SnapManager® 3.2 for Microsoft® Exchange Installation and Administration Guide

Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089 USA
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP
Documentation comments: doccomments@netapp.com
Information Web: http://www.netapp.com

Part number 215-01873_A0
April 2006

Copyright and trademark information

Copyright information

Copyright © 1994–2006 Network Appliance, Inc. All rights reserved. Printed in the U.S.A.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted Network Appliance material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETWORK APPLIANCE "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL NETWORK APPLIANCE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Network Appliance reserves the right to change any products described herein at any time, and without notice. Network Appliance assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Network Appliance. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of Network Appliance.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

NetApp, the Network Appliance logo, the bolt design, NetApp–the Network Appliance Company, DataFabric, Data ONTAP, FAServer, FilerView, MultiStore, NearStore, NetCache, SecureShare, SnapManager, SnapMirror, SnapMover, SnapRestore, SnapVault, SyncMirror, and WAFL are registered trademarks of Network Appliance, Inc. in the United States, and/or other countries. gFiler, Network Appliance, SnapCopy, Snapshot, and The Evolution of Storage are trademarks of Network Appliance, Inc. in the United States and/or other countries and registered trademarks in some other countries. ApplianceWatch, BareMetal, Camera-to-Viewer, ComplianceClock, ComplianceJournal, ContentDirector, ContentFabric, EdgeFiler, FlexClone, FlexVol, FPolicy, HyperSAN, InfoFabric, LockVault, Manage ONTAP, NOW, NOW NetApp on the Web, ONTAPI, RAID-DP, RoboCache, RoboFiler, SecureAdmin, Serving Data by Design, SharedStorage, Simulate ONTAP, Smart SAN, SnapCache, SnapDirector, SnapDrive, SnapFilter, SnapLock, SnapMigrator, SnapSuite, SnapValidator, SohoFiler, vFiler, VFM, Virtual File Manager, VPolicy, and Web Filer are trademarks of Network Appliance, Inc. in the United States and other countries. NetApp Availability Assurance and NetApp ProTech Expert are service marks of Network Appliance, Inc. in the United States. Spinnaker Networks, the Spinnaker Networks logo, SpinAccess, SpinCluster, SpinFS, SpinHA,

SpinMove, and SpinServer are registered trademarks of Spinnaker Networks, LLC in the United States and/or other countries. SpinAV, SpinManager, SpinMirror, SpinRestore, SpinShot, and SpinStor are trademarks of Spinnaker Networks, LLC in the United States and/or other countries.

Apple is a registered trademark and QuickTime is a trademark of Apple Computer, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

Network Appliance is a licensee of the CompactFlash and CF Logo trademarks.

Network Appliance NetCache is certified RealSystem compatible.

Table of Contents

Preface xi

Chapter 1 **Understanding SnapManager** 1

SnapManager overview. 2

How SnapManager works with the other system components 8

How SnapManager works with other backup methods. 13

Chapter 2 **Preparing to Install or Upgrade SnapManager** 15

Preinstall or preupgrade procedure 16

Backing up system resources and data 18

Understanding SnapManager license options 19

Understanding SnapManager COM server identity account requirements. . . 20

Understanding storage system requirements 22

Understanding Windows host system requirements 24

Chapter 3 **Installing or Upgrading SnapManager** 29

Installing SnapManager on a stand-alone Windows host system 31

Installing SnapManager and creating a new Windows cluster 43

Installing SnapManager in an existing Windows cluster. 46

Upgrading to SnapManager 3.2 48

Uninstalling SnapManager 55

Reinstalling SnapManager 62

Chapter 4 **Starting SnapManager for the First Time** 63

Starting SnapManager and connecting to the default server 64

What to do next 69

Chapter 5 **Determining the Number of LUNs Required** 71
Understanding Exchange configuration rules 72
Understanding SnapManager configuration rules for Exchange 74
Understanding NTFS volume mount points 78
Understanding SnapManager support for volume mount points 80
Understanding transaction log archiving using NTFS hard links 84
Example Exchange configurations supported with SnapManager 87

Chapter 6 **Creating Storage System Volumes and LUNs** 93
Developing your SnapManager data configuration plan 94
Calculating LUN size for Exchange databases 96
Calculating single-instance sharing ratio for a database LUN 98
Calculating deleted-item cache size for a database LUN. 100
Calculating LUN size for transaction logs and SnapInfo directory 101
Calculating volume size 104
Effect of new features on volume sizing 107
Preparing storage system volumes and LUNs for SnapManager. 110

Chapter 7 **Configuring the Exchange Data for SnapManager** 113
Understanding the SnapManager Configuration Wizard. 114
Using the Configuration Wizard to configure your data store 118
Migrating an existing SnapManager for Exchange configuration from using drive letters to using mount points. 130

Chapter 8 **Understanding SnapManager Backup** 135
How SnapManager Backup works 136
How SnapManager backup data is organized 141
How SnapManager checks database integrity in backup sets 145
Ways to manage the number of backup sets kept online 150
Ways to manage the backup and deletion of transaction logs 154
When to run a SnapManager backup 157

About Exchange options and Exchange System Manager 159

Chapter 9 **Backing Up Databases with SnapManager** 163

Backing up databases 164

What to do if your SnapManager backup fails 173

Verifying backup databases 176

Using backup management groups in backup and verification. 180

Chapter 10 **Restoring Databases with SnapManager** 183

Understanding SnapManager Restore 184

Guidelines for restoring SnapManager backups 190

Restoring from a SnapManager backup 192

Chapter 11 **Managing Backup and Restore Snapshots**. 199

Explicitly deleting storage group backups 200

Explicitly deleting an individual backup 209

Problem deleting backups due to busy Snapshot copy error 211

Chapter 12 **Using SnapMirror with SnapManager** 213

Other documentation 214

Understanding SnapMirror 215

How SnapManager uses SnapMirror 217

Scheduling SnapMirror replication for SnapManager backups 219

Chapter 13 **Performing Disaster Recovery with SnapManager** 223

Guides you should read and have at hand 224

Preparing for disaster recovery 225

Restoring your Exchange environment 230

Disaster recovery by relocating Exchange virtual servers to a different Windows cluster 261

Chapter 14 **Archiving SnapManager Backups** 299
Understanding SnapManager backup set archival 300
Choosing the best way to archive your SnapManager backups 303
Using NDMP or dump to archive SnapManager backups 304
Using a Windows backup utility to archive SnapManager backups 308
Using Exchange Backup Agent to archive Exchange backups. 311
Using Run Command After Operation to archive automatically. 313

Chapter 15 **Managing SnapManager Reports** 321
Understanding SnapManager reports. 322
Deleting SnapManager reports 323
Printing SnapManager reports 324

Appendix A **SnapManager Command-Line Reference** 325
Guidelines for using the commands 326
snapbackup 327

Appendix B **Configuring SnapManager Application Settings** 335
Overview of SnapManager application settings 336
Connecting to a different Exchange server 338
Changing the Exchange user account. 340
Enabling or disabling database migration back to local disks 341
Selecting the database verification server 342
Selecting the Snapshot copy access method for database verification 346
Configuring Eseutil throttling for database verification 348
Overriding database verification during restore 354
Managing the backup setting 357
Managing the Run Command After Operation default settings 358
Managing fractional space reservation 360
Managing the report directory options 372

Managing the event notification options 374

Index 381

Preface

About this guide

This guide describes how to install and configure SnapManager® 3.2 for Microsoft® Exchange software and use its online backup and restore features. It also describes how to use SnapMirror® functionality with SnapManager.

This guide does not explain how to install, configure, and use the SnapDrive™ features that enable you to create and connect to LUNs, which you must do before you use SnapManager. For this information and details about how to configure Network Appliance™ storage system volumes and enable storage system access, see your SnapDrive documentation.

This guide does not cover basic system or network administration topics, such as IP addressing, routing, and other network topology.

Audience

This guide is for system and database administrators with a working knowledge of Microsoft Exchange. The discussion assumes familiarity with the following topics:

- Microsoft Exchange server administration
- Network functions and operations
- Basic concepts for moving data over a network
- Your operating system, network, and Network Appliance storage system, such as a filer
- CIFS protocols, as used for file sharing and file transfers
- FCP and iSCSI LUN access protocols

Typographic conventions

The following table describes the typographic conventions used in this guide.

Convention	Type of information
Italic type	Words or characters that require special attention. Placeholders for information you must supply. For example, if the guide says to enter the `arp -d` *hostname* command, you enter the characters “arp -d” followed by the actual name of the host. Book titles in cross-references.

Convention	Type of information
`Monospaced` font	Command and daemon names. Information displayed on the system console or other computer monitors. The contents of files. Formulae and calculations.
`Bold monospaced` font	Words or characters you type. What you type is always shown in lowercase letters, unless you must type it in uppercase letters.

Special messages

This guide contains special messages that appear in the following circumstances:

Note

A note provides important information to help you install or operate your system efficiently.

Attention

An attention contains instructions that keep you from crashing your system or losing data.

Understanding SnapManager 1

This section explains how SnapManager 3.2 for Microsoft Exchange works, and how it integrates with the rest of your environment. The following topics are covered:

- "SnapManager overview" on page 2
- "How SnapManager works with the other system components" on page 8
- "How SnapManager works with other backup methods" on page 13

Related topics:

- Chapter 2, "Preparing to Install or Upgrade SnapManager," on page 15
- Chapter 3, "Installing or Upgrading SnapManager," on page 29
- Chapter 4, "Starting SnapManager for the First Time," on page 63

SnapManager overview

SnapManager provides an integrated data management solution for Microsoft Exchange that dramatically boosts the availability, scalability, and reliability of Exchange databases. See the following topics for more information:

- "New functionality for this version" on page 2
- "What SnapManager does" on page 4
- "What SnapManager does not do" on page 5
- "Where you install and run SnapManager" on page 5
- "About the SnapManager graphical user interface" on page 6
- "About the SnapManager command line interface" on page 7
- "How you use SnapManager" on page 7

Related topics:

- "How SnapManager works with the other system components" on page 8
- "How SnapManager works with other backup methods" on page 13

New functionality for this version

SnapManager 3.2 for Microsoft Exchange introduces the following new features:

NTFS volume mount point support: NTFS volume mount point support enables SnapManager 3.2 to manage Exchange databases stored on mounted NTFS volumes (on dedicated disks or shared cluster resource disks) or standard Windows volumes. This removes the 26-drive-letter limitation you might have encountered with previous releases of SnapManager with a large number of databases that need to be restored individually.

For more information, see "Understanding NTFS volume mount points" on page 78, "Understanding SnapManager support for volume mount points" on page 80, and "Migrating an existing SnapManager for Exchange configuration from using drive letters to using mount points" on page 130.

Fractional space reservation policies: If a storage system volume is configured with fractional space reservation (also called "overwrite reserve") of less than 100 percent, write operations to LUNs on that volume are not guaranteed unless the reserve level is monitored and preventive action is taken when overwrite reserve utilization becomes too high. SnapManager 3.2 provides an Exchange-aware space management tool for this type of volume, designed specifically for LUNs that reside on volumes with fractional space reservation set to less than 100 percent and that store Exchange databases or SnapManager SnapInfo directories.

For more information, see "Managing fractional space reservation" on page 360.

Copy-less transaction log archiving: During a SnapManager backup operation, SnapManager archives transaction log files on the live file system to the SnapInfo directory. SnapManager 3.2 automatically optimizes backup operations in which the storage group transaction log files and the associated SnapInfo directory are located on the same NTFS volume. When archiving transaction log files to a SnapInfo directory on the same NTFS volume, SnapManager **creates NTFS hard links** instead of performing a file copy operation. This conserves storage system disk space and improves system performance during the transaction log archival phase of the backup operation.

To enable SnapManager to apply this optimization feature even when your transaction log files reside on multiple NTFS volumes, you can configure your Exchange data to use **multiple SnapInfo directories**, with each SnapInfo directory located on the LUN that stores the transacgtion logs for the respective storage group

For more information, see "Understanding transaction log archiving using NTFS hard links" on page 84.

Age-based backup set retention: Both automatic and explicit Snapshot copy deletion functionality have been enhanced to support the deletion of backups older than a specified number of days.

For more information, see the following topics:

- "Automatic deletion of backups in a management group" on page 151
- "Explicitly deleting storage group backups" on page 200
- "Explicitly deleting an individual backup" on page 209

Control over database verification throughput rate: With previous releases of SnapManager, you have two options for decreasing the load that database verification places on the Exchange server and on the NetApp storage system: **remote database verification** and **deferred database verification**. In both cases, the load is managed by separating the database verification step from the database backup operation. Remote verification distributes the load between two hosts. Deferred verification occurs when automatic verification is disabled during the backup operation and checksum verification of the backup is performed later, either as a separate operation or as a part of a restore operation that uses that backup. When it is used with Exchange 2003 Service Pack 2 (SP2), SnapManager 3.2 offers a third option for decreasing the database verification load: **throttling of Eseutil checksum verification** in order to decrease the verification throughput rate.

For more information, see "Configuring Eseutil throttling for database verification" on page 348.

What SnapManager does

SnapManager provides rapid online backup and near instantaneous restoration of Exchange databases by using online Snapshot™ technology that is part of the Data ONTAP® software and integrating the Microsoft Exchange backup and restore APIs and VSS. SnapManager can also leverage the SnapMirror capabilities of storage systems to provide on-site or off-site SnapManager backup set mirroring for disaster recovery.

Data management: SnapManager supports the following data management capabilities:

- Migrating Exchange databases and transaction logs to LUNs on storage systems
- Backing up Exchange databases and transaction logs from LUNs on storage systems
- Verifying the backed-up Exchange databases and transaction logs
- Managing the SnapManager backup sets
- Restoring Exchange databases and transaction logs from previously created SnapManager backup sets

Data archival for long-term or remote storage of backups: You can use SnapManager to create offline archives of Snapshot copies containing Exchange backup sets for long term or remote backup storage. Three different archive methods are supported:

- Manually initiated archival using NDMP (Network Data Management Protocol) or the storage system's `dump` command
- Manually initiated archival using a Windows backup utility
- Automatic archival using the Run Command After Operation feature with your backup operation

  The SnapVault software can be used to archive backup sets.

The archival of Exchange database backup sets using SnapManager is described in Chapter 14, "Archiving SnapManager Backups," on page 299 and in Chapter 13, "Performing Disaster Recovery with SnapManager," on page 223.

Data replication for disaster recovery: When used with SnapMirror, SnapManager provides the ability to automatically replicate databases stored on the source volume to its mirrored target volume situated locally or remotely.

Data replication using SnapManager with SnapMirror is described in Chapter 12, "Using SnapMirror with SnapManager," on page 213 and in Chapter 13, "Performing Disaster Recovery with SnapManager," on page 223.

What SnapManager does not do

SnapManager 3.2 for Microsoft Exchange does not support the following uses:

- SnapManager does not support Microsoft Exchange 5.5.
- SnapManager does not support SnapDrive versions prior to 4.1.
- SnapManager does not create or restore backups of Microsoft Exchange databases that are stored on storage devices that are provided by companies other than NetApp.
- SnapManager does not support Exchange 2003 recovery storage groups.
- SnapManager does not restore Exchange databases to an alternate location.

Where you install and run SnapManager

You can run SnapManager on your Exchange server or on a different Windows host system. When you run SnapManager on a different Windows network host, it is called **SnapManager remote administration**.

Local administration: Typically, you install SnapManager on the same Windows host system as your Exchange server.

System requirements for a SnapManager local administration system are described in "Understanding Windows host system requirements" on page 24.

Remote administration: If you install SnapManager on a computer remote from the Exchange server, you can run SnapManager remotely to perform any task that you can on a locally installed SnapManager system.

System requirements for a SnapManager remote administration system are described in "Requirements for a remote administration server" on page 27.

Remote verification: From a remote administration server that is configured with SnapDrive and Exchange server, you can also perform remote database verification. Remote verification offloads the CPU-intensive database verification operations that can affect the performance of your production Exchange server.

System requirements for a SnapManager remote administration system used for remote verification are described in "Requirements for a remote verification server" on page 27.

The setup and use of a remote verification server is described in Chapter 9, "Backing Up Databases with SnapManager," on page 163.

About the SnapManager graphical user interface

The SnapManager graphical user interface enables you to manage backup and restore operations of Exchange database files and transaction log files on LUNs. The user interface also enables you to schedule backups and verify the integrity of databases in SnapManager backup sets. You can also use the SnapManager user interface to administer SnapManager for Exchange on another Exchange server computer on the network. SnapManager includes the following components.

SnapManager Configuration Wizard: SnapManager Configuration Wizard ensures that Exchange data is migrated correctly for SnapManager to perform backup and restore operations.. It dismounts the databases in an Exchange storage group and moves the database and transaction log files from the Exchange server to the selected LUNs. It then remounts the databases and creates a SnapInfo directory for storing information about backed-up data sets and transaction logs.

For more information, see Chapter 7, "Configuring the Exchange Data for SnapManager," on page 113.

SnapManager Backup: SnapManager Backup enables you to perform and schedule frequent, automatic online full backups. Each SnapManager backup consists of Snapshot copies of the Exchange databases, transaction log files, and the SnapInfo directory.

For more information, see Chapter 9, "Backing Up Databases with SnapManager," on page 163.

SnapManager Restore: SnapManager enables rapid recovery of an Exchange storage group or database. You can select a particular backup, restore your Exchange database using that backup, and then recover the database to its current state by replaying the transaction logs.

For more information, see Chapter 10, "Restoring Databases with SnapManager," on page 183.

SnapManager Reports: Use the SnapManager Reports tab to access the operational reports that SnapManager automatically creates for all log files, database configurations and migrations, deleted Snapshot copies, backups, and restores. A separate report is created for all configuration, backup, restore, and

delete backup operation. Each report is essentially a history file that includes step-by-step details of the operation, the final status of the operation, and error messages for any errors encountered during the operation.

For more information, see Chapter 15, "Managing SnapManager Reports," on page 321.

About the SnapManager command line interface

The SnapManager command line interface enables you to initiate a backup or verification job. The command supports all of the options available through the Backup and Verification tab or the Backup Wizard in the SnapManager graphical user interface.

How you use SnapManager

You can run SnapManager on your Exchange server or on a different computer. When you run SnapManager on a different computer, it is called "SnapManager remote administration". Using a SnapManager remote administration system, you can perform any task you can on a locally installed SnapManager system. When you perform database verification on a remote system, it is referred to as "remote verification".

The following steps describe a typical way to use SnapManager:

- After installing SnapManager, you use SnapManager Configuration Wizard to dismount your Exchange databases and move them to LUNs on a storage system. The Configuration Wizard ensures that your Exchange data is placed correctly.
- After you configure the Exchange data store, you can use SnapManager Backup to create backups of the Exchange data.
- If the need arises, you can use SnapManager Restore to restore your Exchange data (either entire storage groups or individual databases) from one of the backups.
- Using SnapManager's backup facility to initiate SnapMirror through SnapDrive, you can create mirror replications of these databases to be used for various purposes, such as disaster recovery.

How SnapManager works with the other system components

This section describes how SnapManager works with the other system components. See the following topics for more information:

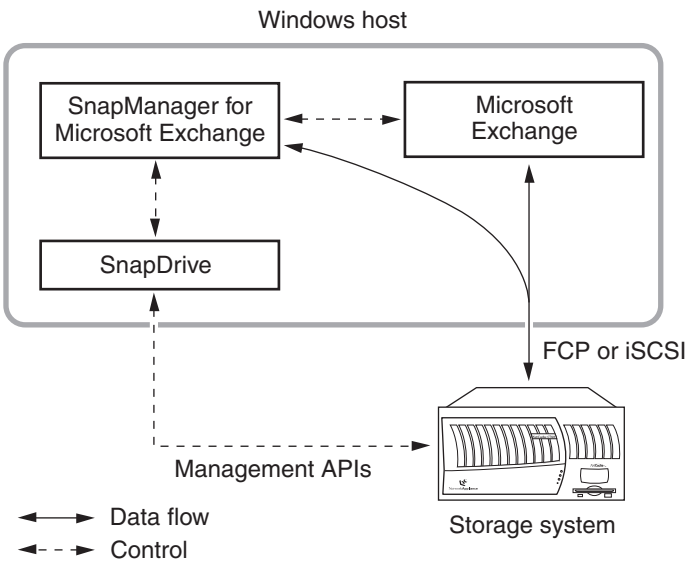
- "System overview" on page 8
- "SnapManager and SnapDrive" on page 9
- "SnapManager and VSS" on page 10
- "SnapManager and Snapshot copies" on page 10

Related topics:

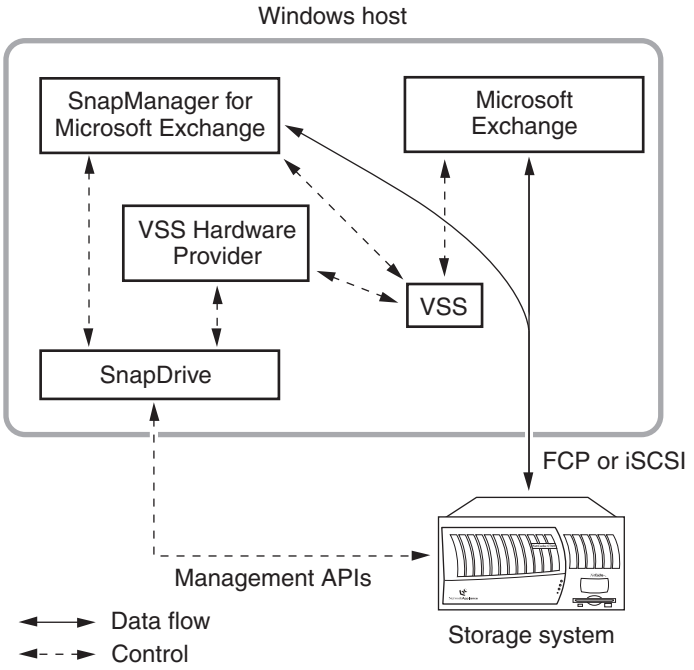
- "SnapManager overview" on page 2
- "How SnapManager works with other backup methods" on page 13

System overview

The following diagrams show how SnapManager interacts with other components of an Exchange installation backed by a NetApp storage system, for the Windows 2000 Server and Windows Server 2003 environments.



SnapManager on Windows 2000 Server



SnapManager on Windows Server 2003

SnapManager and SnapDrive

How SnapManager and SnapDrive work together: SnapManager is an Exchange-aware application that uses the Exchange backup APIs (for Exchange servers running Windows 2000 Server) or VSS (for Exchange servers running Windows Server 2003) to provide backup and restore functionality in an Exchange environment.

SnapDrive integrates with the NTFS Windows file system, Windows Volume Manager, and LUNs to enable the management of storage resources on the storage system in the Windows environment. SnapDrive provides the underlying layer of support for SnapManager.

When to use SnapManager and when to use SnapDrive: You use SnapManager for all backups and related operations. For example, you use SnapManager to establish your Exchange databases on LUNs on a storage system and to back up and restore LUNs on the storage system.

You use SnapDrive only to create and manage the LUNs and storage system volumes that contain your Exchange data and to perform supplemental mirror updates of the transaction log volume when SnapMirror is used.

SnapManager and VSS

What VSS is: Microsoft Volume Shadow Copy Service (VSS) is a new feature of Microsoft Windows Server 2003 that coordinates between data servers, backup applications, and storage management software to support the creation and management of consistent shadow copies, or Snapshot copies. The Data ONTAP VSS Hardware Provider integrates the SnapDrive service and NetApp storage systems running Data ONTAP into the VSS framework. For more information about VSS, see your Data ONTAP VSS Hardware Provider documentation.

How SnapManager uses VSS: In the Windows Server 2003 environment, SnapManager is a VSS requestor, which means that it uses the VSS subsystem to initiate backups.

How you manage VSS Snapshot copies created by SnapManager:

Although SnapManager uses VSS to create Snapshot copies, you manage the resulting Snapshot copies using SnapManager or SnapDrive. You cannot use the VSS administration tool `vssadmin` to manage Snapshot copies created by SnapManager.

Data ONTAP VSS Hardware Provider requirement: Because SnapManager uses VSS to create Snapshot copies on the storage system in the Windows Server 2003 environment, you must have the Data ONTAP VSS Hardware Provider installed for SnapManager to function properly. For more information about the Data ONTAP VSS Hardware Provider, see your Data ONTAP VSS Hardware Provider documentation.

SnapManager and Snapshot copies

About SnapManager and Snapshot copies: A Snapshot copyis a point-in-time, read-only copy of a LUN stored on a storage system volume. SnapManager Backup uses Snapshot functionality to create real-time, online, read-only copies of Exchange databases. A SnapManager backup can consist of several Snapshot copies, depending on how your Exchange data is configured.

Note

You must always use SnapManager to manage SnapManager backups, rather than managing the associated storage system Snapshot copies using SnapDrive, VSS, or storage system administration tools, such as the FilerView® interface.

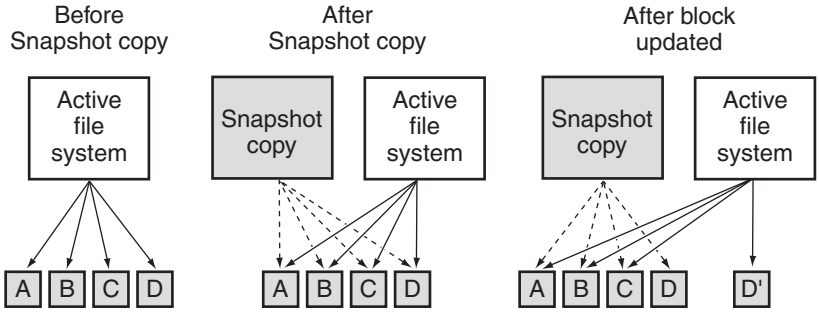
When to use the various Snapshot copy and backup methods: There are multiple ways to take Snapshot copies or backups in an Exchange installation that includes SnapManager. It is important to understand when each of these methods can produce a restorable image and when they cannot.

When one or more Exchange databases are mounted, Snapshot copy-based backups should be performed using only SnapManager. Taking a Snapshot copy of the Exchange databases from the storage system console, FilerView, SnapDrive, or a non-Exchange-aware Windows backup utility results in an inconsistent image of the Exchange database that is unusable for a restore.

The following table illustrates when each of the Snapshot copy or backup methods can create restorable backups.

Tool used to create Snapshot copy or backup	System state		
	Exchange online	All Exchange dbs dismounted	All LUNs disconnected
SnapManager Backup	OK	N/A	N/A
SnapDrive	invalid	OK	N/A
Exchange-aware Windows backup utility	OK (copy backup only)	N/A	N/A
Non-Exchange-aware backup utility	invalid	OK (copy backup only)	N/A
Storage system tools	invalid	invalid	OK

Understanding Snapshot copies: The following figure provides an example of how Snapshot copies work.



Example: Suppose you take a Snapshot copy of a file named file.txt that spans four disk blocks in the active file system. Initially, the Snapshot copy version of file.txt and the version in the active file system are identical: the same blocks on disk store both versions, so the Snapshot copy version of file.txt consumes no additional disk space.

Now suppose that you make a modification to file.txt that affects only one of the four disk blocks. The new data cannot overwrite the original block because that block is needed as part of the Snapshot copy. So the new data is written to a new disk block and the file's inodes are updated accordingly. The active file system inodes now reference the three original disk blocks that have not been touched since the Snapshot copy, plus the one new block. The Snapshot copy inodes still reference the original four blocks.

If you delete file.txt, the blocks holding its data are no longer part of the active file system, but they are still part of the Snapshot copy; deleting file.txt from the active file system does not free any disk space until the Snapshot copy is deleted.

Maximum number of Snapshot copies you can retain: Data ONTAP® software allows a maximum of 255 Snapshot copies per storage system volume. Because SnapManager backups create Snapshot copies, you must delete old SnapManager backups as they are no longer needed to avoid reaching the limit.

Note

The number of Snapshot copies on a volume can be greater than the number of SnapManager backups being retained. For example, if a single volume contains both the SnapInfo directory and the Exchange databases, each SnapManager backup generates two Snapshot copies on that volume.

How SnapManager works with other backup methods

It is best to employ SnapManager technology as a complement to conventional backup processes. See the following topics for more information:

- "SnapManager and your current backup processes" on page 13
- "Type of external backup to use with SnapManager" on page 13
- "Exchange files you should back up using a Windows backup utility" on page 14

Related topics:

- "SnapManager overview" on page 2
- "How SnapManager works with the other system components" on page 8

SnapManager and your current backup processes

SnapManager complements conventional backup processes. For example, SnapManager backups reside on disk. To archive SnapManager backups to another storage medium, such as tape, you use the same tools and processes you currently employ.

However, some backup processes interfere with SnapManager's ability to back up and restore correctly. It is important that you understand which of your current backup tools and processes must be modified or eliminated when you implement SnapManager.

SnapManager backups are not intended to replace periodic disaster recovery measures, such as archiving to tape or other offline media.

Type of external backup to use with SnapManager

Exchange-aware backup tools (such as NTBackup) can create backups of different types. Generally, SnapManager backups replace these backups. However, if you need to create a backup using an Exchange-aware backup tool on a system with SnapManager installed, you must use only a copy or differential backup.

Attention

Using an Exchange backup tool to create a backup of a type other than copy or differential after you implement SnapManager causes your previously created SnapManager backups to become unusable for up-to-the-minute restores.

The following table describes the backup types.

Backup type	Description	Result
Copy	Backs up all selected files; does not clear archive bit	OK SnapManager backups unaffected
Normal (full)	Backs up all selected files and clears archive bit	DO NOT USE Truncates transaction logs; disables SnapManager up-to-the-minute restores
Differential	Backs up all selected files with archive bit set	OK SnapManager backups unaffected
Incremental	Backs up all selected files with archive bit set and clears archive bit	DO NOT USE Truncates transaction logs; disables SnapManager up-to-the-minute restores

Exchange files you should back up using a Windows backup utility

SnapManager does not back up all the files commonly used by an Exchange server. You should use a standard Windows backup utility, such as NTBackup, to back up the following items:

- File systems on hard disks connected to the Exchange server
- Windows registry
- Windows Active Directory
- Internet Information Service (IIS) metabase
- Key Management Service (KMS) database
- Site Replication Services (SRS) database
- System state

Note

You can use NTBackup to back up to a file, instead of using tape, and write or store that file directly on a storage system.

Preparing to Install or Upgrade SnapManager 2

This section describes tasks you need to perform before installing SnapManager 3.2 for Microsoft Exchange or upgrading from a previous version. The following topics are covered:

- "Preinstall or preupgrade procedure" on page 16
- "Backing up system resources and data" on page 18
- "Understanding SnapManager license options" on page 19
- "Understanding SnapManager COM server identity account requirements" on page 20
- "Understanding storage system requirements" on page 22
- "Understanding Windows host system requirements" on page 24

Note

For the most current list of system requirements, see the SnapManager 3.2 for Microsoft Exchange Product Description Page on the NetApp on the Web (NOW) site at http://now.netapp.com/NOW/cgi-bin/software/.

Note

For information about compatible versions of SnapManager, SnapDrive, and Data ONTAP, see the *SnapManager and SnapDrive Compatibility Matrix* on the NOW site at http://now.netapp.com/NOW/knowledge/docs/olio/guides/snapmanager_snapdrive_compatibility/.

Related topics:

- Chapter 1, "Understanding SnapManager," on page 1
- Chapter 3, "Installing or Upgrading SnapManager," on page 29

Preinstall or preupgrade procedure

Before you begin installing or upgrading SnapManager, you must complete the following tasks.

Task	Process
1	Back up system resources and databases, as described in "Backing up system resources and data" on page 18.
2	Determine whether you will be using per-Exchange-server SnapManager licensing or per-storage-system SnapManager licensing. For more information, see "Understanding SnapManager license options" on page 19.
3	Ensure that the SnapManager COM server identity account on *each Exchange server to be used by SnapManager* has Exchange Administrator permissions or greater, as described in "Understanding SnapManager COM server identity account requirements" on page 20. If you need to change an object's permissions, do the following from within the Exchange System Manager: **a.** Right-click the object and select Delegate Control. **b.** In the Exchange Administration Delegation Wizard, change that object's permissions.
4	Configure or upgrade your storage system according to the requirements for SnapManager and SnapDrive, described in "Understanding storage system requirements" on page 22. You might need to install or upgrade any of the following components: ◆ Data ONTAP ◆ iSCSI and/or FCP protocols ◆ SnapManager license ◆ SnapRestore license ◆ SnapMirror license

Task	Process
5	*Upgrading from a previous version of SnapManager.* If you will be upgrading SnapManager and you also upgrade underlying **SnapDrive** or Microsoft **iSCSI initiator** versions, make a note of this now. Later, while preparing to upgrade the SnapManager application (described in "Before you begin the upgrade procedure" on page 49), you must remove the iSCSI dependency with respect to SnapManager.
6	Note whether your storage system has multiple IP addresses.
7	Configure or upgrade your Windows host systems to meet the requirements for SnapDrive and SnapManager, described in "Understanding Windows host system requirements" on page 24. You might need to install, upgrade, or configure the following components: ◆ Microsoft Windows operating system ◆ Microsoft Windows hotfixes ◆ Microsoft Exchange ◆ SnapDrive ◆ SnapDrive preferred IP address (if your storage system has multiple IP addresses) For details, see the *SnapDrive Installation and Administration Guide* for your version of SnapDrive. **Note** If you do not configure a SnapDrive preferred IP address for a storage system that has multiple IP addresses, SnapDrive times out when attempting to create Snapshot copies simultaneously for more than one LUN on a storage system. ◆ Data ONTAP VSS Hardware Provider ◆ iSCSI and/or FCP protocols
8	After you complete these tasks, you are ready to install or upgrade SnapManager. Proceed to "Installing or Upgrading SnapManager" on page 29.

Backing up system resources and data

Before you install SnapManager, you are strongly advised to back up your system resources and data using NTBackup or another industry standard backup utility.

To back up your system resources and data, complete the following steps.

Step	Action
1	Back up the operating system installation on the Exchange server, including the system state.
2	Back up the data on the local drives on the Exchange server.
3	Back up the boot and system drives, and the registry.
4	Use your backup utility to create and maintain a current emergency repair disk (ERD).

Understanding SnapManager license options

You can license SnapManager 3.2 for Microsoft Exchange per Exchange server or on the storage system.

Per-server licensing

A per-server SnapManager license is a 14-character license code for a specific Exchange server.

When you use per-server licensing, no SnapManager license is required on the storage system. Instead, you apply a SnapManager server-side license on the Exchange server. You can specify a server-side license while you are installing SnapManager, or you can defer this activity until after SnapManager has been installed. After SnapManager has been installed, you can apply the license from the About SnapManager dialog box.

Storage system licensing

If a SnapManager license is not enabled on the Exchange server, a seven-character SnapManager license code must be enabled directly on the storage system, using the storage system `license add` command.

If no server license is detected, SnapManager checks the storage system for a SnapManager license whenever a SnapManager operation is initiated. If the SnapManager license is not enabled on the storage system either, the SnapManager operation fails and an error is written to the Windows event log.

Note

With storage system SnapManager licensing, if you use the SnapMirror® software in conjunction with SnapManager, both SnapMirror and SnapManager must be licensed on both the source and target storage systems.

Understanding SnapManager COM server identity account requirements

The COM server identity account used by SnapManager must have proper Exchange permissions for SnapManager to function properly.

Note
SnapManager uses a Windows NT server for fractional space reservation monitoring. That service is configured to run under the local system account.

About the predetermined permission levels for Exchange

There are three predetermined permission levels for Exchange:

- Exchange View Only
- Exchange Administrator
- Exchange Full Administrator

The minimum level required for SnapManager is Exchange Administrator. This requirement can be satisfied using one of these methods:

- Assign Exchange Administrator permissions to the organization object.
- Create an Exchange administrative group and assign the correct permissions to that group.

Note
Right-clicking an object in the Exchange System Manager and selecting Delegate Control opens the Exchange Administration Delegation Wizard, which enables you to change that object's permissions.

About Exchange-specific permission levels

If you require a greater granularity of control for the SnapManager COM server identity account, you can apply Exchange-specific permissions to the object. The minimum Exchange-specific permissions required for SnapManager are as follows:

- Read
- Execute
- Read Permissions
- List Contents
- Read Properties

- Administer Information Store
- View Information Store Status

Note

The user account or group you are configuring must also be a member of the Exchange server's local administrators group.

Understanding storage system requirements

This topic describes the following information:

- "Storage system requirements" on page 22
- "About storage systems that have multiple IP addresses" on page 23

Storage system requirements

To be used with SnapManager, your storage system must meet the following requirements.

Storage system component	Requirements
Data ONTAP	See the SnapDrive software requirements described in the *SnapDrive Installation and Administration Guide* for your version of SnapDrive.
iSCSI or FCP protocols	The appropriate LUN access protocol software must be installed on the storage system that stores the Exchange databases. For more information, see the *SnapDrive Installation and Administration Guide* for your version of SnapDrive.
SnapManager licenses	If SnapManager is licensed per storage system, a SnapManager license is required on the storage system. **Note** With storage system SnapManager licensing, if you use SnapMirror in conjunction with SnapManager, SnapManager must be licensed on both the source and target storage systems.
SnapRestore license	For SnapManager restore operations to work properly, the SnapRestore® feature of SnapDrive must be licensed on the storage system that stores the Exchange databases. For more information, see the *SnapDrive Installation and Administration Guide* for your version of SnapDrive.

Storage system component	Requirements
SnapMirror license	If you plan to use the SnapMirror software in conjunction with SnapManager, a SnapMirror license is required on both the source and target storage systems. For more information, see the *SnapDrive Installation and Administration Guide* for your version of SnapDrive.

About storage systems that have multiple IP addresses

If your storage system has multiple IP addresses, configure the SnapDrive preferred IP address. See the *SnapDrive Installation and Administration Guide* for your version of SnapDrive.

If you do not configure a SnapDrive preferred IP address for a storage system that has multiple IP addresses, SnapDrive times out when attempting to create Snapshot copies simultaneously for more than one LUN on a storage system.

Understanding Windows host system requirements

In the most basic configuration, SnapManager is installed on the same Windows host system as Microsoft Exchange. In addition to this, you can install SnapManager on one or more remote Windows hosts for remote administration of the Exchange computer or for remote verification of the databases contained in SnapManager backup sets.

This topic describes the following information:

- "Windows host system requirements" on page 24
- "Requirements for a remote administration server" on page 27
- "Requirements for a remote verification server" on page 27

Windows host system requirements

To run SnapManager, your system must meet the following requirements.

Windows host component	Requirement if the host system is running Windows 2000 Server	Requirement if the host system is running Windows Server 2003
Operating system	One of the following: ◆ Windows 2000 Server with SP4 ◆ Windows 2000 Advanced Server with SP4	One of the following: ◆ Windows Server 2003 Standard Edition with SP1 ◆ Windows Server 2003 Enterprise Edition with SP1 ◆ Windows Server 2003 Standard Edition R2 ◆ Windows Server 2003 Enterprise Edition R2
Microsoft Windows hotfixes	See the SnapDrive software system requirements.	See the SnapDrive software system requirements.

<table>
<tr><th>Windows host component</th><th>Requirement if the host system is running Windows 2000 Server</th><th>Requirement if the host system is running Windows Server 2003</th></tr>
<tr><td rowspan="2">Microsoft Exchange</td><td>One of the following versions of Microsoft Exchange (Standard or Enterprise Edition):
Exchange 2003 with SP2
Exchange 2003 with SP1
Exchange 2000 with SP3</td><td>One of the following versions of Microsoft Exchange (Standard or Enterprise Edition):
Exchange 2003 with SP2
Exchange 2003 with SP1</td></tr>
<tr><td colspan="2">Note
This requirement does not apply to a remote administration server.

Note
The option to throttle Eseutil.exe database checksum verification (described in “Configuring Eseutil throttling for database verification” on page 348) requires Exchange 2003 with SP2.</td></tr>
<tr><td>SnapDrive</td><td colspan="2">SnapDrive 4.1

If you need to install or upgrade SnapDrive, see the SnapDrive Installation and Administration Guide for detailed instructions.

Note
For a remote administration server, SnapDrive is optional unless you intend to use the remote administration server to remotely administer SnapDrive. For a remote verification server, SnapDrive is required.</td></tr>
</table>

Windows host component	Requirement if the host system is running Windows 2000 Server	Requirement if the host system is running Windows Server 2003
SnapDrive preferred IP address	If your storage system has multiple IP addresses, configure the SnapDrive preferred IP address. See the *SnapDrive Installation and Administration Guide* for your version of SnapDrive. If you do not configure a SnapDrive preferred IP address for a storage system that has multiple IP addresses, SnapDrive times out when attempting to create Snapshot copies simultaneously for more than one LUN on a storage system.	
Data ONTAP VSS Hardware Provider	N/A	Data ONTAP VSS Hardware Provider is included with SnapDrive
iSCSI and/or FCP protocols	The appropriate LUN access protocol software must be installed on the Windows host that runs the Exchange server. See your SnapDrive documentation for complete details about the system requirements: **Note** This requirement does not apply to a remote administration server.	
SnapManager license	If SnapManager is licensed per Exchange server, a SnapManager license is required on the Windows host system. **Note** For per-server SnapManager licensing, you can install SnapManager without specifying a server-side license; after SnapManager has been installed, you can apply the license from the About SnapManager dialog box.	

Requirements for a remote administration server

An Exchange server that is running SnapManager can be remotely administered from another Windows system that is configured as a remote administration server:

- You do not need to install an iSCSI driver or an HBA driver on this system.
- SnapDrive does not need to be installed unless you want to use the remote administration server to remotely administer SnapDrive.
- SnapManager must be installed.

Requirements for a remote verification server

Remote verification is performed using the same mechanisms used for local verification, except that the verification is performed on a host that is different from the Exchange server that initiated the backup. This is the reason that you need SnapDrive and SnapManager installed on your remote verification server, as well as connectivity to the storage system (through FCP or iSCSI).

To run remote verification, your remote Windows system must meet the following requirements:

- SnapDrive must be installed.

  Attention

  Do not try to connect the Exchange server's LUNs to the remote verification server.

- The appropriate LUN driver (iSCSI or FCP) must be installed.
- The remote Windows system must have connectivity (iSCSI or FCP) to the storage system.

  Note

  If you are using iSCSI to connect to the storage system on the remote verification server, an iSCSI connection must be created.

- SnapManager must be installed, but it does not need to be configured. You must specify the user account that you use for the production Exchange server.
- The correct Microsoft Exchange 2000 or 2003 binaries must be installed.

  Microsoft requires that Microsoft Exchange System Management Tools be installed on remote verification machines for licensing compliance.

  To meet the minimum configuration required by SnapManager to run database integrity verification on a remote machine, copy the following files from the `Exchsrvr\bin` directory on your Exchange server to the remote verification server:

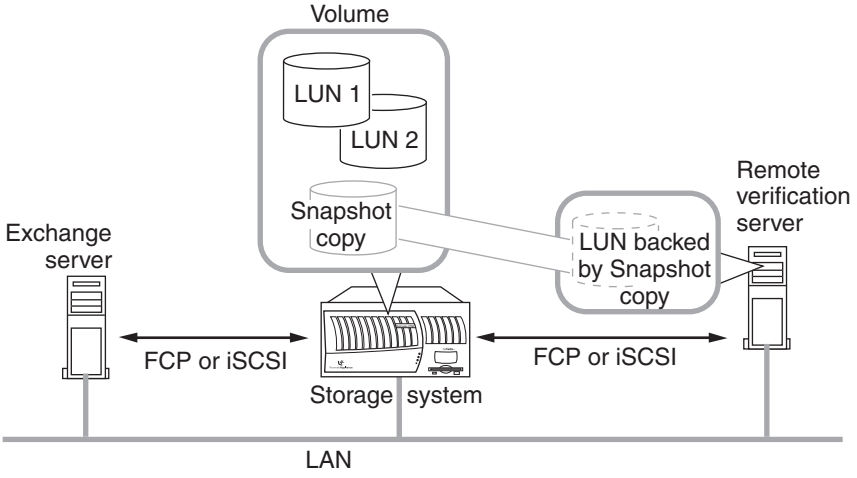
- `eseutil.exe`
- `ese.dll`
- `jcb.dll`
- `exosal.dll`
- `exchmem.dll`

For more information about performing verification on a computer that does not have Exchange installed, see Microsoft KB article 244525.

