a standalone or clustered (MSCS) environment.

Data Protection for Exchange operations use the Tivoli Storage Manager API to communicate with the Tivoli Storage Manager server, and use the Exchange API to communicate with the Exchange Server

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

To reduce the overhead of backup operations on the Exchange server, you can choose to have the backup to Tivoli Storage Manager performed by another server with access to the shadow volumes; this is referred to as an *offloaded backup*. If a restore is required, you can choose to restore from either local snapshot volumes, or from Tivoli Storage Manager server storage.

1.1.2 New features of Data Protection for Exchange

There are new Data Protection for Exchange features available with the V5.3.3 release. Note that VSS features require the installation of Tivoli Storage Manager for Copy Services and other prerequisites as described in Chapter 2, “Pre-installation and planning” on page 19.

- Back up Exchange Server 2003 databases (running on Windows Server® 2003) using Microsoft Volume Shadow Copy Service (VSS) technology
- Perform a VSS backup to the Tivoli Storage Manager server from an alternate system instead of the production system (offloaded backup)
- Restore VSS backups that reside on local shadow volumes using file-level copy mechanisms
- Restore VSS backups that reside on local shadow volumes using hardware-assisted volume-level copy mechanisms (Instant Restore)
- Tivoli Storage Manager policy-based management of VSS snapshot backups
- A single GUI for performing legacy and VSS backup, restore, and query operations
- A single command line interface for performing legacy and VSS backup, restore, and query operations

Figure 1-1 summarizes the components of a Tivoli Storage Manager for Copy Services with Data Protection for Exchange solution providing VSS backup restore services.

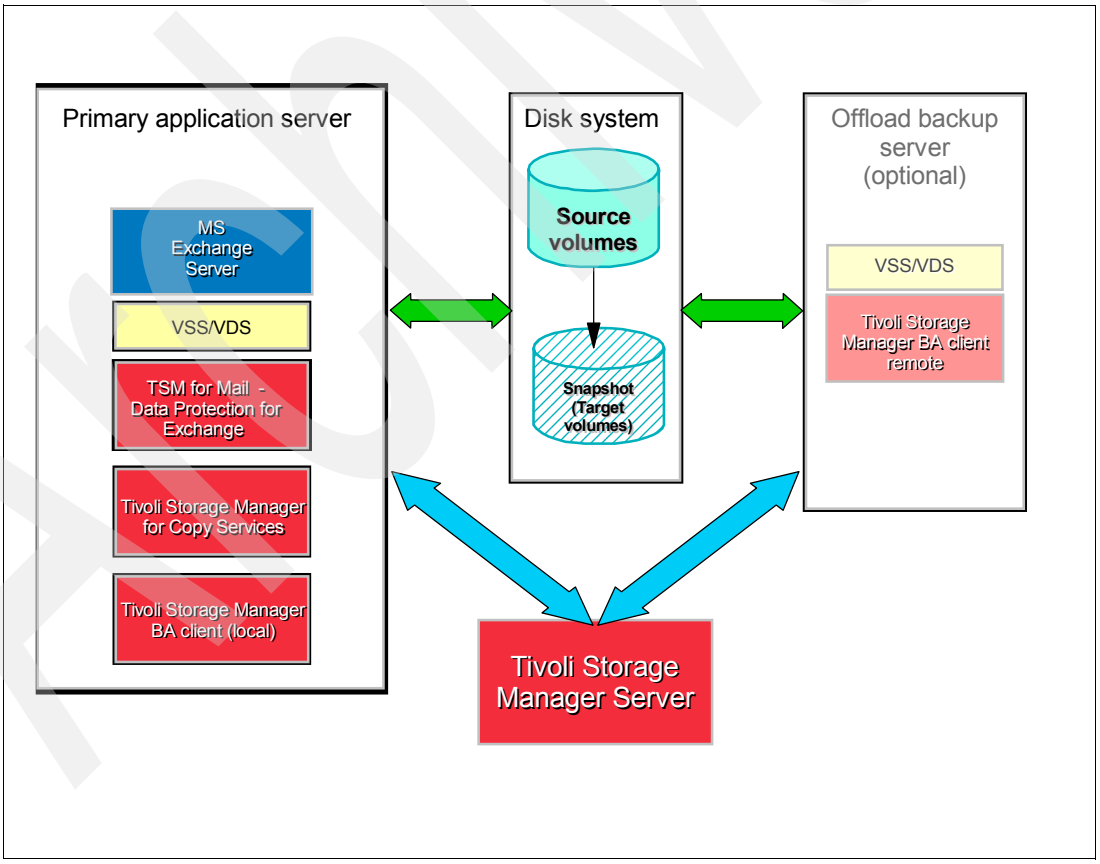


Figure 1-1 Data Protection for Exchange with Tivoli Storage Manager for Copy Services integration

1.2 Snapshots

Snapshot is a common industry term which means the ability to record the data stored on a storage device at any given moment and preserve that snapshot as a way to perform backup, restore, data mining or 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 done 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 of the 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, along with some examples.

1.2.2 Copy-on-write

In the copy-on-write method, a snapshot of a storage volume is created using pre-designated 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 done 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 that is being written to is copied into 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 that describes the data blocks that have changed since the snapshot was first created. Note that original data blocks are copied only once into the snapshot storage, when the first write request is received.

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 snapshot are satisfied from the original volumes if data being read has not changed. Additionally, the snapshot requires that original copy of the data is still valid.

However, this method is highly space-efficient, because the storage required to create a snapshot is minimal to hold 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 onto 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 reside 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 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 LUN for which the snapshot is being created) onto another entity of the same kind and the exact same size. The entire contents of the original volume are copied onto a separate volume. Clone copies are highly available, since 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 into two, with the side effect 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. This is shown in Figure 1-2 on page 6.

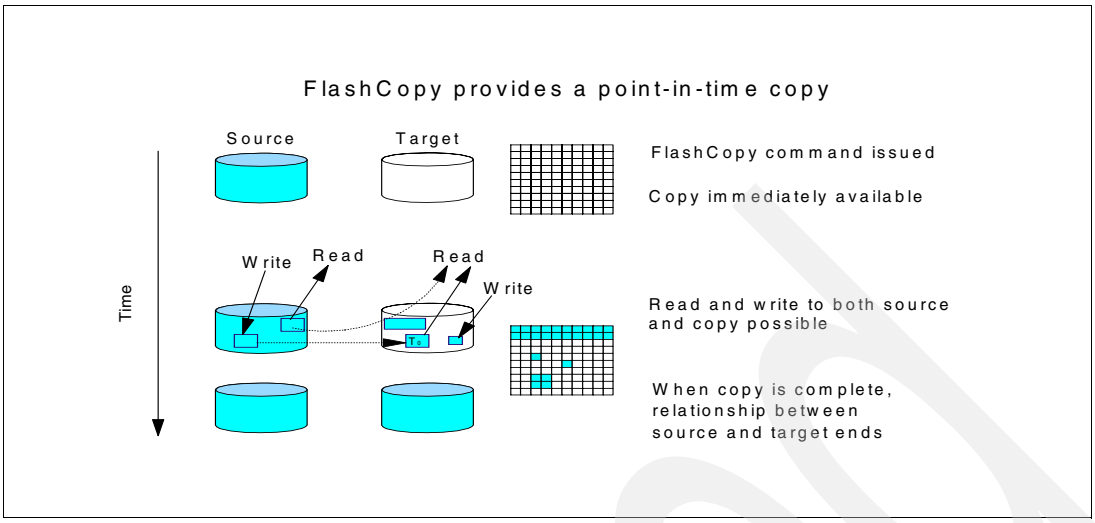


Figure 1-2 FlashCopy concepts

1.2.6 IBM incremental FlashCopy

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 entire content of the volume.

1.3 Volume Shadow Copy Service

The Volume Shadow Copy (VSS) service provided with Microsoft Windows Server 2003 is an enhanced Storage Management feature that provides a framework and an API that enables the creation of consistent point-in-time copies of data known as *shadow copies*.

The VSS service enables the interoperability of third-party storage management programs, business programs, and hardware providers in order to create and manage shadow copies.

Several features in 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

The shadow copy creation can be performed using two distinct snapshot methods:

- full copy
- differential copy (copy-on-write)

The full copy is usually achieved using a hardware provider (see “Provider” on page 8).

1.3.2 The VSS model

VSS is designed to address problems associated with traditional backup methods (such as inaccessible files during a backup and inconsistent file state during backup), and minimize interruptions to production servers during backup, as described here.

The shadow mechanism

- 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 since 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 Exchange) 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 which is writing to the disk is also responsible for bringing all associated files into a consistent state, before creating the shadow copy.

Minimizes application downtime

Creating a shadow copy typically takes about seconds or minutes, depending on the VSS provider. The application is only paused 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 gives the opportunity for individual hardware vendors to add and manage unique features for its 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 will be created with the same time stamp and will present the same disk state.

Native shadow copy support

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

1.3.3 The VSS architecture

The VSS framework coordinates the communication between VSS requestors, VSS writers, and VSS providers.

Figure 1-3 illustrates the VSS architecture.

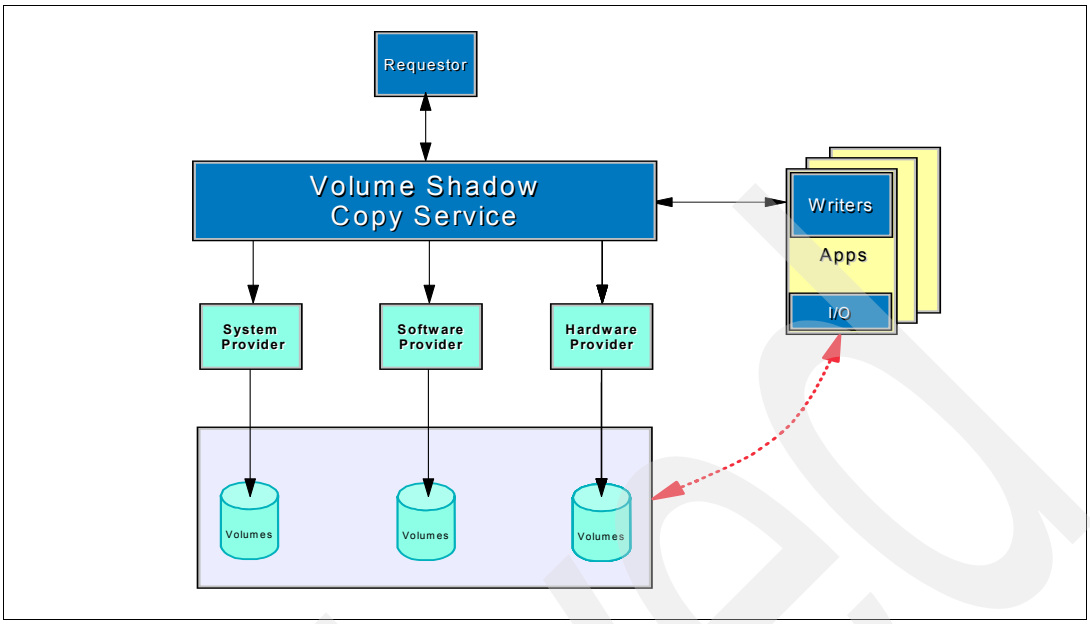


Figure 1-3 VSS architecture

Requestor

The *requestor* is a management application that invokes VSS in order to create and manage shadow copy sets of one or more volumes. This role is typically used to implement other functionalities like 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 Exchange 2003 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 their 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 the *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 like the DS6000/ DS8000/SVC, or SnapDrive on NetApp 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, since 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 Exchange server. If you are using the Windows system software provider, this uses copy-on-write. Therefore, there is significant performance overhead to using a software provider.

However, you should balance this against the ease of setup - using a hardware provider requires more initial configuration than a software provider. We provide additional guidance for selecting which provider to use in “VSS provider” on page 12.

The Volume Shadow Copy Service 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 will be used, if available. If there is no other provider, then the Microsoft system software provider will be 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 which 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 How shadow copies are created

Figure 1-4 on page 9 illustrates the steps in creating a shadow copy.

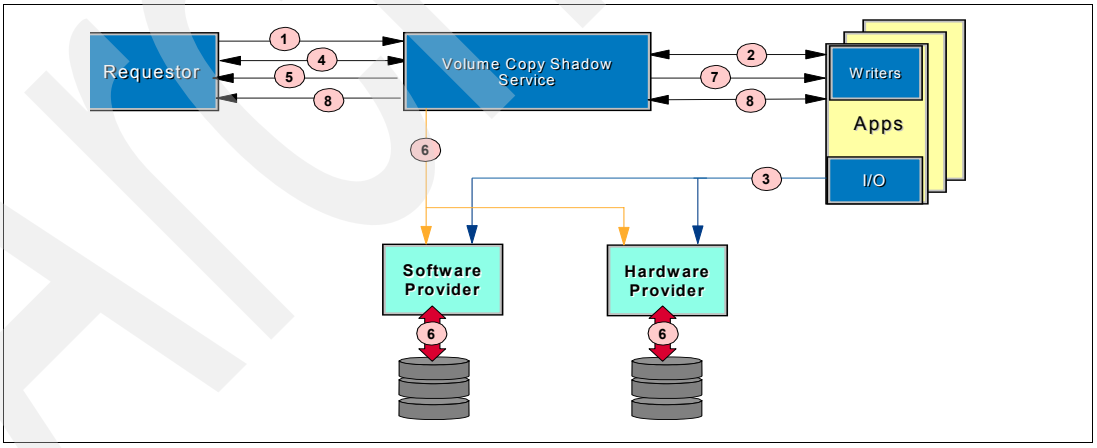


Figure 1-4 Shadow copy creation process

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 it can now complete all queued write I/Os, since 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

There are three types of VSS shadow copy which 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 will be deleted after the backup operation is complete. It is also known as an auto-release shadow copy. 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 which initiated the shadow copy, and mounted onto another server. Transportable shadow copies require use of a VSS hardware provider and enable the offloaded backup function.

1.4 The Microsoft Virtual Disk Service

Microsoft Virtual Disk Service (VDS) was introduced in the Windows 2003 Server 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 in order to translate the general purpose VDS APIs into their specific hardware instructions.

VDS is part of Microsoft’s 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 their specific hardware.

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

Figure 1-5 on page 11 illustrates the Virtual Disk Service architecture.

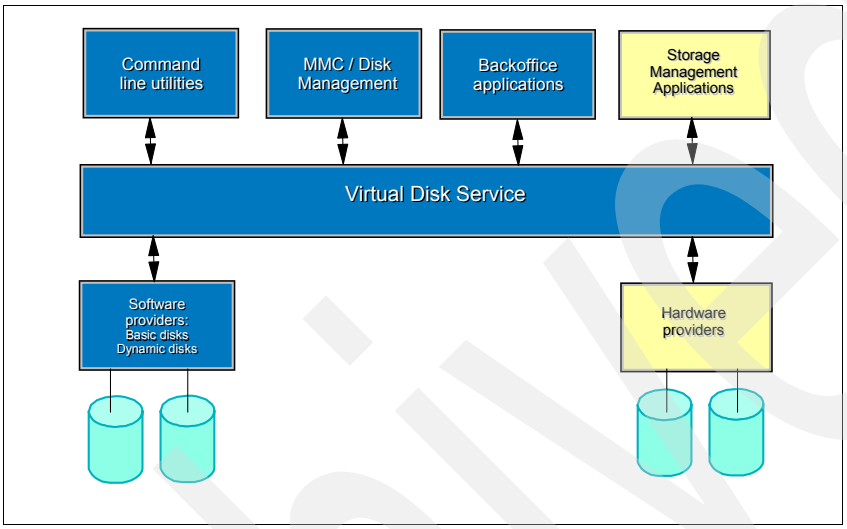


Figure 1-5 VDS architecture

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

1.5 VSS with Tivoli Storage Manager

Tivoli Storage Manager can perform VSS backup of Exchange databases using Tivoli Storage Manager for Mail Data Protection for Exchange together with Tivoli Storage Manager for Copy Services and the Tivoli Storage Manager backup/archive client. We refer to this entire combined solution generically as Data Protection for Exchange, with the understanding that VSS backup requires the additional module Tivoli Storage Manager for Copy Services.

1.5.1 Integration of Data Protection for Exchange with VSS

In a Data Protection for Exchange solution, the three required VSS components (as described in 1.3.3, “The VSS architecture” on page 7) are as follows:

VSS writer

The Microsoft Exchange Server is the VSS writer. It is installed with the Exchange Server 2003 software and requires no special configuration to perform VSS operations.

VSS requestor

The Tivoli Storage Manager backup-archive client is the VSS requestor. The requestor communicates with VSS to access the Exchange data. Data Protection for Exchange serves as the front end for VSS backup; that is, is the user interface for initiating backup and restore operations; however it communicates with the backup-archive client as VSS requestor to actually perform the backup and restore.

VSS provider

The VSS provider manages the volumes where the Exchange 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 Exchange. You will need to configure the provider according to the vendor's specific instructions.

Configuration requirements depend on the type of VSS provider that you use. Some VSS providers are more complex to set up initially, but subsequently provide more powerful functionality and can also decrease the overhead on the Exchange server.

You can choose which VSS provider meets your needs for Exchange backup; here are some guidelines:

- If you are using the standard Windows system provider, very little initial configuration is required. This is the quickest and simplest way to set up Data Protection for Exchange for VSS backups. However, the copy-on-write snapshots are then maintained within the production Exchange server, which will impose an additional overhead. You also cannot perform offloaded backups with this configuration.
- If your Exchange storage is configured on a disk storage system and you plan to perform offloaded backups or full-copy snapshot backups (versus copy-on-write snapshot backups), then a VSS hardware provider specifically designed for that disk system is required.

  Our examples in this publication use the IBM hardware provider (for the IBM System Storage SAN Volume Controller, IBM System Storage DS6000™, and IBM System Storage DS8000™); however, any disk system with a Microsoft-compliant VSS hardware provider designed for it should work. The operation of Data Protection for Exchange VSS backups is essentially identical, regardless of the provider used.
- Using a VSS hardware provider may increase the complexity of the initial setup. On the upside, doing so means that the storage system itself performs the data movement to create snapshots, and also incurs the overhead of maintaining the snapshots, which frees the Exchange production server from this task.

  Furthermore, if you use a VSS hardware provider that supports transportable shadow copies, you can then offload the Tivoli Storage Manager backup workload to another server - in this case, you will have to configure and manage another server for this function.
- If you want to perform VSS Instant Restores, be aware that at the time of writing, this function is supported only with the IBM System Storage SAN Volume Controller (SVC). You must install and configure IBM TotalStorage Support for Microsoft Virtual Disk and Volume Shadow Copy Services as your VSS hardware provider in order to perform VSS Instant Restores, and also configure your Exchange server so that the database and log files are on SVC devices.

1.5.2 Types of Exchange backup

Data Protection for Exchange provides the following five types of backup which can be started either via the command line or the GUI. Some types can be performed only using

legacy backup methods, while some can be performed using either legacy or VSS backup methods. We indicate this for each type. Remember that for a VSS backup, Tivoli Storage Manager for Copy Services is required, together with Data Protection for Exchange and the Tivoli Storage Manager backup/archive client.

Full backup (legacy and VSS)

A full backup backs up the specified storage group(s) as well as associated transaction logs. After the Storage Group and log backups complete, Data Protection for Exchange notifies the Exchange Server that the backup has succeeded, and that the logs can be safely deleted.

Incremental backup (legacy only)

An incremental backup only backs up transaction logs, and then deletes them. These log files are not deleted if the backup fails. To restore an Exchange Server storage group from an incremental backup, the following steps are required:

1. Restore the last full backup.
2. Restore any other incremental backups performed between the full backup and this incremental backup.
3. Restore this incremental backup.

Differential backup (legacy only)

A differential backup only backs up transaction logs, but does not delete them. If you perform a full backup and then perform only differential backups, the last full backup plus the latest differential backup has all the data needed to bring the storage group back to the most recent state. This type of backup is also called a *cumulative incremental backup*. To restore an Exchange Server storage group from a differential backup, the following steps are required:

1. Restore the last full backup.
2. Restore this differential backup, but no other differential backups.

Copy backup (legacy and VSS)

A copy backup is similar to a full backup except that transaction log files are not deleted after the backup. A copy backup is used to make a full backup of the Exchange Server storage group(s) without disrupting any backup series which is using incremental or differential backups.

Database copy backup (legacy only)

A database copy backup is a special type that backs up only the specified database as well as its associated transaction logs. The transaction log files are not deleted after the backup. A database copy backup is used to make a special full backup of the database without disrupting any backup series which is using incremental or differential backups.

Note: When circular logging is enabled, you cannot use differential or incremental backups. This is because data loss could occur if the log wrapped before an incremental or differential backup is done. If you choose a backup strategy that involves incremental or differential backups, you must disable circular logging for the Exchange storage group from the Exchange Administrator program.

Similarly, if you will use VSS backups, Microsoft recommends turning off circular logging. For more information about circular logging, refer to the appropriate Microsoft Exchange documentation, and in particular, to the following:

http://www.microsoft.com/technet/prodtechnol/exchange/2003/vssbp.mspx

1.5.3 Backup methods

We distinguish between two methods for backups: legacy and VSS.

Legacy backup

A *legacy backup* is a specialized API backup that functions with the Exchange server storage engine. This is the type of backup provided by previous releases of Data Protection for Exchange. The following characteristics are true of legacy backups:

- Full, copy, incremental, differential, and database copy backup types are supported.
- Backup granularity is at the database and storage group level.
- Backups are stored on Tivoli Storage Manager server storage.
- Backups are managed through Tivoli Storage Manager server policy.
- Backups can be performed in a Microsoft Cluster Server (MSCS) environment.
- Backups provide Exchange Server database zeroing functionality to make unused or deleted data from databases unreadable.
- Backups provide Exchange Server database integrity check functionality.
- Backup and restore of SRS and KMS databases is supported.

VSS backup

A VSS backup uses Microsoft VSS technology to produce an online snapshot (point-in-time consistent copy) of Exchange data, to local shadow volumes. In Data Protection for Exchange terms, this is known as *backup to local*. This type of backup means the Exchange server is in backup mode (with write I/Os suspended) for only a short period of time because the length of time to perform the snapshot is usually measured in seconds or minutes (depending on the VSS provider), rather than hours.

In addition, a VSS backup allows a snapshot of large amounts of data at one time since the snapshot works at the disk volume level. VSS backups require Tivoli Storage Manager for Copy Services to be installed, in addition to Data Protection for Exchange and the Tivoli Storage Manager backup/archive client.

VSS backups (Tivoli Storage Manager for Copy Services) are only available on Exchange Server 2003 and Windows Server 2003.

After the snapshot is complete, it can be accessed directly through standard operating system functions or other applications. One application of this is to back up and manage the VSS snapshot on an external storage manager (for example, Tivoli Storage Manager). This is known as Data Protection for Exchange *backup to Tivoli Storage Manager*. When this function is selected, then after the snapshot is made, Tivoli Storage Manager is automatically invoked to store the snapshot.

The advantage of VSS backup, rather than a legacy backup as previously discussed, is that the Exchange database is only impacted for a short time to make the snapshot, while still being able to make a full backup to external storage media (for example, tape).

In this way, we can establish two uses for VSS backup: as a backup in itself, so that multiple shadow copy generations can potentially be kept online for rapid restore (*backup to local*), and as a means for extra backup to an external media (*backup to 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 Exchange VSS backup is started, you must specify the backup destination: to local, Tivoli Storage Manager, or both.

The following characteristics are true of VSS backup:

- Full and copy backup types are supported. Incremental, differential, and database copy backup types are *not* supported.
- Backup granularity is at the storage group level only.
- Backups are managed through Tivoli Storage Manager server policy.
- Backups can be stored on local shadow volumes, Tivoli Storage Manager server storage, or both locations using the backup destination as LOCAL, TSM or BOTH, respectively.
- Different policy can also be defined for each storage destination, backup type, and Storage Group.
- Backups to Tivoli Storage Manager server storage can be offloaded to an alternate machine to minimize the impact on production servers. This is possible if a VSS hardware provider which supports transportable shadow copies is used.
- Backups can be performed in a Microsoft Cluster Server (MSCS) environment.
- Backups do not provide Exchange Server database zeroing functionality.
- Backups provide Exchange Server database integrity check functionality.
- Backup and restore of SRS and KMS are not supported.

1.5.4 Restore methods

Similarly, there are two types of restores: legacy and VSS. These are associated with the same type of backup; that is, a legacy backup is restored with a legacy restore, and a VSS backup is restored with a VSS restore. For VSS restore, there are three restore types: VSS restore, VSS fast restore, and VSS Instant Restore.

After a restore of Exchange data, the transaction logs must still be replayed after the restore. The application is not online until the recovery logs are replayed - this is handled automatically by Tivoli Storage Manager.

Note: You cannot mix legacy and VSS restores together.

Legacy restore

A legacy restore is the type of restore provided by previous releases of Data Protection for Exchange. It restores legacy backups (Exchange database files and log files) from Tivoli Storage Manager server storage to their original location. Like a legacy backup, it uses a specialized API restore that functions with the Exchange server storage engine.

VSS restore

A VSS restore restores a VSS backup (of Exchange database files and log files) residing on Tivoli Storage Manager server storage to their original location. The restore is done at a file level. The following characteristics are true of VSS restores:

- Full and copy backup types can be restored. Incremental, differential, and database copy backup types are not supported by VSS and therefore, *cannot* be restored.
- Restore granularity is at the database level.
- A VSS restore can restore one (or more) Storage Groups from a VSS snapshot backup located on Tivoli Storage Manager server 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) environment.
- Due to a Microsoft limitation, Recovery Storage Group (RSG) restores and restores of SRS and KMS backups are not supported.

VSS fast restore

A VSS fast restore restores VSS backups residing on local shadow volumes. The restore is done at a file level. The following characteristics are true of VSS fast restores:

- Full and copy backup types can be restored. Incremental, differential, and database copy backup types are not supported by VSS and therefore *cannot* be restored.
- Restore granularity is at the database level.
- Because the restore is from a locally accessible disk (shadow volumes), it may be faster than a network restore from a backup server.
- A VSS fast restore can restore one (or more) Storage Groups from a VSS snapshot backup located on Tivoli Storage Manager server 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) environment.
- Due to a Microsoft limitation, Recovery Storage Group (RSG) restores and restores of SRS and KMS backups are not supported.

VSS Instant Restore

In a VSS Instant Restore, the target volumes (containing a valid VSS snapshot) are copied back to the original source volumes using *hardware-assisted volume-level copy mechanisms* (such as FlashCopy). This is distinct from the file-level restore, which is performed by VSS restore and VSS fast restore.

With a VSS Instant Restore on a SAN Volume Controller, the Exchange application can return to normal operations shortly after the hardware-assisted volume-level copy is initiated; that is, in a similar time frame to which the original snapshot was created. The actual background copy of the data from target to source continues in background, but because of the virtualization, access to the original source volume is almost immediate.

Of course, as with all Exchange restores, the transaction logs must still be replayed, so you need to also consider the overall recovery time. But in the case of an Instant Restore on SVC, the log replay can start much sooner, because the logs can be applied to the source volume while the background copy is proceeding.

Note the following considerations for VSS Instant Restore:

- Requirements
  - IBM TotalStorage Support for Microsoft Volume Shadow Copy Service
  - Tivoli Storage Manager for Copy Services Microsoft Exchange VSS Integration Snapshot Integration Modules
- At the time of writing, it is supported only on IBM System Storage SAN Volume Controller.
- Backups must be restored to the same storage system as they resided on.
- It can restore one (or more) Storage Groups from a VSS snapshot backup located on Tivoli Storage Manager server 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) environment.
- Due to a Microsoft limitation, Recovery Storage Group (RSG) restores and restores of SRS and KMS backups are not supported.
- Carefully plan the layout of Storage Groups and log files; an Instant Restore will overwrite a complete volume (or volumes).

1.5.5 Shadow copy types with Data Protection for Exchange

The three types of shadow copy were introduced in 1.3.5, “Shadow copy types” on page 10. Here is how they relate to a Data Protection for Exchange configuration.

Persistent shadow copy

A persistent shadow copy is made when the VSS backup destination is LOCAL (*backup to local*). These copies are kept subject to Tivoli Storage Manager expiration management.

Non-persistent shadow copy

A non-persistent shadow copy is made when the VSS backup destination is TSM (*backup to Tivoli Storage Manager*). These shadow copies are used temporarily and deleted after the backup process is complete.

Transportable shadow copy

A transportable shadow copy is used with Tivoli Storage Manager for Copy Services to allow the snapshot to be backed up by another server. This technique is known as an *offloaded backup*, because the snapshot is transported from the Exchange server to the offloaded server.

2

Pre-installation and planning

This chapter gives you an overview of what is required before implementing IBM Tivoli Storage Manager for Copy Services. We discuss the following topics:

- Environment requirements
- Overview of Volume Shadow Copy Service and legacy backups
- Backup strategy
- Using VSS and legacy backups
- How Tivoli Storage Manager Server manages Volume Shadow Copy Service backups
- Microsoft Cluster Server (MSCS) support
- Volume Shadow Copy Service client for Tivoli Storage Manager

2.1 Environment requirements

This section describes the minimum hardware, software and operating system information required for the proper installation of Tivoli Storage Manager for Copy Services that integrates with the Data Protection for Exchange.

2.1.1 IBM Tivoli Storage Manager for Copy Services

Before installing Tivoli Storage Manager for Copy Services on a Microsoft Exchange server, you must be sure that your system meets the following requirements:

Hardware requirements

- 11 MB of free disk space
- 48 MB of RAM (96 MB or higher is highly recommended)
- Intel® Pentium® or equivalent 166 (higher) processor
- Disk system with a Microsoft-compliant VSS provider. If you want to perform offloaded backups, the VSS provider must also support transportable VSS shadow copies. Verify with your disk vendor that the VSS provider is suitable.

Data Protection for Exchange Volume Shadow Copy Services operations are available on any hardware platform that supports Microsoft VSS requirements. The following list identifies some hardware and software storage systems that have been tested with Data Protection for Exchange Volume Shadow Copy Services operations. This list is not intended to be an exclusive list of the disk hardware which can be used.

- IBM System Storage DS6000 and a machine with a processor supported by DS6000 with IBM Common Interface Model (CIM) Agent for DS Open API.
- IBM System Storage DS8000 and a machine with a processor supported by DS8000 with IBM Common Interface Model (CIM) Agent for DS Open API.
- NetApp Fas270 fabric-attached storage (FAS) system with NetApp SnapDrive Version 3.2 (or later).
- IBM System Storage N series with SnapDrive support for Microsoft Volume Shadow Services
- IBM System Storage SAN Volume Controller V 2.1.x (or later)
- Microsoft Windows System Provider (which is a VSS Software Provider)
- IBM System Storage DS4000™ with Engenio Microsoft VSS/VDS provider

Contact your disk storage vendor for exact details of their support for Volume Shadow Copy Services operations.

For the latest information about supported environments for Tivoli Storage Manager for Mail Data Protection for Microsoft Exchange, which is a prerequisite for Tivoli Storage Manager for Copy Services, refer to the following site:

http://www.ibm.com/support/docview.wss?rs=669&context=SSTG2D&uid=swg21233936&loc=en_US&cs=utf-8&lang=en

For the latest information about supported environments for Tivoli Storage Manager for Copy Services, refer to the following site:

http://www.ibm.com/support/docview.wss?rs=3042&context=SSRURH&uid=swg21231465

In all cases, consult this Web site plus any README files distributed with the installation media to determine the latest supported environments.

Software and operating systems requirements

Tivoli Storage Manager for Copy Services requires the levels of Tivoli Storage Manager to be installed which are shown in Table 2-1. The table is divided into two columns. If you plan to run your backups from the Exchange server itself, you need only look at the first column. If you want to run offloaded backups, where a second server performs the backups to Tivoli Storage Manager, then you must *also* install this second server with the software listed in column 2. Your hardware VSS provider must also support transportable shadow copies if you want to use offloaded backups.

Tip: If you are using Tivoli Storage Manager for Copy Services in a MSCS clustered environment, all servers in the cluster require the same levels of Windows, Tivoli Storage Manager and other software.

Table 2-1 Software and operating system requirements

Primary Exchange server	Secondary server (OFFLOAD server)
Tivoli Storage Manager Backup-Archive Client V5.3.4.6 (or later; refer to IBM Technote 1240684) http://www.ibm.com/support/docview.wss?uid=swg21240684	Tivoli Storage Manager Backup-Archive Client V5.3.4.6 (or later; refer to IBM Technote 1240684) http://www.ibm.com/support/docview.wss?uid=swg21240684
Tivoli Storage Manager API V5.3.3 (or later	Tivoli Storage Manager API V5.3.3 (or later)
Tivoli Storage Manager for Mail - Data Protection for Microsoft Exchange Server - V5.3.3 (or later)	Microsoft Exchange Server Management Tools
Tivoli Storage Manager for Copy Services - Microsoft Exchange VSS Integration Module V5.3.3 (or later)	
Tivoli Storage Manager for Copy Services - Hardware Devices Snapshot Integration Module V5.3.4 (or later) - only required if Instant Restore function will be used, which is currently only available for SAN Volume Controller	

Table 2-2 on page 22 maps the levels of Microsoft Windows and Exchange to the various functions provided by Data Protection for Exchange and Tivoli Storage Manager for Copy Services. Note that Windows 2000 is only supported for non-VSS (that is, legacy) backups. For any VSS snapshot operations, Windows 2003 is required. Contact your disk vendor for exact details of their support for Volume Shadow Copy Services.

Important: Microsoft patches required

- Apply all latest Microsoft Hotfixes for Exchange, Windows 2003 or IBM patches for Tivoli Storage Manager Client Software.
- At the time of writing, Microsoft Hotfix KB913648 is required.
- If using dynamic disks, apply KB911062 (however, you cannot use dynamic disks in an Exchange MSCS environment).
- If you experience VSS operation timeouts or failures, particularly with large Storage Groups, apply Microsoft Hotfix KB915331.
- If you are performing Instant Restore in a clustered environment, KB903650 is also required at this time.
- In a clustered environment, KB898790 is required. KB 903650 is also required in a clustered environment if *only* if using Instant Restore.
- KB912944 and KB916048 are required *only* if using the Storport storage driver.

Check the support URLs and READMEs to confirm the latest Hotfix requirements.

Table 2-2 Windows and Exchange levels

Feature	Operating system	Exchange server	VSS provider	Tivoli Storage Manager for Copy Services
Legacy Backup and Restore	Microsoft Windows 2000 [1] Microsoft Windows 2000 [1] or 2003 [2]	Exchange 2000 Server [3] Exchange Server 2003 [4]	None None	None None
Basic VSS Support	Microsoft Windows 2003 [2]	Exchange Server 2003 [4]	Any VSS Provider that is supported by Microsoft rules for VSS providers	Microsoft Exchange VSS Integration Module Version 5.3.3
VSS Offloaded Backup	Microsoft Windows 2003 [2]	Exchange Server 2003 [4]	Any VSS Provider that supports transportable shadow copies [5]	Microsoft Exchange VSS Integration Module Version 5.3.3
VSS Instant Restore	Microsoft Windows 2003 [2]	Exchange Server 2003 [4]	IBM System Storage SAN Volume Controller Version 2.1x (or later) [6] IBM TotalStorage VSS Hardware Provider 2.4.3 (or later)	Microsoft Exchange VSS Integration Module Version 5.3.3 Hardware Devices Snapshot Integration Module Version 5.3.4

[1] Windows 2000 Server, Advanced Server, or Datacenter Server. All versions must be at Service Pack 4 (or later).

[2] Windows Server 2003 32- bit Standard Edition, Enterprise Edition, or Datacenter Edition. All versions must be at Service Pack 1 (or later).

[3] Exchange 2000 Server must be at Service Pack 3 (or later). Microsoft Cluster Services support is available.

[4] Exchange Server 2003 must be at Service Pack 1 (or later). Microsoft Cluster Services support is available and you must install the latest HOTFIX by Microsoft (KB903650) for Cluster setups.

[5] The Volume Shadow Copy Services hardware provider must be installed on both servers that are involved in an off-load backup.

[6] IBM Subsystem Device Driver (SDD) 1.6.0.2 with Host Attachment Scripts 1.1.0.3 or (later) is required.

Note: If you will perform VSS backups, Exchange should be installed only on Windows basic disks.

2.1.2 Tivoli Storage Manager for Copy Services components

There are two installable modules included in the package Tivoli Storage Manager for Copy Services. Once installed, these modules enable certain menu options in the Data Protection for Exchange GUI which are otherwise grayed out. These modules, Microsoft Exchange VSS Integration Module and Hardware Devices Snapshot Integration Module, are described in more detail here.

Microsoft Exchange VSS Integration Module

This component is used with IBM Tivoli Storage Manager for Mail Data Protection for Exchange, and enables the use of Microsoft VSS technology to produce an online snapshot of the Exchange data that can be stored on local shadow volumes or on the Tivoli Storage Manager server storage. A license file (acsexc.lic) is installed in the directory c:\program files\tivoli\tsm\TDPexchange which will allow the use of IBM Tivoli Storage Manager for Copy Services.

This module is required for all VSS operations with Data Protection for Exchange.

Hardware Devices Snapshot Integration Module

This component is used with IBM Tivoli Storage Manager for Mail Data Protection for Exchange. It contains two .dll files (pisnaphdw.dll and pihdw.dll) and two license files (aschdw.lic and acssnp.lic), which are installed in the c:\program files\tivoli\tsm\baclient\plugins directory.

This module is only required to perform a VSS Instant Restore. At the time of writing, VSS Instant Restore is only available for SVC.

2.1.3 Storage layout considerations for Microsoft Exchange

When configuring your Exchange environment, each Exchange Storage Group should be on its own dedicated LUN or set of LUNs, with the associated logs on another dedicated LUN. That is, database files for each Storage Group should be placed on their own dedicated

logical volume, and the associated logs for each Storage Group on another logical volume. Placing other data on these volumes can inhibit Exchange Server performance and also cause problems if you plan to use VSS Instant Restore.

Do not place multiple volumes on the same LUN. Microsoft recommends that you configure a single volume/single partition/single LUN as 1 to 1 to 1.

If you intend to perform VSS Instant Restore on a single database, then it must be placed into its own Storage Group. Attempting to perform a “partial” restore (that is, a restore of only a subset of databases in a Storage Group) will either fail or have undesirable side effects. You can only perform an Instant Restore of *all* the databases in a Storage Group.

2.2 Overview of VSS and legacy backups

In this IBM Redbook, we differentiate between the type of backups which have always been available with Data Protection for Exchange (which we will refer to as legacy backups), and VSS-type backups.

Note: If using a specialized VSS provider, take time to understand the requirements of that specific VSS provider and how that might affect provisioning of storage, as well as Exchange database file and log file locations.

2.2.1 Legacy backup overview

To back up the Exchange database files and log files, legacy backups use the TCP/IP network or SAN (LAN-free) option. The database is backed up to Tivoli Storage Manager directly from the disks used by Exchange; this increases the workload on the Exchange server.

A *legacy backup* is an API backup that functions with the Exchange server. These types of backups are provided by all previous releases of Data Protection for Exchange. A legacy backup creates copies of the Exchange database files and log files. The Exchange Databases *must* be online in order for this type of backup to succeed. Data Protection for Exchange supports FULL, COPY, INCREMENTAL, DIFFERENTIAL, and DBCOPY legacy backups.

Data Protection for Exchange performs the following steps when creating a legacy backup:

1. It starts a session with the Tivoli Storage Manager Server.
2. It notifies the Exchange server that a backup is ready to begin.
3. It sends data from the Exchange Server to the Tivoli Storage Manager server via LAN or SAN.
4. It notifies the Exchange Server that a backup is complete.
5. It ends the session with the Tivoli Storage Manager server.

Using legacy function provides backup and restore functions for the Exchange Storage Groups and associated transaction logs.

2.2.2 VSS backup overview

A VSS backup makes a consistent copy of the volume(s) by using a VSS provider. The snapshot can be maintained as an entity on disk, and it can also be optionally backed up to

Tivoli Storage Manager. Since the time taken to make the snapshot copy is short, this minimizes the impact to the production database. You can optionally use a second server to back up the snapshot copy to Tivoli Storage Manager; this is known as an *offloaded backup*. When the backup is offloaded, there is even less performance overhead on the Exchange server.

Data Protection for Exchange VSS backups and restores are initiated via the Data Protection for Exchange interface. The underlying implementation uses the Tivoli Storage Manager backup-archive client, specifically the remote client agent service, DSMAgent, to communicate with VSS. The DSMAgent is the actual VSS requester which communicates with VSS to coordinate with the Exchange Server (VSS writer) and the owner of the volumes (VSS provider) to create a consistent snapshot of the volumes where the Exchange database and log files reside.

When using VSS backup, you specify one of these three options as the backup destination:

LOCAL This creates a persistent shadow copy (snapshot).

TSM This creates a non-persistent shadow copy which is backed up to Tivoli Storage Manager. The non-persistent shadow copy is deleted after the backup is successfully sent to the Tivoli Storage Manager server.

BOTH This creates a persistent snapshot (that is, it remains as a disk-based snapshot) which is also sent to Tivoli Storage Manager.

Important: Recovery Storage Group (RSG) restores from VSS snapshot backups are not supported by Microsoft.

Backup and Restore of Site Replication Service (SRS) and Key Management Service (KMS) are not supported with VSS; this is due to a Microsoft limitation.

Certification Authority backup: If you need to back up or restore the Certification Authority (CA), you must back up the System State. You can use the Tivoli Storage Manager backup/archive client to do this.

For more information about backup and restore of CA services, see:

`http://www.microsoft.com/technet/prodtechnol/exchange/guides/DROpsGuide`

Data Protection for Exchange serves as a front end for VSS operations; it performs the following actions when a VSS backup operation is initiated:

1. It validates the state of the Exchange server objects.
2. It starts a session with a Tivoli Storage Manager server; communications are opened with the DSMAgent.
3. The DSMAgent verifies that the VSS service is running and that the Exchange server is available.
4. The DSMAgent on the Exchange server lists the backup components through the VSS Writer
5. The DSMAgent performs the VSS snapshot backup preparation.
6. The DSMAgent performs the VSS snapshot.

7. The DSMAgent performs a consistency/integrity check on the VSS backup. If offloaded backup is selected, then the offloaded backup server performs the consistency/integrity check.
8. If the backup destination is LOCAL, the DSMAgent sends metadata to the Tivoli Storage Manager Server. If the backup destination is TSM, the DSMAgent either on the Exchange server or on the offloaded server backs up the data and metadata to the Tivoli Storage Manager server.
9. The DSMAgent marks this backup as “complete” in VSS.
10. The session on the Tivoli Storage Manager server ends.

When performing VSS backup, options such as LANFREE or encryption and compression of the data must be defined in the backup-archive client option file (dsm.opt), not in the Data Protection for Exchange option file. This is because, as previously stated, the backup-archive client performs the role of VSS requestor.

If you are only performing legacy backups, then these options are defined in Data Protection for Exchange’s dsm.opt file. Only full and copy backups are provided when using the VSS backup option.

Note: To use the VSS backup option, you must install the Tivoli Storage Manager for Copy Services Exchange VSS Integration Module.

2.3 Legacy and VSS backup and restore methods

This section describes the various techniques available for Exchange backups and restores.

2.3.1 Legacy backups

Here are some general techniques used with legacy backups.

Full legacy backups

For relatively small databases, consider using full legacy backups because they back up all the data needed (storage group and transaction logs) for restoring the entire storage group. The log files are deleted after a successful full backup.

However, this type of backup imposes a workload on the Exchange server. Over time, as the Exchange database gets larger, this type of backup will take longer to complete, but the restore process is most efficient because only the most recent (or other, if appropriate) full backup needs to be restored. Figure 2-1 on page 27 shows a legacy backup configuration for a clustered Exchange server to Tivoli Storage Manager.

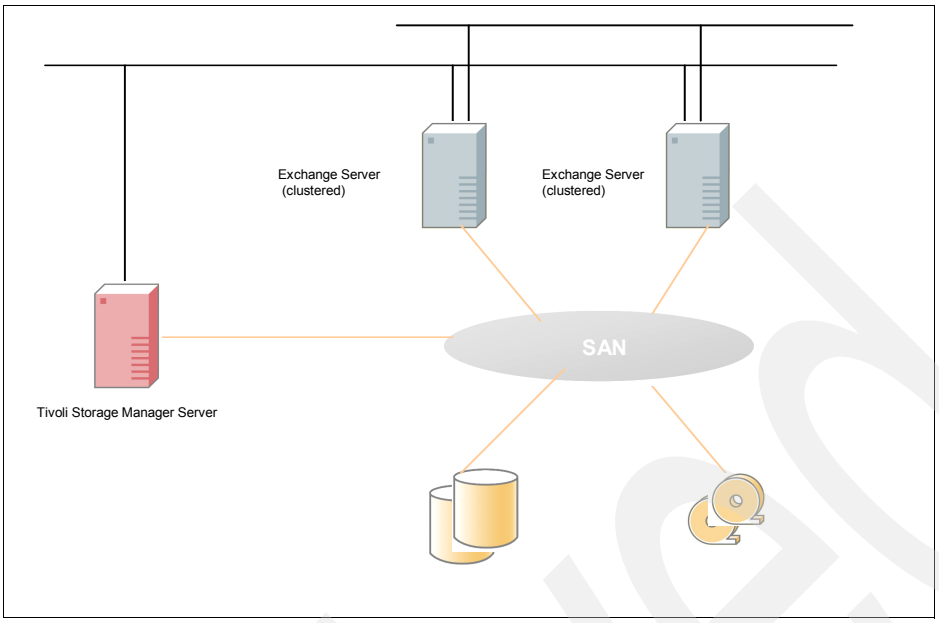


Figure 2-1 Legacy backup configuration for clustered environment

Legacy full plus incremental backups

This backup strategy is commonly used when the normal backup window or network bandwidth cannot support a full backup each time. Typically a full backup is done at time when the Exchange server or network is less utilized (for example, on weekends), and the backup window is larger. Incremental backups (which back up only the transaction logs) are then performed regularly (usually daily) during the week. The transaction logs are deleted after successful backup.

Compared with full backup only, the restore process is more complex because a full backup, as well as subsequent incremental backups, must be restored. To help improve restore time, consider using a collocated storage pool for Exchange backups. In addition, transactions within the logs must be applied, which will increase the recovery time; the more transactions there are to apply, the longer the recovery process will take.

Legacy full plus differential backups

This is similar to full plus incremental, except that the daily backups are differential. A *differential backup* backs up the transaction logs, but does not delete them, since the next differential backup will include all the logs from the previous backup, plus the latest transactions. Therefore differential backup is also known as *cumulative incremental backup*.

This strategy provides a simpler restore than the full plus incremental backup, since only the latest differential backup needs to be restored after the full. However, the same amount of data must be transferred in the differential image as in the series of incremental backups, so the restore will not take significantly less time. The full plus differential approach is recommended if the backup window and network bandwidth can handle the backup of all transaction logs that accumulate between full backups, since each differential backup takes progressively longer. Compared with full plus incremental, this strategy uses more network traffic and Tivoli Storage Manager storage resources, assuming the same frequency of differential and incremental backups.

Legacy copy backups

A legacy copy backup saves a copy of the Exchange database at a specific point in time. A copy backup is similar to a full backup, except that transaction logs are not deleted after the backup. Therefore this type of backup does not disrupt any backup procedures that use incremental or differential backups.

Legacy copy backups can also be used to create backups that you want to keep for a different retention period by binding them to a different management class. For example, you might create a legacy copy backup each month, which is retained for seven years.

2.3.2 VSS backups

Only full and copy backups types can be done via VSS. The characteristics are the same as the equivalent legacy backups, in terms of what is backed up from an Exchange perspective; however, the backup method is different. The VSS full and copy backups are made using a volume-level snapshot, as opposed to legacy backups, which are file-level.

When you make a VSS backup, you also specify a destination of LOCAL, TSM, or BOTH, as introduced in 2.2.2, “VSS backup overview” on page 24. In this section we provide more detail about these options.

VSS backup to LOCAL

VSS backup to LOCAL creates a persistent shadow copy (snapshot) of the volumes that contain the Exchange database and log files to VSS-capable disks. An integrity check is performed on the backup. The persistent shadow copy data will remain on these disks based on the specific policy settings (see 2.5.1, “Management of VSS snapshot backups in Tivoli Storage Manager” on page 34). The expiration policy process is handled by the Tivoli Storage Manager server. Note however, that the backups are still *stored* on local VSS volumes, not in the Tivoli Storage Server storage pools, so they are not protected (for example, via copy storage pools) as backups sent to Tivoli Storage Manager would be.

You can use VSS backup to LOCAL to create more frequent copies of your Exchange database than by using legacy methods, since this snapshot process takes seconds instead of potentially hours, as for legacy backups. Of course, you must make sure there is enough disk space available on the disk system to store the number of versions you will keep, according to the management class. Figure 2-2 shows a VSS LOCAL backup to disk. Note that there is still communication with the Tivoli Storage Manager server, to send metadata about the backup for validation and version control.

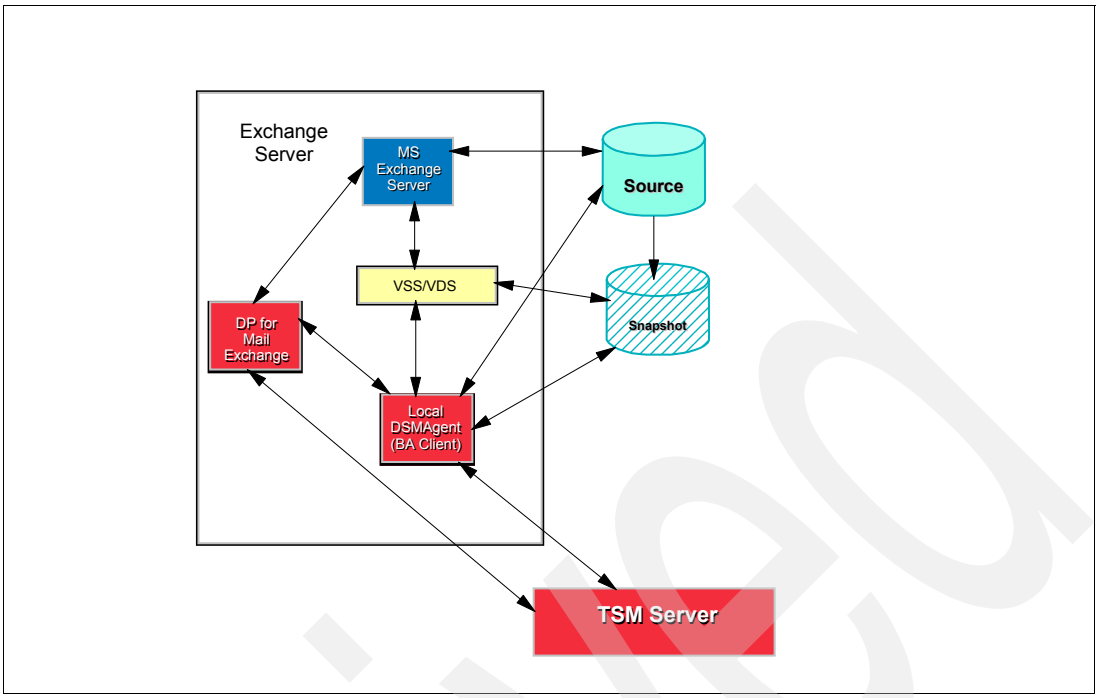


Figure 2-2 VSS backup to local

VSS backup to TSM

A VSS backup to TSM creates a non-persistent shadow copy (snapshot) of the volumes that contain the Exchange database and log files to VSS-capable disks. The snapshot is then backed up to Tivoli Storage Manager by the production server. After the backup is complete to Tivoli Storage Manager, the snapshot is deleted. The Tivoli Storage Manager backup remains in the storage pools based on your policy setting for VSS snapshots (see 2.5.1, “Management of VSS snapshot backups in Tivoli Storage Manager” on page 34).

The process for a VSS backup to Tivoli Storage Manager is as shown in Figure 2-2; the only difference is that the connection between the DSMAgent and the Tivoli Storage Manager server is for transferring the actual data for backup, as well as the metadata.

VSS backup to BOTH

When you specify backup destination BOTH, then both the previous backups are performed: a persistent snapshot backup to VSS disk, which is also sent to the Tivoli Storage Manager server.

VSS offloaded backup

In an offloaded backup, the data backup from the VSS snapshot to the Tivoli Storage Manager server (including the consistency and integrity check) is performed by another server, known as the *offloaded backup server*. The VSS snapshot operation is still performed by the production server; in this case, a transportable snapshot is made. After the snapshot is complete, the target volumes are made available to the alternate (offloaded) server so that it can do the Tivoli Storage Manager backup. This means that the production server is only impacted for the short amount of time it takes to make the snapshot.

Offloaded backup is an optional function, which is ideal for environments where the production server performance is critical and must be minimally impacted by backup. Figure 2-3 on page 30 shows the process of an offloaded backup.

Note: A server used for offloaded backup should be separate from the production Exchange server so that the backup is, in fact, offloaded. If you have a clustered Exchange environment (MSCS), the offloaded server should also not be one of the cluster nodes.

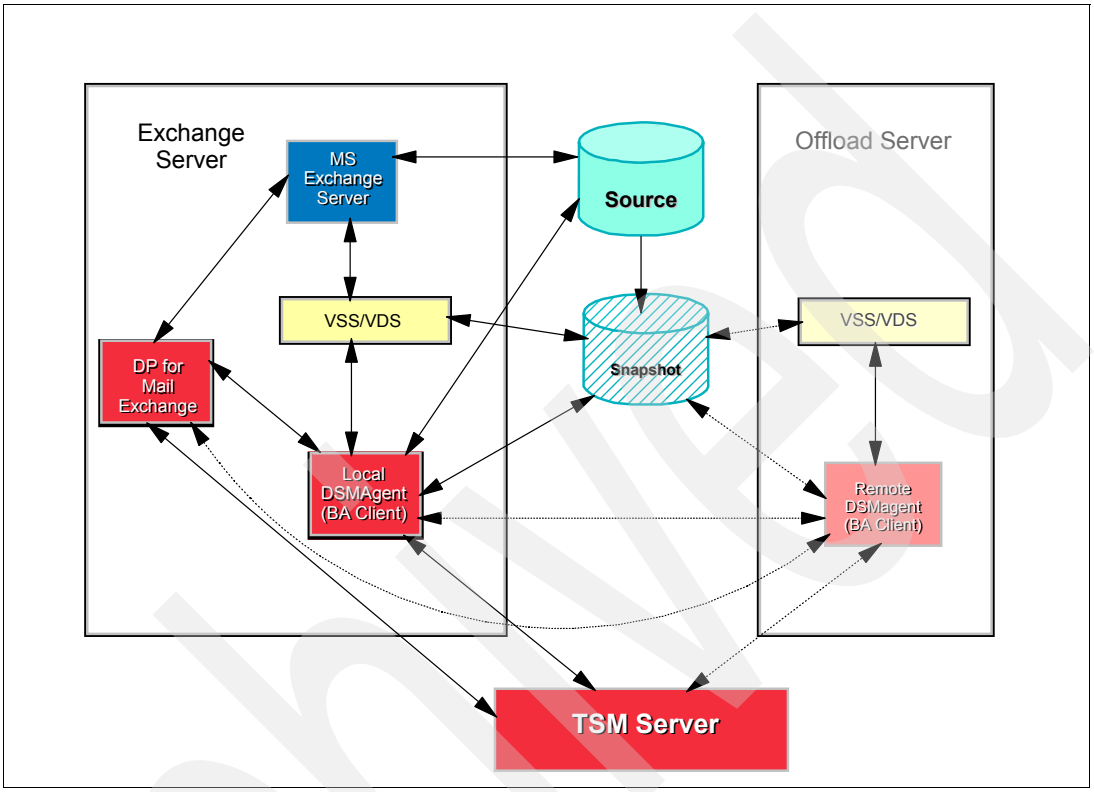


Figure 2-3 VSS offloaded backup

2.3.3 Restore processing

When a restore is initiated, backup copies of the Exchange database files and the transaction logs are returned to the Exchange server. The Exchange Information Store service must be running, but the databases being restored within the storage group must be dismounted. The Data Protection for Exchange GUI automatically dismounts the databases.

Legacy restore

When a legacy restore is initiated from the Data Protection for Exchange GUI, you are prompted to either dismount the databases or cancel the restore operation. If the restore is run from the CLI, the Exchange Administrator must first dismount the necessary databases.

Data Protection for Exchange performs the following actions to restore an Exchange database or storage group.

1. It starts a session with the Tivoli Storage Manager Server.
2. It informs the Exchange Server that a restore is about to start.
3. It restores the specified database and log files from the Tivoli Storage Manager server. The logs are restored to a temporary location as specified by the Exchange Administrator.

   When performing a restore of a mailbox database with Exchange Server 2003, if a Recovery Storage Group exists, then the mailbox database will be restored to the

Recovery Storage Group instead of the original storage group. When recovering to the Recovery Storage Group, you must specify the option to replay restored logs. This option is only valid for legacy restores. VSS restores to the Recovery Storage Group are *not* supported by Microsoft.

4. It informs the Exchange server that the restore has completed. You have the option of either starting the recovery or mounting the database (when the recovery completes).
5. It ends the Tivoli Storage Manager server session.

Depending on what backup strategy you choose, restoring an Exchange Storage Group can involve restoring multiple backup objects from the Tivoli Storage Manager server. For further details on restoring legacy backups, see *Data Protection for Microsoft Exchange Server Installation and Users Guide*, SC32-9058.

VSS restore

Only backups that are made via VSS can be restored via VSS. Therefore, incremental or differential legacy backups cannot be restored with this method, and nor can full or copy legacy backups. Because of current Microsoft restrictions, a Recovery Storage Group (RSG) restore from VSS snapshot backups is not supported. Site Replication Service (SRS) and Key Management Service (KMS) also cannot be restored with VSS. A VSS restore will be directed to the same drive letter(s) and path(s) as when the backup was run.

When you initiate a restore operation, Data Protection for Exchange performs the following actions:

1. It validates the state of the Exchange server objects.
2. Communications are opened with the DSMAgent.
3. When started with the Data Protection for Exchange GUI, it prompts to dismount the databases within the selected storage group.
4. The DSMAGENT verifies that the VSS service is running and that the Exchange server is available.
5. It verifies that the VSS service is running and that the Exchange writer (Exchange server) is available.
6. The Tivoli Storage Manager VSS Requestor (backup-archive client DSMAgent) prepares the VSS snapshot restore.
7. The DSMAgent restores the data. The restore can come from Tivoli Storage Manager storage pool (VSS restore), as a file copy from a persistent shadow copy image (VSS fast restore), or as a hardware assisted volume-level restore from a persistent shadow copy image (VSS Instant Restore). See “VSS fast restore” and “VSS Instant Restore” on page 16 for more information about these topics.
8. The DSMAgent marks the restore as complete in VSS.
9. Optionally, it mounts databases to run the recovery.

Why use VSS backup and restore

VSS backups give you the ability to reduce both the backup window and also the resources needed for a backup. The backup window is reduced because the snapshot is taken much quicker than traditional file-based methods. This necessarily reduces the resources required on the Exchange server. If you use an offloaded backup server, then the resource requirement is even further reduced.

With VSS Instant Restore (see 1.5.4, “Restore methods” on page 15), the set of target volumes is copied back to the original source volumes, using hardware-assisted volume-level

restore from a persistent shadow copy image (VSS Instant Restore). This is the fastest type of restore possible. Note that it will overwrite all data that resides on the local source volumes; any non-Exchange data on these volumes will not have been backed up, and will therefore be overwritten on restore. Therefore, install only Exchange databases and logs on the source volumes.

Also with VSS Instant Restore, since all data on the log volume will replaced, if you want to preserve the new logs created after the backup was done, you will need to copy them off and replace them prior to mounting the databases.

VSS Instant Restore is currently supported only on the IBM SAN Volume Controller.

2.3.4 Using VSS and legacy backups together

You should use both backup methods (VSS and legacy) to back up your Exchange database as recommended and supported by Microsoft. If you also decide to use legacy incremental or differential backups, you should not base these backups on a VSS backup. As stated by Microsoft, you cannot apply incremental and differential backups to a VSS full backup.

If you are using legacy and VSS backup operations, ensure that backup schedules do not overlap. Incremental or differential backups cannot be done following a VSS full or copy backup.

2.4 Backup strategy

A backup strategy is one of the most important parts of your planning considerations, because every environment is unique. Also consider the service level agreements, and make sure, through rigorous testing, that the implemented backup strategy (of legacy and VSS backups) meets those SLA requirements. Here are some guidelines for developing a backup strategy.

- When you perform a VSS LOCAL backup, although the Exchange backup remains on local disk, metadata about the backup is sent to the Tivoli Storage Manager server. We recommend that, for the fastest restore, you define a separate management class pointing to a storage pool on disk only to use for this. The amount of metadata is very small, so it is practical to prevent it from migrating to tape.
- If you are already using Data Protection for Exchange legacy backups, you can use the existing nodename. Otherwise, create a new node for the Exchange legacy and VSS backups.
- You need to create a separate node for the local DSMAgent client if you are running your Exchange server in a cluster.
- You can use an existing node to manage the remote DSMAgent node (for offloaded backup) or create a new node.
- Exchange backups can be directed to a new or existing storage pool on the Tivoli Storage Manager server storage, depending on the retention requirements.
- A new or existing policy domain can be used for Exchange backups.

Important: If you are deploying VSS backups, we recommend that you perform legacy backups as well.

Here are some basic recommendations when integrating VSS with legacy backup:

- If using incremental or differential backups (available on legacy backup only), you must disable circular logging on the Exchange Server storage groups. This means archive logging is used.
- Do not mix incremental and differential backups. Use one or the other.
- Schedule VSS and legacy backups to start at different times, because you do not want these backups to overlap. Determine how long each backup would take and adjust their start times, so that one type of backup will not start before another has finished.
- You cannot restore incremental and differential legacy backups to a full or copy VSS backup.
- Incremental or differential backups cannot be done following a VSS full or copy backup; a legacy backup must be done first.
- When creating management classes for either Exchange legacy backups or VSS backups to TSM, use a timed retention period, rather than number of versions (RETEXTRA/RETONLY options, not VEREXISTS/VERDELETED) to allow the backups to expire based on time.

  Set VEREXISTS and VERDELETED to unlimited so that you will keep as many backups as are created during the required retention period. To keep each backup of this type for at least 30 days, create the management class with these parameters:

  - VEREXISTS nolimit
  - VERDELETED nolimit
  - RETEXTRA 30
  - RETONLY 30
- When creating a management class for VSS backups to LOCAL, use the version options in Tivoli Storage Manager (VEREXISTS/VERDELETED), because the number of versions you will keep depends on how much disk you have available for shadow target copy sets. To keep four versions, (inactive for at least seven days) use these parameters:

  - VEREXISTS 4
  - VERDELETED 4
  - RETEXTRA 7
  - RETONLY 7

Table 2-3 shows a sample backup strategy incorporating both legacy and VSS backups.

Note: We have not mentioned the INCREMENTAL, DIFFERENTIAL or DBCOPY backup types, because you should not mix backup types (VSS and legacy) that truncate logs. These options are possible to use—but be very careful how you plan this type of backup strategy, as they could interrupt each other's backup scheme if mixed.

Table 2-3 Sample VSS and legacy backup strategy

Legacy backup	VSS backup
► Perform a FULL Backup once per week and retain for a month.[1] ► Perform a COPY backup when required and retain for a year.[2]	► Depending on disk limitations, perform a VSS FULL backup to LOCAL at least three times per day and only retain four versions.[3] ► Perform a VSS FULL backup to TSM once per day and retain for a month.[4] ► Perform a VSS COPY backup once per month and retain for a year.[5]

The following will be true if the backup plan presented in Table 2-3 is followed:

[1] A Full Legacy weekly backup allows you to recover your Exchange database from Tivoli Storage Manager within the specified retention period of 30 days. This type of restore will take longer to run because the data is sent via TCP/IP or SAN to Tivoli Storage Manager Server storage.

[2] If required, you can do a Legacy COPY backup, which is retained in Tivoli Storage Manager storage for one year. We have not specified how often to run this type of backup, as it is intended to be our long-term retention policy. Therefore, it should be run as frequently as your service level agreements require.

[3] We have opted for a policy of four versions of VSS FULL backup to LOCAL. This will allow you to run a VSS backup at least three times per day. Depending on your environment and disk availability, you can change these options to suit your environment. Using this backup option allows you fast recovery when required, because the data is on local shadow volumes.

[4] The VSS FULL backup to Tivoli Storage Manager should run at least once per day and be retained in Tivoli Storage Manager storage for a month.

[5] We have used the option of running our VSS COPY backup once a month and retained in Tivoli Storage Manager storage for one year as our long-term storage policy dictated. This type of backup will reduce the workload on your server and your Production Exchange server can continue with normal operations without any extra workload on the server.

2.5 How Tivoli Storage Manager manages VSS backups

Tivoli Storage Manager uses its defined policies to manage VSS backups, including management classes and copy groups. The Tivoli Storage Manager server will determine when backups are expired according to the management classes used.

2.5.1 Management of VSS snapshot backups in Tivoli Storage Manager

For VSS backups, new VSSPOLICY statements are provided to associate different VSS backup types with management classes. These statements are entered in the Data Protection for Exchange configuration file (tdpexc.cfg).

You can have multiple VSSPOLICY statements in the Data Protection for Exchange configuration file (tdpexc.cfg), as seen in Example 2-1. The file is read from the bottom up, exactly like the INCLUDE statements you would configure in your dsm.opt file. If you do not have any VSSPOLICY statements, or if there is no match for a particular backup type, the default management class for the policy domain is used.

If any policy changes are made to the tdpexc.cfg file, you must restart your Tivoli Storage Manager Client Acceptor Daemon (CAD), Tivoli Storage Manager Remote Client Agent Service (DSMAgent) and your Tivoli Storage Manager Scheduler Service For Exchange.

If your DSMAgent service is in a state of Manual (Started), we advise you to stop this service. This would not be necessary if this service is in a Stopped state. The DSMAgent service will only start up when a VSS backup is initiated—but if this service is started and you make changes to your policy settings, your policy settings will not take effect until you have restarted this service.

The basic syntax of a VSSPOLICY statement is:

```
VSSPOLICY <srv-name> "<stg-grp-name>" <backup-type> <backup-dest> <mgmtclass>
```

where

<srv-name> is the Exchange server name. It can be an asterisk (*) to match all Exchange servers.

<stg-grp-name> is the storage group name. It can be an asterisk (*) to match all Exchange storage groups. Use quotes around the storage group name, since these names can contain spaces.

<backup-type> specifies the Exchange backup type: FULL, COPY, or asterisk (*) to match both backup types.

<backup-dest> is the backup destination; TSM (for a backup to Tivoli Storage Manager), LOCAL (for a backup to local disk) or an asterisk (*) to match BOTH types of backups.

<mgmtclass> specifies the Tivoli Storage Manager management class which will be used to bind the types of backups specified.

Example 2-1 shows sample VSSPOLICY statements. A sample configuration file is installed with Data Protection for Exchange. Uncomment the VSSPOLICY statements by removing the initial asterisk (*) to make them effective.

Example 2-1 Sample VSSPOLICY statements

```
* Sample VSSPOLICY Statements
* --------------------------
* These statements are used to bind VSS backups to specific TSM
* Server management classes. Adjust the statements to meet your needs
* and remove the leading asterisks to make them operational.
* Note: Matching of these policy bindings are from the bottom up.
*********************************************************************
*         Server   Storage Group Name  BU Type  BU Dest.  Mgmt Class
*         ------   ------------------  -------  -------   ----------
 VSSPOLICY  *        *                  FULL     TSM       REDBOOK_TSM
 VSSPOLICY  *        *                  COPY     TSM       REDBOOK_TSM_COPY
 VSSPOLICY  *        *                  COPY     LOCAL     REDBOOK_COPY
 VSSPOLICY  *        *                  FULL     LOCAL     REDBOOK_LOCAL
 VSSPOLICY  *        "Human Resources"  FULL     LOCAL     MCLASS3
 VSSPOLICY  SERVER1  "Accounting"       *        LOCAL     MCLASS2
 VSSPOLICY  SERVER1  "SG1       "       *        TSM       REDBOOK1
```

This policy specifies the following rules:

- Any VSS backups of the SG1 storage group on the Exchange server SERVER1 to Tivoli Storage Manager will be bound to the management class REDBOOK1.
- Any VSS backups of the Accounting storage group on the Exchange server SERVER1 to LOCAL will be bound to the management class MCLASS2.
- FULL VSS backups of the Human Resources storage group on any Exchange server to LOCAL will be bound to the management class MCLASS3.
- FULL VSS backups of any other storage group on any other Exchange server to LOCAL will be bound to the management class REDBOOK_LOCAL.

- COPY VSS backups of any other storage group on any other Exchange server to LOCAL will be bound to the management class REDBOOK_COPY.
- COPY VSS backups of any other storage group on any other Exchange server to Tivoli Storage Manager will be bound to the management class REDBOOK_TSM_COPY.
- FULL VSS backups of any other storage group on any other Exchange server to Tivoli Storage Manager will be bound to the management class REDBOOK_TSM.

This policy is complete; that is, any type of backup will match a rule because of the wild-carded VSSPOLICY statements at the top of the file. We recommend using these types of statements so that you explicitly state what management class will be used.

2.5.2 Legacy backup management

Legacy backup management remains the same as before: the management class for legacy backups continues to be defined using Include/Exclude statements in the Data Protection for Exchange client options file (dsm.opt). This means that if you are already using Data Protection for Exchange, you may not have to change these current policy settings.

However, adding VSS backups to the mix may lead you to re-evaluate the frequency and retention of the legacy backups, in order to best exploit a mix of legacy and VSS backups as they affect your current backup SLA.

The Legacy backup process is explained in detail in *Data Protection for Microsoft Exchange Server Installation and Users Guide*, SC32-9058.

2.5.3 Version management of VSS snapshot backups

Note: A VSS snapshot backup done to LOCAL shadow volumes remains active until the backup version is expired according to the policy settings used for local shadow volume backups.

VSS backups to LOCAL

The number of LOCAL backup versions maintained by the Tivoli Storage Manager server is determined by the value specified by the Tivoli Storage Manager server VEREXISTS parameter (defined in the copy group of the management class to which the LOCAL backup is bound). The number of target volume sets available for local backups should equal the VEREXISTS parameter.

For example, if VEREXISTS=2, then at least two sets of target volumes must be allocated for the backup to complete successfully. If only one set of target volumes is allocated, the second and subsequent backup attempts will fail. If more sets of target volumes exist than the number specified by the VEREXISTS parameter, these sets are ignored by the Tivoli Storage Manager server.

Also note that VSS snapshots, when they are made, immediately overwrite any previous contents of the target set. Therefore, you have to be careful of the consequences for version retention if the snapshot operation fails for any reason.

Suppose, for example, that your requirement is to always have two snapshots available on LOCAL. In this scenario, set VEREXISTS=3. This appears counterintuitive—but consider what would happen if VEREXISTS=2 in this scenario.

You successfully make two LOCAL snapshots, then initiate a third snapshot. This uses the target set that was occupied by the first snapshot, since there are only two target sets available. If this snapshot on LOCAL fails for whatever reason, you have already overwritten (and therefore deleted) the previous oldest LOCAL backup, since its space was required to make the new backup. You only have one valid LOCAL snapshot available now, not two as required. This is shown in Figure 2-4.

The general rule is that if you want to keep N LOCAL snapshots, specify VEREXISTS=N+1.

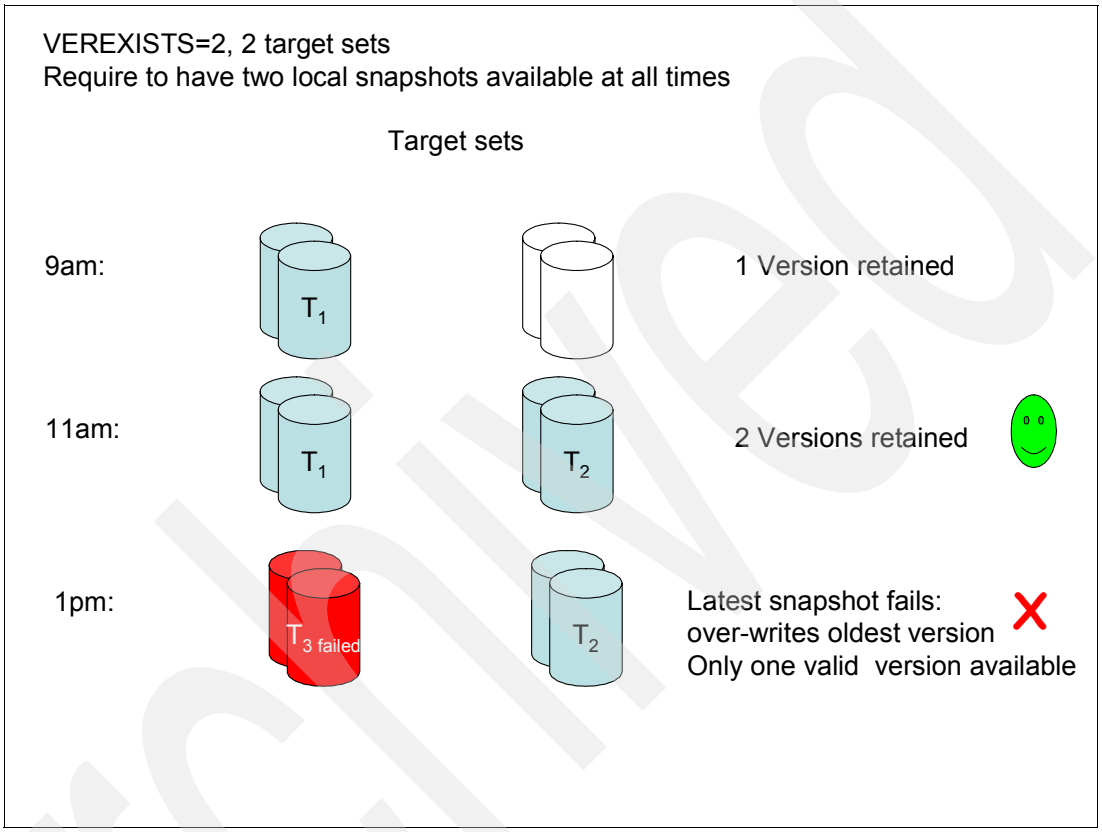


Figure 2-4 What happens if a LOCAL snapshot fails

So instead, set VEREXISTS=3 with three target sets. This means you will always have two LOCAL versions available, regardless of the failure of an individual snapshot, as shown in Figure 2-5 on page 38.

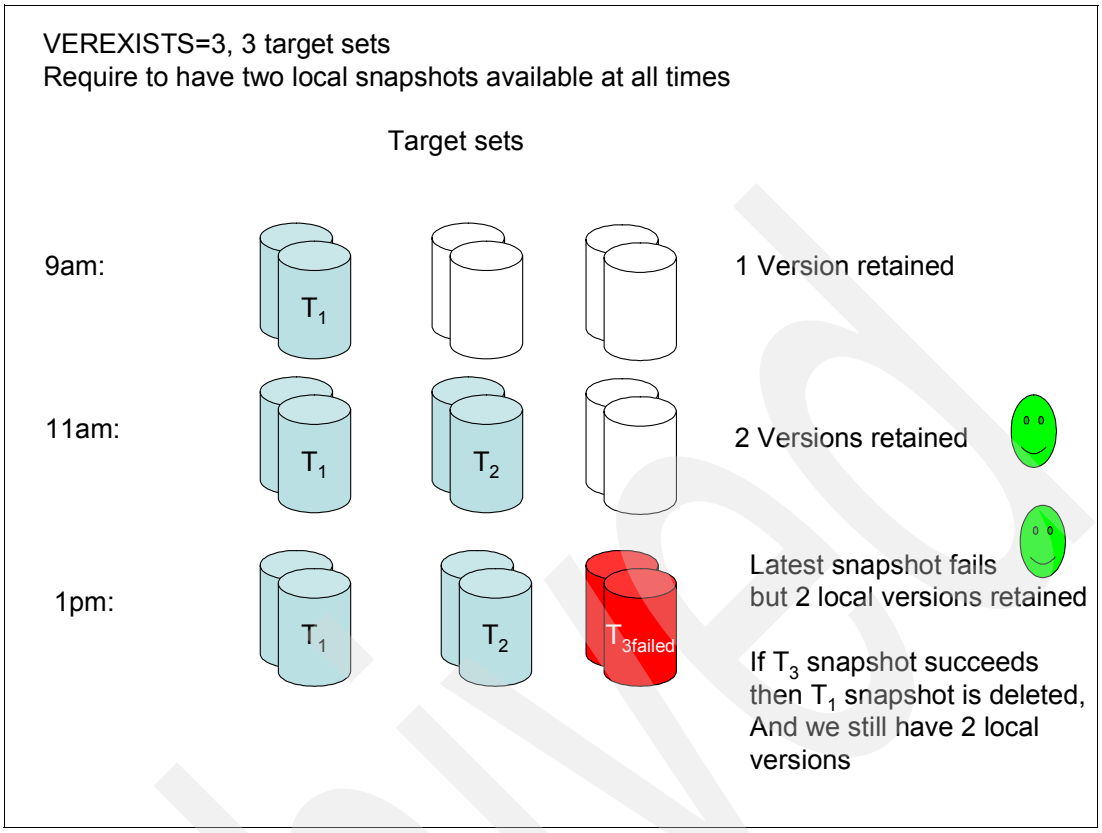


Figure 2-5 Correct number of LOCAL snapshots retained

The policy management of local backups is responsible for reconciling the local backup repository with the information stored on the Tivoli Storage Manager server. For example, if target volume LUNs that were used for a local backup are removed from the storage system, the information representing the backup on the Tivoli Storage Manager server must be reconciled.

Likewise, if the Tivoli Storage Manager server policy has determined that a local backup copy is no longer needed, then the local backup manager must free the target volumes to the storage system so that these LUNs can be used for future backup operations. Tivoli Storage Manager automatically detects these situations and performs the reconciliation.

It is possible for VSS backups 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. Tivoli Storage Manager cannot prevent such a removal.

Obviously, this practice should be avoided. If this happens, 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.

Note: Different hardware providers implementations have different disk space requirements for snapshots. In the case of the IBM SAN Volume Controller and DS6000/8000, the snapshot target volumes require the same amount of space as the source volumes, and must match in size and number of LUNs. However, other point-in-time copy implementations do not require this, so the reserved space required for each snapshot target volume set will be less.

Our examples are based on a provider such as the SVC/DS. However, your disk requirements may be less if using another disk system. For planning purposes, you should check your disk system's space requirements for snapshots, and run tests to determine an average disk size for the target volume set, based on your configuration.

VSS backups to Tivoli Storage Manager

The number of backup versions maintained by the Tivoli Storage Manager server is determined by the value specified by the Tivoli Storage Manager server VEREXISTS, VERDELETED, RETEXTRA and RETONLY parameters defined in the copy group of the management class to which the backup is bound. Typically, we recommend using only RETEXTRA and RETONLY parameters, and setting VEREXISTS and VERDELETED to NOLIMIT. This ensures that your Exchange backups are retained based on time.

For backing up to the Tivoli Storage Manager server storage pools, you only require one target volume set, since the snapshot made is non-persistent and deleted after the backup completes. Therefore, this target volume set is available for re-use.

However, if you doing VSS backups to LOCAL *as well as* VSS backups to Tivoli Storage Manager, be aware that for many VSS hardware implementations (including SVC and DS) there is only one "pool" of snapshot target sets. The backup operation will choose any free target set, regardless of the backup destination specified (LOCAL or to Tivoli Storage Manager. It will therefore overwrite the oldest LOCAL VSS snapshot, meaning you may no longer keep the desired number of LOCAL backup versions.

Therefore, in this case, for the management class used for local backups, if you want to have N local backups at all times, also specify VEREXISTS of N+1 and make, in total, N+1 target sets available for use. That way, there is always an extra target set available for the non-persistent snapshot used to back up to Tivoli Storage Manager, which will not interfere with the local snapshot retention. It also protects against unwanted deletion of snapshots in the event of a backup failure.

Example: VSS backups to LOCAL and Tivoli Storage Manager

We can see how the VEREXISTS parameter works in a typical situation where you want to make regular VSS snapshot backups to a LOCAL disk, as well as more infrequent backups (say, once a day) to Tivoli Storage Manager. Suppose your Exchange database and logs are using 30 GB of LUNs on a SAN Volume Controller. You want to keep Tivoli Storage Manager backups for 30 days, and you also want to keep two local VSS snapshots (persistent).

- Create a management class for backups to LOCAL with VEREXISTS=3.
- Create a management class for backups to Tivoli Storage Manager with a retention period of 30 days (RETEXTRA=30/RETONLY=30). VEREXISTS and VERDELETED should be set to NOLIMIT, since you can make as many backups to Tivoli Storage Manager as you want. This will have no effect on the number of target sets you need, since the snapshot to Tivoli Storage Manager is non-persistent. Therefore, it is deleted from the target set as

soon as it is backed up to the server storage pool. The server backups are retained according to the number of days in RETEXTRA and RETONLY.

Tivoli Storage Manager will retain and expire the backups stored in its storage pools based on the date stamp, so that each backup is kept for 30 days.

- Create three sets of 30 GB Target Volume LUNs for VSS backups. The management class for LOCAL backups should specify VEREXISTS=3. This will ensure there is always a “spare” target set for the non-persistent snapshot for Tivoli Storage Manager backup, while being able to maintain our desired number of two LOCAL snapshots.
- The LOCAL VSS backups will expire according to version control. That is, when the third VSS LOCAL backup is made, the local backup manager frees the target set used for the oldest backup so that the LUNs are available for re-use.

This configuration is shown in Figure 2-6.

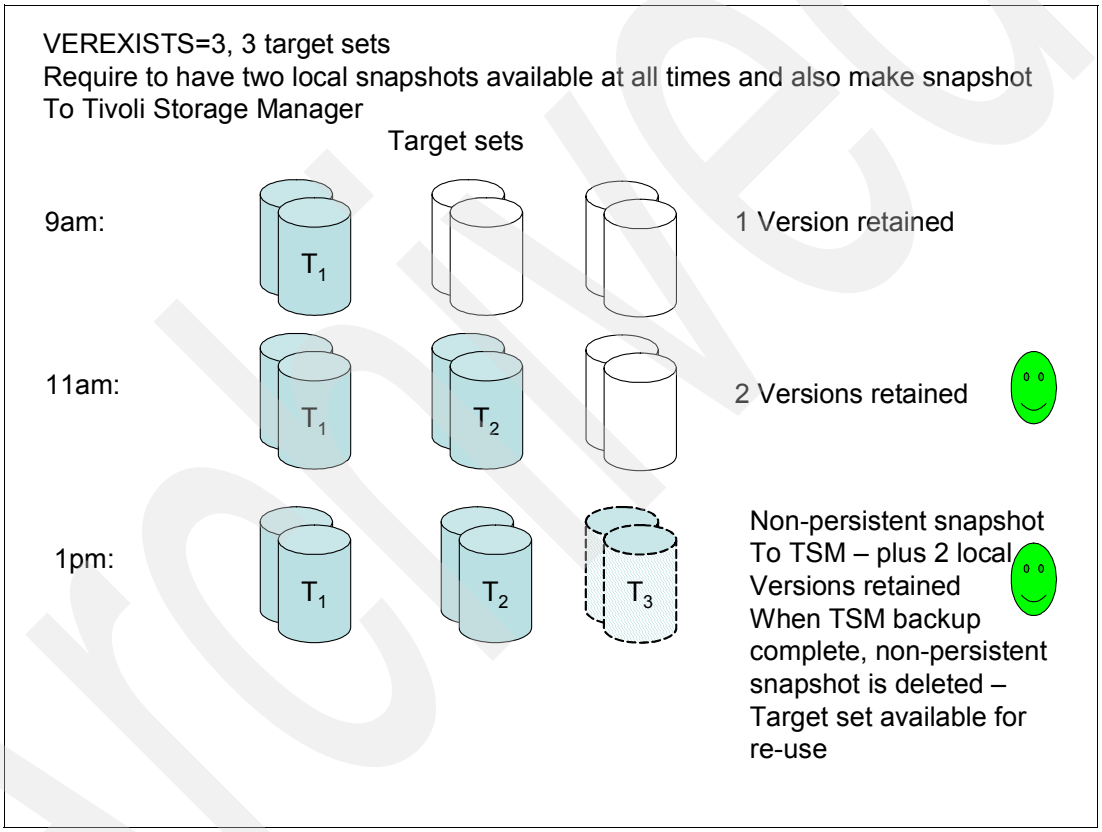


Figure 2-6 Maintaining version control for backups to LOCAL and Tivoli Storage Manager

2.5.4 General policy considerations

In a perfect world, we would have unlimited disk space and be able to configure an unlimited number of target sets to keep an unlimited number of VSS backups. However, this is not realistic, and compromises always have to be made. Here are some considerations to help you decide how many backup versions to keep:

- Overall backup strategy. This is influenced by requirements from your users, management and budgetary requirements, as well as regulatory requirements.
- The length of time that VSS backups need to kept in Tivoli Storage Manager server storage, combined with the frequency of backup. If you make a VSS backup to Tivoli Storage Manager once a day, and your policy says to keep them for 30 days, you will

need 30 times the size of the backup available as storage pool space on the Tivoli Storage Manager server.

- The number of legacy backups to reside on Tivoli Storage Manager server storage.
- The number of VSS backup versions to reside on local shadow volumes. The more versions you need to keep, the more target sets you require.
- The amount of available target volume storage provisioned for VSS operations. You can only keep as many local snapshot copies as there are target volume sets. Remember that your particular VSS hardware provider will determine the size of each target set and the number of sets available.

2.6 Microsoft Cluster Server (MSCS) support

Volume Shadow Copy Services is supported in a Microsoft Cluster environment. We cover installation special considerations for a cluster environment in Chapter 3, “Installation” on page 43 and operational considerations in Chapter 4, “Backup and restore” on page 99.

In particular, note the following points:

- At the time of writing, Hotfix KB903650 from Microsoft is required to support Instant Restore in a clustered environment.
- Dynamic disks are not supported.
- Exchange VSS backups to LOCAL are only visible—and can only be restored from—the cluster node which made them. This is a Microsoft restriction, and does not apply to VSS backups to Tivoli Storage Manager.
- Space on a shared disk is required to store descriptor information about snapshots so that all nodes can see the local snapshot repository information regardless of what node the Exchange server is running on.
- The Tivoli Storage Manager Client Acceptor Daemon (CAD) must be installed on each cluster node so that it can continue in the event of a failover.

For further information about setting up Tivoli Storage Manager for Exchange in a cluster, refer to *Data Protection for Microsoft Exchange Server Installation and Users Guide*, SC32-9058. Refer to *IBM Tivoli Storage Manager in a Clustered Environment*, SG24-6679, for information about general cluster setup for Tivoli Storage Manager.

2.7 Tivoli Storage Manager client configuration for VSS

In order for the VSS components to function with the Tivoli Storage Manager server, the following client setup is required. Data Protection for Exchange VSS functions utilize the Tivoli Storage Manager proxy node capability introduced in Tivoli Storage Manager V5.3. This capability allows multiple different Tivoli Storage Manager nodes to store data under a single node name. It also enables the Data Protection client to communicate with the backup-archive client (Local DSMAgent).

Here is a list of required clients that need to be configured for VSS:

- Data Protection for Exchange Client Node
- Local DSMAgent Client Node
- Remote DSMAgent Client Node (only required if offloaded backups are to be used)

We briefly summarize various configuration considerations here. Full details are provided in Chapter 3, “Installation” on page 43.

Note: All nodes that will be used for VSS functions must be distinct from each other, but existing Data Protection for Exchange and backup-archive client nodes can be re-used if they exist. For clarity, we recommend defining separate dedicated nodes for each of these functions

2.7.1 Data Protection for Exchange client node

This is the Tivoli Storage Manager nodename that will own and manage the Exchange backup data (both legacy and VSS) on the Tivoli Storage Manager Server. This is known as the *target node* that you use when you grant proxy control to other nodes to back up or restore this client’s data. This node name will be specified in the Data Protection for Exchange dsm.opt file as follows:

```
nodename REDBOOK_EXCHANGE
```

2.7.2 Local DSMAgent client node

This is the Tivoli Storage Manager nodename that will be responsible for driving the VSS operations and possibly moving VSS backups to Tivoli Storage Manager. This node can also be your existing backup-archive client node, or you could register a new nodename in the Tivoli Storage Manager server. This node will be used by the Tivoli Storage Manager Client Acceptor Daemon (CAD) and DSMAgent.

If you are running in a cluster environment, it is a best practice to register a separate node from your normal backup-archive client, because you will be required to make this service a non-cluster option. You will be required to register a new service for this node. For each server within your cluster environment, you will be required to have a separate service running, because the service is not cluster-aware.

Within the **grant proxynode** command, this node is an agent node. This nodename is set up in the tdpexc.cfg file as follows:

```
localdsmagentnode REDBOOK_VSS_A
```

2.7.3 Remote DSMAgent client node

This is the (optional) Tivoli Storage Manager nodename that will perform the movement of VSS snapshot data from the VSS disk to the Tivoli Storage Manager server if offloaded backup is configured. Using this option in a cluster environment does not require you to register a separate node for each server within the cluster because this server only acts as a secondary server.

Within the **grant proxynode** command, this node is an agent node. This nodename is set up in the tdpexc.cfg file as follows:

```
remotedsmagentnode REDBOOK_OFFLOAD
```

Note that a CAD and DSMAgent need to be set up and configured on the offloaded backup server, as well.

3

Installation

In this chapter we describe the Data Protection for Exchange installation integrated with Tivoli Storage Manager for Copy Services. This includes the installation of all components including the Backup Archive Client, Data Protection for Exchange, and Tivoli Storage Manager for Copy Services modules.

3.1 Installation overview

We assume that you have detailed knowledge of Tivoli Storage Manager client and server installation and configuration. You should also be familiar with Data Protection for Exchange basic operation. The following IBM Redbooks and publications are useful for reference.

- *IBM Tivoli Storage Management Concepts*, SG24-4877
- *IBM Tivoli Storage Manager Implementation Guide*, SG24-5416
- *Data Protection for MS Exchange Server Installation and Users Guide,* SC32-9058
- *IBM Tivoli Storage Manager Backup-Archive Clients Installation and Users Guide (Windows)*, GC32-0788

If you will be using a MSCS clustered environment, the following redbook is also useful:

- *IBM Tivoli Storage Manager in a Clustered Environment*, SG24-6679

In our lab we set up two environments to show various capabilities of Tivoli Storage Manager for Copy Services in an Exchange environment; specifically, offloaded and non-offloaded backup, as well as fast restore and Instant Restore.

Figure 3-1 and Table 3-1 illustrate our first lab environment setup. The Exchange database was installed on SAN-attached IBM System Storage DS8000 disk, and the VSS shadow backups would also be created on this disk system. The Exchange servers REDBOOK2 and REDBOOK3 were installed in a clustered environment using MSCS.

REDBOOK1 acted as the Active Directory® server and DNS controller. It would also be used as the offloaded backup server. The Tivoli Storage Manager server code was installed with initial configuration complete (including tape device and deviceclass definitions) on the system ZEALOT. Backups sent to Tivoli Storage Manager would reside in a storage pool on tape.

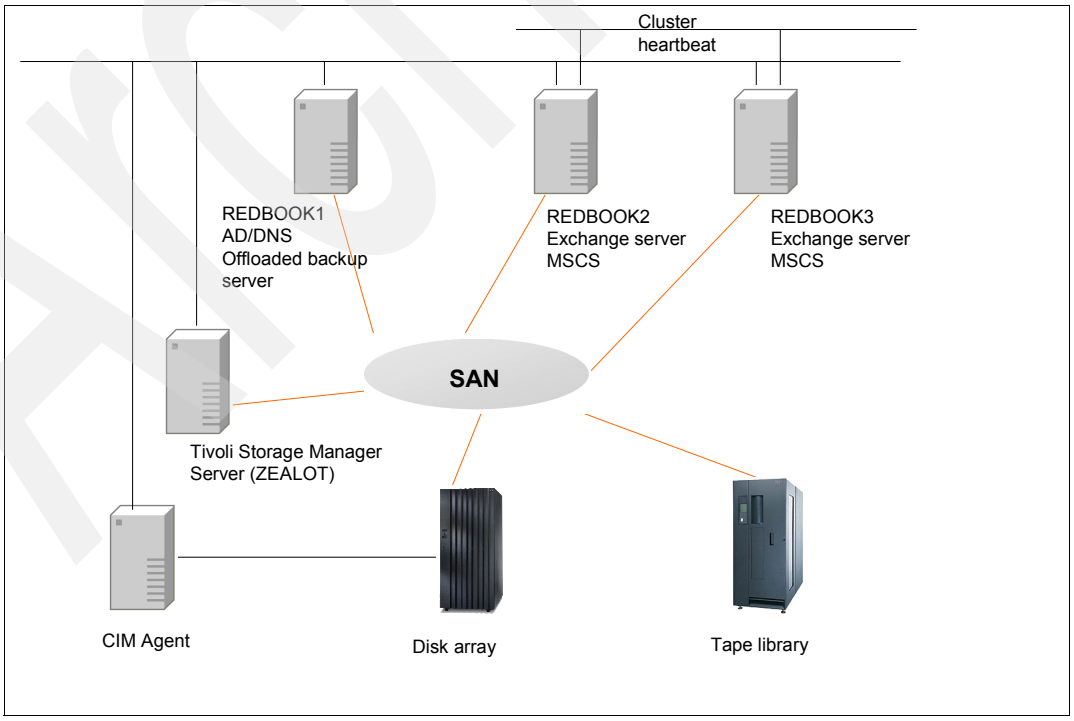


Figure 3-1 Clustered Exchange server setup

The software listed in Table 3-1 indicates what our final configuration was. We show most of the installation in this chapter, apart from the actual operating system, clustering configuration, Microsoft Exchange installation, and Tivoli Storage Manager server initial install and configuration.

Table 3-1 Initial installation of lab

Host name	Purpose	Operating system	IP address	Software installed
REDBOOK1	Active Directory (AD), Domain Name Server (DNS), Offloaded backup server	Windows 2003 SP1	9.43.238.111	MS Exchange Management Tools Backup-archive Client 5.3.4.6 IBM VSS-VDS Support 2.4.2.0016
REDBOOK2	MSCS Exchange node	Windows 2003 SP1	9.43.238.189	MS Exchange 2003 SP2 IBM Tivoli Storage Manager Client 5.3.4.6 IBM Tivoli Storage Manager Data Protection for Exchange 5.3.3 IBM Tivoli Storage Manager for Copy Services Exchange VSS Integration Module 5.3.3 IBM VSS-VDS Support 2.4.2.0016

Host name	Purpose	Operating system	IP address	Software installed
REDBOOK3	MSCS Exchange node	Windows 2003 SP1	9.43.238.217	MS Exchange 2003 SP2 IBM Tivoli Storage Manager Client 5.3.4.6 IBM Tivoli Storage Manager Data Protection for Exchange 5.3.3.0 IBM Tivoli Storage Manager for Copy Services Exchange VSS Integration Module 5.3.3 IBM VSS-VDS Support 2.4.2.0016
RB1EVS	MSCS Cluster Exchange resource		9.43.238.222	
ZEALOT	Tivoli Storage Manager Server	Windows Server 2003	9.43.238.18	Tivoli Storage Manager Server 5.3.3.0
CIM Agent Server panda01	DS8000 CIM	AIX 5.3	9.43.237.18	DS8000 CIM

Our other lab environment used a non-clustered configuration with SAN Volume Controller. It was used to illustrate the Instant Restore function for VSS Exchange backups, and is described in 4.7.3, “VSS Instant Restore” on page 144.

Figure 3-2 on page 47 and Table 3-2 summarize our Exchange 2003 mail store layout, including the assignment of the disks to each entity. All the disks with Exchange data were on the DS8000.

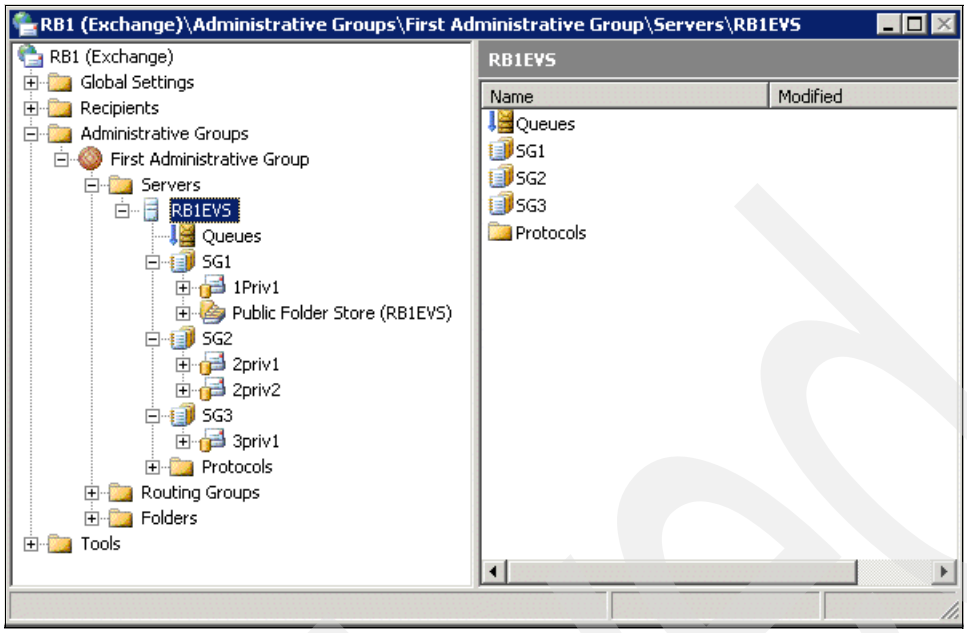


Figure 3-2 Exchange configuration

Note that we adhered to the recommendations given in 2.1.3, “Storage layout considerations for Microsoft Exchange” on page 23, so that the database file for each Storage Group and logs were on separate dedicated LUNs.

Table 3-2 Exchange database distribution

Storage Group	Store	Exchange database	Transaction log
SG1			F:\SG1Logs
	Public Folder	E:\EXCHSRVR\mdbdata\pub1.edb	
	1Priv1	E:\EXCHSRVR\mdbdata\priv1.edb	
SG2			H:\SG2Logs
	2Priv1	G:\SG2\MDBDATA\2priv1.edb	
	2Priv2	G:\SG2\MDBDATA\2priv2.edb	
SG3			J:\SG3Logs
	3Priv1	I:\SG3\MDBDATA\3priv1.edb	

3.1.1 Summary of the installation and configuration steps

Our primary lab configuration had a 2-way MSCS Exchange cluster and an offloaded backup server. We will explain in this section the differences which are required if you are in a non-clustered Exchange environment, or if you are not using an offloaded backup server.

The installation and configuration steps are as follows:

1. Ensure name resolution is working between all participating nodes and the Tivoli Storage Manager server.
2. Create Storage Pools, Policy Domain, Policy Set, Management Class and Backup Copy Group in the Tivoli Storage Manager server, set the default management class and activate the Policy set.
3. Register the Exchange nodename.
4. Register nodenames for the three backup-archive clients for DSMAgents (one for each server in the Exchange cluster and one for the offloaded backup server).
5. Install the Tivoli Storage Manager backup-archive (V5.3.4.3 or later) client on the three machines (Exchange cluster nodes and offloaded backup server).
6. Install Data Protection for Exchange (V5.3.3) on both Exchange cluster nodes.
7. Install IBM Tivoli Storage Manager for Copy Services - Microsoft Exchange VSS Integration Module Version 5.3.3 on both Exchange cluster nodes.
8. Configure Tivoli Storage Manager option and configuration files:
   a. Local DSMAgent options files on each cluster node (or single option file, if non-clustered).
   b. DSMAgent shortcut on each cluster node.
   c. Remote DSMAgent options file on offloaded backup server.
   d. TData Protection for Exchange option file on shared disk (for a clustered configuration only).
9. Configure CAD and remote agent services.
10. Create a cluster service to manage the CAD service (for a clustered configuration only).
11. Configure the proxy node definitions.
12. Install the MS Exchange management tools on the offloaded server.
13. Configure a PATH variable for required executables.
14. Install the VSS-VDS provider on the three machines.
15. Define and configure storage space for VSS backups:
    a. Create VSS_FREE and VSS_RESERVED pools.
    b. Verify the VSS configuration.
16. Use **vssadmin** and **vshadow** commands to verify the environment.

Figure 3-3 on page 49 summarizes the software pieces to be installed in each server. Note that If your Exchange server is not clustered, you will have only one Exchange server, not two, as shown. The offloaded server configuration is optional, if you decide to use another system for doing backups of VSS snapshots to Tivoli Storage Manager.

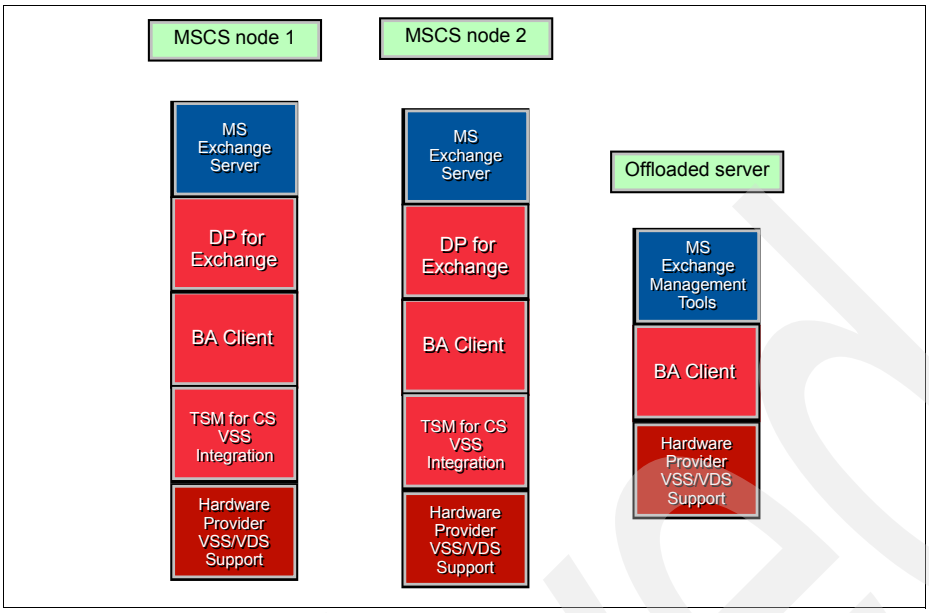


Figure 3-3 Software installed on each system

3.2 Detailed installation procedure

In the following sections we explain the details of the steps listed in 3.1.1, “Summary of the installation and configuration steps” on page 47, so that we can back up Exchange databases using VSS.

3.2.1 Verify name resolution

In our configuration, the server REDBOOK1 was the Active Directory domain controller and DNS. We used a separate domain, RB1.Local. We verified that we could connect between the cluster nodes and the DNS node, by IP address and host name (forward and reverse name resolution).

Also, the Tivoli Storage Manager server must be able to resolve the host names (forward and reverse name resolution) of the Exchange servers and offloaded server. In your case, if you cannot do this, you must make sure your DNS is properly configured before proceeding, because the backup and restore functions will not work correctly.

3.2.2 Create storage pools and policy settings

Example 3-1 illustrates our Tivoli Storage Manager configuration. We set up storage pools and a separate policy domain, including management classes and copy groups, as shown. When setting up your configuration, carefully consider the copy group requirements and how they map to version retention, as described in 2.5, “How Tivoli Storage Manager manages VSS backups”.

Example 3-1 Tivoli Storage Manager server definitions

```
define stgpool LONGTAPEPOOL <dev_class_name> maxscratch=100 reusedelay=2

define stgpool EXCHTAPEPOOL <dev_class_name> maxscratch=100 reusedelay=2
```

```
define stgpool EXCHMETAPOOL DISK description="Storage Pool for VSS Backup
Metadata"

define domain REDBOOK description="MS Exchange Domain" backretention=365

define policyset REDBOOK REDBOOK_PO description="MS Exchange Policy Set"


define mgmtclass REDBOOK REDBOOK_PO REDBOOK_VSS_LOCAL description "VSS LOCAL
MgmtClass"

define mgmtclass REDBOOK REDBOOK_PO REDBOOK_VSS_FULL description "VSS FULL
MgmtClass"

define mgmtclass REDBOOK REDBOOK_PO REDBOOK_VSS_COPY description "VSS COPY Long
Term MgmtClass"

define mgmtclass REDBOOK REDBOOK_PO REDBOOK_LEGACY_EXCHANGE description "Monthly
Legacy MgmtClass"

define mgmtclass REDBOOK REDBOOK_PO REDBOOK_LEGACY_COPY description "Long Term
Legacy MgmtClass"


define copygroup REDBOOK REDBOOK_PO REDBOOK_VSS_LOCAL type=backup
destination=EXCHMETAPOOL verexists=4 verdeleted=4 retextra=nolimit retonly=nolimit

define copygroup REDBOOK REDBOOK_PO REDBOOK_VSS_FULL type=backup
destination=EXCHTAPEPOOL verexists=nolimit verdeleted=nolimit retextra=31
retonly=31

define copygroup REDBOOK REDBOOK_PO REDBOOK_VSS_COPY type=backup
destination=LONGTAPEPOOL verexists=nolimit verdeleted=nolimit retextra=365
retonly=365

define copygroup REDBOOK REDBOOK_PO REDBOOK_LEGACY_EXCHANGE type=backup
destination=EXCHTAPEPOOL verexists=nolimit verdeleted=nolimit retextra=31
retonly=31

define copygroup REDBOOK REDBOOK_PO REDBOOK_LEGACY_COPY type=backup
destination=LONGTAPEPOOL verexists=nolimit verdeleted=nolimit retextra=365
retonly=365


assign defmgmtclass REDBOOK REDBOOK_PO REDBOOK_VSS_LOCAL

activate policyset REDBOOK REDBOOK_PO
```

In our environment, we defined five management classes for the REDBOOK_PO policy domain, in order to categorize and satisfy our retention requirements:

- REDBOOK_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 versioning instead of time, because you must ensure that you have enough disk space to hold all your required snapshots. In our case we specify VEREXISTS=4.

The copygroup for this management class points to a small disk storage pool. This is because even though the VSS backup itself does not use Tivoli Storage Manager storage pool space, some metadata about the backup is stored in a storage pool. Therefore you need a storage pool. We recommend this is on disk only, with no migration to tape, to ensure that the metadata can be quickly accessed in the event of a restore.

- REDBOOK_VSS_FULL: This is the management class used for daily VSS backups that are sent to Tivoli Storage Manger. This kind of backup uses just one non-persistent (temporary) snapshot in order to send the data to the Tivoli Storage Manger Server. Therefore, you just need to ensure that you always have the required disk space for this snapshot. If you perform your backup with destination BOTH, then the target set will be used for both backups: to LOCAL and Tivoli Storage Manager. Therefore, you can reduce the number of target sets which will be required.

  The retention policy for backups to Tivoli Storage Manager should be enforced by time period (in our case, one month).

  REDBOOK_VSS_COPY: This management class is used for long-term backup retention, therefore the retention policy should be enforced by date. In our case, we specified to retain these backups for 365 days. We used a separate management class for these long-term (VSS COPY) backups versus the daily (VSS FULL) backups so that we could enforce the different expiration period.

  Use a different destination storage pool for daily and long-term backups, so they can be managed more efficiently for offsite storage and reclamation.

- REDBOOK_LEGACY_EXCHANGE: This is the management class used for weekly legacy backups. The retention policy is based on date.
- REDBOOK_LEGACY_COPY: This is the management class used for Legacy long-term backups. It is enforced by date policy. And as for VSS backups, you should specify a different storage pool from the weekly legacy backups.

3.2.3 Register Exchange and DSMAgents nodenames

We registered the Exchange nodename REDBOOK_EXCHANGE, and DSMAgent nodenames REDBOOK_VSS_A, REDBOOK_VSS_B, and REDBOOK_OFFLOAD, as shown in Example 3-2.

Example 3-2 Register Tivoli Storage Manager nodename

```
register node redbook_exchange <password> domain=REDBOOK backdelete=yes

register node redbook_vss_a <password> domain=REDBOOK

register node redbook_vss_b <password> domain=REDBOOK

register node redbook_offload <password> domain=REDBOOK
```

3.2.4 Install the backup-archive client code

Install the Tivoli Storage Manager backup-archive client at V5.3.4.6 or higher on all machines that will participate in the backup of Exchange. In our case, we had a clustered setup and an offloaded backup server; therefore, we installed on REDBOOK1, REDBOOK2, and REDBOOK3.

If you are not in a clustered environment, install the client on the single Exchange server. If you have an offloaded backup server, then install the backup-archive client there.

Before you start the installation, we recommend that you obtain the latest code level from this site:

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

Important: Tivoli Storage Manager backup-archive client V5.3.4.6 or higher is required in order to incorporate important fixes.

Refer to the client installation documentation for detailed instructions. We chose a Typical installation; however, 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 that 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.

After the client installs, verify that the Exchange VSS Integrity Checker excvssic.exe exists in the BA Client directory (C:\Program Files\Tivoli\tsm\baclient if you accepted the default directory), and also that the VSS Snapshot Plug-in pivss.dll exists in the baclient\plugins directory (C:\Program Files\Tivoli\tsm\baclient\plugins).

For more information about installation and configuration of the backup-archive client, refer to the latest version of *IBM Tivoli Storage Manager Backup-Archive Clients Installation and User's Guide*.

3.2.5 Install Data Protection for Exchange

Install Tivoli Storage Manager for Mail - Data Protection for Exchange at V5.3.3 or higher on your Exchange server. If you are using MSCS, install on both cluster nodes. We installed on our cluster nodes, REDBOOK2 and REDBOOK3.

Check the file README DPEXC_enu.htm for any late-breaking news.

Note: Data Protection for Exchange must be installed from an account that is a member of both the local Administrators group (or another account with read/write access to the local registry) and the Domain Admins group.

1. Insert the installation CD and wait for the autorun, or run X:\ TDPExchange\ x32\ client\setup from the Windows command line.
2. Select a language for the installation, as shown in Figure 3-4. We chose English (United States).

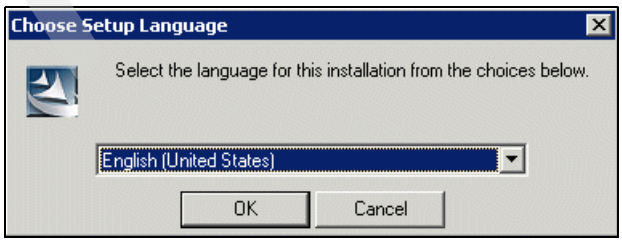


Figure 3-4 Select language for installation

3. Click **Next** in the installation wizard welcome, shown in Figure 3-5 on page 53.

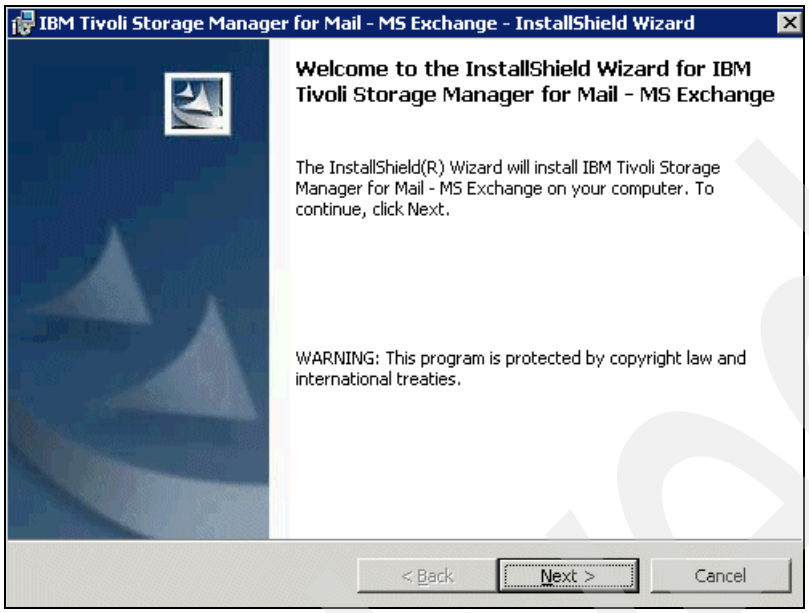


Figure 3-5 InstallShield Wizard welcome

4. Accept the license agreement and click **Next**.
5. Select the destination folder and click **Next**. We choose to install the code in the default installation path, as shown in Figure 3-6.

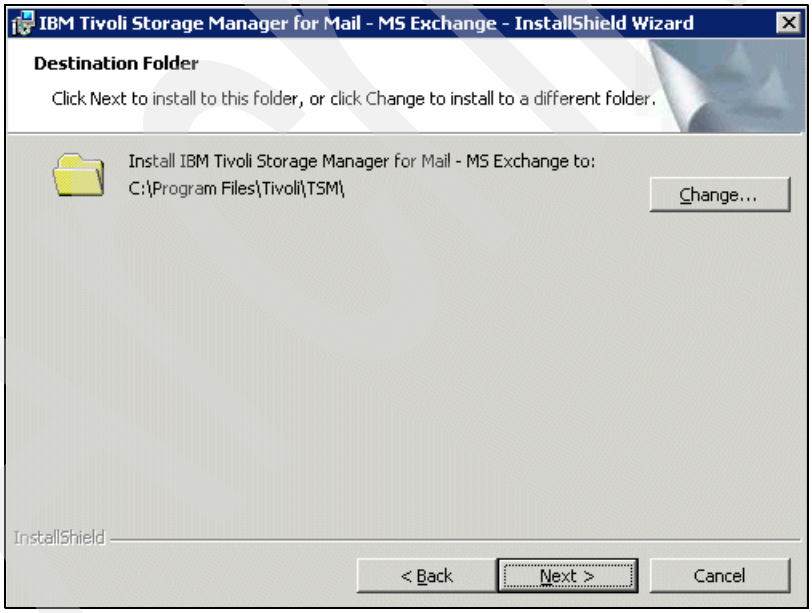


Figure 3-6 TDP installation path

6. On the next window, click **Next** to start the installation.
7. If the installation completes successfully, as shown in Figure 3-7 on page 54, click **Finish**.

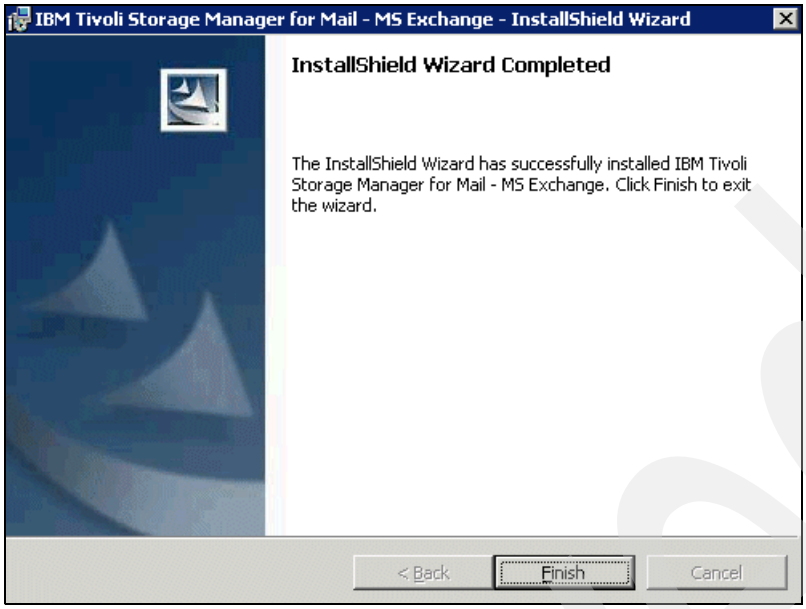


Figure 3-7 Finish Tivoli Storage Manager for Mail installation

8. Verify the license file excclient.lic has been installed in the installation directory: C:\Program Files\Tivoli\TSM\TDPExchange (by default).

3.2.6 Install IBM Tivoli Storage Manager for Copy Services

IBM Tivoli Storage Manager for Copy Services actually consists of two modules: MS Exchange 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 have a SAN Volume Controller as the disk system, and want to use Instant Restore.

Install MS Exchange VSS Integration Module

1. Insert the CD-ROM that contains the Microsoft Exchange VSS Integration Module into the CD-ROM drive. If autostart is not enabled, run X:\TDPExchange\x32\plugin\setup (where x is your CD-ROM drive letter).
2. Click **OK** to start the installation program.
3. Select a language for the installation and click **OK**. We choose English.
4. Click **Next** in the installation wizard welcome; see Figure 3-8 on page 55.