Note

The version of `eseutil` must match the version of Exchange. When you apply an Exchange service pack to the production server, you *must* copy a new version of `eseutil` at the same time, or else verification cannot function correctly.

The connectivity required to perform remote verification is shown in the following illustration.



Installing or Upgrading SnapManager 3

This section contains the procedures for installing or upgrading to SnapManager 3.2 for Microsoft Exchange as well as procedures for other tasks you might need to use at some point after SnapManager has been installed.

Installing SnapManager 3.2 for Exchange: If you are installing SnapManager for the first time, go to one of the following topics, depending on your target environment:

- "Installing SnapManager on a stand-alone Windows host system" on page 31
- "Installing SnapManager and creating a new Windows cluster" on page 43
- "Installing SnapManager in an existing Windows cluster" on page 46

If an earlier version of SnapManager is currently installed, use the procedure in the following topic:

- "Upgrading to SnapManager 3.2" on page 48

After you install SnapManager 3.2, start the application for the first time as described in Chapter 4, "Starting SnapManager for the First Time," on page 63.

After SnapManager 3.2 for Exchange has been installed or upgraded: Unless it is specified for a particular upgrade path or for a particular troubleshooting situation, you do not need to uninstall SnapManager before reinstalling it or upgrading to a newer version. However, if you need to remove all components of SnapManager, use the procedure in the following topic:

- "Uninstalling SnapManager" on page 55

Attention

If you plan to reinstall SnapManager later, be sure to record the drive letter and path of your current SnapInfo directories. After you reinstall SnapManager, be sure to reconfigure SnapManager to use those same SnapInfo directory locations. This preserves SnapManager's records of backups taken before you uninstalled and reinstalled SnapManager.

If you need to reinstall SnapManager (to fix missing or corrupt files, shortcuts, and registry entries), use the procedure in the following topic:

- "Reinstalling SnapManager" on page 62

Related topics:

- Chapter 1, "Understanding SnapManager," on page 1
- Chapter 2, "Preparing to Install or Upgrade SnapManager," on page 15

- Chapter 4, “Starting SnapManager for the First Time,” on page 63

Installing SnapManager on a stand-alone Windows host system

This section describes how to install SnapManager on a stand-alone Windows host system used for any of the following purposes:

- The production Exchange server
- A remote administration server
- A remote verification server

See the following subtopics for more information:

- "Comparison of the two installation modes" on page 32
- "Installing in interactive mode" on page 33
- "Installing in unattended mode" on page 38

Note

Other topics in this section that describe how to install SnapManager for various configurations refer to this topic for some of the detailed installation steps.

Related topics:

- "Installing SnapManager and creating a new Windows cluster" on page 43
- "Installing SnapManager in an existing Windows cluster" on page 46
- "Upgrading to SnapManager 3.2" on page 48
- "Upgrading to SnapManager 3.2" on page 48
- "Uninstalling SnapManager" on page 55
- "Reinstalling SnapManager" on page 62

Comparison of the two installation modes

The software installation utility for SnapManager can be run in either interactive mode or unattended mode. These two modes are described in the following table.

Feature	SnapManager installation mode	
	Interactive	**Unattended**
Access	Require user interaction and access to the graphical user interface	Allows automated installation by executing a script or command line command
Minimum required input	◆ Acceptance of the terms of the license agreement ◆ SnapManager server account ❖ User name ❖ Password	
Optional input	◆ User name ◆ Organization name ◆ SnapManager server-side license key ◆ SnapManager installation directory	
SnapManager software license agreement	Displayed in the installation utility	Displayed at the command line if you pass a specific parameter to the installation utility
After the installation finishes	If a system reboot is required to activate new software, a dialog box appears and prompts you to choose whether you want to reboot the target system.	If a system reboot is required to activate new software, a dialog box appears and prompts you to choose whether you want to reboot the target system. You can override this default behavior by including an optional command line parameter.

Installing in interactive mode

To install SnapManager using the software installation utility in interactive mode, complete the following steps.

Step	Action
1	Install the software from the CD-ROM that came packaged with your media kit or download it. **Attention** Do not use Terminal Services for any type of SnapManager administration, because you might miss critical information that is displayed only in pop-up boxes at the system console. **Note** You do not need to stop Exchange services while you install SnapManager 3.2 for Microsoft Exchange. Exchange can continue to run while you install SnapManager and afterward.

If...	Then...
You are obtaining the software from the network	Download the SnapManager package from the network, save it on the Windows host system, and then launch the SnapManager installation package by double-clicking it in your Windows Explorer screen. **Result:** The software installation utility starts and opens to the Welcome screen.
You are installing the software from CD-ROM	Browse to the SnapManager installation package and double-click `setup.exe`. **Result:** The software installation utility starts and opens to the Welcome screen.

Step	Action
Welcome	
2	In the Welcome screen, click Next. **Result:** The License Agreement screen appears.
License agreement	
3	Read the license agreement. If you accept the terms of the agreement, select the “I accept....” option and then click Next. **Result:** The Customer Information screen appears.

Step	Action
Customer information	
4	In the Customer Information screen, specify the user name, the organization name, and the SnapManager license type. **a.** In the User Name box, enter your user name. **b.** In the Organization box, enter your organization name. **c.** In the License Type option, select your SnapManager license type. If you have a **storage-system-side license** for SnapManager, select Per Filer, and be sure that the SnapManager system-side license is enabled on the storage system. If you have an **Exchange-server-side license** for SnapManager, select Per Server. **d.** If you selected the Per Server license type, use the License Key box to enter the license key for your server-side license. If you do not have a license key, you can leave the License Key box empty for now and enter your server-side license key later from the SnapManager interface. To do this, first go to the menu bar and select Help > About to open the About SnapManager dialog box. From that dialog box, click Update License to open the Update Server-Side License dialog box and specify your license key.
5	Click Next. **Result:** The Destination Folder screen appears.

Step	Action
Destination folder	
6	Note the full path of the folder in which SnapManager will be installed. The default installation directory for SnapManager 3.2 for Microsoft Exchange is as follows: `C:\Program Files\NetApp\SnapManager for Exchange\` **Note** SnapManager 3.2 for Microsoft Exchange is installed in a different directory than previous releases of SnapManager.
7	Optional. If you want to install SnapManager in a directory other than the default installation directory, do the following: **a.** Click Change to open the Change Current Destination Folder dialog box. **b.** Browse to an alternate installation directory. **c.** Click OK to close the dialog box. The Destination Folder screen displays the new specified installation directory path. **d.** Record the newly specified installation directory path.
8	Click Next. **Result:** The SnapManager Server Identity screen appears.

Step	Action
SnapManager server identity	
9	In the Account box of the SnapManager Server Identity screen, specify the user account you want to use to run SnapManager. This account must meet the following requirements: ◆ The account must have administrator privileges on the Exchange server. ◆ The account must also have system administrator server privileges. **Note** This account must have the required permissions. For details, see "Understanding SnapManager COM server identity account requirements" on page 20. If SnapDrive is installed and configured, the text box is prepopulated with the account that SnapDrive is configured for. Otherwise, browse to locate and select the account name. The user account name is specified in either of the following formats: ◆ *DomainName\UserName* ◆ *UserName@DomainName*
10	In the Password box and in the Confirm Password box, enter the user password.
11	Click Next. **Result:** The Ready to Install the Program screen appears. All of the installation specifications are complete.
Ready to install the program	
12	Optional. Review or change your current installation specifications before proceeding by clicking Back.

Step	Action
13	To proceed with the installation using your current specifications, click Install. **Result:** The installation process begins, and the Installing SnapManager for Exchange screen appears. The screen displays the progress of the installation process.
Installing SnapManager for Exchange	
14	Wait until the InstallShield Wizard Completed screen appears; then click Finish to exit the software installation utility.
15	Proceed to Chapter 4, "Starting SnapManager for the First Time," on page 63.

Installing in unattended mode

This topic describes how to install SnapManager by running the software installation utility from a command line. This enables you to install the SnapManager software under the control of a script for an unattended installation.

How to invoke the software installation utility: The command name you specify depends on the SnapManager installation media you will be accessing.

SnapManager installation media	Application name to be run
Software CD	`setup.exe` (located on the CD-ROM)
Software package downloaded from the network	`SME3.2.exe` (the name of the software package itself)

How to display the software license agreement: To display the SnapManager software license agreement, enter the following command either directly at the command line or through a script:

CommandName `/v"SHOWEULA=Yes /qb"`

where *CommandName* is either `setup.exe` or `SME3.2.exe`, depending on the SnapManager installation media being used.

Note

The SHOWEULA=Yes command argument cannot be used in combination with other command line arguments.

How to start the unattended installation: To install SnapManager in unattended mode, enter the following command either directly at the command line or through a script:

CommandName /v"[AGREETOLICENSE={Yes|No}] [USERNAME=*UserName*] [COMPANYNAME=*CompanyName*] [ISX_SERIALNUM=*LicenseKey*] [INSTALLDIR=*InstallationDirectory*] SVCUSERNAME=*Domain\UserName* SVCUSERPASSWORD=*Password* SVCCONFIRMUSERPASSWORD=*PassWord* [REBOOT=0] [/L* *TempDirPath\LogFileName*] /qb"

The following table describes each of the parameters.

Command or Parameter	Description
CommandName	Either setup.exe or SME3.2.exe, depending on the SnapManager installation media being used.
AGREETOLICENSE={Yes|No}	Set this parameter to Yes only if you have read and accept the terms of the SnapManager software license agreement. The installation will not proceed unless you specify this parameter with a value of Yes. If not specified, the default value No is used, and the installation will not proceed.
USERNAME=*UserName*	Optional. If not specified, the default value is retrieved from the registry.
COMPANYNAME=*CompanyName*	Optional. If not specified, the default value is retrieved from the registry.
ISX_SERIALNUM=*LicenseKey*	Optional. Only used to specify an Exchange server-side license for SnapManager.

Command or Parameter	Description
INSTALLDIR=*InstallationDirectory*	Optional. If not specified, the default installation directory is used: `C:\Program Files\NetApp\SnapManager for Exchange\`
SVCUSERNAME=*Domain\UserName*	The account from which SnapManager is to be run. See "Understanding SnapManager COM server identity account requirements" on page 20.
SVCUSERPASSWORD=*Password*	
SVCCONFIRMUSERPASSWORD=*Password*	
REBOOT=0	Optional. After the installation finishes, the installation utility automatically reboots the Windows host system if that is required to activate updated software. If you specify this option, however, the system will not be rebooted.

Command or Parameter	Description
`/L*` *TempDirPath\LogFileName*	Optional. If you specify this option, detailed information about the installation will be written to the specified log file. This information can be used to investigate details about how a particular instance of SnapManager for Microsoft Exchange is installed. The asterisk ("`*`") is a wildcard character that specifies that all of the installation information (such as status messages, nonfatal warnings, and error messages) is to be logged. *TempDirPath* is the fully qualified name of the directory in which the installation log will be created or overwritten. *LogFileName* is the name of the file to which the installation information will be written.

Examples: Consider the following two scenarios.

Installation Details	Scenario 1	Scenario 2
Installation media to be used	CD inserted into the CD-ROM drive on `E:\`	Installation package downloaded to `C:\NetApp\downloads\`
Server account to be specified	Account user name: `MKTG2\Administrator` Account password: `STeeL`	
SnapManager license	Filer-side	Server-side (license key `ABCDEFGHIJKLMN`)

For scenario 1, you would enter the following at the command line or from a script:

```
E:\setup.exe /v"AGREETOLICENSE=Yes
SVCUSERNAME=MKTG2\Administrator SVCUSERPASSWORD=STeeL
SVCCONFIRMUSERPASSWORD=STeeL /qb"
```

For scenario 2, you would enter the following at the command line or from a script:

```
C:\NetApp\downloads\SME3.2.exe /v"AGREETOLICENSE=Yes
SVCUSERNAME=MKTG2\Administrator SVCUSERPASSWORD=STeeL
SVCCONFIRMUSERPASSWORD=STeeL ISX_SERIALNUM=ABCDEFGHIJKLMN /qb"
```

General procedure: To install SnapManager using the software installation utility in unattended mode, complete the following steps.

Step	Action
1	Access the command line of the target host system. **Note** You do not need to stop the Exchange service when you install SnapManager 3.2 for Microsoft Exchange. Exchange can continue to run while you install SnapManager and afterward.
2	At the command line, enter either the command string or the name of the script that executes the command string. **Result:** The software installation utility installs the SnapManager for Microsoft Exchange software in the specified directory. If the `INSTALLDIR` parameter is not specified, the utility installs the software in the default directory `C:\Program Files\NetApp\SnapManager for Exchange\`.
3	Proceed to Chapter 4, "Starting SnapManager for the First Time," on page 63.

Installing SnapManager and creating a new Windows cluster

This topic describes how to install and configure SnapManager 3.2 for Microsoft Exchange during the process of creating a new Windows cluster. See the following subtopics for more information:

- "About Active/Passive configurations" on page 43
- "About Active/Active configurations" on page 43
- "Installing SnapManager in a new Windows cluster" on page 44

Related topics:

- "Installing SnapManager on a stand-alone Windows host system" on page 31
- "Installing SnapManager in an existing Windows cluster" on page 46
- "Upgrading to SnapManager 3.2" on page 48
- "Uninstalling SnapManager" on page 55
- "Reinstalling SnapManager" on page 62

About Active/Passive configurations

In an Active/Passive Exchange cluster, there are two to four clustered nodes and one virtual Exchange server. If the node running Exchange fails, the cluster transfers the virtual Exchange server to the other node, which takes over the disks previously used by the partner node.

For an Active/Passive Exchange cluster, assuming that your Exchange data is on a shared resource, your disk requirements are the same as for a stand-alone Exchange system, with the addition of one LUN for the quorum disk.

Note

The Active/Passive configuration is recommended by Microsoft to avoid performance degradation if a node fails.

About Active/Active configurations

In an Active/Active two-node configuration, there are two clustered nodes and an Exchange virtual server running on each node. If one node fails, the other node takes over the virtual server running on the failed node.

Because both nodes need to be able to run an active Exchange instance, each node requires its own disks, as if it were a self-contained stand-alone system. In addition, one extra LUN is needed for the quorum disk.

Note

Exchange 2000 does not support more than two active nodes in the same cluster.

Installing SnapManager in a new Windows cluster

The procedure for installing SnapManager 3.2 for Microsoft Exchange in a new Windows cluster assumes the following facts:

- You have two to four systems that you are ready to configure into a Windows cluster.
- Microsoft Exchange is not installed on either system.
- You will use a LUN as the quorum disk.

To create the cluster and install and configure SnapManager 3.2 for Microsoft Exchange as part of the cluster, complete the following steps.

Step	Action
1	Create the cluster by following the procedure in your SnapDrive documentation for creating a Windows cluster with a virtual quorum disk.
2	Install and configure Exchange on one node; then install Exchange on the remaining nodes. **Note** Exchange virtual servers are not created during this step. See the Microsoft documentation for information about installing Exchange in a cluster. You do not have to use the default cluster group, but whatever group you use must contain an IP address resource, a network name resource, and at least one physical disk cluster resource (LUN).

Step	Action
3	Using Cluster Administrator, create an Exchange System Attendant Resource in the cluster group where the LUN physical disk resources that store the Exchange databases and transaction logs will reside. **Note** Do this from the node that owns the cluster group containing the LUN physical disk resources. During this step you are prompted for an Exchange data directory. This directory is also where the Exchange system files are placed. You can accept the default location now; these system files can be moved in a later step, if necessary, using the Configuration Wizard. Specify the LUN physical disk resources and the Network Name resource as dependencies for the Exchange System Attendant Resource. **Result:** The required Exchange cluster resources are created.
4	Bring the cluster group online if it is not already, and verify that the Exchange cluster is functioning correctly by moving the cluster group containing the newly created Exchange virtual server to the other node and back.
5	Install SnapManager on all nodes, starting with the node that currently owns the cluster resources. You can install SnapManager in interactive mode or in unattended mode. Procedures for both installation modes are described in "Installing SnapManager on a stand-alone Windows host system" on page 31.
6	Proceed to Chapter 4, "Starting SnapManager for the First Time," on page 63.

Installing SnapManager in an existing Windows cluster

This topic describes how to install and configure SnapManager 3.2 for Microsoft Exchange in an existing Windows cluster.

Related topics:

- "Installing SnapManager on a stand-alone Windows host system" on page 31
- "Installing SnapManager and creating a new Windows cluster" on page 43
- "Upgrading to SnapManager 3.2" on page 48
- "Uninstalling SnapManager" on page 55
- "Reinstalling SnapManager" on page 62

To install and configure SnapManager 3.2 for Microsoft Exchange in an existing Windows cluster, complete the following steps.

Note

Before you complete these steps, make sure that you have prepared your system and environment as described in "Preinstall or preupgrade procedure" on page 16.

Step	Action
1	Verify that the Exchange virtual servers and the cluster services are functioning properly by moving the Exchange virtual server from one cluster node to the other and back. If any errors occur, or if any of the cluster resources do not start properly, resolve the issue before continuing.
2	Install or upgrade SnapDrive as required. For details, see your SnapDrive documentation.

Step	Action
3	*From the node that owns the cluster group that contains the Exchange virtual server*, create the shared LUNs to hold the Exchange databases and transaction log files, according to your SnapManager data configuration plan. For details, see your SnapDrive documentation. **Note** These shared LUNs must be physical disk resources in the cluster group that contains the Exchange virtual server that uses them.
4	Verify that the System Attendant Resource dependencies are set correctly. The System Attendant Resource must depend on all the LUN physical disk resources and the Network Name resource in this cluster group.
5	Verify that the Exchange virtual servers and the cluster services are functioning correctly by moving the cluster group containing the newly created Exchange virtual server to the other node and back.
6	Install SnapManager on all nodes, starting with the node that currently owns the cluster resources. Use either the interactive installation procedure or the unattended installation procedure for a stand-alone Windows host system. Both procedures are described in “Installing SnapManager on a stand-alone Windows host system” on page 31.
7	Proceed to Chapter 4, “Starting SnapManager for the First Time,” on page 63.

Upgrading to SnapManager 3.2

You can upgrade to SnapManager 3.2 for Microsoft Exchange from the following older versions of SnapManager:

- SnapManager 3.1.1 for Microsoft Exchange
- SnapManager 3.1 for Microsoft Exchange
- SnapManager 3.0 for Microsoft Exchange
- SnapManager for Microsoft Exchange 2000 v1.1.*x*
- SnapManager for Microsoft Exchange 2000 v1.0

This topic contains the following information:

- "Before you begin the upgrade procedure" on page 49
- "Comparison of the two upgrade modes" on page 50
- "Upgrading in interactive mode" on page 51
- "Upgrading in unattended mode" on page 52

Related topics:

- "Installing SnapManager on a stand-alone Windows host system" on page 31
- "Installing SnapManager and creating a new Windows cluster" on page 43
- "Installing SnapManager in an existing Windows cluster" on page 46
- "Uninstalling SnapManager" on page 55
- "Reinstalling SnapManager" on page 62
- "Migrating an existing SnapManager for Exchange configuration from using drive letters to using mount points" on page 130

Before you begin the upgrade procedure

Before beginning the upgrade procedure, complete the following steps.

Step	Action
1	If you have not already done so, prepare your target system and environment as described in "Preinstall or preupgrade procedure" on page 16. This procedure consists of the following tasks: ◆ "Backing up system resources and data" on page 18 ◆ "Understanding SnapManager license options" on page 19 ◆ "Understanding SnapManager COM server identity account requirements" on page 20 ◆ "Understanding storage system requirements" on page 22 ◆ "Understanding Windows host system requirements" on page 24 **Note** If you need to interrupt connectivity to the Exchange data when upgrading other components, such as storage systems or connection protocols, take Exchange offline. However, you do not need to stop Exchange services while you upgrade SnapManager; Exchange can continue to run while you upgrade SnapManager.
2	If you upgraded underlying **SnapDrive** or Microsoft **iSCSI initiator** versions to prepare your storage system for upgrading SnapManager, remove the iSCSI dependency with respect to SnapManager during the SnapManager upgrade process. There are two ways to do this: ◆ Run the SnapManager Configuration Wizard and use the Add Microsoft iSCSI Service Dependency screen to remove this dependency. ◆ Stop the Microsoft Exchange System Attendant resource service. Later, after you finish upgrading the SnapManager application, you can restore the dependency.

Step	Action	
3	Prepare the existing SnapManager application.	
	If you are upgrading from...	**Then do this...**
	SnapManager 3.1.1 for Exchange	Exit SnapManager.
	SnapManager 3.1 for Exchange	Exit SnapManager.
	SnapManager 3.0 for Exchange	Exit SnapManager.
	SnapManager for Exchange 2000 v1.1.*x*	Exit SnapManager.
	SnapManager for Exchange 2000 v1.0	Uninstall SnapManager. For details, see "Uninstalling SnapManager" on page 55.
	Note You do not need to stop Exchange services while you upgrade SnapManager; Exchange can continue to run while you upgrade SnapManager.	

Comparison of the two upgrade modes

The software installation utility for SnapManager can be run in either interactive mode or unattended mode. These two modes are described in the following table.

Comparison	SnapManager Upgrade Mode	
	Interactive	**Unattended**
Access	Require user interaction and access to the graphical user interface	Allows automated upgrade by executing a script or command line command
SnapManager software license agreement	Displayed in the software installation utility.	Displayed at the command line if you pass a specific parameter to the installation utility.

Upgrading in interactive mode

To upgrade SnapManager using the software installation utility in interactive mode, complete the following steps.

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td>1</td><td colspan="2">Upgrade to SnapManager 3.2 for Microsoft Exchange by installing the new product.</td></tr>
<tr><td></td><td>If the target system is...</td><td>Then use this procedure...</td></tr>
<tr><td></td><td>A stand-alone Windows host system</td><td>“Installing SnapManager on a stand-alone Windows host system” on page 31</td></tr>
<tr><td></td><td>A new Windows cluster</td><td>“Installing SnapManager and creating a new Windows cluster” on page 43</td></tr>
<tr><td></td><td>An existing Windows cluster</td><td>“Installing SnapManager in an existing Windows cluster” on page 46</td></tr>
<tr><td></td><td colspan="2">Note
When you run the SnapManager installation utility as a part an upgrade, you are asked whether you want to retain your current installation directory. If you change your installation directory, it could cause existing scripts that rely on the SnapManager installation directory path to fail.</td></tr>
<tr><td>2</td><td colspan="2">After upgrading to SnapManager by following one of the installation procedures, proceed to Chapter 4, “Starting SnapManager for the First Time,” on page 63.</td></tr>
</table>

Upgrading in unattended mode

This topic describes how to upgrade SnapManager by running the software installation utility from a command line. This enables you to upgrade the SnapManager software under the control of a script for an unattended upgrade.

How to invoke the software installation utility: The command name you specify depends on the SnapManager installation media you will be accessing.

SnapManager installation media	Application name to be run
Software CD	`setup.exe` (located on the CD-ROM)
Software package downloaded from the network	`SME3.2.exe` (the name of the software package itself)

How to start the unattended installation: To install SnapManager in unattended mode, enter the following command either directly at the command line or through a script:

CommandName /v"REINSTALLMODE=vomus REINSTALL=ALL [/L* *TempDirPath\LogFileName*] /qb"

The following table describes each of the parameters.

Command or parameter	Description
CommandName	Either `setup.exe` or `SME3.2.exe`, depending on the SnapManager installation media being used.
`REINSTALLMODE=vomus`	Causes the software installation utility to recache the new software package.
`REINSTALL=ALL`	Causes the software installation utility to update all the software components.

Command or parameter	Description
`/L*` *TempDirPath\LogFileName*	Optional. If you specify this option, detailed information about the installation will be written to the specified log file. This information can be used to investigate details about how a particular instance of SnapManager for Microsoft Exchange is installed. The asterisk ("*") is a wildcard character that specifies that all of the installation information (such as status messages, nonfatal warnings, and error messages) should be logged. *TempDirPath* is the fully qualified name of the directory in which the installation log will be created or overwritten. *LogFileName* is the name of the file to which the installation information will be written.

Examples: Consider the following two scenarios:

- For scenario 1, assume that you are installing from a CD inserted into the CD-ROM drive on `E:\`. In this case, you would enter the following at the command line:

  ```
  E:\setup.exe /v"REINSTALLMODE=vomus REINSTALL=ALL /qb"
  ```

- For scenario 2, assume that you are upgrading from the installation package downloaded to `C:\NetApp\downloads\`. In this case, you would enter the following at the command line:

  ```
  C:\NetApp\downloads\SME3.2.exe /v"REINSTALLMODE=vomus
  REINSTALL=ALL /qb"
  ```

General procedure: To install SnapManager using the software installation utility in unattended mode, complete the following steps.

Step	Action
1	Access the command line of the target host system.
2	Exit SnapManager, if you have not already done so. **Note** You do not need to stop Exchange services before or during the SnapManager software upgrade process.
3	At the command line, either enter the command string or enter the name of the script that executes the command string. **Result:** The software installation utility installs the SnapManager for Microsoft Exchange software.
4	Proceed to Chapter 4, “Starting SnapManager for the First Time,” on page 63.

Uninstalling SnapManager

This topic describes how to uninstall the SnapManager software. See the following topics for more information:

- "Before you uninstall SnapManager" on page 55
- "Comparison of the two uninstallation modes" on page 57
- "Uninstalling SnapManager in interactive mode" on page 57
- "Uninstalling SnapManager in unattended mode" on page 59

Attention

Do not attempt to remove a currently installed version of SnapManager using a method other than the approach described here. To do so could cause system problems resulting from unknown remaining files.

Note

Unless it is specified for a particular upgrade path or for a particular troubleshooting situation, you do not need to uninstall SnapManager before reinstalling it or upgrading to a newer version.

Related topics:

- "Installing SnapManager on a stand-alone Windows host system" on page 31
- "Installing SnapManager and creating a new Windows cluster" on page 43
- "Installing SnapManager in an existing Windows cluster" on page 46
- "Upgrading to SnapManager 3.2" on page 48
- "Reinstalling SnapManager" on page 62

Before you uninstall SnapManager

If you have used SnapManager to manage your Exchange databases and **you plan to reinstall** SnapManager later, be sure to **record the drive letter and path** of the SnapInfo directory locations **before you uninstall** SnapManager.

Single SnapInfo directory: If you have set up a single SnapInfo directory for all databases on this host, then record the drive letter and path of the LUN that contains a single SnapInfo directory for all Exchange servers and their associated databases.

Multiple SnapInfo directories: If you have set up multiple SnapInfo directories, then then record the drive letter and path of each LUN that contains a SnapInfo directory.

SnapManager Reports records the current SnapInfo directory locations in the most recent logs contained in the **Backup folder** and in the **Config folder**.

After you reinstall SnapManager, be sure to reconfigure SnapManager with **the same** SnapInfo directory locations that were used by SnapManager previously.

Attention

If you configure SnapManager with **different** SnapInfo directory locations than used previously, then SnapManager will no longer have records of any backups taken before the reinstallation of SnapManager occurred. As a result, your prior backup sets could be invalidated or deleted the next time you perform a backup operation.

Optional. Move Exchange data to a local disk: If you want to move your Exchange data store from the storage system back to a local disk, complete the following steps.

Step	Action
1	Use Exchange System Manager to move your databases, transaction logs, and system files from the LUNs onto a local disk with enough space to hold them.
2	Confirm that the data was moved correctly and that your Exchange server is functioning normally.
3	Disconnect or delete your LUNs from your SnapManager host. For information about disconnecting or deleting LUNs, see your SnapDrive documentation.

Comparison of the two uninstallation modes

The software installation utility for SnapManager can be run in either interactive mode or unattended mode. These two modes are described in the following table.

Comparison	SnapManager Uninstallation Mode	
	Interactive	**Unattended**
Access	Require user interaction and access to the graphical user interface	Allows automated uninstallation by executing a script or command line command
Tool used	The Windows utility Add or Remove Programs (in the Control Panel)	The software installation utility for SnapManager for Microsoft Exchange
Options	You can also remove the Report directory.	

Uninstalling SnapManager in interactive mode

To uninstall SnapManager for Microsoft Exchange and all its components by using the Windows Add or Remove Programs utility, complete the following steps.

Note

You can also uninstall SnapManager in unattended mode, as described in "Uninstalling SnapManager in unattended mode" on page 59. For a comparison of the two uninstallation modes, see "Comparison of the two uninstallation modes" on page 57.

Step	Action
1	If SnapManager is running, close it. **Note** You do not need to stop the Exchange service or remove the Exchange databases from the LUNs before you uninstall SnapManager for Exchange will continue to run during the uninstallation process and after the uninstallation is completed.

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td>2</td><td colspan="2">In the Windows 2000 Server or Windows Server 2003 Control Panel, select Add or Remove Programs, and then select the entry for SnapManager for Microsoft Exchange.

Result: Both a Change button and a Remove button appear in that entry.</td></tr>
<tr><td rowspan="3">3</td><td colspan="2">Click one of the buttons, depending to what you want to remove.</td></tr>
<tr><td>If...</td><td>Then...</td></tr>
<tr><td>You only want to remove the SnapManager software and leave the Report folder</td><td>Click Remove.</td></tr>
<tr><td>You want to remove both the SnapManager software and the Report folder</td><td>Do not click Remove. Instead, do the following:

a. Click Change.

b. Select the Remove Reports option.

c. Click Remove.</td></tr>
<tr><td>4</td><td colspan="2">At the prompt, click Yes to proceed with removing the SnapManager software.</td></tr>
<tr><td>5</td><td colspan="2">After the utility finishes removing SnapManager from your computer, close the Add or Remove Programs utility and then close the Control Panel.</td></tr>
</table>

Note

In a cluster configuration, be sure to uninstall SnapManager from all nodes of the cluster.

Uninstalling SnapManager in unattended mode

This topic describes how to uninstall SnapManager using the software installation utility in unattended mode. This enables you to uninstall SnapManager under the control of a script for an unattended uninstallation.

Note

You can also uninstall SnapManager in unattended mode, as described in "Uninstalling SnapManager in interactive mode" on page 57. For a comparison of the two uninstallation modes, see "Comparison of the two uninstallation modes" on page 57.

How to invoke the software installation utility: The command name you specify depends on the SnapManager installation media you will be accessing.

SnapManager installation media	Application name to be run
Software CD	`setup.exe` (located on the CD-ROM)
Software package downloaded from the network	`SME3.2.exe` (the name of the software package itself)

What to specify in the command line: To install SnapManager in unattended mode, enter the following command either directly at the command line or through a script:

CommandName /v"REMOVE=ALL [REMOVEREPORTFOLDER=1] [/L* *TempDirPath\LogFileName*] /qb"

The following table describes each of the parameters.

Command or parameter	Description
CommandName	Either `setup.exe` or `SME3.2.exe`, depending on the SnapManager installation media being used.
`REMOVE=ALL`	Causes the software installation utility to remove SnapManager (as if you selected the Remove option in the Program Maintenance screen).

Command or parameter	Description
`REMOVEREPORTFOLDER=1`	Optional. Causes the software installation utility to remove the Report folder (as if you selected the Remove Report Folder option in the Remove the Program screen).
`/L*` *TempDirPath\LogFileName*	Optional. If you specify this option, detailed information about the installation will be written to the specified log file. This information can be used to investigate details about how a particular instance of SnapManager for Microsoft Exchange is installed. The asterisk ("*") is a wildcard character that specifies that all of the installation information (such as status messages, nonfatal warnings, and error messages) should be logged. *TempDirPath* is the fully qualified name of the directory in which the installation log will be created or overwritten. *LogFileName* is the name of the file to which the installation information will be written.

Examples: Consider the following two scenarios.

Installation details	Scenario 1	Scenario 2
Installation media to be used	CD inserted into the CD-ROM drive on `E:\`	Installation package downloaded to `C:\NetApp\downloads\`
SnapManager license	Filer-sidelicense	Server-side license (key `ABCDEFGHJIJKLMN`)

For scenario 1, enter the following at the command line:

```
E:\setup.exe /v"REMOVE=ALL /qb"
```

For scenario 2, enter the following at the command line:

```
C:\NetApp\downloads\SME3.2.exe /v"REMOVE=ALL
REMOVEREPORTFOLDER=1 /qb"
```

General procedure: To install SnapManager using the software installation utility in unattended mode, complete the following steps.

Step	Action
1	Access the command line of the target host system.
2	At the command line, either enter the command string or enter the name of the script that executes the command string. **Result:** The software installation utility upgrades the SnapManager for Microsoft Exchange software.
3	Proceed to Chapter 4, "Starting SnapManager for the First Time," on page 63.

Note

In a cluster configuration, be sure to uninstall SnapManager from all nodes of the cluster.

Reinstalling SnapManager

You can reinstall the same version of SnapManager on a Windows host system. This option repairs missing or corrupt files, shortcuts, and registry entries.

Note

You do not need to stop Exchange services before or during the SnapManager software reinstallation process.

Unless it is specified for a particular upgrade path or for a particular troubleshooting situation, you do not need to uninstall SnapManager before reinstalling it or upgrading to a newer version.

If you uninstalled SnapManager: If you uninstalled SnapManager, then the reinstallation procedure is identical to a new installation of the software. For installation instructions, see the following topics:

- "Installing SnapManager on a stand-alone Windows host system" on page 31
- "Installing SnapManager in an existing Windows cluster" on page 46

If you had used SnapManager to manage your Exchange databases before you uninstalled the SnapManager application, then be sure to configure SnapManager with **the same** SnapInfo directory location or locations that were used by SnapManager prior to the reinstallation.

Attention

If you configure SnapManager with **different** SnapInfo directory locations than used previously, then SnapManager will no longer have records of any backups taken before the reinstallation of SnapManager occurred.

For more information, see "Uninstalling SnapManager" on page 55.

If you did not uninstall SnapManager: See "Upgrading to SnapManager 3.2" on page 48.

Starting SnapManager for the First Time 4

After you have installed or upgraded to SnapManager 3.2, start the application for the first time, as described in this section:

- "Starting SnapManager and connecting to the default server" on page 64
- "What to do next" on page 69

Attention

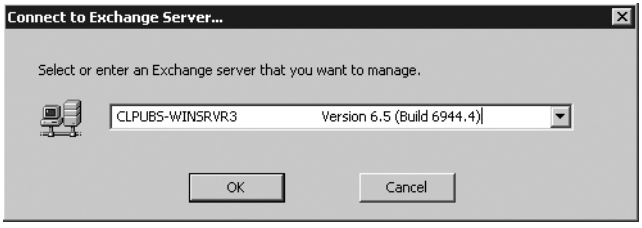
You must run SnapManager from the system console, not from a Terminal Services client. Do not use Terminal Services for any type of SnapManager administration, because you might miss critical information that is displayed only in pop-up boxes at the system console.

Related topics:

- Chapter 5, "Determining the Number of LUNs Required," on page 71
- Chapter 6, "Creating Storage System Volumes and LUNs," on page 93
- Chapter 7, "Configuring the Exchange Data for SnapManager," on page 113

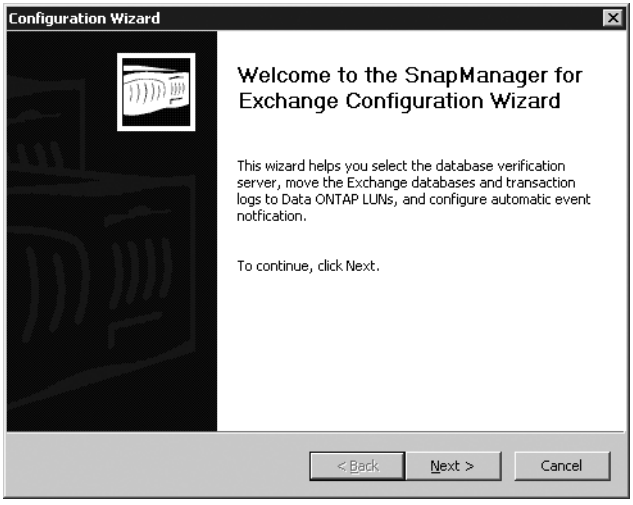
Starting SnapManager and connecting to the default server

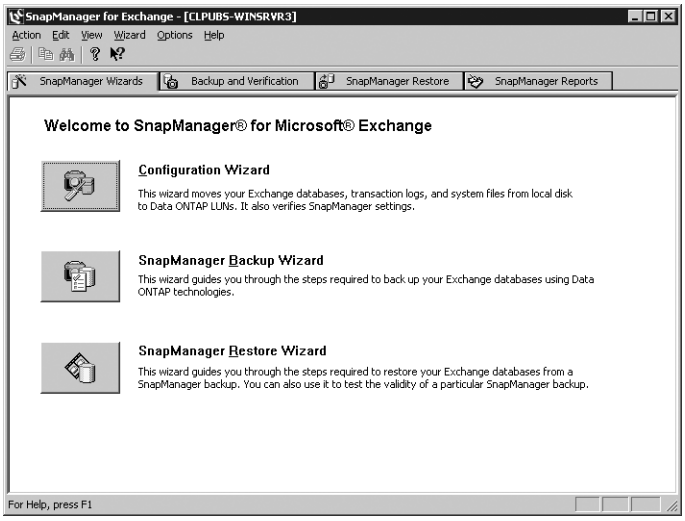
To start SnapManager for the first time, complete the following steps.

Step	Action
1	Start SnapManager 3.2 for Microsoft Exchange. To do this, go to the Start menu and select Program Files > SnapManager for Exchange. **Result:** The SnapManager main window appears. The next step depends on whether you have just upgraded to SnapManager 3.2 or installed SnapManager for the first time: ◆ If you have just upgraded to SnapManager 3.2 for Microsoft Exchange, SnapManager automatically connects to the default Exchange server already configured. Go to Step 3. ◆ If you have just installed SnapManager for the first time, the Connect to Exchange Server dialog box appears so that you can specify the default Exchange server. 

Step	Action
2	Specify the default Exchange Server: **a.** In the drop-down box, select or enter the Exchange server you want to manage. **b.** Click OK. **Result:** SnapManager connects to the specified Exchange server and then creates a share for remote access to the Report directory. The first time SnapManager is launched, it creates a Report directory share, `SMEReportFolder`, to allow for remote administration. The following accounts are granted **Full Control** on this share: ◆ The logged-in user on the local machine ◆ The `Administrators` group on the local machine If SnapManager was recently upgraded to SnapManager 3.2, there might be other existing accounts with permissions on the share: ◆ If only the existing group `Everyone` has permissions on the Report directory share, SnapManager removes the Full Control permissions to the Reports directory for that group. ◆ If multiple existing accounts (including `Everyone`) have permissions on the Report directory share, SnapManager does not modify those accounts.

Step	Action
3	Wait until SnapManager verifies the software versions on the default Exchange server and then prompts you to start the Configuration Wizard. SnapManager performs the following verification activities: ◆ First, SnapManager checks the Microsoft Exchange version. If SnapManager detects that the Microsoft Exchange 2000 or 2003 software does not have the minimum service pack level required by SnapManager, an error message box appears. If this occurs, see the table of "Windows host system requirements" on page 24 and note the requirements for Microsoft Exchange. ❖ If you have a different Exchange server that has the minimum service pack required by SnapManager, you can connect to that instance instead. To do this, open the Connect to Exchange Server dialog box (by selecting Action > Connect to Another Exchange) and then go to Step 2. ❖ Otherwise, close the SnapManager application, upgrade Microsoft Exchange as needed, and then restart SnapManager. ◆ Next, SnapManager checks the SnapDrive version. If SnapManager detects that SnapDrive is installed but that it is a version not supported with this version of SnapManager, a warning dialog box appears. If this occurs, see the table of "Windows host system requirements" on page 24 and note the requirements for SnapDrive. Close the SnapManager application, upgrade SnapDrive as needed, and then restart SnapManager. ◆ Finally, if SnapManager detects that no databases have been configured for use with SnapManager, a message box appears and prompts you to run the Configuration Wizard. 

Step	Action
4	Click OK. **Result:** The message box closes, and SnapManager automatically launches the Configuration Wizard. 

Step	Action
5	Click Cancel to exit the Configuration Wizard without specifying any database or LUN configuration information yet. **Result:** The Configuration Wizard closes, leaving only the SnapManager main window open.  **Note** If you are running SnapManager on a Windows Server 2003 machine with the Windows XP theme enabled, SnapManager is displayed with the Windows XP theme also.

What to do next

Before you run the Configuration Wizard, you must plan your database migration. Database migration planning is covered in the following sections:

- Chapter 5, "Determining the Number of LUNs Required," on page 71
- Chapter 6, "Creating Storage System Volumes and LUNs," on page 93

Note

Only after you have completed your database migration plan should you proceed to Chapter 7, "Configuring the Exchange Data for SnapManager," on page 113. The information in that section instructs you to start the Configuration Wizard manually and then describes how to specify your database and LUN configuration details.

Determining the Number of LUNs Required 5

For SnapManager backup and restore to function, the Exchange data store must be located properly on one or more LUNs, and those LUNs need to be sized appropriately. The ability to restore individual databases imposes additional data configuration requirements.

This section contains background information about Exchange, SnapManager, and SnapManager support for NTFS volume mount points. This information enables you to plan your SnapManager Exchange data store LUN and storage system volume requirements, based on your space and functionality requirements. The following topics are covered:

- "Understanding Exchange configuration rules" on page 72
- "Understanding SnapManager configuration rules for Exchange" on page 74
- "Understanding NTFS volume mount points" on page 78
- "Understanding SnapManager support for volume mount points" on page 80
- "Understanding transaction log archiving using NTFS hard links" on page 84
- "Example Exchange configurations supported with SnapManager" on page 87

Note

For faster backups and restores, use the minimum number of LUNs required for your business and service level commitments. Unless individual database restoration is a requirement in your environment, group your databases together.

After you determine how many LUNs you need for your SnapManager configuration and what data those LUNs will hold, proceed to Chapter 6, "Creating Storage System Volumes and LUNs," on page 93 to calculate required sizes for those LUNs as well as the sizes of the volumes that contain those LUNs.

Related topics:

- Chapter 4, "Starting SnapManager for the First Time," on page 63
- Chapter 6, "Creating Storage System Volumes and LUNs," on page 93
- Chapter 7, "Configuring the Exchange Data for SnapManager," on page 113

Understanding Exchange configuration rules

This topic describes the data configuration requirements inherent to Microsoft Exchange 2000 and 2003.

Related topics:

- "Understanding SnapManager configuration rules for Exchange" on page 74
- "Understanding NTFS volume mount points" on page 78
- "Understanding SnapManager support for volume mount points" on page 80
- "Example Exchange configurations supported with SnapManager" on page 87

Storage groups per server

There can be between one and four storage groups in an Exchange server.

Databases per storage group

A storage group contains from one to five databases.

Recovery storage group

For Exchange 2003 only, there can be a fifth storage group called the Recovery Storage Group. SnapManager does not support backing up or restoring to this special storage group.

Note

The presence of a Recovery Storage Group can interfere with SnapManager's ability to perform a restore. For more information, see "Exchange Recovery Storage Group incompatibility with SnapManager Restore" on page 186.

Storage groups per virtual server

An Exchange Server cluster has one or more Exchange virtual servers. In an active/active 2-node cluster, the maximum number of clustered storage groups is four for the entire clustered system because four is the maximum number of storage groups that can run on a single cluster node. An active/passive Exchange Server cluster can have more than two cluster nodes. The maximum number of Exchange virtual servers in an active/passive cluster is one less than the number

of nodes in the cluster. An active/passive Exchange cluster can have more than four storage groups because only one Exchange virtual server runs on a cluster node at any given time.