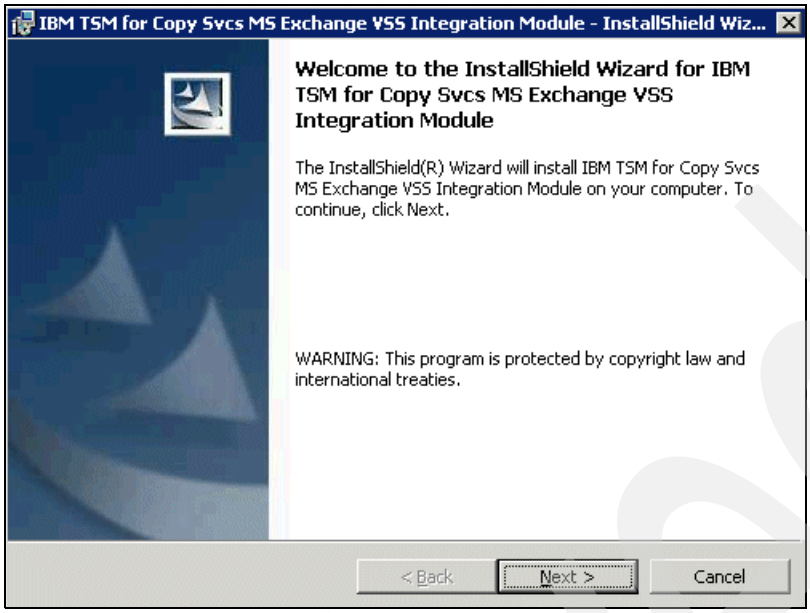


Figure 3-8 InstallShield Wizard welcome

5. Accept the license agreement, and click **Next**.
6. On the next window, click **Install** to start the installation.

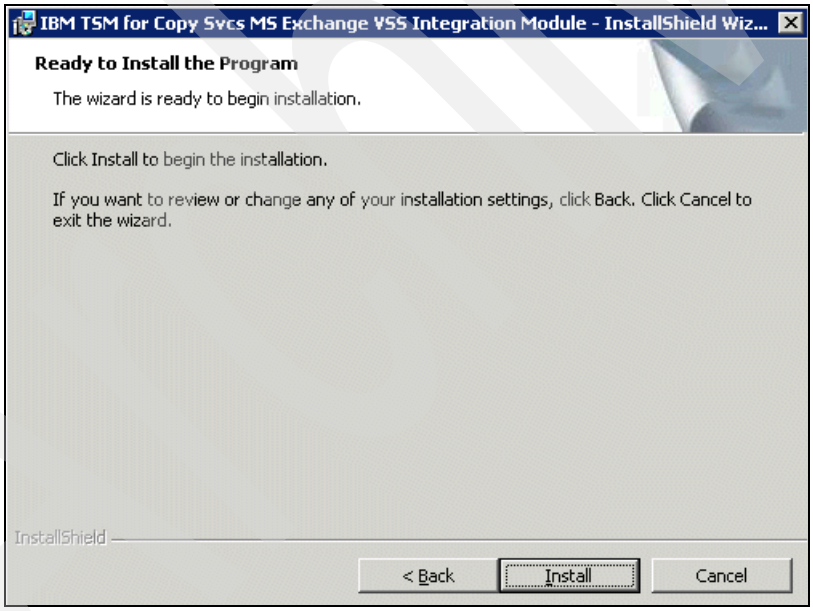


Figure 3-9 Ready to begin installation

7. The installation will complete - click **Finish** when done.

Install Hardware Devices Snapshot Integration Module

If you want to use the Instant Restore feature (currently available only with SAN Volume Controller), you must also install the Hardware Devices Snapshot Integration Module. To do this, run X:\tsmcli\x32\plugin\setup (where X is your CD-ROM drive letter). The first screen is shown in Figure 3-10 on page 56, and the subsequent steps are almost identical to those listed in “Install MS Exchange VSS Integration Module” on page 54.

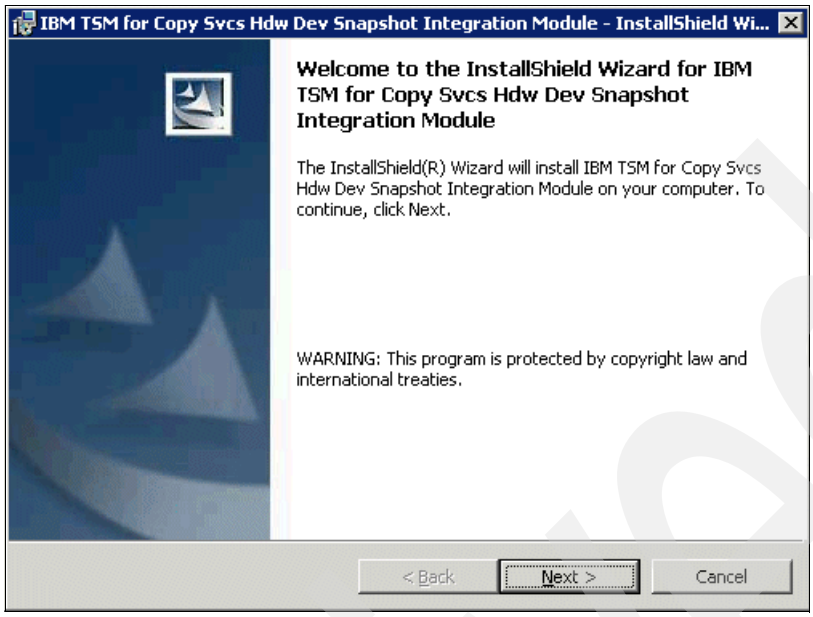


Figure 3-10 InstallShield wizard welcome

3.2.7 Configure the option and config files

Here we have to create or modify various options files to enable the communication.

Create a local DSMAgent option file on REDBOOK2

The Exchange node requires a Tivoli Storage Manager backup-archive client node (DSMAgent) with an associated options file (known here as the DSMAgent option file). By default, and in a single Exchange server configuration, this is the standard name dsm.opt, in the backup-archive client installation directory (default c:\Program Files\Tivoli\TSM\baclient). If you are not running in a clustered environment, you can customize and use this file directly, because you have only one local DSMAgent.

If you are using clustered Exchange servers, then each cluster member requires a Tivoli Storage Manager backup-archive client node (DSMAgent) with an associated options file (DSMAgent option file).

Since we ran in a clustered environment, we created a local DSMAgent configuration file for each of the two Exchange cluster nodes. We placed both files on a shared disk, rather than in the default installation directory, in order to improve the configuration structure and management. This section shows the DSMAgent option file on both REDBOOK2, then on REDBOOK3, which were our cluster nodes. If you have only a single Exchange server (non-clustered), then only configure the file on that server.

As mentioned before, the DSMAgents are Tivoli Storage Manager nodenames. You need to configure the option file (shown here), and later the CAD and the Remote Agent services.

Example 3-3 shows our DSMAgent option file, called dsm_agent_a.opt on REDBOOK2. It references our Tivoli Storage Manager server, and our associated local nodename, REDBOOK_VSS_A, as defined in Example 3-2 on page 51.

Special notes for a clustered environment: The parameter VSSALTSTAGINGDIR in the DSMAgent option file is required *only* in a clustered environment when local VSS backups will be made. The parameter is used to specify a location to store VSS manager files on a shared volume. It should point to a shared drive that does not contain any Exchange objects.

Our example also shows the use of the TCPCLIENTAddress parameter; this is normally only necessary in a clustered environment, or one where the client has multiple IP addresses. In our clustered environment, we set TCPCLIENTAddress to the IP address of the Exchange virtual resource (RB1EVS in our configuration; see Table 3-1 on page 45), rather than the individual REDBOOK2 or REDBOOK3 IP addresses.

Example 3-3 Backup/archive client options file on REDBOOK2: E:\tsmdata\dsm_agent_a.opt

```
commmethod      tcpip
tcpport          1500
vssaltstagingdir e:\tsmvssdir
TCPServeraddress zealot
TCPCLIENTADDRESS 9.43.238.222
Nodename redbook_vss_a
PASSWORDACCESS GENERATE
MANAGEDSERVICES WEBCLIENT
```

Create a DSMAgent BA GUI shortcut on the Start menu

Because we did not use the standard client options file (dsm.opt), we needed a new shortcut to the backup-archive GUI client which would point to our new options file, dsm_agent_a.opt. This is only necessary if you are *not* using the default backup-archive client options file (C:\Program Files\Tivoli\tsm\baclient\dsm.opt).

We created a shortcut, as shown in Figure 3-11 on page 58, specifying the target field as:

```
"C:\Program Files\Tivoli\TSM\baclient\dsm.exe"
-optfile=E:\tsmdata\dsm_agent_a.opt
```

We named the shortcut BA Client GUI redbook_vss_a.

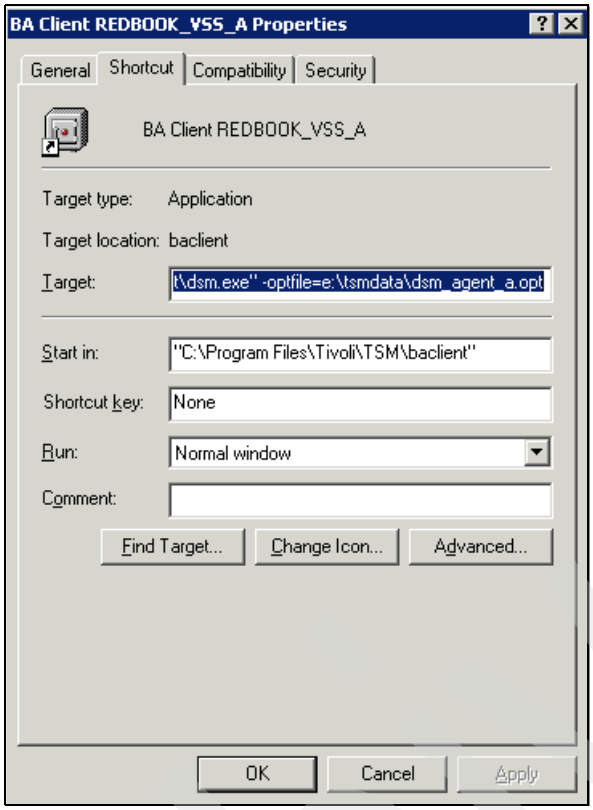


Figure 3-11 Shortcut for GUI, point to correct options file

We launched the BA Client GUI using the shortcut just created in order to store the encrypted password for this node in the registry, because PASSWORDACCESS generate is specified in the options file. This ensured that we did not have to always enter the password when running the GUI.

In your case, if you do not want to create the BA GUI shortcut, you can also store the encrypted password using the command line:

```
C:\Program Files\Tivoli\TSM\baclient>dsmc query session
-optfile=E:\tsmdata\dsm_agent_a.opt
```

Create a local DSMAgent option file on REDBOOK3

Example 3-4 shows the option file we used for the local DSMAgent on REDBOOK3. It is similar to the one already created on REDBOOK2, but this time we specified the node redbook_vss_b. The VSSALTSTAGINGDIR and TCPCLIENTADDRESS are the same as for REDBOOK2.

Example 3-4 Backup/archive client options file on REDBOOK3: `E:\tsmdata\dsm_agent_b.opt`

```
commmethod      tcpip
tcpport          1500
vssaltstagingdir e:\tsmvssdir
TCPServeraddress zealot
TCPCLIENTADDRESS 9.43.238.222
Nodename redbook_vss_b
PASSWORDACCESS GENERATE
MANAGEDSERVICES WEBCLIENT
```

Create a DSMAgent shortcut on the Start menu on REDBOOK3

We created a similar shortcut to the one created on REDBOOK2, since we used a different options file. The target field was:

```
C:\Program Files\Tivoli\TSM\baclient\dsm.exe
-optfile=E:\tsmdata\dsm_agent_b.opt
```

The shortcut was called BA Client GUI redbook_vss_b.

We launched the BA Client GUI using the shortcut just created in order to store the encrypted password for this node in the registry, since PASSWORDACCESS generate is specified in the options file. This ensured that we did not have to always enter the password when running the GUI.

In your case, if you do not want to create the BA GUI shortcut, you can also store the encrypted password using the command line:

```
C:\Program Files\Tivoli\TSM\baclient>dsmc query session
-optfile=E:\tsmdata\dsm_agent_b.opt
```

Create a remote DSMAgent option file on REDBOOK1

This step is only required if you will use an offloaded backup server.

We needed to configure a remote DSMAgent file on our offloaded backup server, REDBOOK1. We could edit the standard client options file, as shown in Example 3-5, and therefore we did not need a new shortcut.

Example 3-5 Backup-archive client options file on REDBOOK1 - C:\Program Files\Tivoli\TSM\baclient\dsm.opt

```
commmethod      tcpip
tcpport          1500
TCPServeraddress zealot
TCPCLIENTADDRESS 9.43.238.111
Nodename redbook_offload
MANAGEDSERVICES WEBCLIENT
PASSWORDACCESS GENERATE
```

We launched the BA Client GUI using the shortcut just created in order to store the encrypted password for this node in the registry, because PASSWORDACCESS generate is specified in the options file. This ensured that we did not have to always enter the password when running the GUI.

You can also store the encripted password using the command line:

```
C:\Program Files\Tivoli\TSM\baclient>dsmc query session
```

Note: The -optfile option is not needed this time because we used the default name and path for the option file.

Create a Data Protection for Exchange option file

We now need to create the Data Protection for Exchange option file. In a non-clustered environment, you can use the standard name and location, which is c:\Program Files\Tivoli \TSM\ TDPExchange\dsm.opt.

In a clustered environment, this must be accessible by both nodes - therefore, instead of using the default name and directory, we specify a different file name, and save it on a shared disk (E drive in this instance) which is failed over with the Exchange instance.

Our Data Protection for Exchange option file is shown in Example .

Example 3-6 TData Protection for Exchange option file: E:\tsmdata\dsm_exch.opt

```
NODename          redbook_exchange
CLUSTERnode       yes
COMPRESSIon       Off
PASSWORDAccess    Generate
COMMMethod        TCPip
TCPPort           1500
TCPServeraddress  zealot
TCPCLIENTADDRESS  9.43.238.222
TCPWindowsize     63
TCPBuffSize       32
SCHEDMODE         Prompted
```

Note that the nodename is REDBOOK_EXCHANGE, which was the nodename defined for backing up Exchange in Example 3-2 on page 51.

Our option file, since we were in a clustered environment, also specified CLUSTERnode yes; the CLUSTERnode options is only required when in a clustered environment. Since we were in a clustered environment, we also specified the TCPCLIENTADDRESS pointing to our Exchange resource virtual address, as listed in Table 3-1 on page 45.

Create Data Protection for Exchange configuration file

The default Data Protection for Exchange configuration file is C:\Program Files\Tivoli\TSM\ TDPExchange\tdpexc.cfg. If you are not running in a clustered environment, then edit this file.

In our clustered environment, we previously configured a unique local DSMAgent option file for each node in the cluster. Similarly, we also needed to configure a Data Protection for Exchange unique configuration file for each node in the cluster. These files were almost identical, except that the LOCALDSMAgentnode parameter pointed to the corresponding local DSMAgent on each node.

In this way, the correct configuration file can be used, depending on which node is currently hosting the Exchange instance. This file can be placed in the standard location “C:\Program Files\Tivoli\TSM\ TDPExchange\tdpexc.cfg or in a shared location for better management purposes. If you choose to use a shared location, use a naming convention such as X:\ tsmdata\ tdpexc_<hostname>.cfg, where the X is a shared drive in the Exchange cluster group. We used a shared location and naming convention, as shown in Example 3-7 on page 61 and Example 3-8 on page 61.

Because we used an offloaded backup server, we specified the REMOTEDSMAgent node pointing to our offloaded node, which was called REDBOOK_OFFLOAD. This parameter is only required if you are using an offloaded backup server.

This configuration file will also contain the VSSPOLICY statements. As described in 2.5.1, “Management of VSS snapshot backups in Tivoli Storage Manager” on page 34, VSSPOLICY statements in the Data Protection for Exchange configuration file are used to bind VSS backups to specific Tivoli Storage Manager Server management classes. The policy bindings are matched from the bottom up.

*Example 3-7 E:\ tsmdata\ tdpexc_**REDBOOK2**.cfg*

```
BUFFers     3
BUFFERSIze     1024
LOGFile     tdpexc.log
LOGPrune     60
MOUNTWait     Yes
TEMPLOGRestorepath
LASTPRUNEDate     08/02/2006 09:44:15
*********************************************************************
*          Server   Storage Group Name  BU Type  BU Dest.  Mgmt Class
*          ------   ------------------  -------  -------   ----------
VSSPOLICY  *        *                   FULL      TSM       REDBOOK_VSS_FULL
VSSPOLICY  *        *                   COPY      TSM       REDBOOK_VSS_COPY
VSSPOLICY  *        *                   FULL      LOCAL     REDBOOK_VSS_LOCAL
VSSPOLICY  *        *                   COPY      LOCAL     REDBOOK_VSS_LOCAL
*********************************************************************
BACKUPMETHod     VSS
LANGuage     ENU
*BACKUPDESTination     LOCAL
LOCALDSMAgentnode redbook_vss_a
REMOTEDSMAgentnode     REDBOOK_OFFLOAD
```

*Example 3-8 E:\ tsmdata\ tdpexc_**REDBOOK3**.cfg*

```
BUFFers     3
BUFFERSIze     1024
LOGFile     tdpexc.log
LOGPrune     60
MOUNTWait     Yes
TEMPLOGRestorepath
LASTPRUNEDate     08/02/2006 09:44:15
*          Server   Storage Group Name  BU Type  BU Dest.  Mgmt Class
*          ------   ------------------  -------  -------   ----------
VSSPOLICY  *        *                   FULL      TSM       REDBOOK_VSS_FULL
VSSPOLICY  *        *                   COPY      TSM       REDBOOK_VSS_COPY
VSSPOLICY  *        *                   FULL      LOCAL     REDBOOK_VSS_LOCAL
VSSPOLICY  *        *                   COPY      LOCAL     REDBOOK_VSS_LOCAL
*********************************************************************
BACKUPMETHod     VSS
LANGuage     ENU
*BACKUPDESTination     LOCAL
LOCALDSMAgentnode redbook_vss_b
REMOTEDSMAgentnode     REDBOOK_OFFLOAD
```

Figure 3-12 on page 62 summarizes the various configuration files in a clustered environment.

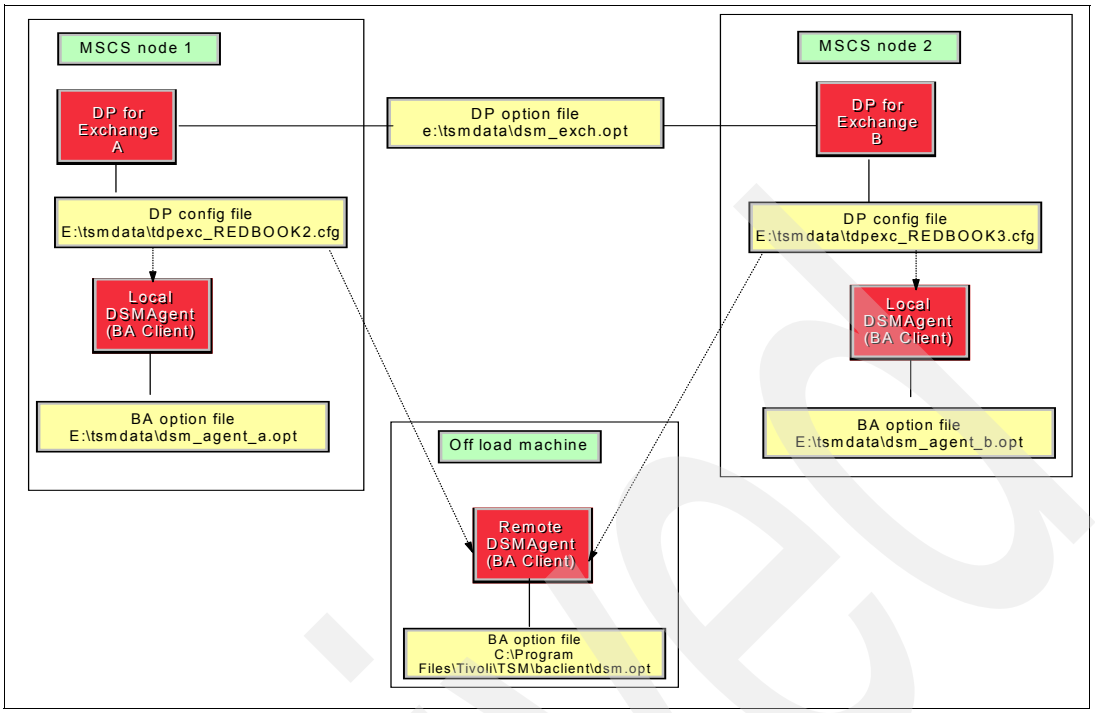


Figure 3-12 Summary of configuration files in a clustered Exchange environment

Figure 3-13 summarizes the various configuration files in a non-clustered environment.

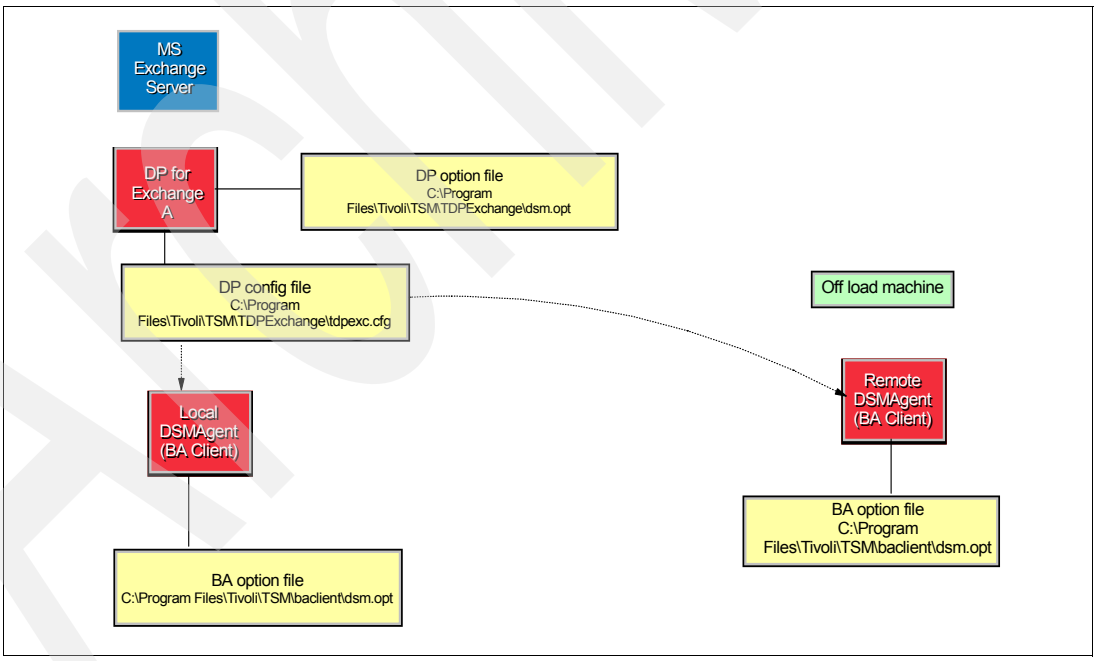


Figure 3-13 Summary of configuration files in a non-clustered Exchange environment

Create a Data Protection for Exchange GUI shortcut

In order to launch the Data Protection for Exchange backup and restore operations with the GUI, you can configure a shortcut for the tdpexc.exe. This is not required in a non-clustered environment, unless you have used some non-default option or configuration files.

In our clustered environment, we created an identical shortcut on each cluster node as follows:

- In a clustered environment you need to specify the Exchange virtual server name with the /excserver parameter. You can find it using the Exchange System Manager, as shown in Figure 3-14 - our virtual server is called RB1EVS.

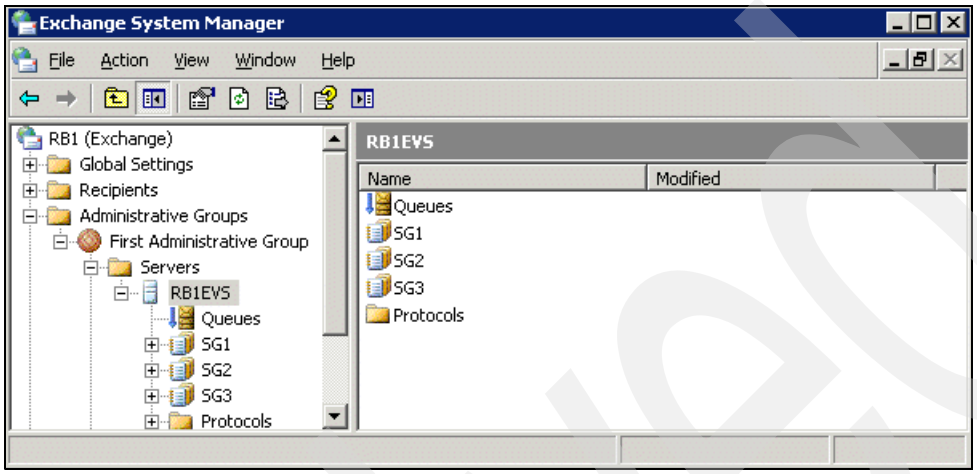


Figure 3-14 Exchange System Manager

- In a clustered environment, the Data Protection for Exchange option file is located on a shared disk (instead of the standard installation directory location), therefore you need to specify this file with the /tsmoptfile parameter.
- If you chose to store the Data Protection for Exchange configuration files in a shared location (as we did in "Create Data Protection for Exchange configuration file" on page 60), using a naming convention like X:\ tsmdata\ tdpexc_<hostname>.cfg, then you need to specify the configuration file with the /configfile parameter. Using the suggested naming convention you can specify this parameter like this, so that the appropriate host name will be used, depending on where the Exchange instance is currently hosted.

  ```
  /configfile=X:\tsmdata\tdpexc_%COMPUTERNAME%.cfg.
  ```

To create a suitable shortcut in our clustered environment, on the node which is currently hosting the Exchange instance, we created a shortcut with the following target:

```
"C:\Program Files\Tivoli\TSM\TDPExchange\tdpexc.exe"
/tsmoptfile=e:\tsmdata\dsm_exch.opt /excserver=RB1EVS
/configfile=e:\tsmdata\tdpexc_%COMPUTERNAME%.cfg
```

We called the shortcut TDP redbook_exchange, as shown in Figure 3-15.

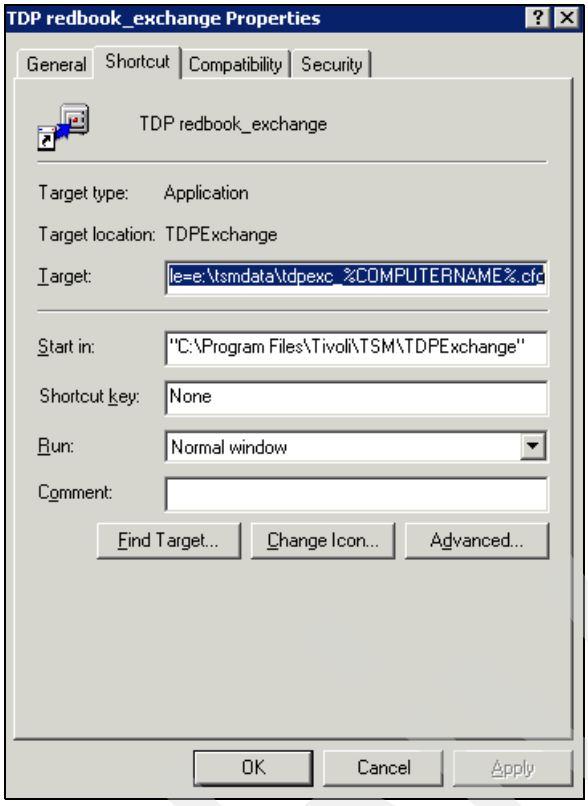


Figure 3-15 Shortcut to run Data Protection for Exchange

We launched the TDP GUI using the shortcut just created in order to store the encrypted password from this node in registry. Then we moved the Exchange cluster group to the other node and copied (or you can create) the respective shortcut there. We launched the TDP GUI using the shortcut just created in order to store the encrypted password from this second node in the registry.

3.2.8 Configure the CAD and remote agent services

Now we needed to configure the client acceptor (CAD) and remote agent services for the local DSMAgent node (or nodes in a cluster environment) and remote DSMAgent node in order to permit communication between the Data Protection for Exchange and backup-archive client and the Tivoli Storage Manager server.

We performed the following steps on the Exchange server (this would be done on both cluster nodes, in an MSCS environment). If you are using an offloaded server, perform the configuration on that server too.

You can use either the Backup Archive setup wizard or **`dsmcutil`** to perform these tasks.

1. From the backup/archive GUI, select **Utilities** → **Setup Wizard**.
2. The wizard starts, as shown in Figure 3-16.
3. Select **Help me configure the TSM Web Client** and click **Next**.

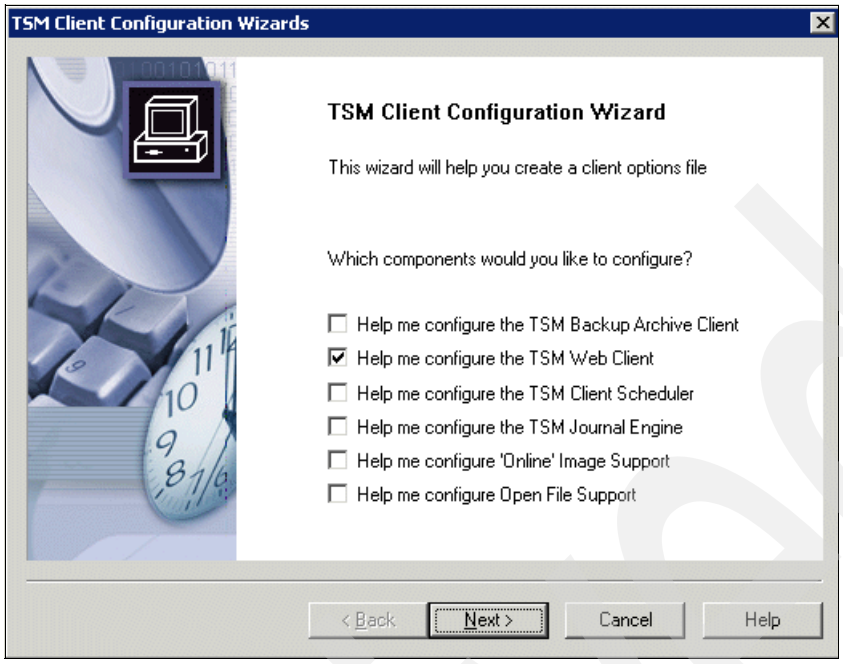


Figure 3-16 Client configuration wizard

4. Select **Install a new Web Client agent** and click **Next**; see Figure 3-17.

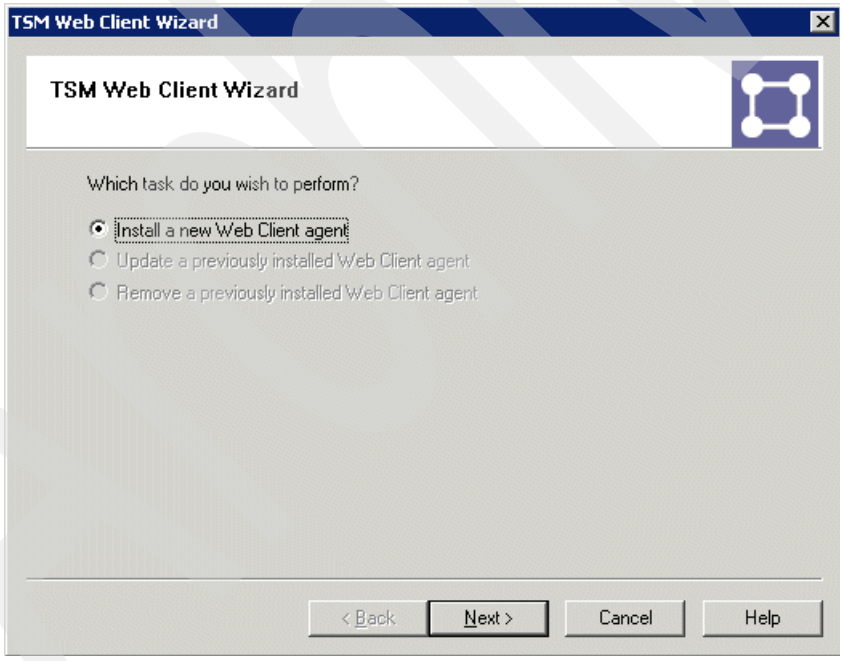


Figure 3-17 Select Install a new Web Client agent

5. As shown in Figure 3-18, enter a name for the CAD service and click **Next**. We accepted the default.

> **Note:** The CAD service name should be the same in all cluster nodes in order to properly be started by a cluster generic service.

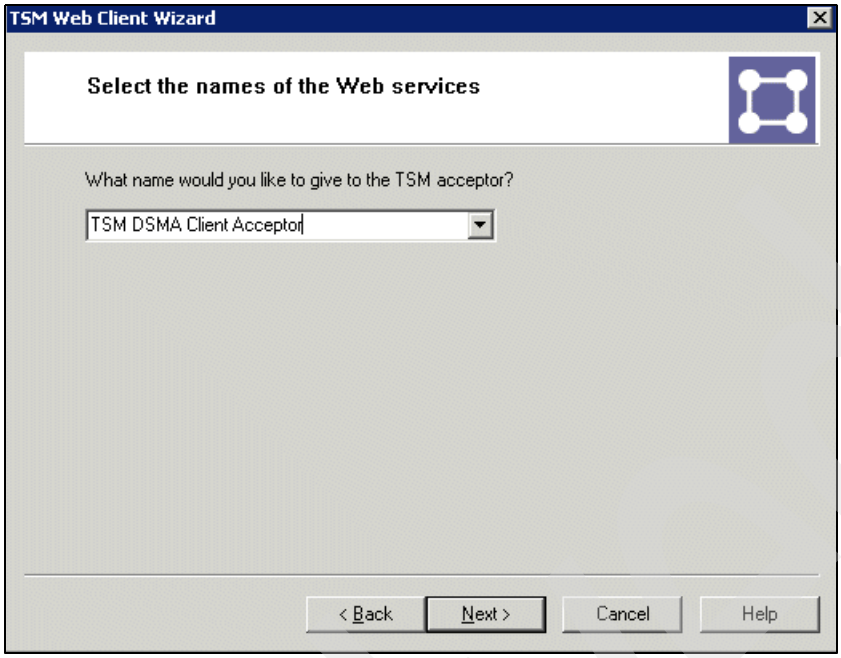


Figure 3-18 Choose CAD service name

6. As shown in Figure 3-19 on page 66, browse and select the DSMAgent option file created in “Create a local DSMAgent option file on REDBOOK2” on page 56, “Create a local DSMAgent option file on REDBOOK3” on page 58, and “Create a remote DSMAgent option file on REDBOOK1” on page 59, depending on where you are performing the configuration.

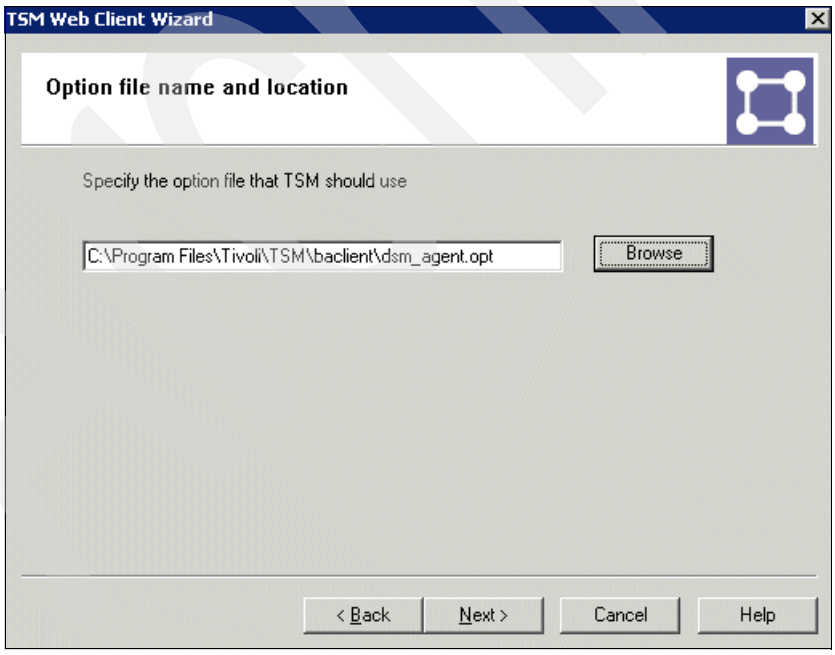


Figure 3-19 Specify the backup-archive client option file

7. Choose the HTTP port and click **Next**. Normally, you can accept the default, as shown in Figure 3-20.

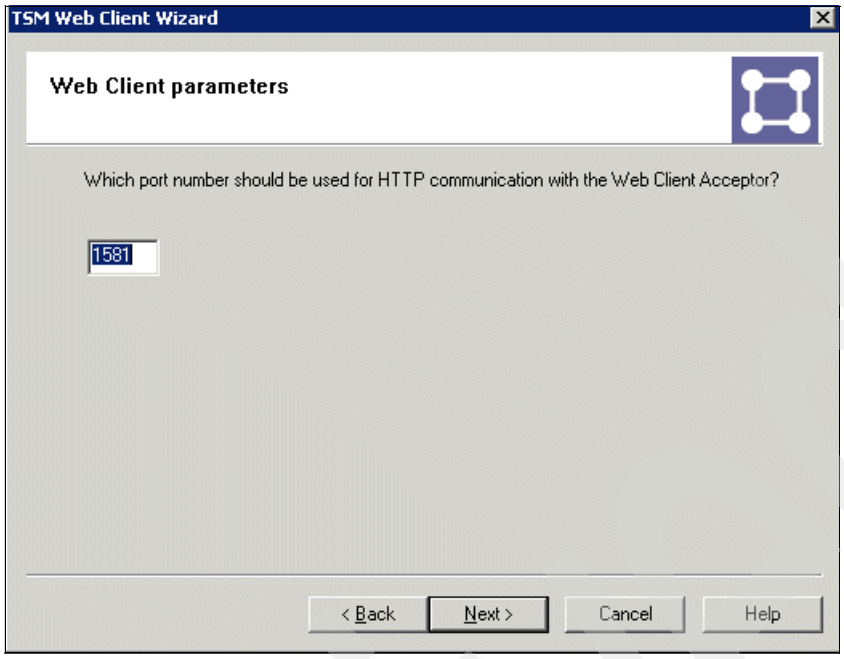


Figure 3-20 HTTP port

8. As shown in Figure 3-21 on page 67, fill the nodename and password fields and click **Next**. This is your Tivoli Storage Manager backup-archive client nodename and password as defined in Example 3-2 on page 51.

   Complete the field appropriately for each system (for example, in our case we specified on REDBOOK2 - REDBOOK_VSS_A, REDBOOK3 - REDBOOK_VSS_B, and REDBOOK_OFFLOAD for the offloaded server).

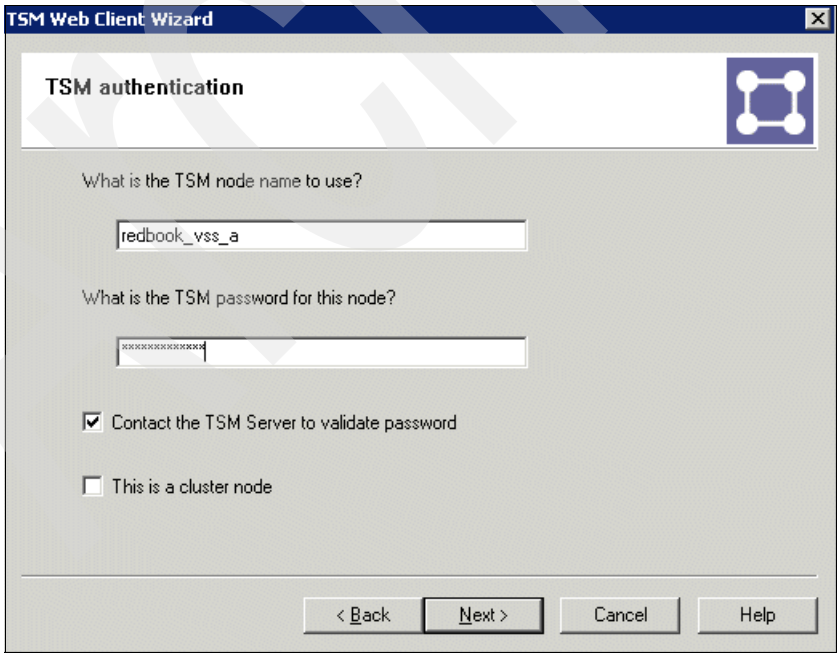


Figure 3-21 Specify the client nodename and password

9. The CAD should be started manually. We accepted the defaults in Figure 3-22 to use the System account. However, to use another Local Administrator account, enter the account name and password. Click **Next**.

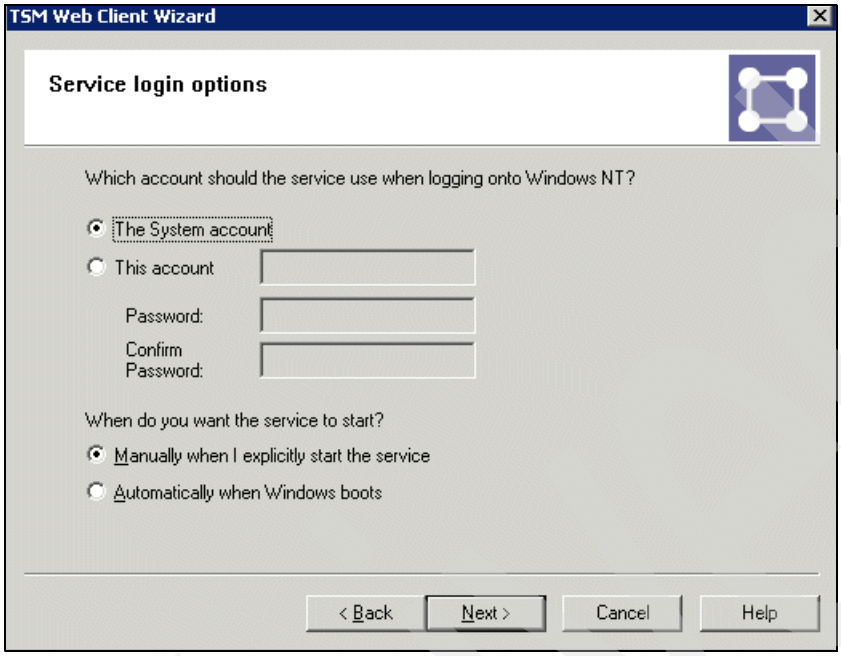


Figure 3-22 Service login options

10. Choose the Remote Agent service name and click **Next**. We accepted the default in Figure 3-23 on page 68.

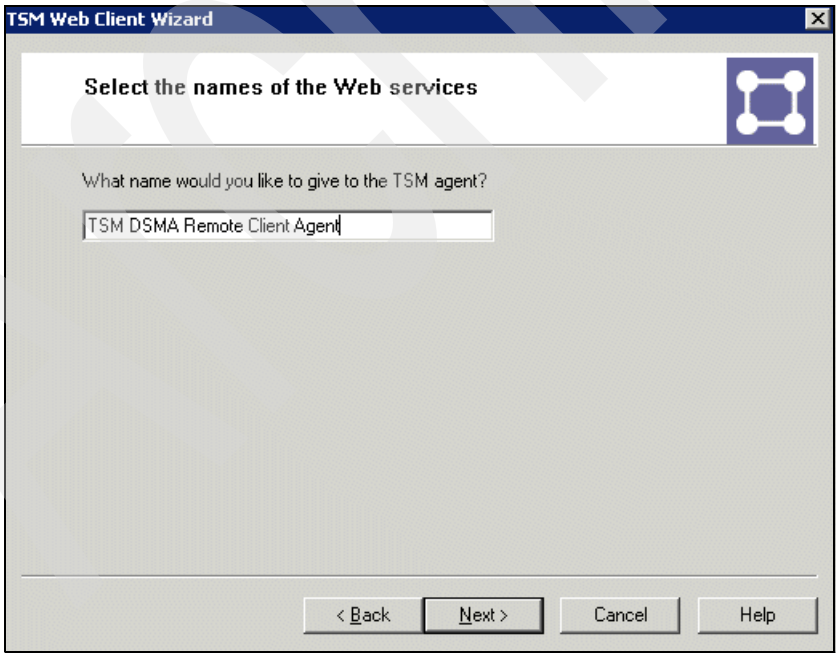


Figure 3-23 Remote Client Agent name

11. Select **No** to revoke the remote access privileges to the Web Client, as shown in Figure 3-24, and click **Next**.

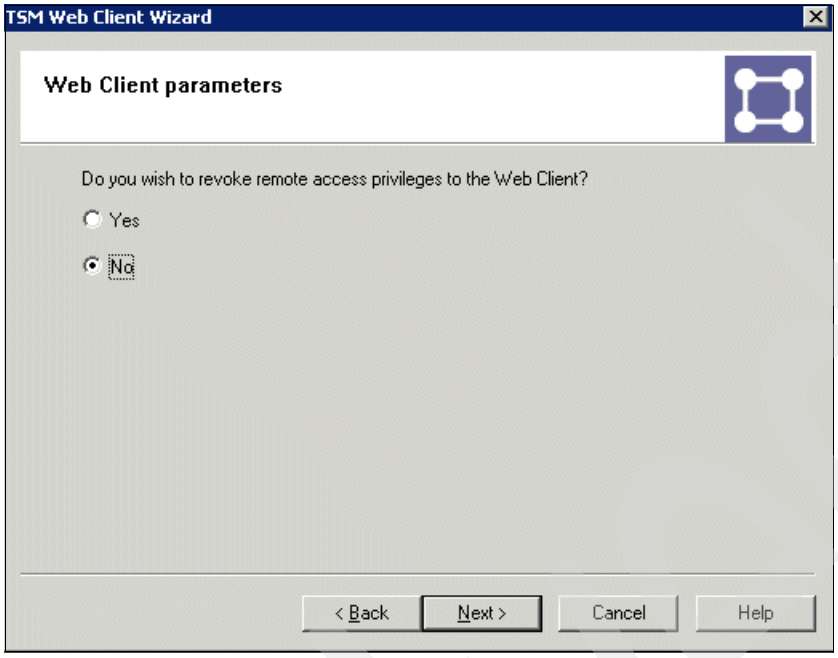


Figure 3-24 Web Client parameters

- On Figure 3-25 on page 69, select **No** so that the service does not start automatically, and click **Next** (however, if you are doing this on an offloaded server, select Yes).

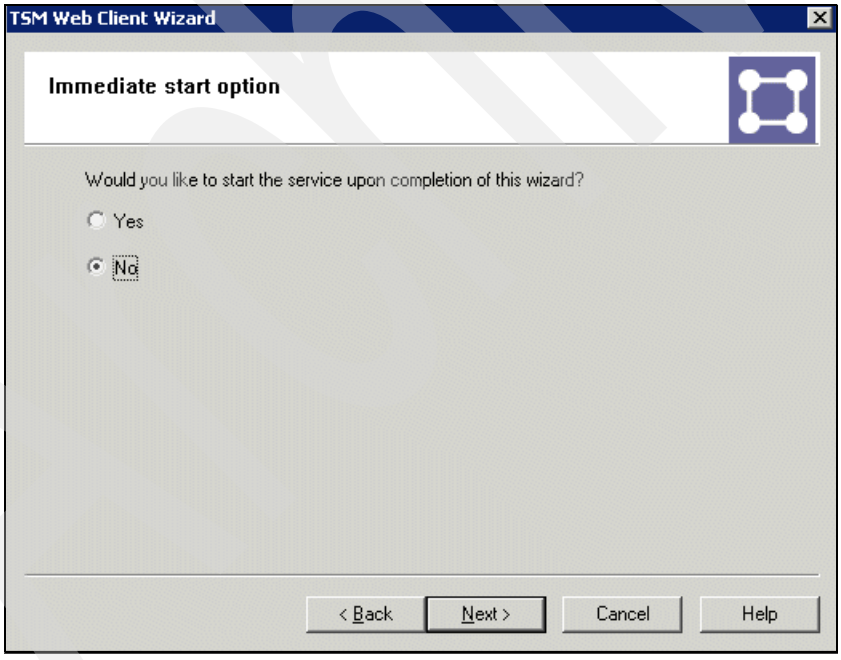


Figure 3-25 Immediate start option

12. On the completion screen shown in Figure 3-26, click **Finish**.

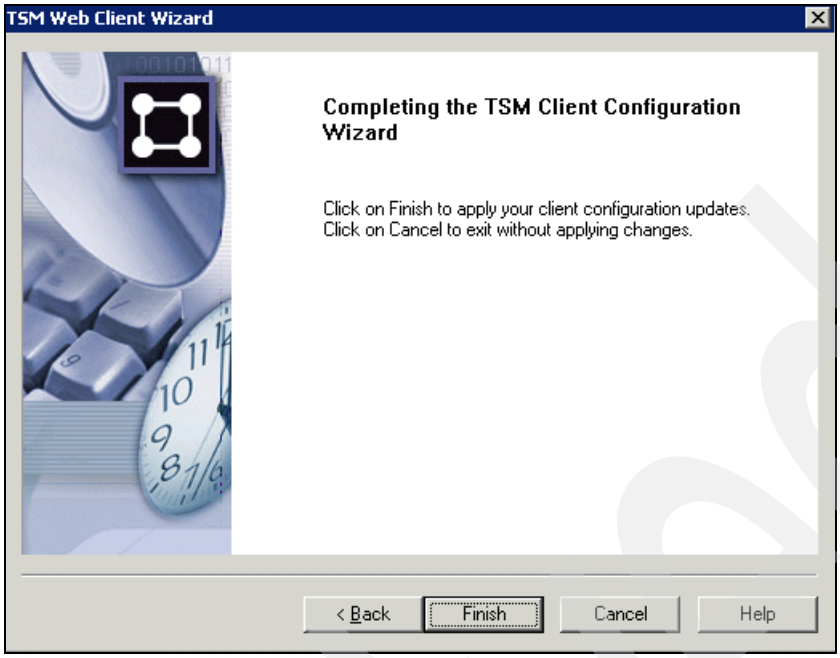


Figure 3-26 Complete the wizard

If you are using an offload server, you must also create the CAD and Remote Agent on that system. In this case the offload machine's CAD service should be configured to start automatically, by selecting Yes in Figure 3-25 on page 69.

3.2.9 Create a cluster service to manage the CAD service

In a clustered environment, you need to create a cluster service to properly start the CAD service in the node which is hosting the Exchange instance. You may also run the CAD as a local resource; however, we encountered problems doing this in our lab environment. Therefore, we recommend running the CAD as a cluster resource.

To create a cluster service for the CAD:

1. Launch the Cluster Administrator. On the Exchange cluster group, (RB1EVS, in our case) right-click and select **New** → **Resource**, as shown in Figure 3-27.

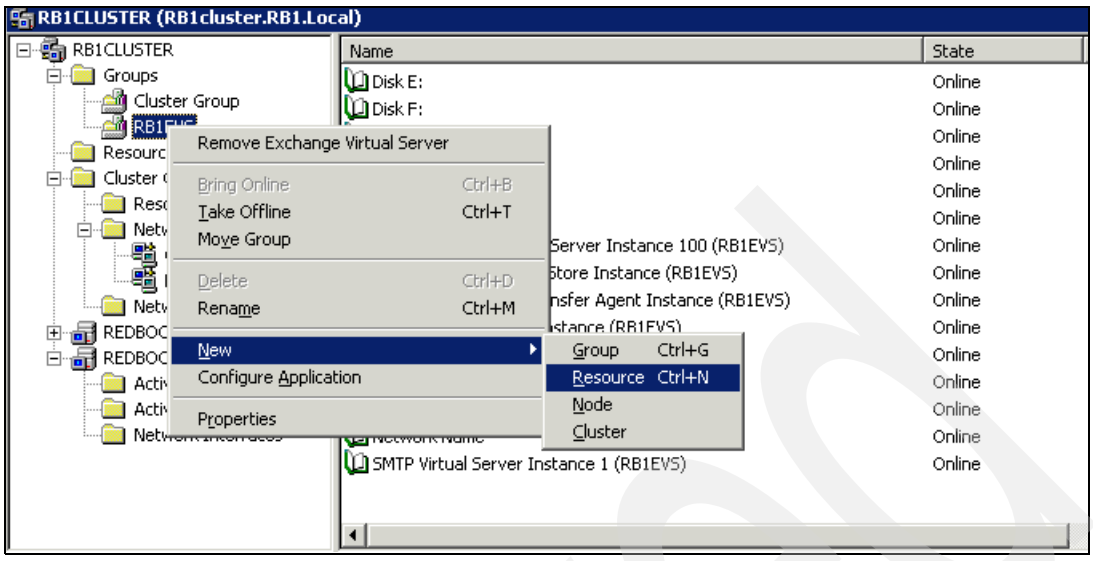


Figure 3-27 Create new cluster resource

2. Choose a name for the resource, and select the Resource Type as **Generic Service**, as shown in Figure 3-28. Click **Next**.

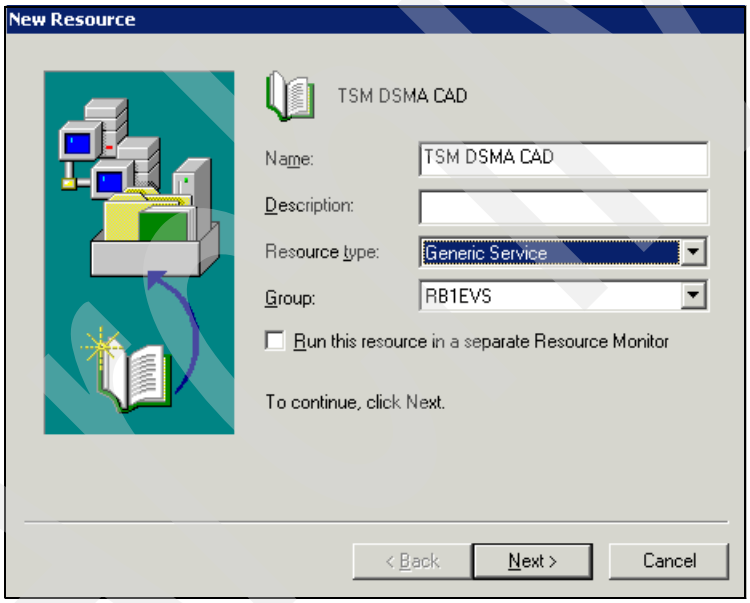


Figure 3-28 New resource

- As shown in Figure 3-29, select both cluster nodes as possible owners and click **Next**.

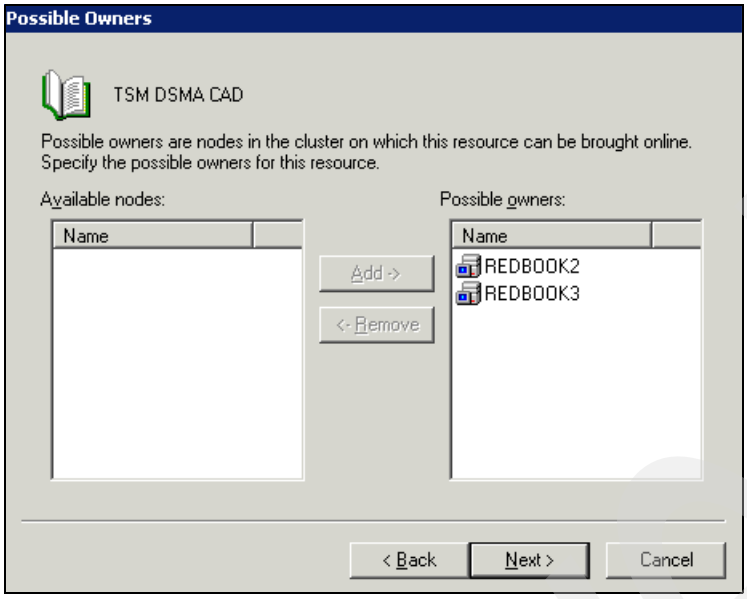


Figure 3-29 Select resource possible owners

3. Select the Exchange Information Store Instance as a resource dependence, as shown in Figure 3-30, and click **Next**.

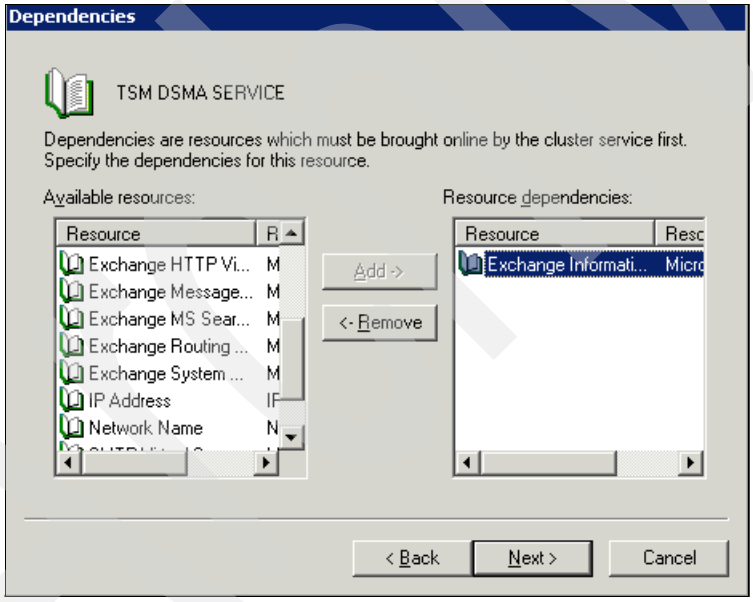


Figure 3-30 Resource dependence name

- As shown in Figure 3-31 on page 73, enter the same CAD service name as you specified in Figure 3-18 on page 66.

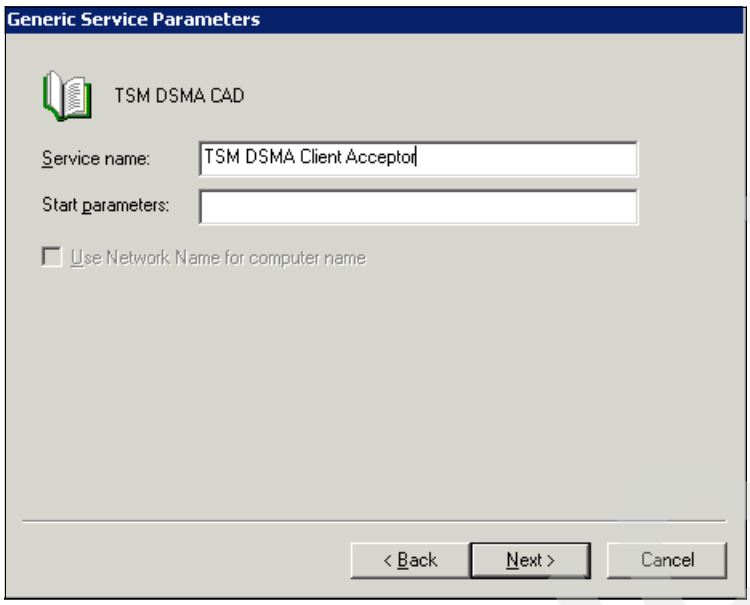


Figure 3-31 Specify the CAD service name

4. Click **Finish** on Figure 3-32.

> **Important:** Do *not* add any registry key. The DSMAgents are using different nodenames on each cluster node, therefore you cannot propagate the encrypted password.

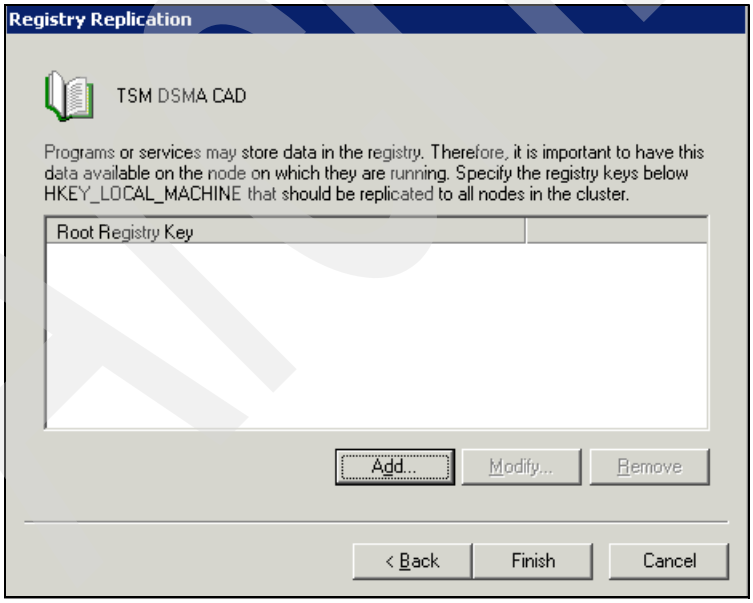


Figure 3-32 Registry Replication

5. Back on the Cluster Administrator, right-click the resource you just created and select **Properties**, as shown in Figure 3-33 on page 74.

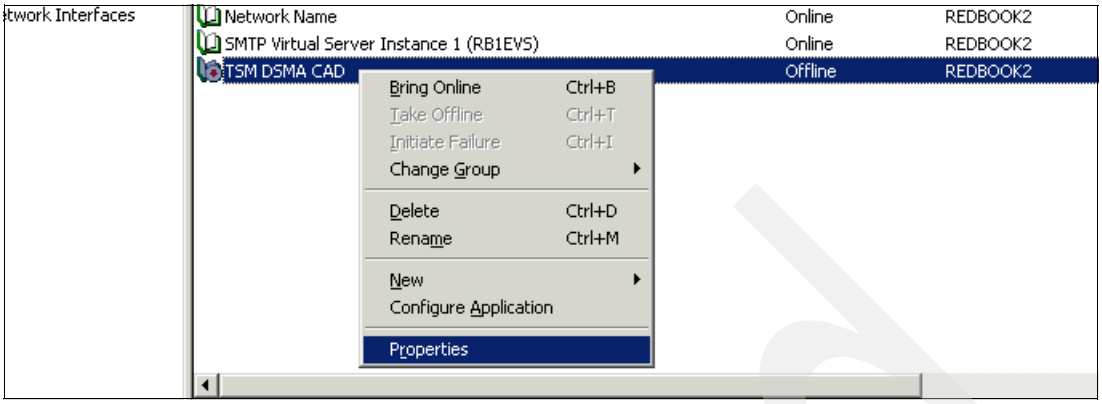


Figure 3-33 Select properties of new service

6. Select the **Advanced** tab, deselect **Affect the group** and click **OK**, as shown in Figure 3-34.

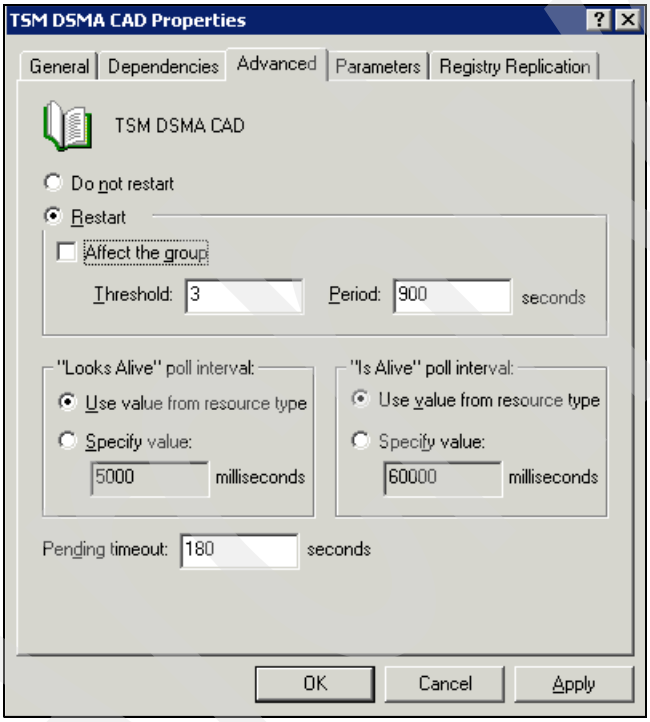


Figure 3-34 Resource properties

7. Bring the resource online by right-clicking and selecting **Bring online**.

3.2.10 Configure the proxy node definitions

Data Protection for Exchange VSS support uses the Tivoli Storage Manager proxy node capability introduced in Tivoli Storage Manager V5.3.

We used the **`grant proxynode`** command to associate the target node which owns the data with the agent nodes acting on behalf the target node.

In Example 3-9, the first two **`grant proxynode`** commands allow the local DSMAgents REDBOOK_VSS_A, and REDBOOK_VSS_B to act as proxy nodes for the Exchange node

REDBOOK_EXCHANGE. This allows them to send VSS backups to Tivoli Storage Manager. If you are not in a cluster environment, you only need one **grant proxynode** command for your single local DSMAgent.

The third **grant proxynode** command grants authority to the remote DSMAgent (offload server) to act on behalf of the Exchange node. This statement is only needed if you are doing offloaded backup.

Example 3-9 Configure proxy nodes

```
grant proxynode target=redbook_exchange agent=redbook_vss_a

grant proxynode target=redbook_exchange agent=redbook_vss_b

grant proxynode target=redbook_exchange agent=redbook_offload
```

3.2.11 Install the Exchange management tools on the offloaded server

If you are using an offloaded backup server, you must install the Microsoft Exchange management tools on that server. This will allow it to verify the snapshot backups made. The management tools are available on the Exchange installation CD. Before installing the management tools, you must first install Microsoft Internet Information Services (IIS) Manager. Consult your Exchange documentation or the following Web site for information about how to install the management tools:

http://www.microsoft.com/technet/prodtechnol/exchange/guides/E2k3AdminGuide/2e1e5993-92b5-4511-9e06-88c6720e311f.mspx?mfr=true

Note: The management tools must be installed at the same level and patch as the Exchange server. In our case, the Exchange server had Service Pack 2 for Exchange, therefore we also had to upgrade the offloaded server with Exchange Service Pack 2.

3.2.12 Add the Exchange Server binary directory to the PATH variable

On all systems (Exchange server, clustered Exchange server and offload server, if used), add the Exchange Server binary directory to the PATH system variable, if it is not already there.

1. Right-click **My Computer** → **Properties** → **Advanced Tab** → **Environment Variables**
2. In System Variables, select the Path variable and click **Edit**.
3. Add C:\Program files\Exchsrvr\bin separated by a semi-colon (;), as shown in Figure 3-35 on page 76.

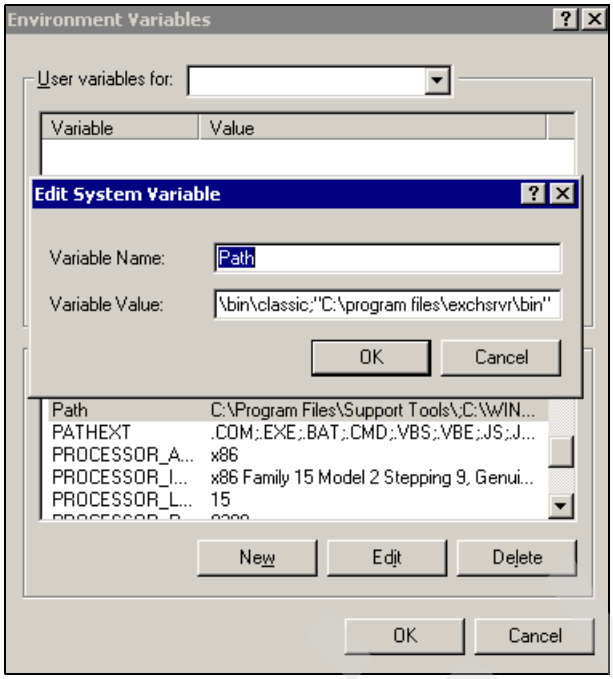


Figure 3-35 Set path

4. Confirm you can run eseutil.exe from the root (C:\) directory.

3.2.13 Installing the hardware provider

The hardware provider installation process is different, depending on your disk hardware vendor. Consult the specific documentation provided with your disk system. As an example, we describe the installation and configuration for our environment using an IBM System Storage DS8000. Note that this hardware provider is also used by the IBM System Storage DS6000 or SAN Volume Controller.

1. Obtain the VSS provider for your storage disk system. Typically you download this from your vendor's Web site. We obtained the DS8000 VSS provider from:

   `http://www-1.ibm.com/support/docview.wss?uid=ssg1S4000372&rs=503`

   Note: At the time of writing, the IBM SVC VSS provider is not yet supported with SVC V4.1. Check the IBM support Web site for SVC to see if this has changed.

2. As a local administrator, run the VSS hardware provider executable.
3. The Welcome window opens, similar to Figure 3-36 on page 77. Click **Next** to continue with the InstallShield Wizard.

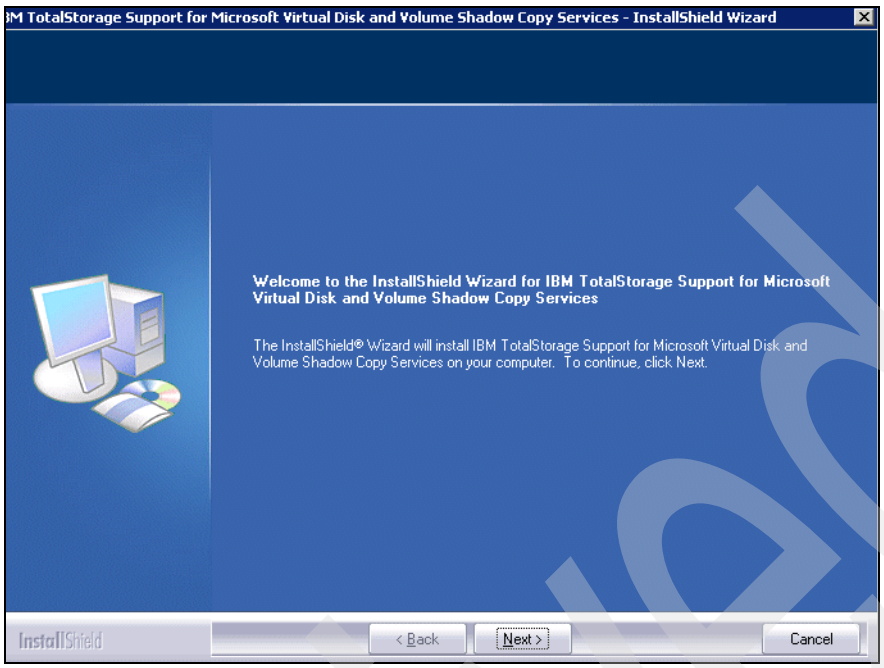


Figure 3-36 DS8000 hardware provider welcome screen

4. The License Agreement window opens. Read the license agreement information, accept it, and click **Next**.
5. Choose the destination location and click **Next** to continue, as shown in Figure 3-37. The default directory is C:\Program Files\IBM\Hardware Provider for VSS-VDS.

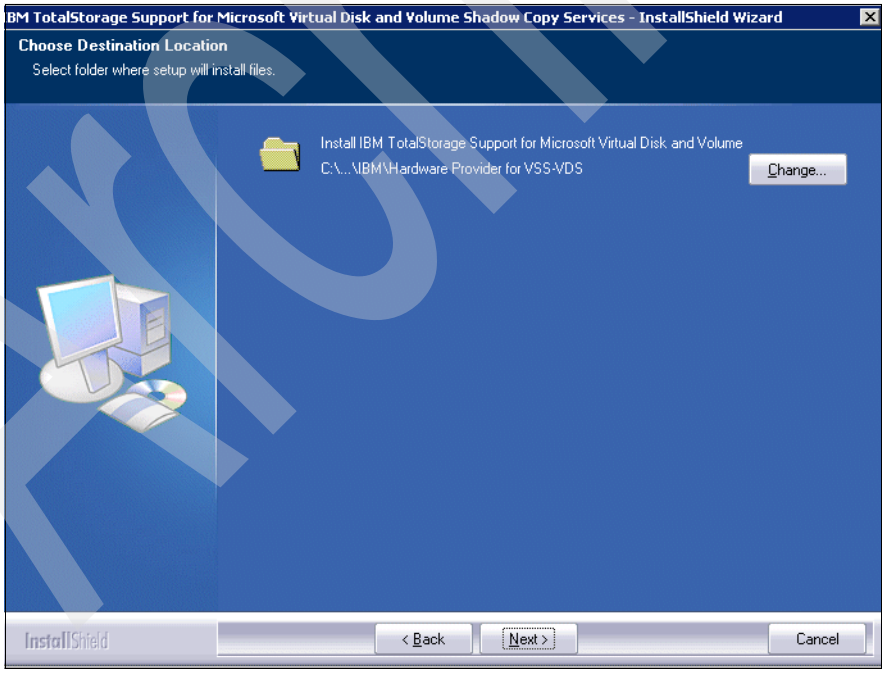


Figure 3-37 Choose destination directory

6. As shown in Figure 3-38 on page 78, select the components to install. For the DS6000 or DS8000, we recommend checking both VSS and VDS support for ESS, as shown. For SVC, you only have to check the VSS for SVC package.

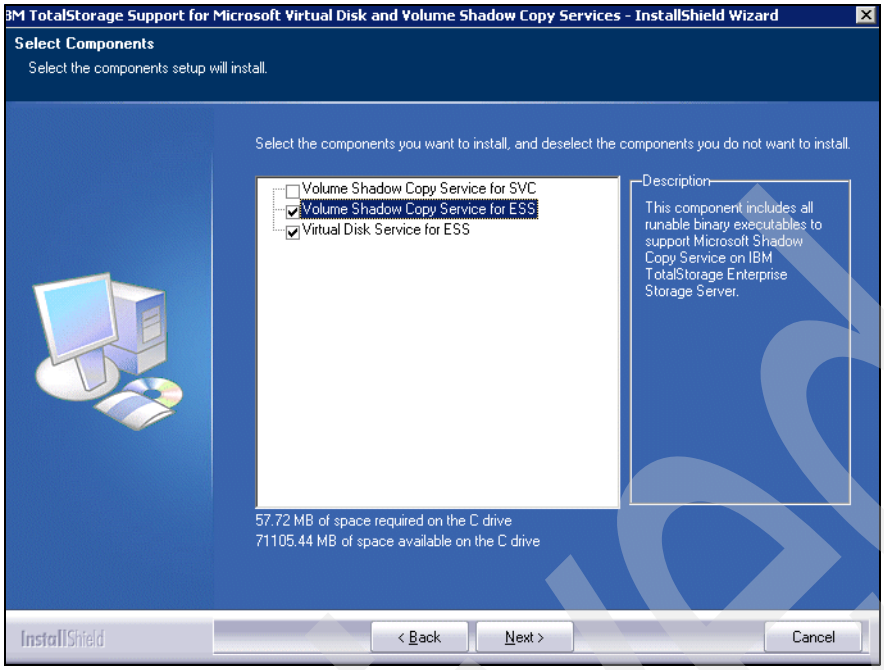


Figure 3-38 Select components

7. Next, specify the location of your CIM Agent. In a DS8000 or DS6000, this will be installed on a system accessible via TCP/IP. You need to obtain from the storage administrator where the CIM Agent is installed, plus the port and a CIM User/password. For an SVC environment, the CIM Agent is installed on the Master Console.

   In our environment, we had already set up a CIM Agent on an external machine in order to integrate the DS8000 Storage Management with other products. We entered the TCP/IP address of the CIM Agent host, communication port, and a CIM User, and clicked **Next** to continue, as shown in Figure 3-39 on page 79. You can choose either the HTTP port or the HTTPS port.

   Important: At the time of writing, SSL/HTTPS cannot be used if you will use SVC Instant Restore. Check the documentation and README to see if this still applies. You may have to disable SSL in the SVC CIMOM. For details on how to do this, see Appendix A, “Disabling SSL in the SVC CIMOM” on page 177.

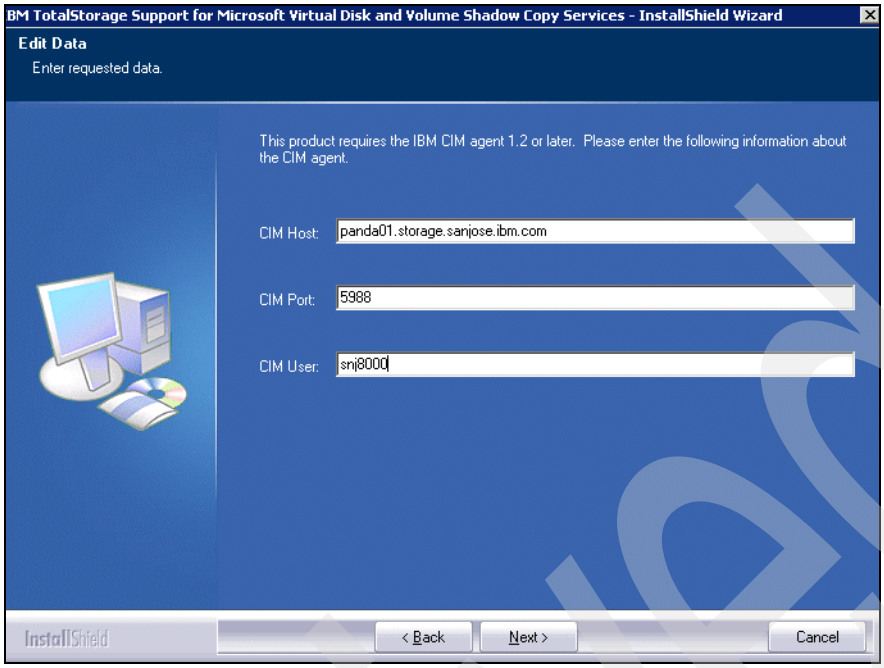


Figure 3-39 CIM host, port and user

8. In Figure 3-40, enter the password for the CIM User, and click **Next**.

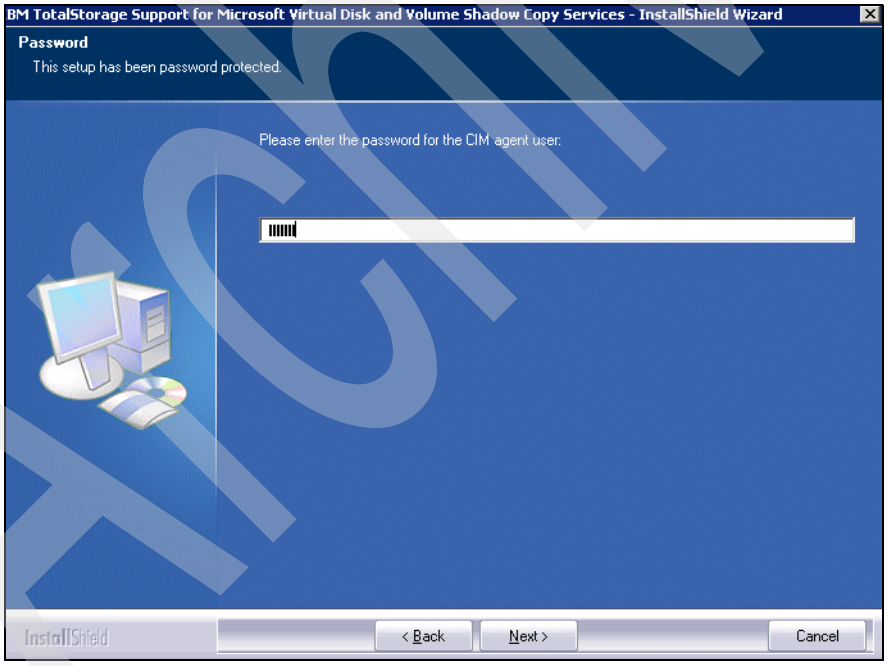


Figure 3-40 Enter CIM user password

9. In Figure 3-41 on page 80, indicate whether you want to use Secure Sockets Layer (SSL) to connect to the CIM agent and click **Next**.

> **Important:** At the time of writing, SSL cannot be used if you will use SVC Instant Restore. Check the documentation and README to see if this is still true.

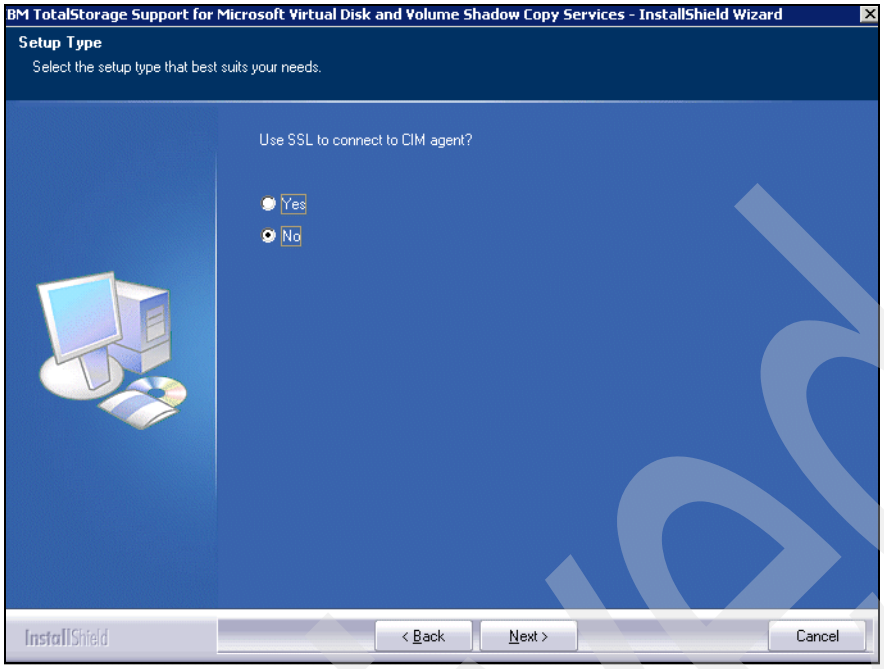


Figure 3-41 Use SSL?

10. On the next screen, you can either go back and change your selections, or click **Install** to begin the installation.
11. When the installation is complete, click **Finish**.
12. Start the IBM TotalStorage Hardware Provider for VSS service via the Windows services applet, as shown in Figure 3-42.

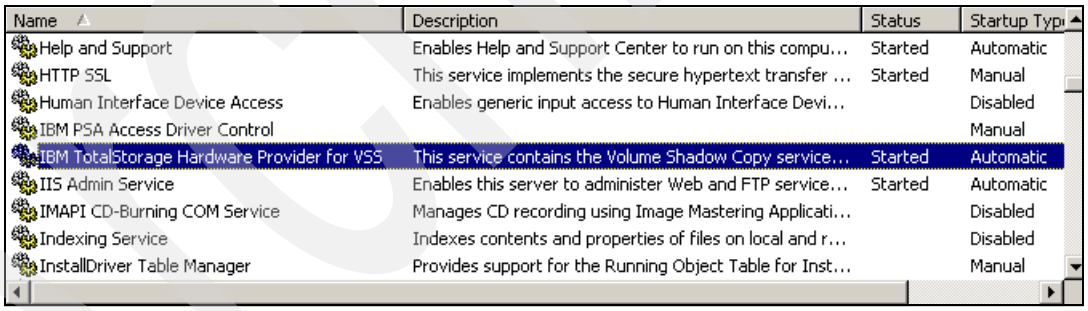


Figure 3-42 Hardware Provider Service started.

Verify CIM configuration parameters

Your VSS provider probably provides some kind of verification command; refer to your hardware provider's documentation for detailed information. For the IBM VSS provider which we installed, we used the **`ibmvcfg`** command in the installation directory to display and alter the CIM configuration.

Note that if you alter any CIM configuration parameters, you will need to restart the IBM TotalStorage Hardware Provider for VSS service for changes to take effect. Example 3-10 shows our VSS configuration.

Example 3-10 ibmvcfg showcfg

```
C:\Program Files\IBM\Hardware Provider for VSS-VDS>ibmvcfg showcfg

cimomHost:                          panda01.storage.sanjose.ibm.com
username (cimom):                   snj8000
namespace:                          \root\ibm
cimomPort:                          5988
usingSSL:                           false
FlashCopyVer:(only applies to ESS)  2
vssFreeInitiator:                   5000000000000000
vssReservedInitiator:               5000000000000001

C:\Program Files\IBM\Hardware Provider for VSS-VDS>
```

Verify the hardware provider

The command **vssadmin** is pre-installed on the Windows 2003 server, and therefore can be used for any hardware provider. The **vssadmin** command has many functions for verifying and configuring a VSS environment. Enter **vssadmin** with no options to see the various options available, as shown in Example 3-11.

Example 3-11 vssadmin commands

```
C:\>vssadmin
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001 Microsoft Corp.

Error: Invalid command.

---- Commands Supported ----

Add ShadowStorage     - Add a new volume shadow copy storage association
Create Shadow         - Create a new volume shadow copy
Delete Shadows        - Delete volume shadow copies
Delete ShadowStorage  - Delete volume shadow copy storage associations
List Providers        - List registered volume shadow copy providers
List Shadows          - List existing volume shadow copies
List ShadowStorage    - List volume shadow copy storage associations
List Volumes          - List volumes eligible for shadow copies
List Writers          - List subscribed volume shadow copy writers
Resize ShadowStorage  - Resize a volume shadow copy storage association
Revert Shadow         - Revert a volume to a shadow copy
Query Reverts         - Query the progress of in-progress revert operations.
```

Example 3-12 shows the **vssadmin list providers** command, which displays the hardware providers installed. We can see that the IBM TotalStorage Hardware Provider for VSS is present.

Example 3-12 vssadmin list hardware providers

```
C:\>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001 Microsoft Corp.

Provider name: 'Microsoft Software Shadow Copy provider 1.0'
```

```
   Provider type: System
   Provider Id: {b5946137-7b9f-4925-af80-51abd60b20d5}
   Version: 1.0.0.7

Provider name: 'IBM TotalStorage Hardware Provider for VSS'
   Provider type: Hardware
   Provider Id: {d90dd826-87cf-42ce-a88d-b32caa82025b}
   Version: 2.4.3.0220
```

3.2.14 Define storage space to hold VSS backups

Now you have to perform some additional configuration for VSS. You need to create the entities VSS_FREE and VSS_RESERVED for use by VSS. The process for doing this depends on your VSS hardware provider; consult the hardware provider documentation. As an example, we show the configuration on the IBM System Storage DS8000 and SAN Volume Controller.

Creating the VSS_FREE and VSS_RESERVED pools

Before using VSS for the first time, you must designate which volumes that the services can use as snapshot target volumes. This designation is done by creating a VSS_FREE pool and a VSS_RESERVED pool, represented by entities that are created on the storage unit. The process is different for disk systems. Once the VSS_FREE and VSS_RESERVED pools are created, volumes can be added to the free pool by simply assigning a volume to it.

On the DS8000:

1. Create a DS Volume Group called VSS_FREE.
2. Create a Virtual Host Connect named VSS_FREE as an Intel - Windows 2003 Server and assign it the WWPN 5000000000000000.
3. Create and assign free volumes to the DS VSS_FREE volume group.
4. Create a DS Volume Group called VSS_RESERVED.
5. Create a Virtual Host Connect named VSS_RESERVED as an Intel - Windows 2003 Server and assign it the WWPN 5000000000000001.

Example 3-13 shows that we created the required host objects for VSS_FREE and VSS_RESERVED on the DS8000. Note that we also have host connects for our servers REDBOOK1, REDBOOK2, and REDBOOK3, because they need to access the VSS shadow disks.

Example 3-13 VSS_FREE and VSS_RESERVED configuration on DS8000

```
dscli> lshostconnect -dev IBM.2107-1300271
Name                     ID   WWPN             HostType  Profile              po
rtgrp volgrpID ESSIOport
================================================================================
================================================================================
VSS_RESERVED             0014 5000000000000001 Win2003   Intel - Windows 2003
    0 V19      all
VSS_FREE                 0015 5000000000000000 Win2003   Intel - Windows 2003
    0 V18      all

redbook2                 0032 210000E08B89C1CD Win2003   Intel - Windows 2003
    0 V55      IO233
```

```
redbook3                 0033 210000E08B892CC0 Win2003   Intel - Windows 2003
    0 V56      IO233
redbook1                 0034 210000E08B892BCD Win2003   Intel - Windows 2003
    0 V57      IO233

dscli> lsvolgrp -dev IBM.2107-1300271
Date/Time: August 9, 2006 4:24:24 PM CDT IBM DSCLI Version: 5.0.500.100 DS: IBM.
2107-1300271
Name                ID  Type
=======================================
VSS_FREE            V18 SCSI Map 256
VSS_RESERVED        V19 SCSI Map 256
```

On the SVC

Example 3-14 shows the VSS_FREE and VSS_RESERVED configuration for an SVC. You can see the host definitions for the VSS_FREE and VSS_RESERVED hosts.

Example 3-14 VSS_FREE and VSS_RESERVED configuration on SVC

```
IBM_2145:ITSOSVC01:admin>svcinfo lshost 0
id 0
name VSS_FREE
port_count 1
type generic
mask 1111
iogrp_count 4
WWPN 5000000000000000
node_logged_in_count 0
state offline

IBM_2145:ITSOSVC01:admin>svcinfo lshost 7
id 7
name VSS_RESERVED
port_count 1
type generic
mask 1111
iogrp_count 4
WWPN 5000000000000001
node_logged_in_count 0
state offline
IBM_2145:ITSOSVC01:admin>
```

Verifying Exchange Server, Storage Groups, Logging and VSS

Before attempting to perform a backup or restore operation, verify that Data Protection for Exchange is installed and configured correctly by running the **query exchange** command on the server where Exchange is installed and running. This command shows the list of storage groups, and also VSS information, including the local and remote DSMAgent nodes as shown. If you are not using an offloaded backup server, you would not see the remote DSMAgent node.

In our clustered environment, to run the Exchange query, as in Example 3-15, we first copied the Data Protection for Exchange option file e:\tsmdata\ dsm_exch.opt to the default name

and directory C:\Program Files\Tivoli\TSM\TDPExchange\dsm.opt since the **tdpexcc query exchange** command only accepts the default options file. We specified our Data Protection for Exchange configuration file, with the /configfile parameter.

In a clustered environment, run this on both nodes.

Example 3-15 Verify Data Protection for Exchange configuration

```
C:\Program Files\Tivoli\TSM\TDPExchange>tdpexcc query exchange /excserver=RB1EVS
/configfile=e:\tsmdata\tdpexc_redbook2.cfg

IBM Tivoli Storage Manager for Mail:
Data Protection for Microsoft Exchange Server
Version 5, Release 3, Level 3.0
(C) Copyright IBM Corporation 1998, 2006. All rights reserved.

Microsoft Exchange Server Information
-------------------------------------

Server Name:                 RB1EVS
Domain Name:                 Redbook1.RB1.Local
Exchange Server Version:     6.5.7638.1

Storage Groups with Databases and Status
----------------------------------------

SG1
 Circular Logging - Disabled
   1Priv1                                        Online
   Public Folder Store (RB1EVS)                  Online

SG2
 Circular Logging - Disabled
   2priv1                                        Online
   2priv2                                        Online

SG3
 Circular Logging - Disabled
   3priv1                                        Online

Volume Shadow Copy Service (VSS) Information
--------------------------------------------

Writer Name           : Microsoft Exchange Writer
Local DSMAgent Node   : REDBOOK_VSS_A
Remote DSMAgent Node  : REDBOOK_OFFLOAD
Writer Status         : Online
Selectable Components  : 3

C:\Program Files\Tivoli\TSM\TDPExchange>
```

Verify DS Open API support for Microsoft VSS-VDS configuration

After you have created the VSS_FREE and VSS_RESERVED pools for VSS, you need to assign volumes to the VSS_FREE pool. These volumes will be used as the target for VSS

shadow operations. Consult your disk system documentation for information about how to create volumes and assign them. Remember, for each snapshot that you want to create for the Exchange database, you must have a set of target LUNs of suitable size. In the case of the DS6000/8000/SVC, these LUNs must be the same number and size as those used in the Exchange database. In other disk systems, you may not need the same configuration, so consult your hardware copy services documentation for information about how the snapshot function is implemented.

To verify your configuration, list the volumes assigned to the VSS_FREE pool. The specific implementation for this command varies according to your disk system. On the DS8000, issue the command: **ibmvcfg listvols | findstr 500000000**, as shown in Example 3-16 on page 85.

This command lists all volumes currently in the volume group VSS_FREE, because we specified its WWPN.

Example 3-16 List volumes in the VSS_FREE pool on DS8000

```
C:\Program Files\IBM\Hardware Provider for VSS-VDS>ibmvcfg listvols | findstr
500000
11      13002711105     2.00 GB         5000000000000000
12      13002711201     10.00 GB        5000000000000000
15      13002711500     50.00 GB        5000000000000000
22      13002712240     1.00 GB         5000000000000000
22      13002712241     1.00 GB         5000000000000000
22      13002712242     1.00 GB         5000000000000000
22      13002712243     1.00 GB         5000000000000000
22      13002712244     1.00 GB         5000000000000000
22      13002712245     1.00 GB         5000000000000000
22      13002712246     1.00 GB         5000000000000000
22      13002712247     1.00 GB         5000000000000000
22      13002712248     1.00 GB         5000000000000000
22      13002712249     1.00 GB         5000000000000000
22      1300271224A     1.00 GB         5000000000000000
22      1300271224B     1.00 GB         5000000000000000
22      1300271224C     1.00 GB         5000000000000000
22      1300271224D     1.00 GB         5000000000000000
22      1300271224E     1.00 GB         5000000000000000
22      1300271224F     1.00 GB         5000000000000000
22      13002712250     1.00 GB         5000000000000000
22      13002712257     4.00 GB         5000000000000000
22      13002712259     4.00 GB         5000000000000000
30      13002713004     1.00 GB         5000000000000000
38      13002713820     10.00 GB        5000000000000000
38      13002713821     10.00 GB        5000000000000000
38      13002713822     10.00 GB        5000000000000000
48      13002714800     50.00 GB        5000000000000000
....

C:\Program Files\IBM\Hardware Provider for VSS-VDS>
```

Example 3-17 shows two ways to list the volumes mapped to VSS_FREE on the SVC: by using the SVC command line, and by using the **ibmvcfg** command from the VSS provider.

Example 3-17 List volumes in the VSS_FREE pool on DS8000

```
**** At SVC command line
IBM_2145:ITSOSVC01:admin>svcinfo lshostvdiskmap
id               name             SCSI_id        vdisk_id       vdisk_name
wwpn             vdisk_UID
0                VSS_FREE         0              9              vdisk9
5000000000000000 60050768018600C47000000000000013
0                VSS_FREE         1              8              vdisk8
5000000000000000 60050768018600C47000000000000012

**** Using VSS provider

C:\Program Files\IBM\Hardware Provider for VSS-VDS>ibmvcfg listvols | findstr VSS

9.43.86.29      8       vdisk8          0.98GB          VSS_FREE
9.43.86.29      9       vdisk9          0.98GB          VSS_FREE
```

3.2.15 Using vssadmin and vshadow commands

You can use other commands to verify your environment. We have already discussed **vssadmin**, but you will also find the **vshadow** command useful. This command is included with the Microsoft VSS SDK, which you can get from the following site:

http://www.microsoft.com/downloads/details.aspx?FamilyID=0B4F56E4-0CCC-4626-826A-ED2C4C95C871&displaylang=en

Example 3-18 shows we use **vssadmin** to list the source volumes which are eligible to have shadow copies made. You can also use **vssadmin** to make and delete shadow copies.

Example 3-18 Sample vssadmin and vshadow commands

```
C:\Admin-DW\Exchange Utils\Vshadow>vssadmin list volumes
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001 Microsoft Corp.

Volume path: C:\
    Volume name: \\?\Volume{8345f2cf-07b4-11db-b957-806e6f6e6963}\
Volume path: E:\
    Volume name: \\?\Volume{aadfb120-110e-11db-b453-000d60494c64}\
Volume path: G:\
    Volume name: \\?\Volume{aadfb126-110e-11db-b453-000d60494c64}\
Volume path: I:\
    Volume name: \\?\Volume{aadfb12c-110e-11db-b453-000d60494c64}\
Volume path: F:\
    Volume name: \\?\Volume{aadfb123-110e-11db-b453-000d60494c64}\
Volume path: H:\
    Volume name: \\?\Volume{aadfb129-110e-11db-b453-000d60494c64}\
Volume path: J:\
    Volume name: \\?\Volume{aadfb12f-110e-11db-b453-000d60494c64}\
```

Now, in order to perform a final validation of the setup, before using the Data Protection for Exchange VSS service, we use **vshadow** to manually create the three types of VSS snapshots. This is a test of our environment, which is completely independent of the Tivoli Storage Manager components (backup-archive client, Data Protection for Exchange, Tivoli Storage Manager for Copy Services). However, ensure you can create persistent, non-persistent, and (if using an offloaded backup server), transportable snapshots using **vshadow** before proceeding with any Tivoli Storage Manager tests.

Our recommended best practice is to run each of these tests at least four times in succession. If you encounter any problems, carefully verify each stage of the proceeding state and correct the problem before going on. Note that you only need to test the transportable snapshot process if you are using an offloaded backup server.

We ran these tests on REDBOOK2. Because we were in a clustered environment, we also ran the same suite on REDBOOK3. When we tested the transportable shadow copy function, we imported the copy onto our offload server, REDBOOK1.

After these tests successfully completed, we proceeded to making VSS backups with Data Protection for Exchange, as shown in Chapter 4, “Backup and restore” on page 99.

Important: We show here how to manually create and delete VSS snapshots for testing purposes. Be very careful performing these operations once you start doing Tivoli Storage Manager VSS backups, because Data Protection for Exchange has no awareness of backups performed manually. You must take care not to accidentally overwrite or delete a VSS Exchange backup which you want to keep, using a **vshadow** command.

Create a persistent shadow using vshadow

First we created a persistent shadow copy. Example 3-19 shows a query command to confirm that we do not have any shadows made yet.

Example 3-19 Query for existence of any shadow copy

```
C:\Admin-DW\Exchange Utils\Vshadow>vshadow -q

VSHADOW.EXE 2.2 - Volume Shadow Copy sample client
Copyright (C) 2005 Microsoft Corporation. All rights reserved.


(Option: Query all shadow copies)
- Setting the VSS context to: 0xffffffff

Querying all shadow copies in the system ...


There are no shadow copies in the system


C:\Admin-DW\Exchange Utils\Vshadow>
```

Figure 3-43 on page 88 shows the current disks available on the server we were testing.

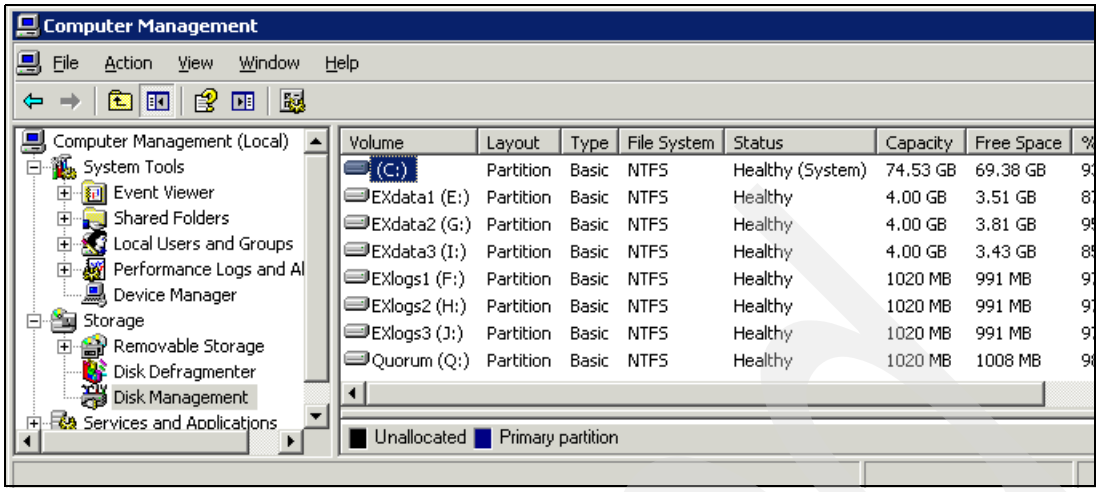


Figure 3-43 Disk management without any shadow copy

Now we made a persistent shadow copy of one drive (in this case, E). We used the command shown in Example 3-20:

```
vshadow -p e:
```

Example 3-20 Create a persistent shadow copy of E: drive

```
C:\Admin-DW\Exchange Utils\Vshadow>vshadow -p e:

VSHADOW.EXE 2.2 - Volume Shadow Copy sample client
Copyright (C) 2005 Microsoft Corporation. All rights reserved.


(Option: Persistent shadow copy)
(Option: Create shadow copy set)
- Setting the VSS context to: 0x00000009
(Gathering writer metadata...)
(Waiting for the asynchronous operation to finish...)
Initialize writer metadata ...
Discover directly excluded components ...
- Excluding writer 'MSDEWriter' since it has no selected components for restore.
Discover components that reside outside the shadow set ...
- Component '\System Files' from writer 'System Writer' is excluded from backup
(it requires C:\ in the shadow set)
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\b2e86828-8f9a-4a8a-97b4-f76cb1c14443\Logs' fr
om writer 'Microsoft Exchange Writer' is excluded from backup (it requires F:\ in
the shadow set)
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\acbd96c6-9655-474f-bd68-75513bf41cbf\Logs' fr
om writer 'Microsoft Exchange Writer' is excluded from backup (it requires H:\ in
the shadow set)
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\acbd96c6-9655-474f-bd68-75513bf41cbf\613ddb09
-5158-490e-9d3e-b36456ea9ecd' from writer 'Microsoft Exchange Writer' is excluded
from backup (it requires G:\ in the sh
adow set)
```

```
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\acbd96c6-9655-474f-bd68-75513bf41cbf\e78c2874
-61bb-435d-bbaa-ebe636d74baa' from writer 'Microsoft Exchange Writer' is excluded
from backup (it requires G:\ in the sh
adow set)
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\ef0d26ab-fc9a-4ba6-ba51-2bb5bddb610d\Logs' fr
om writer 'Microsoft Exchange Writer' is excluded from backup (it requires J:\ in
the shadow set)
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\ef0d26ab-fc9a-4ba6-ba51-2bb5bddb610d\069a9dfe
-4f0b-4684-8998-5e69db2e120f' from writer 'Microsoft Exchange Writer' is excluded
from backup (it requires I:\ in the sh
adow set)
- Component '\Registry' from writer 'Registry Writer' is excluded from backup (it
requires C:\ in the shadow set)
- Component '\Event Logs' from writer 'Event Log Writer' is excluded from backup
(it requires C:\ in the shadow set)
- Component '\IISMETABASE' from writer 'IIS Metabase Writer' is excluded from
backup (it requires C:\ in the shadow set)

- Component '\COM+ REGDB' from writer 'COM+ REGDB Writer' is excluded from backup
(it requires C:\ in the shadow set)
- Component '\Cluster Database' from writer 'Cluster Service Writer' is excluded
from backup (it requires C:\ in the sha
dow set)
- Component '\WMI' from writer 'WMI Writer' is excluded from backup (it requires
C:\ in the shadow set)
Discover all excluded components ...
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\b2e86828-8f9a-4a8a-97b4-f76cb1c14443' from wr
iter 'Microsoft Exchange Writer' is excluded from backup (it has an excluded
descendent: 'Logs')
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\acbd96c6-9655-474f-bd68-75513bf41cbf' from wr
iter 'Microsoft Exchange Writer' is excluded from backup (it has an excluded
descendent: 'Logs')
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\ef0d26ab-fc9a-4ba6-ba51-2bb5bddb610d' from wr
iter 'Microsoft Exchange Writer' is excluded from backup (it has an excluded
descendent: 'Logs')
Discover excluded writers ...
- The writer 'System Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'Microsoft Exchange Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'Registry Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'Event Log Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'IIS Metabase Writer' is now entirely excluded from the backup:
```

```
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'COM+ REGDB Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'Cluster Service Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'WMI Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
Discover explicitly included components ...
Verifying explicitly specified writers/components ...
Select explicitly included components ...
Creating shadow set {cf9ebeb3-d5f0-4bf4-8f23-f548a9f3860c} ...
- Adding volume \\?\Volume{aadfb120-110e-11db-b453-000d60494c64}\ [E:\] to the
shadow set...
Preparing for backup ...
(Waiting for the asynchronous operation to finish...)
(Waiting for the asynchronous operation to finish...)
Creating the shadow (DoSnapshotSet) ...
(Waiting for the asynchronous operation to finish...)
(Waiting for the asynchronous operation to finish...)
Shadow copy set succesfully created.

List of created shadow copies:


Querying all shadow copies with the SnapshotSetID
{cf9ebeb3-d5f0-4bf4-8f23-f548a9f3860c} ...

* SNAPSHOT ID = {11b72d4b-eaf0-4197-973d-e867a65fd45c} ...
   - Shadow copy Set: {cf9ebeb3-d5f0-4bf4-8f23-f548a9f3860c}
   - Original count of shadow copies = 1
   - Original Volume name: \\?\Volume{aadfb120-110e-11db-b453-000d60494c64}\ [E:\]
   - Creation Time: 8/15/2006 2:45:42 PM
   - Shadow copy device name: \\?\Volume{aadf3152-2c81-11db-9a77-000d60494c64}
   - Originating machine: Redbook2.RB1.Local
   - Service machine: Redbook2.RB1.Local
   - Not Exposed
   - Provider id: {d90dd826-87cf-42ce-a88d-b32caa82025b}
   - Attributes:  No_Auto_Release Persistent Hardware

- Mark all writers as succesfully backed up...
Completing the backup (BackupComplete) ...
(Waiting for the asynchronous operation to finish...)
(Waiting for the asynchronous operation to finish...)

Snapshot creation done.

C:\Admin-DW\Exchange Utils\Vshadow>
```

Now the query command shows the new shadow set; see Example 3-21 on page 91.

Note the Attributes field specifies *No_Auto_Release Persistent Hardware;* to confirm we made a persistent snapshot.

Example 3-21 Query for existence of any shadow copy

```
C:\Admin-DW\Exchange Utils\Vshadow>vshadow -q

VSHADOW.EXE 2.2 - Volume Shadow Copy sample client
Copyright (C) 2005 Microsoft Corporation. All rights reserved.


(Option: Query all shadow copies)
- Setting the VSS context to: 0xffffffff

Querying all shadow copies in the system ...

* SNAPSHOT ID = {11b72d4b-eaf0-4197-973d-e867a65fd45c} ...
   - Shadow copy Set: {cf9ebeb3-d5f0-4bf4-8f23-f548a9f3860c}
   - Original count of shadow copies = 1
   - Original Volume name: \\?\Volume{aadfb120-110e-11db-b453-000d60494c64}\ [E:\]
   - Creation Time: 8/15/2006 2:45:42 PM
   - Shadow copy device name: \\?\Volume{aadf3152-2c81-11db-9a77-000d60494c64}
   - Originating machine: Redbook2.RB1.Local
   - Service machine: Redbook2.RB1.Local
   - Not Exposed
   - Provider id: {d90dd826-87cf-42ce-a88d-b32caa82025b}
   - Attributes:  No_Auto_Release Persistent Hardware


C:\Admin-DW\Exchange Utils\Vshadow>
```

Figure 3-44 shows that the disk for the shadow copy was now available on the server, compared with Figure 3-43. This is because it is a persistent copy; therefore, it remains until specifically deleted.

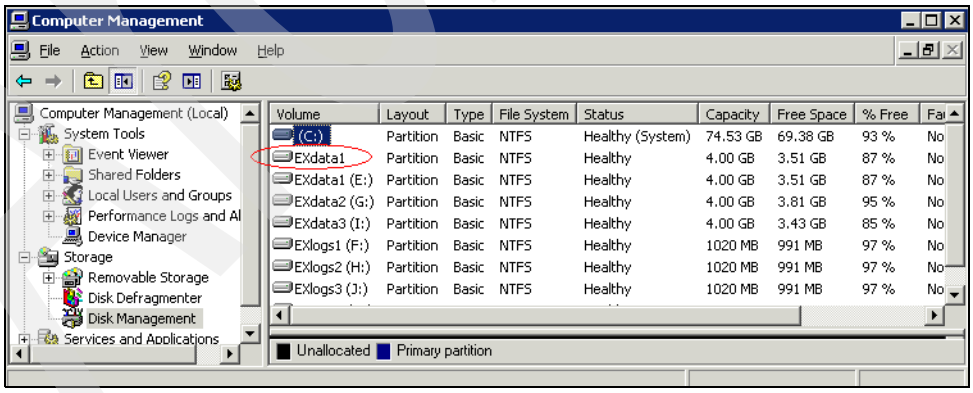


Figure 3-44 Disk Management after the persistent shadow copy creation

Now we deleted the shadow copy, as shown in Example 3-22.

Example 3-22 Delete of all shadow copies

```
C:\Admin-DW\Exchange Utils\Vshadow>vshadow -da

VSHADOW.EXE 2.2 - Volume Shadow Copy sample client
Copyright (C) 2005 Microsoft Corporation. All rights reserved.


(Option: Delete all shadow copies)
This will delete all shadow copies in the system. Are you sure? [Y/N] y

- Setting the VSS context to: 0xffffffff
- Deleting shadow copy {11b72d4b-eaf0-4197-973d-e867a65fd45c} on
\\?\Volume{aadfb120-110e-11db-b453-000d60494c64}\ from
provider {d90dd826-87cf-42ce-a88d-b32caa82025b} [0x00010009]...

C:\Admin-DW\Exchange Utils\Vshadow>
```

Create a non-persistent shadow copy using vshadow

We created a non-persistent shadow copy of the E drive; this is the default for the **vshadow** command. The output is shown in Example 3-23. Note that the Attributes field specifies *Auto_Release Hardware*, to confirm we made a non-persistent snapshot.

Example 3-23 Create a non-persistent shadow copy of E: drive

```
C:\Admin-DW\Exchange Utils\Vshadow>vshadow e:

VSHADOW.EXE 2.2 - Volume Shadow Copy sample client
Copyright (C) 2005 Microsoft Corporation. All rights reserved.


(Option: Create shadow copy set)
(Gathering writer metadata...)
(Waiting for the asynchronous operation to finish...)
Initialize writer metadata ...
Discover directly excluded components ...
- Excluding writer 'MSDEWriter' since it has no selected components for restore.
Discover components that reside outside the shadow set ...
- Component '\System Files' from writer 'System Writer' is excluded from backup
(it requires C:\ in the shadow set)
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\b2e86828-8f9a-4a8a-97b4-f76cb1c14443\Logs' fr
om writer 'Microsoft Exchange Writer' is excluded from backup (it requires F:\ in
the shadow set)
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\acbd96c6-9655-474f-bd68-75513bf41cbf\Logs' fr
om writer 'Microsoft Exchange Writer' is excluded from backup (it requires H:\ in
the shadow set)
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\acbd96c6-9655-474f-bd68-75513bf41cbf\613ddb09
-5158-490e-9d3e-b36456ea9ecd' from writer 'Microsoft Exchange Writer' is excluded
from backup (it requires G:\ in the sh
adow set)
```

```
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\acbd96c6-9655-474f-bd68-75513bf41cbf\e78c2874
-61bb-435d-bbaa-ebe636d74baa' from writer 'Microsoft Exchange Writer' is excluded
from backup (it requires G:\ in the sh
adow set)
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\ef0d26ab-fc9a-4ba6-ba51-2bb5bddb610d\Logs' fr
om writer 'Microsoft Exchange Writer' is excluded from backup (it requires J:\ in
the shadow set)
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\ef0d26ab-fc9a-4ba6-ba51-2bb5bddb610d\069a9dfe
-4f0b-4684-8998-5e69db2e120f' from writer 'Microsoft Exchange Writer' is excluded
from backup (it requires I:\ in the sh
adow set)
- Component '\IISMETABASE' from writer 'IIS Metabase Writer' is excluded from
backup (it requires C:\ in the shadow set)

- Component '\Registry' from writer 'Registry Writer' is excluded from backup (it
requires C:\ in the shadow set)
- Component '\Event Logs' from writer 'Event Log Writer' is excluded from backup
(it requires C:\ in the shadow set)
- Component '\COM+ REGDB' from writer 'COM+ REGDB Writer' is excluded from backup
(it requires C:\ in the shadow set)
- Component '\WMI' from writer 'WMI Writer' is excluded from backup (it requires
C:\ in the shadow set)
- Component '\Cluster Database' from writer 'Cluster Service Writer' is excluded
from backup (it requires C:\ in the sha
dow set)
Discover all excluded components ...
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\b2e86828-8f9a-4a8a-97b4-f76cb1c14443' from wr
iter 'Microsoft Exchange Writer' is excluded from backup (it has an excluded
descendent: 'Logs')
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\acbd96c6-9655-474f-bd68-75513bf41cbf' from wr
iter 'Microsoft Exchange Writer' is excluded from backup (it has an excluded
descendent: 'Logs')
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\ef0d26ab-fc9a-4ba6-ba51-2bb5bddb610d' from wr
iter 'Microsoft Exchange Writer' is excluded from backup (it has an excluded
descendent: 'Logs')
Discover excluded writers ...
- The writer 'System Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'Microsoft Exchange Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'IIS Metabase Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'Registry Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'Event Log Writer' is now entirely excluded from the backup:
```

```
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'COM+ REGDB Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'WMI Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'Cluster Service Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
Discover explicitly included components ...
Verifying explicitly specified writers/components ...
Select explicitly included components ...
Creating shadow set {8d916e2e-cd62-4c22-b592-35b0d06471a2} ...
- Adding volume \\?\Volume{aadfb120-110e-11db-b453-000d60494c64}\ [E:\] to the
shadow set...
Preparing for backup ...
(Waiting for the asynchronous operation to finish...)
(Waiting for the asynchronous operation to finish...)
Creating the shadow (DoSnapshotSet) ...
(Waiting for the asynchronous operation to finish...)
(Waiting for the asynchronous operation to finish...)
Shadow copy set succesfully created.

List of created shadow copies:


Querying all shadow copies with the SnapshotSetID
{8d916e2e-cd62-4c22-b592-35b0d06471a2} ...

* SNAPSHOT ID = {aad6c91e-c4ed-491e-9ef0-e1ec9206d2a3} ...
   - Shadow copy Set: {8d916e2e-cd62-4c22-b592-35b0d06471a2}
   - Original count of shadow copies = 1
   - Original Volume name: \\?\Volume{aadfb120-110e-11db-b453-000d60494c64}\ [E:\]
   - Creation Time: 8/15/2006 3:36:38 PM
   - Shadow copy device name: \\?\GlobalRoot\Device\HarddiskVolume28
   - Originating machine: Redbook2.RB1.Local
   - Service machine: Redbook2.RB1.Local
   - Not Exposed
   - Provider id: {d90dd826-87cf-42ce-a88d-b32caa82025b}
   - Attributes:  Auto_Release Hardware

- Mark all writers as succesfully backed up...
Completing the backup (BackupComplete) ...
(Waiting for the asynchronous operation to finish...)
(Waiting for the asynchronous operation to finish...)

Snapshot creation done.

C:\Admin-DW\Exchange Utils\Vshadow>
```

Because the snapshot is automatically released, we could only see the disk used in Disk Manager for a very short time, and then it was gone. Therefore, we did not need to delete the shadow.

Create a transportable shadow copy using vshadow

Finally, since we had an offloaded backup server, we created a transportable shadow copy of the E drive, specifying the -t option, as shown in Example 3-24. The transportable shadow copy carries with it certain descriptor information, which is stored in a file of type XML. We specified the name and location of the file we wanted to use for output on the **vshadow** command.

Example 3-24 Create a non-persistent shadow copy of e: drive

```
C:\Admin-DW\Exchange Utils\Vshadow>vshadow -t=export.xml e:

VSHADOW.EXE 2.2 - Volume Shadow Copy sample client
Copyright (C) 2005 Microsoft Corporation. All rights reserved.


(Option: Transportable shadow set. Saving xml to file 'export.xml')
(Option: Create shadow copy set)
- Setting the VSS context to: 0x00000020
(Gathering writer metadata...)
(Waiting for the asynchronous operation to finish...)
Initialize writer metadata ...
Discover directly excluded components ...
- Excluding writer 'MSDEWriter' since it has no selected components for restore.
Discover components that reside outside the shadow set ...
- Component '\System Files' from writer 'System Writer' is excluded from backup
(it requires C:\ in the shadow set)
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\b2e86828-8f9a-4a8a-97b4-f76cb1c14443\Logs' fr
om writer 'Microsoft Exchange Writer' is excluded from backup (it requires F:\ in
the shadow set)
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\acbd96c6-9655-474f-bd68-75513bf41cbf\Logs' fr
om writer 'Microsoft Exchange Writer' is excluded from backup (it requires H:\ in
the shadow set)
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\acbd96c6-9655-474f-bd68-75513bf41cbf\613ddb09
-5158-490e-9d3e-b36456ea9ecd' from writer 'Microsoft Exchange Writer' is excluded
from backup (it requires G:\ in the sh
adow set)
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\acbd96c6-9655-474f-bd68-75513bf41cbf\e78c2874
-61bb-435d-bbaa-ebe636d74baa' from writer 'Microsoft Exchange Writer' is excluded
from backup (it requires G:\ in the sh
adow set)
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\ef0d26ab-fc9a-4ba6-ba51-2bb5bddb610d\Logs' fr
om writer 'Microsoft Exchange Writer' is excluded from backup (it requires J:\ in
the shadow set)
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\ef0d26ab-fc9a-4ba6-ba51-2bb5bddb610d\069a9dfe
-4f0b-4684-8998-5e69db2e120f' from writer 'Microsoft Exchange Writer' is excluded
from backup (it requires I:\ in the sh
```

```
adow set)
- Component '\COM+ REGDB' from writer 'COM+ REGDB Writer' is excluded from backup
(it requires C:\ in the shadow set)
- Component '\Registry' from writer 'Registry Writer' is excluded from backup (it
requires C:\ in the shadow set)
- Component '\Event Logs' from writer 'Event Log Writer' is excluded from backup
(it requires C:\ in the shadow set)
- Component '\IISMETABASE' from writer 'IIS Metabase Writer' is excluded from
backup (it requires C:\ in the shadow set)

- Component '\WMI' from writer 'WMI Writer' is excluded from backup (it requires
C:\ in the shadow set)
- Component '\Cluster Database' from writer 'Cluster Service Writer' is excluded
from backup (it requires C:\ in the sha
dow set)
Discover all excluded components ...
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\b2e86828-8f9a-4a8a-97b4-f76cb1c14443' from wr
iter 'Microsoft Exchange Writer' is excluded from backup (it has an excluded
descendent: 'Logs')
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\acbd96c6-9655-474f-bd68-75513bf41cbf' from wr
iter 'Microsoft Exchange Writer' is excluded from backup (it has an excluded
descendent: 'Logs')
- Component '\Microsoft Exchange Server\Microsoft Information
Store\RB1EVS\ef0d26ab-fc9a-4ba6-ba51-2bb5bddb610d' from wr
iter 'Microsoft Exchange Writer' is excluded from backup (it has an excluded
descendent: 'Logs')
Discover excluded writers ...
- The writer 'System Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'Microsoft Exchange Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'COM+ REGDB Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'Registry Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'Event Log Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'IIS Metabase Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'WMI Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
- The writer 'Cluster Service Writer' is now entirely excluded from the backup:
  (it does not contain any components that can be potentially included in the
backup)
Discover explicitly included components ...
Verifying explicitly specified writers/components ...
```

```
Select explicitly included components ...
Creating shadow set {b1def135-bea4-46fb-bc6f-c0089e7fb992} ...
- Adding volume \\?\Volume{aadfb120-110e-11db-b453-000d60494c64}\ [E:\] to the
shadow set...
Preparing for backup ...
(Waiting for the asynchronous operation to finish...)
(Waiting for the asynchronous operation to finish...)
Creating the shadow (DoSnapshotSet) ...
(Waiting for the asynchronous operation to finish...)
(Waiting for the asynchronous operation to finish...)
Shadow copy set succesfully created.
Saving the backup components document ...
Writing the file 'export.xml' ...
- Mark all writers as succesfully backed up...
Completing the backup (BackupComplete) ...
(Waiting for the asynchronous operation to finish...)
(Waiting for the asynchronous operation to finish...)

Snapshot creation done.
```

To prepare for the import of the transportable shadow copy, we needed to make the XML descriptor file available on the server where the copy would be imported, which was REDBOOK1. An easy way to do this is to simply copy the XML file to REDBOOK1, as shown in Example 3-25.