Understanding SnapManager configuration rules for Exchange

This topic contains SnapManager configuration rules for Exchange data stores:

- "Exchange data store configurations enforced" on page 74
- "Exchange data store configurations to avoid" on page 75
- "Exchange data store configurations recommended" on page 76
- "Exchange message tracking in an MSCS configuration" on page 76

Related topics:

- "Understanding Exchange configuration rules" on page 72
- "Understanding NTFS volume mount points" on page 78
- "Understanding SnapManager support for volume mount points" on page 80
- "Example Exchange configurations supported with SnapManager" on page 87

Exchange data store configurations enforced

The Configuration Wizard enforces the following rules when you are configuring your Exchange data store for SnapManager 3.2 for Microsoft Exchange.

Exchange databases: Exchange databases cannot share a LUN with databases from different storage groups, and they cannot share a LUN with transaction logs (even if they are from the same storage groups).

Note

All databases on a LUN are restored together. To be able to restore an individual database without restoring the rest of its storage group, that database must have its own LUN.

Exchange transaction logs: Transaction logs from different storage groups can share a LUN.

SnapManager SnapInfo directory: A SnapInfo directory can have its own LUN, or it can share a LUN with transaction logs. If you want to take advanage of NTFS hard links (described in "Understanding transaction log archiving using NTFS hard links" on page 84), the SnapInfo directory cannot share a LUN with Exchange databases.

SAN boot LUN: You cannot place database files, transaction log files, or a SnapInfo directory on a SAN boot LUN (a LUN configured as a boot device for a SAN host).

Exchange storage group system files: The Exchange storage group system files must be on a LUN containing the **transaction log files** for that storage group.

SnapManager versions prior to SnapManager 3.2 for Microsoft Exchange placed the storage group system files on a LUN that stores the Exchange databases in configurations that used VSS to backup Exchange. The Configuration Wizard in this version of SnapManager automatically moves storage group system files to the same LUN as the transaction logs if you to modify the database or transaction log location for that storage group.

Exchange data store configurations to avoid

Nothing should be stored on the Exchange LUNs except what SnapManager puts there. If you add more databases or move databases to different LUNs without using the Configuration Wizard, you can create an invalid configuration that could cause SnapManager backup or restore operations to fail.

Note

After adding or moving Exchange data stores, always run the Configuration Wizard. This ensures that the Exchange data stores are stored in valid locations so that SnapManager backup and restore operations can finish successfully.

Before you migrate your Exchange database and transaction log files to LUNs, note the following recommendations against certain invalid configurations that could be created outside of the SnapManager Configuration Wizard.

No other files on LUNs used by any database files: Do not manually store any directories or files (including system paging files) on the LUNs used for by the Exchange data store files (database files and transaction log files).

No other files on the LUN used by the SnapInfo directory: Do not manually store any directories or files on the LUN used by the SnapInfo directory.

No Exchange database files on a LUN that hosts mount points: Do not manually store Exchange database files on a LUN that hosts NTFS volume mount points. For more information, see “Understanding SnapManager support for volume mount points” on page 80.

Exchange data store configurations recommended

For best results, consider the following Exchange data store recommendations:

- Use dedicated volumes for your Exchange data.
- Do not place LUNs containing data from different Exchange servers in the same volume. This recommendation helps you to avoid the following problems:
  - SnapManager backups created for another Exchange server on the same volume use up Snapshot copies for that volume but are only restorable for the Exchange server they were taken for.
  - Conflicting backup schedules between the two Exchange servers can lead to creating "busy Snapshot copies".
- Do not place LUNs in the storage system's root volume. The root volume is reserved for use by Data ONTAP.
- For faster backups and restores, use the minimum number of LUNs required for your business and service level commitments. Unless individual database restoration is a requirement in your environment, group your databases .

Exchange message tracking in an MSCS configuration

When using Exchange message tracking with SnapManager in an MSCS configuration, locate the message tracking directory on a shared LUN that does not store a database.

How the message tracking directory location is specified: To create an Exchange virtual server in an MSCS configuration, you install the Exchange binaries on both nodes and then create a new System Attendant cluster resource. As part of creating the System Attendant cluster resource, Exchange prompts you to `Enter [a] path to the data directory`. Exchange places the new databases and other related files—including the SMTP and MTA queues, as well as the message tracking log and MS Search files (if configured)—on this path on a shared disk.

The effect of SnapManager Restore on a database LUN: Suppose the path you specify as the System Attendant cluster resource data directory is a shared LUN that is later also specified (using the SnapManager Configuration Wizard) as the LUN for an Exchange database. In this scenario, the Exchange message tracking log and the Exchange database are located on the same LUN.

SnapManager does not prevent this configuration, nor does this configuration pose an immediate problem. Later, however, when a SnapManager Restore operation is performed, the restore process brings the entire LUN back from Snapshot copy, complete with the desired database and an old copy of the message tracking log.

To avoid restoring an old message tracking log: To prevent a SnapManager Restore of a database from also restoring an old copy of the message tracking log, locate the message tracking directory on a shared LUN that does not store a database.

If your message tracking directory is already on a database LUN: If you have already created a System Attendant cluster resource with the data directory on a shared LUN that will also be used to store an Exchange database, you can move the message tracking location to a different location on a shared disk:

- For a description of how to move the message tracking location in Exchange Server 2000, see Microsoft Knowledge Base article 317700.
- For a description of how to move the message tracking location in Exchange Server 2003, see Microsoft Knowledge Base article 841089.

Understanding NTFS volume mount points

This topic contains highlights about NTFS mount points as they relate to Microsoft Exchange:

- "About NTFS volume mount points" on page 78
- "Volume mount point limitations" on page 78
- "Volume mount point limitations in a clustered environment" on page 79

Related topics:

- "Understanding Exchange configuration rules" on page 72
- "Understanding SnapManager configuration rules for Exchange" on page 74
- "Understanding SnapManager support for volume mount points" on page 80
- "Example Exchange configurations supported with SnapManager" on page 87

About NTFS volume mount points

A volume mount point is a drive or volume in Windows that is mounted to a folder that uses the NTFS file system. A mounted drive is assigned a drive path instead of a drive letter. Volume mount points enable you to exceed the 26-drive-letter limitation. By using volume mount points, you can graft, or mount, a target partition into a folder on another physical disk. For more information about volume mount points, see the Microsoft Web site.

Volume mount point limitations

With the NTFS volume mount points feature, you can create volume mount points on a dedicated disk or a shared cluster resource disk.

Volume mount points are not supported in the following scenarios:

- When they are used as a storage location for the Exchange 2003 binaries
- When they are used with Exchange clusters that are running Microsoft Exchange 2000 Server or earlier
- When they are used with Windows clusters that are running Microsoft Windows 2000 or earlier

  For more details, see the full text of Microsoft Knowledge Base article 318458.
- When you create a volume mount point on a server cluster, consider the following key items regarding volume mount points:

Volume mount points cannot go between clustered and nonclustered disks.

You cannot create mount points that refer to the Quorum disk.

Volume mount point limitations in a clustered environment

When creating mount points on a server cluster, keep these additional limitations in mind:

- Volume mount points are not supported on clustered Windows 2000 servers.
- The mounted volume must be of the same type as its root; that is, if the root volume is a shared cluster resource, the mounted volume must also be shared, and if the root volume is dedicated, the mounted volume must also be dedicated.
- You cannot create mount points to the Quorum disk.
- If you have a mount point from one shared cluster resource disk to another, ensure that the disks are in the same group and that the mounted disk resource is dependent on the root disk source.

  For more details, see the full text of Microsoft TechNet article 280297.

Understanding SnapManager support for volume mount points

This topic describes SnapManager support of NTFS volume mount points, which is new in this version of SnapManager:

- "Drive letter limitations and individual database restoration" on page 80
- "Mounted volume environments supported by SnapManager" on page 81
- "Mounted volume restrictions with SnapManager" on page 81
- "Mounted volume naming conventions with SnapManager" on page 82
- "Using mounted volumes in SnapManager" on page 82

Related topics:

- "Understanding Exchange configuration rules" on page 72
- "Understanding SnapManager configuration rules for Exchange" on page 74
- "Understanding NTFS volume mount points" on page 78
- "Example Exchange configurations supported with SnapManager" on page 87

Drive letter limitations and individual database restoration

Windows supports up to 26 drive letters. Because SnapManager needs one LUN and therefore one available drive letter to perform backups, verifications, or restores, you can allocate a maximum of 25 drive letters. In addition, certain SnapManager operations require that additional drive letters be available:

- Databases that need to be restored individually each require their own LUN and drive letter. If you have a large number of databases to be individually restored, you might run out of drive letters.
- Performing a remote verification of more than one backup set requires a second LUN and therefore another available drive letter or mount point.

With previous releases of SnapManager for Exchange, you can avoid running out of available drive letters by determining which databases must be restored individually, and which can be combined on a LUN with one or two other databases (all of which are restored together). With this approach, you must still reserve at least one free drive letter for SnapManager.

With SnapManager 3.2 for Exchange, your configuration is not limited to the 26 drive letters supported by Windows. By using the NTFS volume mount point support that is part of SnapDrive, SnapManager can manage Exchange databases that are stored on mounted volumes as well as those stored on standard Windows volumes.

Mounted volume environments supported by SnapManager

The following table summarizes the environments in which SnapManager 3.2 for Exchange supports volumes mounted on Data ONTAP LUNs. Additional details regarding limitations and enforcement imposed by SnapManager are described in other sections of this document.

Microsoft Exchange	Windows host environment			
	Windows 2000 Server		Windows Server 2003	
	Stand-alone	Clustered [1]	Stand-alone	Clustered
Exchange 2000	Yes	No	N/A [2]	
Exchange 2003	Yes	No	Yes	Yes

[1] Windows 2000 Server does not support mounted volumes in a cluster.

[2] Microsoft Exchange 2000 is not supported on Windows Server 2003.

Mounted volume restrictions with SnapManager

In addition to the limitations inherent to the NTFS volume mount point feature of Windows (described in "Understanding NTFS volume mount points" on page 78), SnapManager imposes the following additional restrictions.

No Exchange database files on a mount point root: An NTFS volume that hosts mount points cannot also store Exchange database files. However, transaction log files can reside on such a volume.

- The SnapManager Configuration Wizard does not allow you to place Exchange database files on an NTFS volume that has mount points.
- SnapManager Backup does not allow you to back up a database on an NTFS volume that has mount points.

Note

If Exchange databases reside on a LUN, do not add mount points to that LUN, even after you finish a SnapManager backup operation. A subsequent LUN-level SnapManager restore operation would remove those volume mount points, disrupting access to the data on the mounted volumes referenced by these volume mount points.

Mounted volume naming conventions with SnapManager

A mounted volume is a volume that is mapped to a folder and referenced by a mount point that is created in an empty directory. The SnapManager user interface represents a mounted volume based on the path of a volume mount point that references that mounted volume, as follows:

DriveLetter:*MountPointName*

where

- *DriveLetter* represents the drive letter to which the mounted volume is assigned
- *MountPointName* represents the mount point name assigned to the empty directory used to reference the mounted volume

Example:

```
F:\ My_Mount_Point
```

Using mounted volumes in SnapManager

The path-style representation of a mounted volume can appear in any part of the SnapManager user interface that refers to LUNs accessed by SnapManager:

- Configuration Wizard screens that include a **Disk List selection**:
  - Where to Move Databases
  - Where to Move Transaction Logs
  - Where to Move SMTP and MTA System File
  - Where to Put the SnapInfo Directory

  LUns that are referenced more than once: If the storage system is configured with multiple references to the same LUN, each such LUN reference is listed with a label that lists any other references to the same LUN. For example, suppose the **drive letter** `H:` and the **mount point** `G:\DB\` reference the same LUN. In this case, the Disk List selection contains two entries for the one LUN:

  ```
  LUN H:  <G:\DB\>
  LUN G:\DB\  <H>
  ```

  LUNs that have mounted volumes: If SnapManager accesses a LUN with an NTFS volume that is referenced by a mount point, that LUN is listed with a label that indicates this. For example, suppose the drive letter `F:` references a LUN that hosts a mount point. In this case, the Disk List selection lists that LUN as follows:

  ```
  LUN F:  (MPRoot)
  ```

  The Configuration Wizard does not allow you to store Exchange database files on LUNs that host NTFS volume mount points.

- The **location of the storage group components** listed in the left navigation pane of the Backup and Verification Backup tab and the SnapManager Backup Wizard:
  - SnapInfo directory
  - EDB and STM paths
  - Storage group log path
- The **location of the storage group components** listed in the right display pane of the SnapManager Restore tab and the SnapManager Restore Wizard:
  - SnapInfo directory
  - EDB and STM paths
  - Storage group log path
- To specify which method is to be used to **access database backup Snapshot copies during database integrity verification**, use the Access LUN in Snapshot tab to assign either a drive letter or directory path to access the backup Snapshot copy as a mounted LUN. You can access this setting from the following locations within the SnapManager user interface:
  - Configuration Wizard
  - Options menu
  - Backup Wizard
  - Restore Wizard

  For more information, see "Selecting the Snapshot copy access method for database verification" on page 346.

Understanding transaction log archiving using NTFS hard links

During a SnapManager backup operation, SnapManager archives transaction log files on the live file system to the SnapInfo directory. To optimize backup operations in which the storage group transaction log files and the associated SnapInfo directory are located on the same NTFS volume, SnapManager archives transaction log files to the SnapInfo directory by **creating NTFS hard links** instead of **performing a file copy** operation. This conserves storage system disk space and improves system performance during the transaction log archival phase of the backup operation.

See the following topics for more information:

- "About NTFS hard links" on page 84
- "About transaction log archiving using NTFS hard links" on page 85
- "About multiple SnapInfo directories" on page 86

About NTFS hard links

A hard link is a directory entry for a file, and it serves as a file system-level shortcut to the file. An application can use a hard link like any other file name. Unlike an application-level link, all changes made to a file accessed using a hard link are applied automatically and transparently; any updates to the file contents are seen by all applications that access the file using a hard link. Unlike a symbolic link, a hard link cannot cross file systems; that is, a hard link created on one NTFS volume cannot point to a file in a different NTFS volume.

About multiple NTFS hard links: Every file can be considered to have at least one hard link. Within a given NTFS volume, a single file can have multiple hard links. This enables a single file to appear in multiple directories or to appear multiple times (under different names) within the same directory. Because all of the links reference the same file, multiple applications can open any of the hard links and modify the same file.

Note

The NTFS file system will not delete a file until all hard links to the file have been deleted.

The benefits of using multiple NTFS hard links: When a hard link is created for an *existing* file on an NTFS volume, NTFS simply adds hard link information and a reference count to the file's directory entry at the NTFS level. Neither the original file nor the file-based reference (the application-level link) are duplicated. While the physical file remains intact in its original location, the

same content can be accessed by two or more names. Because the file system is responsible for managing the various path names to a single physical content, using a hard link can conserve system resources and storage system disk space as compared to performing a standard file copy operation.

About transaction log archiving using NTFS hard links

During a SnapManager backup operation, SnapManager archives transaction log files on the live file system to the SnapInfo directory. The transaction log files are needed for SnapManager restore operations at the later time.

Transaction log archiving using file copy: When SnapManager uses a file copy operation to copy the transaction log files from the live file system to the SnapInfo directory, this method of transaction log archiving has the following effects:

- Management of path names and the copy operation incurs file system overhead and storage system overhead, resulting in slower host and storage system performance.
- Each additional copy of a transaction log file not only consumes storage system disk space but also increases the use of overwrite reserve for the LUN.

Transaction log archiving using NTFS hard links: SnapManager 3.2 supports an optimization feature for cases in which the backup operation archives transaction log files to a SnapInfo directory that resides on the same volume. To achieve this optimization, SnapManager archives transaction log files to the SnapInfo directory by creating NTFS hard links to the live transaction log files, without physically copying the log file.

After the SnapManager backup operation completes, Exchange truncates the transaction log files. However, the physical log files on the original location are not deleted, because the NTFS file system detects that other hard links to the files still exist. Instead, the original NTFS hard links to the live transaction log files are removed, and the links to the SnapInfo directory remain intact and available for access during SnapManager restore operations.

SnapManager automatically uses NTFS hard links to archive transaction logs if they reside on the same LUN as the SnapInfo directory.

Entries in the backup report: Transaction log archival is logged differently in the SnapManager backup report, depending on which archival method is used.

If a transaction log file is archived by **performing a file copy operation**, the backup report entry is similar to the following:

```
Log file copying from:
L:\Program Files\Exchsrvr\mdbdata\E000000A.log
Log file copying to:
S:\SME_SnapInfo\EXCH__CLPUBS-WINSRVR3\SG__First Storage
Group\CLPUBS-WINSRVR3__recent\Logs\E000000A.log
```

If the same transaction log file is archived by **creating an NTFS hard link** instead of performing a file copy operation, the backup report entry is similar to the following:

```
Log file:
L:\Program Files\Exchsrvr\mdbdata\E000000A.log
Archived to:
S:\SME_SnapInfo\EXCH__CLPUBS-WINSRVR3\SG__First Storage
Group\CLPUBS-WINSRVR3__recent\Logs\E000000A.log
```

About multiple SnapInfo directories

The primary reason that SnapManager supports multiple SnapInfo directories is to facilitate the use of NTFS hard links for archiving transaction logs, thereby conserving system resources and storage system disk space. The use of multiple SnapInfo directories also has the additional benefit of minimizing your exposure to the loss of backups in case the SnapInfo directory is lost.

The following paragraphs describe both of the benefits of configuring your Exchange data to use **multiple SnapInfo directories**.

Broader application of copy-less transaction log archiving: The use of NTFS hard links to archive transaction logs can only be applied to backup operations in which the transaction logs reside on the same NTFS volume as the SnapInfo directory. If your SnapManager environment is configured with a single SnapInfo directory for all Exchange storage groups, SnapManager can still use NTFS hard links to archive transaction logs, but only if all transaction logs for all storage groups are located on a single LUN on the same volume as the SnapInfo directory.

In most SnapManager environments, however, the Exchange transaction log files are stored on multiple LUNs in multiple storage system volumes. In this configuration, the use of NTFS hard links to archive transaction logs requires a separate SnapInfo directory for each Exchange storage group, with each SnapInfo directory placed on the same NTFS volume as the Exchange transaction logs for that storage group.

Example Exchange configurations supported with SnapManager

This topic contains sample configurations that illustrate possible ways to satisfy the configuration rules for SnapManager 3.2 for Exchange:

- "Single storage group and individual database restoration not required" on page 88
- "Single storage group and individual database restoration required" on page 89
- "Multiple storage groups and individual database restoration not required" on page 90
- "Multiple storage groups and individual database restoration required" on page 91

Related topics:

- "Understanding Exchange configuration rules" on page 72
- "Understanding SnapManager configuration rules for Exchange" on page 74
- "Understanding NTFS volume mount points" on page 78
- "Understanding SnapManager support for volume mount points" on page 80

For more information about SnapManager for Exchange data store configuration, see the *SnapManager for Microsoft Exchange Best Practices Guide*.

Note

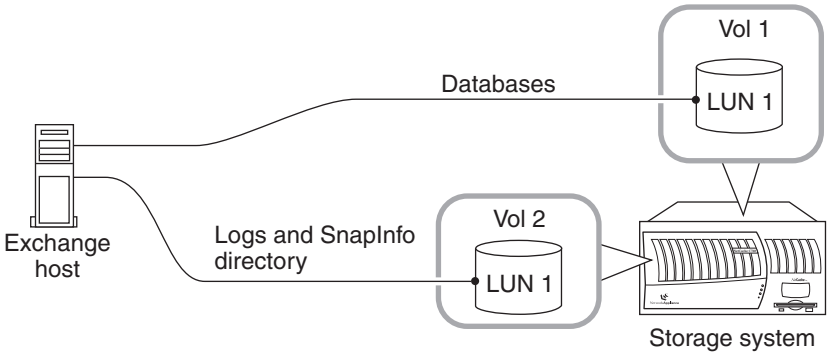
The LUN numbers are for illustration only; they do not correspond to any configuration setting on your host system. In addition, your configuration will vary based on your sizing and capability requirements.

Single storage group and individual database restoration not required

This example configuration has the following characteristics:

- One storage group with up to five databases
- Individual database restoration not required

Because this Exchange server has only one storage group, only one LUN is required for the databases. A total of two LUNs are required for this configuration, as shown in the following diagram.



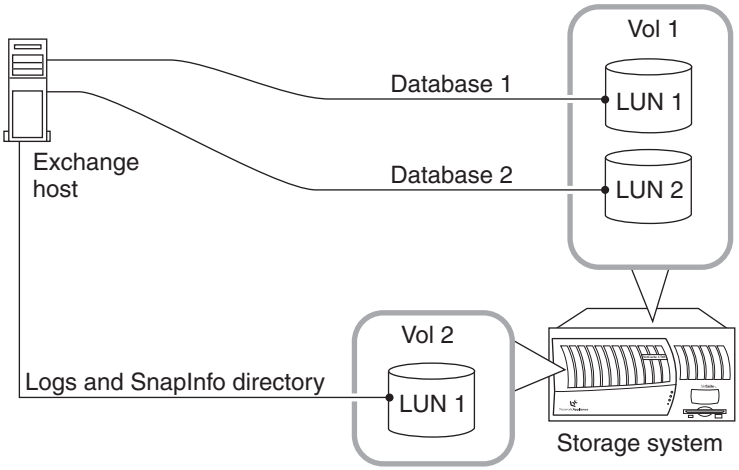
Sample configuration 1

Single storage group and individual database restoration required

This example configuration has the following characteristics:

- One storage group with two databases
- Individual database restoration required

Because the ability to restore either of the databases individually is required, each database must be placed on its own LUN. Therefore, three LUNs are required for this configuration, as shown in the following diagram.



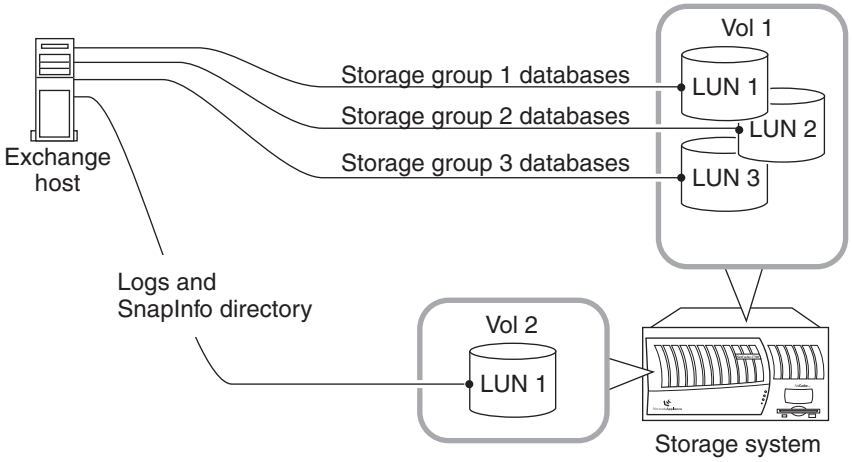
Sample configuration 2

Multiple storage groups and individual database restoration not required

This example configuration has the following characteristics:

- Three storage groups with up to five databases each
- Individual database restoration not required

Four LUNs are required for this configuration, as shown in the following diagram.



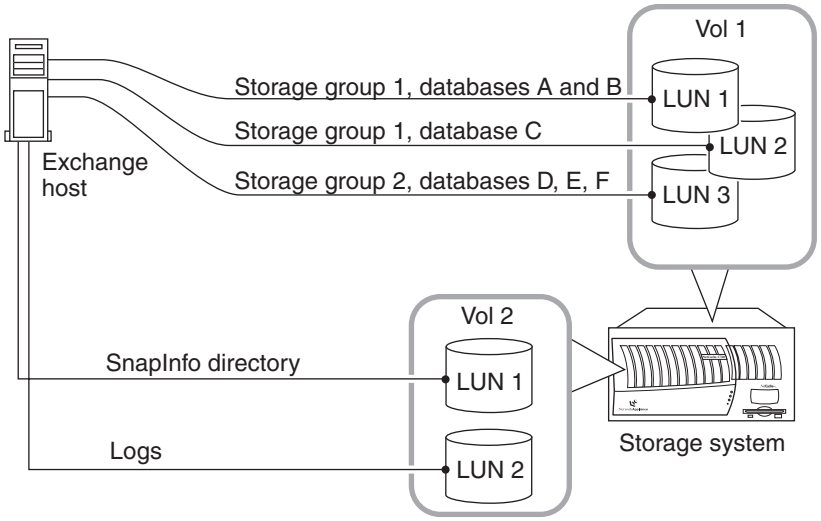
Sample configuration 3

Multiple storage groups and individual database restoration required

This example configuration has the following characteristics:

- Two storage groups with three databases each
- Individual database restoration required for database C in the first storage group

With this configuration, database C in storage group 1 can be restored without restoring any of the other databases in its storage group. However, databases A and B have to be restored at the same time. A total of five LUNs are used for this configuration, as shown in the following diagram.



Sample configuration 4

Note

Configuring many databases on their own LUNs for individual restoration can cause you to run out of drive letters.

For more information about drive letter limitations, see "Drive letter limitations and individual database restoration" on page 80.

Creating Storage System Volumes and LUNs 6

After you determine how many LUNs you need for your SnapManager configuration and what data those LUNs will hold, use the information in this section to develop your SnapManager data configuration plan and prepare storage system volumes and LUNs for use with SnapManager. This entails calculating and recording the required sizes for the LUNs, which also determines the sizes of the volumes that contain the LUNs. Use the information you record in your SnapManager data configuration plan to create or modify the storage system volumes and LUNs on your storage system.

This section covers the following topics:

- "Developing your SnapManager data configuration plan" on page 94
- "Calculating LUN size for Exchange databases" on page 96
- "Calculating single-instance sharing ratio for a database LUN" on page 98
- "Calculating deleted-item cache size for a database LUN" on page 100
- "Calculating LUN size for transaction logs and SnapInfo directory" on page 101
- "Calculating volume size" on page 104
- "Effect of new features on volume sizing" on page 107
- "Preparing storage system volumes and LUNs for SnapManager" on page 110

Related topics:

- Chapter 4, "Starting SnapManager for the First Time," on page 63
- Chapter 5, "Determining the Number of LUNs Required," on page 71
- Chapter 7, "Configuring the Exchange Data for SnapManager," on page 113

Developing your SnapManager data configuration plan

As you calculate the required sizes of the storage system volumes and LUNs required for your Exchange configuration, you need to record this information in one place; this composes your SnapManager data configuration plan. This information is used to create or upgrade your volumes and LUNs during the SnapManager configuration procedure.

The information you record in your SnapManager data configuration plan could also be invaluable if problems arise later with your Exchange system. Knowing the volume and drive for each of your LUNs can aid the diagnosis and resolution of many potential issues.

To create your SnapManager data configuration plan, complete the following steps.

Step	Action
1	For each LUN you need, record the following information: ◆ Purpose ◆ Size ◆ Volume and qtree ◆ Assigned drive letter or mount point For details about calculating LUN size for an Exchange database, see the following topics: ◆ "Calculating LUN size for Exchange databases" on page 96 ◆ "Calculating single-instance sharing ratio for a database LUN" on page 98 ◆ "Calculating deleted-item cache size for a database LUN" on page 100 For details about calculating LUN size for transaction log files and the SnapInfo directory or directories, see "Calculating LUN size for transaction logs and SnapInfo directory" on page 101

Step	Action
2	For each volume you need to store LUNs, record the following information: ◆ Location (storage system name) ◆ Purpose ◆ Type (traditional or flexible) ◆ Fractional reserve (%) ◆ Automatic Snapshot copy deletion setting (enabled or disabled) ◆ LUNs contained ◆ Volume autogrow (enabled or disabled) For details about calculating volume size, see “Calculating volume size” on page 104.

Calculating LUN size for Exchange databases

This topic describes how to calculate the required size for the LUNs to hold your Exchange databases. The size of the LUN to hold Exchange databases must be at least as big as the sum of the expected maximum sizes of all databases on that LUN.

- "Estimated database values" on page 96
- "Calculation formula" on page 96
- "Example" on page 96

Estimated database values

To calculate the expected maximum size for an Exchange database LUN, you need the following values (or estimates) for each database on the LUN:

- Number of mailboxes in the database
- Mailbox quota
- Single-instance sharing ratio

  For more information about calculating the single-instance sharing ratio, see "Calculating single-instance sharing ratio for a database LUN" on page 98.
- Size of the deleted item cache (expressed as a percentage of the overall size of the data)

  For more information about calculating the deleted-item cache size, see "Calculating deleted-item cache size for a database LUN" on page 100.

Calculation formula

The following formula calculates the expected Exchange database size:

```
database size = ((number of mailboxes * mailbox quota) / single
instance sharing ratio) + deleted item cache
```

The sum of the maximum expected database size for each database in your LUN provides the maximum expected database LUN size.

Example

The following facts and assumptions represent a sample Exchange installation:

- There is one storage group, with one database.
- There are 1,000 mailboxes with 100-MB quotas in the database.
- The single-instance sharing ratio is equal to 1.5.
- The deleted-item cache is 20% of the database.

For this example, the database size requirement calculation would be as follows:

```
database size = (((1,000 * 100 MB)/1.5) * 1.2) = 80,000 MB (~80 GB)
```

Note

In this calculation, the addition of 20% of the database size (to allow for the size of the deleted item cache in this example) is expressed by multiplying the estimated storage group size by a factor of 1.2 (or 120%).

The calculated maximum LUN size for this database is approximately 80 GB. If you want to allow for 10 GB of free space, increase the LUN size from 80 GB to 90 GB.

Calculating single-instance sharing ratio for a database LUN

This topic describes how to calculate the single-instance sharing ratio used to calculate the expected maximum size for an Exchange database LUN.

Single-instance sharing ratio for a new Exchange installation

For a new installation of Microsoft Exchange, use the value 1.5 for your single-instance sharing ratio.

Note
After you have a more mature installation, recalculate the ratio using the procedure below.

Single-instance sharing ratio for an existing Exchange installation

Use the following procedure to calculate the single-instance sharing ratio for your installation.

Calculation guidelines: Use these guidelines when calculating the single instance ratio:

- Track the ratio over time during peak production times; then choose the lowest ratio value recorded.
- If you obtain different ratio values for different databases within a storage group, choose the lowest value for that storage group in your calculation.

Calculating the single-instance ratio: To calculate the single-instance sharing ratio for your installation, complete the following steps.

Step	Action
1	Run the Windows Performance Monitor utility (also known as "Perfmon").
2	Right-click the graph and select Add Counters. **Result:** The Add Counters dialog box is displayed.
3	In the Performance Object drop-down list, select the performance object MSExchangeIS Mailbox.
4	In the Select Counter From List option, select Single Instance Ratio.

Step	Action
5	Select all databases in the instances list for the storage group you are measuring.
6	Click Add.

Calculating deleted-item cache size for a database LUN

To calculate the deleted-item cache size for your installation, complete the following steps.

Step	Action
1	Run the Windows Performance Monitor utility (also known as "Perfmon").
2	Right-click the graph and select Add Counters. **Result:** The Add Counters dialog box is displayed.
3	In the Performance Object drop-down list, select the performance object MSExchangeIS Mailbox.
4	In the Select Counter From List option, select Total Size of Recoverable Items.
5	Select all databases in the instances list for the storage group you are measuring.
6	Click Add. **Result:** PerfMon provides the total size of recoverable items (in the selected storage group) in kilobytes.
7	To calculate the deleted-item cache size as a percentage value for use in the LUN size "Calculation formula" on page 96, divide the total size of recoverable items (in kilobytes) by the total size of the database (in kilobytes).

Calculating LUN size for transaction logs and SnapInfo directory

This topic describes how to calculate the required size for the LUNs to hold your transaction logs and SnapInfo directory or directories. A SnapInfo directory can reside on the same LUN as the transaction logs, or it can be placed on a separate LUN. Use the following calculations as they apply to your planned configuration of SnapManager for Exchange:

- "Transaction log and SnapInfo directory LUN size calculation" on page 101
- "SnapInfo directory LUN size calculation" on page 102
- "Transaction logs LUN size calculation" on page 102

Note

For information about using multiple SnapInfo directories, see "About transaction log archiving using NTFS hard links" on page 85 and "About multiple SnapInfo directories" on page 86.

Transaction log and SnapInfo directory LUN size calculation

The size of the LUN containing the transaction logs and SnapInfo directory depends on how much message traffic your Exchange server gets and your backup usage. The size calculation is performed per storage group.

Estimated transaction log values: The following values (or estimates) are required for each storage group whose transaction logs will be stored on this LUN:

- How many transaction log files are generated between backups
- How many backups will be retained online

Note

You can estimate how many transaction log files are generated by noting the maximum number of transaction logs that accumulate in the transaction log directory immediately before a backup over a period of several days.

Calculation formula: The following formula calculates the LUN size required for a LUN containing transaction logs and the SnapInfo directory:

```
transaction log & SnapInfo LUN size = ((number of transaction logs
generated * 5 MB) * (number of backups to keep online + 1 for the
active file system))
```

Example: Given the following parameters, at least 6 GB of LUN drive is required to accommodate the transaction logs and SnapInfo directory for the example Exchange databases. This is expressed by the formula following the parameters.

- The server generates, at most, 200 transaction logs between backups.
- Each transaction log is 5 MB.
- The plan is to keep five SnapManager backups online at the same time.

```
transaction log & SnapInfo LUN size = ((200 * 5 MB)*(5+1)) = 6,000
MB (~6 GB)
```

SnapInfo directory LUN size calculation

The SnapInfo directory contains the logs for all backups currently retained online. Therefore, if your SnapInfo directory is on a separate LUN from your transaction logs, the LUN size calculation is similar to the calculation for a combined transaction log and SnapInfo LUN, except that you do not have to include space for the current logs.

Calculation formula: The following formula calculates the LUN size required for a LUN containing only the SnapInfo directory:

```
SnapInfo LUN size = ((number of transaction logs generated * 5 MB)
* (number of backups to keep online))
```

Example: Given the following parameters, at least 5 GB of LUN drive is required to accommodate the SnapInfo directory for the example Exchange databases. This is expressed by the formula following the parameters.

- The server generates, at most, 200 transaction logs between backups.
- Each transaction log is 5 MB.
- The plan is to keep five SnapManager backups online at the same time.

```
transaction log & SnapInfo LUN size = ((200 * 5 MB)*5) = 5,000 MB
(~5 GB)
```

Transaction logs LUN size calculation

If the SnapInfo directory is on a separate LUN from your transaction logs, the LUN size calculation for the transaction log LUN has to take into account only how many logs accumulate between backups.

Calculation formula: The following formula calculates the LUN size required for a LUN containing only the transaction logs:

```
transaction log LUN size = number of transaction logs generated * 5
MB
```

Example: Given the following parameters, at least 1 GB of LUN drive is required to accommodate the transaction logs for the example Exchange databases. This is expressed by the formula following the parameters.

- The server generates, at most, 200 transaction logs between backups.
- Each transaction log is 5 MB.

```
transaction log LUN size = 200 * 5 MB = 1,000 MB (~1 GB)
```

Calculating volume size

This topic describes how to calculate the required size for the volumes to contain your LUNs:

- "Considerations for converting to individual database restoration" on page 104
- "Database volume size calculation" on page 104
- "Transaction log volume size calculation" on page 105
- "Volume size calculation for multiple Exchange LUNs" on page 106

Note

For a summary description of Data ONTAP fractional space reservation and a detailed description of SnapManager fractional space reservation policies, see "Managing fractional space reservation" on page 360.

Considerations for converting to individual database restoration

If you are upgrading an existing SnapManager implementation and you are creating new LUNs to use individual database restore, your space requirements increase. This is because the database must be copied from its current location to the new location; in effect, it exists in both places until the move is complete. Depending on the size of the volume containing both LUNs, you might need to increase the volume size.

For more information about sizing your volumes, see "Calculating volume size" on page 104. Remember to include both the old and new LUNs when calculating the volume size.

Database volume size calculation

The calculation for the Exchange database volume size depends on the size of the databases in the volume, the rate of change of your data, and your backup usage.

Estimated database volume values: To calculate the volume size requirement for a LUN holding Exchange databases, you need the following values or estimates for your installation:

- The size of the LUNs (as calculated using the database LUN formula)
- The approximate percentage of the databases that you expect to change between backups
- How many backups you plan to retain online

Calculation formula: The following formula calculates the minimum volume size requirement for the Exchange database LUNs:

```
minDatabaseVolumeSize = (2 * LUN size) + (number of online backups
* percentage data change * max database size)
```

Example: For the example, assume the following facts:

- Approximately 10% of the database changes between backups.
- Five backups will be retained online.

The minimum volume size for the database LUN is calculated as follows:

```
(2 * 90 GB) + (5 * 10% * 80 GB) = 220 GB
```

Transaction log volume size calculation

The size of the transaction log volume depends on how much traffic your Exchange server gets, and your backup usage.

Estimated transaction log values: The following values or estimates are required for the entire volume where the transaction logs are stored:

- How many transaction log files are generated between backups
- How many backups will be retained online

Calculation formula: The following formula calculates the transaction log volume size:

```
transaction log volume size = (transaction log LUN size in MB * 2)
+ (2 * number of transaction logs generated * 5 MB * number of
backups to keep online)
```

This is always less than four times the size of the transaction log LUN. Therefore, if disk capacity is not constrained, you can use this simplified formula:

```
transaction log volume size = 4 * transaction log LUN size
```

Example: For the example, the transaction log volume size could be calculated using the full formula, as follows:

```
transaction log volume size = (6,000 MB * 2) + (2 * 200 * 5 MB * 5)
= 12,000 + 10,000 MB = 22,000 MB (~22 GB)
```

Alternatively, you could calculate the volume using the simplified formula, as follows:

```
transaction log volume size = (6,000 MB * 4) = 24,000 MB (~24 GB)
```

Volume size calculation for multiple Exchange LUNs

If you plan to use a single storage system volume for storing multiple LUNs to hold Exchange or SnapManager data, the volume sizing requirements of all the components must be summed to calculate the size requirement for the volume.

Note

Microsoft recommends that Exchange databases and transaction logs be kept on separate volumes. This example is for illustration only.

Example: Assume now that you want to create one volume for an Exchange installation with the following characteristics:

- Four storage groups, each with 1,000 mailboxes and 100-MB quotas
- Single instance sharing ratio of 1.5
- Deleted item cache is 20% of the data
- A combined maximum of 800 transaction logs generated between backups
- 10% database change between backups
- Five online backups retained

LUN size requirements	Resulting volume size requirement
Each storage group requires a 90-GB LUN, as calculated previously.	4 LUNs * 220 GB = 880 GB
The transaction log and SnapInfo LUN requires the following LUN size: (800 * 5 MB) * (5+1) = 24,000 MB or about 24 GB.	(2 * 24,000 MB) + (2 * 800 * 5 MB * 5) = 88,000 MB or approximately 88 GB
Result: The five LUNs must reside in a volume whose size is approximately 880 + 88 = 968 GB.	

Effect of new features on volume sizing

Several new features in SnapManager for Exchange 3.2 are designed to reduce the amount of disk space required to run SnapManager:

- Transaction log archiving using NTFS hard links

  For more information, see "About transaction log archiving using NTFS hard links" on page 85.
- Fractional space reservation

  For more information, see "Managing fractional space reservation" on page 360.
- Option to backup transaction logs that Exchange will truncate

  For more information, see page "Ways to manage the backup and deletion of transaction logs" on page 154.

These new features will have an affect on some of the sizing formulas in this chapter. Following are the updated formulas:

Transaction log archiving using NTFS hard links

Configurations in which the transaction logs reside on the same NTFS volume and LUN can take advantage of the new NTFS hard link support in SnapManager. During a backup, SnapManager copies the transaction log files to the SnapInfo directory for safe keeping. However, in supported configurations that can take advantage of NTFS hard links, a link is created to the file rather than copying the file itself. Since there are fewer blocks changed on the storage system volume as a result of this feature, the formula to calculate the size of the storage system volume for the Exchange transaction logs needs to be slightly modified. The difference in this case is that the `number of transaction logs generated` does not need to be multiplied by a factor of two as with the original formula. In the following updated formula, the `number of transaction logs generated` is only accounted for once, so the "`2 *`" is removed from the original formula.

The following formula calculates the transaction log volume size:

```
TransactionLogVolumeSize = (transaction log LUN size in MB * 2)
+ (number of transaction logs generated * 5 MB * number of
backups to keep online)
```

As an example, the transaction log volume size could be calculated using the full formula, as follows:

```
TransactionLogVolumeSize = (6,000 MB * 2) + (200 * 5 MB * 5) =
12,000 + 5,000 MB = 17,000 MB (~17 GB)
```

Fractional space reservation

Prior to the support for fractional space reservation in SnapManager, there was a requirement that the volume size on the storage system be at least twice the size of the LUN that it contains plus allow extra volume space to store SnapManager backups as well as accommodate changes in the Exchange data. With the new fractional space reservation support in SnapManager enabled, this factor of 2 can been relaxed to a factor that is greater than 1 and less than or equal to 2.

This change affects two storage system volume size calculation formulas:

- Volume size for Exchange databases
- Volume size for Exchange transaction logs and SnapManager SnapInfo directory

Only the `transaction log LUN size in MB * 2` portion of the formulas are updated from the original formulas. The updated portion of the formula can be expressed as `transaction log LUN size in MB * (1+n)` , where `n` is a number greater than 0 and less than or equal to 1.

Volume size for Exchange databases: The following formula calculates the volume size for the Exchange database LUNs:

```
DatabaseVolumeSize = ((1+n) * LUN size) + (number of online backups
* percentage data change * max database size)
```

As an example, assume the following facts:

- Approximately 10% of the database changes between backups.
- Five backups will be retained online.
- Fractional space reservations are in use with a setting of 65 (or enough space reservation to accommodate 65% of the size of the LUN)

In this case, the minimum volume size for the database LUN is calculated as follows:

```
((1 + 0.65) * 90 GB) + (5 * 10% * 80 GB) = 188 GB
```

Volume size for transaction logs and SnapInfo directory: The following formula calculates the volume size for the transaction log and SnapInfo LUNs:

```
TransactionLogVolumeSize = (transaction log LUN size in MB * (1
+ n)) + (2 * number of transaction logs generated * 5 MB *
number of backups to keep online)
```

As an example, assume the following facts:

- Approximately 10% of the database changes between backups.
- Five backups will be retained online.

- Fractional space reservations are in use with a setting of 65 (or enough space reservation to accommodate 65% of the size of the LUN)

In this case, the minimum volume size for the transaction log and SnapInfo LUNs is calcualted as follows:

```
TransactionLogVolumeSize = (6,000 MB * 1.65) + (2 * 200 * 5 MB *
5) = 9,900 + 10,000 MB = 19,900 MB (~20 GB)
```

Option to back up transaction logs that Exchange will truncate

This is another feature that can be used to save on amount storage system volume space consumed. However, since you cannot predict the number of transaction logs Exchange will truncate or when it will truncate them, you cannot accurately calculate the amount of disk space that can be saved by using this configuration.

Preparing storage system volumes and LUNs for SnapManager

To prepare storage system volumes and LUNs to be used with SnapManager, complete the following steps.

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td rowspan="4">1</td><td colspan="2">Create or update storage system volumes and LUNs for use with SnapManager.</td></tr>
<tr><td>If...</td><td>Then do this...</td></tr>
<tr><td>This is a new installation of SnapManager</td><td>Use your storage system administration tools and SnapDrive to create the storage system volumes and LUNs required for your new installation of SnapManager.</td></tr>
<tr><td>This is an upgraded installation of SnapManager</td><td>Update your existing storage system volumes and LUNs as needed:
a. Review your existing storage system volumes and LUNs against the requirements for your upgraded installation of SnapManager.
b. Use your storage system administration tools and SnapDrive to make any necessary changes to the storage system volumes and LUNs.</td></tr>
<tr><td colspan="2">New or updated storage system requirements are outlined in your SnapManager data configuration plan, described in “Developing your SnapManager data configuration plan” on page 94.</td></tr>
</table>

Step	Action
2	If your configuration plan includes Exchange **database LUNs** that reside in volumes that have overwrite reserve configured to less than 100 percent, do the following: **a.** Ensure that the Data ONTAP Snapshot copy autodeletion policy is disabled on each of these fractional space-reserved volumes. For detailed information, see "Viewing fractional space reservation status" on page 365. **b.** Verify the SnapManager fractional space reservation policy settings for each fractional space-reserved storage system volume. The two trigger points are set to default values and might need to be modified to meet your organization's service level agreements and business continuance plans. For detailed information, see "Configuring fractional space reservation policies" on page 367.
3	Proceed to Chapter 7, "Configuring the Exchange Data for SnapManager," on page 113.

Configuring the Exchange Data for SnapManager 7

This section describes how to configure your Microsoft Exchange data using SnapManager 3.2 for Microsoft Exchange. The following topics are covered:

- "Understanding the SnapManager Configuration Wizard" on page 114
- "Using the Configuration Wizard to configure your data store" on page 118
- "Migrating an existing SnapManager for Exchange configuration from using drive letters to using mount points" on page 130

Attention

You must run SnapManager from the system console, not from a Terminal Services client. Do not use Terminal Services for any type of SnapManager administration, because you might miss critical information that is displayed only in pop-up boxes at the system console.

Related topics:

- Chapter 4, "Starting SnapManager for the First Time," on page 63
- Chapter 5, "Determining the Number of LUNs Required," on page 71
- Chapter 6, "Creating Storage System Volumes and LUNs," on page 93

Understanding the SnapManager Configuration Wizard

The primary function of the Configuration Wizard is to migrate Exchange databases to Data ONTAP LUNs so that the databases can be backed up and restored using SnapManager. For more information, go to any of the following topics:

- "What the Configuration Wizard does" on page 114
- "When to use the Configuration Wizard" on page 115
- "About the Exchange and SnapManager components" on page 115
- "Viewing the placement of Exchange and SnapManager components" on page 116
- "Settings configurable only with the Configuration Wizard" on page 116

What the Configuration Wizard does

The Configuration Wizard enables you to move your Exchange data in the following ways.

From local disk to LUN: To enable management by SnapManager.

- If Exchange databases need to be moved, the wizard dismounts the databases in a storage group, moves the Exchange database and transaction log files to the selected LUN, and remounts the databases.

  Note
  SnapManager takes Exchange databases offline during the move operation.

- The wizard creates a SnapInfo directory that SnapManager uses to store information about the backup sets and the backed-up transaction logs.
- The wizard disables circular logging for all storage groups that are moved to a LUN, to enable up-to-the-minute recovery of those storage groups.
- The wizard also guides you through several application settings. These settings include enabling notification of SnapManager events using e-mail, and enabling notification of SnapManager events using the storage system Syslog or the AutoSupport feature.

From LUN to LUN: If resource management issues require this. For example, consolidating Exchange on another storage system.

From LUN to local disk: If no longer managed using SnapManager. However, this is not supported in MSCS configurations.

When to use the Configuration Wizard

You can use the Configuration Wizard in the following situations.

For initial configuration: Before you can use SnapManager to back up and restore an Exchange data store, you must use the SnapManager Configuration Wizard to migrate the databases and transaction logs from your Exchange servers to the LUNs you configured on your storage system with SnapDrive.

To view or change the database configuration: After the initial configuration, you can rerun the Configuration Wizard at any time to review or make changes to your Exchange data store configuration.

To validate the database configuration: If you add databases or move databases to different LUNs without using SnapManager, run the Configuration Wizard to ensure that the databases are stored in valid locations and to create a mapping between those databases and their respective SnapInfo subdirectories.

Attention

Use the SnapManager Configuration Wizard to move Exchange databases, transaction logs, or storage group system files. SnapManager ensures that these files are place in locations that meet SnapManager configuration requirements. Incorrectly located Exchange database, transaction logs, or storage group system files impairs SnapManager operation. If Exchange System Manager is used to move Exchange database, transaction logs, or storage group system files, run the SnapManager Configuration Wizard after the operation to ensure that these files are in correct locations.

About the Exchange and SnapManager components

When you use the Configuration Wizard, you are specifying the placement of several components of Exchange and SnapManager:

Storage group system path: Path to the directory that contains the Exchange storage group system files. SnapManager places storage group system files on the same LUN that stores the transaction logs for that storage group. The storage group system files must remain where the Configuration Wizard places them.

Storage group databases: The databases in a storage group or store.

Database: The paths for the `.edb` and `.stm` files for the Exchange database. The `.edb` file stores message and attachment content generated by MAPI clients, and message properties such as author, recipients, subject, and priority. The `.stm` file holds native Internet content (for example, MIME).

Transaction log files: The location of the Exchange transaction logs. The transaction logs contain changes made to the Exchange databases since the last backup, enabling an up-to-the-minute restore.

SMTP queue path: The directories used by the SMTP queue.

MTA queue path: The directories used by the MTA queue.

SnapInfo directory: Contains SnapManager backup information, copies of transaction log files, and other data critical to the backup set.

Viewing the placement of Exchange and SnapManager components

To view the current placement of the Exchange and SnapManager components, you can use the Configuration Wizard or the Backup and Verification tab.

Configuration Wizard: To see more information about the databases listed in the Configuration Wizard, highlight the database name (in any of the following screens), and then click Details:

- Where to Move Databases
- Where to Move Transaction Logs
- Where to Move SMTP and MTA System File

Backup and Verification tab: To see more information about the components listed in the left navigation pane of the Backup and Verification tab, select the components and then select View > Properties.

Settings configurable only with the Configuration Wizard

The following table lists SnapManager database management settings that can be configured or changed only through the Configuration Wizard. For each setting, the table lists the name of the corresponding screen in the Configuration Wizard.

SnapManager Setting	Configuration Wizard Screen
Database-LUN mappings	Where to Move Databases
Transaction log file-LUN mappings	Where to Move Transaction Logs
SMTP and MTA file-LUN mappings	Where to Move SMTP and MTA System File
SnapInfo directory location	Where to Put the SnapInfo Directory
Microsoft iSCSI Service as a dependency	Add Microsoft iSCSI Service Dependency

SnapManager Setting	Configuration Wizard Screen
SnapManager event notification enabling for SMTP email, storage system syslog, and AutoSupport	Configure Automatic Event Notification

Using the Configuration Wizard to configure your data store

This topic describes how to use the Configuration Wizard to configure basic SnapManager settings and migrate your Exchange databases to Data ONTAP LUNs so that they can be backed up and restored using SnapManager. See the following procedures for details:

- "Configuring the Exchange data store" on page 118
- "Moving databases using the Configuration Wizard" on page 126
- "Moving transaction logs using the Configuration Wizard" on page 128

Configuring the Exchange data store

This topic describes how to migrate the Exchange data stores.

About the SMTP and MTA queue location: The SMTP and MTA queues are used by Exchange. In general, the location of these files does not matter, as long as they do not reside on the same LUN as the Exchange databases.

- For stand-alone systems, the SMTP and MTA system files can be placed on any disk or LUN that does not contain Exchange databases (the default location of the original local installation disk is acceptable).
- For Windows clusters, the SMTP and MTA system files must be moved to a **shared LUN** that does not contain Exchange databases.

Note

This is the "data directory" that Exchange prompts you to specify when creating a new Exchange virtual server on a cluster. This will become the default system path, and the Configuration Wizard places the MTA and SMTP queues there by default.

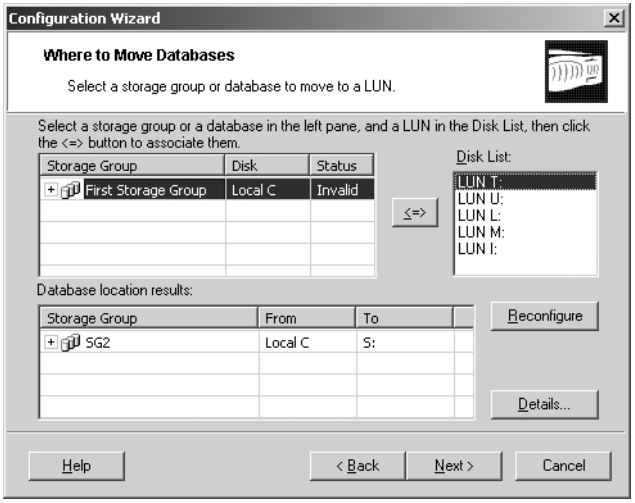
About the Report directories in a Windows cluster: If you want to have one set of report directories no matter what node you are running SnapManager from, move your report directory to a shared disk resource that does not contain Exchange or SnapManager data.

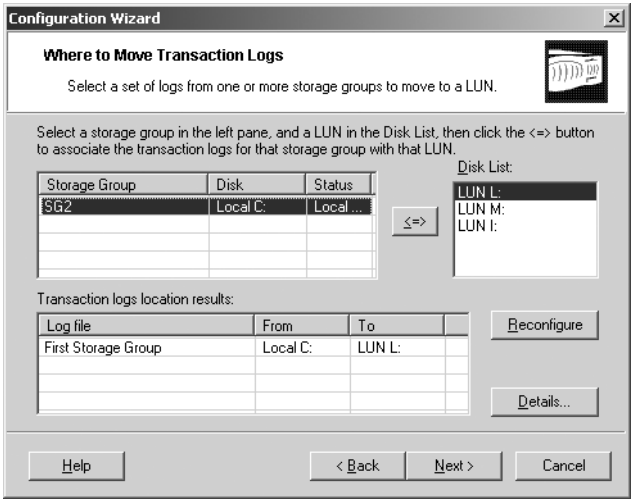
See "Locating the report directory in a Windows cluster" on page 322.

Data store migration procedure: To configure your Exchange data store for SnapManager 3.2 for Microsoft Exchange, complete the following steps.

Step	Action
1	If you have not already done so, start the SnapManager for Exchange application. To do this, go to the Windows Start menu and select Program Files > SnapManager for Exchange. **Result:** The SnapManager for Exchange main window appears.
2	If you want to view or change the Exchange server managed by SnapManager, do this using the Connect to Exchange Server dialog box. To open this dialog box, go to the SnapManager menu bar and select Action > Connect to Another Exchange. For more information, see "Connecting to a different Exchange server" on page 338. **Note** To access the Reports on another Exchange server, you must connect using an Exchange server user account that belongs to the `Administrators` group on that machine. For more information, see Step 2 in "Starting SnapManager and connecting to the default server" on page 64.
3	If the Configuration Wizard is not already started, click the Configuration Wizard button to start it now. **Result:** The Configuration Wizard launches and the Welcome screen appears.
Welcome	
4	To begin the configuration, click Next. **Result:** The Database Verification Server screen appears.

Step	Action
Database Verification Server	
5	Use the Database Verification Server screen to specify the Exchange server to be used to perform Exchange database verification. ◆ If you want to specify the database verification server now, type or browse to an Exchange server in the Verification Server box. **Note** If the computer used for database verification does not have Exchange installed, you must put the necessary files on it. For details, see "Understanding Windows host system requirements" on page 24. ◆ If you want to specify the database verification server later, select the option labeled "Select a verification server later using the Options menu." **Note** You do not need to specify a verification server now. To do so later, when you are ready to select a database verification server, select Options > Database Verification Settings (to open the Verification Settings dialog box). For more information, see "Selecting the database verification server" on page 342.
6	Click Next. **Result:** The Where to Move Databases screen appears.

Step	Action
Where to Move Databases	
7	In the Where to Move Databases screen, associate your Exchange storage groups (Stores) or databases with the correct LUNs according to your SnapManager data configuration plan. For more information about using this window, see "Moving databases using the Configuration Wizard" on page 126. **Example:** In the following example, the SG2 storage group has already been associated with LUN S. When you click the move (<=>) button, the First Storage Group is associated with LUN T, and you can proceed to the next window. 
8	After you associate all databases with a LUN, click Next. **Result:** The Where to Move Transaction Logs screen appears.

Step	Action
Where to Move Transaction Logs	
9	In the Where to Move Transaction Logs screen, associate your transaction logs with the correct LUNs according to your SnapManager data configuration plan. For more information about using this screen, see "Moving transaction logs using the Configuration Wizard" on page 128. **Example:** In the following example, the transaction logs for the First Storage Group have been associated with LUN L. When you click the move (<=>) button, the transaction logs for SG2 will be associated with LUN L also, and you can proceed to the next window. 
10	After you associate all transaction logs with a LUN, click Next. **Result:** The Where to Move SMTP and MTA System Files screen appears.

Step	Action
Where to Move SMTP and MTA System Files	
11	In the Where to Move SMTP and MTA System Files screen, determine the location of your SMTP and MTA system files. **Note** The SMTP and MTA system files cannot reside on a LUN that also contains Exchange databases. For more information about using this screen, see "About the SMTP and MTA queue location" on page 118.
12	After you determine the location of all listed system files, click Next. **Result:** The Where to Put the SnapInfo Directory screen appears.
Where to Put the SnapInfo Directory	
13	In the Where to Put the SnapInfo Directory screen, select the SnapInfo files and the LUN to which you want to move them, and then click the move (<=>) button. For information about using multiple SnapInfo directories, see "About transaction log archiving using NTFS hard links" on page 85 and "About multiple SnapInfo directories" on page 86.
14	Click Next. **Result:** The Add Microsoft iSCSI Service Dependency screen appears.
Add Microsoft iSCSI Service Dependency	
15	If you are installing SnapManager on a stand-alone system that has the Microsoft iSCSI initiator installed, select whether you want to configure your Microsoft iSCSI service as a dependency for the Microsoft Exchange System Attendant. **Note** You are advised to select Yes so that Microsoft Exchange cannot start before the Microsoft iSCSI service is ready to accept connections.

Step	Action
16	Click Next. **Result:** The Configure Automatic Event Notification screen appears.
Configure Automatic Event Notification	
17	Use the Configure Automatic Event Notification screen to configure the automatic event notification options for SnapManager: ◆ Configure automatic SMTP e-mail notification for event notification. ◆ Enable Syslog (storage system event log) support. ◆ Enable AutoSupport for SnapManager. ◆ Limit event logging to failure events After you complete the Configuration Wizard, you can also view or change these settings by selecting Options > Notification Settings to access the Auto Notification Settings dialog box. For more detailed information, see "Using the Auto Notification Settings dialog box" on page 375. **Note** You are advised to enable all of the automatic event notification options; this ensures that, if any problems with your SnapManager backups occur, you are alerted and can take corrective action in a timely manner.
18	Click Next. **Result:** The Completing the Configuration Wizard screen appears.

Step	Action
Completing the Configuration Wizard	
19	Review the configuration summary in the Completing the Configuration Wizard window. If the configuration summary is satisfactory, click Finish to display a list of tasks the Configuration Wizard performs, based on the configuration information you specified. **Result:** The SnapManager Configuration Wizard displays the task list to be used.
Configurator Status	
20	To migrate your databases and their transaction logs and SnapInfo files to the LUNs you specified, click Start Now. **Result:** The SnapManager Configuration Wizard moves the databases and transaction logs to their specified LUNs and displays a task check-off list. **Note** If you are moving the location of Exchange databases in this step, it could take some time to complete. When the migration finishes successfully, SnapManager displays a message box. This message also reminds you to make a backup immediately.
21	Click OK to close the message box.
22	Create a SnapManager backup immediately. Any time you use the Configuration Wizard to move data from one drive to another, backups performed prior to the move become invalid. After you migrate your databases to a new LUN, always perform an immediate backup. For information about creating a SnapManager backup, see “Backing Up Databases with SnapManager” on page 163.

Moving databases using the Configuration Wizard

The SnapManager 3.2 for Microsoft Exchange Configuration Wizard enables you to choose which LUNs will store your Exchange databases when you complete the wizard. You use the Where to Move Databases window to perform these tasks:

- Moving a storage group to a LUN

  For details, see "Moving storage groups to a LUN" on page 126.
- Moving an individual database to a LUN

  For details, see "Moving individual databases to a LUN" on page 126.
- Changing the location of a storage group or database

  For details, see "Changing the location of a storage group or database" on page 127.
- Viewing the full path for your storage groups or databases

  For details, see "Viewing the full path for your database files" on page 127.

Note

The list of available drives changes as you make choices that rule out other choices.

Moving storage groups to a LUN: To put an entire storage group on a single LUN, complete the following steps.

Step	Action
1	In the upper storage group list, select the storage group you want to move.
2	In the Disk List, select the drive letter for the LUN or local disk you want to move the storage group to.
3	Click move (<=>). **Result:** The selected storage group and disk are now associated, and the storage group files will be moved to that disk when the Configuration Wizard moves your data.

Moving individual databases to a LUN: To move an individual database to a LUN, complete the following steps.

Step	Action
1	In the upper storage group list, expand the storage group containing the database you want to move and select the database you want to move.
2	In the Disk List, select the drive letter for the disk you want to move the database to.
3	Click move (<=>). **Result:** The selected database and disk are now associated, and the database file will be moved to that disk when the Configuration Wizard moves your data.

Changing the location of a storage group or database: To change the location of a storage group you already associated with a LUN or local disk, complete the following step.

Step	Action
1	In the Database Location Results, highlight the storage group you want to move and click Reconfigure. **Result:** The selected storage group or database is returned to the list of unconfigured databases and you can reassociate it with any available disk. **Note** If the Exchange system file path for a storage group is currently on the database LUN (placed there for a previous version of SnapManager) and then you use the Configuration Wizard to reconfigure a storage group database path or transaction log file path, then the Configuration Wizard automatically moves the system file path to the same LUN as the transaction log file path.

Viewing the full path for your database files: To view the full path for your database or storage group files, complete the following steps.

Step	Action
1	Highlight a storage group or database in the Database Location Results and click Details. **Result:** The Storage Group Properties window is displayed for the selected storage group.
2	To see the file path for the databases in this storage group, highlight the database and click Details. **Result:** The current paths and file names for the selected database are displayed, along with the new paths and file names if the location of the selected database has changed.

Moving transaction logs using the Configuration Wizard

The SnapManager 3.2 for Microsoft Exchange Configuration Wizard enables you to choose which LUNs will store your Exchange transaction logs when you complete the wizard. You use the Where to Move Transaction Logs window to perform these tasks:

- Moving a transaction log file to a LUN

  For details, see "Moving transaction logs to a LUN" on page 128.
- Changing the location of a transaction log file

  For details, see "Changing the location of a transaction log files" on page 129.
- Viewing the full path for your transaction logs

  For details, see "Viewing the full path for your transaction log files" on page 129.

Note

The list of available drives changes as you make choices that rule out other choices.

Moving transaction logs to a LUN: To put the transaction logs for a storage group on a disk, complete the following steps.

Step	Action
1	In the upper storage group list, select the storage group whose transaction logs you want to move.
2	In the Disk List, select the drive letter for the LUN or local disk you want to move the transaction logs to.
3	Click move (<=>). **Result:** The transaction logs for the selected storage group and LUN are now associated, and the transaction log files will be moved to that LUN when the Configuration Wizard moves your data.

Changing the location of a transaction log files: To change the location of transaction log files you already associated with a LUN, complete the following step.

Step	Action
1	In the Transaction Logs Location Results, highlight the storage group for the transaction files you want to move and click Reconfigure. **Result:** The selected storage group is returned to the list of unconfigured transaction logs and you can reassociate it with any available LUN or local disk.

Viewing the full path for your transaction log files: To view the full path for your transaction log files, complete the following step.

Step	Action
1	Highlight a storage group in the Transaction Logs Location Results and click Details. **Result:** The Properties window is displayed for the selected storage group. The current paths and file names for the transaction logs for the selected database are displayed, along with the new paths and file names if the location of the transaction log files has changed.

Migrating an existing SnapManager for Exchange configuration from using drive letters to using mount points

If you have an existing SnapManager for Exchange configuration that uses **drive letters** to map to Data ONTAP LUNs, you can easily migrate that configuration to a new configuration that uses **volume mount points** instead of drive letters to map to the Data ONTAP LUNs.

Overview

The migration process described in this topic uses both SnapDrive and SnapManager. Although this method will cause any affected storage groups to be taken offline briefly (due to the paths being changed), you will not need to copy the databases themselves from one LUN to another. This saves time and, as a result, minimizes the amount of time that the storage groups are off line.

Note

Not all drive letters are eliminated. A drive letter is used for the mount point root volume.

Configuration guidelines

The following paragraphs describe configuration guidelines for migrating an existing SnapManager for Exchange configuration that uses drive letters to map to Data ONTAP LUNs to a new configuration that uses volume mount points instead of drive letters to map to the Data ONTAP LUNs.

Mount point root: The mount point root can be any of the following:

- The local `C:\` drive
- The LUN that stores the transaction log files
- A separate dedicated LUN

The best practice is to use the LUN that stores the transaction log files, as in the example that follows. Using a separate LUN as the mount point root adds an additional point of failure to the Exchange server.

Note

In Microsoft cluster configurations, the mount point root must reside on a shared storage device such as the transaction logs LUN.

Environments that use more than one storage group: For configurations using more than one storage group, consider using one LUN with a drive letter for the transaction logs of each storage group.

MSCS environments: In Microsoft cluster configurations, the entire Exchange virtual server will be brought offline during a migration even if only a single storage group is migrated. This is because the System Attendant cluster resources requires dependencies on the physical disk cluster resources and taking the the physical disk resource for the transaction logs offline for one storage group will still take the System attendant resource off line and therefore all other storage groups.

Example

Example scenario: The migration process is described in a procedure that uses the following sample configuration:

- A single storage group.
- A single database is located on LUN `I:\`.
- The Exchange transaction logs, MTA and SMTP system files, and the SnapManager SnapInfo directory are collocated on LUN `L:\`.
- The mount point root LUN will require a drive letter, and the LUN containing the transaction logs will be used as the mount point root.

Example procedure: To migrate an existing SnapManager for Exchange configuration from using drive letters to to using mount points, complete the following steps:

Step	Action
1	Launch the Windows Explorer, and then browse to the root of the transaction logs LUN (`L:\`).
2	Using the Windows Explorer, create a folder under the root of `L:\`. In this example, we use a directory name of `database`.
3	Launch the SnapDrive MMC, right click on the database LUN `I:\`, and then select Change Drive Letter and Paths.
4	In Change Drive Letter and Paths, click Add.
5	When prompted, enter the path to the appropriate directory on your mount point root LUN. In this example, we use the directory `L:\database`.

Step	Action
6	To verify that the additional LUN mappings have been successfully created, do one of the following: ◆ Verify that the multiple mappings are reflected in the SnapDrive MMC. In this example, the LUNs show drive letters of `L:\` and t`L:\database\`. ◆ Browse to the root of the mount point root LUN, drive `L:\`. The icon for the folder `database` changes from the standard Windows folder icon to the Windows icon representing a mount point. Double clicking the mount point (directory) name takes you to the root of the mounted LUN rather than to an empty directory on the mount point root LUN. **Note** Do not remove the original drive letter mapping `I:\` yet. For the Configuration Wizard to function properly, SnapManager requires that the original drive letter mappings be in place along with the newly added mount points. Unneeded mappings are removed in a later step.
7	Launch SnapManager for Exchange, and then run the Configuration Wizard.
8	In the Welcome screen, click Next.
9	In the Database Verification Server screen, click Next. **Note** Though changes can be made here if desired, doing so is not part of this example.
10	In the Exchange Server to Configure screen, verify that you are about to configure the correct server, and then click Next.

Step	Action
11	In the Where to Move Databases screen, do the following: **a.** Select the storage group listed in the Database Location Results field, and then click the Reconfigure button. The storage group appears in the list of unconfigured databases, and you can reassociate it with any available disk. **b.** Select `LUN L:\database\`, and then click the move (<=>) button to associate the database with the new path. The storage group appears in the Database Location Results field again. The old drive letter `LUN I` appears under the From column. The new mount point path `L:\database\:` appears under the To column. **c.** Click Next.
12	In the Where to Move Transaction Logs screen, click Next.
13	In the Where to Move SMTP and MTA System Files screen, click Next.
14	In the Where to Put the SnapInfo Directory screen, click Next.
15	Keep clicking Next to proceed through the next few screens, making additional configurations if desired. At the final screen, click Finish. **Result:** The Configurator Status window appeasr.
16	When you are ready to proceed, click Start Now. **Result:** The databases are taken off line, and the migration proceeds.
17	After the SnapManager Configuration Wizard completes successfully, return to the SnapDrive MMC.
18	Using the SnapDrive MMC, right-click the database LUN `I:\`, and then select Change Drive Letter and Paths.

Step	Action
19	In Change Drive Letter and Paths, highlight the original drive letter for the database LUN (`I:\`) and click Remove. **Result:** The SnapDrive MMC displays the two LUNs `L:\` and `L:\database`.

Understanding SnapManager Backup 8

This section provides background information about SnapManager Backup and SnapManager backup sets. The following topics are covered:

- "How SnapManager Backup works" on page 136
- "How SnapManager backup data is organized" on page 141
- "How SnapManager checks database integrity in backup sets" on page 145
- "Ways to manage the number of backup sets kept online" on page 150
- "Ways to manage the backup and deletion of transaction logs" on page 154
- "When to run a SnapManager backup" on page 157
- "About Exchange options and Exchange System Manager" on page 159

Attention

You must run SnapManager from the system console, not from a Terminal Services client. Do not use Terminal Services for any type of SnapManager administration, because you might miss critical information that is displayed only in pop-up boxes at the system console.

Related topics:

- Chapter 9, "Backing Up Databases with SnapManager," on page 163
- Chapter 10, "Restoring Databases with SnapManager," on page 183
- Chapter 11, "Managing Backup and Restore Snapshots," on page 199

How SnapManager Backup works

SnapManager Backup uses Snapshot functionality to create online, read-only copies of the Exchange databases. After the selected storage groups are backed up, the transaction logs that are already committed to the databases captured in the backup are deleted. For more information, see the following topics:

- "About Exchange storage group sets" on page 136
- "SnapManager minimum unit of backup" on page 136
- "Types of backups SnapManager can perform" on page 137
- "Backup tasks in a Windows 2000 Server environment" on page 137
- "Backup tasks in a Windows Server 2003 environment" on page 138
- "Transaction log backups can contain two Snapshot copies per backup" on page 138

About Exchange storage group sets

Exchange storage groups (Stores) stored on a single volume that belong to the same Exchange server are referred to collectively as a "storage group set". When you select an Exchange storage group for backup, all storage groups composing its storage group set are automatically selected for backup.

SnapManager Backup backs up the complete set of storage groups—all of which constitute the storage group set—in parallel. (Thus, these storage groups share the same backup name and date-time stamp.)

Note

Even though the backup includes all storage groups in the storage group set, you can still restore the storage groups individually.

SnapManager minimum unit of backup

Although SnapManager supports individual database restore, the minimum unit of backup, or the smallest object you can back up, is an individual **Exchange storage group**.

Note

For easiest administration, it is best to back up all the storage groups in the same Exchange server at the same time.

Types of backups SnapManager can perform

SnapManager Backup performs backups at the volume level:

Volume-wide backup: When a Snapshot copy is taken of a LUN for a SnapManager backup, the entire storage system volume is captured in that Snapshot copy. However, that backup is valid only for that Exchange server. If data from other Exchange servers resides on the same volume, it is not restorable from that Snapshot copy.

Multiple-volume backups: SnapManager performs backups in parallel on all LUNs that belong to the same Exchange server and share a single storage system volume. When a storage group set spans multiple volumes, the resulting backup set contains multiple database Snapshot copies but is still restorable as a single entity.

Partial backups: If the backup of some of the storage groups or databases in the storage group set fails, those in the set that were backed up successfully can still be restored. Because each database constitutes its own backup, or file, it is restored discretely, independent of backups of the others in its storage group set, even though the backup of all databases and storage groups in the set was performed by the backup job.

Backup tasks in a Windows 2000 Server environment

In a Windows 2000 Server environment, SnapManager Backup performs the following tasks when creating a backup. The list of tasks is performed in its entirety for each volume that contains files for the storage groups to be backed up. For example, if two separate volumes are involved, the task list is performed once for the first volume, then again for the second volume.

1. Check the SnapManager license.
2. Rename the most recent SnapInfo directory before a new backup.
3. Rename the previous most rrecent Snapshot copy before a new backup.
4. Create a SnapInfo directory for this backup.
5. Initiate online backup.
6. Back up database files.
7. Create database Snapshot copy.
8. Back up and truncate transaction logs.
9. Create SnapInfo Snapshot copy.
10. Verify physical integrity of the Exchange database files.

11. Delete the oldest SnapInfo Snapshot copies for the deleted backups.
12. Delete any specified older backups.

Backup tasks in a Windows Server 2003 environment

In a Windows Server 2003 environment, SnapManager Backup performs the following tasks when creating a backup. The list of tasks is performed in its entirety for each volume that contains files for the storage groups to be backed up. For example, if two separate volumes are involved, the task list is performed once for the first volume, then again for the second volume.

1. Check SnapManager license.
2. Rename most recent SnapInfo directory, if required.
3. Rename most recent Snapshot copy, if naming is set to “generic”.
4. Create SnapInfo directory for this backup.
5. Initiate VSS backup.
6. Gather Exchange metadata and start VSS Snapshot copy set.
7. Add all required volumes to VSS Snapshot copy set.
8. Create volume shadow copy.

   The transaction logs are backed up and truncated during this step.
9. Verify physical integrity of the Exchange database files.
10. Create SnapInfo Snapshot copy.
11. Delete SnapInfo Snapshot copies for the deleted backups.
12. Delete any specified older backups.

Transaction log backups can contain two Snapshot copies per backup

When SnapManager for Exchange is used in conjunction with Microsoft Exchange Server 2003 on a Windows Server 2003, it uses the Microsoft Volume Shadow Copy Service (VSS) subsystem to provide backup and restore functionality. If, in this environment, the SnapInfo directory has been configured on the same volume as the transaction log, then a single SnapManager backup will create two Snapshot copies on that volume instead of just one:

1. A VSS Snapshot copy in the transaction log. This `exchsnap__*` Snapshot copy is created at the same time as the corresponding database Snapshot copy of the same name.
2. The SnapInfo backup Snapshot copy for protecting the SnapInfo directory. This is the `eloginfo__*` Snapshot copy created at the end of the SnapManager backup. This Snapshot copy is used for transaction log verification and for backup protection. If the backup set was archived, this Snapshot copy, along with the Exchange Snapshot copy, can be used for a SnapManager restore operation.

Note

For VSS backups, the snapshot of the transaction log LUN is used instead of the snapshot of the snapinfo directory LUN to verify the integrity of the transaction logs in the backup during remote database verification operation.

When SnapManager uses VSS for backup and restore functionality and SnapInfo is on the same volume as the transaction log, this is expected behavior.

Suppose the SnapInfo directory is on the same LUN as the transaction log in an Exchange Server 2003 environment with Windows Server 2003. The console output shows that the transaction log volume contains Snapshot copies with the same name as the Exchange database Snapshot copy. Example:

Exchange database Snapshot copy. Example:

```
Volume netappnj1_logs
working...

date         name
____________ ________
Jan 30 01:04 eloginfo__mailnj1__recent
Jan 30 01:00 exchsnap__mailnj1__recent
Jan 29 13:03 eloginfo__mailnj1_08-29-2006_13.00.00__daily
Jan 29 13:00 exchsnap__mailnj1_08-29-2006_13.00.00__daily
Jan 29 01:04 eloginfo__mailnj1_08-29-2006_01.00.00
Jan 29 01:00 exchsnap__mailnj1_08-29-2006_01.00.00
Jan 28 13:03 eloginfo__mailnj1_08-28-2006_13.00.00__daily
Jan 28 13:00 exchsnap__mailnj1_08-28-2006_13.00.00__daily
Jan 28 01:04 eloginfo__mailnj1_08-28-2006_01.00.00
Jan 28 01:00 exchsnap__mailnj1_08-28-2006_01.00.00
Jan 27 15:36 eloginfo__mailnj1_08-27-2006_15.30.15
Jan 27 15:30 exchsnap__mailnj1_08-27-2006_15.30.15
Jan 20 15:35 eloginfo__mailnj1_08-20-2006_15.27.35
Jan 20 15:27 exchsnap__mailnj1_08-20-2006_15.27.35
```

If you are not aware of the configuration details, you might expect to see only the `eloginfo__` Snapshot copies and not the `exchsnap__` Snapshot copies.

Note

Volume size is unchanged because the backup set still captures the same total number of changed blocks on the storage system even though we are using two Snapshot copies instead of one.

How SnapManager backup data is organized

SnapManager stores Exchange backup data in backup sets. See the following topics for more information:

- "SnapManager backup sets" on page 141
- "SnapInfo directory" on page 141
- "SnapInfo subdirectory names" on page 142
- "SnapManager backup set names" on page 142
- "SnapManager Snapshot copy naming conventions" on page 142
- "Exchange database Snapshot copy names" on page 143
- "SnapInfo directory Snapshot copy names" on page 144

SnapManager backup sets

A SnapManager backup set, sometimes called just the "backup set", consists of all data that you would need to be able to perform a restore, regardless of whether this data exists on the same LUNs or volumes. A backup set contains the following items from the same backup set:

- Exchange databases
- Exchange transaction logs
- SnapInfo directory

SnapInfo directory

The SnapInfo directory stores information about each storage group set created by SnapManager Backup, copies of transaction log files, and other data critical to the backup set. The location of this directory is specified when you run the Configuration Wizard. By default, the directory name is `SME_SnapInfo`. However, you can specify a different directory name.

By default, the SnapInfo directory is on the LUN that stores the Exchange transaction log files, but this is not a requirement. The SnapInfo directory cannot reside on the same LUN that stores the Exchange database files.

Every time a SnapManager backup set is created, SnapManager creates a new backup set subdirectory under the SnapInfo directory. SnapManager populates this subdirectory with the transaction logs backed up as part of that backup set, as well as the recovery information for that specific Snapshot copy. A complete backup set consists of this SnapInfo subdirectory and the corresponding Snapshot copies of the LUNs that store the Exchange databases and transaction logs.

SnapInfo subdirectory names

The SnapInfo directory name is `EXCH__` followed by the Exchange server host name:

`EXCH__`*ExchServerName*

For example, the subdirectory for databases belonging to the Exchange server on the Windows host system `CLPUBS-WINSRVR3` would be named as follows:

`EXCH__CLPUBS-WINSRVR3`

SnapManager backup set names

SnapManager backup set names are displayed in the SnapManager Restore tab and in the SnapManager Restore Wizard. These names include the following information about the backed-up databases:

- Server name
- Management group
- Time stamp

SnapManager Snapshot copy naming conventions

The Snapshot copies created by SnapManager backup operations are automatically named by Data ONTAP. The name of each Snapshot copy created during a SnapManager backup operation includes information that identifies the Snapshot copy contents.

Exchange server name: Database Snapshot copy names and SnapInfo directory Snapshot copy names include the name of the Exchange server for which the backup was taken (indicated in this document by the variable *ExchServerName*).

Backup management group: Database Snapshot copy names and SnapInfo directory Snapshot copy names include the backup management group to which you assigned the full database backup. SnapManager provides backup management groups for designating various levels of backup retention: Standard, Daily, and Weekly.

- If you assign a full database backup to the **Standard** backup management group, the Snapshot copy names for the databases and SnapInfo directory do not include a backup management group name.
- If you assign a full database backup to the **Daily** or **Weekly** management groups, the Snapshot copy names for the databases and SnapInfo directory include the name of the backup management group (indicated in this document by the variable *BkpMgmtGrp*).

For more information about using backup management groups, see "Using backup management groups in backup and verification" on page 180.

Most recent backup: Older versions of SnapManager for Exchange (before 3.0) always appended the string `recent` to the name of the most recently created Snapshot copy. This was to allow external scripts, for example archive scripts, to be able to identify and operate on the most recent Snapshot copy.

With the addition of the Run Command After Operation feature in SnapManager 3.0 for Microsoft Exchange, appending `recent` is no longer necessary because the scripts can be integrated into the backup process. For more information about the Run Command After Operation feature, see "Using Run Command After Operation to archive automatically" on page 313.

Starting with SnapManager 3.0 for Microsoft Exchange, SnapManager offers two conventions for naming backup Snapshot copies:

- **Unique backup naming.** The most recent Snapshot copy name contains the Snapshot copy creation date and time (indicated by the variable *date_time*) instead of the string `recent`. The most recent backup is identified by the Snapshot copy name with the most recent date and time. This removes the need for the rename of the Snapshot copy when the next backup is created.
- **Generic backup naming.** The most recent Snapshot copy name contains the string `recent` instead of a date and timestamp. The most recent backup is identified by the Snapshot copy name that includes the string `recent`. This is the Snapshot copy naming convention used by older versions of SnapManager and is the default setting.

The backup naming convention is selected in the Backup Setting dialog box. For information about using this dialog box, see "Managing the backup setting" on page 357.

Note

You are advised to select the unique naming convention option unless you have legacy scripts that require the presence of a backup with "recent" in its name. You need select the unique naming convention explicitly (using the Options > Backup Setting menu or the Backup Naming Convention screen of the Backup Wizard) because, for backward compatibility purposes, the generic naming convention is selected by default.

Exchange database Snapshot copy names

For Exchange database backups, Snapshot copy names begin with the string `exchsnap__`.

Backup management group	Format of the Exchange database Snapshot copy name
Standard	Depending on the naming convention selected: ◆ `exchsnap__`*ExchServerName_date_time* ◆ `exchsnap__`*ExchServerName*`__recent`
Daily or Weekly	Depending on the naming convention selected: ◆ `exchsnap__`*ExchServerName_date_time__BkpMgmtGrp* ◆ `exchsnap__`*ExchServerName*`__recent`

SnapInfo directory Snapshot copy names

For SnapInfo directory backups, Snapshot copy names begin with the string `eloginfo__`.

Backup management group	Format of the SnapInfo directory Snapshot copy name
Standard	Depending on the naming convention selected: ◆ `eloginfo__`*ExchServerName_date_time* ◆ `eloginfo__`*ExchServerName*`__recent`
Daily or Weekly	Depending on the naming convention selected: ◆ `eloginfo__`*ExchServerName_date_time__BkpMgmtGrp* ◆ `eloginfo__`*ExchServerName*`__recent`

How SnapManager checks database integrity in backup sets

SnapManager uses `Eseutil`, a Microsoft Exchange utility, to verify the Exchange database files in a backup set. This utility is installed automatically with Microsoft Exchange in the `\Exchsrvr\bin` directory. SnapManager uses `Eseutil` to verify the **page-level integrity** of the databases in a backup and to verify that the databases in a backup and the transaction logs associated with that backup have not incurred **physical-level corruption**. For more information about physical and logical level corruption, see your Microsoft Exchange documentation.

For more information about how SnapManager checks database integrity in backup sets, see the following topics for more information:

- "LUN requirements for verifying the databases in a backup set" on page 145
- "Managing database verification load" on page 146
- "Options for when to verify the databases in a backup set" on page 147
- "Options for where to run Microsoft Eseutil" on page 148
- "Viewing backup verification status" on page 148

Attention

You are strongly advised to restore only from backups whose databases have been verified. By default SnapManager Restore requires that you restore only from verified backups. However, you can override this requirement. For details, see "Overriding database verification during restore" on page 354.

LUN requirements for verifying the databases in a backup set

When you verify the databases in a backup set, Microsoft `Eseutil` requires that all of the databases files are mounted at the same time. At a more granular level this means that SnapManager, using SnapDrive commands, mounts all the LUNs that contain the backup sets selected for database verification. Each LUN that will be mounted requires one available drive letter or mount point.

To run the `Eseutil` command, the verification server (whether local or remote) must have a sufficient number of drive letters or mount points available to mount all the LUNs that store the database backup sets you are verifying.

Verifying database backups stored on a single LUN or across multiple LUNs: To run database verification against backup sets that are stored on a single LUN or across multiple LUNs, the Exchange server that is used as the verification server must have at least one drive letter or mount point available for every LUN so that the LUNs can be mounted.

Verifying multiple backup sets using a remote verification server: To run SnapManager remote verification for more than one backup set in a single job, two unassigned drive letters or mount points must be available. In all other situations, only one unassigned drive letter or mount point is required.

The extra drive letter or mount point is for mounting the LUN in a Snapshot copy that stores the SnapInfo directory for the purpose of transaction log verification (a feature introduced in SnapManager 3.1 for Microsoft Exchange). After SnapManager verifies the transaction logs for the first backup set, it does not dismount LUN or release the assigned drive letter for this LUN. This saves an extra, unnecessary LUN mounting operation for the verification of the transaction log for the second backup set.

Before you perform remote verification for more than one storage group in a single job, check that a second drive letter or mount point is available. If this is not possible, you must schedule the backup or verification jobs to verify one backup set at a time.

Managing database verification load

Running database verification on a production Exchange server (the Windows host system running the Exchange virtual server used to create the databases) can place a significant load on both the Exchange server and the Data ONTAP storage system. For this reason, verification can degrade Exchange response, particularly during peak work hours.

There are three ways to manage database verification load. The first two methods involve separating the database verification and database backup operations, thereby distributing the load; you can defer database verification, or you can run database verification from another Exchange server. A third method, available only if you are running SnapManager 3.2 with Microsoft Exchange 2003 SP2, is to slow down the database integrity verification process to decrease the load on the Windows host and the storage system.

The following paragraphs describe all three methods of managing database verification load.

Deferred database verification: By default, a SnapManager full database backup operation runs `Eseutil` immediately after the backup is finished. Instead of allowing a database backup to automatically verify the databases when the operation is finished, you can disable that feature. You can then run a separate database verification operation any time after the full database backup operation is finished. To perform a deferred verification, select the “Verify databases and

transaction logs in the most recent unverified backups" operation in the SnapManager Backup Wizard or the Backup and Verification tab. For details, see "Backing up databases" on page 164.

Remote database verification: To prevent database verification from affecting the performance of your production Exchange server, you can run verification on another Exchange server. For details, see "Requirements for a remote verification server" on page 27 and "Selecting the database verification server" on page 342.

Eseutil throttling: SnapManager 3.2 introduces a third option for managing database verification, that you can combine with either or both of the existing options, to reduce the load even further. When installed with Microsoft Exchange 2003 Service Pack 2, SnapManager 3.2 supports the ability to throttle `Eseutil` (the Microsoft Exchange consistency checker utility) in database checksum verification mode so that database verification takes longer to finish. For details, see "Configuring Eseutil throttling for database verification" on page 348.

Options for when to verify the databases in a backup set

You can verify the databases in your SnapManager backup sets at various times.

Automatically verify full database backup sets upon creation: By default, SnapManager verifies the databases in a backup set at the time the backup is created. This is simple and ensures that each database in the backup set is verified. However, this method significantly increases the time required to complete the backup. For a description of how to start or schedule database backup with automatic database verification, see "Backing up databases" on page 164.

Explicitly start or schedule database verification only: With this method, a single operation can be initiated to verify the databases contained in one or more backup sets that have already been created. You can start the verification immediately, or you can schedule the verification to occur later, when it does not affect performance or delay later backups. For a description of how to start or schedule database verification, see "Verifying backup databases" on page 176.

Defer verification until you restore from the backup set: If you attempt to restore from a backup set on which a database consistency check has not been run successfully, SnapManager prompts (but does not require) you to first verify the databases in that backup set. See "Importance of verifying databases to be restored" on page 186.

Note

Database verification is performed on a LUN backed by Snapshot copy. If you take a Snapshot copy of a volume while a LUN backed by Snapshot copy exists, you create a "busy Snapshot copy," which might cause problems when you attempt to delete Snapshot copies. To avoid this, do not schedule backups while a verification is in progress.

Options for where to run Microsoft Eseutil

Regardless of when you verify the databases in a backup set, the verification can be done on the production Exchange server or on a remote verification system.

From the production Exchange server: In the simplest SnapManager configuration, verification is run from the production Exchange server. However, because the Microsoft `Eseutil` command used for the verification is CPU-intensive, performing the verification on the production Exchange server host system during peak usage could affect Exchange performance.

From a remote verification server: Performing the verification on a remote system minimizes the impact of verification on Exchange system resources and backup schedule. To prevent verification from affecting the performance of your production Exchange server, you can run verification on another computer.

Viewing backup verification status

SnapManager Restore shows you a list of the backups that have been taken. For each backup, the date and time of the backup is displayed, as well as one of these symbols:

- Green check-mark

  The databases in backups shown with this symbol are verified.
- Yellow question mark

  The databases in backups shown with this symbol are not verified.
- Red exclamation mark

  The databases in backups shown with this symbol failed verification and cannot be restored.
- File with a red exclamation mark

  The databases in backups shown with this symbol are verified, but the transaction logs for the backup failed verification. If you need to restore from backups with this symbol, contact technical support.