Example 3-25 Copy XML file to offload server

```
C:\Admin-DW\Exchange Utils\Vshadow>copy export.xml \\redbook1\c$\
        1 file(s) copied.
C:\Admin-DW\Exchange Utils\Vshadow>
```

Now on REDBOOK1, we checked our basic disk configuration, as shown in Figure 3-45. We saw there is only one local disk available currently.

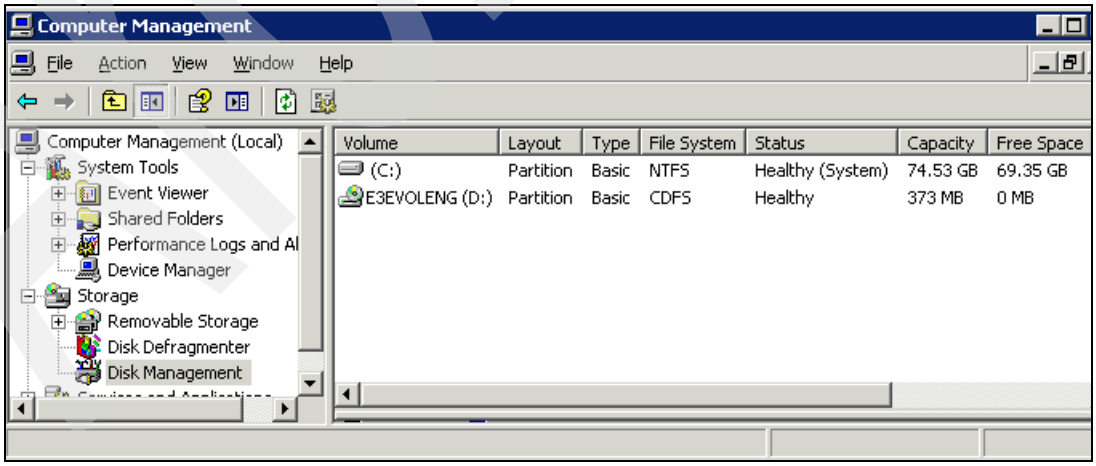


Figure 3-45 Disk management on the offloaded backup server before the shadow copy import.

On REDBOOK1, we imported the transportable shadow copy by specifying the descriptor file, using the -i option, as shown in Example 3-26 on page 98.

Example 3-26 Import the transportable shadow copy on the offload machine

```
C:\Admin-DW\Exchange Utils\vshadow>vshadow -i=c:\export.xml

VSHADOW.EXE 2.2 - Volume Shadow Copy sample client
Copyright (C) 2005 Microsoft Corporation. All rights reserved.


(Option: Import shadow copy set from file 'c:\export.xml')
Reading the file 'c:\export.xml' ...
- Setting the VSS context to: 0xffffffff
Importing the transportable snapshot set ...
(Waiting for the asynchronous operation to finish...)
Shadow copy set succesfully imported.

C:\Admin-DW\Exchange Utils\vshadow>
```

Now when we refreshed Disk Management on REDBOOK1, we saw the new volume for the shadow copy; see Figure 3-46. Because the transportable copy is non-persistent, the disk will only be visible for a short time.

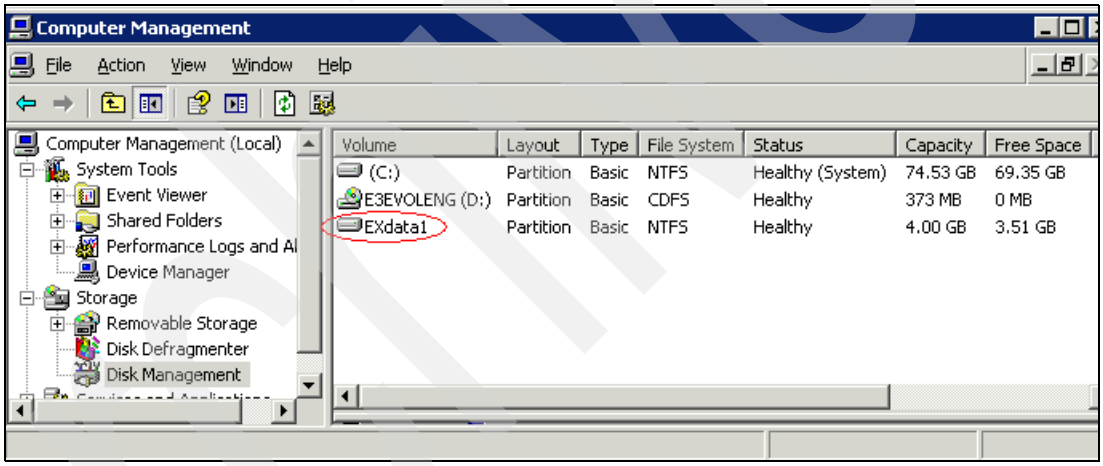


Figure 3-46 Disk management on offload machine while importing the transportable copy

4

Backup and restore

In this chapter we describe the graphical and command line interfaces to Data Protection for Exchange. Then we show you how to perform basic backup and restore operations. These operations include:

- Performing a legacy backup of Exchange Storage Groups and transaction logs
- Performing a VSS backup of Exchange storage groups and transaction logs
- Performing a VSS offloaded backups of Exchange Storage groups and transaction logs
- Restoring Exchange Storage Groups and transaction logs

We also explain how to monitor Tivoli Storage Manager server sessions during backup and restore, and how to use the **vssadmin** and **vshadow** commands to show the creation of the backups.

4.1 GUI overview

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

- Common menu bar
- Toolbar
- Backup window
- Restore window

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

Figure 4-1 shows the Data Protection for Exchange GUI. We describe how to launch the GUI in 4.1.3, “Launching the GUI” on page 106. Because we have installed Tivoli Storage Manager for Copy Services, the VSS Backup option is available for selection. If it was not installed, this option would be grayed out.

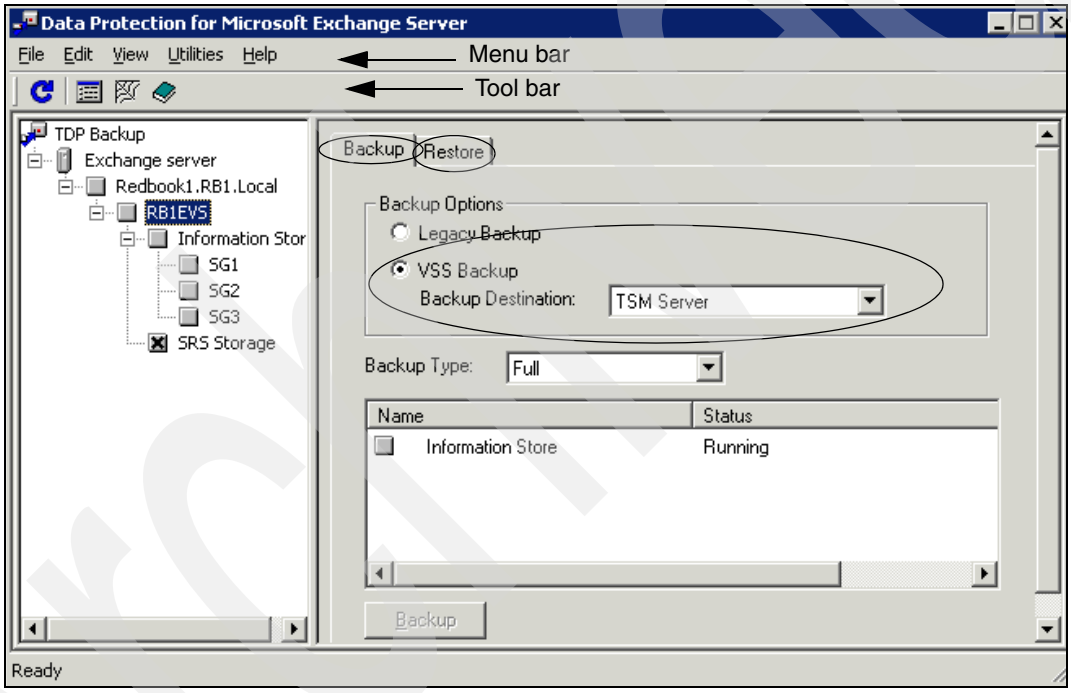


Figure 4-1 Data Protection for Exchange GUI

4.1.1 Menu bar

The Data Protection for Exchange GUI menu bar has these items and menu list functions:

File Exit the program.

Edit Configure Data Protection for Exchange. The default configuration settings are contained in the tdpexc.cfg file.

View Refresh the Tree View.

Utilities Change the Tivoli Storage Manager password or display Tivoli Storage Manager server information.

Help Access Data Protection for Exchange help, view online books, Tivoli Storage Manager Web access, and information about Data Protection for Exchange

Edit menu

There are several options in the Edit menu.

Configuration

You can modify the Data Protection for Exchange configuration file, as seen in Figure 4-2. If a configuration file is not specified, the file tdpexc.cfg is used. If no configuration file is found, a default file is created which contains all the default settings for the parameters. To specify a different configuration file, start the GUI from the command line with the /configfile parameter.

Select **Edit** → **Configuration** to display the Data Protection for Exchange Settings dialog.

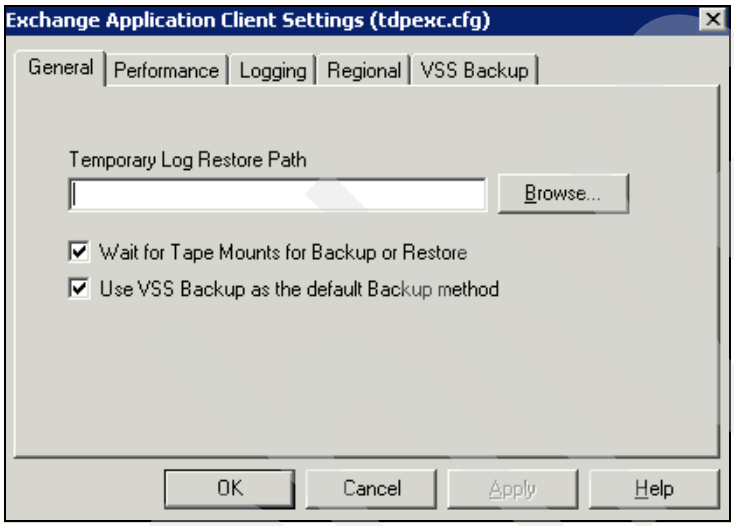


Figure 4-2 General options

The dialog has these five tabs with associated settings:

- **General Tab**
  - **Temporary Log Restore Path**

    Enter the default temporary path to use when restoring logs and patch files. For best performance, the path specified should be on a different physical device than the current active logger. If you choose to not enter a path, the default is the value of the TEMP environment variable.

    When performing full, copy, or database copy restores, all log files residing in the specified path are erased. This option is only used on legacy operations.
  - **Wait for Tape Mounts for Backup or Restore**

    Check this box if you want Data Protection for Exchange 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 need to wait until the required tape volume mounts.

    This setting specifies whether Data Protection for Exchange should wait for the media mount or stop the current operation. Wait 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. If you use VSS as the default, the **Local DSMAGENT Node name** parameter must be specified (as shown in Figure 4-5 on page 104 on the VSS Backup tab). This parameter is grayed out if the Microsoft Exchange VSS Integration Module from Tivoli Storage Manager for Copy Services is not installed. Remember that VSS backups can only be restored using VSS.

By default, this box is unchecked, so that legacy backups are the default.

- **Performance Tab**

The Performance tab is shown in Figure 4-3.

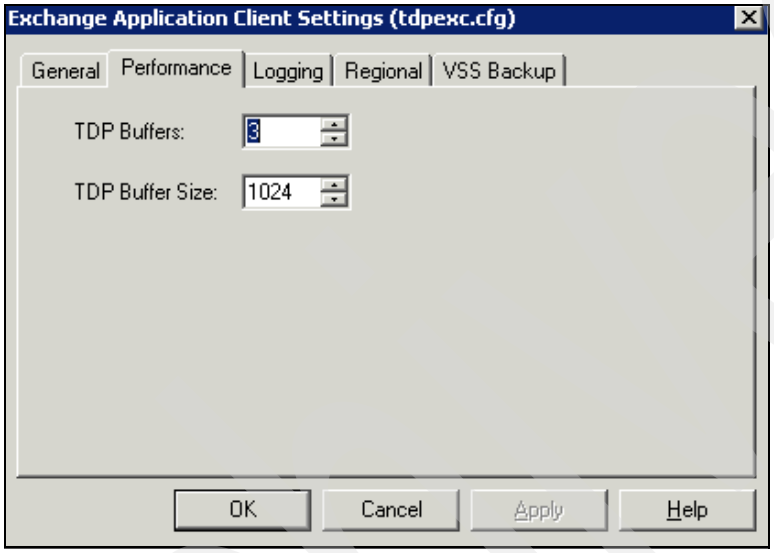


Figure 4-3 Performance options

This tab allows you to change the TDP Buffers.

– **TDP Buffers** (default value: 3)

A number (2 to 8) that specifies the number of communication data buffers Data Protection for Exchange uses when transferring data between Data Protection for Exchange and the Tivoli Storage Manager server. Each buffer is the size specified in the **TDP Buffer Size** parameter. This parameter applies to legacy backups only.

– **TDP Buffer Size** (default value: 1024)

A number (64 to 8192) that specifies the size of the buffers used by Data Protection for Exchange to transfer data to the Tivoli Storage Manager server. This parameter applies to legacy backups only.

Most testing has shown that the default buffer number and size of buffers gives the best performance. However, some environmental factors may affect your performance differently, for example, database and network speed. If you change these buffers, conduct controlled “before and after” testing to determine what affect the changes have.

- **Logging Tab**

The logging tab is shown in Figure 4-4 on page 103.

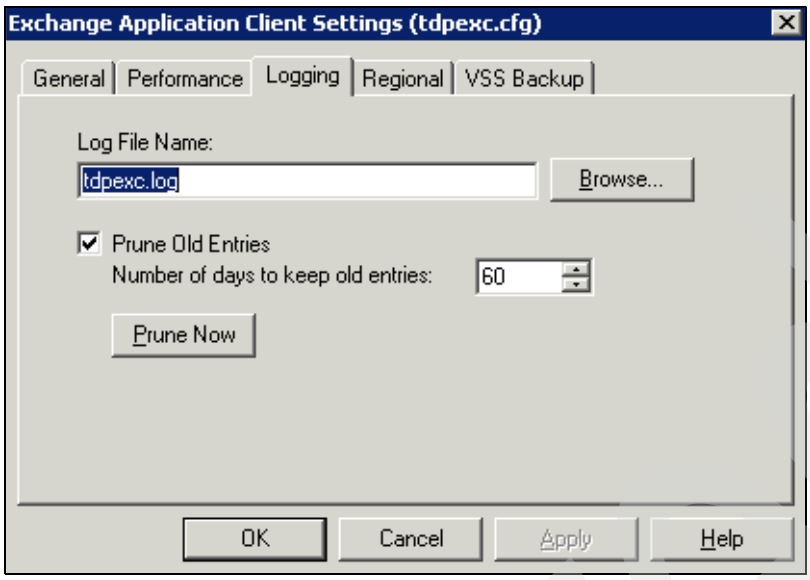


Figure 4-4 Logging options

- **Log File Name** (default value: tdpexc.log) as seen in Figure 4-4.

  Name of the file where Data Protection for Exchange will log its output.

- **Prune Old Entries** (default value: selected)

  Enables pruning of the activity log. Specify the number of days (0 to 9999) to keep old entries. Data Protection for Exchange prunes entries greater than this number when it is initialized. The default value is to keep the entries for 60 days. Click **Prune Now** to prune the activity log immediately.

- **Regional Tab**
  - **Language** (default value: American English)

    Specify the language to use for displaying the GUI and Data Protection for Exchange messages.You have to restart the GUI if you change the language.

  - **Date Format** (format: mm/dd/yyyy)
  - **Time Format** (default value: hh:mm:ss)
  - **Number Format** (default value: xxx,xxx.dd)
- **VSS Backup Tab**

  Figure 4-5 on page 104 shows the VSS Backup tab.

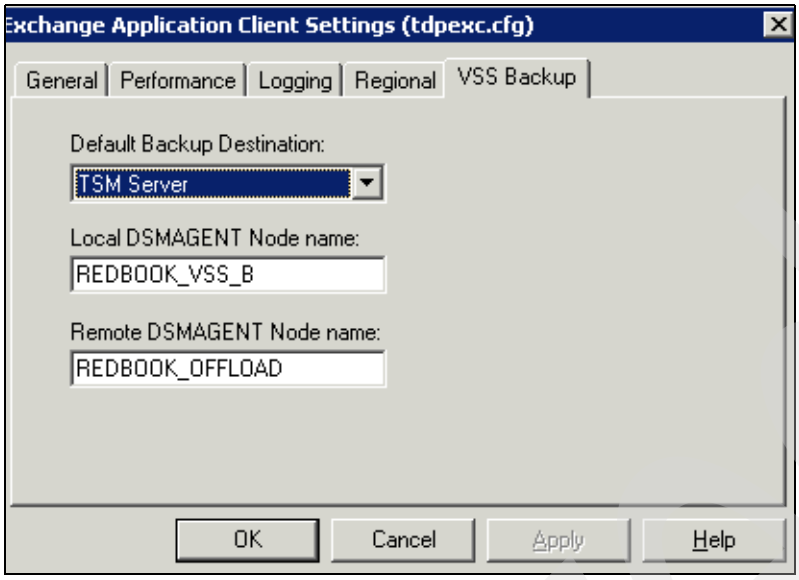


Figure 4-5 VSS Backup View

– **Default Backup Destination** (default value: Tivoli Storage Manager Server), as seen in Figure 4-5.

Default storage location for your backups. The destination can be one of:

- **Tivoli Storage Manager Server**

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

- **Local**

  The backup is stored on local persistent shadow volumes only.

- **Both**

  The backup is stored on both Tivoli Storage Manager server storage and local shadow volumes. If this parameter is selected, the Tivoli Storage Manager server backup cannot be offloaded.

– **Local DSMAGENT Node name**

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 is required to perform VSS backups and restores.

– **Remote DSMAGENT Node name**

Specify the Tivoli Storage Manager node name (agent node) of the remote client machine that moves the VSS data from local shadow volumes to Tivoli Storage Manager server storage during offloaded backups. This option is only required if you are using and offloaded backup server.

View menu

The View menu gives you the following options:

- **Refresh tree view**

  Selecting this option refreshes the display tree. When the tree is refreshed, all selections you have made for backup or restore are cleared, all List View information for all Storage

Groups is cleared, and the GUI rebuilds and completely expands the directory tree on the left-hand side.

If you simply move back and forth between the Backup and Restore tabs without refreshing, you do not lose the current selections or Tree View. After performing a Backup, you must refresh the Restore directory tree to see the new backup.

- **Show only Active objects**

  With this option, only active backup objects are displayed in the List View. This is the default.

- **Show all objects**

  If selected, then both active and inactive objects are displayed in the List View.

- **Auto Select**

  Select this option to quickly select the backup objects to restore. When **Auto Select** is off, you must click all objects to be restored. When **Auto Select** is on (the default value), additional selections are automatically made as you click. To override the characteristics of **Auto Select**, deselect the **Auto Select** option and manually select what you need.

  When **Auto Select** on, it is effective when you click a full, differential, or incremental backup in the List View, and also when you click a storage group or server name in the Tree View. **Auto Select** ignores copy and database copy backups.

  – If you click a full backup, the latest associated differential or all associated incremental backups are selected.

  – If you click a differential backup, the associated full backup is also selected.

  – If you click an incremental backup, the associated full backup and all associated earlier incremental backups are also selected.

  Auto Select will not make additional selections in the following two situations:

  – If a combination of differential and incremental backups exists for a full backup. For example, if you clicked on a full backup that had associated incremental *and* differential backups, only the full backup is selected.

  – If a differential or incremental backup is selected and no associated full backup can be found.

Utilities menu

- **Change Tivoli Storage Manager Password**

  This dialog prompts you to enter the old password, then enter the new password twice, in order to verify the new password.

- **Tivoli Storage Manager Server Information**

  This window (shown in Figure 4-6 on page 106) shows information about the configuration and connection to the Tivoli Storage Manager server.

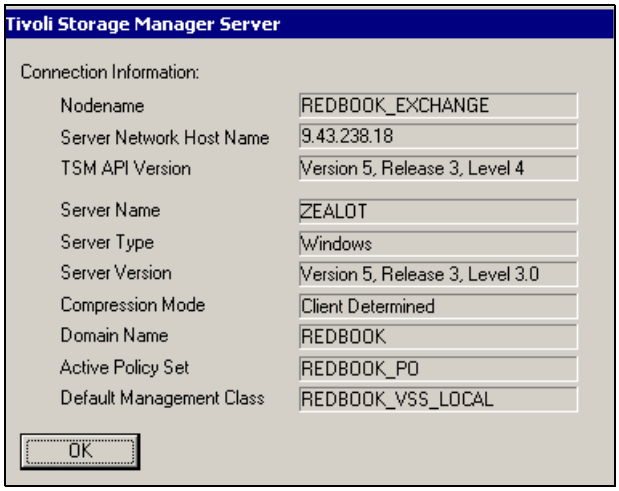


Figure 4-6 Tivoli Storage Manager configuration

The fields are:

- 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

Help menu

From the help menu, you can launch Data Protection for Exchange online help, view the manual (*Data Protection for Exchange Installation and User's Guide*), launch an online help panel with links to IBM, Tivoli Storage Manager, and Exchange Server Web site links, and show the product version.

4.1.2 Toolbar

The Toolbar provides short cuts to frequently used tasks such as:

- Refresh the Tree View
- Edit Data Protection for Exchange configuration
- Display IBM, Tivoli Storage Manager, and Exchange Server Web site links
- Display the *Data Protection for Exchange Installation and User's Guide*

4.1.3 Launching the GUI

To launch the GUI, navigate **Start** → **Programs** → **Tivoli Storage Manager** → **Data Protection For Exchange** → **Exchange Client GUI** or use the **`tdpexc`** command from the installation directory.

It can take the following parameters:

/configfile

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

For example, to specify the configuration file, file.cfg, located in the \temp\test directory during the GUI invocation, enter:

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

/excserver

If specified, this parameter overrides the default Exchange server, which is the local Exchange server.

Important: If you are running Data Protection for Exchange in a cluster (MSCS), you *must* use the **/excserver** parameter.

```
tdpexc /EXCSERVer=exc1
```

/tsmoptfile

If specified, 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:

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

If you need 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 “Create a Data Protection for Exchange GUI shortcut” on page 62.

4.1.4 Backup and restore window

Data Protection for Exchange provides separate windows for backup and restore operations. Each window contains its own directory tree, list, and tab controls.

Considerations

- Both legacy and VSS operations are performed from the same tab.
- When the GUI starts, the backup window is the initial display.
- VSS-related features are grayed out unless the Exchange VSS Integration Module is installed.

Highlighting and selecting

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

- If a Storage Group is highlighted in the Restore Tree, all Tivoli Storage Manager backups for that Storage Group are displayed in the List View.
- If the Site, Organization, or Domain name is highlighted in the Backup Tree, information about the Site, Organization, or Domain, Exchange server, and version level are displayed in the List View.
- If the Information Store item is highlighted in the Backup Tree, the List View displays status for all Storage Groups.
- If the server name is highlighted in the Restore Tree, the List View displays *all* Storage Groups and their backups (indented under the Storage Group).

To select an item for backup or restore, click the square selection box to the left of the item name. Clicking 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.

Messages

If you select multiple Copy, Full, or Database Copy backups, or any combination of these backups for restore, a warning message will ask you if you want to continue. If you continue, all backups will be restored but only the latest backup will take effect. All the time spent restoring the earlier backups will be wasted.

When you select to restore a backup, Data Protection for Exchange first checks to make sure any affected databases are dismounted. If they are not, you will be prompted to either stop them or cancel the restore. After a restore, you can either check the **Mount Databases After Restore** option, or mount them from outside Data Protection for Exchange.

4.2 The command line interface

The Data Protection for Exchange CLI is called tdpexcc.exe. It is located in the directory where Data Protection for Exchange is installed; \program files\tivoli\tsm\TDPExchange is the default directory.

Issue the **`tdpexcc ?`** or **`tdpexcc help`** command to display help for the command line interface.

For a detailed explanation of the command line, refer to *Data Protection for Microsoft Exchange Server Installation and Users Guide*, SC32-9058.

We will show examples of backup and restore operations using both the GUI and CLI.

4.3 Our test environment

Before trying any backup operations, make sure that Data Protection for Exchange and the Tivoli Storage Manager server are properly configured in your environment, as described in the previous chapters.You must have local registry rights to perform a Data Protection for Exchange backup.

In our lab we set up two Exchange environments: one with a DS8000 disk system and MSCS clustering, the other non-clustered using a SAN Volume Controller. The clustered DS8000 configuration was used for most of our examples. However, for the Instant Restore scenario (4.7.3, “VSS Instant Restore” on page 144), we used a SAN Volume Controller configuration. Figure 3-1 on page 44 shows our DS8000 clustered Exchange environment.

Here are the nodenames used:

- Data Protection for Exchange nodename: **REDBOOK_EXCHANGE**
- Local DSMAgents: **REDBOOK_VSS_A** and **REDBOOK_VSS_B** (one on each cluster node)
- RemoteDSMAgent: **REDBOOK_OFFLOAD**
- Tivoli Storage Manager server: **ZEALOT**
- Exchange Cluster Node: **RB1EVS**

4.4 Legacy Exchange backup

To perform a non-VSS (legacy) backup, follow these steps:

1. Start the Data Protection for Exchange GUI as described in 4.1.3, “Launching the GUI” on page 106. You can either launch it directly or use a shortcut.

   We show a recommended shortcut if you are running Data Protection for Exchange in a MSCS cluster in “Create a Data Protection for Exchange GUI shortcut” on page 62, and Figure 3-15 on page 64.

   If you are running in a clustered (MSCS) environment:

   – If you are backing up the Site Replication(SRS), you must initialize the SRS database through the cluster administrator. The SRS must be running in order to be backed up.

2. Select one or more Storage Groups to back up. You cannot back up more than one application (SRS, KMS, IS) in a single operation.
3. In the Backup Options section of the Backup windows, select the Legacy Backup method.
4. Specify the type of backup to perform with the Backup Type drop-down menu. You cannot perform a database copy of an SRS or KMS database.
5. Click **Backup** to begin the backup operation.

In the following section we show detailed example operations using the GUI.

4.4.1 GUI legacy full backup

After launching the GUI, Figure 4-7 on page 109 shows the main screen with the different options for legacy or VSS backup.

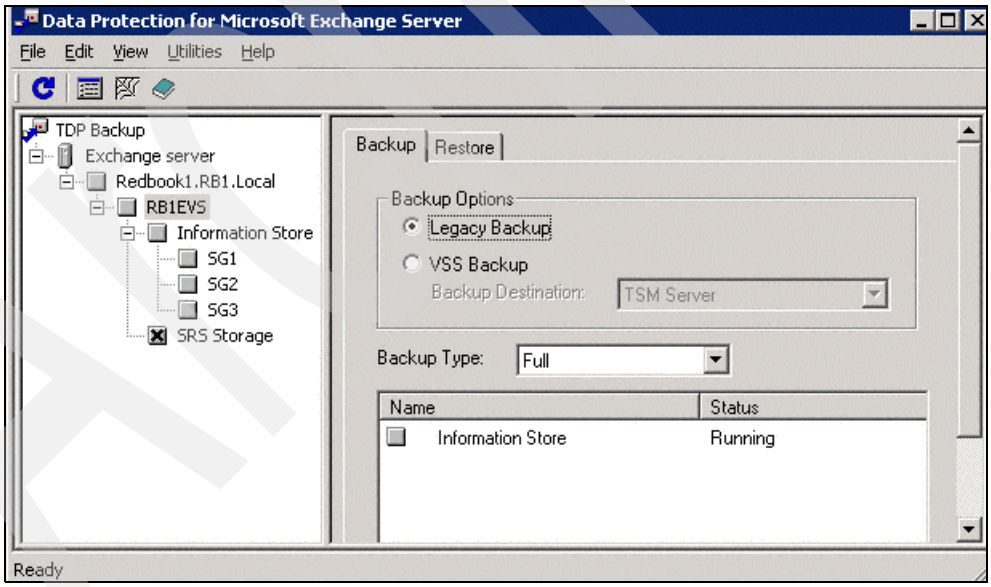


Figure 4-7 GUI options for a backup

As you can see, server RB1EVS is a member of domain Redbook1.RB1.local. It contains three storage groups: SG1, SG2 and SG3. You can back up one or more Storage Groups. We selected legacy backup with type full.

If you choose a full backup, both the databases and the associated transaction logs will be backed up. When the backup completes, the log files are deleted. When a full backup

completes successfully, all previous legacy backups are inactivated in Tivoli Storage Manager, and marked for expiration according to your management policy.

Figure 4-8 shows the entire Information store is being backed up. Note the expanded tree display in the right-hand pane, indicating exactly what will be backed up. Under **Backup Options**, the Legacy Backup radio button is selected.

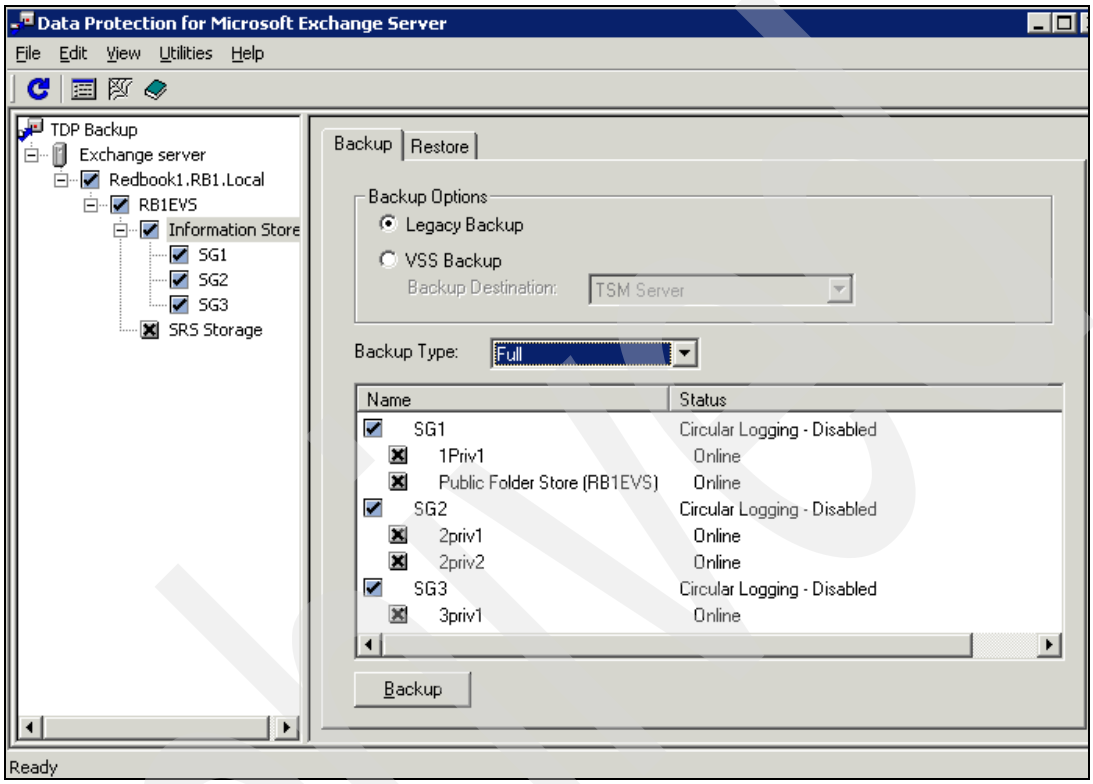


Figure 4-8 Legacy full backup

We clicked **Backup** to start the operation. Figure 4-9 on page 110 shows the progress message.

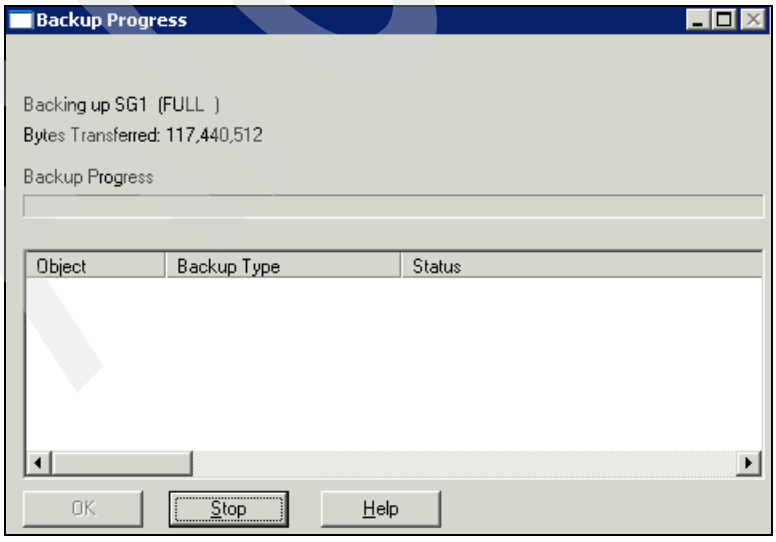


Figure 4-9 Backup progress

After the backup is complete, the completion message in Figure 4-10 is displayed. We clicked **OK** to finish. If any errors appear, it means that the backup has failed.

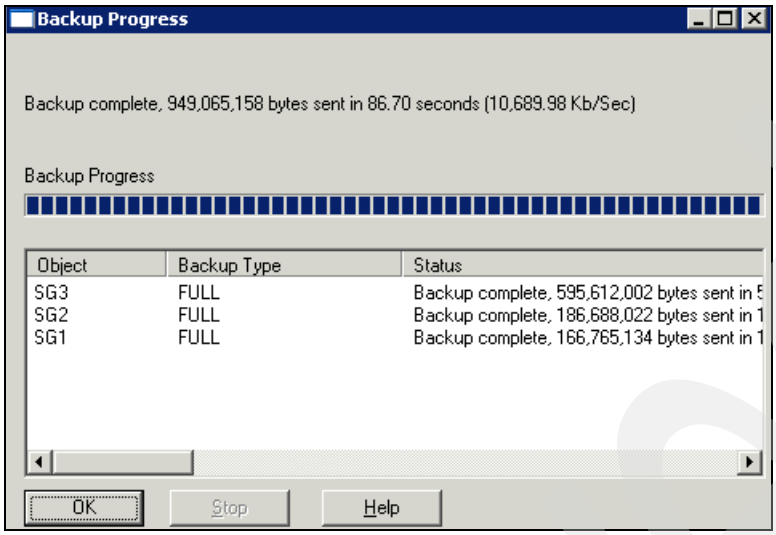


Figure 4-10 Backup complete

To check on the backup, click the **Restore** tab, as shown in Figure 4-11. This display shows that Tivoli Storage Manager recognizes that a legacy full backup has completed and also what management class it is bound to. You can see that the backup has included all the Storage Groups, since there is one entry for each Storage Group.

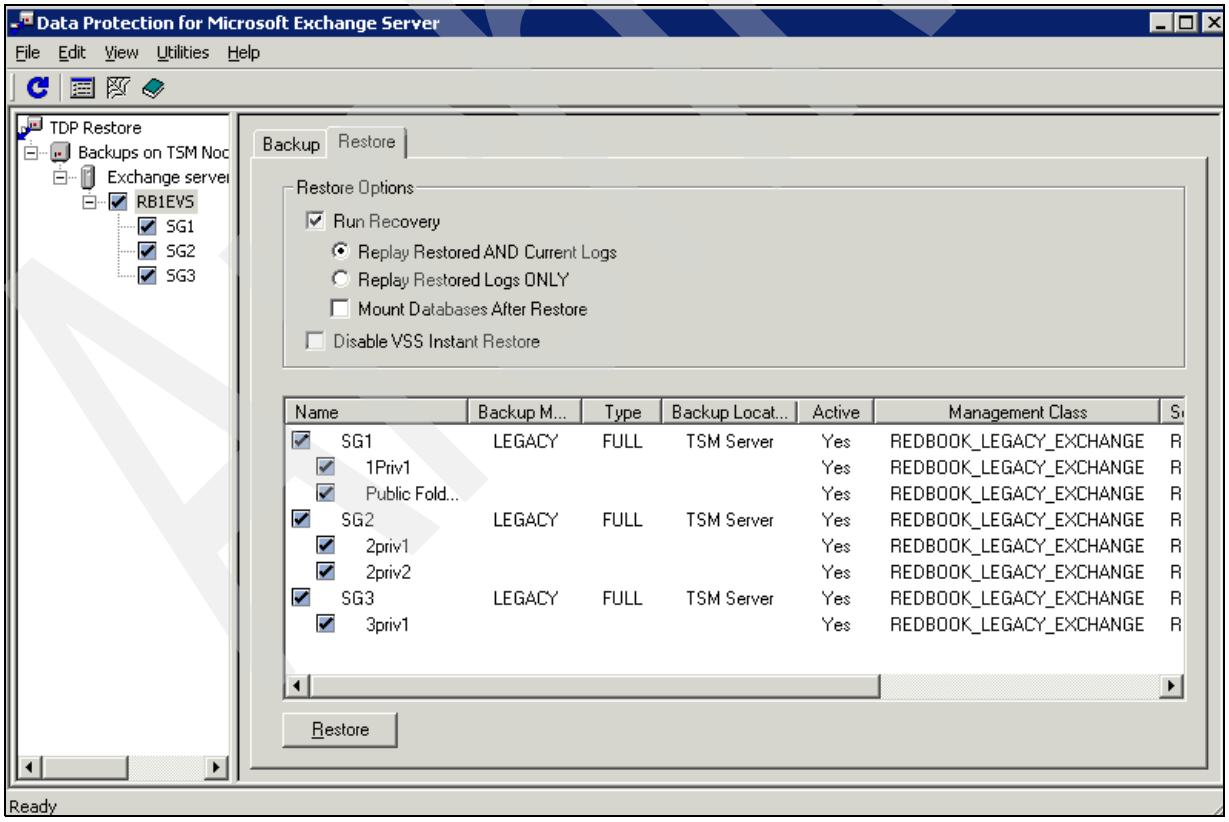


Figure 4-11 Legacy backup display

4.4.2 CLI legacy full backup

Example 4-1 shows the same operation using the command line.

Example 4-1 CLI for a legacy full backup

```
C:\PROGRA~1\Tivoli\TSM\TDPExchange>tdpexcc backup * full /backupdestination=TSM
/backupmethod=LEGACY /EXCSERVER=RB1EVS

IBM Tivoli Storage Manager for Mail:
Data Protection for Microsoft Exchange Server
Version 5, Release 3, Level 3.0
(C) Copyright IBM Corporation 1998, 2006. All rights reserved.

Starting storage group backup...

Beginning full backup of SG1, 1 of 3.
Full: 0   Read: 166765134  Written: 166765134  Rate: 10,948.34 Kb/Sec
Backup of SG1 completed successfully.

Beginning full backup of SG2, 2 of 3.
Full: 0   Read: 186688022  Written: 186688022  Rate: 11,208.89 Kb/Sec
Backup of SG2 completed successfully.

Beginning full backup of SG3, 3 of 3.
Full: 0   Read: 595612002  Written: 595612002  Rate: 11,374.62 Kb/Sec
Backup of SG3 completed successfully.


Total storage groups requested for backup:  3
Total storage groups backed up:             3
Total storage groups expired:               0
Total storage groups excluded:              0

Throughput rate:                            11,235.42 Kb/Sec
Total bytes transferred:                    949,065,158
Elapsed processing time:                    82.49 Secs
```

4.4.3 GUI legacy copy backup

Figure 4-12 on page 113 shows a copy legacy backup. It is the same as a full backup, except that the **Backup Type** is Copy.

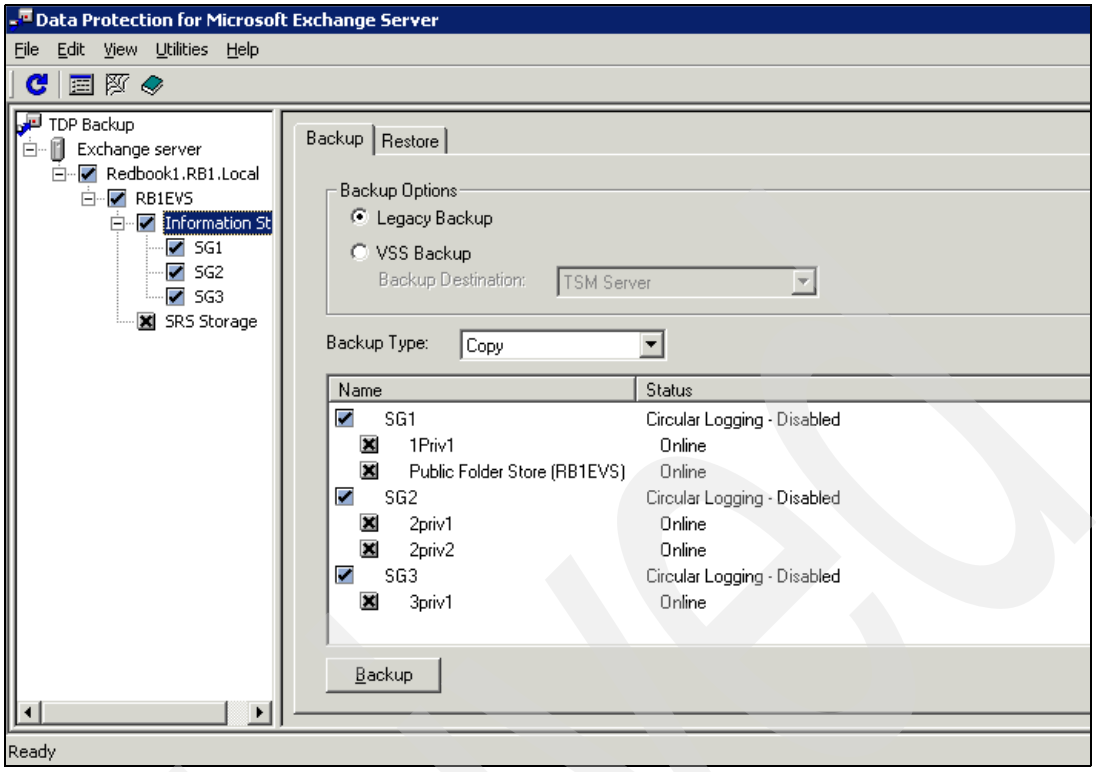


Figure 4-12 Copy backup

After the copy backup completes, we redisplay the stored backups, as shown in Figure 4-13 on page 114. Note that both backups are listed: the copy, and the full backup which we completed previously.

You can see that Tivoli Storage Manager recognizes the different backup types, and that the correct management classes have been used, as specified in our VSSPolicy statements.

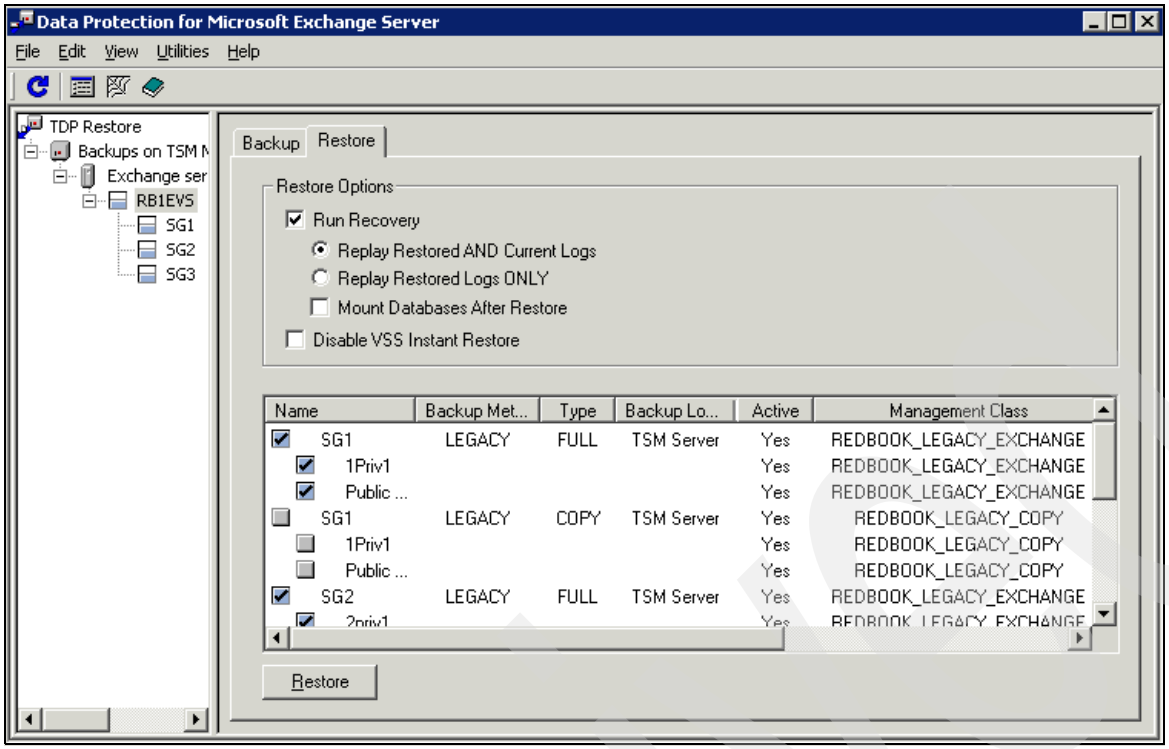


Figure 4-13 Legacy full and copy backups

4.4.4 CLI legacy copy backup

Example 4-2 shows you the same legacy copy backup, initiated from the command line.

Example 4-2 Command line for a legacy copy backup

```
C:\PROGRA~1\Tivoli\TSM\TDPExchange>tdpexcc backup * copy /backupdestination=TSM
/backupmethod=LEGACY /EXCSERVER=RB1EVS

IBM Tivoli Storage Manager for Mail:
Data Protection for Microsoft Exchange Server
Version 5, Release 3, Level 3.0
(C) Copyright IBM Corporation 1998, 2006. All rights reserved.

Starting storage group backup...

Beginning copy backup of SG1, 1 of 3.
Full: 0   Read: 166765134  Written: 166765134  Rate: 11,028.41 Kb/Sec
Backup of SG1 completed successfully.

Beginning copy backup of SG2, 2 of 3.
Full: 0   Read: 191930958  Written: 191930958  Rate: 11,057.97 Kb/Sec
Backup of SG2 completed successfully.

Beginning copy backup of SG3, 3 of 3.
Full: 0   Read: 590369066  Written: 590369066  Rate: 11,384.92 Kb/Sec
Backup of SG3 completed successfully.


Total storage groups requested for backup:  3
```

```
Total storage groups backed up:            3
Total storage groups expired:              0
Total storage groups excluded:             0

Throughput rate:                           11,251.52 Kb/Sec
Total bytes transferred:                   949,065,158
Elapsed processing time:                   82.37 Secs
```

Legacy backups are maintained according to the specified policy in the management class; they expire independently of the VSS backups.

4.5 VSS Exchange backup

This procedure assumes that Data Protection for Exchange, Tivoli Storage Manager backup-archive client, the Tivoli Storage Manager server, the Tivoli Storage Manager for Copy Services and the disk system are properly configured in your environment. You must have local registry rights (for all versions of Exchange Server) to perform Data Protection for Exchange backups. You must have suitable target LUNs in your disk system assigned to the VSS_FREE pool for use as snapshot target volumes, as discussed in 3.2.14, “Define storage space to hold VSS backups” on page 82.

This is the general procedure to perform a VSS backup; in other sections we show specific examples.

1. Confirm that the Local DSMAgent Nodename is correctly specified. You can confirm this node name in the Data Protection for Exchange window - select **Edit** → **Configuration** → **VSS Backup Tab**. Figure 4-5 on page 104 shows you how to specify this option.
2. Start the Data Protection for Exchange GUI. Remember that if your Exchange server is clustered, the /excserver parameter is required, or use a shortcut as shown in “Create a Data Protection for Exchange GUI shortcut” on page 62.
3. From the Tree View, select one or more storage groups to backup up. You can also select one or more storage groups to backup up in the List View.
4. In the **Backup Options** section of the Backup window, select the VSS Backup method. Note that this method will automatically be selected if the **Use VSS as the default Backup method** parameter is selected in the Data Protection for Exchange configuration window (as shown in Figure 4-2 on page 101).
5. Specify the storage destination of your backup from the **Backup Destination** drop-down menu.
6. Specify the type of backup to perform from the **Backup Type** drop-down menu.
7. Click **Backup** to begin the backup operation.

4.5.1 GUI VSS full backup to Tivoli Storage Manager

In Figure 4-14 on page 116, we selected a full VSS backup of all Exchange storage groups to Tivoli Storage Manager. The **Backup Destination** is TSM Server, and the **Backup Type** is full. We clicked **Backup** to start the backup.

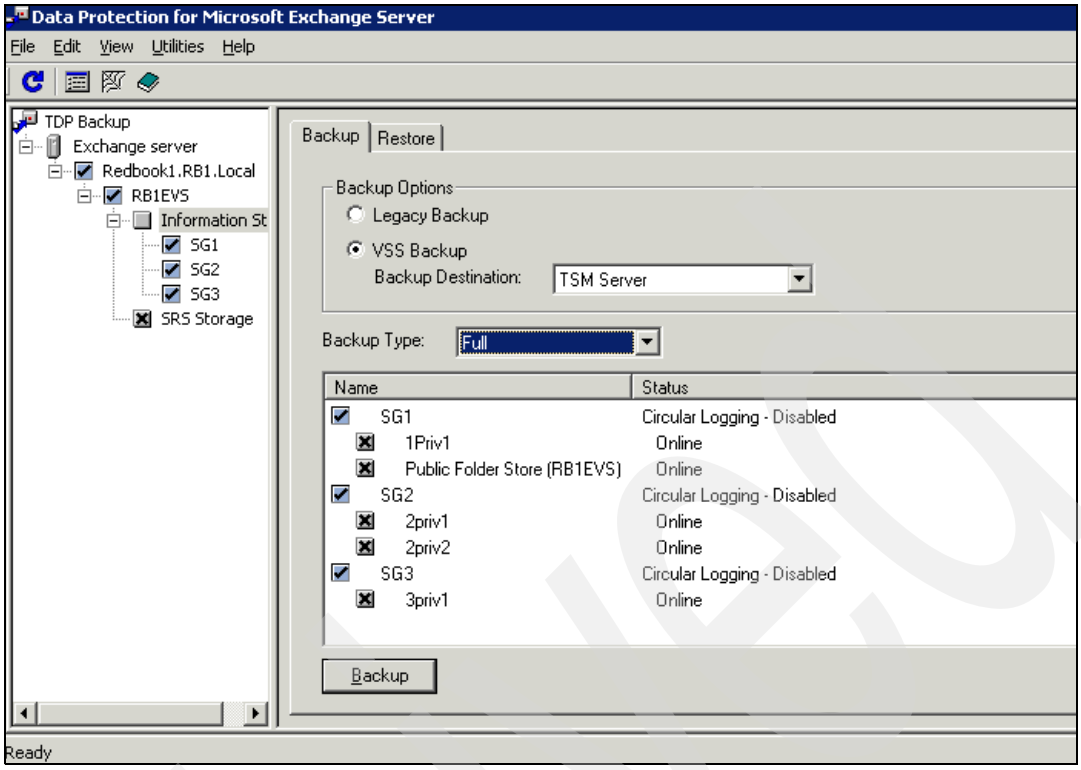


Figure 4-14 VSS Tivoli Storage Manager full backup

Figure 4-15 shows that the Data Protection for Exchange client is connecting to the Local DSMAgent - REDBOOK_VSS_B; this is the local backup-archive client nodename.

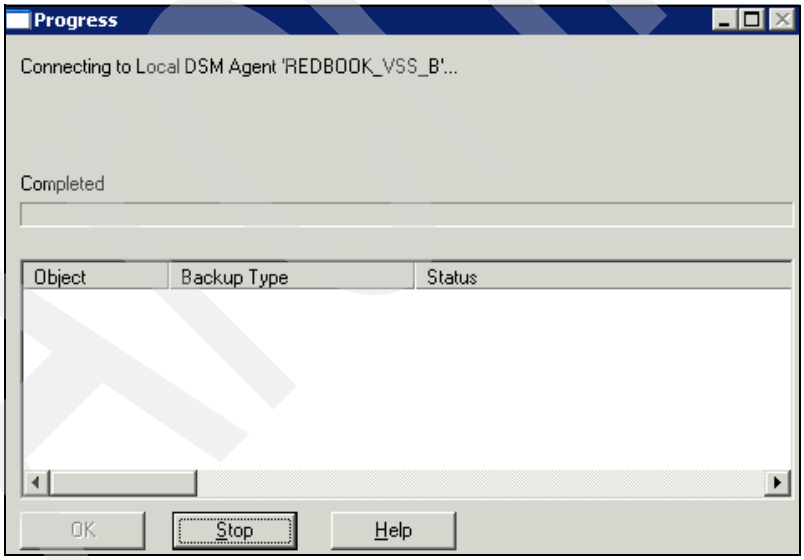


Figure 4-15 Backup process connecting to the local DSMAgent

Figure 4-16 on page 117 shows the start of a VSS backup of the Storage Groups specified.

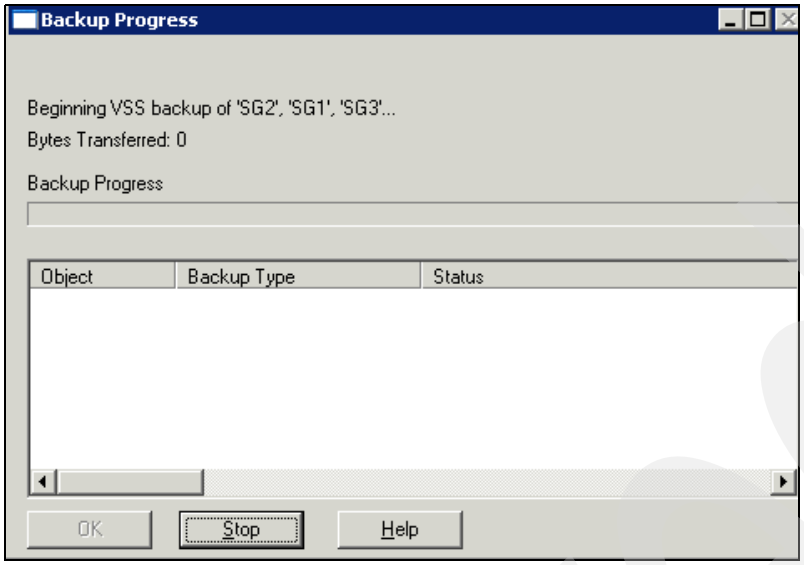


Figure 4-16 Backup process

Figure 4-17 shows that the Local DSMAgent is preparing a snapshot backup using the Data Protection for Exchange client.

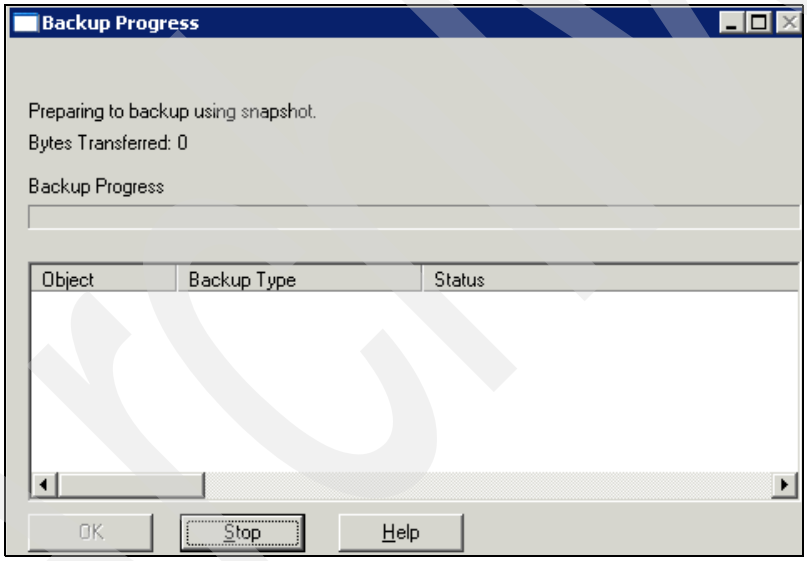


Figure 4-17 Backup process snapshot

As soon as the snapshot has been taken, the Exchange database is available for continuing end-user activity. The outage time to take the snapshot backup is short, typically in the order of seconds.