Note

You can also determine whether the transaction logs for a specific backup have been verified by opening the Restore tab and selecting that backup. The transaction log verification status is displayed as part of the backup information in the right pane.

Ways to manage the number of backup sets kept online

When planning your SnapManager backup schedules, you also need to manage the number of Snapshot copy-based backup sets that are stored online. See the following topics for more information:

- "Maximum number of Snapshot copies per volume" on page 150
- "Criteria used to delete backups" on page 151
- "Automatic deletion of backups in a management group" on page 151
- "Explicit deletion of backup Snapshot copies" on page 153

Maximum number of Snapshot copies per volume

The Data ONTAP software used with SnapManager 3.2 for Microsoft Exchange supports a maximum of 255 Snapshot copies per storage system volume.

Note

Snapshots not created by SnapManager also count toward this total.

Because each SnapManager backup operation creates Snapshot copies, a SnapManager backup operation will fail if the storage system volume that contains the database LUN exceeds the 255 Snapshot copy capacity.

To avoid reaching the limit of 255 Snapshot copies per volume, delete your old SnapManager backups when they are no longer needed. SnapManager provides two ways to delete backups:

Automatic deletion of older backups in the management group: This is a SnapManager Backup option that you can select when you start or schedule a backup operation. This is the recommended method for managing the number of Snapshot copies you store on your system.

Explicit deletion of backups or SnapInfo Snapshot copies only: This is an action you can take, independent of the backup operation, to delete individual or multiple backup Snapshot copies. You can use the explicit deletion facility to delete any of the following items:

- Entire backup sets that are assigned to a specific backup management group
- Only the SnapInfo directory Snapshot copies that are assigned to a specific backup management group
- Snapshots of LUNs created during a restore operation

Criteria used to delete backups

You can delete backups using an age-based criteria or a quantity-based criteria.

Age-based Snapshot copy deletion: You can automatically or explicitly delete backups that are assigned to a particular backup management group and that are older than a specified number of days. This deletion criteria is specified by selecting the "Delete backups older than" box and then entering **the number of days for which you want to keep the most recent backups** for the backup management group.

- Procedural details for specifying this criteria for automatic deletion are included in "Backing up databases" on page 164.
- Procedural details for specifying this criteria for explicit deletion are included in "Managing Backup and Restore Snapshots" on page 199.

Quantity-based Snapshot copy deletion: You can automatically or explicitly delete backups that are assigned to a particular backup management group so that only a specified number of backups remain for that backup management group. This deletion criteria is specified by selecting the "Delete (oldest) backups in excess of" box and then entering **the number of the most recent backups you want to keep** for the backup management group.

- Procedural details for specifying this criteria for automatic deletion are included in "Backing up databases" on page 164.
- Procedural details for specifying this criteria for explicit deletion are included in "Managing Backup and Restore Snapshots" on page 199.

Note

It is possible for the total number of Snapshot copies on a volume to exceed the number of SnapManager backups being retained. For example, if a single volume contains both the SnapInfo directory and the Exchange databases, each SnapManager backup generates two Snapshot copies on that volume.

Automatic deletion of backups in a management group

When you start or schedule a database backup job, you can specify a backup deletion criteria (based on Snapshot copy age or quantity) that SnapManager uses to automatically delete the oldest backups for that **storage group** and **backup management group** after the backup is finished. If you choose one of the automatic deletion criteria, SnapManager retains only the backups created within a certain number of days or only the number of backups you specify.

Note

Automatic deletion of older backups in a management group is the recommended method for managing the number of Snapshot copies stored on your system.

For more information about backup management groups, see “How backup management groups are used” on page 180.

Attention

Do not use SnapDrive or the storage system administration tools to delete Snapshot copies created by SnapManager. Doing so will leave behind unwanted data that cannot be removed.

What is deleted by automatic deletion: Automatic deletion deletes only backups with the following characteristics:

- Its backup management group is the same as the type just created.
- It has the prefix `exchsnap__` (database backup) or `eloginfo__` (transaction logs backup).
- It is the oldest backup for this storage group of this type.
- If it is not deleted, there would be more backups of this backup retention level than you specified in the “Delete backups older than” box or the “Delete backups in excess of” box.

What is preserved by automatic deletion: SnapManager does not count backups that failed verification when counting the number of stored backups. Therefore, more backups might be preserved than you specify in the “Delete backups older than” or “Delete backups in excess of” box. For example, suppose you are backing up storage groups A and B, that reside on the same volume and which contain the following backup sets.

SnapManager backup set	Description
Storage Group A on volume 1	
`exchsnap__orbit3_01-23-2006_16.21.07`	Old backup—good
`exchsnap__orbit3__recent`	Recent backup—good
Storage Group B on volume 1	
`exchsnap__orbit3_01-23-2006_16.21.07`	Old backup—good
`exchsnap__orbit3__recent`	Recent backup—inconsistent

Also suppose you have set the “Delete backups in excess of” box to `2` to preserve the most recent two backup sets.

In order to preserve two good backups for Storage Group B, SnapManager will not delete the Snapshot copy `exchsnap__orbit3_01-23-2006_16.21.07`. Therefore, because both storage groups reside on the same volume, three backups for Storage Group A remain instead of two.

What else can be protected from automatic deletion: For any backup job in which you use automatic deletion, you can also choose to ensure that the deletion is limited so as not to create a break in the continuity of transaction logs between the previous backup and the present time. Doing so allows you to retain up-to-the-minute restore ability for older backups from other management groups. See "Option to retain up-to-the-minute restore ability" on page 155.

Explicit deletion of backup Snapshot copies

For any explicit deletion of backups, you can choose to delete backups or delete Snapshot copies of LUNs created during a restore operation. When you choose to delete backups, you can also choose to ensure that the deletion is limited so as not to create a break in the continuity of transaction logs between the previous backup and the present time. Doing so allows you to retain up-to-the-minute restore ability for older backups from other management groups. See "Option to retain up-to-the-minute restore ability" on page 155.

Explicit deletion of an individual backup: With this method, you delete individual selected Snapshot copies for either full database backups or transaction logs. The procedures are described in "Explicitly deleting an individual backup" on page 209.

Explicit deletion of multiple backups: With this method, you select a database to be deleted, the types of backup set components to be deleted (full database backups or SnapInfo directory backups), and the type of backup management group to be deleted. The procedure is described in "Explicitly deleting storage group backups" on page 200.

Note

You can also explicitly delete the LUN Snapshot copies that were created during a restore operation. For a description of **restore Snapshot copies**, see "Understanding SnapManager Restore" on page 184. For a description of how to view and delete these Snapshot copies, see "Explicitly deleting Snapshot copies created by SnapManager Restore" on page 205.

Ways to manage the backup and deletion of transaction logs

SnapManager provides advanced options that allow you to manage the **transaction logs** associated with the backup management group.

- For any backup job, you can choose to skip the **backup** of transaction logs that Exchange will truncate after the SnapManager Backup operation finishes.

  See "Option to back up transaction logs that Exchange will truncate" on page 154.
- When you delete backup Snapshot copies (whether automatically or explicitly), you can choose to skip the **deletion** of Snapshot copies of LUNs that contain transaction logs related to the selected backup management group, if deleting those logs would that break the continuity of transaction logs between the previous backup and the present time.

  See "Option to retain up-to-the-minute restore ability" on page 155.
- When you explicitly delete backup sets (or related SnapInfo Snapshot copies) that contain selected storage groups, you can expand the scope of the deletion to include backups that contain **only some** of the selected storage groups (in addition to backups that contain **all** of the selected storage groups).

  See "Explicitly deleting backups and SnapInfo Snapshot copies" on page 200.

Option to back up transaction logs that Exchange will truncate

By default, SnapManager Backup jobs back up selected database files and all associated transaction logs. This part of the backup process also entails creating a database Snapshot copy, truncating transaction logs (by removing any entries already committed to the database), and creating a SnapInfo Snapshot copy.

If you do not need to retain up-to-the-minute restore ability from a backup that is not the most recent, you can reduce the amount of disk space that is consumed by transaction log backups by choosing to skip the backup of transaction logs that Exchange will truncate after the SnapManager Backup operation finishes.

This feature is managed using the "Back up transaction logs that will be truncated by Exchange at the end of the backup" option in the Advanced Options dialog box.

- The option to back up all transaction logs (including those that Exchange will truncate after the backup operation finishes) is selected by default.

- When this option is deselected (so that you do not back up transaction logs that Exchange will truncate after the SnapManager Backup operation finishes), database and transaction log verification cannot be deferred.

This option is automatically selected the next time SnapManager is started.

Option to retain up-to-the-minute restore ability

If you delete backups that are not the oldest backups in your backup list, and the corresponding transaction logs are also deleted, this makes the older remaining backups no longer available for an up-to-the-minute restore. The reason is that the transaction logs are no longer contiguous from the time when the older backup was taken to the present time. This can happen when you are deleting backups of a particular backup management group.

When you automatically or explicitly delete backups for a backup management group (whether based on Snapshot copy age or quantity), you also have the option to ensure that this is done without creating a break in the continuity of transaction logs between the previous backup and the present time. Limiting the backup deletion in this way allows you retain the ability to use the older backups in an up-to-the-minute restore.

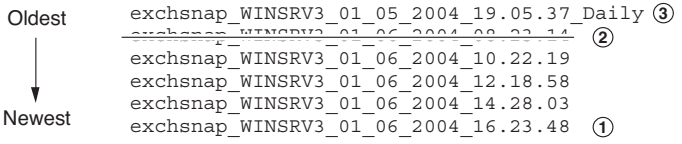
- To enable this safeguard, use the "Retain up-to-the-minute restore ability for older backups in other backup management groups" option in the Advanced Options dialog box, at the cost of using more space on your storage system for the logs that are not deleted. This option is selected by default.
- If you know you will not need to perform an up-to-the-minute restore from the older backups, then you should allow the logs to be deleted in order to free up more space on the storage system holding the backups. This option is automatically selected the next time SnapManager is started.

Example: As an example, suppose that you have the following backups stored:




```
exchsnap_WINSRV3_01_05_2004_19.05.37_Daily
exchsnap_WINSRV3_01_06_2004_08.23.14
exchsnap_WINSRV3_01_06_2004_10.22.19
exchsnap_WINSRV3_01_06_2004_12.18.58
exchsnap_WINSRV3_01_06_2004_14.28.03
```

Now, you perform a Standard backup, and specify that only the four most recent Standard backups be retained. After this backup is complete, the oldest Standard backup is deleted, and the daily backup becomes point-in-time only:



① New Standard backup created
② Oldest Standard backup deleted
③ Daily backup becomes point-in-time only

To avoid this situation, you can enable the “Retain up-to-the-minute restore ability for older backups in other backup management groups” option.

About using only one backup management group: If all backups have the same backup management group designation, deselecting this option has no effect. That is, the SnapInfo directories (transaction logs) will be deleted according to the “Delete backups” setting, and the “Retain up-to-the-minute restore ability” option is effectively ignored.

For more information about using backup management groups, see “Using backup management groups in backup and verification” on page 180.

When to run a SnapManager backup

You need to balance frequency of backups against any overhead incurred by the database verification process. In addition, you must ensure that no SnapManager operations overlap with each other. See the following topics for more information:

- "Backing up databases following data migration" on page 157
- "Best time to run a SnapManager backup" on page 157
- "Frequency of backups" on page 157
- "Recommendations for scheduling backups" on page 158

Backing up databases following data migration

At the end of the Exchange database and transaction log migration process, the Configuration Wizard reminds you to make an immediate backup of the Exchange databases. Making an immediate backup of the Exchange databases is critical because any previous non-SnapManager backups will no longer be valid.

Best time to run a SnapManager backup

To minimize the impact of a SnapManager backup on Exchange client response time, it is best to run the Exchange database integrity verification of a SnapManager backup operation—the most CPU-intensive part of the backup—during off-peak Exchange usage hours, or from a remote machine. Typically, off-peak times are between 6:00 p.m and 7:00 a.m.

Note

To avoid degrading the performance of your production Exchange server, run your database verification operations on a remote server.

Frequency of backups

You do not have to perform multiple SnapManager full backups every day, but the more you do, the fewer Exchange transaction logs need to be played forward at restore time. At a minimum, you should perform one SnapManager full database backup every 24 hours.

Recommendations for scheduling backups

The more often you create SnapManager backups, the fewer Exchange transaction logs there are to be played forward at restore time, resulting in a faster restore. However, for best results, observe the following recommendations for scheduling backups and verifications:

- Do not schedule any SnapManager operations to overlap each other. Only one SnapManager operation can be running on the same machine at the same time.
- Do not schedule a backup to occur while a database verification is being performed, even if the verification is performed on a remote verification machine. This can result in a backup that cannot be deleted easily. For more information about this problem, see "Problem deleting backups due to busy Snapshot copy error" on page 211.
- Do not schedule verifications on the Exchange server during peak usage hours. The verification process is CPU-intensive and could degrade Exchange performance if run on the Exchange server during peak usage hours.

One way to conform to the preceding recommendations is to schedule your backups to occur during peak usage hours, and then use the off-peak hours to perform database integrity verifications.

Note

If you are scheduling backups in a Windows cluster, schedule them on only one node. If the Exchange virtual server fails over to another node, the node that takes over that virtual server performs the backup as scheduled. If the entire node fails, you need to set up the backup schedule again.

About Exchange options and Exchange System Manager

This topic describes considerations for using certain Exchange and Exchange System Manager features in a SnapManager environment:

- "Moving Exchange data" on page 159
- "Displaying the time of the last full backup" on page 159
- "Triggering Exchange page zeroing and deleted item retention" on page 160

Moving Exchange data

To display the time of the last full backup of a given database, use the **SnapManager Configuration Wizard** rather than Exchange System Manager.

Attention

Do not use the Exchange System Manager to move Exchange databases or transaction logs for any Exchange system that has been configured using SnapManager. Doing so prevents SnapManager from functioning correctly.

Displaying the time of the last full backup

To display the time of the last full backup of a given database, use the **SnapManager Restore tab** rather than Exchange System Manager.

Note

When managing an Exchange 2000 server from a machine that has the Exchange Server 2003 version of Exchange System Manager installed and non-VSS Snapshot copies are used, ESM might not display the date of the last backup. For details, see "About Exchange System Manager" on page 160.

Using the SnapManager Restore tab: To view the time of the last full backup using the SnapManager Restore tab, complete the following steps.

Step	Action
1	In the SnapManager user interface, select the Restore tab.
2	In the left navigation pane, click to expand the view for the Exchange server name (if needed).
3	In the left navigation pane, double click the storage group name to expose the available backup sets.

Step	Action
4	In the left navigation pane, double click the backup set name to display its properties in the right pane.
5	Note the time stamp information included in the right pane: **Name:** Displays the backup set name. If SnapManager is configured to use **unique** backup naming (the default setting) as opposed to **generic** naming, the backup name includes the date and time stamp. **Backup Date and Time:** Displays the date and time at which the backup was taken.

About Exchange System Manager: The version of Exchange System Manager (ESM) that ships with Exchange Server 2003 supports a new feature that allows the administrator to view the last time that a full backup of particular Exchange database took place. This time stamp information is displayed on the database Properties page in the "Time of last full backup" field. ESM 2003 can be used to manage both Exchange 2000 and Exchange 2003 servers.

For an Exchange 2003 database, ESM 2003 displays a date and time stamp, whether the backup was taken with SnapManager for Microsoft Exchange (VSS Snapshot copy) or via a streaming method such as NTBackup.

For an Exchange 2000 database, ESM 2003 displays a time and date stamp only if the backup was created using a streaming type of backup application such as NTBackup. ESM 2003 does not display a time and date stamp if you are managing an Exchange 2000 server from a machine that has the Exchange Server 2003 version of ESM installed and non-VSS Snapshot copies are used. This is because SnapManager 3.2 for Microsoft Exchange supports Exchange 2000 on Windows 2000 Server (but not on Windows Server 2003), and VSS Snapshot copies are not available in Windows 2000.

Triggering Exchange page zeroing and deleted item retention

Exchange includes the following two optional features that depend on the complete read of every database page during a backup:

- **Page zeroing** is used by high-security installations. This feature provides the ability to zero out database pages that were deleted.
- **Deleted item retention** settings enables you to mark items and mailboxes for deletion after they are backed up.

Attention

If you need to ensure that deleted items are archived into at least one backup set, select the "Do not permanently delete mailboxes and items until the store has been backed up" option. However, be aware that this option overrides the "Deleted item retention" intervals for items and mailboxes. Therefore, to be able to recover deleted items without having to restore and extract Exchange data from tape, do not permanently delete mailboxes and items until the store has been backed up.

Because SnapManager uses Snapshot technology, and therefore does not read every page during a backup, these features are not triggered when only SnapManager is used to perform backups.

You can cause these Exchange features to be triggered by scheduling a periodic backup using a standard backup utility, such as NTBackup, and that the extra backup operation adheres to the following characteristics:

- Make sure that the backup you use for this purpose is a **copy** or **differential** backup. Performing any other type of backup causes existing SnapManager backups to become unusable for up-to-the-minute restores.
- Make sure that the extra backup operation is not performed at the same time as a SnapManager backup.

Backing Up Databases with SnapManager 9

This section describes how to back up Exchange database storage sets with SnapManager Backup. The following topics are covered:

- "Backing up databases" on page 164
- "What to do if your SnapManager backup fails" on page 173
- "Verifying backup databases" on page 176
- "Using backup management groups in backup and verification" on page 180

Attention

You must run SnapManager from the system console, not from a Terminal Services client. Do not use Terminal Services for any type of SnapManager administration, because you might miss critical information that is displayed only in pop-up boxes at the system console.

Related topics:

- Chapter 8, "Understanding SnapManager Backup," on page 135
- Chapter 10, "Restoring Databases with SnapManager," on page 183
- Chapter 11, "Managing Backup and Restore Snapshots," on page 199

Backing up databases

You can create or schedule a SnapManager backup using the SnapManager Backup Wizard or the Backup and Verification tab. See the following topics for more information:

- "Information you need to specify for a backup" on page 164
- "Backing up using the SnapManager Backup Wizard" on page 165.
- "Backing up using the Backup and Verification tab" on page 167.

Information you need to specify for a backup

To perform a SnapManager backup, provide the following information:

- What storage groups (Stores) you want to back up
- What backup management group you want to assign to this backup

  For details, see "How backup management groups are used" on page 180.
- Whether you want to use the unique naming convention

  For details, see "Managing the backup setting" on page 357.
- Whether you want to automatically delete the oldest backups of this backup management group

  For details, see "Automatic deletion of backups in a management group" on page 151.
- Whether you want to back up transaction logs that will be truncated by Exchange at the end of the backup

  For details, see "Option to back up transaction logs that Exchange will truncate" on page 154.
- Whether you want to retain up-to-the-minute restore ability for any backups from other backup management groups that are older than backups you will be deleting

  For details, see "Option to retain up-to-the-minute restore ability" on page 155.
- Whether you want to verify the backup databases and transaction logs after the backup is created

  Although it is possible to restore from an unverified backup, you are strongly advised to restore only from verified backups.
- Whether you want the mirror to be updated after the backup (if the volumes you are backing up to are SnapMirror sources)

  For details, see "How SnapMirror replication works" on page 217.
- Whether you want to run a command after the backup is complete

For details, see "Using Run Command After Operation to archive automatically" on page 313.

- Whether you want to run the backup now or schedule it for later
- If you want to schedule the backup to run later, the job scheduling information

Backing up using the SnapManager Backup Wizard

To back up the Exchange databases using the SnapManager Backup Wizard, complete the following steps.

Step	Action
1	In the SnapManager for Microsoft Exchange main window, click the SnapManager Backup Wizard icon.
2	Click Next. **Result:** The Databases to Back Up or Verify screen appears. The Microsoft Exchange Servers navigation tree in the left panel lists the Exchange data stores that are managed from the current Exchange server. ◆ Storage groups or databases that reside on the same volume are shown with disk icons of the same color. ◆ Storage groups or databases that span multiple volumes are shown with disk icons with three colors. ◆ Storage groups or databases that cannot be backed up by SnapManager are listed with the label `Invalid` next to the LUN drive letter or mount point.
3	Follow the instructions in the Backup Wizard to initiate your backup. For a list of information you need to provide as you complete this step, see "Information you need to specify for a backup" on page 164.
4	At the Completing the Backup Wizard dialog box, click Finish after you verify that all the settings in the window are true. **Result:** The Backup Status window appears.

Step	Action
5	In the Backup Status Window, click Start Now to start the backup. **Result:** The backup is performed and the Snapshot copy is written to the volume. SnapManager Backup completes each task and checks it off on the list shown in the Backup Task List view. You can switch back and forth between the task check-off list and the progress report using the Switch buttons on either window. If the backup is successful, the Task view shows the check-off list with the tasks completed. **Note** If Notification is enabled, e-mail is sent and the event is posted to the Windows event log.

Backing up using the Backup and Verification tab

To back up your Exchange data store using the Backup tab, complete the following steps.

Step	Action
1	In the SnapManager interface, select the Backup and Verification tab. **Result:** The Backup and Verification tab is activated. The Microsoft Exchange Servers navigation tree in the left panel lists the Exchange data stores that are managed from the current Exchange server. ◆ Storage groups or databases that reside on the same volume are shown with disk icons of the same color. ◆ Storage groups or databases that span multiple volumes are shown with disk icons with three colors. ◆ Storage groups or databases that cannot be backed up by SnapManager are listed with the label `Invalid` next to the LUN drive letter or mount point.
2	In the Backup window, select the storage groups (Stores) you want to back up.
3	In the Backup Management Group field, select the management group for the backup you want to create. For more information about backup management groups, see "How backup management groups are used" on page 180.

Step	Action
4	If you want to delete older backups of this backup management group automatically, select one of the “Delete backups” options in the Advanced Options dialog box. **Note** Make sure to select the one of the “Delete backups” options to manage your Snapshot copies. If you do not select automatic backup deletion, backups will be retained indefinitely. This would require manual removal of backups, or sufficient storage capacity for all backups and transaction logs. For more information, see “Automatic deletion of backups in a management group” on page 151 and “Explicit deletion of backup Snapshot copies” on page 153.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>5</td><td>By default, automatic deletion of older backups within a backup management group is done selectively, in such a way that it does not cause a break in the continuity of transaction logs between the previous backup and the present time.

However, if you do not need to retain up-to-the-minute restore ability from a backup that is not the most recent, you can allow the automatic deletion feature to delete all older backups within the backup management group. This reduces storage system space consumption.

Note
If all backups have the same backup management group designation, deselecting this option has no effect.

For more information, see “Option to retain up-to-the-minute restore ability” on page 155.

To view or change this setting, click Advanced, and then select or deselect the “Retain up-to-the-minute restore ability for older backups in other management groups” option.
<table>
<tr><th>If you want to...</th><th>Then do this...</th></tr>
<tr><td>Avoid creating a break in the continuity of transaction logs (between the previous backup and the present time)</td><td>Select the “Retain up-to-the-minute restore ability for older backups in other management groups” option.

Result: Snapshots of LUNs that contain transaction logs related to this backup management group will not be deleted from the SnapInfo directory.</td></tr>
<tr><td>Reduce storage system space consumption by transaction logs (by allowing more transaction logs to be deleted)</td><td>Deselect the “Retain up-to-the-minute restore ability for older backups in other management groups” option.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>6</td><td>By default, SnapManager backs up selected database files and all associated transaction logs, so that up-to-the-minute restores are possible from all backups.

However, if you do not need to retain up-to-the-minute restore ability from a backup that is not the most recent, you can omit the backup of transaction logs that Exchange will truncate after the backup finishes. To do this, you disable the “Back up transaction logs that will be truncated by Exchange at the end of the backup” option. This reduces the amount of disk space consumed by transaction log backups that Exchange will truncate after the backup finishes.

For more information, see “Option to back up transaction logs that Exchange will truncate” on page 154.

To view or change this setting, click Advanced, and then select or deselect the “Back up transaction logs that will be truncated by Exchange at the end of the backup” option.

<table>
<tr><th>If you want to...</th><th>Then do this...</th></tr>
<tr><td>Retain up-to-the-minute restore ability from a backup that is not the most recent</td><td>Select the “Back up transaction logs that will be truncated by Exchange at the end of the backup” option selected.

This option is automatically selected each time you launch SnapManager.</td></tr>
<tr><td>Reduce the amount of disk space consumed by transaction log backups that Exchange will truncate after the backup finishes</td><td>Deselect the “Back up transaction logs that will be truncated by Exchange at the end of the backup” option.

The option remains disabled only until you exit SnapManager.

Note
Deselecting this option causes SnapManager Backup to also remove the option to defer database verification.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td rowspan="4">7</td><td>If…</td><td>Then…</td></tr>
<tr><td>You want to verify the backup immediately after the backup is complete</td><td>Select the Verify Backed Up Databases and Transaction Logs check box.</td></tr>
<tr><td>You want to verify your backup later</td><td>Do not select the Verify Backed Up Databases and Transaction Logs check box.

See “Deferred database verification” on page 146.</td></tr>
<tr><td colspan="2">Note
Although it is possible to restore from an unverified backup, You are strongly advised to restore only from verified backups.</td></tr>
<tr><td>8</td><td colspan="2">If you want to run a command after the backup is complete, select the Run Command After Operation check box.

This is usually done to archive backups. For details, see “Using Run Command After Operation to archive automatically” on page 313.</td></tr>
<tr><td>9</td><td colspan="2">If your volume is a SnapMirror source volume and you do not want the destination volume to be updated after this backup is complete, clear the Update SnapMirror After Operation check box.</td></tr>
<tr><td rowspan="3">10</td><td>If…</td><td>Then…</td></tr>
<tr><td>You want to run your backup immediately</td><td>Click Backup Now, and then proceed to Step 14.

Result: The Backup Status window appears, showing the Task list.</td></tr>
<tr><td>You want to defer your backup until later</td><td>ClickSchedule to use the Windows Task Manager to schedule your backup, and then proceed to the next step.</td></tr>
</table>

Step	Action
11	In the Schedule Jobs window, name your backup job, provide the user ID and password for the job, then click OK. **Note** If this name already exists as a Windows scheduled task and you want to replace it with a new job, select the Replace if it Exists check box, then click OK. **Result:** The Schedule Job window is displayed.
12	In the Schedule Job window, use the Schedule tab to specify the parameters of your job schedule: ◆ When the job is to run ◆ If you want the job to repeat, at what frequency
13	After you schedule your job, click OK. **Result:** The backup job runs at the times you specified in the Schedule Task view. The backup process is complete. **Note** You can use the Control Panel to modify the schedule or cancel the scheduled job.
14	In the Backup Status window, click Start Now to back up the selected storage groups. **Result:** The backup is performed and the Snapshot copy is written to the volume. SnapManager Backup completes each task and checks it off on the list shown in the Backup Task List view. You can switch back and forth between the task check-off list and the progress report using the Switch buttons on either window. If the backup is successful, the Task view shows the check-off list with the tasks completed. **Note** If Notification is enabled, e-mail is sent and the event is posted to the Windows Application event log.

What to do if your SnapManager backup fails

If your SnapManager backup fails, check the backup report for details about what SnapManager was trying to do when the failure occurred. You can also review the following list of common backup failures:

- "Backups during cluster failovers" on page 173
- "Snapshot limit reached" on page 173
- "SnapInfo directory being accessed" on page 173
- "SnapInfo directory out of space" on page 174
- "Data does not match" on page 174
- "Busy Snapshot copy" on page 174
- "Snapshot already exists" on page 174
- "Out of disk space" on page 174
- "SnapManager server initialization failed" on page 175

Backups during cluster failovers

If a Windows cluster move group or a storage system cluster failover occurs during a SnapManager backup, the backup fails, and you need to restart the backup after the move group or failover is complete.

Snapshot limit reached

If any of the volumes containing the LUNs being backed up reach the Snapshot copy limit of 255, whether those Snapshot copies were created by SnapManager or not, SnapManager backup fails. For more information about the Snapshot copy limit, see "Maximum number of Snapshot copies you can retain" on page 12.

Note

Automatic backup deletion is performed only after a successful backup is complete. Therefore, you must be able to create new Snapshot copies before you begin a new backup procedure.

SnapInfo directory being accessed

Because a SnapManager backup might include renaming a SnapInfo subdirectory and Windows does not allow a directory name to be changed while it is being accessed, accessing the SnapInfo directory with a tool like Windows Explorer

could cause the backup to fail. Make sure that you do not hold any exclusive access to the SnapInfo directory on the Exchange host when a backup is performed.

SnapInfo directory out of space

Expand the LUN that contains the SnapInfo directory.

Note

When you expand a LUN, make sure that sufficient space remains in the volume for Snapshot copy creation, so that SnapManager can continue to function correctly. For more information about volume sizing, see "Calculating volume size" on page 104.

Data does not match

You made changes to your Exchange data store since SnapManager was started. You can refresh your view by pressing F5, or you can restart SnapManager.

Busy Snapshot copy

If you initiate a backup when a LUN backed by Snapshot copy exists, the result is a Snapshot copy that cannot be deleted; when you try, you get a "busy Snapshot copy" error and Event 249 is logged by SnapDrive in the event log. This can cause SnapManager backups to fail.

For information about recovering from this error, see "Problem deleting backups due to busy Snapshot copy error" on page 211.

Snapshot already exists

Either of the following circumstances might cause this error to occur:

- The system clock on the host running SnapManager might not be synchronized with the clock on the storage system. These two clocks must be synchronized in order for SnapDrive to function correctly.
- If a SnapMirror replication is running when you attempt to initiate a SnapManager backup, the backup can fail. You can avoid this problem by making sure that any SnapMirror replications have enough time to complete before you initiate another SnapManager backup.

Out of disk space

This error occurs when an out-of-disk-space condition occurs on a storage system volume that stores an Exchange database or transaction log. If this occurs, resize the volume or expand the LUN.

SnapManager server initialization failed

Either of the following circumstances might cause this error to occur:

- You have exited the SnapManager application, but SnapManager.exe or smesrvr.exe processes are still running. To correct this problem, terminate any orphaned SnapManager processes.
- The permissions associated with the SnapManager server account, or the server account itself, have been changed. In this case, SnapManager might not function correctly.

Verifying backup databases

If you created a database backup Snapshot copy without automatically verifying the databases at the time the backup was created, you can verify the databases in that backup as a separate operation. See the following topics for more information:

- "Information you need to specify for a database verification" on page 176
- "Starting or scheduling database verification" on page 178

Attention

If you attempt to perform a database verification (or a backup with database verification) when SnapManager is running from a Terminal Services client instead of from a system console, the operation will fail.

Information you need to specify for a database verification

A database integrity verification job is specified using a combination of parameters.

Job-specific parameters: Each time you start or schedule a database verification, you must specify the following information in either the Backup Wizard or in the Backup and Verification tab:

- The databases for which you want to verify any unverified backup Snapshot copies
- Within the selected databases, the backup management groups for which you want to verify any unverified backup Snapshot copies

  For more information, see "Using backup management groups in backup and verification" on page 180.
- For the selected databases and backup management groups, the number of unverified backup Snapshot copies you want to verify

  Note

  If you request verification of a greater number of unverified Snapshot copies than specified by your database and backup management group selections, the verification will proceed, and therefore all backups will be verified.
- Whether you want to run a command after the backup is complete (usually done to archive backups)

  This feature is typically used to automatically archive a backup, as described in "Using Run Command After Operation to archive automatically" on page 313.

- Whether you want to run the verification now or schedule it for later

Note

If you want to schedule the verification to run later, you also need to know the job scheduling information.

Verification settings: The following list summarizes the settings that pertain to database verification:

- Which Exchange server is used to perform database verification

  This is configured using the Verification Server tab of the Database Verification Settings dialog box, described in "Selecting the database verification server" on page 342.

  If you will be specifying a remote verification server, be sure it is set up properly, as described in "Requirements for a remote verification server" on page 27.

Note

Whether you run database verification either remotely or locally, the verification is performed on a LUN backed by Snapshot copy. If you take a Snapshot copy of the same volume while a LUN backed by Snapshot copy exists, you create a "busy Snapshot copy," which might cause problems when you attempt to delete some Snapshot copies. For this reason, you must be careful not to schedule backups while a verification is in progress. For information about busy Snapshot copies, see "Problem deleting backups due to busy Snapshot copy error" on page 211.

- Which method is used to access database backup Snapshot copies during database integrity verification

  For more information, see "Selecting the Snapshot copy access method for database verification" on page 346.

- *If SnapManager is installed with Exchange 2003 SP2:* Whether to configure throttling of the database checksum verification rate

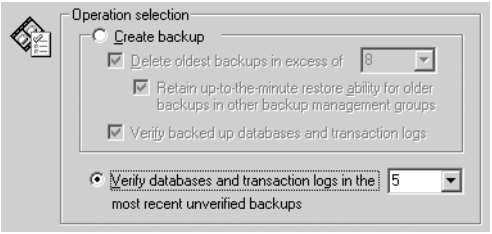
  For more information, see "Configuring Eseutil throttling for database verification" on page 348.

- *If you must restore from an unverified backup:* Whether you want to override the verification requirement for restoring databases from SnapManager backups

  For more information, see "Overriding database verification during restore" on page 354.

Starting or scheduling database verification

To run or schedule database verification, complete the following steps *from the production Exchange server* (not from the remote verification server).

Step	Action
1	On the production Exchange server, click the Backup and Verification tab.
2	Select the storage group (Store) you want to run the verification on.
3	Select the Verify Databases and Transaction Logs in the Most Recent Unverified Backups option. 
4	Select how many of the most recent unverified backups you want to verify. **Note** Only unverified backups are counted. For example, if you select to verify the two most recent unverified backups, and the most recent backup's databases have already been verified, then the two previous backups are verified.
5	In the Backup Management Group field, select the backup management group of the backups you want to verify. If you want to verify the most recent backups regardless of their backup management group, select All.
6	If you want to run a command after the verification is complete, select the Run Command After Operation check box. This is usually done to archive backups. For details, see "Using Run Command After Operation to archive automatically" on page 313.

Step	Action
7	If your volume is a SnapMirror source volume and you do not want the destination volume to be updated after this verification is complete, clear the Update SnapMirror After Operation check box.
8	Click Verify Now, and on the Backup Status window, click Start Now. **Note** To schedule the verification for later, click Schedule instead and follow the prompts in the dialog boxes. **Result:** Verification is run on the databases in the backup you selected. If verification is successful, a dialog box appears telling you so. If any backup database fails verification, delete that backup and create another.

Using backup management groups in backup and verification

When you create a database backup, you have the option to assign it to one of the backup management groups. The database Snapshot copy names and SnapInfo directory Snapshot copy names reflect the management group to which you assigned the backup. The purpose of backup management groups is to enable you to designate various levels of backup retention. See the following topics for more information:

- "How a backup is assigned a backup management group" on page 180
- "How backup management groups are used" on page 180
- "Changing the backup management group" on page 182

How a backup is assigned a backup management group

When you create a backup, you can assign it to any one of the SnapManager backup management groups:

- Standard
- Daily
- Weekly

When you start or schedule a database backup, the Backup Wizard and the Backup and Verification tab prepopulate the backup management group selection field with the Standard group.

The choice of backup management group—combined with the backup Snapshot copy naming convention selected (**unique** or **generic**)—affects the name assigned to the backup Snapshot copy. The name of each Snapshot copy created during a SnapManager backup operation includes information that identifies the Snapshot copy contents. This is described in "SnapManager Snapshot copy naming conventions" on page 142.

How backup management groups are used

The primary purpose of backup management group is to facilitate a database backup strategy. Backup management groups are used to determine which backups are targeted for automatic deletion of older backups, database verification for unverified backup Snapshot copies, and explicit deletion of backups.

For example, when you run or schedule a backup, you can specify how many of the most recent backups you want to retain. Only backups of the specified backup management group are deleted.

Note

The backup management group neither depends on nor enforces how often backups are performed. Backup management groups are only a backup labeling convention that you can assign to a backup set.

Options for a database backup: When you run or schedule a database backup, you can specify how many of the most recent backups you want to retain. Only backups of the specified backup management group are deleted. The procedural details are included in "Backing up databases" on page 164.

Options for a database verification: When you run or schedule a database verification separate from the database backup operation, you can limit the backups you want to verify by specifying a particular backup management group. The procedural details are included in "Verifying backup databases" on page 176.

Options for an explicit deletion of multiple backup Snapshot copies:

When you explicitly delete multiple backups, you can specify that only backups belonging to a certain backup management group be deleted. The procedural details are included in "Explicitly deleting backups and SnapInfo Snapshot copies" on page 200.

Backup example using backup management groups: Suppose your company wants to take regular backups between 7:30 a.m. and 7:30 p.m. You want to keep the last backup of the day and retain it for a few weeks, and you want to keep one backup per week for several months for archiving.

To achieve this using backup management groups, you could use the Standard backup management group for the backups during the day, and use a separate backup job to create one backup in the Daily management group at the end of the day. Then, once a week, you could use another job to create a backup in the Weekly backup management group.

You could then decide how many backups to retain independently for each backup management group. For example, you could keep ten Standard backups, seven Daily backups (one week's worth), and four Weekly backups (one month's worth).

If your Daily or Weekly backup job failed for any reason, you could promote the most recent successful Standard backup to replace the Daily or Weekly backup by changing its backup management group.

Changing the backup management group

Use the Change Backup Management Group dialog box to change the backup management group to which the selected backup set belongs.

To change the backup management group, complete the following steps.

Step	Action
1	In the SnapManager main window, select the SnapManager Restore tab.
2	Select (left-click) the backup whose management group you want to change.
3	Right-click the backup and select Change Management Group from the pop-up menu. **Result:** The Change Backup Management Group dialog box is displayed.
4	Review the backups listed in the Backups Sharing This Snapshot list. **Note** The backup management group for all these backups is changed if you complete this operation. This is because they share a common Snapshot copy.
5	In the New Management Group list, select the backup management group you want to change to. **Note** When you change a backup's backup management group, you also change that backup's name, because the name includes the backup management group.
6	Click OK. **Result:** The backup management group for this backup and all backups listed in the All Backups Sharing This Snapshot list is changed. **Note** The report for the backup management group change is in the Miscellaneous report directory.

Restoring Databases with SnapManager 10

This section describes how to recover data from a SnapManager backup set with SnapManager Restore. The following topics are covered:

- "Understanding SnapManager Restore" on page 184
- "Guidelines for restoring SnapManager backups" on page 190
- "Restoring from a SnapManager backup" on page 192

Attention

You must run SnapManager from the system console, not from a Terminal Services client. Do not use Terminal Services for any type of SnapManager administration, because you might miss critical information that is displayed only in pop-up boxes at the system console.

Related topics:

- Chapter 8, "Understanding SnapManager Backup," on page 135
- Chapter 9, "Backing Up Databases with SnapManager," on page 163
- Chapter 11, "Managing Backup and Restore Snapshots," on page 199

Understanding SnapManager Restore

What SnapManager Restore does

SnapManager Restore enables you to restore your Exchange databases from a backup that you created previously with SnapManager Backup, or from an archive, then optionally recover the databases up to their current state by replaying the associated transaction logs. This would become necessary if your Exchange data became corrupted or unavailable.

SnapManager 3.2 for Microsoft Exchange supports restoring an entire storage group or an individual database.

How SnapManager Restores works

SnapManager Restore uses the following process when restoring from a backup.

Attention

If you are restoring in a Windows cluster, do not attempt to manage any cluster resources while the restore is running.

Stage	Process
1	Checks that the selected backup was verified, or that the Database Verification Override was selected. **Attention** You are strongly advised to restore only from verified backups. For details, see "Importance of verifying databases to be restored" on page 186.
2	Creates a Snapshot copy of the volume containing the storage group or database to be restored, so that the pre-restore state is preserved.
3	Restores the Exchange data from the Snapshot copy of the LUN.
4	Restores the required transaction log for replay.

Stage	Process
5	Uses the Exchange recovery process to play forward transaction logs into the restored databases. **Note** On Windows 2000 Server, the hard recovery process is used. On Windows Server 2003, the soft recovery process is used.

SnapManager Restore types

You can use SnapManager Restore to do either of the following types of restore:

- An up-to-the-minute restore
- A point-in-time restore

Up-to-the-minute restore: In an up-to-the-minute restore, all the transaction logs that were not committed to the databases, from the time the backup set was created up to the most current time, are played forward and applied to the databases. This includes transaction logs from the backup sets, as well as the existing transaction logs in the transaction log directory. A contiguous set of transaction logs is required for an up-to-the-minute restore to succeed.

This option is selected by default.

Example: Suppose you run SnapManager Backup every day at noon, and on Wednesday at 4 p.m. you decide to restore from a previous backup. For some reason, the backup set from Wednesday lunchtime failed verification, so you decide to restore from the Tuesday lunchtime backup. After that backup is restored, all the transaction logs are played forward and applied to the restored databases, starting with those that were not committed when you created Tuesday's backup set and continuing through the latest transaction log written on Wednesday at 4 p.m.

Point-in-time restore: In this case, only the transaction logs that existed in the active file system at the time the backup was taken (and were not committed to the databases) are replayed. All the transaction logs beyond the point-in-time that exist in the transaction log directory belonging to the restored storage group are removed.

You can use this method to restore a database or storage group back to a time before a corruption occurred.

For more information about choosing the restore type, see "Guidelines for choosing the type of restore to perform" on page 190.

Importance of verifying databases to be restored

Using SnapManager 3.2 for Microsoft Exchange, you can override the verification requirement when restoring from a SnapManager backup. However, you are strongly advised to restore only from verified backups. The verification process protects you from restoring a backup with any physical-level corruption. Physical-level database corruption can occur silently in Exchange databases. The only way to know whether a particular database backup incurred physical-level corruption is to run database verification on that backup.

Exchange Recovery Storage Group incompatibility with SnapManager Restore

For Exchange 2003 running on Windows 2000, when the Exchange Recovery Storage Group is present, Exchange automatically performs any restore to that storage group. Therefore, SnapManager Restore cannot function correctly if a Recovery Storage Group is present in this configuration.

If you are running Exchange 2003 on Windows 2000, and you configured a Recovery Storage Group, you need to delete it or override the Recovery Storage Group restore redirection before a SnapManager Restore can be completed successfully. For more information about overriding the Recovery Storage Group restore redirection, see Microsoft Knowledge Base article 824126.

About Restore Snapshot copies

Every time you perform a restore, a Snapshot copy is created on the volume containing the transaction logs. The name of this Snapshot copy contains the prefix `rstrsnap__`.

After you verify that a restore was completed successfully and you are satisfied with the results, you can delete the restore Snapshot copy using the Action menu. For details, see "Explicitly deleting Snapshot copies created by SnapManager Restore" on page 205.

Transaction log sequence verification options

When you perform a restore, you can optionally choose to decrease the time the restore takes by skipping the pre-restore transaction log sequence and database metadata checks. If you skip these checks, and a problem exists with your transaction log sequencing or your database metadata, your restore will fail.

You can choose from the following metadata checks:

- An exhaustive check of the metadata

  For this option, select both the Verify Transaction Log Sequence... and the Exhaustive Verification check boxes.

  For more information about this option, see "What the exhaustive transaction log sequence verification does" on page 187.

- A quicker, less comprehensive check of the transaction logs

  For this option, select the Verify Transaction Log Sequence... check box and clear the Exhaustive Verification check box.

  For more information about this option, see "What the non-exhaustive transaction log sequence verification does" on page 187.
- No metadata verification

  For this option, clear both the Verify Transaction Log Sequence... and the Exhaustive Verification check boxes.

Note

For backward compatibility with previous SnapManager versions, select the exhaustive check, which is selected by default.

What the exhaustive transaction log sequence verification does

The exhaustive option of the transaction log sequence verification performs the following checks:

- The transaction log headers are analyzed, and the following conditions are verified:
  - The transaction logs are all present and sequenced correctly.
  - The signatures of all the transaction logs match.
  - Each transaction logs' create time matches the next log's previous time.
- A Snapshot copy of the databases in this backup is mounted, the database's headers are analyzed, and the following conditions are verified:
  - The database signature matches the log database signature.
  - The database header in the Snapshot copy matches the database metadata in the SnapInfo directory (Windows 2000 only).