Figure 4-18 on page 118 shows the integrity check of the snapshot backup. The integrity check is always executed for full VSS backups. You can choose to not perform the integrity check for copy backups (see 4.5.3, “GUI VSS copy backup to Tivoli Storage Manager”). However, we recommend performing the integrity check in all cases.

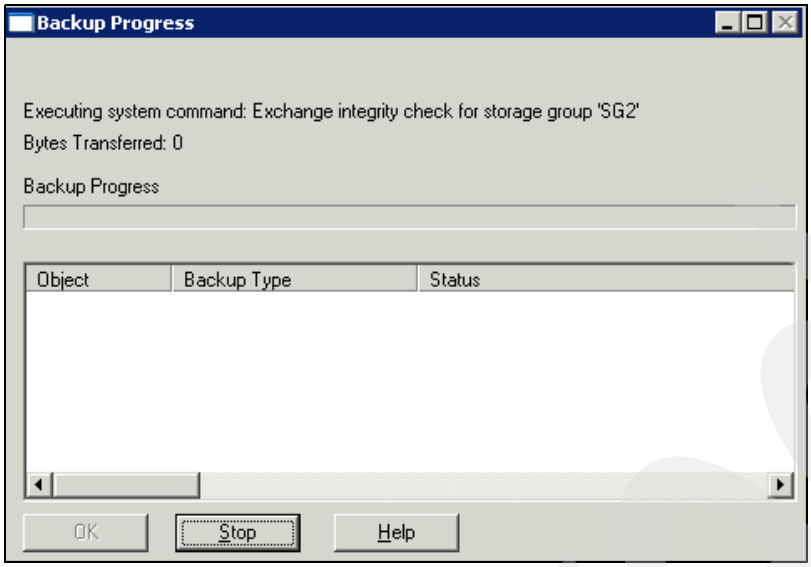


Figure 4-18 Integrity check

Now the backed-up data on the VSS snapshot is sent to Tivoli Storage Manager, as shown in in Figure 4-19. Under the covers, a non-persistent VSS snapshot was made.

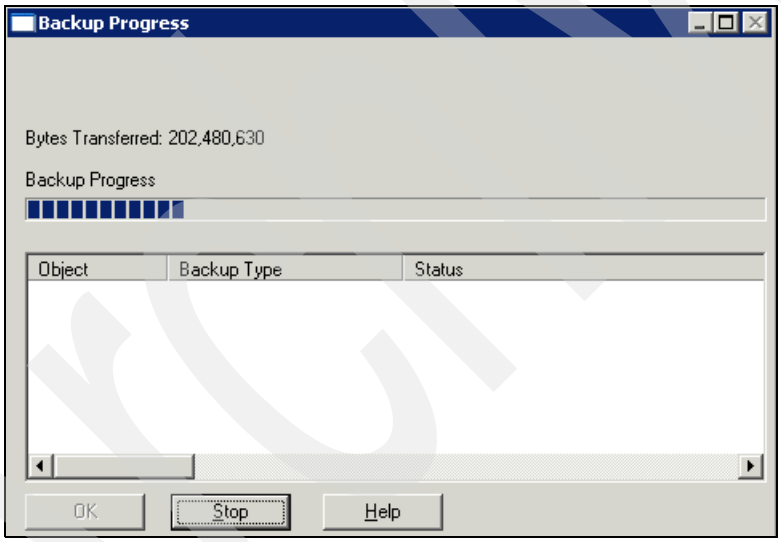


Figure 4-19 VSS Tivoli Storage Manager backup progress

Figure 4-20 on page 119 shows the completion of the Exchange backup to Tivoli Storage Manager. We clicked **OK** to finish.

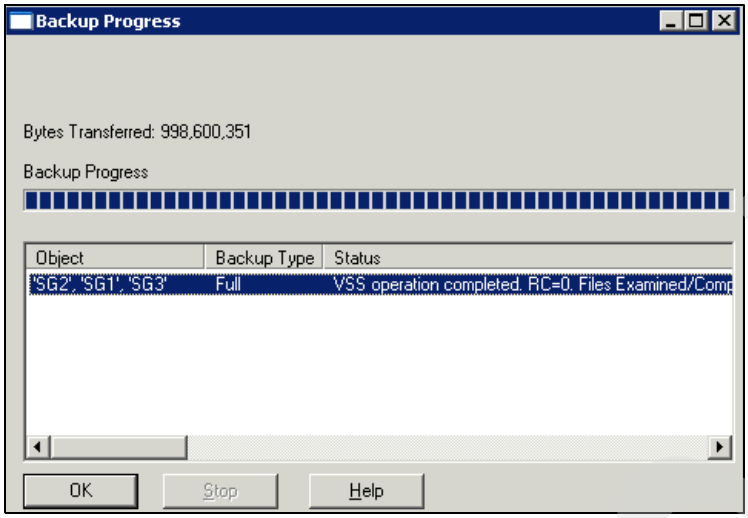


Figure 4-20 VSS Tivoli Storage Manager backup complete

When we look at the backup just made, via the Restore tab, Figure 4-21 shows how Tivoli Storage Manager separates the legacy and VSS backups. As previously mentioned, these backups are expired according to their policy settings. The legacy and VSS backups expire independently from one another.

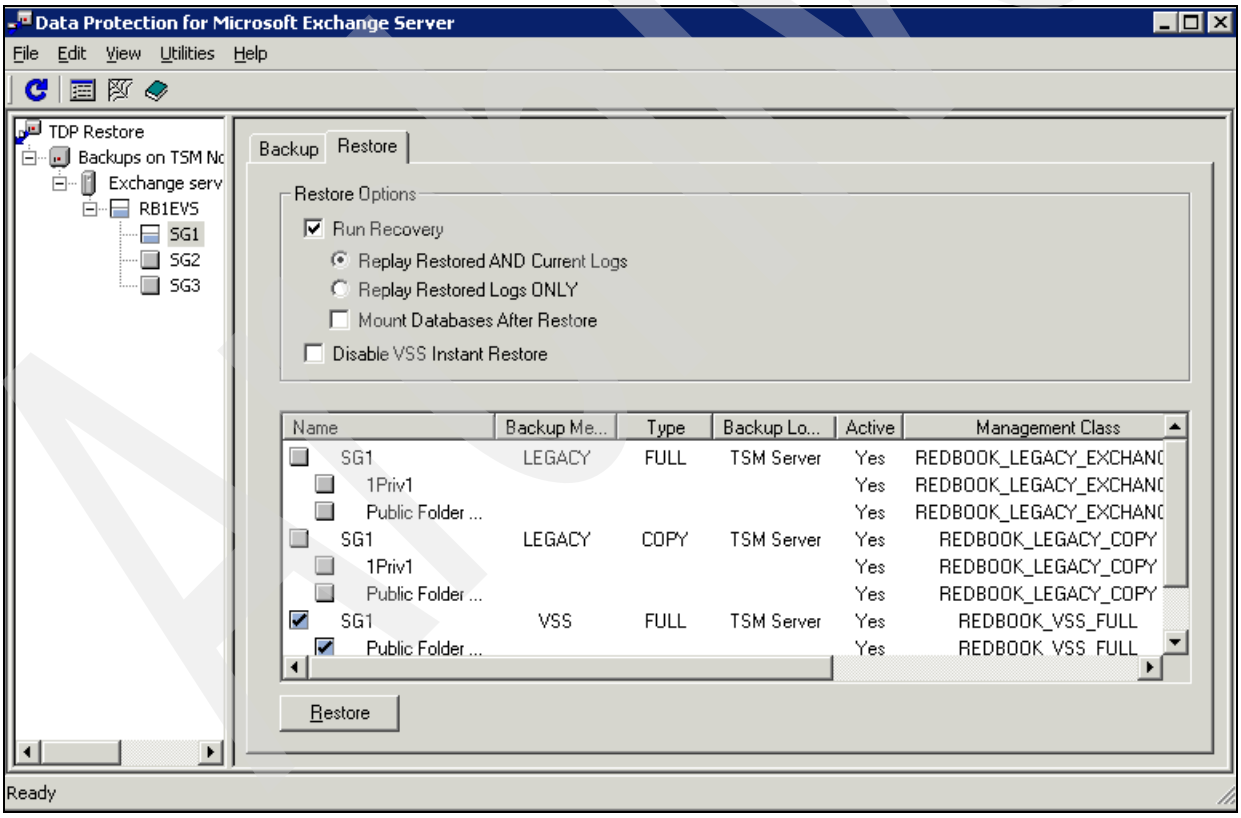


Figure 4-21 Confirmation of status of backups

4.5.2 CLI VSS full backup to Tivoli Storage Manager

Example 4-3 shows the command line option for a full VSS backup to Tivoli Storage Manager. We opted to back up all Storage Groups; however, you can back up your storage groups individually, if you prefer.

Note that in this backup, the Local DSMAgent is now REDBOOK_VSS_A. This is because the Exchange server is now running on the other node in the cluster; because we have a clustered environment, we can run backups from whichever node is hosting the Exchange instance.

Example 4-3 Command line option for a full VSS backup to Tivoli Storage Manager

```
C:\PROGRA~1\Tivoli\TSM\TDPExchange>tdpexcc backup * FULL /backupdestination=TSM
/backupmethod=VSS /EXCSERVER=RB1EVS

IBM Tivoli Storage Manager for Mail:
Data Protection for Microsoft Exchange Server
Version 5, Release 3, Level 3.0
(C) Copyright IBM Corporation 1998, 2006. All rights reserved.

Connecting to TSM Server as node 'REDBOOK_EXCHANGE'...
Connecting to Local DSM Agent 'REDBOOK_VSS_A'...
Starting storage group backup...

Beginning VSS backup of 'SG2', 'SG1', 'SG3'...


Preparing to backup using snapshot.
Executing system command: Exchange integrity check for storage group 'SG2'
Executing system command: Exchange integrity check for storage group 'SG1' 0
Executing system command: Exchange integrity check for storage group 'SG3' 6
   Files Examined/Completed/Failed: [ 74 / 74 / 0 ]   Total Bytes: 996502864

VSS Backup operation completed with rc = 0
   Files Examined   : 74
   Files Completed  : 74
   Files Failed     : 0
   Total Bytes      : 996502864
```

4.5.3 GUI VSS copy backup to Tivoli Storage Manager

Figure 4-22 on page 121 shows a copy backup of the Exchange Storage Groups. A Copy backup backs up the Storage Groups and the Exchange transaction logs but (unlike a full backup) does not delete the logs after the backup completes.

If you prefer, you can choose not to do an integrity check when running a copy backup; this decreases the time taken for the backup. To do this, select Backup type **Copy without Integrity Check**.

We opted to use the integrity check option for this copy backup (which is recommended), by selecting Backup type of **Copy**. We clicked **Backup** to start.

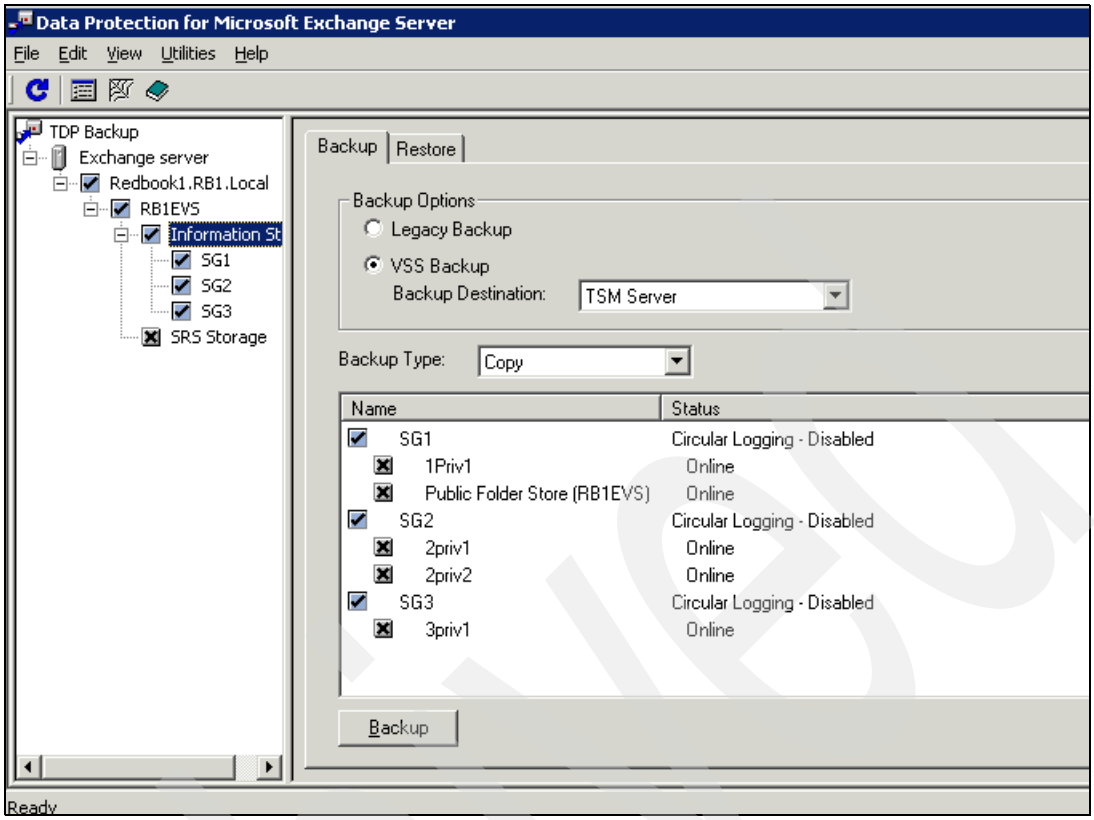


Figure 4-22 Tivoli Storage Manager VSS copy backup

Figure 4-23 shows that the Copy backup completed successfully. The intervening screenshots are the same as shown in 4.5.1, “GUI VSS full backup to Tivoli Storage Manager”. We clicked **OK** to finish the backup.

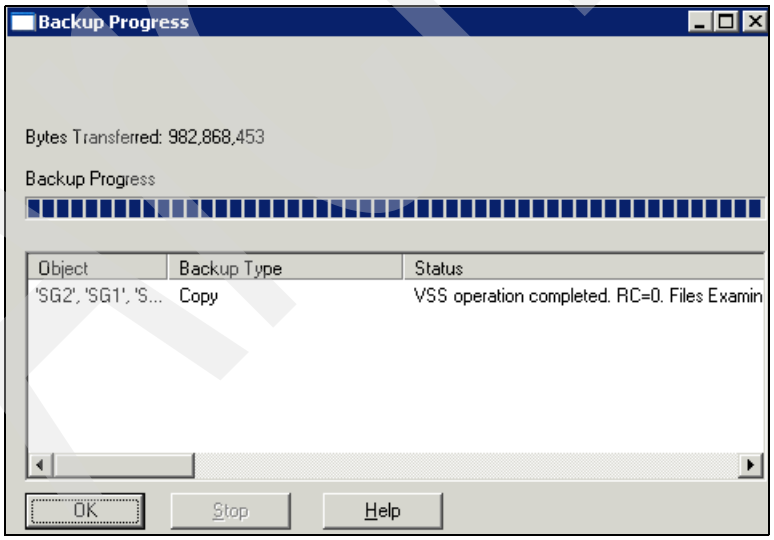


Figure 4-23 Tivoli Storage Manager VSS copy backup completion

Figure 4-24 on page 122 shows the new VSS copy backup listed.

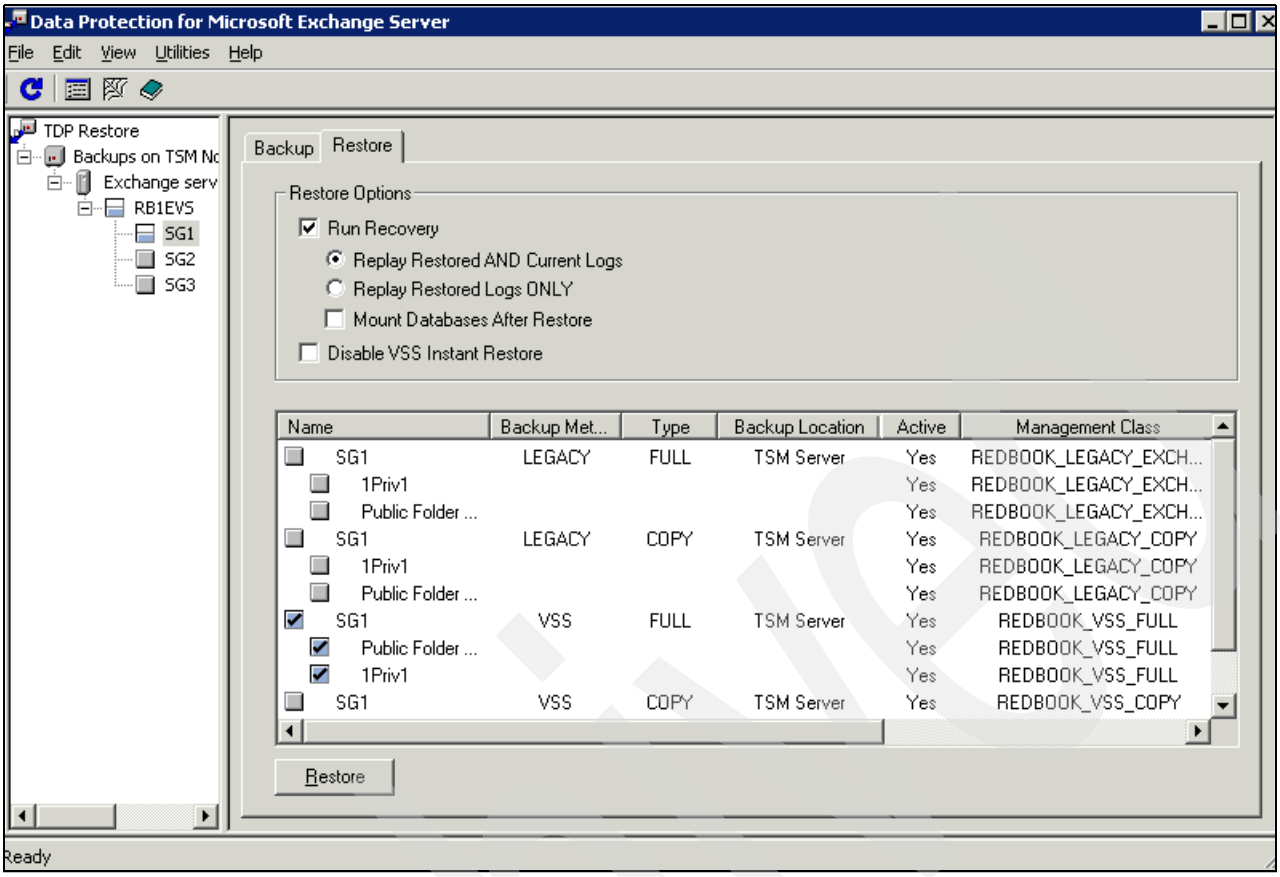


Figure 4-24 Backup status confirmation

4.5.4 CLI copy backup to Tivoli Storage Manager

Figure 4-4 on page 122 shows how to do a CLI copy VSS backup of all Storage Groups to Tivoli Storage Manager.

The default is to execute the integrity check. To skip this, use the **/SKIPINTEGRITYCHECK** option.

Example 4-4 VSS Tivoli Storage Manager CLI copy backup

```
C:\PROGRA~1\Tivoli\TSM\TDPExchange>tdpexcc backup * COPY /backupdestination=TSM
/backupmethod=VSS /EXCSERVER=RB1EVS

IBM Tivoli Storage Manager for Mail:
Data Protection for Microsoft Exchange Server
Version 5, Release 3, Level 3.0
(C) Copyright IBM Corporation 1998, 2006. All rights reserved.

Connecting to TSM Server as node 'REDBOOK_EXCHANGE'...
Connecting to Local DSM Agent 'REDBOOK_VSS_A'...
Starting storage group backup...

Beginning VSS backup of 'SG2', 'SG1', 'SG3'...


Preparing to backup using snapshot.
```

```
Executing system command: Exchange integrity check for storage group 'SG2'
Executing system command: Exchange integrity check for storage group 'SG1' 2
Executing system command: Exchange integrity check for storage group 'SG3' 1
   Files Examined/Completed/Failed: [ 71 / 71 / 0 ]   Total Bytes: 980771214

VSS Backup operation completed with rc = 0
   Files Examined   : 71
   Files Completed  : 71
   Files Failed     : 0
   Total Bytes      : 980771214
```

4.5.5 GUI VSS offloaded backup

Figure 4-25 on page 123 shows how to select an offloaded backup. You can only do this if you have configured an offloaded backup server. In this case, after the snapshot is complete, the snapshot disks are backed up to Tivoli Storage Manager by the offloaded backup server, thereby minimizing the performance impact of the backup operation on the Exchange server.

We selected TSM Server (Offloaded) as the **VSS Backup Destination**. We clicked **Backup** to start the backup operation. The offloaded backups server is automatically invoked to perform the backup; however, you cannot tell that this is happening. But you can monitor the Tivoli Storage Manager server sessions to see what is going on, as shown in Example 4-10 on page 132.

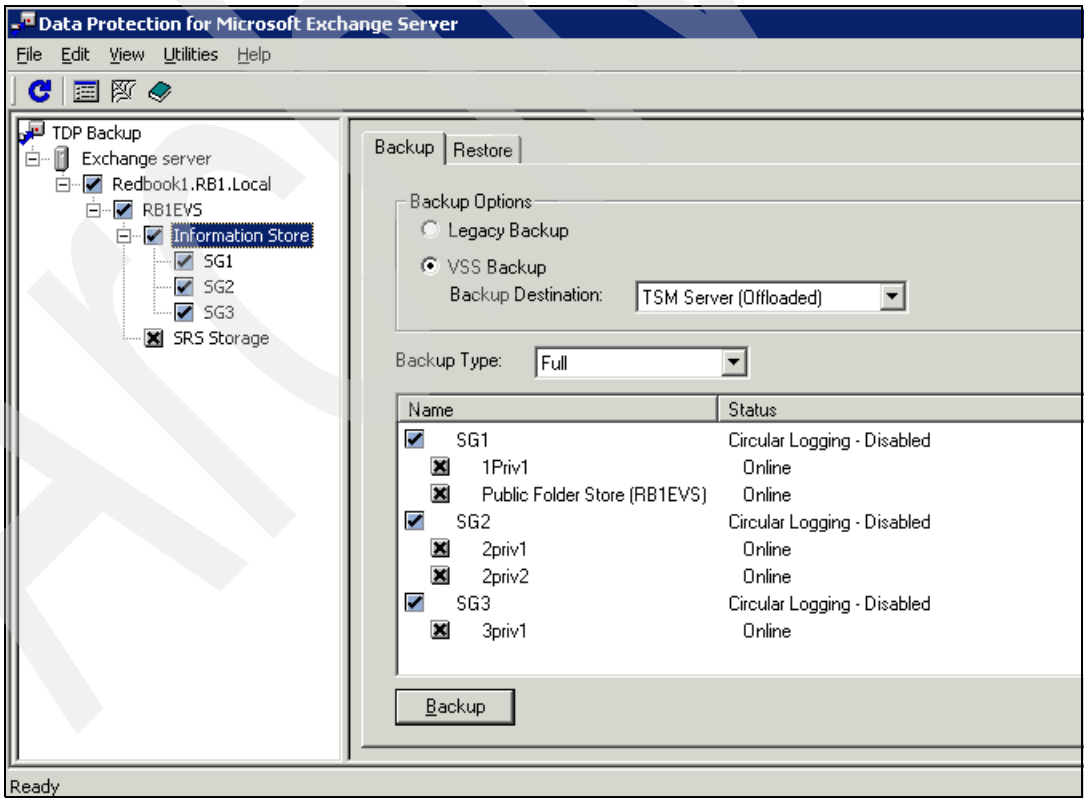


Figure 4-25 VSS offloaded backup

Figure 4-26 shows the completion of an offloaded backup. We clicked **OK** to complete the backup process. The intervening screenshots are the same as shown in 4.5.1, “GUI VSS full backup to Tivoli Storage Manager”.

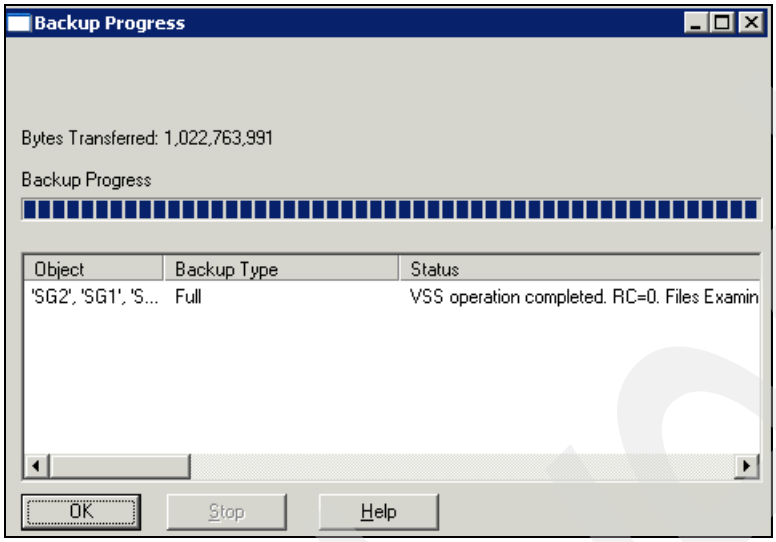


Figure 4-26 VSS offload backup completion

4.5.6 CLI VSS offloaded backup

Example 4-5 shows you the command line option for an offloaded full VSS backup to Tivoli Storage Manager. We opted to back up all Storage Groups. However, you can choose individual Storage Groups, if you prefer.

Note that, as with the GUI, there is no indication that an offloaded backup is being performed. However, you can monitor the Tivoli Storage Manager server sessions to see what is going on, as shown in Example 4-10 on page 132.

Example 4-5 VSS offload ed backup using the CLI

```
C:\PROGRA~1\Tivoli\TSM\TDPExchange>tdpexcc backup * FULL /backupdestination=TSM
/backupmethod=VSS /EXCSERVER=RB1EVS /OFFLOAD

IBM Tivoli Storage Manager for Mail:
Data Protection for Microsoft Exchange Server
Version 5, Release 3, Level 3.0
(C) Copyright IBM Corporation 1998, 2006. All rights reserved.

Connecting to TSM Server as node 'REDBOOK_EXCHANGE'...
Connecting to Local DSM Agent 'REDBOOK_VSS_A'...
Starting storage group backup...

Beginning VSS backup of 'SG2', 'SG1', 'SG3'...


Preparing to backup using snapshot.
Preparing to backup using snapshot
Preparing to backup using snapshot.
Executing system command: Exchange integrity check for storage group 'SG2'
Executing system command: Exchange integrity check for storage group 'SG2'
Executing system command: Exchange integrity check for storage group 'SG2'
```

```
Executing system command: Exchange integrity check for storage group 'SG1'
Executing system command: Exchange integrity check for storage group 'SG1'06
Executing system command: Exchange integrity check for storage group 'SG1' 6
Executing system command: Exchange integrity check for storage group 'SG3' 8
Executing system command: Exchange integrity check for storage group 'SG3'34
Executing system command: Exchange integrity check for storage group 'SG3' 4
   Files Examined/Completed/Failed: [ 67 / 67 / 0 ]   Total Bytes: 975568516

VSS Backup operation completed with rc = 0
   Files Examined   : 67
   Files Completed  : 67
   Files Failed     : 0
   Total Bytes      : 975568516
```

4.5.7 GUI VSS local backup

Figure 4-27 shows a VSS local backup of all the Exchange Storage Groups. This type of backup makes a persistent snapshot backup to the SAN disks. The **Backup Destination** is selected as local. The data expiration is based on your policy setting. Click **Backup** to start the backup.

Important: If you plan to use Instant Restore on SVC, back up each Storage Group as a separate operation. An Instant Restore must be performed on the same objects that were originally backed up to LOCAL, because of the way the SVC Consistency Groups work. Backing up each Storage Group separately will allow you to have maximum flexibility in what you select for Instant Restore.

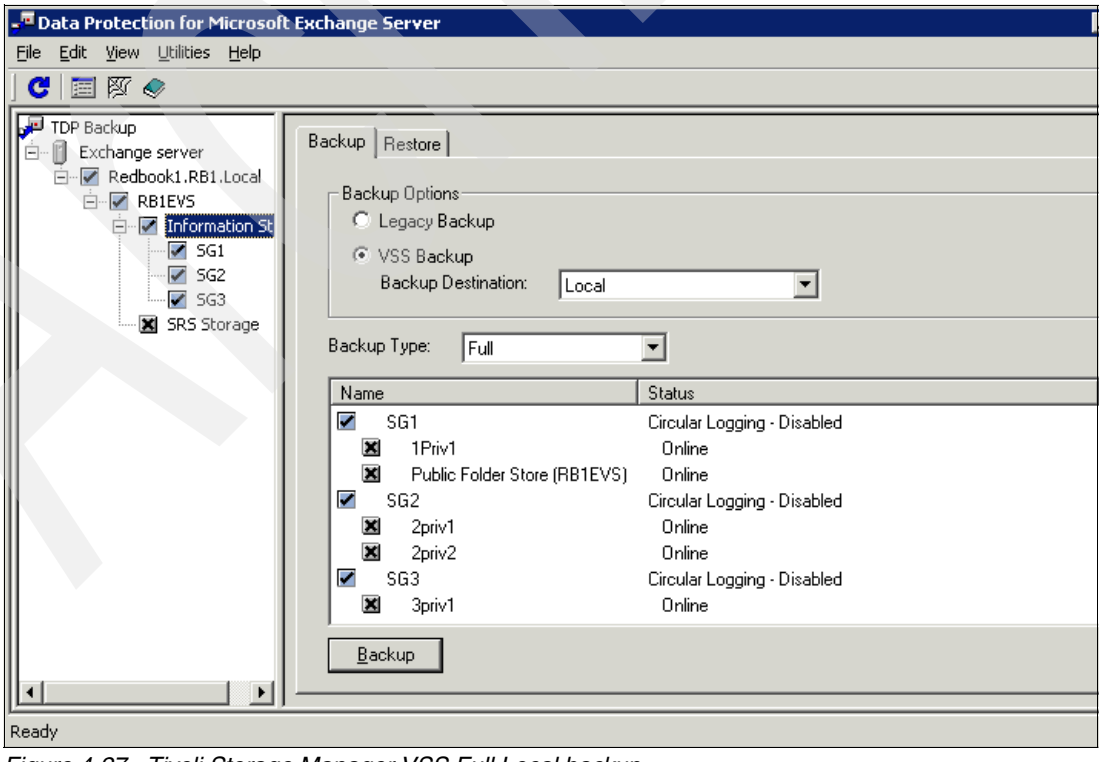


Figure 4-27 Tivoli Storage Manager VSS Full Local backup

Figure 4-28 on page 126 shows the progress of a VSS local backup.

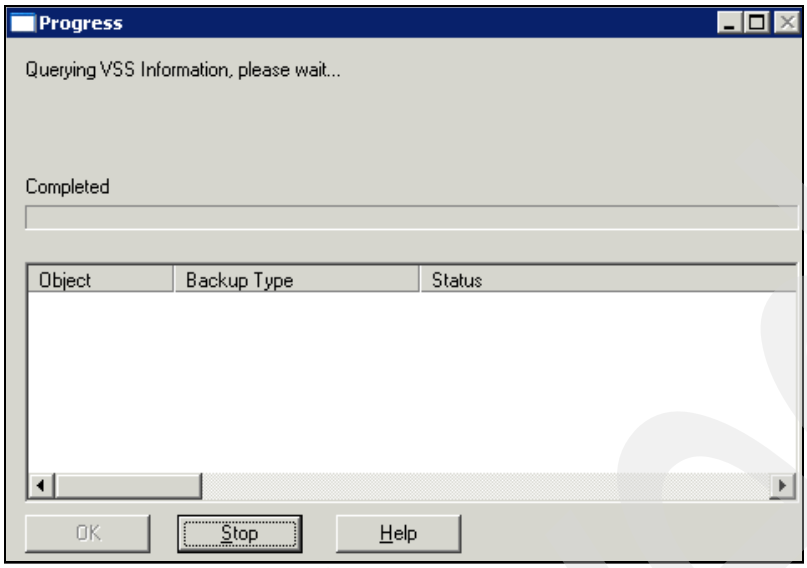


Figure 4-28 VSS Local backup progress

Figure 4-29 shows the successful completion of a VSS local backup.The intervening screenshots are the same as in 4.5.1, “GUI VSS full backup to Tivoli Storage Manager”. Click **OK** to finish.

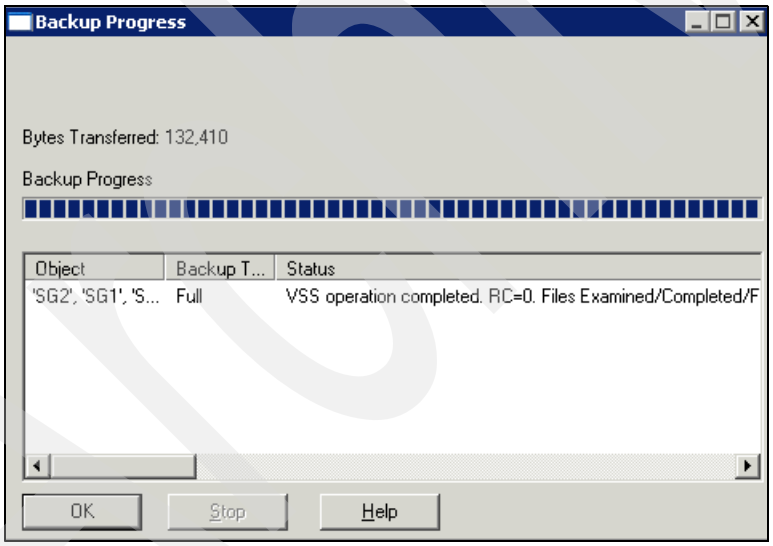


Figure 4-29 VSS local backup complete

Figure 4-30 on page 127 shows the new backup listed.

Cluster environment considerations: Local VSS backups are visible only from the Exchange cluster node where they were created. Therefore, they can only be restored from the Exchange cluster node from where it was created. This is due to a Microsoft restriction at the time of writing. If you cannot see a particular local backup object, retry on the other cluster node.

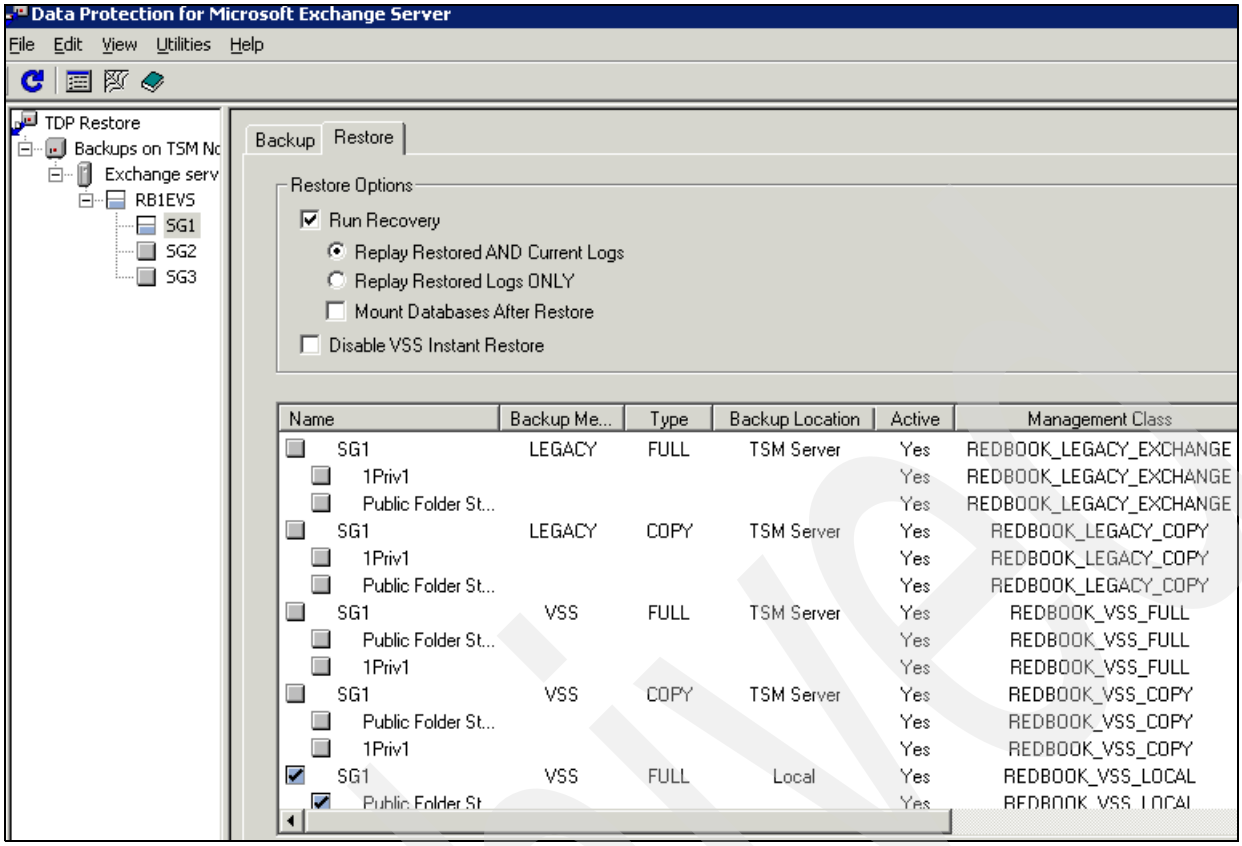


Figure 4-30 List of backups

4.5.8 CLI VSS local backup

Example 4-6 shows the command line option for a local VSS backup. In this example, we backed up a single Exchange Storage Group, SG2, instead of using the wildcard, an asterisk (*), to back up all Storage Groups.

Example 4-6 CLI VSS local backup

```
C:\PROGRA~1\Tivoli\TSM\TDPExchange>tdpexcc backup "SG2" FULL
/backupdestination=LOCAL /backupmethod=VSS /EXCSERVER=RB1EV
S

IBM Tivoli Storage Manager for Mail:
Data Protection for Microsoft Exchange Server
Version 5, Release 3, Level 3.0
(C) Copyright IBM Corporation 1998, 2006. All rights reserved.

Connecting to TSM Server as node 'REDBOOK_EXCHANGE'...
Connecting to Local DSM Agent 'REDBOOK_VSS_A'...
Starting storage group backup...

Beginning VSS backup of 'SG2'...


Preparing to backup using snapshot.
Executing system command: Exchange integrity check for storage group 'SG2'
   Files Examined/Completed/Failed: [ 13 / 13 / 0 ]   Total Bytes: 32149
```

```
VSS Backup operation completed with rc = 0
   Files Examined   : 13
   Files Completed  : 13
   Files Failed     : 0
   Total Bytes      : 32149
```

4.5.9 GUI VSS backup to both

This type of backup makes a copy of your Exchange database to a snapshot disk, and also sends it to the Tivoli Storage Manager server. Figure 4-31 on page 128 shows how to select this option, with the **Backup Destination** of Both. Click **Backup** to start the backup.

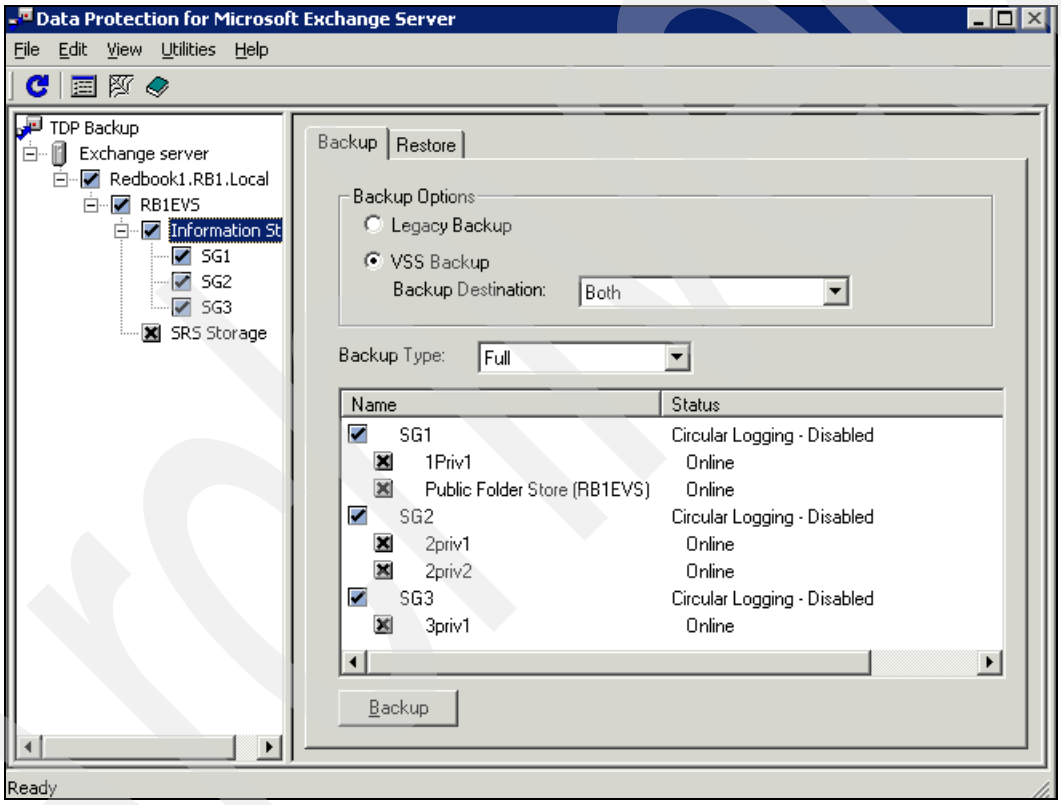


Figure 4-31 VSS Both option backup

Figure 4-32 on page 129 shows that the VSS backup is complete. The intervening screenshots are the same as shown in 4.5.1, “GUI VSS full backup to Tivoli Storage Manager”.

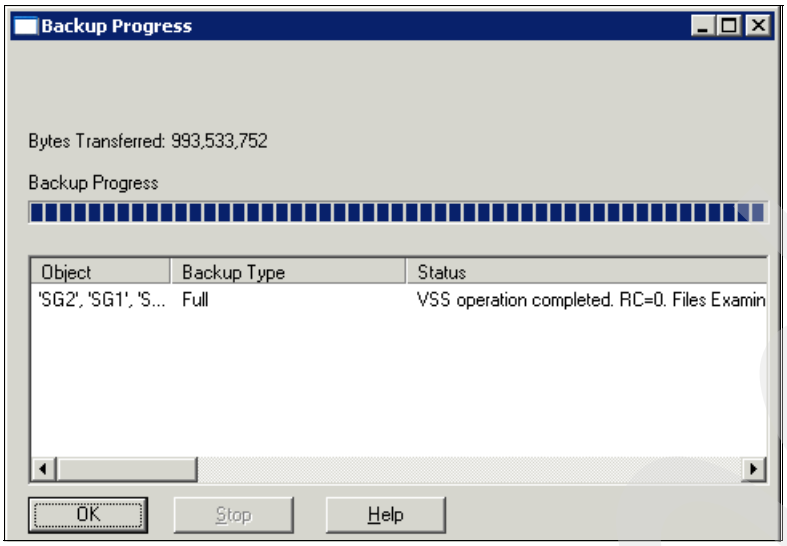


Figure 4-32 VSS Both backup progress

Figure 4-33 shows the new backup listed. Tivoli Storage Manager inactivates backups based on the backup type used. We had just run a backup with the Both option, which created a VSS local full and a VSS Tivoli Storage Manager full backup. Therefore, the previous VSS local and VSS Tivoli Storage Manager full backups were marked inactive and the backup we had just made was active. These inactivated backups will expire based on your policy settings.

You have to scroll through the full list of backups to see all the active and inactive backups.

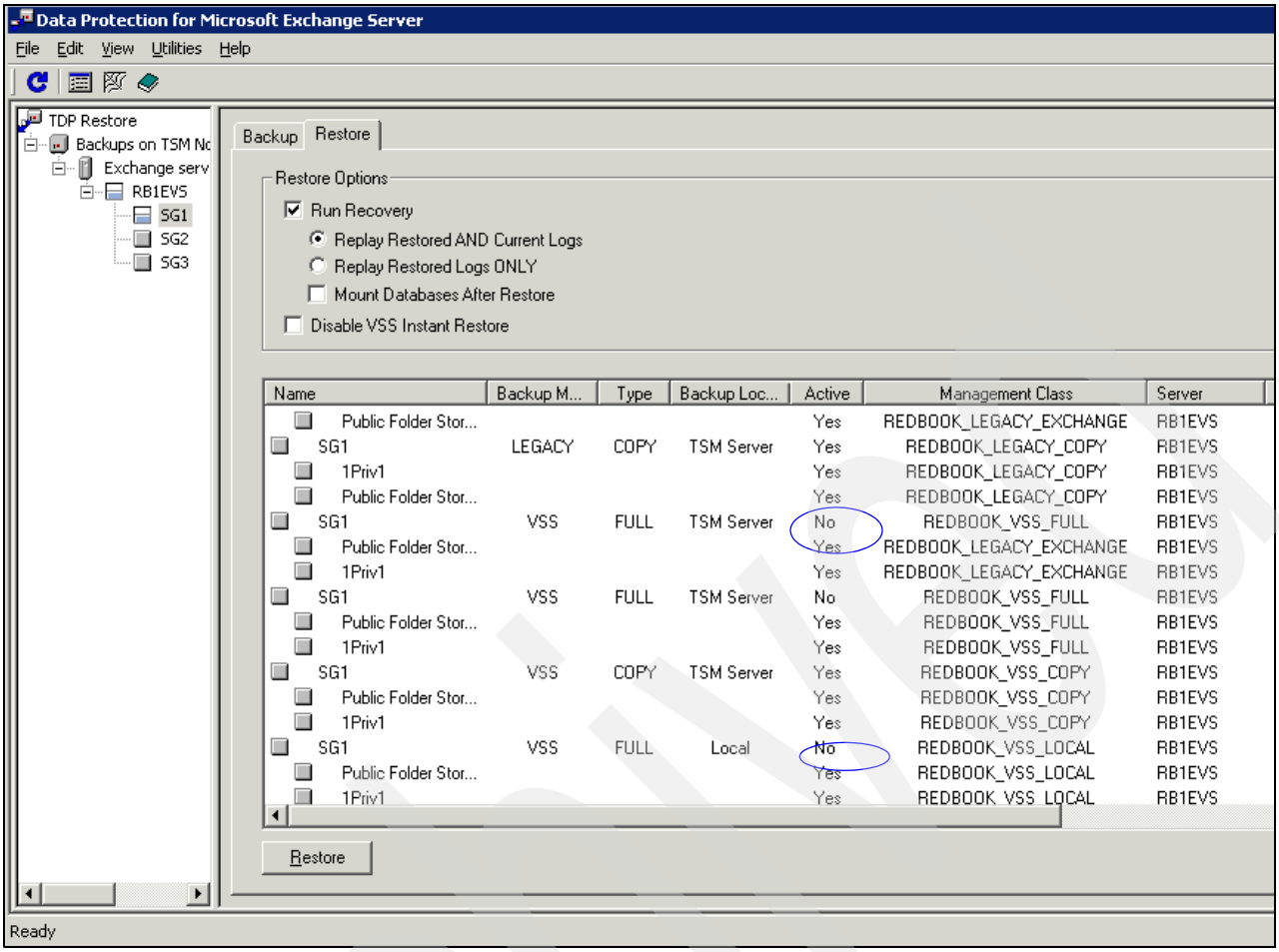


Figure 4-33 Tivoli Storage Manager backup management

4.5.10 CLI VSS backup to both

Example 4-7 shows how to run a backup to Both, using the CLI. In this case we selected a particular Storage Group (SG2) to back up.

Example 4-7 CLI for the Both option backup using VSS

```
C:\PROGRA~1\Tivoli\TSM\TDPExchange>tdpexcc backup "SG2" FULL
/backupdestination=BOTH /backupmethod=VSS /EXCSERVER=RB1EVS


IBM Tivoli Storage Manager for Mail:
Data Protection for Microsoft Exchange Server
Version 5, Release 3, Level 3.0
(C) Copyright IBM Corporation 1998, 2006. All rights reserved.

Connecting to TSM Server as node 'REDBOOK_EXCHANGE'...
Connecting to Local DSM Agent 'REDBOOK_VSS_A'...
Starting storage group backup...

Beginning VSS backup of 'SG2'...
```

```
Preparing to backup using snapshot.
Executing system command: Exchange integrity check for storage group 'SG2'
   Files Examined/Completed/Failed: [ 28 / 28 / 0 ]   Total Bytes: 197267607

VSS Backup operation completed with rc = 0
   Files Examined   : 28
   Files Completed  : 28
   Files Failed     : 0
   Total Bytes      : 197267607
```

4.5.11 Tivoli Storage Manager server sessions for a VSS backup

To supplement the output produced by the GUI or CLI, particularly for testing purposes, you will want to monitor the Tivoli Storage Manager server sessions during backups.

Example 4-8 shows the sessions on the Tivoli Storage Manager server (via the **QUERY SESSIONS** command) while a VSS backup to Tivoli Storage Manager is running. The Exchange server nodename (REDBOOK_EXCHANGE) initiates a session.

The Local DSMAgent (REDBOOK_VSS_B) session is actually backing up the Exchange data. You can see this, because the amount of data sent by the REDBOOK_VSS_B session is very high: 235.7 MB.

Example 4-8 VSS Tivoli Storage Manager backup sessions i

```
3,944 Tcp/Ip IdleW  5.8 M    3.2 K     518 Node  TDP MSE- REDBOOK_EXCHANGE
                                                  xchg
3,945 Tcp/Ip RecvW    0 S   42.7 K 235.7 M Node  TDP MSE- REDBOOK_EXCHANGE
                                                  xchg     (REDBOOK_VSS_B)
3,946 Tcp/Ip IdleW  5.7 M      537     294 Node  TDP MSE- REDBOOK_EXCHANGE
                                                  xchg     (REDBOOK_VSS_B)
```

Example 4-9 shows the sessions on the Tivoli Storage Manager server when running a local VSS backup. In this case, only metadata is sent to the Tivoli Storage Manager server. Therefore, the amount of data sent (76.8 K) is much lower compared with Example 4-8.

This metadata is stored in the storage pool for the management class to which local backups are bound.

Example 4-9 Local VSS Sessions and Metadata Sent to Tivoli Storage Manager

```
4,096 Tcp/Ip IdleW  5.2 M    3.2 K     518 Node  TDP MSE- REDBOOK_EXCHANGE
                                                  xchg
4,097 Tcp/Ip IdleW    0 S  112.2 K  76.8 K Node  TDP MSE- REDBOOK_EXCHANGE
                                                  xchg     (REDBOOK_VSS_A)
4,098 Tcp/Ip IdleW  5.1 M      537     294 Node  TDP MSE- REDBOOK_EXCHANGE
                                                  xchg     (REDBOOK_VSS_A)
```

Example 4-10 shows the sessions active when you run a VSS offloaded backup. The backup is initiated by the Exchange Server nodename (REDBOOK_EXCHANGE) - number 4,490. The Local DSMAgent (REDBOOK_VSS_B) starts a session which initiates the Remote DSMAgent (REDBOOK_OFFLOAD) that backs up the Exchange database. Note the most data is sent by the REDBOOK_OFFLOAD session, number 4,515.

Example 4-10 VSS OFFLOAD Backup Sessions in the Tivoli Storage Manager Server

```
4,490 Tcp/Ip IdleW  5.5 M    2.6 K     518 Node  TDP MSE- REDBOOK_EXCHANGE
                                                  xchg
4,491 Tcp/Ip IdleW    0 S    3.0 K   3.4 K Node  TDP MSE- REDBOOK_EXCHANGE
                                                  xchg     (REDBOOK_VSS_B)
4,493 Tcp/Ip IdleW  5.4 M      537     294 Node  TDP MSE- REDBOOK_EXCHANGE
                                                  xchg     (REDBOOK_VSS_B)
4,515 Tcp/Ip RecvW    0 S    2.9 K 110.6 M Node  TDP MSE- REDBOOK_EXCHANGE
                                                  xchg     (REDBOOK_OFFLOAD)
4,517 Tcp/Ip IdleW  1.3 M      537     297 Node  TDP MSE- REDBOOK_EXCHANGE
                                                  xchg     (REDBOOK_OFFLOAD)
```

We provide more information about monitoring backup operations, including logs, in 5.3, “Monitoring backups” on page 163 and 5.4, “Verifying backups” on page 164.

4.5.12 Exchange file spaces in Tivoli Storage Manager

Example 4-11 shows how Tivoli Storage Manager separates a legacy backup and a VSS backup in the Tivoli Storage Manager server. The first three backups show Filespace Type VSS, because they were done as VSS backups. The latter backups appear as Filespace Type API_ExcData.

All the file spaces are owned by the Exchange node name REDBOOK_EXCHANGE, regardless of which Local DSMagent actually performed the backup.

Example 4-11 Tivoli Storage Manager Query file space output

```
tsm: ZEALOT>q fi redbook_exchange

Node Name       Filespace   FSID Platform Filespace Is Files- Capacity   Pct
                Name                      Type        pace        (MB)  Util
                                                    Unicode?
--------------- ----------- ---- -------- --------- --------- -------- -----
REDBOOK_EXCHAN- RB1EVS\Mic-   29 TDP MSE- VSS          Yes         0.0   0.0
 GE             rosoft           xchg
                Exchange
                Writer\{7-
                6fe1ac4-1-
                5f7-4bcd--
                987e-8e1a-
                cb462fb7}-
                \SG2\acbd-
                96c6-9655-
                -474f-bd6-
                8-75513bf-
                41cbf
REDBOOK_EXCHAN- RB1EVS\Mic-   30 TDP MSE- VSS          Yes         0.0   0.0
 GE             rosoft           xchg
                Exchange
                Writer\{7-
                6fe1ac4-1-
                5f7-4bcd--
                987e-8e1a-
                cb462fb7}-
```

```
                \SG1\b2e8-
                6828-8f9a-
                -4a8a-97b-
                4-f76cb1c-
                14443
REDBOOK_EXCHAN- RB1EVS\Mic-   31 TDP MSE- VSS          Yes         0.0   0.0
 GE             rosoft           xchg
                Exchange
                Writer\{7-
                6fe1ac4-1-
                5f7-4bcd--
                987e-8e1a-
                cb462fb7}-
                \SG3\ef0d-
                26ab-fc9a-
                -4ba6-ba5-
                1-2bb5bdd-
                b610d
REDBOOK_EXCHAN- RB1EVS\SG2    32 TDP MSE- API:ExcD-     No          0.0   0.0
 GE                               xchg     ata
REDBOOK_EXCHAN- RB1EVS\SG3    33 TDP MSE- API:ExcD-     No          0.0   0.0
 GE                               xchg     ata
REDBOOK_EXCHAN- RB1EVS\SG1    34 TDP MSE- API:ExcD-     No          0.0   0.0
 GE                               xchg     ata
```

4.6 Legacy Exchange restore

Note: You must have local registry rights (for all versions of Exchange Server) to perform a Data Protection for Exchange restore.

When you restore a Storage Group, be aware that data which exists in the Storage Group is overwritten and is no longer available after the restore is complete.

Perform the following steps to restore an Exchange server Storage Group:

1. Start the Data Protection for Exchange GUI.
2. Click the **Restore** tab.
3. From the Tree View, select the Exchange server Storage Group to restore. To restore a particular database, first highlight the Storage Group in the Tree View. Then select the database to be restored in the List View. To restore all available Storage Groups, highlight the Exchange server in the Tree View.

   The List View displays the following information about your backups:

   – Backup Method (Legacy or VSS)
   – Type (Full, Incremental, Differential, Copy, Database Copy)
   – Backup Location (TSM Server or VSS Device)
   – Management Class (The Tivoli Storage Manager server management class to which the backup belongs.)

4. Select the appropriate restore options that you want to perform.
5. Click **Restore** to begin the restore operation.

Note: When performing a restore of mailbox databases with Exchange Server 2003, if a Recovery Storage Group exists, mailbox databases will be restored to the Recovery Storage Group instead of to the original storage group. Also, when restoring a mailbox database to a Recovery Storage Group, you must specify the **Replay Restored Logs ONLY** option in the GUI Restore Window; otherwise, the restore operation may fail.

This note *only* applies to legacy restores. VSS Restores to the Recovery Storage Group are not supported by Microsoft.

Microsoft recommendations for any restore should be adhered to. For further information with regard to legacy restores, refer to *Using Tivoli Data Protection for Microsoft Exchange Server*, SG24-6147 and *Data Protection for Microsoft Exchange Server Installation and Users Guide*, SC32-9058.

4.7 VSS Exchange restore

Here are some general considerations for VSS restores. Unless otherwise specified, the term "VSS restore" refers to all restore types that use VSS (VSS restore, VSS fast restore, VSS Instant Restore):

- The Recovery Storage Group is ignored when a VSS restore is initiated and the data is placed directly into the production database. This is a Microsoft restriction.
- VSS backups to be restored must be from the same snapshot (that it, it must contain the same time stamp). VSS backups that contain different time stamps must be restored one at a time and cannot be restored together in a single operation.
- A VSS Instant Restore overwrites the entire contents of the source volumes. If you do not want this, you can select to disable VSS Instant Restore; in this case the restore will be done at a file level, and other data on the source volumes will not be overwritten.
- When performing a VSS Instant Restore, you should not attempt to perform a "partial" restore. That is, if a Storage Group contains more than one database, your Instant Restore must select *all* the Storage Groups. If you only select a subset of the Storage Groups for an Instant Restore of a VSS LOCAL backup, Data Protection for Exchange will allow you to attempt this, but it will likely fail or have undesirable side effects.

  If you need to restore just one database from a VSS LOCAL backup, make sure to check the **Disable VSS Instant Restore** box in the GUI, or use the CLI option /INSTANTRestore=NO.

  If you need to have VSS Instant Restore capability for single databases, you will need to place them into their own storage group.
- Unlike legacy restores (which only dismount the database being restored), VSS restores dismount *all* databases in the storage group that is being restored. This is a Microsoft requirement.

If a hardware provider is used, the disks that contain Exchange data must be configured as basic.

Be aware that when a VSS restore from local shadow volumes is performed, the bytes transferred will display "0". That is because no data ("0") is restored from the Tivoli Storage Manager server.

Restore options summary

There are three ways to perform a VSS-based restore:

VSS restore This is a file-based restore from a VSS backup in Tivoli Storage Manager storage. This process is essentially the same as a legacy restore.

VSS fast restore This is a file-based restore from a VSS persistent snapshot. Because the snapshot is available locally, there is no network overhead to transfer the restore data from the Tivoli Storage Manager storage pools, so this may be faster than VSS restore.

VSS Instant Restore This is a hardware-assisted snapshot restore from a shadow copy. This is currently available only on the SAN Volume Controller. Because the restore uses the disk system's copy services, rather than restoring files individually, it is the fastest type of restore.

In the following sections, we explain these restore options in more detail.

4.7.1 VSS restore

Figure 4-34 shows an Exchange server Storage Group. In this scenario, we will restore the Storage Group SG1.

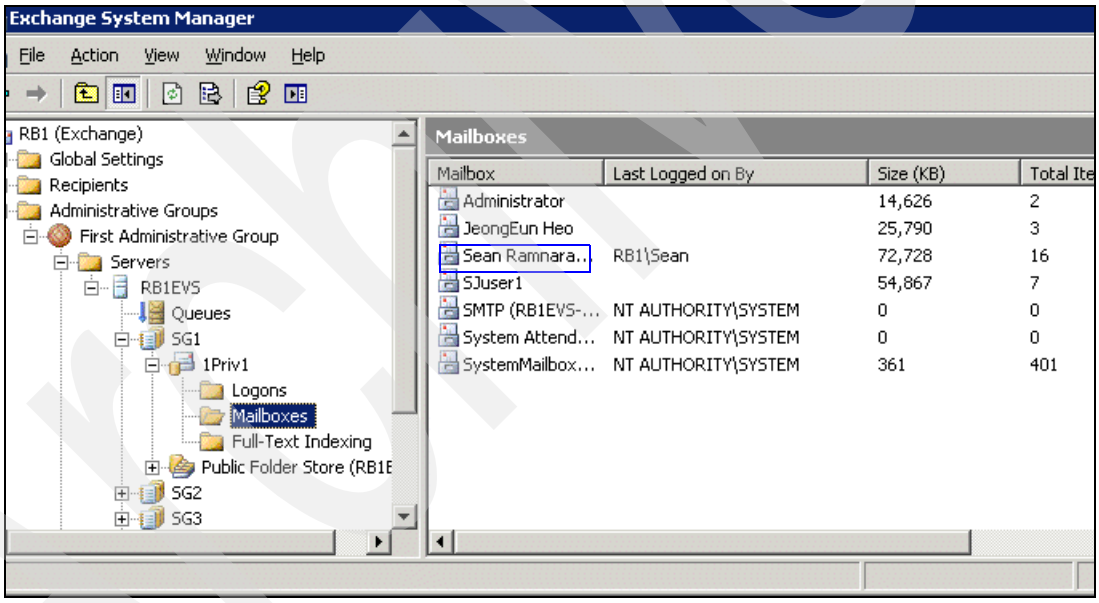


Figure 4-34 Current configuration of an Exchange Storage Group

To simulate a real restore requirement, we deleted a mail box from Storage Group SG1, as shown in Figure 4-35 on page 136. We right-clicked the mailbox and selected **Exchange tasks**.

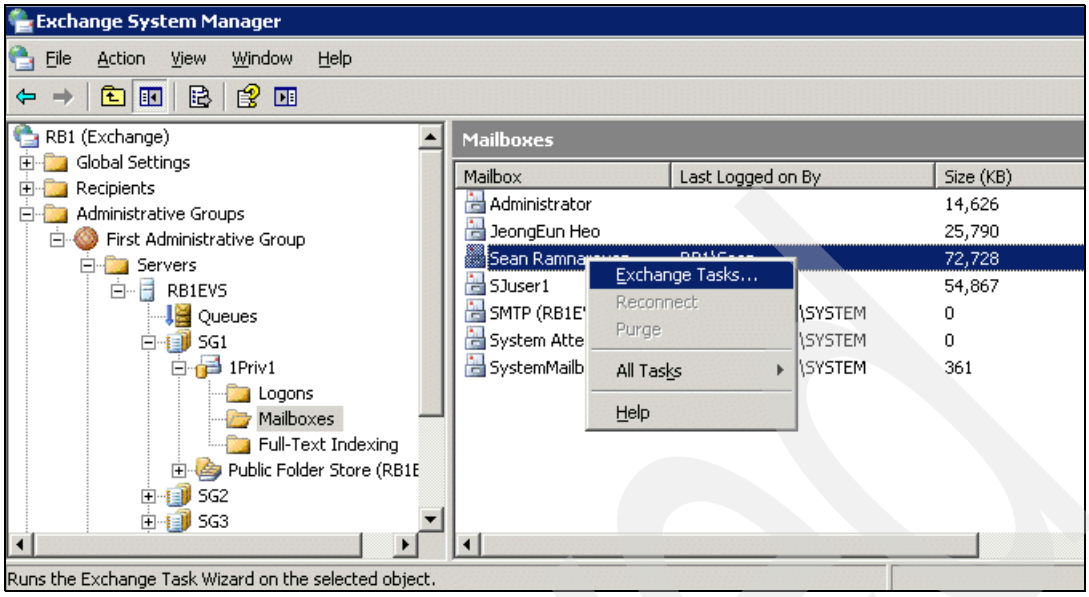


Figure 4-35 Select Mailbox to delete

In Figure 4-36, we selected Delete Mailbox.

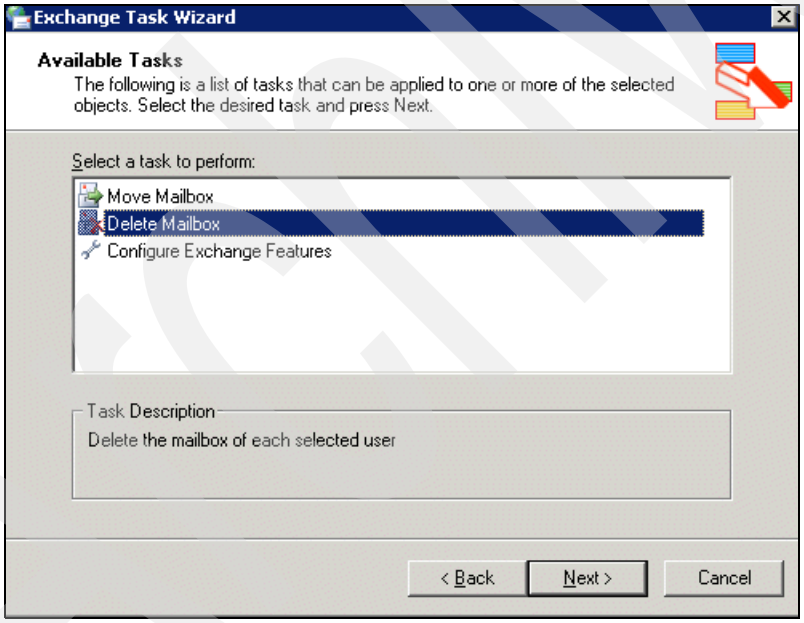


Figure 4-36 Delete a Mailbox

You can see the warning that was shown in Figure 4-37 on page 137.

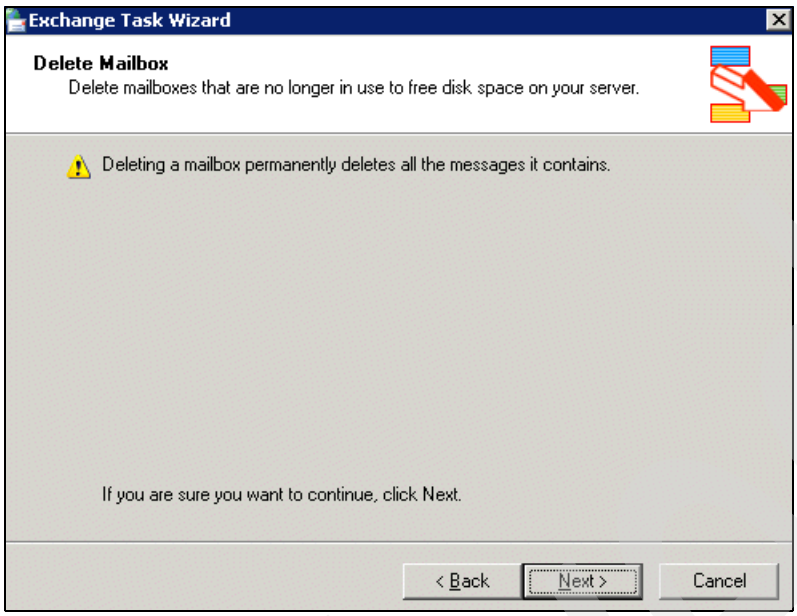


Figure 4-37 Mailbox Process Delete

Figure 4-38 shows that the Mailbox has been deleted.

Figure 4-38 User Mailbox has been deleted

Now, in the Exchange Manager display, note the red X next to `Sean's Mailbox`; this indicates it has been deleted, as shown in Figure 4-39 on page 138.

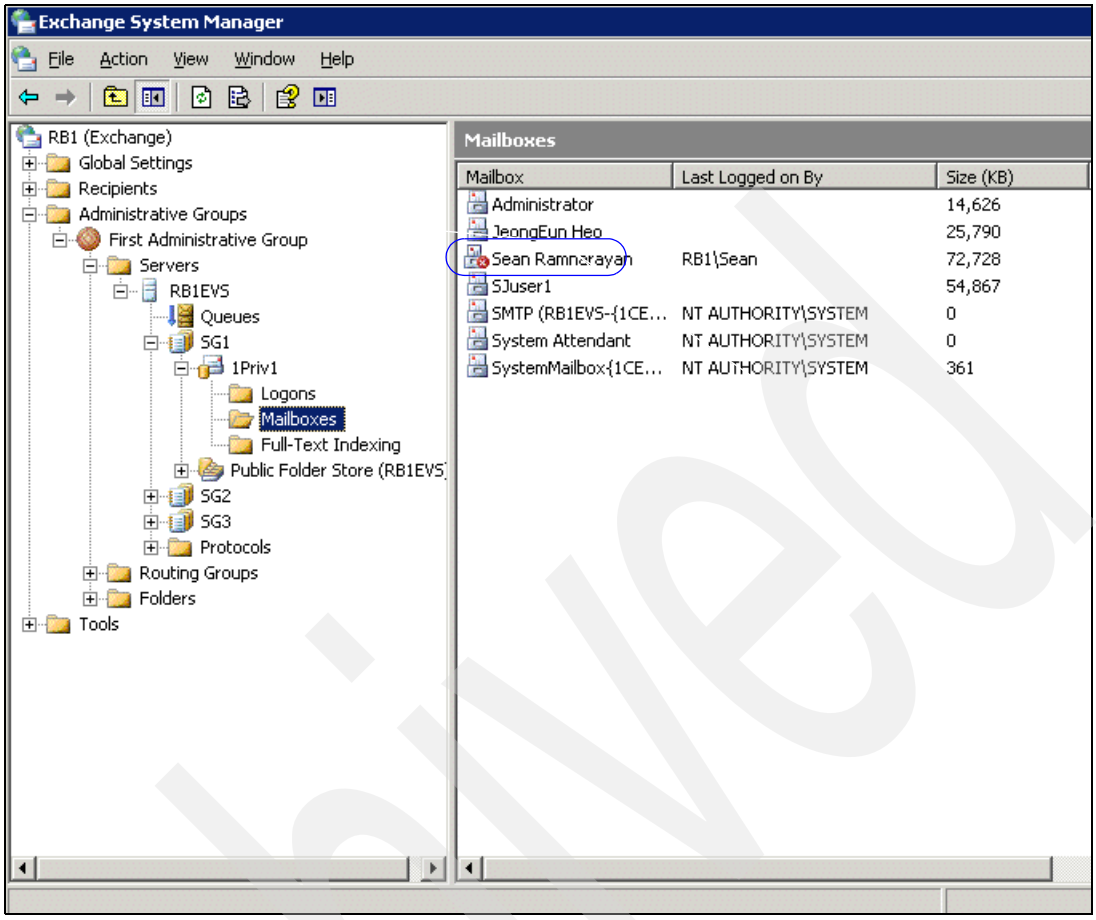


Figure 4-39 Highlighted deleted mailbox

After a refresh, Figure 4-40 on page 139 shows that the user's mailbox has been purged from the Exchange server.

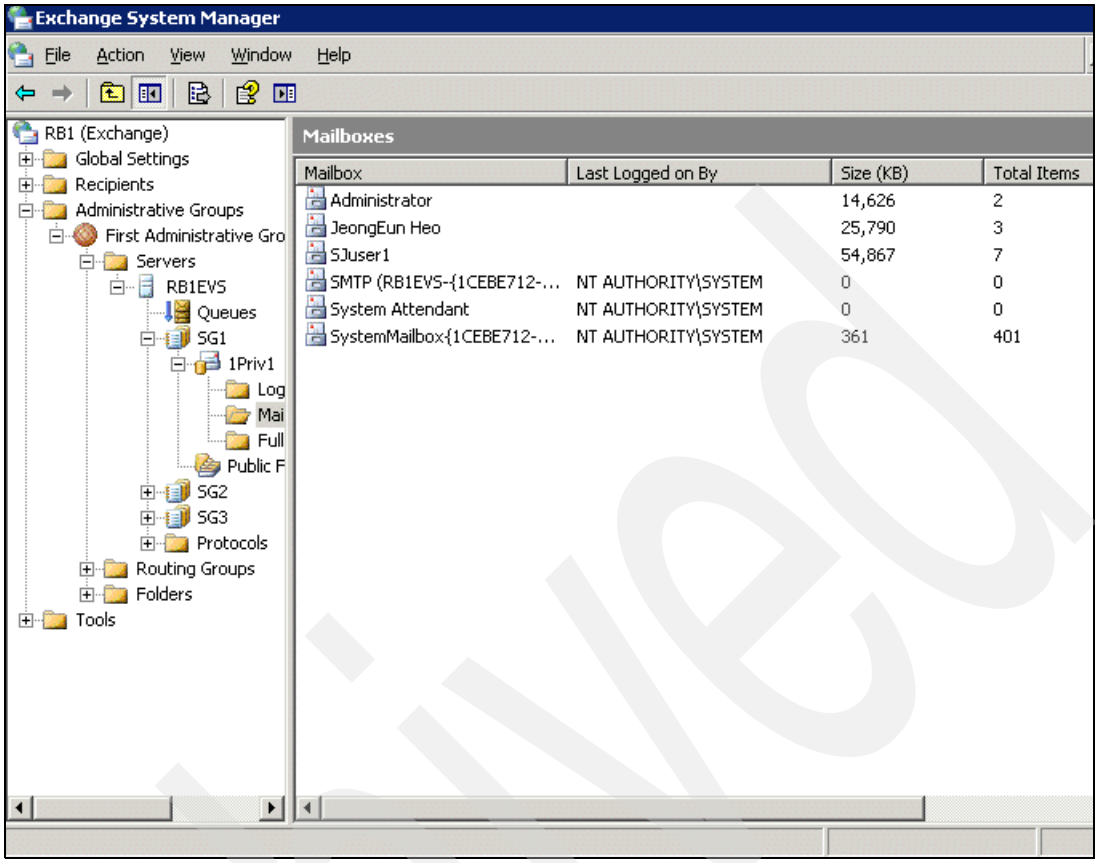


Figure 4-40 Purge of user mailbox

At this point we started restoring, as shown in Figure 4-41 on page 140. Because a VSS restore is at the Storage Group level, we needed to restore all of SG1, which we had selected.

We choose to restore from the VSS backup on the Tivoli Storage Manager server; it was the only one currently available. Microsoft does not provide a VSS individual mailbox restore function. We had disabled VSS Instant Restore, although in this case, this option had no effect due to the following reasons:

- The storage system was a DS8000, which did not support Instant Restore at the time of writing.
- The backup was on the Tivoli Storage Manager server, and Instant Restore can only be done from a VSS snapshot backup.

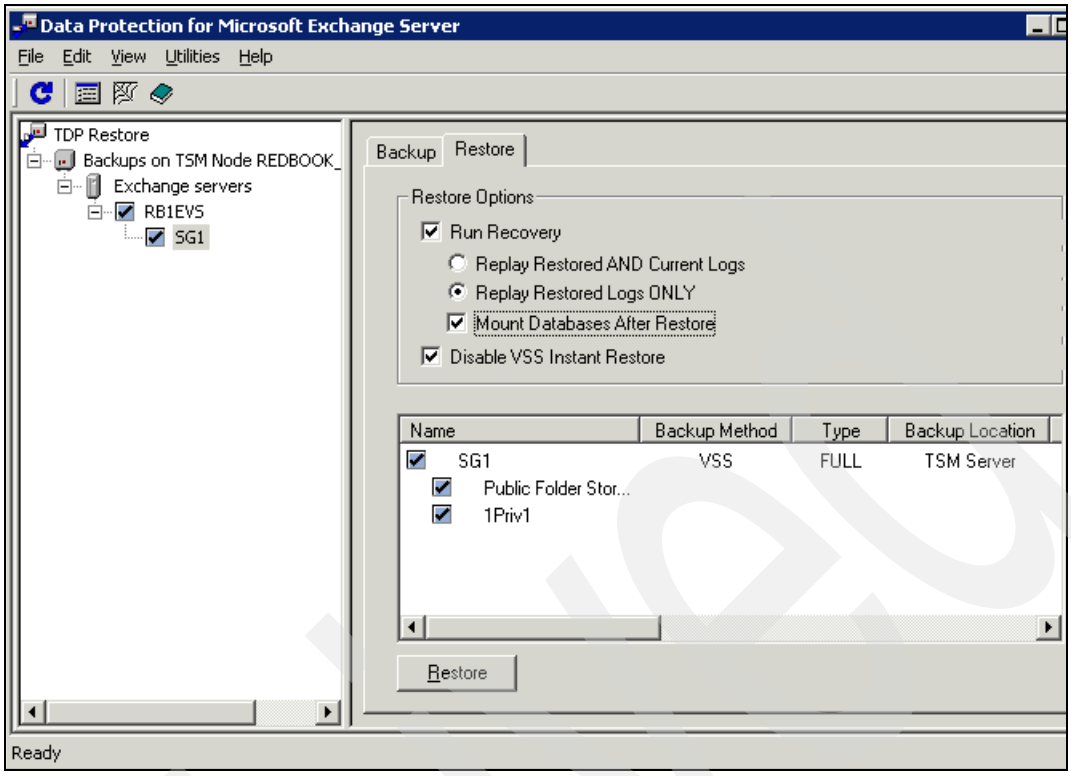


Figure 4-41 Restore Option

Figure 4-42 shows the warning screen displayed when a VSS restore is started; it describes what will happen on the restore. If you are unsure about whether you should perform the restore at this time, click **No**. Otherwise, click **Yes** to start the restore.

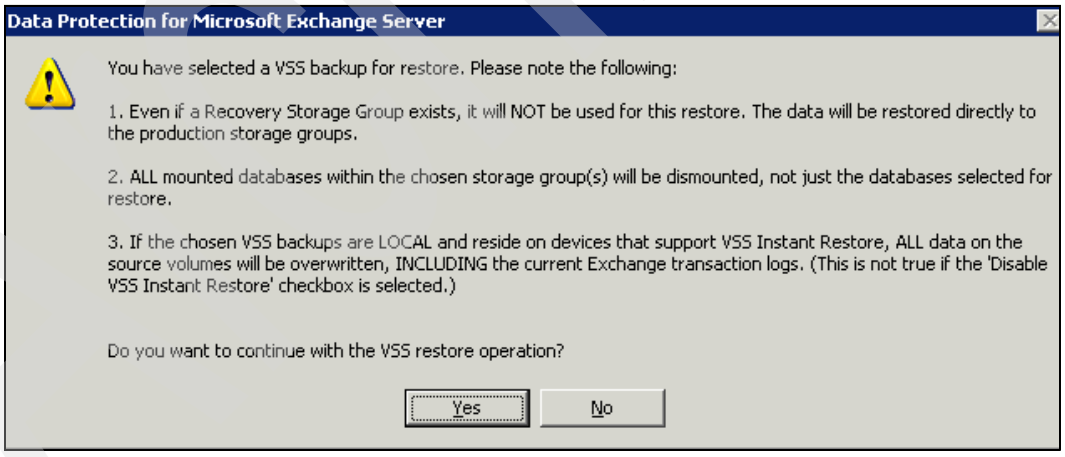


Figure 4-42 Restore process

Figure 4-43 on page 141 shows the restore process of the SG1 Storage Group.

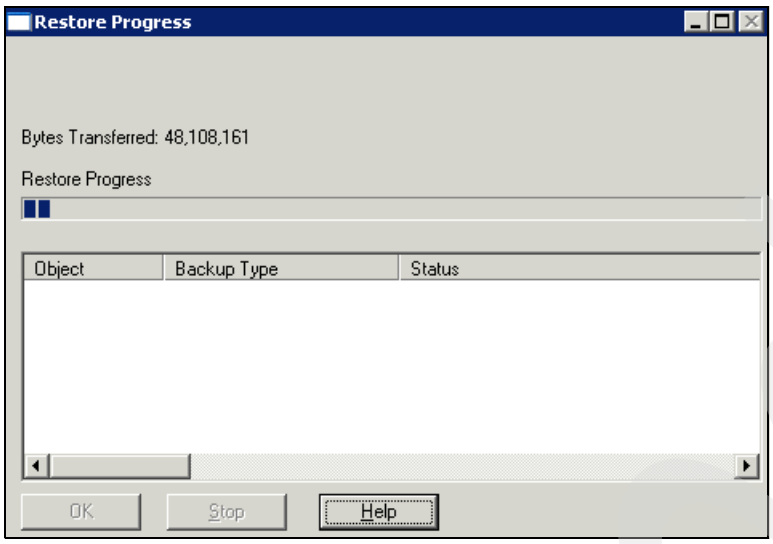


Figure 4-43 Restore Progress

Figure 4-44 shows the Storage Group was successfully restored.

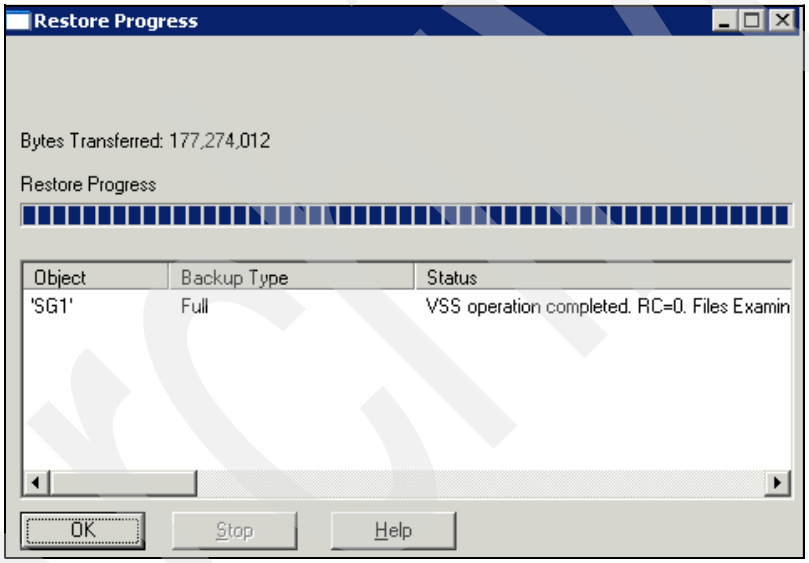


Figure 4-44 Successful Restore Process

As you can see in Figure 4-45 on page 142 for the Exchange Manager, Sean's mailbox was now back in the SG1 Storage Group.

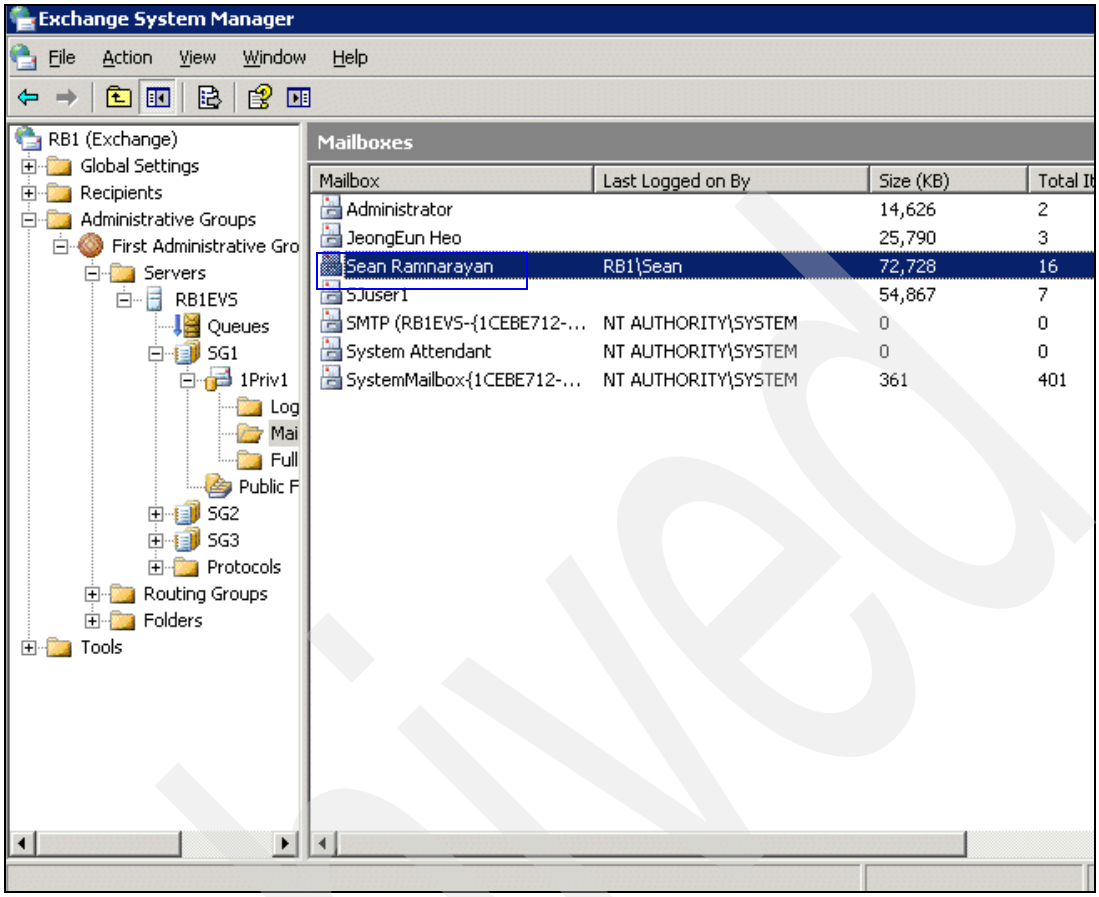


Figure 4-45 Exchange Storage Group after restore

4.7.2 VSS fast restore

In this restore, we copy the files from a VSS snapshot, using the VSS fast restore method. First we deleted a mailbox, to simulate the need for a restore, using the same procedure as in Figure 4-35 on page 136 and following. To initiate the restore, we selected the **Restore** tab. We selected to restore the backup stored on local, which is a VSS snapshot backup.

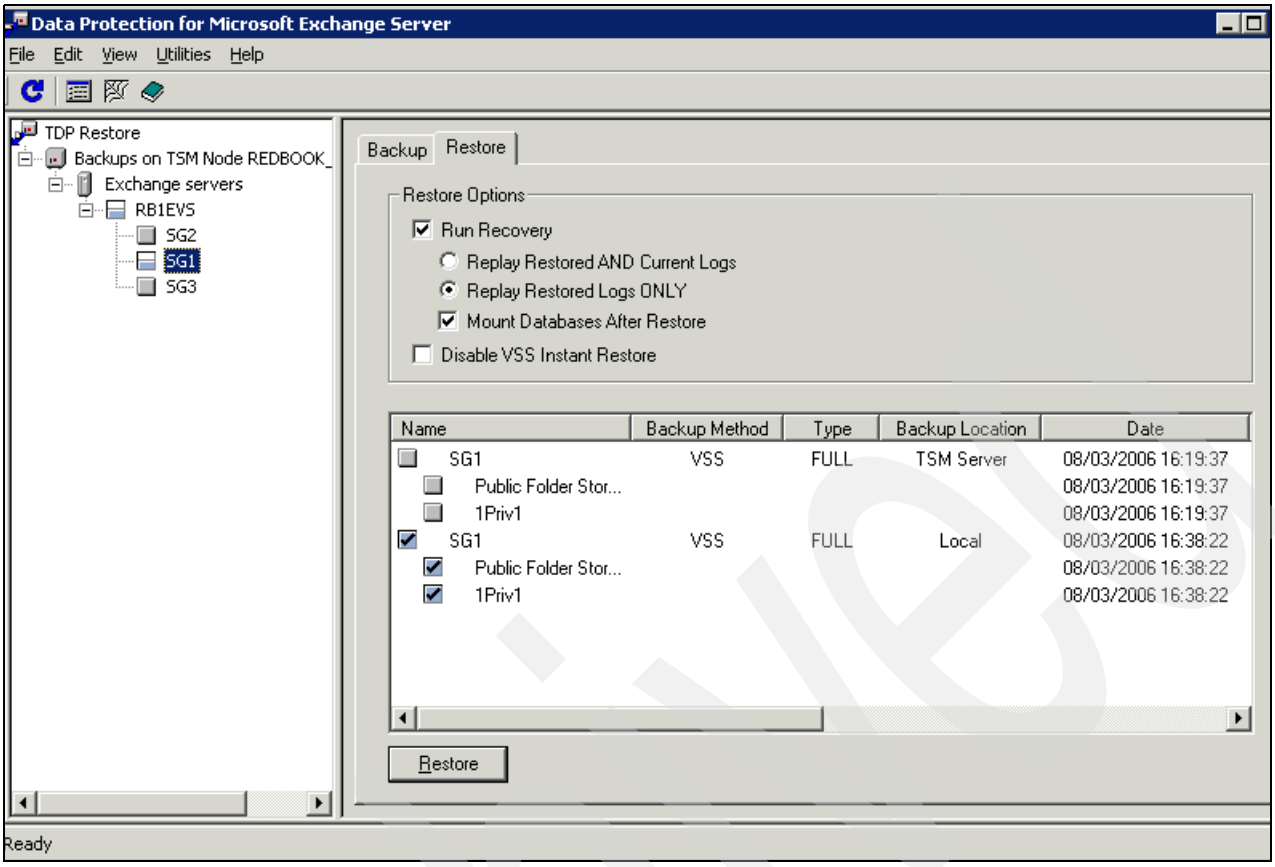


Figure 4-46 Fast restore selection

Figure 4-47 shows the familiar warning message about the implications of the VSS restore. We clicked **Yes** to start the restore.

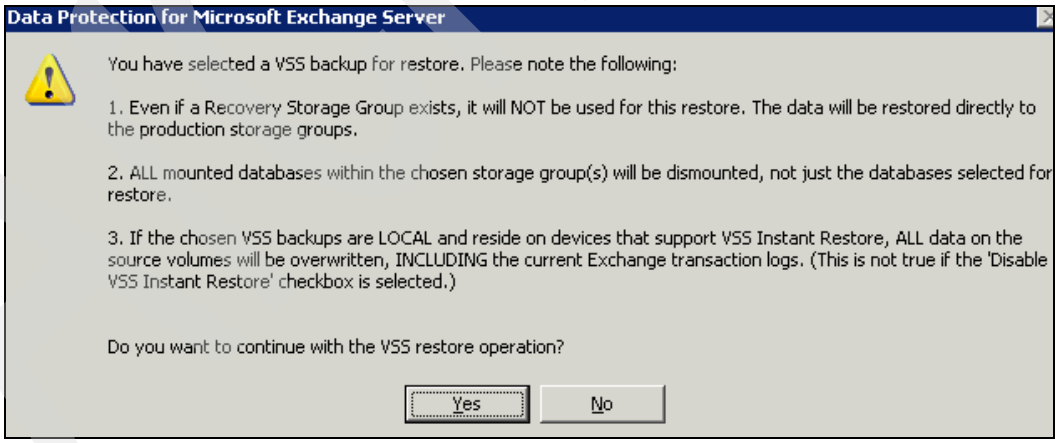


Figure 4-47 VSS fast restore warning message

Figure 4-48 on page 144 shows the completion of a VSS fast restore.

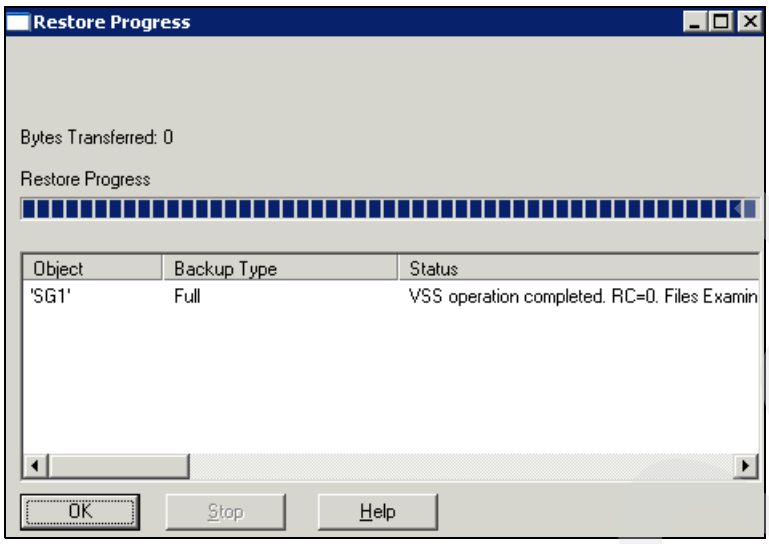


Figure 4-48 VSS fast restore complete

Figure 4-49 shows that the user's mailbox is available to the SG1 Storage Group after the VSS fast restore.

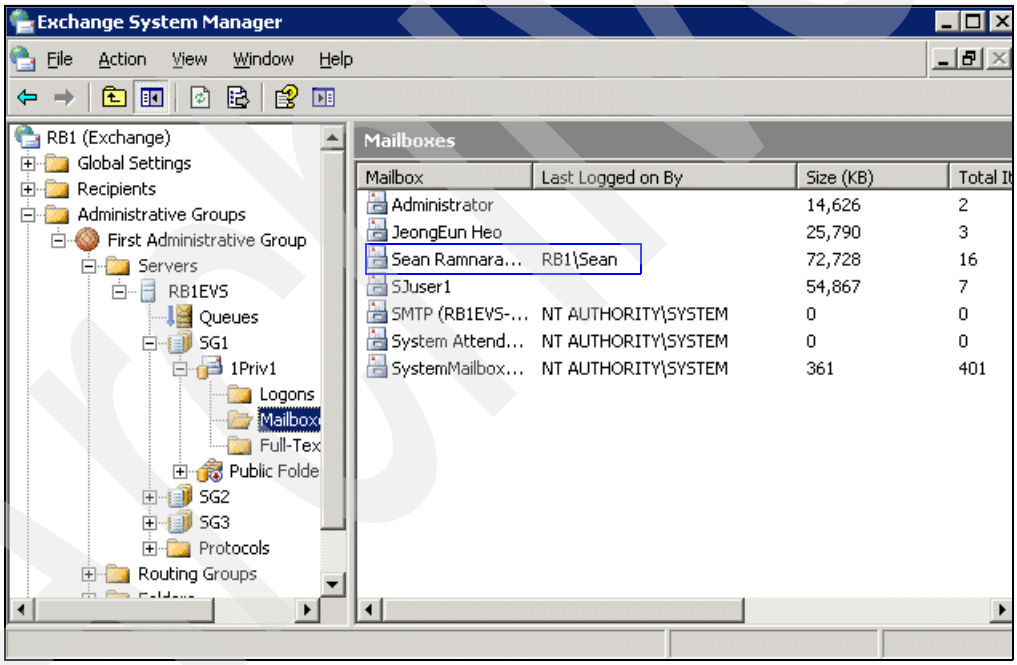


Figure 4-49 Exchange Storage Group after a VSS fast restore

4.7.3 VSS Instant Restore

At the time of writing, VSS Instant Restore is only available when your Exchange Server databases are on SVC LUNs. This scenario uses another Exchange configuration with different Storage Groups, stored on a SAN Volume Controller. Figure 4-50 shows the Exchange configuration for the server ONYX. We will restore Storage Group STG3 as our test example.

Important: When you perform an Instant Restore, all the data on the source LUNs will be overwritten. Therefore, in laying out your Exchange database file for the Storage Groups, make sure that you follow the recommendations given in 2.1.3, “Storage layout considerations for Microsoft Exchange” on page 23. Each Exchange Storage Group should be on its own dedicated LUN, and the associated Logs for the Storage Group on another dedicated LUN. When you perform an Instant Restore of a Storage Group, both the database and log LUNs will be overwritten. Therefore, if you had files or logs from another Storage Group, that would also be overwritten.

Also, because of the way that the SVC uses Consistency Groups for snapshots, a VSS Instant Restore must be performed on the same objects which were backed up. That is, if you made a LOCAL backup of more than one Storage Group, then the Instant Restore must be performed on the same storage groups. Therefore we recommend that if you are using Instant Restore, back up each Storage Group individually.

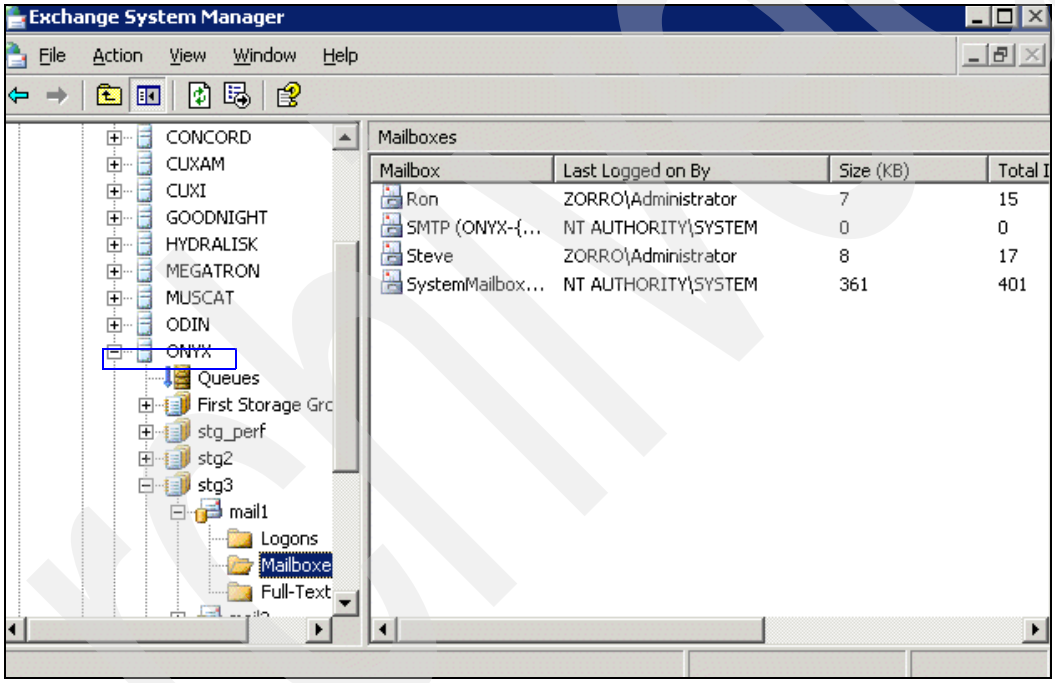


Figure 4-50 Exchange server Storage Groups

Figure 4-51 on page 146 shows that the mailbox for `Steve` has been deleted and purged from the Exchange server.

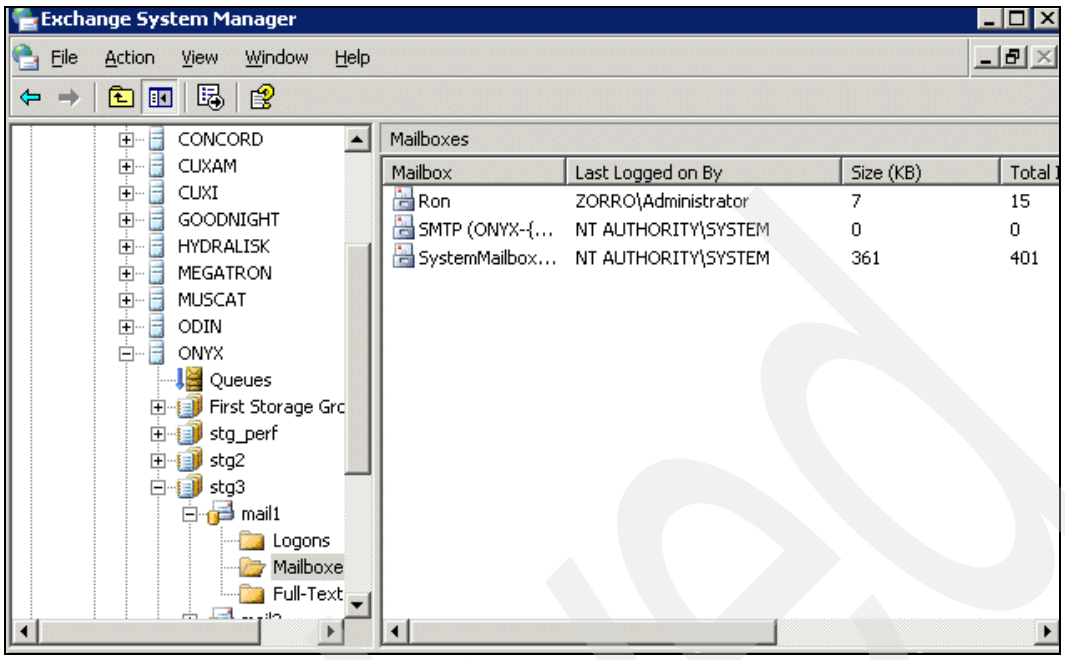


Figure 4-51 Exchange Server mailbox deletion and purge

Now we initiated the VSS Instant Restore, as shown in Figure 4-52. We choose to restore the STG3 Storage Group from a full Local backup. The **Disable VSS Instant Restore** was unchecked here, to ensure that Instant Restore will be performed.

Important: You can only perform an Instant Restore on an entire Storage Group, so if the Storage Group contains more than one database, do not attempt to select a subset of the databases for restore.

We opted not to mount the Exchange Storage Group automatically after the restore, so that we could confirm that the correct data had been restored before mounting the Storage Group.

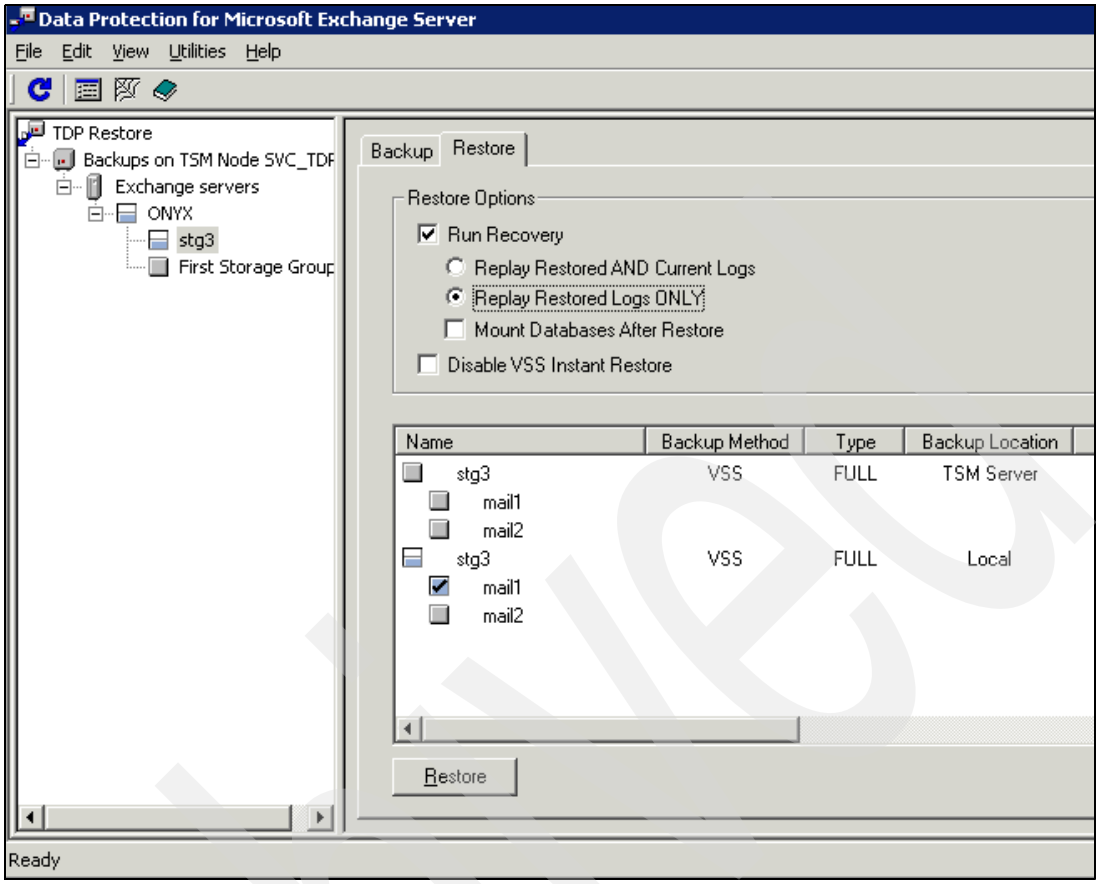


Figure 4-52 VSS Instant Restore

Figure 4-53 shows the warning message. Note that all the source LUNs will be overwritten, since we had specified Instant Restore. We clicked **Yes** to continue.

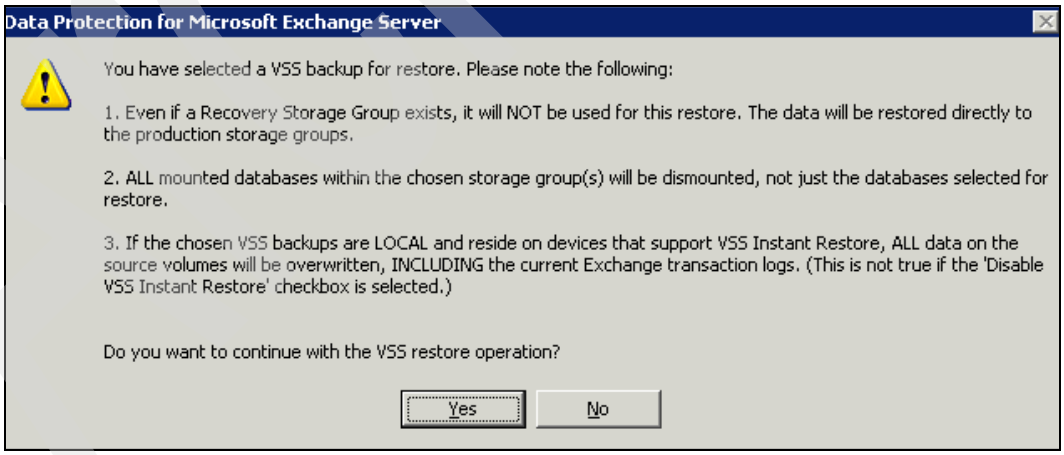


Figure 4-53 VSS Instant Restore confirmation

Figure 4-54 shows the progress of a VSS Instant Restore.

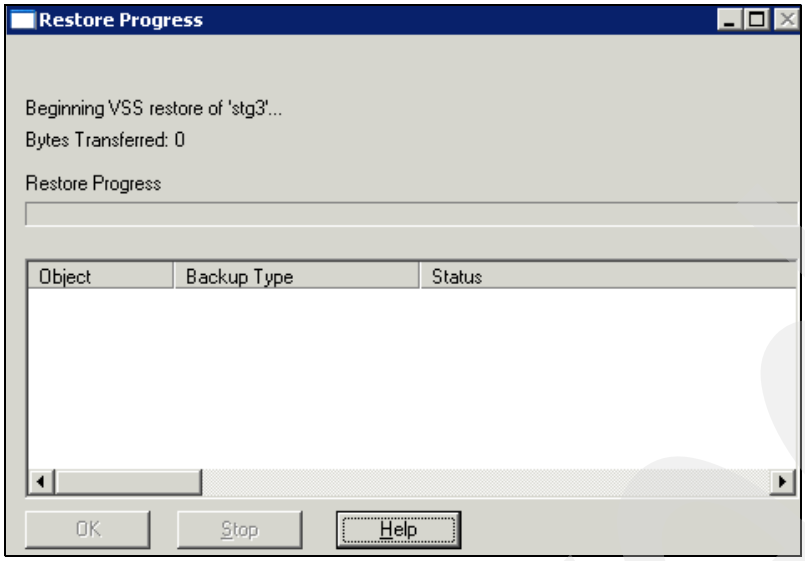


Figure 4-54 VSS Instant Restore progress

Figure 4-55 on page 148 shows the Instant Restore successfully completed. We clicked **OK** to continue.

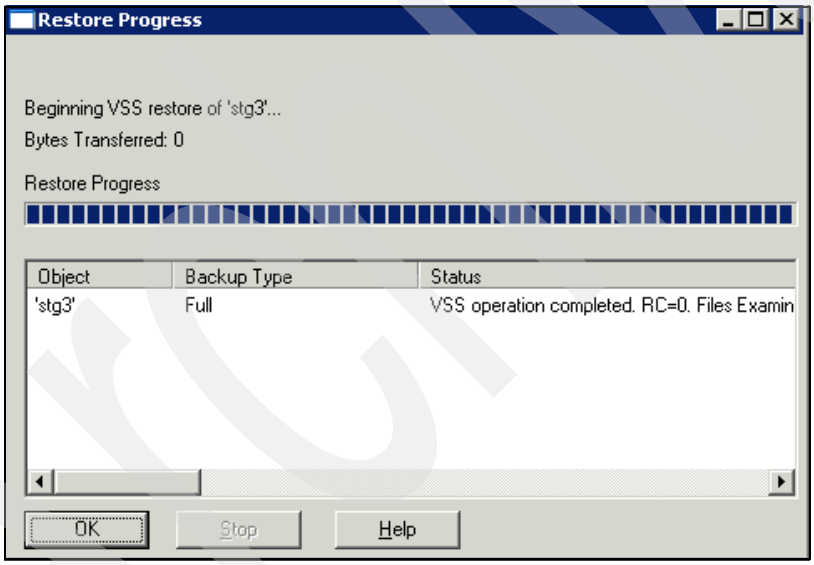


Figure 4-55 VSS successful Instant Restore

Figure 4-56 shows that Steve's mailbox is restored back to the ONYX Storage Group after the successful VSS Instant Restore. To verify that the correct data was restored, we performed the following steps:

1. We checked the space used for the ONYX STG3 Storage Group on the Tivoli Storage Manager server.
2. Before the restore, we recreated Steve's mail box (empty).
3. We restored the ONYX STG3 Storage Group.
4. We confirmed on the drive where the STG3 Storage Group resides that the data size matched the size seen in Tivoli Storage Manager.
5. We mounted the STG3 Storage Group.

6. We refreshed the STG3 Storage group to view ALL mailboxes and confirm that Steve's mailbox was restored.

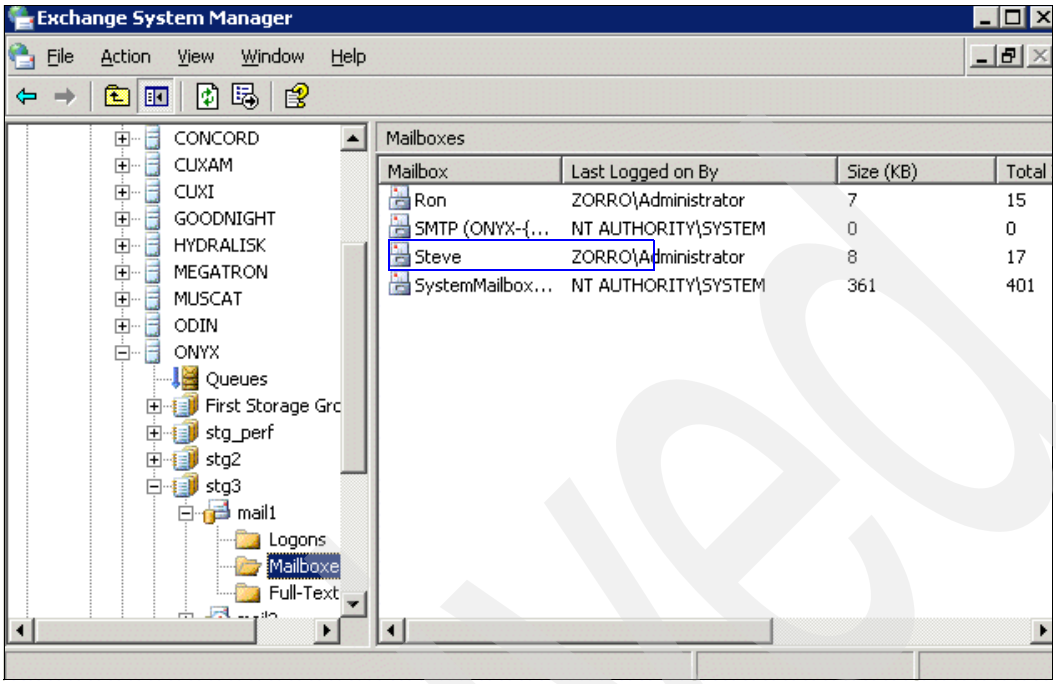


Figure 4-56 Confirmation of VSS Instant Restore

4.7.4 Tivoli Storage Manager server sessions for a VSS restore

Example 4-12 shows the sessions in Tivoli Storage Manager when a VSS restore is initiated. The Data Protection for Exchange nodename initiates the session, but the Local DSMAgent (REDBOOK_VSS_A in this case) actually restores the data to the Exchange server. Restores are never offloaded; instead, they are always performed by the Local DSMAgent.

Example 4-12 Restore Session in the Tivoli Storage Manager server

```
12,743 Tcp/Ip IdleW    5 S    3.2 K     559 Node  TDP MSE- REDBOOK_EXCHANGE
                                                   xchg
12,744 Tcp/Ip IdleW    5 S    9.9 K   1.1 K Node  TDP MSE- REDBOOK_EXCHANGE
                                                   xchg     (REDBOOK_VSS_A)
```

4.8 Using vssadmin and vshadow commands

Chapter 3, "Installation" on page 43 introduced the **vssadmin** and **vshadow** commands. Example 4-13 shows the volumes in our configuration that are eligible to have VSS shadow copies made; we used the **vssadmin list volumes** command. Apart from the C drive, these are all volumes on the DS8000.

Example 4-13 List eligible snapshot volumes

```
C:\Admin-DW\Exchange Utils\Vshadow>vssadmin list volumes
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001 Microsoft Corp.
```

```
Volume path: C:\
    Volume name: \\?\Volume{8345f2cf-07b4-11db-b957-806e6f6e6963}\
Volume path: E:\
    Volume name: \\?\Volume{aadfb120-110e-11db-b453-000d60494c64}\
Volume path: G:\
    Volume name: \\?\Volume{aadfb126-110e-11db-b453-000d60494c64}\
Volume path: I:\
    Volume name: \\?\Volume{aadfb12c-110e-11db-b453-000d60494c64}\
Volume path: F:\
    Volume name: \\?\Volume{aadfb123-110e-11db-b453-000d60494c64}\
Volume path: H:\
    Volume name: \\?\Volume{aadfb129-110e-11db-b453-000d60494c64}\
Volume path: J:\
    Volume name: \\?\Volume{aadfb12f-110e-11db-b453-000d60494c64}\
```

Example 4-14 shows a query of shadow copies, **vshadow -q**. At this stage, there were no shadow copies available.

Example 4-14 List shadow copies - no copies currently

```
C:\Admin-DW\Exchange Utils\Vshadow>vshadow -q

VSHADOW.EXE 2.2 - Volume Shadow Copy sample client
Copyright (C) 2005 Microsoft Corporation. All rights reserved.


(Option: Query all shadow copies)
- Setting the VSS context to: 0xffffffff

Querying all shadow copies in the system ...


There are no shadow copies in the system
```

Example 4-15 on page 150 shows the volumes used after a shadow copy backup is made. In this case, it was a VSS Exchange backup to Local. The output shows the source LUN drive letters and the associated target LUN volume ids; in this case, volumes G and H were shadow copied.

Example 4-15 List shadow copies - one snapshot

```
C:\Admin-DW\Exchange Utils\Vshadow>vshadow -q

VSHADOW.EXE 2.2 - Volume Shadow Copy sample client
Copyright (C) 2005 Microsoft Corporation. All rights reserved.


(Option: Query all shadow copies)
- Setting the VSS context to: 0xffffffff

Querying all shadow copies in the system ...

* SNAPSHOT ID = {412397bd-dd62-4553-bd20-a4bc28348b90} ...
   - Shadow copy Set: {4618368a-91f4-4028-8a58-f137902c5157}
```

```
   - Original count of shadow copies = 2
   - Original Volume name: \\?\Volume{aadfb129-110e-11db-b453-000d60494c64}\ [H:\]
   - Creation Time: 8/7/2006 11:04:50 AM
   - Shadow copy device name: \\?\Volume{89390ee7-24da-11db-bd76-000d6047a347}
   - Originating machine: REDBOOK3.RB1.Local
   - Service machine: REDBOOK3.RB1.Local
   - Not Exposed
   - Provider id: {d90dd826-87cf-42ce-a88d-b32caa82025b}
   - Attributes:  No_Auto_Release Persistent Hardware

* SNAPSHOT ID = {475a5d07-269e-4a07-b146-f64a89ccb6fd} ...
   - Shadow copy Set: {4618368a-91f4-4028-8a58-f137902c5157}
   - Original count of shadow copies = 2
   - Original Volume name: \\?\Volume{aadfb126-110e-11db-b453-000d60494c64}\ [G:\]
   - Creation Time: 8/7/2006 11:04:50 AM
   - Shadow copy device name: \\?\Volume{89390ee8-24da-11db-bd76-000d6047a347}
   - Originating machine: REDBOOK3.RB1.Local
   - Service machine: REDBOOK3.RB1.Local
   - Not Exposed
   - Provider id: {d90dd826-87cf-42ce-a88d-b32caa82025b}
   - Attributes:  No_Auto_Release Persistent Hardware
```

5

Operations

In this chapter we cover the following topics:

- Automating VSS backups
- Considerations for scheduled operations
- Monitoring VSS backups
- Verifying VSS backups
- Some performance considerations
- Managing snapshot-based backups
- Troubleshooting tips

5.1 Automating backups

You can use the Tivoli Storage Manager server scheduler or an alternate scheduling package to automate VSS and legacy Exchange backups. In this chapter we describe using the Tivoli Storage Manager server scheduler for this purpose.

To automate Exchange backups using the scheduler, you need to install the Tivoli Storage Manager scheduler client as a Windows service on your Exchange server. We assume you already have Data Protection for Exchange installed and configured for backups.

Here is a summary of the steps needed to automate your Exchange backups. In the next section, we describe a detailed sample procedure.