What the non-exhaustive transaction log sequence verification does

The non-exhaustive option of the transaction log sequence (selected if you clear the Exhaustive Verification check box) uses the transaction log file names to verify that the transaction log sequence is correct and that all log files are present.

About temporary log files

When running on Windows 2000 Server, SnapManager Restore creates temporary files. Usually, these files are deleted after the restore is done, but you can retain them for debugging by selecting the Keep Log and Patch Files in Temp Directory After Restore check box in the Restore tab or Wizard.

If the directory or subdirectory you specify to contain these files does not exist, SnapManager creates it automatically. SnapManager does not access this directory directly. Rather, it is accessed through the administrative share for the drive letter specified, for example, C$. If the administrative share does not exist, SnapManager prompts you for whether you want SnapManager to create the share automatically.

Note

The temporary files cannot be placed in the root directory. For example, C:\Temp is a valid location for the temporary files; putting them in C:\ causes the restore to fail.

About restoring in a Windows cluster

SnapManager takes the storage group that is to be restored offline before performing the restore, if that storage group is still online.

In a Windows cluster, all resources that are directly or indirectly dependent on the LUN that is to be restored are taken offline, as well as the LUN itself. This means that the entire Exchange virtual server (all storage groups) is offline.

If a cluster move group operation occurs during the restore (for example, if the node that owns the resources goes down) you must restart the SnapManager user interface and the restore.

Ability to restore databases in a clustered Exchange virtual server without taking offline the cluster physical disk resource or the Exchange virtual server

SnapManager 3.2 can restore databases in a clustered Exchange virtual server without taking offline the cluster physical disk resource or Exchange virtual server. This feature applies to LUN restore operations that use the single-file SnapRestore (SFSR) method as well as to those that use the LUN clone split restore method supported with Data ONTAP 7.1. Keeping the LUNs online during a SnapManager restore operation minimizes downtime during restore for databases in storage groups that share a cluster group but are not being restored.

About performing an up-to-the-minute restore after a point-in-time restore from the most recent backup

If you perform a point-in-time backup from the most recent backup and then decide to perform an up-to-the-minute backup from the same backup, SnapManager will successfully complete each operation. However, the results might not be what you intended, because any transactions that occurred after the backup was taken and before the point-in-time restore will not be restored. The reason is that when you perform the point-in-time restore, the transaction logs containing transactions recorded after the selected backup are removed.

For this reason, use caution when selecting a point-in-time restore.

Guidelines for restoring SnapManager backups

Guidelines for choosing the type of restore to perform

Follow these general guidelines to help you decide whether to use a point-in-time or up-to-the-minute restore:

- If you want to roll forward all the transactions up to the most current time, use an up-to-the-minute restore.
- If you want to recover the databases as they were at a particular point in time, for example, at the point when the most recent backup was created, use a point-in-time restore.
- For to an up-to-the-minute restore to succeed, a contiguous set of all required transaction logs must be in the SnapInfo folder and the storage group transaction log directory.
- After a point-in-time restore of a backup that is not the most recent one, all existing backups become point-in-time restorable only. Backups created after the restore will be available for up-to-the-minute restores.
- After a point-in-time restore of the most recent backup, you can still perform an up-to-the-minute restore from any backup, including the most recent backup. However, you will lose all transactions that occurred between when you created the last backup and when you performed the point-in-time restore.

  For more information about why this occurs, see "About performing an up-to-the-minute restore after a point-in-time restore from the most recent backup" on page 189.
- If you are restoring individual databases, you can perform only an up-to-the-minute restore.

Guidelines when restoring a backup

Follow these guidelines when restoring from a SnapManager backup:

- If possible, you should always use the most recent backup for an up-to-the-minute restore. Otherwise, more transaction logs need to be replayed, causing the restore to take more time.

  The most recent backup's name contains `recent` if you did not use the unique name option, or the most recent time stamp if you did.
- You can restore an entire storage group, or, if you configured your data store appropriately, individual databases. If you need to restore more than one storage group, you must run SnapManager Restore more than once.

- If you renamed a storage group since the backup was made, you cannot recover it from a backup taken before the storage group was renamed.
  - If you rename a storage group, make sure that you back it up as soon as possible.
  - If you must recover a storage group from a backup taken before the storage group was renamed, rename the storage group back to its old name, then recover it from the backup.

Restoring from a SnapManager backup

Ways to access SnapManager Restore

You can access SnapManager Restore to restore databases or storage groups from a SnapManager backup in two ways:

- From the SnapManager Restore Wizard

  For details, see "Information you need to perform a restore" on page 192.
- From the SnapManager Restore tab

  For details, see "Restoring using the Restore tab" on page 194.

Information you need to perform a restore

You need to provide the following information to perform a SnapManager restore:

- The storage group that you want to restore, or that contains the databases you want to restore

  Note

  All databases residing on the same LUN must be restored together.

- Whether you want to perform an up-to-the-minute restore (the default) or a point-in-time restore

  For more information about the restore types, see "SnapManager Restore types" on page 185. For more information about choosing a restore type, see "Guidelines for choosing the type of restore to perform" on page 190.
- Whether you want to perform a restore or only a test restore
- Whether you want to verify the transaction log sequence and database metadata before the restore

  For more information on this option, see "Transaction log sequence verification options" on page 186.
- If it is not a test, and you are running on Windows 2000 Server, where you want the temporary log and patch files to be placed

  For more information about where to put the temporary files, see "About temporary log files" on page 187.
- If it is not a test, whether you want your Exchange databases to be remounted after the restore is complete
- If it is a test up-to-the-minute restore, whether you want to check the current transaction logs

  This option confirms that all the required transaction logs are present.

- If the backup has not been verified previously, whether you want to verify the backup before restoring it

Restoring databases using the Restore Wizard

To restore an Exchange storage group from a backup set using the SnapManager Restore Wizard, complete the following steps.

Note

Only one storage group or any of the databases in that storage group can be restored at a time.

Step	Action
1	Make sure that all Explorer windows are closed on the Exchange server running SnapManager.
2	Disable any SnapManager operations that are scheduled to run against the Exchange data you are restoring, including any jobs scheduled on remote management or remote verification servers.
3	From the SnapManager main menu, select Wizard > SnapManager Restore to open the SnapManager Restore Wizard.
4	Follow the instructions in the wizard. For a list of information you need to provide as you complete this step, see "Information you need to perform a restore" on page 192.
5	After you finish the Restore Wizard, the Restore Status window appears. Click Start Now to start the restore. **Result:** Your database or storage groups are restored from the backup you selected. Use the Switch button to switch between the task list and the progress report.
6	After the restore is complete, click OK. **Result:** Your restore is now complete and your Exchange server comes back online.

Step	Action
7	You can optionally perform a SnapManager backup and verification to verify that your restored database is free of physical-level corruption.

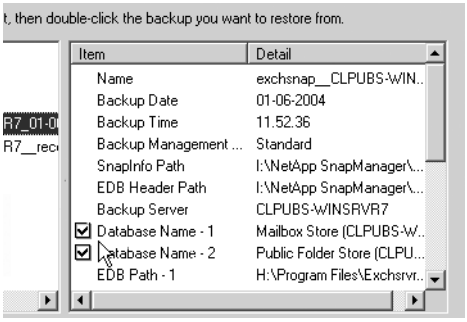
Restoring using the Restore tab

To restore all the Exchange databases from a backup using the SnapManager Restore tab, complete the following steps.

Step	Action
1	Make sure that all Windows Explorer windows are closed on the Exchange server running SnapManager.
2	Disable any SnapManager operations that are scheduled to run against the Exchange data you are restoring, including any jobs scheduled on remote management or remote verification servers.
3	Select the SnapManager Restore tab to display the backup sets you can select to be restored.
4	Select the storage group (Store) that you want to restore.
5	Double-click the backup under the storage group that you want to restore.

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td>6</td><td colspan="2">If you do not want to restore all the databases in this storage group, clear the check box in the details window for the databases you do not want to restore.

Note
If you are running Exchange 2003, all databases in the storage group are dismounted during the restore, even if they are not all being restored.

 
</td></tr>
<tr><td>7</td><td colspan="2">If you are running on Windows Server 2000, enter a temporary location for your log and patch files in the Temporary Location for Log and Patch Files field.

For more information about where to put the temporary files, see “About temporary log files” on page 187.</td></tr>
<tr><td>8</td><td>If…</td><td>Then…</td></tr>
<tr><td></td><td>You want an up-to-the-minute restore</td><td>Select the Up-to-the-Minute Restore ratio button.</td></tr>
<tr><td></td><td>You want a point-in-time restore</td><td>Select the Point-in-Time Restore radio button.</td></tr>
</table>

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td>9</td><td colspan="2">If you do not want to perform exhaustive verification of the transaction log sequence and database metadata before the restore, clear the Verify Transaction Log Sequence and Database Metadata Before Restore and Exhaustive Verification check boxes.

For more information about these options, see “Transaction log sequence verification options” on page 186.</td></tr>
<tr><td>10</td><td colspan="2">If you want SnapManager to automatically remount your restored databases immediately after the restore, make sure that the Mount Database Automatically After Restore check box is selected.</td></tr>
<tr><td>11</td><td colspan="2">If you are running on Windows 2000 Server and you want to use the temporary files SnapManager creates for the restore for troubleshooting, select the Keep Files in Temporary Directory After Restore check box.

Otherwise, the temporary files are deleted after the restore.</td></tr>
<tr><td rowspan="3">12</td><td>If…</td><td>Then…</td></tr>
<tr><td>This is a test restore</td><td>Click the Test Restore button and continue to Step 13.

Result: The Select Test Restore Options window is displayed.</td></tr>
<tr><td>This is not a test restore</td><td>Click the Restore button and skip to Step 14.

Result: In the Restore Status window, a scrollable data window is displayed, showing the tasks that are performed for this restore.</td></tr>
<tr><td>13</td><td colspan="2">In the Select Test Restore Options window, select whether you want to check the current logs (for up-to-the-minute restores only) and run database verification, and then click OK.

Result: In the Restore Status window, a scrollable data window appears displaying the tasks that are performed for this restore.</td></tr>
</table>

Step	Action
14	To start the restore, click Start Now. **Result:** Your database or storage groups are restored from the backup you selected. Use the Switch button to switch between the task list and the progress report.
15	After an actual restore, you can optionally perform a SnapManager backup and verification to verify that your restored database is free of physical-level corruption.

Managing Backup and Restore Snapshots 11

This section describes how to delete Exchange backup and restore Snapshot copies. The following topics are covered:

- "Explicitly deleting storage group backups" on page 200
- "Explicitly deleting an individual backup" on page 209
- "Problem deleting backups due to busy Snapshot copy error" on page 211

Attention

Do not use SnapDrive or the storage system administration tools to delete Snapshot copies created by SnapManager. Doing so will leave behind unwanted data that cannot be removed.

Attention

You must run SnapManager from the system console, not from a Terminal Services client. Do not use Terminal Services for any type of SnapManager administration, because you might miss critical information that is displayed only in pop-up boxes at the system console.

Related topics:

- Chapter 8, "Understanding SnapManager Backup," on page 135
- Chapter 9, "Backing Up Databases with SnapManager," on page 163
- Chapter 10, "Restoring Databases with SnapManager," on page 183

Explicitly deleting storage group backups

Use the "Delete backups" dialog box to explicitly delete multiple Snapshot copies from **one or more storage groups**. You can delete entire backup sets, only the SnapInfo Snapshot copies related to selected backup sets, or Snapshot copies created during previous restore operations. For more information, see the following topics:

- "Explicitly deleting backups and SnapInfo Snapshot copies" on page 200
- "Explicitly deleting Snapshot copies created by SnapManager Restore" on page 205

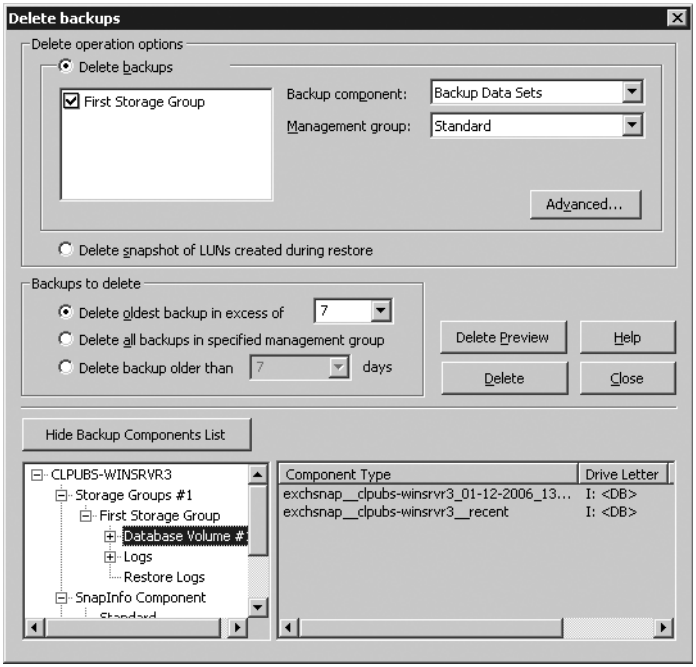
Note

To explicitly delete an individual backup, use the SnapManager Restore tab, as described in "Explicitly deleting an individual backup" on page 209.

Explicitly deleting backups and SnapInfo Snapshot copies

To explicitly delete backups (or only the SnapInfo Snapshot copies related to those backup sets) that contain one or more selected storage groups, complete the following steps.

Step	Action
1	In the SnapManager main window, select Action > Delete Backup. **Result:** The Delete Backups dialog box displays.
2	Select the Delete Backups radio button.

Step	Action
3	If you want to display a list of the backup components on your SnapManager system, click Show Backup Components List.  **Note** You cannot select an individual backup component for deletion using this list.
4	Select one or more storage group sets whose backups are to be deleted.

Step	Action
5	To expand the scope of the deletion to include backups that contain **only some** of the selected storage groups (in addition to backups that contain **all** of the selected storage groups), do the following: **a.** Click Advanced to open the "Advanced Options" dialog box. **b.** Select the "Delete backups that contain databases belonging to one or more of the selected storage groups" option. **Result:** For this backup deletion operation only, multiple backup deletions will delete backups containing any one or more of the selected databases. **Note** This option is useful only if you created backups that did not contain all storage groups in a storage group set. For easiest backup administration, it is best if you always back up an entire storage group set.

Step	Action
6	The Backup Component selection narrows the scope of the deletion by specifying the type of backup components to be deleted. This option is set to Backup Data Sets by default, so that you will delete entire backup sets, including related transaction logs and SnapInfo directories. You can narrow this selection further by selecting SnapInfo Snapshots Only. **Note** Usually you delete complete backup sets. However, if you need a way to free some space or reduce your Snapshot copy count without deleting a SnapManager backup, you can delete SnapInfo Snapshot copies without affecting the associated backup.
7	The Management Group selection further narrows the scope of the deletion by specifying the backup management group of the backups you want to delete. This option is set to Standard by default, but you can change it to Daily, Weekly, or All.
8	If you want to retain up-to-the-minute restore ability for older backups in other backup management groups, leave that option selected. To access this option, click Advanced to open the "Advanced Options" dialog box. ◆ If you select this option, transaction logs will be deleted **only from the specified backup management group**; transaction logs will not be deleted from other backup management groups. ◆ If you clear this option, transaction logs will be deleted **from other backup management groups** as well. **Note** If you selected All for the backup management group, this option has no effect and is disabled. For more information about this option, see "Option to retain up-to-the-minute restore ability" on page 155.

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td rowspan="4">9</td><td colspan="2">Use the “Backups to delete” panel to specify which backups, of those in the specified storage group and backup management group, that you want to delete.</td></tr>
<tr><td>If you want to delete…</td><td>Then…</td></tr>
<tr><td>The oldest backups so that only a specified number of backups remain for that backup management group (quantity-based deletion)</td><td>Do the following:
a. Select the “Delete oldest backups in excess of” option.
b. Specify how many of the newest backups in the specified backup management group you want to preserve.</td></tr>
<tr><td>All the backups in the specified backup management group</td><td>Select the “Delete all backups in the specified management group” option.</td></tr>
<tr><td>Only the backups that are older than a specified number of days (age-based deletion)</td><td>Do the following:
a. Select the “Delete backups older than” option.
b. Specify the number of days for which you want to keep the most recent backups.</td></tr>
</table>

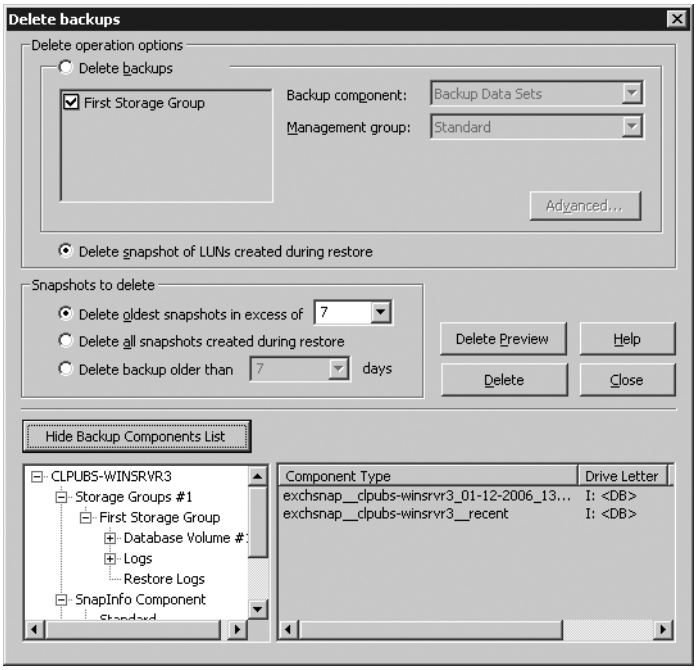
Step	Action	
10	**If you want to…**	**Then…**
	See what backup components would be deleted with the parameters you have entered without deleting them	Click Delete Preview and proceed to Step 11. **Result:** The Delete Backup Data Set Preview window is displayed. After a moment, a count and list of the backup components identified for deletion are displayed.
	Delete the backup components	Click Delete. **Result:** The backup components identified by your selections are deleted. When the deletion is complete, a status popup is displayed. You have completed this procedure.
11	If, after previewing the deletion, you want to delete the backup components listed in the preview, click Delete on the Delete Backup Data Set Preview window. **Result:** The backup components listed in the preview window are deleted.	

Explicitly deleting Snapshot copies created by SnapManager Restore

To delete Snapshot copies created during previous restores, complete the following steps.

Note
This is the only way to delete Snapshot copies created by SnapManager Restore.

Step	Action
1	In the SnapManager main window, select Action > Delete Backup. **Result:** The Delete Backups dialog box displays.
2	Select the “Delete snapshot of LUNs created during restore” option.

Step	Action
3	If you want to display a list of the backup components on your SnapManager system, click Show Backup Components List.  **Note** You cannot select an individual backup component for deletion using this list.

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td>4</td><td colspan="2">Use the “Snapshots to delete” panel to specify which restore Snapshot copies you want to delete.</td></tr>
<tr><td></td><td>If you want to delete…</td><td>Then…</td></tr>
<tr><td></td><td>The oldest restore Snapshot copies so that only a specified number of backups remain (quantity-based deletion)</td><td>Do the following:
a. Select the “Delete oldest snapshots in excess of” option.
b. Specify how many of the newest restore Snapshot copies you want to preserve.</td></tr>
<tr><td></td><td>All the restore Snapshot copies</td><td>Select the “Delete all snapshots created during restore” option.</td></tr>
<tr><td></td><td>Only the restore Snapshot copies that are older than a specified number of days (age-based deletion)</td><td>Do the following:
a. Select the “Delete backups older than” option.
b. Specify the number of days for which you want to keep the most recent restore Snapshot copies.</td></tr>
</table>

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td rowspan="3">5</td><td>If you want to…</td><td>Then…</td></tr>
<tr><td>See what restore Snapshot copies would be deleted without deleting them</td><td>Click Delete Preview and proceed to Step 6.

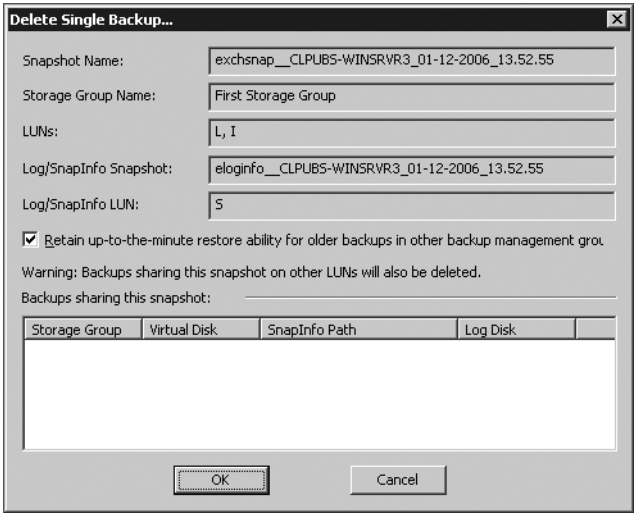
Result: The Delete Backup Data Set Preview dialog box appears. After a moment, a count and list of the restore Snapshot copies identified for deletion are displayed.</td></tr>
<tr><td>Delete the restore Snapshot copies</td><td>Click Delete.

Result: The restore Snapshot copies identified by your selections are deleted. When the deletion is complete, a status popup is displayed. You have completed this procedure.</td></tr>
<tr><td>6</td><td colspan="2">If, after previewing the deletion, you want to delete the restore Snapshot copies listed in the preview, click Delete on the Delete Backup Data Set Preview dialog box.

Result: The restore Snapshot copies listed in the preview window are deleted.</td></tr>
</table>

Explicitly deleting an individual backup

To delete an individual backup, complete the following steps.

Step	Action
1	Select the SnapManager Restore tab in the SnapManager interface.
2	Select the storage group (Store) in which the backup resides.
3	Right-click the backup you want to delete and select Delete . **Result:** The Delete Single Backup dialog box appears and displays current information about the selected restore backup.  **Note** You cannot delete the most recent backup for any storage group.
4	Be sure to review the list of backups sharing this Snapshot copy; all of these backups will be deleted at the same time.

Step	Action
5	If you want to retain up-to-the-minute restore ability for older backups in other backup management groups, leave that option selected. ◆ If you select this option, transaction logs will be deleted **only from this backup management group**; transaction logs will not be deleted from other backup management groups. ◆ If you clear this option, transaction logs will be deleted **from other backup management groups** as well. For more information about this option, see "Option to retain up-to-the-minute restore ability" on page 155.
6	Click OK. **Result:** The backup is deleted.

Problem deleting backups due to busy Snapshot copy error

If you attempt to delete a backup and you get an error message saying that the Snapshot copy is busy and cannot be deleted, you have a backup that was taken of a LUN backed by another Snapshot copy. In this case, you need to delete the more recently taken backup before the older backup can be deleted.

To see if you have busy Snapshot copies, you can view your Snapshot copies in FilerView or use the storage system `snap list` command. For more information about deleting busy Snapshot copies, see the *System Administration Block Access Guide* for your version of Data ONTAP.

Note

To avoid this situation in the future, make sure that you do not take backups while you have any LUNs backed by Snapshot copies (for example, during a verification or while archiving from a LUN backed by a Snapshot copy). For more information about scheduling your SnapManager tasks, see "Recommendations for scheduling backups" on page 158.

Using SnapMirror with SnapManager 12

This section describes how SnapManager uses SnapMirror to enable you to replicate Exchange database backups to mirrored volumes. The following topics are covered:

- "Other documentation" on page 214
- "Understanding SnapMirror" on page 215
- "How SnapManager uses SnapMirror" on page 217
- "Scheduling SnapMirror replication for SnapManager backups" on page 219

Other documentation

For more information about configuring and using SnapMirror, see the following guides:

- For an overview of SnapMirror—including a detailed explanation of what mirror volumes are, how they work, when to use or access data stored on a SnapMirror destination volume, and direction about how to set up and configure SnapMirror on a storage system—see *Data Protection: Online Backup and Recovery Guide* for your version of Data ONTAP.
- For details about how SnapMirror is used with SnapDrive to create a destination volume for replicating LUNs and for a description of SnapMirror replication—including reasons for using it and the benefits it offers—see your SnapDrive documentation.
- For details about how to connect to a LUN in a SnapMirror destination volume, see your SnapDrive documentation.
- For details about how to access Exchange data from mirrored volumes to recover from failure, see “Restoring your Exchange environment” on page 230.

Understanding SnapMirror

SnapMirror creates replicas of volumes hosting LUNs. SnapMirror mirrors a Snapshot copy of data on a source volume to one or more volumes configured as destinations of the source volume. SnapMirror can replicate a source volume to a destination volume on the same storage system or to a different storage system. When you use SnapMirror to replicate volumes from one storage system to another, the destination storage system can be in a different geographical location. This ability to duplicate data in different locations is a key component of a sound disaster recovery plan.

Data stored in a mirror on a destination volume can be accessed through SnapDrive. Because the mirror is volume wide, Snapshot copies of other data sets on the source volume are mirrored also.

SnapMirror updates the destination volumes to reflect incremental changes on the source volume. The result of this process is an online, read-only destination volume that contains the same data as the source at the time of the most recent update (using SnapManager Backup, in this case).

Attention

Because SnapManager uses SnapMirror in asynchronous mode, any disk writes that occurred on the source volume after the most recent SnapMirror replication update are not available if a catastrophic failure occurs before the next update. This is because they were not replicated to the SnapMirror destination volume.

Requirements for using SnapMirror with SnapManager

To use SnapMirror with SnapManager, you must have previously configured SnapMirror on both the source volume to be replicated and its destination volumes. How to complete these tasks is explained in your SnapDrive documentation. Your configuration must satisfy the following requirements:

- There must be one or more SnapMirror source volumes hosting LUNs.
- There must be one or more SnapMirror destination volumes for each source volume.
- The size of the destination volumes must be equal to or greater than the size of the source volume.
- SnapMirror licenses must be enabled on both the source and destination storage systems.
- You must manually configure and initialize the SnapMirror replication between source and destination volumes.

- You must disable the SnapMirror replication schedule on your storage system.
- You must configure the SnapMirror replication as asynchronous.

How SnapManager uses SnapMirror

When SnapMirror updates occur

If Exchange data backed up by SnapManager resides in a volume that is configured as a SnapMirror source volume with one or more appropriately configured destination volumes, a SnapManager backup of an Exchange database stored on that volume causes SnapDrive to request a SnapMirror update for that volume. The schedule you define for backups sets the schedule for mirror replication.

SnapMirror replication type

When you use SnapMirror to replicate SnapManager backups, SnapMirror replication is asynchronous. This means that changes made between SnapManager backups are not reflected in the SnapMirror target volume, and any restore from the target volume would restore the databases to their state at the time of the last SnapManager backup. However, you can use SnapDrive to minimize the time between SnapMirror replications.

For more information about scheduling your SnapMirror replications, see "Scheduling SnapMirror replication for SnapManager backups" on page 219.

SnapMirror replication unit

When you use SnapMirror to replicate SnapManager backups, you can replicate only volumes, not qtrees. SnapMirror qtree replication is not supported by SnapManager.

How SnapMirror replication works

In previous releases of SnapManager for Microsoft Exchange, the SnapMirror mirror update was always initiated for each Snapshot copy as it was taken. This approach resulted in redundant mirror updates. With SnapManager 3.0 for Microsoft Exchange and later, the mirror update request is delayed until SnapManager explicitly requests it, after the SnapManager backup is complete.

Note

If you do not want the SnapMirror destination volume to be updated after a backup is taken, you can override the update using the Backup Wizard or the Backup tab.

The following table provides an overview of how SnapMirror destination replication works.

Stage	Process
1	Configure SnapMirror relationship between source volumes and destination volumes. Create a Custom schedule with schedule parameters (“- - - -“). Initialize the Mirror to perform initial transfer of contents from source volume to destination volume
2	Select the “Update Snapmirror after operation” option for the operation.
3	If any volume whose data is captured in the backup is a SnapMirror source volume, SnapDrive requests information about all SnapMirror destination volumes for the source volume.
4	SnapDrive sends a SnapMirror destination update request to all the related destination volumes.
5	SnapMirror updates the destination volumes to reflect incremental changes on the source volume.

Scheduling SnapMirror replication for SnapManager backups

Replication scheduling considerations

When you configure the storage system volume containing your Exchange data as a SnapMirror source volume, every time a SnapManager backup is taken, the SnapMirror destination volume is optionally updated.

Taken alone, this schedule might not provide an optimal SnapMirror replication schedule. This is because any changes that occur between replications are not replicated to the destination volume until the next replication update. Any restore from the destination volume would restore the Exchange data to its state at the last backup time; subsequent changes to the Exchange data store would not be restored.

Rather than increasing the frequency of SnapManager backups, you can use the rolling Snapshot copy capability of SnapDrive to provide frequent replication of the LUNs that contain the Exchange transaction logs. With more current transaction logs, a restore from the destination volume replays the transaction logs, resulting in an up-to-the-minute restore for the time of the last transaction log update. This method enables you to keep your destination volume more current without running the risk of overlapping your SnapManager operations.

Advantages of SnapDrive rolling Snapshot copies

When you use the SnapDrive update mirror, special Snapshot copies called rolling Snapshot copies are used. These Snapshot copies are created only for SnapMirror replication. For more information about rolling Snapshot copies, see your SnapDrive documentation.

There are three major advantages to using SnapDrive rolling Snapshot copies to augment your SnapMirror replication schedule for SnapManager:

- Fewer changes are made to the Exchange data between replications.

  When you use SnapDrive to initiate frequent updates to the transaction logs, a restore from the destination volume replays the transaction logs, resulting in an up-to-the-minute restore for the time of the last transaction log update.
- Fewer SnapManager backups are required.

  It is not recommended to take SnapManager backups every few minutes. This can result in overlapping SnapManager operations and more difficulty managing the large number of resulting backups.
- Fewer Snapshot copies are retained.

  A maximum of two rolling Snapshot copies are retained at any time.

Scheduling replication for SnapManager using both SnapManager and SnapDrive

To create a SnapMirror replication schedule for your SnapManager backups using both SnapManager and the SnapDrive command-line interface tool (`sdcli`), complete the following steps.

Step	Action
1	Configure a mirror on the storage system for the volume occupied by the LUNs backed up by SnapManager. Create an empty replication schedule ("- - - -") where you would normally enter the schedule parameters. For more information about setting a SnapMirror replication schedule, see your SnapDrive documentation and the Data ONTAP *Data Protection: Online Backup and Recovery Guide*.
2	Schedule your SnapManager backups according to your local requirements using either the SnapManager Backup Wizard or the Backup tab. For more information about SnapManager backup schedules, see "Recommendations for scheduling backups" on page 158 and "Backing up databases" on page 164.
3	Add the `sdcli` command to the Windows Scheduled Tasks using the appropriate command-line switches. Take the following requirements into account: ◆ You must know the letter of the drive where the transaction logs reside. ◆ The task must run under the same account as the SnapDrive service. **Example:** The following command can be scheduled successfully on the local host, assuming that Z: is the drive where the transaction logs reside: `sdcli snap update_mirror -d Z` For more information about `sdcli`, see your SnapDrive documentation.

Example schedule

The following table shows an example of a schedule documenting the additional intervals when the volume containing the transaction logs is replicated. The schedule shown in this table allows for a thirty-minute elapse time between the SnapManager backup and the transaction logs drive replication.

You might need to adjust the timings in this example for your environment to account for these requirements:

- The first supplemental replication after the backup must not begin before the backup is complete, including verification, and the ensuing SnapMirror volume update is also complete.
- The subsequent supplemental replications must not begin before the previous supplemental replication is complete.

Regularly scheduled SnapManager backup	Supplemental SnapMirror replication of transaction logs
7:00 a.m.	7:30 a.m. 8:30 a.m. 9:30 a.m. 10:30 a.m. 11:30 a.m. 12:30 p.m.
1:00 p.m.	1:30 p.m. 2:30 p.m. 3:30 p.m. 4:30 p.m. 5:30 p.m. 6:30 p.m. 7:30 p.m. 8:30 p.m. 9:30 p.m.
10:00 p.m.	10:30 p.m.

Performing Disaster Recovery with SnapManager 13

This section describes how you can prepare for disaster, and then use SnapManager and either SnapMirror or archiving to restore Exchange databases that were destroyed or compromised because of catastrophic conditions. The following topics are covered:

- "Guides you should read and have at hand" on page 224
- "Preparing for disaster recovery" on page 225
- "Restoring your Exchange environment" on page 230
- "Disaster recovery by relocating Exchange virtual servers to a different Windows cluster" on page 261

Guides you should read and have at hand

In addition to this guide, you should be familiar with the following guides and have them at hand, available for reference during disaster recovery:

- For information about how to connect to and use the LUNs stored in a mirrored destination volume, see your SnapDrive documentation.
- For information about administering Data ONTAP, see the *System Administration Storage Management Guide* for your version of Data ONTAP.
- For information about data replication using SnapMirror, see the *System Administration Data Protection Guide* for your version of Data ONTAP.
- For detailed information about disaster preparedness and recovery for Microsoft Exchange Server, see the following documents published by Microsoft Corporation:
  - For Exchange 2000, see *Disaster Recovery for Microsoft Exchange 2000 Server*. This white paper is available on the Microsoft Web site as Knowledge Base article 326052.
  - For Exchange 2003, see *Exchange Server 2003 Disaster Recovery Operations Guide*. This TechNet guide is available on the Microsoft Web site from a link in Knowledge Base article 867704.
- For additional information about disaster recovery in the Microsoft environment, see
  - Microsoft Windows documentation
  - Microsoft Exchange documentation

Preparing for disaster recovery

Preparing for disaster ahead of time is key to recovering from it.

- "Overview" on page 225
- "Backing up your Exchange environment" on page 227
- "Replicating your Exchange environment" on page 228

Overview

The first steps to recovery from catastrophic failure of an Exchange database or storage system should take place long before the event occurs.

Recommendations for disaster recovery preparation: Every environment and site is unique and every company has different requirements, depending on the amount of time recovery can take, archiving resources, and other factors. Taking these differences into account, consider the following general disaster recovery preparation recommendations:

- If you are using SnapMirror to mirror your data, keep the storage system storing the destination SnapMirror volumes in a different physical location than your primary production system. In extreme cases, an entire site can be destroyed in a catastrophic event.
- If you are using archiving, the archive media, such as a NearStore® system or tape, should be located off site.
- Instate a policy of redundant knowledge by ensuring that more than one person knows how to restore the system.
- Record your Exchange data configuration, and keep detailed records and logs of changes you make to your Windows and Exchange environments. Keep hardcopy duplicates of these records off site.

Components required to restore your environment: To be able to reconstruct your Exchange environment after a catastrophic failure, you must be able to recover the following three components:

- Windows environment

  You can either back up or replicate your Windows environment.

  For more information about backing up your Windows environment, see "Backing up your Exchange environment" on page 227.

  For more information about replicating your Windows environment, see "Replicating your Exchange environment" on page 228.
- Exchange server

You can either back up your Exchange server or reconstruct it using the Exchange recovery mode. To be able to reconstruct your Exchange server, you must have restored or replicated your Windows environment exactly.

For more information about backing up your Exchange server, see "Backing up your Exchange server" on page 227.

For more information about replicating your Windows environment, see "Replicating your Exchange environment" on page 228.

- Exchange data

  You use SnapManager for Microsoft Exchange to create backups of your Exchange data, then move that data off site, either by archiving those backups or using SnapMirror to mirror them to another storage system at a remote site.

Two methods to get Exchange data off site: You can use either of these methods to get your Exchange data off site for disaster recovery:

- You can use SnapMirror to mirror your storage system data to a storage system in another location.

  For more information about using SnapMirror with SnapManager, see "Using SnapMirror with SnapManager" on page 213.

- You can archive the data to physical media, such as tapes, and store that media off site.

  For more information about archiving Exchange data, see "Archiving SnapManager Backups" on page 299.

If you're unsure which method to use, see the following table, which outlines advantages and disadvantages of each method:

Method to get Exchange data off site	Advantages	Disadvantages
Using SnapMirror	◆ Restoring from a SnapMirror destination is significantly faster than restoring from tape. ◆ The destination can be updated more frequently than tape, resulting in more current archives.	◆ Another storage system is required in the remote location. ◆ WAN connectivity to the remote location is required.

Method to get Exchange data off site	Advantages	Disadvantages
Archiving SnapManager backups	◆ The required equipment might already be available and in use.	◆ Restoring from tape is significantly slower than restoring from a storage system. ◆ Tapes must be stored and managed.

Backing up your Exchange environment

To be able to reconstruct your Exchange environment after a catastrophic failure, you must be able to restore both your Windows environment and your Exchange server.

Backing up your Windows environment: SnapManager for Microsoft Exchange, the Exchange server, and the storage systems are dependent on the Windows environment. Before you can use any of the processes in this section, the Windows environment must be completely restored. Therefore, it is important that you back up your Windows environment so that you can restore the same state as part of the recovery process.

To back up your Windows environment, you must complete, at a minimum, the following high-level process.

Task	Process
1	Back up your Exchange server, including your Windows operating system and any applications running concurrently with the Exchange server.
2	Use your backup utility to create and maintain a current emergency repair disk (ERD).

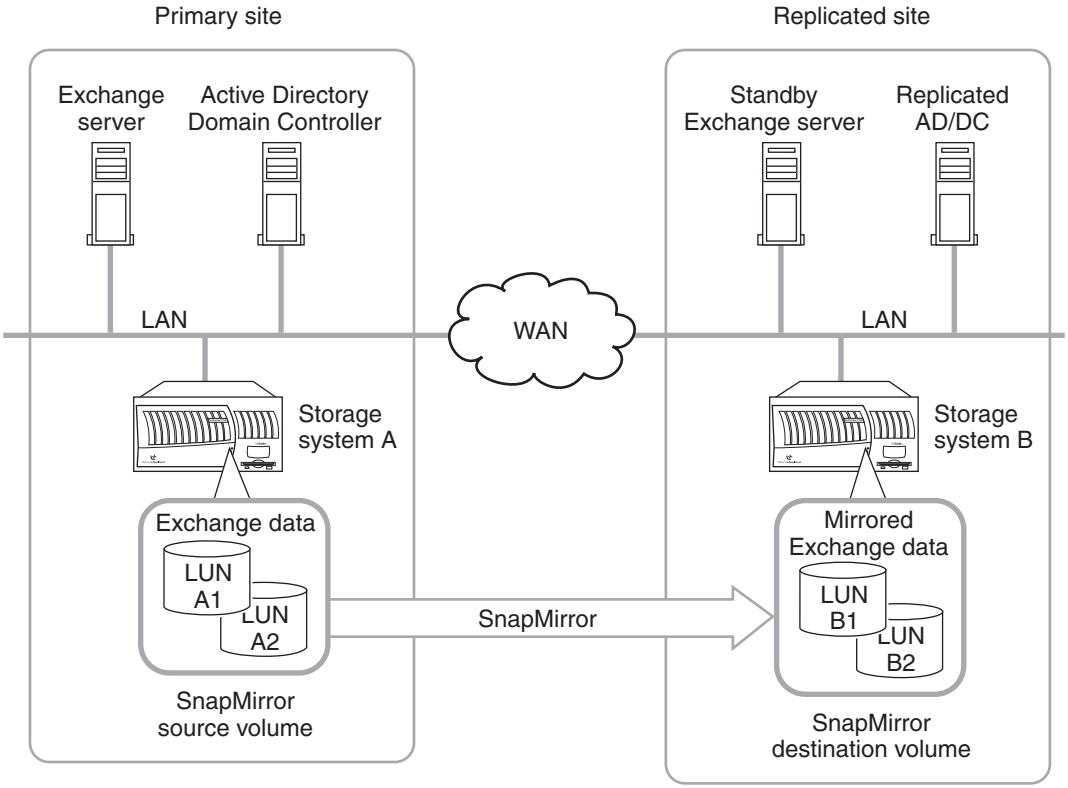
Backing up your Exchange server: To ensure that you back up all the required components on your Exchange server, follow the process outlined in the appropriate Microsoft document: *Disaster Recovery for Microsoft Exchange 2000 Server.*

Replicating your Exchange environment

If you want the ability to recover from a total site outage in a minimum amount of time, you can replicate your Exchange environment to a remote site. Then, if the primary site is destroyed, you can re-create your Exchange environment on the replicated site.

For more information about re-creating your Exchange environment on the replicated site, see "Recovering a failed storage system and server to a replicated environment" on page 252.

The following diagram shows a typical Exchange site replication:



Example Site Replication

Note the following facts about this site configuration:

- The Windows environment (Active Directory, Domain Controller, etc.) is replicated through the Wide Area Network (WAN) to the replicated site.

For more information about replicating your Windows environment and using a replicated environment to recover from a disaster, see your Windows documentation.

- The Exchange data on the storage system is mirrored using SnapMirror to a storage system on the replicated site.

  For more information about setting up SnapMirror, see your Data ONTAP *System Administration Data Protection Guide.*

- The standby Exchange server is configured identically to your primary Exchange server, except for the following differences:
  - It does *not* yet have Exchange installed.
  - It is not yet a member of the domain (leave it in workgroup mode).
  - It has a different name than the primary Exchange server.

Restoring your Exchange environment

This topic describes the recovery from catastrophic loss of a SnapManager for Exchange environment:

- "Overview" on page 230
- "Recovering Exchange data using archives" on page 233
- "Recovering Exchange data using SnapMirror" on page 236
- "Restoring a storage system volume using SnapManager backup archives" on page 238
- "Recovering a failed Exchange server" on page 239
- "About recovering both a failed storage system and a failed Exchange server" on page 244
- "Recovering both a failed storage system and Exchange server using SnapMirror" on page 245
- "Recovering both a failed storage system and Exchange server using archiving" on page 249
- "Recovering a failed storage system and server to a replicated environment" on page 252
- "Returning to your original site replication configuration" on page 256

Overview

The following paragraphs outline the process of recovering from catastrophic loss of a SnapManager for Exchange environment.

Exchange environment recovery processes: Recovery from catastrophic loss of an Exchange environment that integrates SnapManager for Microsoft Exchange and NetApp storage systems is outlined in the following process.

Task	Process
1	Recovering the Windows environment All procedures in this document assume that you already recovered your Windows environment. For more information about recovering your Windows environment, see the Microsoft documentation listed in "Guides you should read and have at hand" on page 224.

Task	Process
2	Recovering the Exchange server This process is performed using the backup application you used to back up the Exchange server.
3	Recovering the Exchange databases This process is performed using SnapManager for Microsoft Exchange.

A SnapManager for Exchange restore from archive operation should be considered a "point-in-time" restore: A SnapManager for Exchange restore from archive operation is typically considered a point-in-time restore based on the time that the backup was created by SnapManager, regardless of whether the "Up-to-the-minute restore" option or the "Point-in-time restore" option was selected on the SnapManager Restore tab.

For a SnapManager up-to-the-minute restore operation to successfully restore an Exchange database up to the point of failure, a contiguous set of Exchange transaction log files that were generated between the time that the archived backup set was created and the time that the failure occurred would need to be available to SnapManager. This means that all SnapManager backups taken after the archived backup was created need to be online and available, in addition to any transaction logs that were generated between the time of the most recent SnapManager backup and the time of the failure.

The reason that a restore from archive is considered a point-in-time restore is that a restore from archive operation is typically performed when none of the SnapManager online backups are available or usable. Selecting the "Up-to-the-minute restore" option instructs SnapManager to use any contiguous log files that it can find to perform the restore. If it does not find any logs in addition to the logs captured by the backup which is being restored, then the restore will still succeed. The SnapManager restore report that is generated as part of the restore operation will include the file names of the Exchange transaction log files that were restored.