1. On the Tivoli storage Manager Server:
   a. Define a schedule to run a Windows command file in the policy domain where the Data Protection for Exchange client node is registered.
   b. Associate the Data Protection for Exchange node to the defined schedule.
2. On the machine where Data Protection for Exchange and Exchange Server is installed:
   a. Install the Tivoli Storage Manager Scheduler client as a Windows service for Data Protection for Exchange. If you already have a scheduler service for your backup-archive client, install another one for Data Protection for Exchange. In a clustered environment, install the Tivoli Storage Manager scheduler as a Windows service on both cluster nodes.
   b. Create a command file containing Data Protection for Exchange commands to perform the desired backup.
   c. In a cluster environment, create a new cluster resource that represents the Tivoli Storage Manager scheduler. Verify that the cluster resource is started.

5.1.1 Sample procedure

This example assumes the following environment:

1. The Data Protection for Exchange nodename is registered to a Tivoli Storage Manager server:
   – The nodename is REDBOOK_EXCHANGE.
   – The password is REDBOOK_EXCHANGE.
   – The policy domain is REDBOOK.
2. The event to be scheduled:
   – A daily full legacy backup of all Storage groups. This is based on a sample script provided with Data Protection for Exchange. We will also show how to modify the script to perform VSS backup operations.
   – The backups begin between 20:00 and 20:15
3. Exchange Server 2003 is installed on a Windows 2003 system

5.1.2 Installing the Tivoli Storage Manager scheduler client on the Exchange server

We assume the following environment is already set up:

- The Tivoli Storage Manager backup-archive client is installed on the Exchange Server in the c:\Program Files\Tivoli\TSM\baclient directory.

- Data Protection for Exchange is installed on the Exchange Server in the c:\Program Files\Tivoli\TSM\TDPExchange directory.
- The communication options in the dsm.opt option files point to the Tivoli Storage Manager server to which the Exchange data is to be backed up. The options file that is defined for Data Protection for Exchange is used by the scheduler when validating the node and password. The options file is also used when contacting the Tivoli Storage Manager server for schedule information.

Perform the following steps on the Exchange server to set up the Tivoli Storage Manager scheduler client:

1. Login using a Windows account with administrative privileges.
2. In a command prompt window, issue the following command:

   ```
   cd c:\"program files"\Tivoli\TSM baclient
   ```

   Tip: If a Tivoli Storage Manager scheduler is already installed on the Exchange server (for regular backups of the Windows operating system), you need to install another scheduler service (with a unique name) to run the schedules defined for Data Protection for Exchange.

3. Issue the following command:

   ```
   dsmcutil inst /name:"TSM Exchange Scheduler Service" /node:REDBOOK_EXCHANGE
   /password:REDBOOK /autostart:yes /clientdir:"c:\program
   files\tivoli\tsm\baclient" /optfile="c:\program
   files\tivoli\tsm\tdpexchange\dsm.opt" /startnow:no
   ```

   The /node parameter points to the Data Protection for Exchange nodename, /clientdir is the directory where the backup-archive client is installed, and /optfile points to the TData Protection for Exchange options file.

   After the **dsmcutil** command completes, you will be able to see the new scheduler installed in the services applet, as shown in Figure 5-1. You can now proceed to 5.1.3, “Automating the backup schedule”.

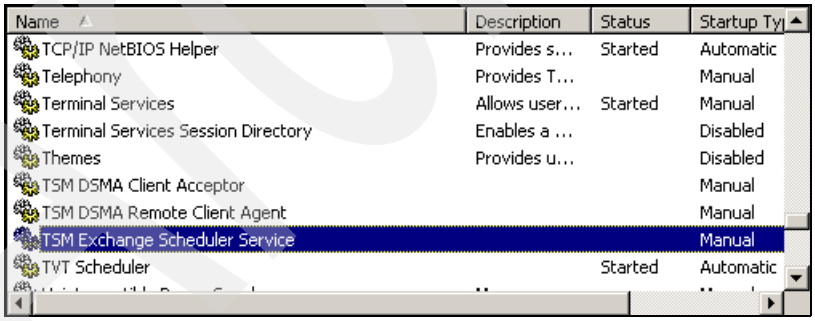


Figure 5-1 Data Protection for Exchange scheduler service

Cluster considerations

To set up the scheduler for a clustered Exchange Server environment, there are a few differences.

1. If you have not already done so, copy the Data Protection for Exchange options file (dsm.opt) to a shared drive associated with the virtual server.

2. In the **dsmcutil** command (step 3 in 5.1.2, “Installing the Tivoli Storage Manager scheduler client on the Exchange server” on page 154), specify the /autostart option to: no and add the /clusternode and /clustername options to indicate your cluster virtual address. Also, make sure the /optfile parameter points to the correct location of the options file; for example:

   ```
   /autostart:no /clusternode:yes /clustername:RB1EVS /optfile:x:\tsmdata\dsm.opt
   ```

3. Move the Exchange virtual server to the other node, then rerun the **dsmcutil** command on that node to create the scheduler service on the other node. Make sure the schedule service name is the same on both nodes, and has the same logon authority.

   Example 5-1 shows the output of the **dsmcutil** command in one node in a cluster environment.

Example 5-1 Install scheduler service in cluster environment

```
C:\PROGRA~1\Tivoli\TSM\baclient>dsmcutil inst /name:"TSM Exchange Scheduler
Service" /node:REDBOOK_EXCHANGE /password:REDBOOK_EXCHANGE /autostart:no
/clientdir:"C:\program files\tivoli\tsm\baclient" /optfile:x:\tsmdata\dsm.opt
/clusternode:yes /clustername:RB1EVS /startnow:no

TSM Windows NT Client Service Configuration Utility
Command Line Interface - Version 5, Release 3, Level 4.3
(C) Copyright IBM Corporation, 1990, 2006, All Rights Reserved.
Last Updated Jun 20 2006
TSM Api Verison 5.3.4

Command: Install TSM Client Service
Machine: REDBOOK3(Local Machine)

Locating the Cluster Services ...
clussvc is installed and running

Installing TSM Client Service:

      Machine          : REDBOOK3
      Service Name     : TSM Exchange 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 Exchange Scheduler Service' .
Updated registry value 'ADSMClientKey' .
Updated registry value 'OptionsFile' .
Updated registry value 'EventLogging' .
Updated registry value 'ClientNodeName' .
Updated registry value 'ClusterNode' .
Updated registry value 'ClusterGroupName' .

Generating registry password ...
```

```
Authenticating TSM password for node REDBOOK_EXCHANGE ...

Connecting to TSM Server via client options file 'x:\tsmdata\dsm.opt' ...

Password authentication successful.

The registry password for TSM node REDBOOK_EXCHANGE has been updated.
```

---

4. Start the Cluster Administrator. Select the Exchange Server Cluster Group and create a new Resource to represent the Data Protection for Exchange scheduler (**File** → **New** → **Resource**).

   Specify the following parameters:

   Resource Type: Generic Service as seen in Figure 5-2.

   Group: The Exchange Virtual Server as seen in Figure 5-2.

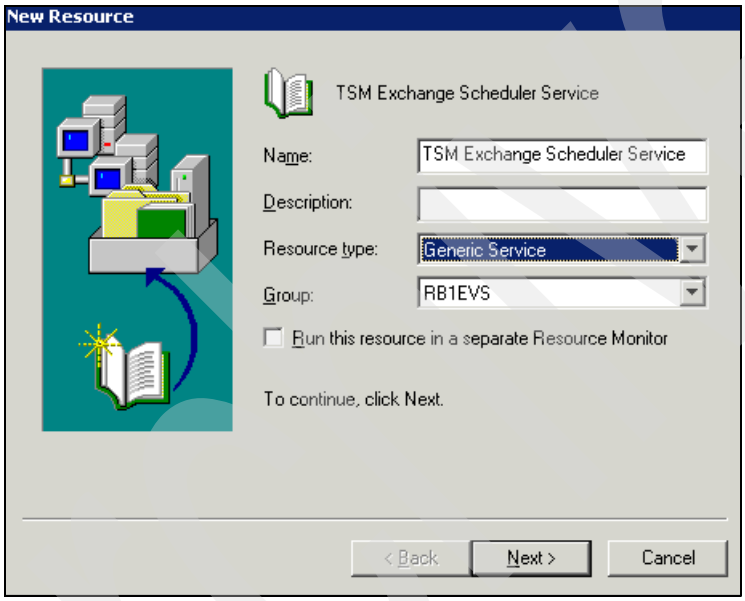


Figure 5-2 Generic Service

Possible Owners: Ensure that both node machines are listed. If they are not listed, add them, as seen in Figure 5-3 on page 158.

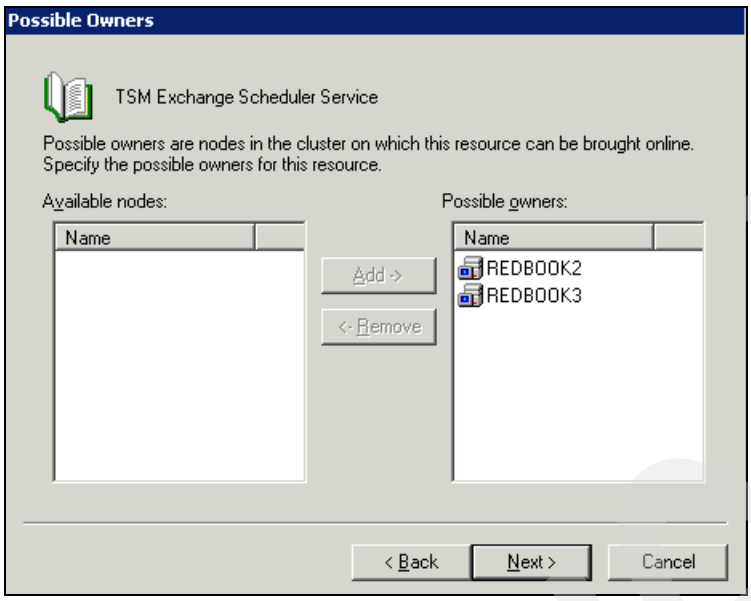


Figure 5-3 Possible Owners

Resource Dependencies: Ensure that the Exchange Virtual Server and the shared drives where the options file is located are listed. We opted to use the Local DSMAgent Resource, as seen in Figure 5-4.

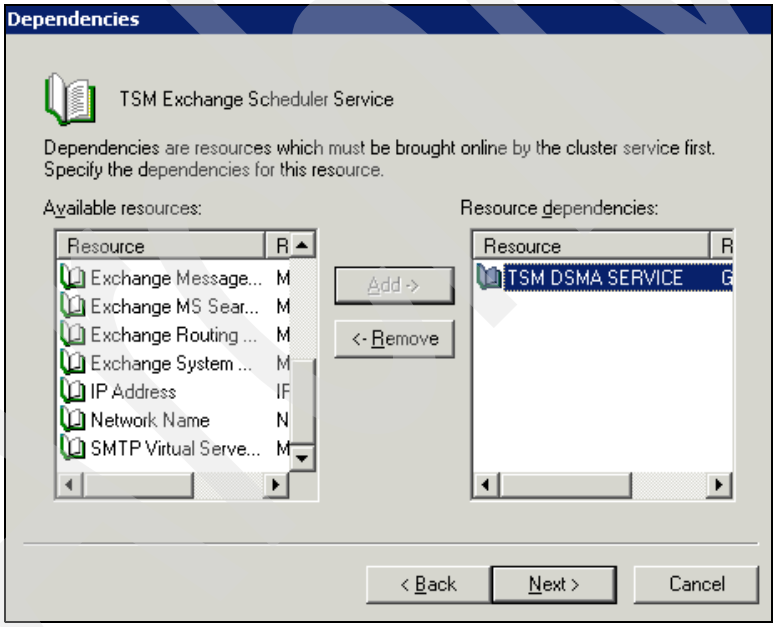


Figure 5-4 Resource Dependencies

Generic Service → Service Name: Specify the exact name of the scheduler service which you just created, and also the start parameters as shown in Figure 5-5 on page 159.

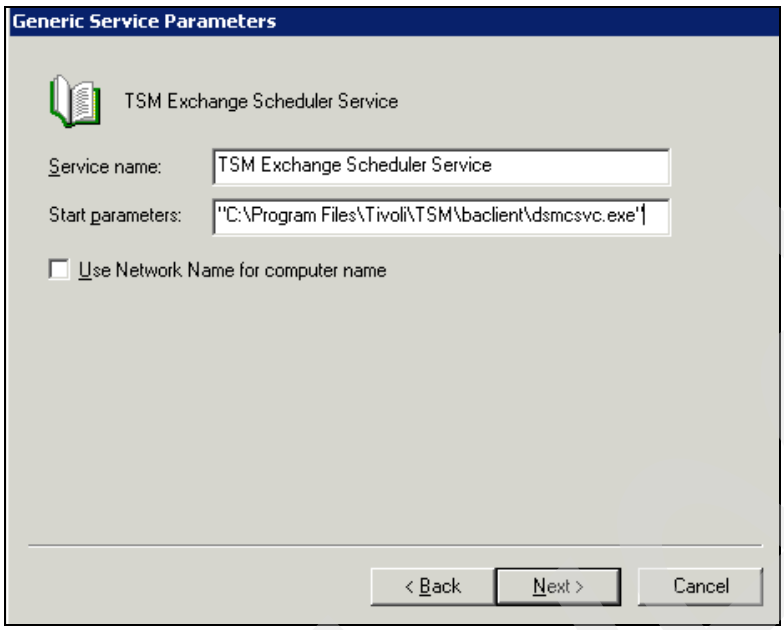


Figure 5-5 Generic Service Parameters

5. Select the new resource and modify its properties. Under the **Registry Replication** → **Root Registry Key** parameter, add the exact key where the Data Protection for Exchange node name is listed; for example:

   HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ADSM\CurrentVersion\BackupClient\NODES\<nodename>\<TSMServerName>

   Replace the <nodename> with your Data Protection for Exchange node name, and <TSMServerName> with your Tivoli Storage Manager server name; for example:

   HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ADSM\CurrentVersion\BackupClient\NODES\REDBOOK_EXCHANGE\ZEALOT

   As seen in Figure 5-6 on page 160, you do not have to start with the HKEY_LOCAL_MACHINE, but from SOFTWARE.

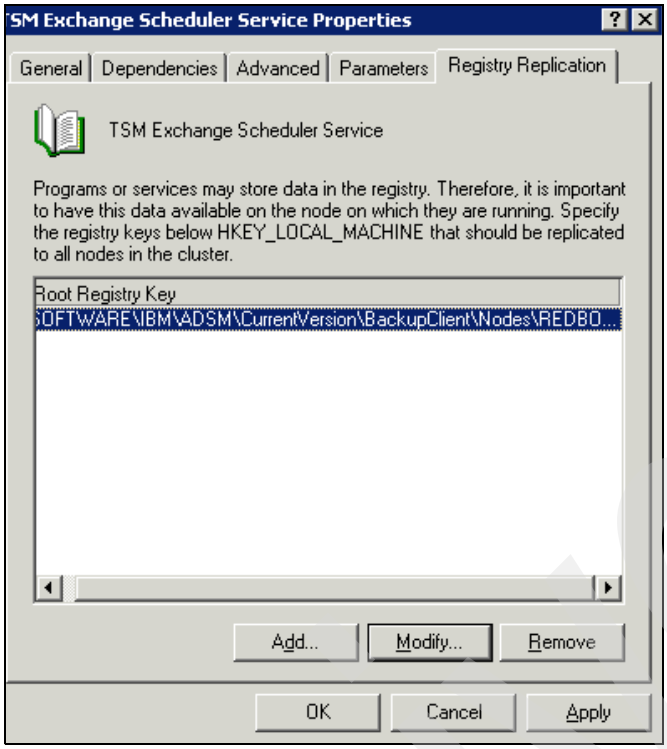


Figure 5-6 Registry Replication

5.1.3 Automating the backup schedule

We assume you have created the scheduler service for the Exchange backups, as described in 5.1.2, “Installing the Tivoli Storage Manager scheduler client on the Exchange server” on page 154.

1. Create a command file (for example, c:\excfull.bat). A sample command file (excfull.smp) is provided in the directory where Data Protection for Exchange is installed. This sample file contains the command **tdpexcc** and other commands necessary to perform a scheduled full legacy backup of all Exchange Server storage groups to the Tivoli Storage Manager server. You simply have to customize it with appropriate value for your environment.

Clustered environment considerations:

If you are in a clustered environment, note the following considerations for creating a command file:

- Your command file can reside on the local C drive. However, if you do this, you have to manually make sure it is kept consistent on all cluster nodes.

  Alternatively, you can create the command file on a shared drive. The schedule you define on the Tivoli Storage Manager server needs to point to this command file, in the objects parameter of the **define schedule** command.
- The /tsmoptfile and /logfile options specified in the **tdpexcc** command must reflect the location of the options and log file on the Exchange File Share.
- The Exchange virtual server must be specified in the **tdpexcc** command, using the /excserver option.

Example 5-2 displays the contents of the file excfull.smp. Another sample script, excincr.smp does an incremental legacy backup.

Example 5-2 Sample legacy full backup script excfull.smp

```
@ECHO OFF
rem  ================================================================
rem   Sample Command File - excfull.smp
rem
rem   Sample command file containing commands to do a scheduled
rem   full backup of the Microsoft Exchange Server databases to
rem   TSM storage.
rem
rem   This file is meant to be executed by the TSM central scheduler
rem   in response to a defined schedule on the TSM server.
rem
rem   Complete paths must be given for all file names and non-system
rem   commands.
rem
rem   Copy this file to excfull.cmd and edit it to match your
rem   local environment.
rem
rem  ================================================================

rem  ================================================================
rem   Replace "X:" with the drive where Data Protection for Exchange
rem   is installed.
rem  ================================================================

set exc_dir="X:\Program Files\Tivoli\TSM\TDPExchange"

cd /d %exc_dir%

rem  ================================================================
rem   The 2 lines below put a date and time stamp in a log file for
rem   you.
rem
rem   Note: You can change "excfull.log" to whatever you prefer.
rem  ================================================================
echo Current date is: >> excfull.log
date /t < NUL >> excfull.log
echo Current time is: >> excfull.log
time /t < NUL >> excfull.log

rem  ================================================================
rem   Now call the command line to do the full backup:
rem
rem   Note: You can change "excsch.log" to whatever you prefer.
rem  ================================================================
tdpexcc backup * full /tsmoptfile=dsm.opt /logfile=excsch.log >> excfull.log
```

2. Example 5-3 shows a modified excfull.bat command file used for a full legacy backup, using the extra parameters for a cluster environment (/excserver and so on).

Example 5-3 Contents of excful.bat customized for a cluster environment

```
@ECHO OFF

set exc_dir="C:\Program Files\Tivoli\TSM\TDPExchange"

cd /d %exc_dir%


echo Current date is: >> excfull.log
date /t < NUL >> excfull.log
echo Current time is: >> excfull.log
time /t < NUL >> excfull.log

tdpexcc backup * copy /backupdestination=TSM /backupmethod=LEGACY
/EXCSERVER=RB1EVS /configfile=x:/tsmdata/tdpexc.cfg /tsmoptfile=x:/tsmdata/dsm.opt
>> excfull.log
```

3. Define the schedule on the Tivoli Storage Manager server. Here is a sample administrative command.

   ```
   def sched redbook exchange_legacy_full action=command objects=c:\excfull.bat
   priority=2 starttime=20:00 duration=15 duru=minutes period=1 perunit=day
   dayofweek=any
   ```

4. Associate the Data Protection for Exchange nodename with this schedule:

   ```
   def association redbook_do exchange_legacy_full redbook_exchange
   ```

5. A schedule is now defined in the Tivoli Storage Manager server, and this schedule will run daily at 20:00.

5.1.4 Scheduling a VSS Exchange backup

To create a VSS Exchange backup schedule, perform the following steps:

1. Copy the excfull.bat file to another name, for example excvss.bat. Modify the **tdpexcc** command for a VSS backup (specify at least BACKUPMethod=VSS). In a clustered environment, note the same considerations listed in the shaded box on page 160.
2. Define another schedule for another start-time in the Tivoli Storage Manager server.

   Note: Remember that you cannot run legacy and VSS backups at the same time.

3. Define the association to the VSS backup schedule for the Exchange backup nodename.
4. A schedule is now defined in the Tivoli Storage Manager server for your VSS Exchange backups.

Example 5-4 shows the excvss.bat command file used for a VSS Exchange backup.

Example 5-4 Contents of excvss.bat

```
@ECHO OFF

set exc_dir="C:\Program Files\Tivoli\TSM\TDPExchange"

cd /d %exc_dir%
```

```
echo Current date is: >> excvss.log
date /t < NUL >> excvss.log
echo Current time is: >> excvss.log
time /t < NUL >> excvss.log

tdpexcc backup * copy /backupdestination=TSM /backupmethod=VSS /EXCSERVER=RB1EVS
/configfile=x:/tsmdata/tdpexc.cfg /tsmoptfile=x:/tsmdata/dsm.opt >> excvss.log
```

5.2 Scheduler considerations

Consider the following when defining a Tivoli Storage Manager schedule:

- If both legacy and VSS backups are to be scheduled, do not overlap these schedules in time, as the second backup will fail. This is because Exchange will not allow legacy and VSS backups to process concurrently.
- If you are using the Tivoli Storage Manager server-prompted scheduling mode, make sure that the Data Protection for Exchange option file has the TCPCLIENTADDRESS and TCPCLIENTPORT options specified.
- If you make any changes to the Data Protection for Exchange option files that affect the scheduler, the scheduler service needs to be restarted in order to pick up the changes.

  Important: In a cluster environment, use the Cluster Administrator to stop and restart your scheduler service.

- If PASSWORDACCESS GENERATE is not specified in the dsm.opt file, then the Tivoli Storage Manager password needs to be specified on the **tdpexcc** command. To specify the password, use the /tsmpassword parameter in the command file being run by the scheduler. We typically recommend using PASSWORDACCESS GENERATE to avoid storing the password in clear text.

5.3 Monitoring backups

Verifying that a backup succeeded is as important as the backup itself. We recommend that you monitor your backups each day, so that you can be confident of the quality of the backups.

5.3.1 Log management

As part of your daily routine, review the backup logs for any errors or inconsistencies. This section provides information about the different type of logs you can view in order to monitor the health of your system. In 5.4, “Verifying backups” on page 164, we show sample log outputs.

Tivoli Storage Manager activity log

The Tivoli Storage Manager activity log contains all messages normally sent to the server console during a server operation. For Data Protection for Exchange purposes, you will see messages recording the start and end of each client session, as well as error messages sent to the server console in the activity log.

Data Protection for Exchange log

Data Protection for Exchange logs output to the file tdpexc.log in the Data Protection for Exchange installation directory; by default, this is c:\program files\tivoli\tsm\TDPExchange.

To change the log file location, use the parameter on backup operations, which is /logfile=x:\test\exchange.log. Legacy backups will only write to the Data Protection for Exchange log file, and not to the backup-archive client log file in the next section.

Backup-archive client log files

The following backup-archive client log files will also contain output from VSS backups:

- dsmsched.log
- dsmerror.log
- agtsverr.log
- dsmwebcl.log

Tivoli Storage Manager API log

The Tivoli Storage Manager API logs information to the file dsierror.log file in the Data Protection for Exchange installation directory, by default c:\program files\tivoli\tsm\TDPExchange.

Windows Event logs

Using Event Viewer and event logs, you can gather information about hardware, software and system problems. The VSS snapshot operations write detailed information to the Application log.

- Application log - This log contains events logged by programs, for example VSS snapshot information.
- Security log - This log contains valid and invalid logon attempts and events related to resource use, such as creating, opening or deleting files or other objects.
- System log - This log contains events logged by the Windows system components.

Tivoli Storage Manager scheduler logs

There are two files which contain information related to scheduling: smsched.log and dsmerror.log. These files are located in the installation directory for the backup-archive client is installed. The default directory is c:\program files\tivoli\tsm\baclient.

VSS provider logs

Your VSS provider will probably have its own log files for errors. For the IBM SVC and DS provider, the log file is called IBMVSS.log

5.4 Verifying backups

This section contains sample log file outputs, to demonstrate how you can verify the backup.

5.4.1 Tivoli Storage Manager activity log messages

The Tivoli Storage Manager server can be monitored using either the administrative client or the Tivoli Storage Manager ISC Web interface. We used the administrative command line to view the activity log.

Example 5-5 shows you the contents of the activity log relating to a VSS backup. The log shows the start time of the backup, the type of backup and which Storage Group is being backed up, and the completion status of the backup, including statistics.

Example 5-5 Tivoli Storage Manager activity log

```
tsm: ZEALOT>q act search=redbook_exchange begint=15:00

Date/Time            Message
-------------------- ------------------------------------------------------------
08/09/2006 15:15:38  ANR0406I Session 16857 started for node REDBOOK_EXCHANGE
                      (WinNT) (Tcp/Ip redbook3.rb1.local(6432)).(SESSION:16857)
08/09/2006 15:15:38  ANR0403I Session 16857 ended for node REDBOOK_EXCHANGE
(WinNT).(SESSION: 16857)
08/09/2006 15:15:41  ANR0406I Session 16858 started for node REDBOOK_EXCHANGE
                      (WinNT) (Tcp/Ip redbook3.rb1.local(6436)).(SESSION:16858)
08/09/2006 15:15:41  ANR0406I Session 16859 started for node REDBOOK_EXCHANGE
                      (TDP MSExchg) (Tcp/Ip
redbook3.rb1.local(6437)).(SESSION:16859)
08/09/2006 15:15:43  ANR0397I Session 16860 for node REDBOOK_VSS_B has begun a
                      proxy session for node REDBOOK_EXCHANGE. (SESSION: 16860)
08/09/2006 15:15:44  ANR0399I Session 16860 for node REDBOOK_VSS_B has ended a
                      proxy session for node REDBOOK_EXCHANGE. (SESSION: 16860)
08/09/2006 15:15:44  ANR0403I Session 16859 ended for node REDBOOK_EXCHANGE (TDP
MSExchg).(SESSION: 16859)
08/09/2006 15:15:47  ANR0406I Session 16861 started for node REDBOOK_EXCHANGE
                      (TDP MSExchg) (Tcp/Ip
redbook3.rb1.local(6472)).(SESSION:16861)
08/09/2006 15:15:48  ANR0397I Session 16862 for node REDBOOK_VSS_B has begun a
                      proxy session for node REDBOOK_EXCHANGE. (SESSION: 16862)
08/09/2006 15:15:51  ANE4940I (Session: 16862, Node: REDBOOK_EXCHANGE)
                      Performing a full, local + TSM backup of object
                      'Microsoft Exchange' component 'SG2' using shadow
copy.(SESSION: 16862)
08/09/2006 15:15:52  ANR0397I Session 16863 for node REDBOOK_VSS_B has begun a
                      proxy session for node REDBOOK_EXCHANGE. (SESSION: 16863)
08/09/2006 15:18:28  ANE4941I (Session: 16862, Node: REDBOOK_EXCHANGE)  Backup
                      of object 'Microsoft Exchange' component 'SG2' finished
successfully.(SESSION: 16862)
08/09/2006 15:18:32  ANE4952I (Session: 16862, Node: REDBOOK_EXCHANGE)  Total
                      number of objects inspected:       28(SESSION: 16862)
08/09/2006 15:18:32  ANE4953I (Session: 16862, Node: REDBOOK_EXCHANGE)  Total
                      number of objects archived:        28(SESSION: 16862)
08/09/2006 15:18:32  ANE4958I (Session: 16862, Node: REDBOOK_EXCHANGE)  Total
                      number of objects updated:          0(SESSION: 16862)
08/09/2006 15:18:32  ANE4960I (Session: 16862, Node: REDBOOK_EXCHANGE)  Total
                      number of objects rebound:          0(SESSION: 16862)
08/09/2006 15:18:32  ANE4957I (Session: 16862, Node: REDBOOK_EXCHANGE)  Total
                      number of objects deleted:          0(SESSION: 16862)
08/09/2006 15:18:32  ANE4970I (Session: 16862, Node: REDBOOK_EXCHANGE)  Total
                      number of objects expired:          0(SESSION: 16862)
08/09/2006 15:18:32  ANE4959I (Session: 16862, Node: REDBOOK_EXCHANGE)  Total
                      number of objects failed:           0(SESSION: 16862)
08/09/2006 15:18:32  ANE4961I (Session: 16862, Node: REDBOOK_EXCHANGE)  Total
                      number of bytes transferred: 193.13 MB(SESSION: 16862)
08/09/2006 15:18:32  ANE4963I (Session: 16862, Node: REDBOOK_EXCHANGE)  Data
```

```
                      transfer time:                    15.37 sec(SESSION:16862)
08/09/2006 15:18:32  ANE4966I (Session: 16862, Node: REDBOOK_EXCHANGE)  Network
                      data transfer rate:        12,862.85 KB/sec(SESSION:16862)
08/09/2006 15:18:32  ANE4967I (Session: 16862, Node: REDBOOK_EXCHANGE)
                      Aggregate data transfer rate:      1,208.84KB/sec(SESSION:
16862)
08/09/2006 15:18:32  ANR0399I Session 16863 for node REDBOOK_VSS_B has ended a
                      proxy session for node REDBOOK_EXCHANGE. (SESSION: 16863)
08/09/2006 15:18:32  ANE4968I (Session: 16862, Node: REDBOOK_EXCHANGE)  Objects
                      compressed by:                     0%(SESSION: 16862)
08/09/2006 15:18:32  ANE4964I (Session: 16862, Node: REDBOOK_EXCHANGE)  Elapsed
                      processing time:            00:02:43(SESSION: 16862)
08/09/2006 15:18:32  ANR0399I Session 16862 for node REDBOOK_VSS_B has ended a
                      proxy session for node REDBOOK_EXCHANGE. (SESSION: 16862)
08/09/2006 15:18:32  ANR0403I Session 16861 ended for node REDBOOK_EXCHANGE
                      (TDP MSExchg).(SESSION: 16861)
```

Refer to the Tivoli Storage Manager documentation for the complete syntax of the **QUERY ACTLOG** command. The command offers various filtering options that can be used to limit the number of messages displayed and the time it takes to process this query. If you do not specify any parameters with this command, all messages generated in the last hour are displayed.

Data Protection for Exchange log

You cannot switch off Data Protection for Exchange logging; logging messages will always be directed to a log file. If a log file is not specified, a default log file will be created in the Data Protection for Exchange installation directory. For VSS backups, the files dsmsched.log and dsmwebcl.log in the backup-archive directory will be used.

Example 5-6 shows an example of the command output from a VSS backup. You can redirect this output to a file to save it if required. In this case, we send the output to the file x:\TSMDATA\exchconsole.log using standard redirect.

```
tdpexcc backup "SG2" FULL /backupdestination=LOCAL /tsmoptfile=x:\tsmdata\dsm.opt
/configfile=c:\progra~1\tivoli\tsm\tdpexchange\tdpexc.cfg /backupmethod=VSS
/EXCSERVER=RB1EVS /logfile=x:\tsmdata\excfull_test1.log >>
x:\tsmdata\exchconsole.log
```

Example 5-6 displays the type of backup (in our case, a VSS), the Storage Group which was backed up (in our case, SG2), the DSMAgent being used (in our case, REDBOOK_VSS_B), the preparing of a snapshot backup, the integrity check of the Storage Group backup, the completion status of the backup, and the statistics on files examined, files completed for backup, failed files, and total bytes sent. In our example, we backed up a single Storage Group.

Example 5-6 Data Protection for Exchange command output log

```
IBM Tivoli Storage Manager for Mail:
Data Protection for Microsoft Exchange Server
Version 5, Release 3, Level 3.0
(C) Copyright IBM Corporation 1998, 2006. All rights reserved.

ACN5057I The e:\tsmdata\excsch.log log file has been pruned successfully.

Connecting to TSM Server as node 'REDBOOK_EXCHANGE'...
```

```
Connecting to Local DSM Agent 'REDBOOK_VSS_B'...
Starting storage group backup...

Beginning VSS backup of 'SG2'...


Preparing to backup using snapshot.
Executing system command: Exchange integrity check for storage group 'SG2'
   Files Examined/Completed/Failed: [ 5 / 2 / 0 ]   Total Bytes: 6489520
   Files Examined/Completed/Failed: [ 5 / 2 / 0 ]   Total Bytes: 18352984
   Files Examined/Completed/Failed: [ 5 / 2 / 0 ]   Total Bytes: 29987044
   Files Examined/Completed/Failed: [ 5 / 2 / 0 ]   Total Bytes: 41784964
   Files Examined/Completed/Failed: [ 5 / 2 / 0 ]   Total Bytes: 53550112
   Files Examined/Completed/Failed: [ 5 / 2 / 0 ]   Total Bytes: 65380804
   Files Examined/Completed/Failed: [ 13 / 3 / 0 ]   Total Bytes: 74565413
   Files Examined/Completed/Failed: [ 14 / 4 / 0 ]   Total Bytes: 85421983
   Files Examined/Completed/Failed: [ 14 / 4 / 0 ]   Total Bytes: 94860833
   Files Examined/Completed/Failed: [ 15 / 10 / 0 ]   Total Bytes: 105749843
   Files Examined/Completed/Failed: [ 15 / 10 / 0 ]   Total Bytes: 117580535
   Files Examined/Completed/Failed: [ 15 / 10 / 0 ]   Total Bytes: 129443999
   Files Examined/Completed/Failed: [ 15 / 10 / 0 ]   Total Bytes: 140914199
   Files Examined/Completed/Failed: [ 15 / 10 / 0 ]   Total Bytes: 152744891
   Files Examined/Completed/Failed: [ 15 / 10 / 0 ]   Total Bytes: 164477267
   Files Examined/Completed/Failed: [ 15 / 10 / 0 ]   Total Bytes: 176307959
   Files Examined/Completed/Failed: [ 15 / 10 / 0 ]   Total Bytes: 188040335
   Files Examined/Completed/Failed: [ 16 / 11 / 0 ]   Total Bytes: 198240876
   Files Examined/Completed/Failed: [ 28 / 28 / 0 ]   Total Bytes: 202512771
   Files Examined/Completed/Failed: [ 28 / 28 / 0 ]   Total Bytes: 202512771
   Files Examined/Completed/Failed: [ 28 / 28 / 0 ]   Total Bytes: 202512771
   Files Examined/Completed/Failed: [ 28 / 28 / 0 ]   Total Bytes: 202512771

SS Backup operation completed with rc = 0
   Files Examined   : 28
   Files Completed  : 28
   Files Failed     : 0
   Total Bytes      : 202512771
```

The next log file shown is the Exchange log file (tdpexc.log this is the default), as seen in Example 5-7. It shows the start and end time of the backup, the type of backup, the backup request, and the backup destination. The example shows you the completion state of the backup and the backup statistics. You can change the default log file by using the \logfile parameter in your batch file or command, for example:

/logfile=x:\tsmdata\exchange.log

Example 5-7 Data Protection for Exchange log file

```
08/09/2006 15:11:42 ============== Log file pruned using log retention period of
60 day(s)
08/09/2006 15:11:42 ============== No log entries pruned
08/09/2006 15:11:48
========================================================================
08/09/2006 15:11:48 Request                   : QUERY Exchange
08/09/2006 15:11:48 Exchange Server            : RB1EVS
08/09/2006 15:11:48
------------------------------------------------------------------------
```

```
08/09/2006 15:11:48 ============================================================
08/09/2006 15:11:48 Request                          : VSS Backup
08/09/2006 15:11:48 Component List                   : 'SG2'
08/09/2006 15:11:48 Backup Type                      : full
08/09/2006 15:11:48 Backup Destination               : TSM and Local
08/09/2006 15:11:48 Local DSMAGENT Node              : REDBOOK_VSS_B
08/09/2006 15:11:48 Offload to Remote DSMAGENT Node  :
08/09/2006 15:11:48 Mount Wait                       : Yes
08/09/2006 15:11:48 ------------------------------------------------------------
08/09/2006 15:14:34 VSS Backup operation completed with rc = 0
08/09/2006 15:14:34    Files Examined   : 28
08/09/2006 15:14:34    Files Completed  : 28
08/09/2006 15:14:34    Files Failed     : 0
08/09/2006 15:14:34    Total Bytes      : 202512771
```

Tivoli Storage Manager API log

The Tivoli Storage Manager API log, dsierror.log, does not contain backup statistics, but instead contains API error information. For example, if you specify an incorrect password for the Data Protection for Exchange GUI when running a restore to another server, the authentication problem message is logged into the dsierror.log file. Example 5-8 shows an example of the dsierror.log file.

Example 5-8 API log file - dsierror.log

```
08/09/2006 15:27:01 ANS1353E Session rejected: Unknown or incorrect ID entered
08/09/2006 15:29:24 ANS1353E Session rejected: Unknown or incorrect ID entered
08/09/2006 15:35:09 ANS1235E An unknown system error has occurred from which TSM
cannot recover.
08/09/2006 15:43:14 ANS1353E Session rejected: Unknown or incorrect ID entered
08/09/2006 16:03:18 ANS1353E Session rejected: Unknown or incorrect ID entered
```

Windows Event log

The Exchange server writes event information to the Windows event log. When running a VSS backup, detailed events are logged in the Event log showing the process steps and also if any failures occur during the VSS backup.

Figure 5-7 shows an example of the Event Viewer. It is instructive to step through these events one by one to see exactly what is happening here, and to confirm that your VSS backups completed successfully.

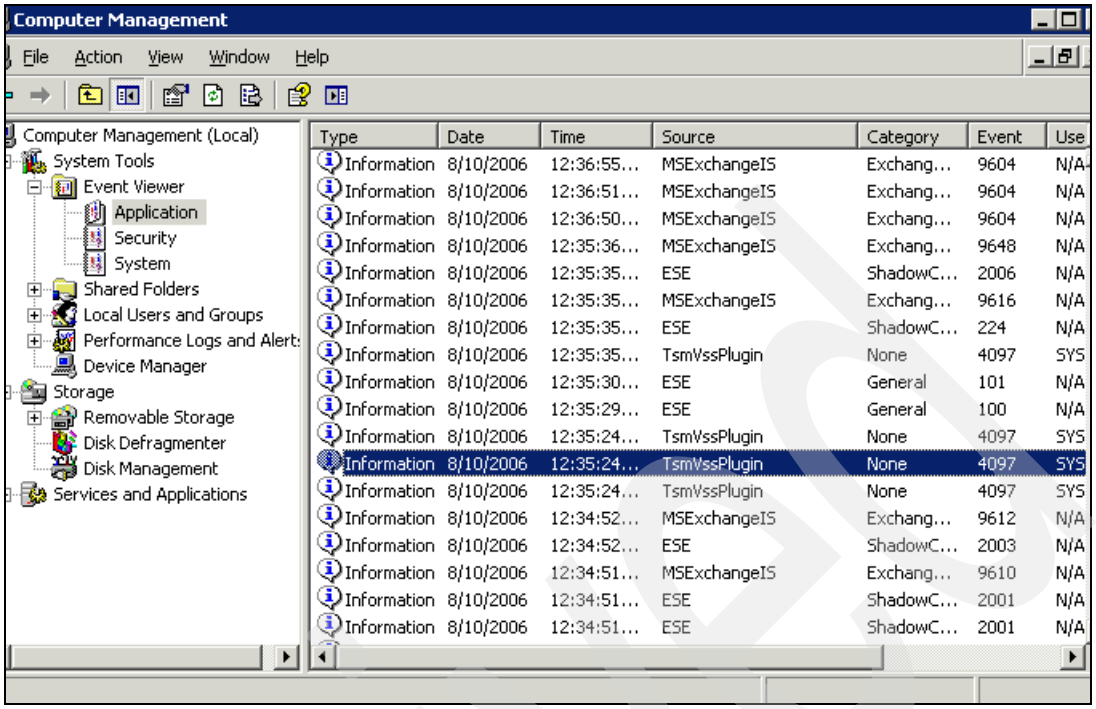


Figure 5-7 Windows event log

Figure 5-8 on page 169 and Figure 5-9 on page 170 are examples of a detailed description of a VSS backup. We recommend using the arrow keys to show all the messages about the backup in turn, in order to understand the process in detail.

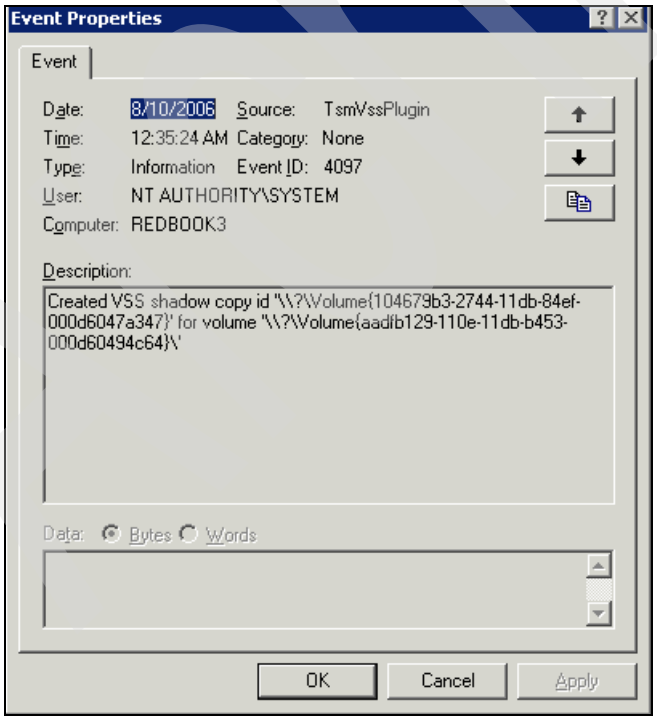


Figure 5-8 Sample Windows VSS backup event - 1

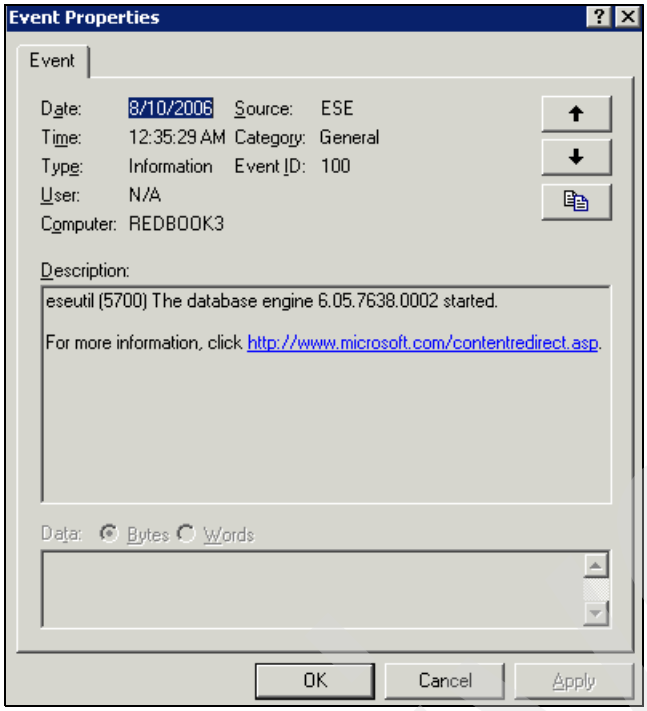


Figure 5-9 Sample Windows VSS backup event - 2

Tivoli Storage Manager client logs

The dsmerror.log and dsmsched.log are used when a backup is initiated from the scheduler for legacy and VSS backups. The dsmerror.log is also used when running a VSS backup via the GUI or command line; it contains all errors when a VSS backup is initiated.

Example 5-9 shows that a VSS backup was initiated but the staging directory could not be found and the default staging directory would be used. We discuss the staging directory parameter, VSSALTSTAGINGDIR in 3.2.7, “Configure the option and config files” on page 56.

Example 5-9 dsmerror.log

```
07/19/2006 15:15:19 ANS5253W The system could not create Volume Shadow Copy
Services staging directory 'k:\tsmvssdir\adsm.sys\vss_staging'.
07/19/2006 15:15:19 ANS1620I A 'LOCAL' backup version backupdate
'07/19/200612:13:56' is not consistent with local repository and has been deleted
from the server (object name='RB1EVS\Microsoft Exchange
Writer\{76fe1ac4-15f7-4bcd-987e-8e1acb4\LOCAL\FULL\00000000000000\Microsoft
Exchange Server\Microsoft Information
Store\RB1EVS\b2e86828-8f9a-4a8a-97b4-f76cb1c14443\LOCAL\FULL\00000000000000\Micros
oft Exchange Server\Microsoft Information
Store\RB1EVS\b2e86828-8f9a-4a8a-97b4-f76cb1c14443\SG1', ID = '0:1292779').
```

The dsmsched.log file logs all schedule information related to legacy and VSS backups. As seen in Example 5-10 on page 171, a scheduled backup has been initiated. You can see the schedule name, the action (command, incremental, full), the objects and the start and end time of the schedule.

In our example the following entry does not indicate the success or failure of the backup operation; it only shows that the Tivoli Storage Manager server successfully issued the scheduled command associated with the event name:

```
Scheduled event ‘REDBOOK_TEST’ completed successfully
```

To verify the success of the process, note the return code of the subsequent entry:

```
Finished command. Return code is: 0
```

If the backup process failed, the return code will be indicated as follows:

```
Finished command. Return code is: 1
```

Example 5-10 dsmsched.log

```
08/09/2006 15:11:42 Querying server for next scheduled event.
08/09/2006 15:11:42 Node Name: REDBOOK_EXCHANGE
08/09/2006 15:11:42 Session established with server ZEALOT: Windows
08/09/2006 15:11:42   Server Version 5, Release 3, Level 3.0
08/09/2006 15:11:42   Server date/time: 08/09/2006 15:15:41  Last access:
08/09/2006 15:15:38

08/09/2006 15:11:42 --- SCHEDULEREC QUERY BEGIN
08/09/2006 15:11:42 --- SCHEDULEREC QUERY END
08/09/2006 15:11:42 Next operation scheduled:
08/09/2006 15:11:42 ------------------------------------------------------------
08/09/2006 15:11:42 Schedule Name:         REDBOOK_TEST
08/09/2006 15:11:42 Action:                Command
08/09/2006 15:11:42 Objects:               e:\tsmdata\excfull.bat
08/09/2006 15:11:42 Options:
08/09/2006 15:11:42 Server Window Start:   15:14:54 on 08/09/2006
08/09/2006 15:11:42 ------------------------------------------------------------
08/09/2006 15:11:42
Executing scheduled command now.
08/09/2006 15:11:42
Executing Operating System command or script:
   e:\tsmdata\excfull.bat
08/09/2006 15:14:38 Finished command.  Return code is: 0
08/09/2006 15:14:38 ANS1908I The scheduled command completed successfully.
08/09/2006 15:14:38 Scheduled event 'REDBOOK_TEST' completed successfully.
08/09/2006 15:14:38 Sending results for scheduled event 'REDBOOK_TEST'.
08/09/2006 15:14:38 Results sent to server for scheduled event 'REDBOOK_TEST'.
```

The file dsmwebcl.log logs information related to the CAD and the DSMAgent user. In Example 5-11, we see that the REDBOOK_EXCHANGE is the DSMAgent user. This type of user information is logged when a VSS backup is initiated and the Local or Remote DSMAgent client is called to start a backup or restore.

Example 5-11 dsmwebcl.log

```
08/09/2006 17:05:55 (dsmcad) IBM Tivoli Storage Manager
08/09/2006 17:05:55 (dsmcad) Client Acceptor - Built Jun 20 2006 17:07:12
08/09/2006 17:05:55 (dsmcad) Version 5, Release 3, Level 4.3
08/09/2006 17:05:56 (dsmcad) Dsmcad is working in   Webclient mode.
08/09/2006 17:05:56 (dsmcad) ANS3000I HTTP communications available on port 1581.
```

```
08/09/2006 17:05:56 (dsmcad) ANS3000I TCP/IP communications available on port
8939.
08/09/2006 17:06:25 (dsmagent) IBM Tivoli Storage Manager
08/09/2006 17:06:25 (dsmagent) Remote Client Agent - Built Jun 20 2006 17:06:32
08/09/2006 17:06:25 (dsmagent) Version 5, Release 3, Level 4.3
08/09/2006 17:06:28 (dsmagent) ANS3002I Session started for user REDBOOK_EXCHANGE
(TCP/IP 9.43.238.217).
08/09/2006 17:06:31 (dsmagent) ANS3003I Session ended for user REDBOOK_EXCHANGE.
08/09/2006 17:06:35 (dsmagent) ANS3002I Session started for user REDBOOK_EXCHANGE
(TCP/IP 9.43.238.217).
08/09/2006 17:11:13 (dsmagent) ANS3003I Session ended for user REDBOOK_EXCHANGE.
```

Staging directory log files

Staging directory log files are generated when a VSS backup is initiated. For every VSS backup that is run, a new staging subdirectory is created with the current date and time stamp. By default, this is c:\adsm.sys\vss_staging\REDBOOK_EXCHANGE\9.43.238.18 was created by the system. Within this directory you would find audit log files which are created for each Exchange Storage Group. These files will check your VSS volumes for any errors, before using the volumes.

To specify a different staging directory, use the VSSALTSTAGINGDIR parameter in the backup-archive client dsm.opt file as follows:

```
vssaltstagingdir x:\tsmvssdir
```

In a clustered environment, specify a shared disk that does not contain any Exchange data stores. For more information about this topic, refer to 3.2.7, “Configure the option and config files” on page 56.

5.5 Performance considerations

Many factors will determine the performance of your backup and restore. These include:

- Disk configuration
- Network type
- Server configuration
- Data capacity

There are a number of tuning parameters which you can adjust to achieve better performance, and you can also tune buffers or implement LAN-free backups. Detailed discussion of Tivoli Storage Manager performance tuning is beyond the scope of this Redbook; however, we provide some general guidelines here. For more information, see *IBM Tivoli Storage Manager Performance Tuning Guide,* SC32-9101.

By implementing buffering, you can take advantage of asynchronous execution threads which Data Protection for Exchange uses when transferring data between Exchange and the Tivoli Storage Manager server. This option is only valid for legacy backups. Buffering is configured using the BUFFSIZE and the BUFFERS option in the Exchange tdpexc.cfg file.

When running VSS backups, the backup-archive client (local DSMAgent) dsm.opt file is used.

Within the dsm.opt file you can tune the following performance-related parameters:

- TCPWINDOWSIZE
- TCPBUFFSIZE
- TXNBYTELIMIT

You could also consider using the LAN-free backup to back up your data, as this will send data over the SAN, rather than the LAN.

Also, consider how the following issues affect performance:

- Backups to local shadow volumes do not send data to the Tivoli Storage Manager server. Only metadata is sent to the Tivoli Storage Manager server.
- During a VSS backup, integrated Exchange integrity checking reads every page in the files to be backed up. This increases the backup time. You can disable the integrity check in some circumstances; however, we do not recommend this.
- The time required to perform a snapshot ranges from seconds to minutes, depending on the type of VSS provider used. Establish a baseline time for VSS snapshots outside of Tivoli Storage Manager (for example, by using **vshadow** as described in 3.2.15, “Using vssadmin and vshadow commands” on page 86).

5.6 Managing snapshot-based backups

Snapshot-based backups (that is, VSS local backups) are managed by the VSSPOLICY settings. These VSS policy settings are the management classes configured in your Tivoli Storage Manager server. *All* Local snapshot backups are managed by the Tivoli Storage Manager server version options. These versions will determine how long your data will reside on your VSS disks.

For VSS backup data sent to Tivoli Storage Manager server storage, the snapshot backup is deleted after the data is successfully backed up to the Tivoli Storage Manager server storage, because a non-persistent snapshot is used. As discussed in 2.5, “How Tivoli Storage Manager manages VSS backups” on page 34, you must consider the following when managing snapshot backups:

- The VSS disk space required when selecting the number of versions to be kept
- The size of each LUN that needs to be assigned for snapshot space
- The extra space required to do a VSS backup to Tivoli Storage Manager

5.7 Troubleshooting tips

When problems are encountered, the most important step to solving the problem is diagnosis; in particular, isolating the circumstances when the problem does and does not occur. Use of the log files as described previously in this chapter is a critical tool for problem diagnosis. The following list provides tips which can be useful in finding the source of your problem:

- Analyze whether the problem concerns all or individual servers. If only some servers are affected, probably the problem is in their individual configuration.
- Are all Storage Groups affected, or just one Storage Group? If only one Storage Group is affected, try to find any differences in configuration for this Storage Group.
- Consider when the problem occurs: is it 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 to determine whether it is a scheduling problem or a Data Protection for Exchange problem.
- Is it a legacy or VSS backup problem?
- Is the problem reproducible on both the CLI and GUI?
- Try to correctly identify the problem source. For example, is it related to Exchange or Tivoli Storage Manager? Is it a Tivoli Storage Manager client or server problem?
- Is it a LAN or SAN problem?
  - If you are having SAN problems, check the ENABLELANFREE parameter in the options file and check whether your SAN configuration has been setup correctly.
  - If it is a LAN backup, determine whether your TCP/IP network has been configured correctly and whether the problem only pertains to your Exchange server or to all other servers in your environment.
- If running in a cluster environment, check the CLUSTERNODE parameter in the options file and verify that you are using the correct /excserver option for the CLI and GUI.
- Check whether your cluster has failed over or not and what caused the failover.
- The VSHADOW test shown in 3.2.15, “Using vssadmin and vshadow commands” on page 86 is an excellent problem determination tool.

When considering these possibilities, try to see what is the same and what is different, and try to create the pattern of the situation causing the problem. The following is a list of items that may help solve your problem:

- Windows Event Log - Trace the Event log for Legacy and VSS backups writes to these logs.
- Names - See whether the spelling and case are correct and whether you use special characters.
- Verify that you have given the backup or restore the appropriate permissions.
- Check legacy, VSS, Exchange, Tivoli Storage Manager, and MSCS cluster configurations (if used) and Service Pack levels.
- Check your VSS disk infrastructure, if configured as specified by your VSS provider.
- Examine your schedule scripts.
- Consider the order of actions you issued and the events you had in response to your actions.

You could run a trace to determine where the problem exists. The trace will give you detailed trace information about the action you perform. If you use this parameter, trace information will be 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 Exchange server for legacy backups, or in your Local or Remote DSMAgent dsm.opt file. If this file does not exist, a new one will be created. If the file exists, the new events are appended to the file.

```
/TraceFlag=ALL
```

This is the default. You could trace only specific events, but this 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, or in the Local or Remote DSMAgent dsm.opt file for VSS backups.

If the problem persists, contact the IBM help desk for support. You can also find more information (including detailed trace formats) in the *IBM Tivoli Storage Manager Problem Determination Guide,* SC23-9101, which is available at:

http://publib.boulder.ibm.com/tividd/td/TSMM/SC32-9103-00/en_US/HTML/index.html.

A

Disabling SSL in the SVC CIMOM

In this appendix we describe how to disable SSL in the SVC CIMOM. This is required if you will use the Instant Restore function.

Disable SSL

Here are the instructions for turning SSL off in the SVC CIMOM.

1. Edit the CIMOM properties file, C:\Program Files\IBM\svcconsole\cimom\cimom.properties to make sure the correct HTTP port is chosen. The Server Communication method should be HTTP, and DigestAuthentication set to false.

   The lines in the file should look like the following:

   ```
   Port=5998
   ServerCommunication=HTTP
   DigestAuthentication=false
   ```

2. Change the WebSphere® files to use the new CIMOM settings. You have to edit the cimom.properties file in each of these directories:

   – C:\Program Files \IBM\svcconsole\console\embeddedWAS\installedApps\DefaultNode\ICAConsole.ear\ ICAConsole.war\WEB-INF

   – C:\Program Files\IBM\svcconsole\console\embeddedWAS\installedApps\DefaultNode\SVCConsole. ear\SVCConsole.war\WEB-INF

   – C:\Program Files\IBM\svcconsole\console\embeddedWAS\config\cells\DefaultNode\applications\ICAConsole.ear\deployments\ICAConsole\ICAConsole.war\WEB-INF

   – C:\Program Files\IBM\svcconsole\console\embeddedWAS\config\cells\DefaultNode\applications\SVCConsole.ear\deployments\SVCConsole\SVCConsole.war\WEB-INF

   In each of the cimom.properties files in these directories, add a line:

   ```
   Port=5998
   ```

   Also, ensure that the SslEnabled parameter is set to: `false`.

   ```
   SslEnabled=false
   ```

3. Restart the CIMOM service: *CIM Object Manager - SVC* and WebSphere service: *IBM WebSphere Application Server V5 - SVC*.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

IBM Redbooks

For information about ordering these publications, see “How to get IBM Redbooks” on page 180. Note that some of the documents referenced here may be available in softcopy only.

- *IBM Tivoli Storage Management Concepts*, SG24-4877
- *IBM Tivoli Storage Manager Implementation Guide*, SG24-5416
- *Using Tivoli Data Protection for Microsoft Exchange Server*, SG24-6147
- *IBM Tivoli Storage Manager in a Clustered Environment*, SG24-6679

Other publications

These publications are also relevant as further information sources:

- *Data Protection for Microsoft Exchange Server Installation and Users Guide*, SC32-9058
- *IBM Tivoli Storage Manager Performance Tuning Guide,* SC32-9101
- *IBM Tivoli Storage Manager Problem Determination Guide,* SC23-9103
- *IBM Tivoli Storage Manager Backup-Archive Clients Installation and Users Guide (Windows),* GC32-0788

Online resources

These Web sites are also relevant as further information sources:

- Microsoft

  http://www.microsoft.com/
- Data Protection for Exchange supported environments

  http://www.ibm.com/support/docview.wss?rs=669&context=SSTG2D&uid=swg21233936&loc=en_US&cs=utf-8&lang=en
- Tivoli Storage Manager product support

  http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliStorageManager.html
- Tivoli Storage Manager for Copy Services supported environments

  http://www.ibm.com/support/docview.wss?rs=3042&context=SSRURH&uid=swg21231465
- Tivoli Storage Manager client fixes for Microsoft VSS

  http://www.ibm.com/support/docview.wss?uid=swg21240684

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

P

Q

R

S

T

V

W

Using IBM Tivoli Storage Manager to Back Up Microsoft Exchange with VSS

Using IBM Tivoli Storage Manager to Back Up Microsoft Exchange with VSS

Fast backup and restore of Microsoft Exchange Databases

Integration with VSS

Use hardware-based copy services

Typical Microsoft Exchange environments are growing larger and increasingly are managing data and applications critical to a business. This makes backup and restore a greater challenge. Microsoft Volume Shadow Copy Service (VSS) is a way to use the instant copy capabilities of disk storage hardware for faster backup, thereby reducing the time taken for backup as well as reducing the impact which the backup operation has on the Exchange server.

IBM Tivoli Storage Manager for Copy Services, together with Data Protection for Mail, leverages VSS functionality in an integrated, easy-to-use way, to back up and restore Exchange databases. It supports a wide variety of disk hardware and uses the same interface as traditional Data Protection for Mail operations.

This IBM Redbook will help you plan, configure and run IBM Tivoli Storage Manager for Copy Services in your Microsoft Exchange environments.

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

SG24-7373-00 ISBN 0738489514