Rules and guidelines for disaster recovery: Before you perform disaster recovery using SnapManager for Microsoft Exchange, make sure that you understand the following rules and guidelines:

- If you archive only your database LUNs (and not the LUN containing the transaction logs), you will only be able to perform a point-in-time restore. The Exchange databases will be restored back to the time when the backup

was created. Changes made to the databases after this time cannot be recovered.

- If you archive and restore your transaction log LUN along with the database LUNs, and the transaction log LUN contains transaction logs that accumulated after the archived backup was created, then you have the option of selecting an up-to-the-minute restore. In this case, the database would be restored up to the time when the archive was created. Changes made to the database after the archive was created cannot be recovered.
- If you are using SnapMirror, you can use an up-to-the-minute restore to restore your databases to the point in time of the last SnapMirror replication to the target volume containing the transaction logs LUN.
- If you are restoring from an archive, the LUN files from the archive must be restored into their original location in the active file system of the storage system's volume.
- The drive letters assigned to the LUNs that are restored must be the same drive letters that were used when the archive was created.
- You cannot recover a LUN or transaction logs into a read-only file system, such as a Snapshot copy.
- For SnapManager Restore to work properly, SnapManager for Microsoft Exchange must be licensed on the storage system that stores the Exchange databases or the local Windows machine running SnapManager.
- For SnapManager Restore to work properly, SnapRestore must be licensed on the storage system that stores the Exchange databases.
- The recovery processes in this guide do not address a large-scale disaster in which supporting Windows infrastructure, such as Active Directory and DNS, is damaged or lost. Before attempting recovery of the Exchange server or the storage system, you must recover the supporting infrastructure.

Which recovery procedure to use: You can use the following table to determine which recovery process most closely matches your needs.

If…	Then use…
You want to recover Exchange databases from a SnapMirror destination volume	"Recovering Exchange data using SnapMirror" on page 236
Your Exchange server is online and you want to recover Exchange databases from archive	"Recovering Exchange data using archives" on page 233

If…	Then use…
Your storage system volume has failed or been destroyed and you used archiving	"Restoring a storage system volume using SnapManager backup archives" on page 238
Your Exchange server has failed or been destroyed	"Recovering a failed Exchange server" on page 239
Both your Exchange server and your storage system have failed and you want to recover on the same hardware	The applicable procedure: ◆ "About recovering both a failed storage system and a failed Exchange server" on page 244 ◆ "Recovering both a failed storage system and Exchange server using SnapMirror" on page 245 ◆ "Recovering both a failed storage system and Exchange server using archiving" on page 249
Both your Exchange server and your storage system have failed or been destroyed, and you want to recover your Exchange environment using a replicated environment on a new Exchange server	The applicable procedure: ◆ "Recovering a failed storage system and server to a replicated environment" on page 252 ◆ "Returning to your original site replication configuration" on page 256

Recovering Exchange data using archives

To restore the Exchange databases from an archive of a SnapManager backup set, complete the following steps.

Step	Action
Prepare your environment	
1	Identify and locate the archived backup set that you want to restore.

Step	Action
2	If your Exchange databases are still mounted, dismount all databases belonging to the storage group to be restored.
3	Note the drive letter belonging to the storage group to be restored from archive.
4	As an extra safety measure, use SnapDrive to manually create a Snapshot copy of the LUNs to be restored from archive.
5	Use SnapDrive to delete the LUNs to be restored to avoid a file name conflict when the LUNs are restored from archive.
Restore storage system data	
6	Using the archive tool you used to create the archive, restore the archived LUNs to the storage system volume.
7	Use SnapDrive to connect to the restored LUNs, using the same drive letters you used before.
8	Verify that the reconnected LUNs are accessible.
9	Restore the SnapInfo directory and all of its contents from the archive to a temporary location accessible from the SnapManager host. SnapManager requires the SnapInfo directory to restore from the archive, and will request this location in a later step. **Note** You might have archived only the SnapInfo directory or the entire LUN containing it. In either case, you now need access only to the SnapInfo directory on that LUN or to a copy of the SnapInfo directory.
Restore Exchange data	

Step	Action
10	Exit SnapManager if it is running, and restart it in Restore From Archive mode by opening a command window and using the following command-line flag: **`restorearchive`** **Example:** `C:\Program Files\NetApp\SnapManager For Microsoft Exchange\SnapManager.exe -restorearchive` **Note** Use this SnapManager mode only to restore SnapManager archives. Before performing any other SnapManager operations, close SnapManager and restart it without the command-line flag. **Result:** The SnapManager Restore From Archive window is displayed.
11	In the Restore From Archive window, enter or browse to the path where the SnapInfo directory was restored. The path to the restored SnapInfo directory includes the following components: `\snapinfo\`*`server_name`*`\`*`storage_group_name`*`\`*`snapshot_name`*. The *snapshot_name* should be the same name as the Snapshot copy from which the LUN file for the database was archived.
12	Click OK.
13	In the Restore From Archive window, double-click to select the backup set that you want to restore. **Note** When peforming a restore from archive operation with SnapManager on systems running Windows 2000 Server, the backup sets displayed under the restore tab will show up as unverified whether or not they have in fact been verified. The administrator will have to either verify the database again as part of the restore prodedure or restore the database unverified if you have knowledge that it had been previously verified.

Step	Action
14	Click Start Restore. If the backup is not verified, you are prompted whether to verify it. **Note** You can override the verification requirement; however, you are strongly advised to use only verified backups for restore.
15	Click Yes to continue.
16	Click Start Now to begin the restore process.
17	After the restore is complete, launch the Outlook® client and verify that your data was properly restored and that the Exchange server is operating correctly.
18	Perform a SnapManager backup and verification to verify that your restored database is free of physical-level corruption.

Recovering Exchange data using SnapMirror

This section explains how to recover LUNs from a failed volume on a storage system or a failed storage system using SnapMirror. These LUNs contain the Snapshot copies of the databases to be restored.

You can configure SnapMirror to use a destination volume on the same storage system or a different, remote storage system. Whether the destination volume is on the same storage system as the failed volume or a different one, the procedure you follow to recover is largely the same.

To recover Exchange data using a SnapMirror destination volume, complete the following steps.

Step	Action
1	Identify the destination mirror volume so that you know the volume to mount when you encounter that step.

Step	Action
2	Ensure that the storage system hosting the SnapMirror destination volumes is online and that the volumes are available and shared through CIFS. For information about creating CIFS shares, see your SnapDrive documentation. For information about general storage system administration, see your *Data ONTAP System Administration Storage Management Guide.*
3	Make sure that all databases that are stored on LUNs on the failed volume are dismounted. For information about dismounting stores, see the Microsoft Exchange documentation.
4	From the SnapDrive MMC, disconnect the LUNs that resided on the failed volume. Take note of the drive letters or mount points that were used for these disks. For information about disconnecting LUNs, see your SnapDrive documentation. **Note** If you are unable to disconnect a LUN, it might contain databases that are still online, or there could be another application that is still accessing that LUN.

Step	Action
5	From the SnapDrive MMC or command-line interface, connect to the LUN files in the active file system of the SnapMirror destination volume. SnapDrive will also break the mirror during this process. **Note** Do not mount the Exchange databases yet. The SnapManager Restore process mounts the databases. If you get an error when connecting, such as "Disk is in exclusive use," use FilerView to ensure that the LUN is unmapped from all igroups and online. For information about connecting LUNs, see your SnapDrive documentation. **Result:** A Single File Snap Restore (SFSR) is automatically performed, using the most recent Snapshot copy (which could have been created by SnapDrive or SnapManager).
6	Run SnapManager and use SnapManager Restore to restore the most recent backup for each storage group. For more information about using SnapManager Restore, see "Restoring Databases with SnapManager" on page 183.
7	Launch the Outlook client and verify that your data was properly restored and that the Exchange server is operating correctly.
8	Perform a SnapManager backup and verification to verify that your restored database is free of physical-level corruption.

Restoring a storage system volume using SnapManager backup archives

This scenario explains how to recover LUNs from a failed storage system volume or a failed storage system using archived SnapManager backups.

To recover a failed storage system volume using SnapManager backup archives, complete the following steps.

Step	Action
1	Recover the storage system so that it is online and available. For information about bringing the storage system online and making it available to your client, see the *Software Setup Guide* and *System Administration Storage Management Guide* for your version of Data ONTAP.
2	Prepare the archive media and the backup application so that they are ready to be used for the recovery. If you are using a NearStore system, ensure that the data is accessible.
3	Perform the procedure for archive recovery described in "Recovering Exchange data using archives" on page 233.

Recovering a failed Exchange server

To recover an Exchange server, you must use NTBackup or a third-party backup and restore application, relying on its documentation for direction. To recover the Exchange databases, you use SnapManager.

This procedure assumes that backups of the Exchange server were made; it also assumes that the most recent backup includes the system state of the Exchange server just before the disaster occurred.

Recovering a failed Exchange 2000 or 2003 server: To recover a failed Exchange 2000 or 2003 server, complete the following steps.

If you are restoring to different hardware, you might need to refer to one of the following Microsoft Knowledge Base articles, as appropriate for your operating system:

- For Exchange 2000, see article 297289.
- For Exchange 2003, see article 822945.

Steps	Action
1	Ensure that the storage system is online and that the volumes containing the LUN files are available across CIFS. For information about creating CIFS shares, see your SnapDrive documentation. For information about general storage system administration, see the *System Administration Storage Management Guide* for your version of Data ONTAP.

<table>
<tr><th>Steps</th><th colspan="2">Action</th></tr>
<tr><td>2</td><td colspan="2">The server you restore Exchange on does not need to be the same hardware you were running Exchange on before the disaster. However, it must have the same name as the previous Exchange server, and it must have sufficient capacity.</td></tr>
<tr><td></td><td>If…</td><td>Then…</td></tr>
<tr><td></td><td>You are restoring your Exchange server back to the same hardware</td><td>Proceed to Step 3.</td></tr>
<tr><td></td><td>You are restoring your Exchange server to a brand new server</td><td>Name the new server using the same name as the original Exchange server and proceed to Step 3.
Note
If you are restoring from tape, your new hardware configuration must match the old hardware configuration exactly, including interface cards and firmware versions.</td></tr>
<tr><td></td><td>You are restoring your Exchange server to a different, preexisting server</td><td>Reset the machine account in the domain and name the server, using the same name as the original Exchange server, and proceed to Step 4.
For more information about performing this step, see the appropriate Microsoft Knowledge Base article, as listed before this procedure.
Attention
Do not install Exchange at this time. Use the KB article only to rename the server. Make sure that you perform the account reset, as specified in the Knowledge Base article, rather than deleting the account and re-creating it.</td></tr>
</table>

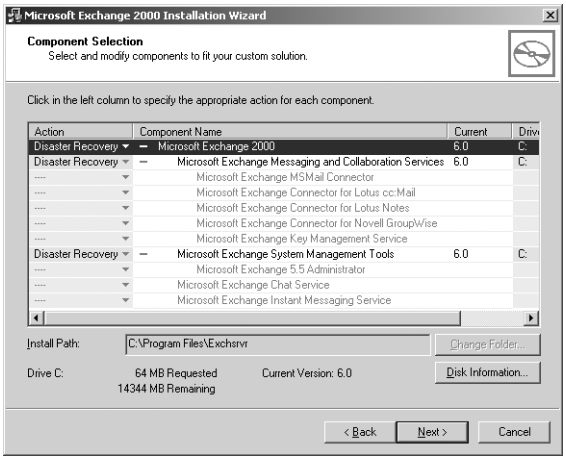
<table>
<tr><th>Steps</th><th colspan="2">Action</th></tr>
<tr><td>3</td><td colspan="2">Perform a full restore of the Exchange server, without the Exchange databases, using the backup application you used to create the backup.

See the documentation for your backup software and the Disaster Recovery for Microsoft Exchange 2000 Server document.</td></tr>
<tr><td rowspan="3">4</td><td>If...</td><td>Then...</td></tr>
<tr><td>Your backup software backed up the SnapDrive software</td><td>Proceed to Step 5.</td></tr>
<tr><td>Your backup software was not configured to back up the SnapDrive software</td><td>Reinstall the same version of SnapDrive used before the disaster occurred.

For information about installing SnapDrive, see your SnapDrive documentation.</td></tr>
<tr><td>5</td><td colspan="2">Using SnapDrive, connect the LUNs, or ensure that they are connected, and that you are using the same drive letters used before the disaster.</td></tr>
</table>

<table>
<tr><th>Steps</th><th colspan="2">Action</th></tr>
<tr><td>6</td><td>If...</td><td>Then...</td></tr>
<tr><td></td><td>Your backup software backed up the Exchange Server software</td><td>Proceed to Step 7.</td></tr>
<tr><td></td><td>Your backup software was not configured to back up the Exchange Server software</td><td>Install Exchange and any required Exchange service packs in disaster recovery mode.

For details, see the appropriate Microsoft Knowledge Base article, as listed before this procedure.

Note
Do not mount any storage groups yet.</td></tr>
<tr><td colspan="3"> 
</td></tr>
</table>

<table>
<tr><th>Steps</th><th colspan="2">Action</th></tr>
<tr><td rowspan="3">7</td><td>If...</td><td>Then...</td></tr>
<tr><td>Your backup software backed up the SnapManager software</td><td>Proceed to Step 8.</td></tr>
<tr><td>Your backup software was not configured to back up the SnapManager software</td><td>Reinstall the same version of SnapManager used before the disaster and run the Configuration Wizard to ensure that your configuration matches exactly the configuration used before the disaster.
Note
Because you are reconstructing your original configuration, no data is moved by the Configuration Wizard. However, running the Configuration Wizard is necessary for SnapManager to function correctly.</td></tr>
<tr><td>8</td><td colspan="2">Restore the most recent backup using SnapManager Restore.
For more information about using SnapManager Restore, see “Restoring Databases with SnapManager” on page 183.</td></tr>
<tr><td>9</td><td colspan="2">Launch the Outlook client and verify that your data was properly restored and that the Exchange server is operating correctly.</td></tr>
<tr><td>10</td><td colspan="2">Perform a SnapManager backup and verification to verify that your restored database is free of physical-level corruption.</td></tr>
</table>

About recovering both a failed storage system and a failed Exchange server

If both the storage system and the Exchange server fail, in most cases, you should recover the storage system first so that the data—or the space to recover the data—is available.

Successful recovery of the Exchange server depends on the existence of following components:

- A recent, usable backup of the Exchange server or a replicated Windows environment to enable the re-creation of the Exchange server
- Archive of a recent, verified SnapManager backup set or SnapMirror destination volumes containing the SnapManager backup set

Which failed storage system and server recovery procedure to use:

The procedure you use to recover both a failed storage system and a failed Exchange server depends on whether you employed SnapMirror or archiving. Use the appropriate procedure, as follows.

If you employed…	Then use…
SnapMirror	"Recovering both a failed storage system and Exchange server using SnapMirror" on page 245
Archiving	"Recovering both a failed storage system and Exchange server using archiving" on page 249

Recovering both a failed storage system and Exchange server using SnapMirror

To recover both the storage system and the Exchange server using SnapMirror replication, complete the following steps.

Step	Action
1	Ensure that the storage system hosting the SnapManager destination volumes is online and that the volumes are available and shared through CIFS. For information about creating CIFS shares, see your SnapDrive documentation. For information about general storage system administration, see the *Data ONTAP System Administration Storage Management Guide* for your version of Data ONTAP.

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td>2</td><td colspan="2">Perform a full restore of the Exchange server, without the Exchange databases, using the backup application you used to create the backup.

For more information about restoring your Exchange server, see the documentation for your backup software and the appropriate Microsoft disaster recovery document as described in “Guides you should read and have at hand” on page 224.

Note
If a backup of the Exchange server is not available and your Windows environment is an exact duplicate of the environment before the failure, you can reconstruct the Exchange server. For details, see “Recovering a failed storage system and server to a replicated environment” on page 252, using your new environment as the replicated environment.</td></tr>
<tr><td rowspan="3">3</td><td>If...</td><td>Then...</td></tr>
<tr><td>Your backup software backed up SnapDrive</td><td>Proceed to Step 4.</td></tr>
<tr><td>Your backup software was not configured to back up SnapDrive</td><td>Reinstall the same version of SnapDrive used before the disaster occurred.

For information about installing SnapDrive, see your SnapDrive documentation.</td></tr>
</table>

Step	Action
4	From the MMC on the Exchange server, use SnapDrive to connect to the LUNs in the active file system of the SnapMirror destination volume. Make sure that you use the same drive letters for the same LUNs as your original configuration. **Note** Do not mount the Exchange databases yet. The SnapManager Restore process mounts the databases. If you get an error when connecting, such as "Disk is in exclusive use," use FilerView to ensure that the LUN is unmapped from all igroups and online. For information about connecting LUNs, see your SnapDrive documentation. **Result:** The mirror is broken and an SFSR is performed, restoring the LUNs from the most recent SnapManager or SnapDrive Snapshot copy. Another SFSR will be performed in a later step, during the SnapManager restore.

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td rowspan="3">5</td><td>If...</td><td>Then...</td></tr>
<tr><td>Your backup software backed up SnapManager</td><td>Proceed to Step 6.</td></tr>
<tr><td>Your backup software was not configured to back up SnapManager</td><td>Reinstall the same version of SnapManager used before the disaster and run the Configuration Wizard to ensure that your configuration matches exactly the configuration used before the disaster.

Note
Because you are reconstructing your original configuration, no data is moved by the Configuration Wizard. However, running the Configuration Wizard is necessary for SnapManager to function correctly.</td></tr>
<tr><td>6</td><td colspan="2">Restore the most recent backup using SnapManager Restore.

For more information about using SnapManager Restore, see “Restoring Databases with SnapManager” on page 183.</td></tr>
<tr><td>7</td><td colspan="2">Launch the Outlook client and verify that your data was properly restored and that the Exchange server is operating correctly.</td></tr>
<tr><td>8</td><td colspan="2">Perform a SnapManager backup and verification to verify that your restored database is free of physical-level corruption.</td></tr>
</table>

Recovering both a failed storage system and Exchange server using archiving

To recover both the storage system and the Exchange server using archiving, complete the following steps.

Step	Action	
1	Bring the failed storage system back online.	
2	Perform a full restore of the Exchange server, without the Exchange data, using the backup application you used to create the backup. For more information about restoring your Exchange server, see the documentation for your backup software and the appropriate Microsoft disaster recovery document as described in "Guides you should read and have at hand" on page 224. **Note** If a backup of the Exchange server is not available and your Windows environment is an exact duplicate of the environment before the failure, you can reconstruct the Exchange server. For details, see "Recovering a failed storage system and server to a replicated environment" on page 252, using your new environment as the replicated environment.	
3	**If...**	**Then...**
	Your backup software backed up SnapDrive	Proceed to Step 4.
	Your backup software was not configured to back up SnapDrive	Reinstall the same version of SnapDrive used before the disaster occurred. For information about installing SnapDrive, see your SnapDrive documentation.
4	Using the archive tool you used to create the archive, restore the archived database LUNs to the storage system volume.	

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td rowspan="3">5</td><td>If...</td><td>Then...</td></tr>
<tr><td>You archived the LUNs containing the SnapInfo directory and the transaction logs</td><td>Restore these LUNs.</td></tr>
<tr><td>You did not archive the LUNs containing the SnapInfo directory and the transaction logs</td><td>Create new LUNs using the same drive letters as your original configuration, in the same volumes as they were before.</td></tr>
<tr><td>6</td><td colspan="2">Using SnapDrive on the Exchange server, connect to the LUNs you restored from archive with the same drive letters as your original configuration.
Note
Do not mount the Exchange databases yet. The SnapManager Restore process mounts the databases.</td></tr>
</table>

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td rowspan="3">7</td><td>If...</td><td>Then...</td></tr>
<tr><td>Your backup software backed up SnapManager</td><td>Proceed to Step 8.</td></tr>
<tr><td>Your backup software was not configured to back up SnapManager</td><td>Reinstall the same version of SnapManager used before the disaster and run the Configuration Wizard to ensure that your configuration matches exactly the configuration used before the disaster.

Note
Because you are reconstructing your original configuration, no data is moved by the Configuration Wizard. However, running the Configuration Wizard is necessary for SnapManager to function correctly.</td></tr>
<tr><td>8</td><td colspan="2">Perform the procedure for archive recovery described in “Recovering Exchange data using archives” on page 233, starting with Step 9.</td></tr>
</table>

Recovering a failed storage system and server to a replicated environment

To recover both the storage system and the Exchange server to a replicated environment, complete the following steps.

Note

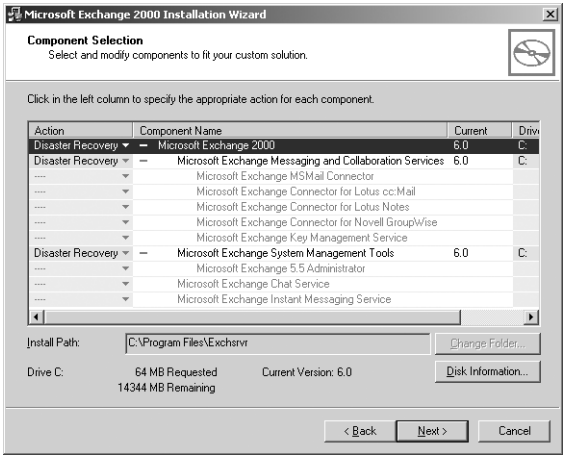
This procedure assumes that you have your Windows environment replicated, as described in "Replicating your Exchange environment" on page 228. This includes a replicated Active Directory Domain Controller, so your supporting Windows environment matches your previous environment exactly.

For this configuration, the term "original Exchange server" refers to the Exchange server running in your original environment that has failed. The term "recovery Exchange server" refers to the Windows host that will run Exchange in the replicated environment after you complete this procedure.

Step	Action
1	Ensure that you have `rsh` access to the storage system hosting the SnapMirror destination volumes. For more information about managing access from administration hosts, see the *System Administration Storage Management Guide* for your version of Data ONTAP.
2	Ensure that the storage system hosting the SnapMirror destination volumes is online and that the volumes are available and shared through CIFS. For information about creating CIFS shares, see your *Data ONTAP System Administration File Access Management Guide*. For information about general storage system administration, see your *Data ONTAP System Administration Storage Management Guide.*

Step	Action
3	Follow the steps in the appropriate Microsoft Knowledge Base article to reset the computer account and rename the standby Exchange server in your new environment to the name of the original Exchange server: ◆ If your original Exchange server was running Exchange 2000, use article 297289. ◆ If your original Exchange server was running Exchange 2003, use article 822945. **Attention** Do not install Exchange yet. This is done in a later step. Make sure that you perform an account reset, rather than deleting the account and re-creating it.
4	Make sure that the same version of SnapDrive that was running on your original Exchange server is installed on your standby Exchange server.
5	From the MMC on the standby Exchange server, use SnapDrive to connect to the LUNs in the active file system of the SnapMirror destination volume. Make sure that you use the same drive letters for the same LUNs as your original configuration. For information about connecting LUNs, see your SnapDrive documentation. **Note** If you get an error when connecting, such as "Disk is in exclusive use," use FilerView to ensure that the LUN is unmapped from all igroups and online. **Result:** The mirror is broken and then the LUN is restored using the most recent SnapDrive Snapshot copy.

Step	Action
6	If the LUN that stores the transaction logfiles resides on a different volume than the LUN that stores the SnapInfo directory and the volume containing the transaction logs LUN is not mirrored, you must create a new LUN—in the active file system of a SnapMirror destination volume that does not contain a LUN with Exchange databases—for the transaction logs. **Note** It is not a requirement to replicate the volume that contains the LUN that stores the Exchange transaction logs, and this LUN can reside on its own separate and un-mirrored volume. As a result, the LUN that stores the Exchange transaction logs LUN might not get replicated to the SnapMirror destination storage system. If you need to create a new LUN for the transaction logs, complete the following steps: **a.** On the destination storage system, create a volume of a size equal to or greater than that of the volume on the source storage system that contains the LUN for the transaction logs. **b.** Use SnapDrive to create a LUN of equal or greater size. The same drive letter must be used.

Step	Action
7	Using the Microsoft Knowledge Base article you used in Step 3, install Exchange and any required Exchange service packs *in disaster recovery mode* on your standby Exchange server.  **Result:** When you complete this step, your standby Exchange server should be running exactly the same version of Exchange, including service packs, as your original Exchange server.
8	On the standby Exchange server, install the same version of SnapManager as was running on your original Exchange server.
9	Launch SnapManager and run the SnapManager Configuration Wizard to ensure that the correct configuration is used. If necessary, modify the configuration so that it matches exactly the configuration before the failure.
10	Restore the most recent backup using SnapManager Restore. For more information about using SnapManager Restore, see "Restoring Databases with SnapManager" on page 183.
11	Launch the Outlook client and verify that your data was properly restored and that the standby Exchange server, which now becomes your primary Exchange server, is operating correctly.

Step	Action
12	After you repair or replace your primary site, you can return to your original configuration. For more information about returning to your original site replication configuration, see "Returning to your original site replication configuration" on page 256.

Returning to your original site replication configuration

If you needed to perform disaster recovery using a replicated site, you probably want to return to your original site replication configuration. Because Exchange is now running on the replicated site, you must perform this operation correctly to avoid data loss as you switch back over to the original site.

To return to using Exchange on your primary site after you perform disaster recovery using your replicated site, complete the following steps.

Note

In this procedure, your original primary site is called the primary site (although before you perform the procedure, it is not running Exchange), and the site and server you are currently running Exchange on are called the replicated site and the standby Exchange server.

This procedure references two Microsoft Knowledge Base articles. The article that you use depends on your version of Exchange. For Exchange 2000, use article 297289. For Exchange 2003, use article 822945.

Attention

Do not install any application software on the primary site until instructed to do so.

Step	Action
Prepare primary site	
1	Repair or replace the storage system on your primary site. For more information about setting up your storage system, see the *System Administration Storage Management Guide* for your version of Data ONTAP.

Step	Action
2	Reconstruct the Windows environment, including the Active Directory Domain Controller, on your primary site by replicating the environment back from the replicated site.
Create temporary mirror	
3	Using SnapMirror, create a mirror with the replicated site as the (temporary) source and the primary site as the (temporary) destination. **Note** Remember that a destination volume must be at least as large as its source volume. If your original destination volume was larger then your original source volume, you need to increase the size of the temporary destination volume to match the size of the temporary source volume. If your original primary storage system was not affected by the disaster, you can use the `snapmirror resync` command to perform this step more quickly. For more information about this command, see the *System Administration Data Protection Guide* for your version of Data ONTAP.
Capture Exchange data	
4	On the standby Exchange server, perform a SnapManager backup and verification of all storage groups.
5	Block all user access to Exchange. **Note** This step is necessary because all changes to the Exchange data store made after the mirror is updated are lost when you switch over to the primary site.

Step	Action
6	Use SnapDrive to perform an update mirror operation using the following `sdcli` command once for every volume containing Exchange or SnapInfo data: **`sdcli snap update_mirror -d`** *drive* For more information about the SnapDrive command-line interface, see your SnapDrive documentation.
7	Shut down the standby Exchange server.
Reconstruct primary Exchange server	
8	Using the appropriate Microsoft Knowledge Base article for your version of Exchange, reset the machine account in the domain. **Attention** Make sure that you perform the account reset, as specified in the Knowledge Base article, rather than deleting the account and re-creating it.
9	Install and configure Windows on the primary Exchange server. **Attention** If you repaired the original Exchange server, wipe its disks and reinstall the operating system. Do not attempt to bring the server back online with the original software.
10	Install any Windows service packs that were installed on the primary Exchange server.
11	Ensure that you have `rsh` access to the newly reconstructed or repaired storage system.
12	Install and configure SnapDrive on the primary Exchange server.

Step	Action
13	Using SnapDrive, connect to the LUNs in the active file system of the newly reconstructed or repaired storage system. **Attention** Be sure you use the same drive letters that were used in your original primary site, and as should be in use in your recovery site. **Result:** The reverse direction mirror you created in Step 3 is broken and an SFSR is performed.
14	Using the appropriate Microsoft Knowledge Base article for your version of Exchange, install Exchange and any required Exchange service packs *in disaster recovery mode* on the primary Exchange server.
15	Install the same version of SnapManager for Microsoft Exchange that was installed on the primary Exchange server.
16	Launch SnapManager and run the SnapManager Configuration Wizard, making sure to keep all data on the same drives where it was before.
Restore and verify Exchange data	
17	Use SnapManager Restore to restore the backup you created in Step 4.
18	Launch the Outlook client and verify that your data was properly restored and that the new primary Exchange server is operating correctly.
Re-create mirror	
19	Delete the (reversed) mirror configuration you created in Step 3.
20	Re-create your original mirror, with your newly reconstructed storage system as the source, and the replicated site as the destination.
Reconfigure replicated site	

Step	Action
21	Return your standby Exchange server to standby mode by performing these steps: **a.** Wipe the disks. **b.** Using a different name than the primary Exchange server, reinstall the correct version of the operating system and any required service packs. **c.** Place the standby Exchange server into a workgroup. (This step is optional.) **Result:** Your replicated site is ready once again in case of the loss of or damage to your primary site.

Disaster recovery by relocating Exchange virtual servers to a different Windows cluster

This section describes a disaster recovery method that consists of relocating Exchange virtual servers to a different Windows cluster. See the following topics for more information:

- "About this method" on page 261
- "Preparing to configure the production and DR sites" on page 262
- "Configuring the production and DR sites" on page 263
- "Bringing the production site online" on page 266
- "Bringing the DR sites online" on page 271
- "Failing over to a DR site" on page 273
- "Failing back to the production site" on page 278
- "Changing the IP addresses of SMTP and HTTP virtual server cluster resources" on page 295

About this method

The following paragraphs summarize a disaster recovery scenario that uses SnapManager and SnapMirror in a clustered environment.

The configuration consists of a Windows cluster with Microsoft Exchange and NetApp products at a production site along with a different but similarly configured cluster at a disaster recovery (DR) site. There are likely to be numerous DR sites, geographically remote from one another.

The Exchange data and the SnapManager backup sets are stored on Data ONTAP LUNs. The backup sets are asynchronously mirrored from the production site to the DR sites using SnapMirror. SnapManager for Exchange is used for Exchange backup and recovery as well as to drive the SnapMirror replication schedule. SnapDrive is used for LUN provisioning and management.

In the event of a disaster, an Exchange virtual server can fail over from the production site to a DR site and then, after the original production site has been repaired, the DR site can fail back to the production site. Exchange data that changed while running at the DR site is mirrored back to the production site and retained.

Preparing to configure the production and DR sites

Before you begin configuring your production and DR sites, ensure that you complete the prerequisite tasks described in this section.

Windows host systems: Each Windows host system must be installed with the following:

- One of the following versions of Windows:
  - Windows 2000 Advanced Server
  - Windows Server 2003 Enterprise Edition
- Exchange Server 2003
- SnapManager for Exchange 3.1 or newer
- A version of SnapDrive, 3.2D1 or newer, that is supported by SnapManager
- A version of Data ONTAP that is supported by your version of SnapDrive

Note

Data ONTAP 7.1 introduced functionality that enables faster restore times, which is recommended for use with SnapManager. SnapManager 3.2 supports SnapDrive 4.1 only, which in turn supports Data ONTAP 7.0.*x* and 7.1.

Windows clusters: Each Windows cluster must meet the following requirements:

- The production and DR clusters must be in the same Active Directory site.
- The Exchange virtual server name must be maintained.

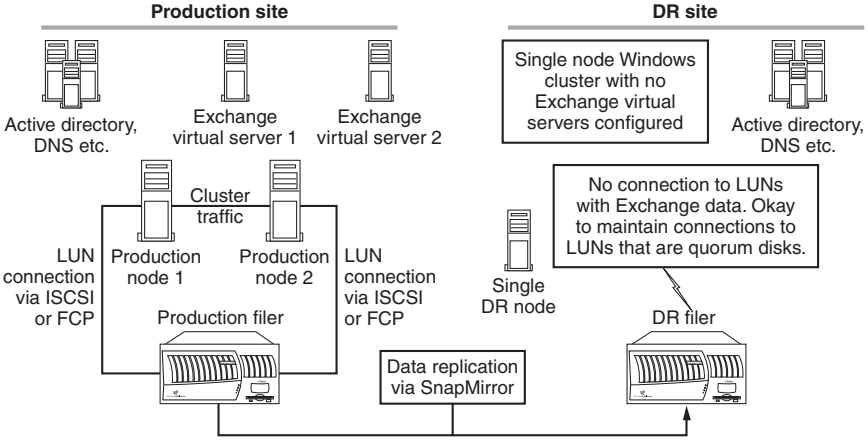
Supporting documentation: Although this document describes how to move an Exchange virtual server from one Windows cluster to another in a Microsoft and NetApp environment, it does *not* describe how to restore the supporting Windows infrastructure.

For more information about Exchange disaster recovery and its dependencies, see the following Microsoft articles:

- For Exchange 2000, see Microsoft article KB326052, *White Paper - Disaster Recovery for Microsoft Exchange 2000 Server.*
- For Exchange Server 2003, see Microsoft article KB867704, *The "Exchange Server 2003 Disaster Recovery Operations Guide" is available*.

Configuring the production and DR sites

The production and DR sites can consist of one or more Windows clusters running one or more Exchange virtual servers where each cluster has one or more nodes (two nodes or more are recommended). Data storage for Exchange is provided by one or more storage systems. The following example shows a two-node production Windows cluster running one Exchange virtual server on each node. The DR Windows cluster contains a single node. There is one storage system at each site.



Exchange Disaster Recovery Topology

The production and DR sites are set up with storage system volumes of identical sizes. Initially, SnapMirror relationships are configured between the source volumes on the production site and destination volumes on the DR sites. While in production, data is mirrored from SnapMirror source volumes at the production site to SnapMirror destination volumes at each of the DR sites.

If a disaster occurs at the production site, you can fail over operations to one of the DR sites. After the original production site is repaired, the DR site can fail back to the production site and the data will be mirrored back in the opposite direction using SnapMirror.

Where to locate the quorum disks: To properly configure Windows clusters, you need to understand the proper location of quorum disks:

- Because the Windows clusters at the production site and at the DR sites are each autonomous clusters, each cluster requires its own quorum disk.

  If you use a Data ONTAP LUN as a quorum disk, that LUN must reside on a storage system at the same site where the Windows cluster itself resides:

  - For the production Windows cluster, locate the quorum disk LUN on the storage system at the production site.

- For a DR Windows cluster, locate the quorum disk LUN on a storage system at that DR site.

- There is no need to mirror the quorum disk from the production storage system to the DR storage system. Therefore, to avoid transferring unnecessary data across a WAN, locate the quorum disk LUNs on non-mirrored storage system volumes.

Tip for creating and mapping LUNs: Standardizing across all clusters (at the production site and at all DR sites) on an identical mapping of **LUN names** to **drive letters** can simplify disaster recovery activities, from initial configuration through maintenance, failover, and failback.

For example, the following mapping of LUN names and drive letters could be adopted by the database administrators at the production site and each DR site.

Drive letter	LUN name	LUN storage purpose
`I:`	`db.lun`	Microsoft Exchange databases
`L:`	`logs.lun`	Microsoft Exchange transaction logs
`T:`	`data.lun`	Microsoft Exchange “data directory”
`N:`	`snapinfo.lun`	SnapManager SnapInfo directory

Note

If you adopt the best practice of keeping detailed and up-to-date notes about your DR plans, remember to keep a printed hardcopy.

NetApp storage system performance considerations: Exchange performance might be significantly lower at the DR site than at the production site:

- If the storage system at the DR site is a less powerful model than the one at the production site, it will yield lower performance than the storage system at the production site.
- In the event of a disaster, a single DR cluster could potentially host multiple Exchange virtual servers from more than one production cluster.

Because of this, you should be aware that Exchange performance at the DR site could be significantly lower than would be expected at the production site.

Configuration procedure: To configure the production and DR sites, complete the following steps.

Step	Action
1	At the production site, create the storage system volumes. Typically, the size and number of volumes will be determined with the help of Network Appliance during the sales cycle. Volume sizing information is also available in the *SnapManager for Exchange Installation and Administration Guide* and in the *Exchange Best Practices Guide* (TR3233).
2	At the DR site, create the storage system volumes. **Note** The SnapMirror source and destination volumes must be identical in size. The supporting infrastructure required for the Exchange virtual server, the Windows cluster, and the storage system must be in place, up to date, and functioning at the DR site. This includes, but is not limited to, Active Directory, DNS, WINS, and Network connectivity.
3	Configure SnapMirror with a non-schedule. This is described in the *SnapDrive Installation and Administration Guide*, in the section "Using SnapMirror with SnapDrive."
4	To minimize data loss, you can configure SnapDrive to replicate the transaction log volume more frequently in between SnapManager backups. This is described in the *SnapManager Installation and Administration Guide*, in the section "Using SnapMirror with SnapManager."

Bringing the production site online

Complete the following steps at the production site.

Step	Action
1	Configure a Windows cluster and then install Windows Server on all nodes of the cluster, but do *not* install or configure Exchange yet. **Note** The quorum disk can be a Data ONTAP LUN, but this is not a requirement. For more information, see "Where to locate the quorum disks" on page 263. For details about configuring the cluster, refer to Microsoft documentation.
2	Using the Cluster Administrator, create a cluster resource group named "Exchange" for the Exchange cluster resources. **Note** The cluster group names of "Exchange" and "Exchange DR" are used in this document for clarity and only as examples. Using these cluster group names is not a requirement.
3	Create a new "IP address" cluster resource in the Exchange DR cluster group. **Note** Due to the TCP/IP subnet configuration at the DR site, this IP address will probably be different from that of the production site.
4	Create a new "Network Name" cluster resource in the Exchange DR cluster group. **Note** Later, in the procedure "Bringing the DR sites online" on page 271, you will use the same network name for the Exchange virtual server at the DR site as was in use at the production site.
5	Install SnapDrive on all cluster nodes, following the instructions in the *SnapDrive Installation and Administration Guide*.

Step	Action
6	If using iSCSI, establish an iSCSI connection from one of the production site cluster nodes to the production storage system.
7	On a SnapMirror source volume on the production storage system, create LUNs to store the following: ◆ Exchange databases ◆ Exchange transaction logs ◆ SnapManager SnapInfo directory To do this, complete the following steps: **a.** Using SnapDrive, create "shared" LUNs on a SnapMirror source volume on the storage system at the production site. Refer to "Tip for creating and mapping LUNs" on page 264. **b.** When prompted by SnapDrive, select the Exchange cluster resource group you created in Step 2. This creates the shared physical disk resources on the cluster nodes of the production site.

Step	Action
8	On a SnapMirror source volume on the production storage system, create a separate LUN to store the "Exchange data directory": **a.** Using SnapDrive, create another "shared" LUN on a SnapMirror source volume on the storage system at the production site. Again, refer to "Tip for creating and mapping LUNs" on page 264. **b.** When prompted by SnapDrive, select the Exchange cluster resource group you created in Step 2. This places the LUN in the Exchange cluster resource group created in Step 7. Later, when you create the Exchange System Attendant cluster resource for the first time, you will be prompted for this LUN. This LUN will also be used for the Exchange SMTP and MTA queues and Microsoft Search. SnapManager can be used later to configure the SMTP and MTA locations, if desired. **Note** The Microsoft Search Directory can be moved manually, as described in the Microsoft TechNet document "Working with Exchange Server 2003 Stores."
9	Install Exchange on all nodes in the cluster and then apply any Exchange service packs to all nodes in the cluster. **Note** Install the same version of Exchange and apply the same Exchange service pack to all nodes in the production cluster. In the next procedure, "Bringing the DR sites online" on page 271, you will use this same version and service pack on all nodes in the DR cluster.

Step	Action
10	Using the Cluster Administrator, do the following: **a.** Create a new Exchange System Attendant cluster resource in the Exchange cluster resource group. This automatically creates all of the other Exchange cluster resources. **b.** When prompted for the Exchange "data directory," use the separate LUN you created in Step 7. The prompt will include a drive letter and path. The drive letter will simply be the first available drive letter within the cluster resource group. Only the drive letter needs to be changed. The path can remain unmodified.
11	Install and configure SnapManager on all nodes of the cluster.
12	Make the cluster node you are working on the owner of the Exchange cluster resource group: **a.** Use the Cluster Administrator to perform a "move group" operation. **b.** When SnapManager prompts for a location for the MTA and SMTP files, place them on the separate LUN you created for the Exchange "data directory" in Step 7. These files need to be kept on a separate LUN from the Exchange database, transaction logs, and the SnapManager SnapInfo directory.
13	Verify that the Exchange virtual server at the production site is up and running: **a.** Use the Cluster Administrator to make sure that the cluster resources are online. **b.** Use the Exchange System Manager to make sure that the database is mounted.

Step	Action
14	Create a SnapManager backup and confirm that SnapMirror is functioning properly. There are three ways to check that SnapMirror replication occurred: ◆ View the backup report in the "SnapManager Reports tab". ◆ View the events logged in the "Windows Application Event log". ◆ View the SnapMirror information on the "Storage system".

SnapManager Reports tab: Look at the backup report for the backup that was just run. The following text will appear toward the end of the report:

```
*** REQUEST SNAPMIRROR UPDATE AFTER BACKUP ***
Starting SnapMirror update...

Querying disk list for SnapMirror update...

Requesting SnapMirror update for LUN [I:] on volume [exch_db] of
storage system [exch-dr-filer]...
Request for SnapMirror update for LUN [I:] was completed
successfully.

Requesting SnapMirror update for LUN [L:] on volume [exch_logs] of
storage system [exch-dr-filer]...
Request for SnapMirror update for LUN [L:] was completed
successfully.
```

Windows Application Event log: This is an example of the events that might be seen when there are two volumes in use:

```
Event Type: Information
Event Source: SnapDrive
Event Category: SnapMirror event
Event ID: 144
Date:  7/14/2005
Time:  2:08:47 PM
User:  N/A
Computer: EXCHANGE
Description:
A SnapMirror update request to destination (exch-filer:exch_db) was
successfully sent.

Event Type: Information
```

```
Event Source: SnapDrive
Event Category: SnapMirror event
Event ID: 144
Date:  7/14/2005
Time:  2:08:50 PM
User:  N/A
Computer: EXCHANGE
Description:
A SnapMirror update request to destination (exch-filer:exch_logs)
was successfully sent.
```

Storage system: Using a web browser, bring up FilerView on the storage system that is the SnapMirror destination:

a. To bring up FilerView, enter `http://filername/na_admin` into the address field of the web browser, where *filername* is the name of the storage system at the production site.

Example: `http://dr_filer/na_admin`

b. When the page loads, click the FilerView link.

c. Click SnapMirror and then click Manage. Information about the SnapMirror relationships is displayed.

Bringing the DR sites online

There can be numerous DR sites around the globe. To prepare the DR sites for disaster recovery, complete the following steps *at each DR site*.

Attention

Only one Exchange virtual server with a given network name can be online at a time, otherwise connectivity issues will arise.

Step	Action
1	Install Windows Server on all nodes of the cluster and then configure the default cluster group, but do *not* install or configure Exchange yet. **Note** The quorum disk can be a Data ONTAP LUN, but this is not a requirement. For more information, see "Where to locate the quorum disks" on page 263. For details about configuring the cluster, refer to Microsoft documentation.
2	Install SnapDrive on all cluster nodes, following the instructions in the *SnapDrive Installation and Administration Guide*.
3	If using iSCSI, establish an iSCSI connection from one of the cluster nodes at this DR site to the DR storage system. **Note** Do *not* connect to any of the LUNs that will be used by the Exchange virtual server yet. This is done later as part of the recovery procedure.
4	Install Exchange on all nodes in the cluster and then apply any Exchange service packs to all nodes in the cluster. **Note** Be sure to use the same Exchange version and service pack that you installed on the nodes of the production cluster, described in the "Bringing the production site online" on page 266. Install the same version of Exchange and apply the same Exchange service pack to all nodes in the DR cluster.
Create the cluster resource group and install SnapManager for Exchange	
Although it saves time if you create this cluster resource group and the cluster resources prior to disaster, it is not a requirement. You can choose to postpone performing the remaining steps in this procedure until you need to fail over to this DR site.	

Step	Action
5	Using the Cluster Administrator, create a cluster resource group named “Exchange DR” for the Exchange cluster resources. **Note** The cluster group names of “Exchange” and “Exchange DR” are used in this document for clarity and only as examples. Using these cluster group names is not a requirement.
6	Create a new “IP address” cluster resource in the Exchange DR cluster group. **Note** Due to the TCP/IP subnet configuration at the DR site, this IP address will probably be different from that of the production site.
7	Using the Cluster Administrator, do the following: **a.** Create a new “Network Name” cluster resource in the Exchange DR cluster group. Use the same network name for the Exchange virtual server at the DR site as was in use at the production site. **b.** Leave the Exchange DR cluster group (or just the Network Name cluster resource) offline. It will be brought online at a later time as part of the recovery procedure. The Network Name cluster resource at the DR site *cannot* be online while the same Network Name cluster resource is online at the production site.
8	Do *not* add Exchange cluster resources yet. This is done later, as part of the recovery procedure.
9	Install SnapManager for Exchange on all nodes of the cluster, but do *not* configure it yet.

Failing over to a DR site

At the DR site to which you want to fail over, perform the following steps.

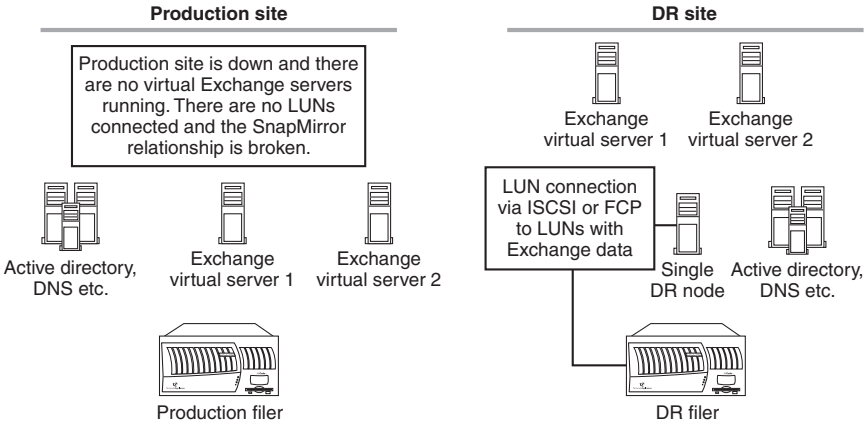
Step	Action
1	Ensure that the Exchange cluster group at the production site is offline. **Note** Only one Exchange virtual server with a given network name can be online at a time. This is required because the virtual Exchange server on the DR cluster will be brought online with the same network name.
2	If the DR cluster will take over the Exchange services *within one hour* of the time that the production site went offline, use the Active Directory Users and Computers MMC to reset the machine account for the Exchange virtual server. If you fail to do this, you might encounter client authentication issues. **Attention** Do *not* delete and re-create this account. Doing so will make it impossible to recover the Exchange server.
3	If the production cluster is different from the DR cluster, update the DNS record for the virtual Exchange server's network name with the IP address at the production cluster. **Note** Until you complete the Active Directory, DNS, and WINS replication to reflect the IP change and refresh the client cache, client connectivity issues might occur.
4	Using the Cluster Administrator, check the Network Name cluster resource in the Exchange DR cluster resource group to ensure that the correct name is in use. It must exactly match the network name that was in use for the Exchange virtual server at the production site.

Step	Action
5	If, when this DR site was brought online, the cluster resource group was not created and SnapManager for Exchange was not installed, do so now: **a.** Locate the procedure "Bringing the DR sites online" on page 271. **b.** Complete all the steps in the section "Create the cluster resource group and install SnapManager for Exchange" on page 272.
6	Using SnapDrive, do the following: **a.** Reconnect to the LUNs on the SnapMirror destination volume using the same drive letters that were used at the production site and, when prompted, specify a Virtual Disk Type of "shared." If you do not use the same drive letters that were used at the production site, the SnapManager restore operation will fail. The drive letters will not be available if they are still configured as physical disk resources for any reason, even if they are not actually mapped to LUNs. If the production Exchange server with SnapManager is still available, the drive letter to LUN mappings can be found in the SnapManager Configuration reports that reside in a special shared directory under the SnapManager installation directory. **b.** When prompted, select the Exchange DR cluster resource group. This creates the shared physical disk resources on the cluster nodes.
7	Using the Cluster Administrator, add the Exchange System Attendant cluster resource. This creates the remaining resources automatically and uses all of the same drive letters. You will *not* be able to change them.
8	Install and configure SnapManager on all nodes of the cluster.

Step	Action
9	Make the cluster node you are working on the owner of the Exchange cluster resource group: **a.** Use the Cluster Administrator to perform a "move group" operation. **b.** When SnapManager prompts for a location for the MTA and SMTP files, place them on the separate LUN you created for the Exchange "data directory." These files need to be kept on a separate LUN from the Exchange database, transaction logs, and the SnapManager SnapInfo directory. Specify the same path for the SnapInfo directory; otherwise, the backup sets will not be visible under the SnapManager Restore tab.
10	Perform a SnapManager for Exchange restore operation with the following options selected: ◆ "Use the most recent backup set" ◆ "Up-to-the-minute restore" ◆ "Mount databases automatically after restore"
11	Verify that the virtual Exchange server on the DR cluster is up and running: **a.** Use the Cluster Administrator to verify that the Exchange virtual server is online. **b.** Use the Exchange System Manager to verify that the Exchange databases are mounted.
12	If the cluster is configured with SMTP or HTTP virtual server cluster resources, these resources could fail shortly after you bring them online. To prevent this from happening, follow the steps in "Changing the IP addresses of SMTP and HTTP virtual server cluster resources" on page 295 before proceeding.
13	Create a SnapManager backup immediately.

Step	Action
14	If you expect the DR cluster to remain online for any length of time, use SnapManager to configure reoccurring scheduled backup jobs. For details, see Appendix , “Backing up databases,” on page 164.

Here is an example of a configuration at the DR site:



Exchange Disaster Recovery Topology with DR Site Online

Failing back to the production site

To fail back to the production site, complete the following steps.

Step	Action
1	Before proceeding with this failback procedure, be sure that any **LUN clone split** operations have completed. The LUN clone split functionality, introduced in Data ONTAP 7.1, supports significantly faster online Snapshot copy restore times when using SnapManager or SnapDrive to restore. This functionality is enabled by default. To check that any LUN clone split operations have completed, use the storage system's `lun clone split status` command, or by viewing the Operation Status column in the SnapDrive MMC. For detailed information about this command, see the *Data ONTAP 7.1 Block Access Management Guide for iSCSI and FCP.* **Attention** If you attempt a failback procedure immediately after a failover that uses a LUN clone split (such as a dry run of a failover and failback), the LUN clone split operation could interfere with SnapMirror when trying to resynchronize the data back to the production site.
2	Create a final SnapManager backup on the DR cluster.
3	Prevent further user access by bringing the Exchange cluster resources offline, but leave the physical disk cluster resources online for the next step.

Step	Action

4	To ensure that you can bring the Exchange databases back online at the production site without first having to perform a SnapManager restore operation, verify that each Exchange database is in a consistent state. To do this, use the Exchange Server Database Utilities (`Eseutil.exe`) tool with the `/mh` option to view the header of each Exchange database and then check the value displayed next to "State" in the command output.
	
	The following example shows the `Eseutil /mh` command run against the database `priv1.edb`, located in the directory `I:\EXCHSRVR\mdbdata`. Only the first part of the command output is shown here:
	
	`C:\Program Files\Exchsrvr\bin>` **`eseutil /mh I:\EXCHSRVR\mdbdata\priv1.edb`**
	`Microsoft(R) Exchange Server Database Utilities`
	`Version 6.5`
	`Copyright (C) Microsoft Corporation. All Rights Reserved.`
	
	`Initiating FILE DUMP mode...`
	`Database: I:\EXCHSRVR\mdbdata\priv1.edb`
	`File Type: Database`
	`Format ulMagic: 0x89abcdef`
	`Engine ulMagic: 0x89abcdef`
	`Format ulVersion: 0x620,11`
	`Engine ulVersion: 0x620,11`
	`Created ulVersion: 0x620,11`
	`DB Signature: Create time:05/06/2005 16:35:18 Rand:2129456 Computer:`
	`cbDbPage: 4096`
	`dbtime: 136725 (0x21615)`
	`State: Clean Shutdown`
	
	Note
	If the database is in a consistent state, the information output under the "`Initiating FILE DUMP mode`" section includes the line "`State: Clean Shutdown`".
	
	Repeat this step for every database you need to bring back online at the production site.

Step	Action
5	Use the Cluster Administrator to delete the Exchange System Attendant cluster resource in the Exchange DR cluster resource group. This deletes all of the Exchange cluster resources, but the Physical Disk, IP, and Network Name resources remain intact. **Attention** Do *not* select the Remove Virtual Exchange Server option (available by right-clicking the Exchange DR cluster resource group). This option takes the Exchange server out of Active Directory. The following error might appear in the Windows Application Event Log: `Event Type: Error` `Event Source: MSExchangeCluster` `Event Category: Services` `Event ID: 1027` `Date:  6/23/2005` `Time:  4:46:46 PM` `User:  N/A` `Computer: EXCHSRVR` `Description:` `SA: System Attendant resource has been deleted improperly. The objects in Active Directory corresponding to this Exchange Virtual Server have not been removed. If you unintentionally deleted the System Attendant resource, you can restore it and its dependent resources to their original configuration by re-creating the System Attendant resource using the same parameters as before. If you want to remove the Exchange Virtual Server corresponding to this System Attendant resource, you have to re-create the System Attendant resource with the same parameters as before and then select the option "Remove Exchange Virtual Server" in the context menu of the group or System Attendant resource using the Cluster Administrator tool. For more information, click http://www.microsoft.com/contentredirect.asp.` `Data:` `0000: 00 00 00 00 ....` This error is expected here.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>6</td><td>Mirror the modified Exchange data on the SnapMirror destination volumes at the DR site back to the SnapMirror source volumes at the production site.<table><tr><th>If...</th><th>Then...</th></tr><tr><td>The original SnapMirror source volumes and Snapshot copies remain intact</td><td>Go to Step 7.</td></tr><tr><td>The data on the original SnapMirror source volume or the volume itself was lost</td><td>Go to Step 17.</td></tr></table></td></tr>
<tr><td colspan="2">If the original SnapMirror source volumes and Snapshot copies remain intact</td></tr>
<tr><td>7</td><td>Mirror only the changed blocks on the DR storage system volumes back over to the production storage system volumes.

To do this, go to the original SnapMirror source storage system command line interface and, for every volume that is being used by this Exchange/SnapManager configuration, issue the <code>snapmirror resync</code> command to mirror only the changed data at the DR site back to the production site.

Suppose you have an Exchange/SnapManager configuration with two volumes. In this example, the storage systems at the production site and the DR site are named <code>prod_filer</code> and <code>dr_filer</code>, respectively, and the volume names on both storage systems are <code>db_vol</code> and <code>logs_vol</code>. The following sequence of two commands illustrates how the <code>resync</code> command might be issued for this example configuration:

<code>prod_filer> snapmirror resync -S dr_filer:db_vol prod_filer:db_vol</code>

<code>prod_filer> snapmirror resync -S dr_filer:logs_vol prod_filer:logs_vol</code></td></tr>
</table>

Step	Action
8	Monitor the status of the operation by using the `snapmirror status` command on the production storage system, and do not proceed until the SnapMirror "`State`" is "`Snapmirrored`" for all volumes in this configuration. **Note** You can also check the status of the operation using FilerView on the production storage system.
9	Use SnapDrive to update the mirror. You can do this using either the SnapDrive graphical user interface (MMC) or the SnapDrive command-line interface (`sdcli.exe`). Only one mirror update per storage system volume is required; it is not necessary to perform an update for each drive letter. When SnapDrive is used to perform a SnapMirror update, updating a single LUN on a given volume actually updates all of the LUNs on the volume.
10	Monitor the status of the operation by using the `snapmirror status` command on the production storage system, and do not proceed until the SnapMirror "`State`" is "`Snapmirrored`" for all volumes in this configuration.
11	At the production storage system, break the reverse SnapMirror relationship. You can do this using either the `snapmirror break` command or FilerView. The data that changed at the DR site is now mirrored back to the production site.
12	Break the "resync" mirror in the reverse direction.

Step	Action
13	Reinstate the original SnapMirror relationship. To do this, issue another `snapmirror resync` command, but this time from the DR storage system. The following sequence of two commands illustrates how the `snapmirror resync` command might be issued. Following is an example of how this command might look using the example storage system and volume names used in Step 7. `dr_filer>` **`snapmirror resync db_vol`** `dr_filer>` **`snapmirror resync logs_vol`**
14	Confirm that the SnapMirror relationship has been re-created in the original direction: **a.** Open a web browser on the storage system that is the SnapMirror destination. **b.** To bring up FilerView, enter `http://filername/na_admin` into the address field of the web browser, where *filername* is the name of the storage system at the production site. For the example storage system names used in Step 7, the URL would be `http://prod_filer/na_admin`. **c.** After the page loads, click the FilerView link. **d.** Click SnapMirror and then click Manage. Information about the SnapMirror relationships displays. **e.** Be sure that the "`State`" is "`Snapmirrored`."
15	Go to Step 23 to finish the failback to the production site.

Step	Action	
If the data on the original SnapMirror source volume or the volume itself was lost		
16	**If...**	**Then...**
	Only the data on the original source volume was lost	Go to Step 17.
	The volume itself was lost	Do the following: **a.** Recreate the original SnapMirror source volume. **b.** Go to Step 17.

Step	Action
17	Create a new SnapMirror relationship in the reverse direction (from the SnapMirror destination volume at the DR site back to the SnapMirror source volume at the production site) and then initialize the mirror. This transfers all data from the original SnapMirror destination volume at the DR site back to the original SnapMirror source volume at the production site. This can be done using the storage system's command line or by using the FilerView graphical user interface. To do this using FilerView, complete the following steps: **a.** Open a web browser on the storage system that is the SnapMirror destination. **b.** To bring up FilerView, enter `http://filername/na_admin` into the address field of the web browser, where *filername* is the name of the storage system at the production site. For the example storage system names used in Step 7, the URL would be `http://prod_filer/na_admin`. **c.** After the page loads, click the FilerView link. **d.** Click SnapMirror and then click Manage. Information about the SnapMirror relationships displays. **e.** Be sure that the "`State`" is "`Snapmirrored`."
18	Using SnapDrive, update the mirror. This can be done using the SnapDrive GUI (MMC) or the command line (sdcli.exe). It is not required that an update be performed for each drive letter. Rather, only one update per storage system volume is required. When SnapDrive is used to perform a SnapMirror update, updating a single LUN on a given volume actually updates all of the LUNs on the volume.
19	Confirm that all data has been mirrored back to the repaired original SnapMirror source volume.
20	Break the mirror using the `snapmirror break` command or FilerView.

Step	Action
21	Un-configure the reverse SnapMirror relationship. This can be done using the storage system's a line or by using the FilerView graphical user interface. To do this using FilerView, complete the following steps: **a.** Open a web browser on the storage system that is the SnapMirror destination. **b.** To bring up FilerView, enter `http://filername/na_admin` into the address field of the web browser, where *filername* is the name of the storage system at the production site. For the example storage system names used in Step 7, the URL would be `http://prod_filer/na_admin`. **c.** After the page loads, click the FilerView link. **d.** Click SnapMirror and then click Manage. Information about the SnapMirror relationships displays.

Step	Action
22	Reestablish the original SnapMirror relationship in the original direction so that data from the production storage system is mirrored to the DR storage system. This can be done using the storage system's `snapmirror resync` command or by using the FilerView graphical user interface. Perform this task on the DR storage system. **a.** Open a web browser on the storage system that is the SnapMirror destination. **b.** To bring up FilerView, enter `http://filername/na_admin` into the address field of the web browser, where *filername* is the name of the storage system at the production site. For the example storage system names used in Step 7, the URL would be `http://dr_filer/na_admin`. **c.** After the page loads, click the FilerView link. **d.** After FilerView loads, click "SnapMirror" and then click "Manage." Information about the SnapMirror relationships is displayed. **e.** Create a SnapMirror relationship and then initialize it. **f.** Be sure that the "`State`" is "`Snapmirrored`."
Fail back to the production site	
23	Launch the Cluster Administrator on one of the nodes at the DR site: **a.** Bring the Network Name and IP address cluster resources offline in the Exchange DR cluster resource group. After the original mirror is reestablished, the DR cluster's physical disk resources show as failed. **b.** Use the Cluster Administrator to delete these failed cluster resources.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>24</td><td>If the DR cluster will take over the Exchange services within one hour of the time that the production site went offline, use the Active Directory Users and Computers MMC to reset the machine account for the Exchange virtual server. If you fail to do this, you might encounter client authentication issues.

Attention
Do not delete and re-create this account. Doing so will make it impossible to recover the Exchange server.</td></tr>
<tr><td>25</td><td>If the production cluster is different from the DR cluster, update the DNS record for the virtual Exchange server’s network name with the IP address at the production cluster.

Note
Until you complete the Active Directory, DNS, and WINS replication to reflect the IP change and refresh the client cache, client connectivity issues might occur.</td></tr>
<tr><td>26</td><td>Verify that the DR site is in the same state that it was in prior to the disaster:

a. Use the Cluster Administrator to verify that the Exchange DR cluster group is ready.

b. Use the storage system console or FilerView to verify that the original SnapMirror relationship is back in place.</td></tr>
<tr><td>27</td><td>To complete the failback, bring back online the LUNs belonging to the Exchange virtual server and the original MSCS cluster group.

<table><tr><th>If...</th><th>Then...</th></tr><tr><td>The original Windows cluster at the production site was not lost</td><td>Proceed to “Clean up the cluster physical disk resources” on page 289.</td></tr><tr><td>The original Windows cluster at the production site was lost</td><td>Proceed to “Recreate the cluster resource group and the Exchange virtual server” on page 292.</td></tr></table></td></tr>
</table>

Clean up the cluster physical disk resources: Follow these steps to complete the failback if the Windows cluster at the production site is operational and both the Exchange cluster resource group and the Exchange cluster resources exist.

In this case, the cluster physical disk resources need to be cleaned up in case the cluster physical disk resources are in a failed state at the production site.

Step	Action
1	Using the Cluster Administrator, do the following: **a.** Bring up the properties page for the Exchange System Attendant cluster resource. **b.** Remove the dependencies for all but one physical disk resource (LUN). **c.** Save the changes and exit the dialog box. The Exchange System Attendant cluster resource requires a dependency on at least one physical disk resource. This step will allow you to delete all but one of the physical disk resources.
2	If any of the LUNs that were removed as dependencies are still mounted, use SnapDrive to disconnect them
3	Using SnapDrive, do the following: **a.** Reconnect to the LUNs on the SnapMirror source volume using the same drive letters as before and, when prompted, specify a Virtual Disk Type of “shared.” The drive letters will not be available if they are still configured as physical disk resources for any reason, even if they are not actually mapped to LUNs. **b.** When prompted, select the Exchange cluster resource group. This creates the shared physical disk resources on the cluster nodes. **c.** Connect all of the LUNs except the one that was left as a dependency in the previous step.

Step	Action
4	Using the Cluster Administrator, do the following: **a.** Bring up the properties page again for the System Attendant cluster resource. **b.** Replace the reconnected LUNs as dependencies and remove the one that was left over from last time. **c.** Save the changes and exit the dialog box.
5	Using SnapDrive, do the following: **a.** Reconnect the final LUN, using the same drive letter as before and, when prompted, specify a Virtual Disk Type of "shared." The drive letters will not be available if they are still configured as physical disk resources for any reason, even if they are not actually mapped to LUNs. **b.** When prompted, select the Exchange cluster resource group. This creates the shared physical disk resources on the cluster nodes.
6	Go back to the Cluster Administrator and replace the System Attendant dependency on the last LUN.
7	Verify that the configuration is correct by running through the SnapManager Configuration Wizard. Be sure to save any changes if they need to be made.
8	If the cluster is configured with SMTP or HTTP virtual server cluster resources, these resources could fail shortly after you bring them online. To prevent this from happening, follow the steps in "Changing the IP addresses of SMTP and HTTP virtual server cluster resources" on page 295.
9	Using the Cluster Administrator, bring the Exchange cluster group online.

Step	Action
10	If the MS Search Instance cluster resource fails to come online, use SnapDrive to restore the LUN that was configured for the Exchange "data directory." These files need to be kept on a separate LUN from the Exchange database, transaction logs, and the SnapManager SnapInfo directory. Choose the most recent Snapshot copy with the "`eloginfo__`" prefix. **Note** The LUN containing the data directory is not restored as part of a SnapManager restore operation.
11	Perform a SnapManager for Exchange restore operation using the Snapshot copy you created at the beginning of the failback procedure and with the following options selected: ◆ "Use the most recent backup set" ◆ "Up-to-the-minute restore" ◆ "Mount databases automatically after restore" **Note** If the database was verified to be in a "Clean Shutdown" state after Exchange was taken offline on the DR cluster, you can forgo the SnapManager restore.
12	Verify that the virtual Exchange server on the production cluster is up and running: **a.** Use the Cluster Administrator to verify that the Exchange virtual server and the cluster resources are online. **b.** Use the Exchange System Manager to verify that the Exchange databases are mounted.
13	Continue with the recurring scheduled backup jobs that were in place prior to the failover.

Recreate the cluster resource group and the Exchange virtual server: Follow these steps to complete the failback if the Windows cluster at the original production site was lost and needs to be rebuilt from scratch.

In this case, the cluster resource group and the Exchange virtual server have to be re-created.

Step	Action
1	Install Windows Server on all nodes of the cluster.
2	Configure the default cluster group so that you have a working cluster without Exchange. **Note** The quorum disk can be a Data ONTAP LUN, but this is not a requirement. For detailed information about configuring the cluster, refer to Microsoft documentation.
3	Using the Cluster Administrator, create Exchange cluster resource group.
4	Install SnapDrive on all cluster nodes, following the instructions in the *SnapDrive Installation and Administration Guide*.
5	If using iSCSI, establish an iSCSI connection from one of the cluster nodes at the production site to the production storage system.
6	Using SnapDrive, perform the following steps: **a.** Reconnect to all of the LUNs using the original drive letters and, when prompted, specify a Virtual Disk Type of "shared." **b.** Place the LUNs in the Exchange cluster resource group. This creates the shared physical disk resources on the cluster nodes.
7	Install Exchange plus any service packs on all nodes of the cluster. The same service pack must be applied that was in use at the original production cluster and the DR cluster.

Step	Action
8	Using the Cluster Administrator, create an “IP Address” cluster resource in the Exchange cluster group.
9	If this IP address is different from that of the DR cluster or the original production cluster, update the DNS record for the virtual Exchange server’s network name. **Note** Until you complete the Active Directory, DNS, and WINS replication to reflect the IP change and refresh the client cache, client connectivity issues might occur.
10	Using the Cluster Administrator, do the following: **a.** Create a Network Name cluster resource in the Exchange cluster resource group, using the same Exchange server name as the original cluster and DR cluster. **b.** Create a new Exchange System Attendant cluster resource in the Exchange cluster resource group. This automatically creates all of the other Exchange cluster resources. **c.** When prompted by Exchange, specify the same drive letter for the system directory.
11	If the cluster is configured with SMTP or HTTP virtual server cluster resources, these resources could fail shortly after you bring them online. To prevent this from happening, follow the steps in “Changing the IP addresses of SMTP and HTTP virtual server cluster resources” on page 295 before proceeding.
12	Install and configure SnapManager on all nodes of the cluster.

Step	Action
13	Perform a SnapManager for Exchange restore operation using the Snapshot copy you created at the beginning of the failback procedure and with the following options selected: ◆ "Use the most recent backup set" ◆ "Up-to-the-minute restore" ◆ "Mount databases automatically after restore" **Note** If the database was verified to be in a "Clean Shutdown" state after Exchange was taken offline on the DR cluster, you can skip the SnapManager restore.
14	Verify that the virtual Exchange server on the production cluster is up and running: **a.** Use the Cluster Administrator to verify that the Exchange virtual server and the cluster resources are online. **b.** Use the Exchange System Manager to verify that the Exchange databases are mounted.
15	Use SnapManager to re-create the automated backup jobs, described in the *SnapManager for Exchange Installation and Administration Guide*.

Changing the IP addresses of SMTP and HTTP virtual server cluster resources

After a failover or failback, the SMTP and HTTP virtual server cluster resources might fail after being online for a few minutes if both of the following conditions are true:

- The cluster is configured with the SMTP virtual server cluster resources, HTTP virtual server cluster resources, or both.
- The IP address for the virtual Exchange server at the DR site is different from the IP address at the production site.

If these resources fail, the following events appear in the Windows application event log:

```
Event Type: Error
Event Source: MSExchangeCluster
Event Category: Services
Event ID: 1005
Date:  8/25/2005
Time:  3:44:04 PM
User:  N/A
Computer: EXCHSRVR1
Description:
SMTP Virtual Server Instance (EVS1): The IsAlive check for this
resource failed.

For more information, click
http://www.microsoft.com/contentredirect.asp.
Data:
0000: 4c 27 00 00              L'..


Event Type: Error
Event Source: MSExchangeCluster
Event Category: Services
Event ID: 1005
Date:  8/25/2005
Time:  3:44:07 PM
User:  N/A
Computer: EXCHSRVR1
Description:
Exchange HTTP Virtual Server Instance (EVS1): The IsAlive check for
this resource failed.

For more information, click
http://www.microsoft.com/contentredirect.asp.
Data:
0000: 4c 27 00 00              L'..
```

To prevent the SMTP or HTTP virtual server cluster resources from failing after a cluster failover or failback, update the IP address as described in the two procedures that follow.

SMTP resource: For the SMTP resource, complete the following steps.

Step	Action
1	Launch the Exchange System Manager.
2	Browse to the Exchange virtual server name.
3	Expand the Exchange server name, Protocols, and SMTP.
4	Right-click Default SMTP Virtual Server and select Properties.
5	On the “General” page, select the correct IP address from the drop down list.
6	Click OK and then close the Exchange System Manager.
7	Using the Cluster Administrator, bring the SMTP virtual server cluster resource online.

HTTP resource: For the HTTP resource, complete the following steps.

Step	Action
1	Launch the Exchange System Manager.
2	Browse to the Exchange virtual server name.
3	Expand the Exchange server name, Protocols, and HTTP.
4	Right-click“Exchange Virtual Serve” and select Properties.
5	On the “General” page, select the correct IP address from the drop-down list.
6	Click OK and then close the Exchange System Manager.
7	Now launch the Internet information Services Manager.
8	Expand the local computer name and then expand the “Web Sites” folder.
9	Right-click Exchange Virtual Serve” the select properties.

Step	Action
10	When the properties appear, select the “Web Site” page and then set the correct IP address.
11	When done, click OK and then close the IIS Manager.
12	Using the Cluster Administrator, bring the SMTP virtual server cluster resource online.

Archiving SnapManager Backups 14

This section describes how to create offline archives of Snapshot copies containing SnapManager backup sets. The following topics are covered:

- "Understanding SnapManager backup set archival" on page 300
- "Choosing the best way to archive your SnapManager backups" on page 303
- "Using NDMP or dump to archive SnapManager backups" on page 304
- "Using a Windows backup utility to archive SnapManager backups" on page 308
- "Using Exchange Backup Agent to archive Exchange backups" on page 311
- "Using Run Command After Operation to archive automatically" on page 313

Understanding SnapManager backup set archival

This topic provides background information about archiving SnapManager backup sets.

Why organizations archive data

Organizations archive data for many reasons, central of which is disaster recovery. Archiving data enables an organization to create a complete, self-consistent replica of a collection of data suitable for bringing back online at some future date. Where backup is concerned with users accidentally destroying files or individual hardware components failing, disaster recovery addresses recovery from events that might disable an entire building or geographical area.

Organizations archive data for purposes other than disaster recovery. Space constraints often require that older data be archived. Reasons organizations archive and restore data are as diverse as their businesses. Some organizations restore data for use in historical analysis, some restore data for use in litigation.

Importance of archiving a complete backup set

Archived data might be used to re-create an Exchange data store from the ground up. For this reason, it's important to understand all the components of a SnapManager backup set, and what those components are named, so that you know that your archives contain all the data required to restore your Exchange data.

SnapManager backup sets

A SnapManager backup set includes the following components:

- Exchange database Snapshot copies
- Exchange transaction log Snapshot copies
- SnapInfo directory Snapshot copy

SnapManager Snapshot copy naming conventions

The naming conventions for SnapManager Snapshot copies depend on whether your SnapManager host system is running Windows 2000 Server or Windows Server 2003.

Snapshot naming conventions for Windows 2000 Server: If your SnapManager host system is running Windows 2000 Server, your Snapshot copy names will be as follows:

- Exchange database Snapshot copies

- For the standard backup management group:

  `exchsnap__`*exchangeservername_date_time*

- For all other backup management groups:

  `exchsnap__`*exchangeservername_date_time__backupmgmtgroup*

- SnapInfo directory and transaction log Snapshot copies
  - For the standard backup management group:

    `eloginfo__`*exchangeservername_date_time*

  - For all other backup management groups:

    `eloginfo__`*exchangeservername_date_time__backupmgmtgroup*

Note

If you did not select the Use Unique Name option when you created the SnapManager backup, the most recent Snapshot copy name contains `recent` instead of *date_time.* This is for backward compatibility with previous versions of SnapManager, which did not include the Run Command After Operation feature.

Snapshot naming conventions for Windows Server 2003: If your SnapManager host system is running Windows Server 2003, your Snapshot copy names will be as follows:

- Exchange database and transaction log Snapshot copies
  - For the standard backup management group:

    `exchsnap__`*exchangeservername_date_time*

  - For all other backup management groups:

    `exchsnap__`*exchangeservername_date_time__backupmgmtgroup*

- SnapInfo directory Snapshot copy
  - For the standard backup management group:

    `eloginfo__`*exchangeservername_date_time*

  - For all other backup management groups:

    `eloginfo__`*exchangeservername_date_time__backupmgmtgroup*

Note

If you did not select the Use Unique Name option when you created the SnapManager backup, the most recent Snapshot copy name contains `recent` instead of *date_time.* This is for backward compatibility with previous versions of SnapManager, which did not include the Run Command After Operation feature.

Guidelines for archiving

Follow these guidelines when you create archives:

- Only archive verified backups.

  If you are not sure whether a backup is verified, you can use the SnapManager Restore tab to check; a backup with a green check mark is verified.
- Create an archive of the most recent backup.
  - If you didn't use the unique name option when the backup was created, the most recent Snapshot copy in the storage system's LUN drive volume that stores the Exchange databases is always named /exchsnap_*servername*_recent or /exchsnap_*servername*_recent_*backupmgmtgroup*. *Servername* is the name of the Exchange server from which the Snapshot copy was taken, and *backupmgmtgroup* is the name of the backup management group.
  - If you used the unique name option, look for the Snapshot copy with the most recent date and time.
- LUNs cannot be archived using the CIFS or NFS protocols. Use the storage system's `dump` command or an NDMP backup application to archive LUNs.

Considerations for scheduling SnapManager Backup for archiving

Scheduling SnapManager backups for archiving must take into consideration many factors, including the following:

- Archive method used
- Service Level Agreements for disaster recovery
- Number of SnapManager backups performed per day
- Exchange client activity schedules
- Backup verification time

Archiving individual storage groups or databases

Archiving individual storage groups or databases from SnapManager backups is not recommended. This task requires a full understanding of the Snapshot copy naming conventions used by SnapManager for Microsoft Exchange and should not be attempted without knowing which Snapshot copies contain the appropriate storage groups and transaction logs for a given point in time. Archiving complete Exchange server backups (all storage groups) is recommended.

Choosing the best way to archive your SnapManager backups

There are different methods for collecting the necessary parts of the SnapManager backup set for archiving. They each have their own advantages and disadvantages. Read the section for each method to decide which one works best for your organization. The three methods are as follows:

- Use NDMP or the storage system's `dump` command to archive the LUNs containing the Exchange data and the SnapInfo directory directly from the storage system to the archive medium.

  For more information about this method, see "Using NDMP or dump to archive SnapManager backups" on page 304.

- Mount the LUNs in a SnapManager backup Snapshot copy and share it, then use NTBackup or another Windows backup utility to copy the LUNs' contents to the archive medium.

  For more information about this method, see "Using a Windows backup utility to archive SnapManager backups" on page 308.

- Create an Exchange copy-type backup directly to the archive medium using an Exchange-aware backup application.

  For more information about this method, see "Using Exchange Backup Agent to archive Exchange backups" on page 311.

Using NDMP or dump to archive SnapManager backups

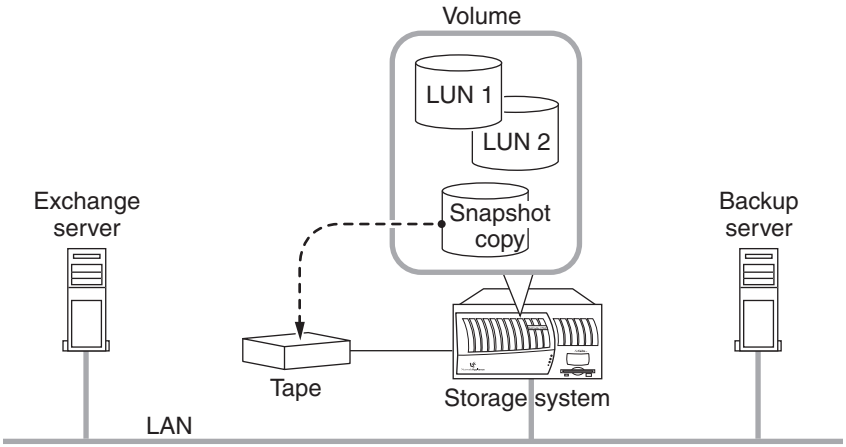
You can use NDMP or the storage system's `dump` command to archive the LUNs containing the Exchange data and the SnapInfo directory directly from the storage system to the archive medium. NDMP and the `dump` command are the most efficient methods for creating archives of the LUN drive files. See the following topics for more information:

- "About this method" on page 304
- "Path name to use when archiving using NDMP or dump" on page 305
- "Usage example" on page 306

About this method

When you use NDMP or `dump` to archive your SnapManager backups, you use NDMP or the storage system's `dump` command to archive each LUN that contains data for that backup set. Using NDMP or the `dump` command enables you to archive your SnapManager backup sets without involving Exchange or the Exchange server at all. Snapshots are taken of the LUNs, then copied to the archive medium and deleted.

This archive method is represented by the following diagram:



Archiving using NDMP or dump

For more information about backing up storage system data to tape, see the *System Administration Data Protection Guide* for your version of Data ONTAP.

Advantages: Using NDMP or `dump` to archive SnapManager backups provides the following advantages:

- Because this method does not rely on mounting a Snapshot copy, it does not risk the creation of busy Snapshot copies.
- Because this method archives the entire raw LUN, restoring is simply a matter of replacing the LUNs.
- If your archive procedure does not send the data over the network, this method can be significantly faster than other methods.

Disadvantages: The advantages of using NDMP or `dump` to archive SnapManager backups must be weighted against the following disadvantages:

- Because you are archiving raw LUNs, the entire LUN containing the Exchange data is archived, so you archive more data than you need.

  If archiving extra data is undesirable, you can use NTBackup or another Windows backup utility to back up the corresponding SnapInfo directory. This must be coordinated so that the two pieces of the archive are kept together for later retrieval.
- If you archive the SnapInfo directory separately, you must ensure that you get both required components from different locations into the same archive.

Path name to use when archiving using NDMP or dump

When using NDMP or `dump` to archive your SnapManager backups, specify the database LUN using its absolute path name

`/vol/`*volume_name*`/.snapshot/`*snapshot_name*`/`*LUN_name*

where the three variables represent the following text strings:

Variable	Description
volume_name	Name of the volume containing the data to be archived
snapshot_name	Name of the Snapshot copy containing the LUNs to be archived For more information about SnapManager Snapshot copy naming conventions, see "SnapManager Snapshot copy naming conventions" on page 300.
LUN_name	Name of the LUN containing the data to be archived

For example, the absolute path name of the LUN `exch1db.lun` in the Snapshot copy `exchsnap__SRVR3_01-20-2006_12.05.58_Daily` on the volume `ExchVol`n is:

```
/vol/ExchVol/.snapshot/exchsnap__SRVR3_01-20-
2006_12.05.58__Daily/exch1db.lun
```

Usage example

Suppose you want to use a script to archive your SnapManager backups to tape in the following environment:

- The script is run on the computer running Exchange and SnapManager.
- The name of the storage system is `Filer1`.
- The name of the LUN containing the Exchange databases is `exch1db.lun`.
- The name of the LUN containing the Exchange transaction logs and the SnapInfo directory is `exch1logs.lun`.
- The name of the volume containing the Exchange databases is `Exchvol`.

Example script: The following script uses the storage system `dump` command to dump the database, transaction logs, and SnapInfo LUNs to tape. This script relies on `rsh` functioning on the Exchange server using the SnapManager user account.

```
REM Back up the LUN containing the Exchange database.
REM For this example, a level 0 backup is performed
REM to the tape device named nrst0a.

rsh Filer1 dump 0f nrst0a /vol/ExchVol/.snapshot/%1/exch1db.lun

REM Before appending the next backup to the tape,
REM reposition to the end of the tape so the next
REM write will not overwrite the existing data.

rsh Filer1 mt -f nrst0a eom

REM Back up the LUN containing the Exchange
REM transaction log files and the SnapManager SnapInfo
REM directory.

rsh Filer1 dump 0f nrst0a /vol/ExchVol/.snapshot/%2/exch1logs.lun
```

Invoking the script and passing parameters: To invoke this script using the SnapManager Run Command After Operation feature, use the following command:

```
C:\SnapManager Scripts\scriptname.txt $ExchSnapshot $InfoSnapshot
```

The command-line parameters `%1` and `%2` might provide values similar to the following, respectively:

- `exchsnap__SRVR3_01-20-2006_12.05.58__Daily`
- `eloginfo__SRVR3_01-20-2006_12.05.58__Daily`

For more information about the Run Command After Operation feature, see "Using Run Command After Operation to archive automatically" on page 313.

Invoking the script without using command-line parameters: If you prefer not to use the Run Command After Operation feature and you are not using the unique name option for your backups, you can hardcode the Snapshot copy names into the script.

For example, the `dump` command for the database might look like this, for an Exchange server named `SRVR3`:

```
rsh Filer1 dump 0f nrst0a
/vol/Exch/.snapshot/exchsnap__SRVR3__recent__Daily/exch1logs.lun
```

Using a Windows backup utility to archive SnapManager backups

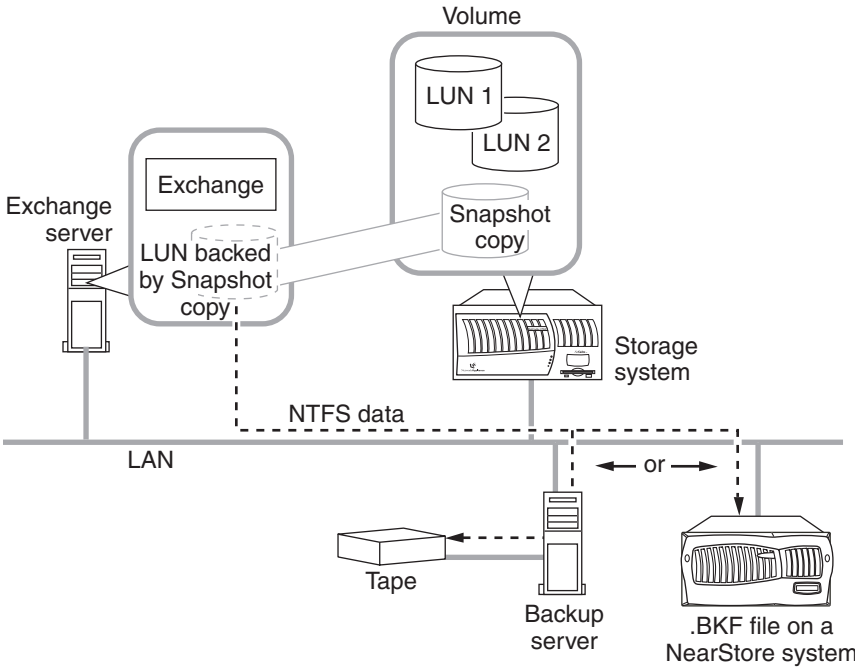
The following topics discuss archiving SnapManager backups using a Windows backup utility:

- "About this method" on page 308
- "Usage example" on page 309

About this method

When you use a Windows backup utility to archive your SnapManager backups, you mount the LUNs backed by the backup Snapshot copy you want to archive, and then use NTBackup or another Exchange-aware Windows backup utility to copy the archive data to your archive medium. In this case, the NTFS data is backed up, rather than the raw LUNs.

This archive method is represented by the following diagram:



Archiving using Windows backup utility

Note

The LUN does not need to be mounted on the Exchange server; another computer can be used for this function.

Components that must be included in the archive: The archive must include the following two components:

- The SnapInfo directory as it was backed up directly from the Exchange server
- The Exchange data as extracted from the LUN backed by Snapshot copy

Advantages: Using a Windows backup utility to archive SnapManager backups provides the following advantages:

- Because you are archiving NTFS data, not raw LUNs, you can archive exactly the data that you need, and no more.
- The procedures and tools used for this method are probably familiar and available to you.

Disadvantages: The advantages of using a Windows backup utility to archive SnapManager backups must be weighed against the following disadvantages:

- Because this method relies on mounting a Snapshot copy, you must be careful to avoid scheduling any backups while the archiving is performed. This is because creating a Snapshot copy of a mounted Snapshot copy results in a Snapshot copy that cannot be deleted. For more information about busy Snapshot copies, see "Problem deleting backups due to busy Snapshot copy error" on page 211.
- You must make sure that you get both required components from different locations into the same archive.

Usage example

Suppose you want to use a script to mount a Snapshot copy of the LUNs that contain the Exchange databases, back up the databases using NTBackup, dismount the LUNs, and then back up the SnapInfo directory in the following environment:

- The script is run on the computer running Exchange and SnapManager.
- The drive letter for the Exchange database is S:.
- The Snapshot copy is mounted as drive V:.

  The drive letter used for the LUN mount must be available when the script is run.

Example script: The following script mounts a Snapshot copy of the LUNs that contain the Exchange databases and backs them up using NTBackup. It then dismounts the LUNs and backs up the SnapInfo directory. The `/N` and `/D` options are used to demonstrate the options to name the tape and add a description.

```
REM Mount a LUN backed by the Snapshot copy of the Exchange
REM database as drive letter V:\.

sdcli snap mount -k s -s %1 -d v

REM Use NTBackup to back up the database files. The path
REM to the databases in your environment might be different.

ntbackup backup "V:\Program Files\Exchsrvr\mdbdata" /N %1 /D %2

REM Dismount the Snapshot copy mounted as drive letter V:\.
REM The below example is shown with an optional parameter (-f)
REM to forcefully disconnect the drive letter.

sdcli snap unmount -d v -f

REM Use NTBackup to back up the snapinfo directory.
REM This backup appends the media so as not to
REM overwrite the database backup. The path to the
REM snapinfo directory is passed as the third
REM parameter on the command line used to launch
REM this script.

ntbackup backup %3 /T%1 /A
```

Invoking the script and passing parameters: To invoke this script using the SnapManager Run Command After Operation feature, use the following command:

```
C:\SnapManager Scripts\scriptname.txt $ExchSnapshot $SnapInfoName
$SnapInfoPath
```

The command-line parameters `%1`, `%2`, and `%3` might provide values similar to the following, respectively:

- %1: `exchsnap__SRVR3_01-20-2006_12.05.58__Daily`
- %2: `01-20-2006_12.05.58__Daily`
- %3: `I:\SME_SnapInfo\SRVR3\SG_First Storage Group\01-20-2006_12.05.58__Daily`

For more information about the Run Command After Operation feature, see "Using Run Command After Operation to archive automatically" on page 313.

Using Exchange Backup Agent to archive Exchange backups

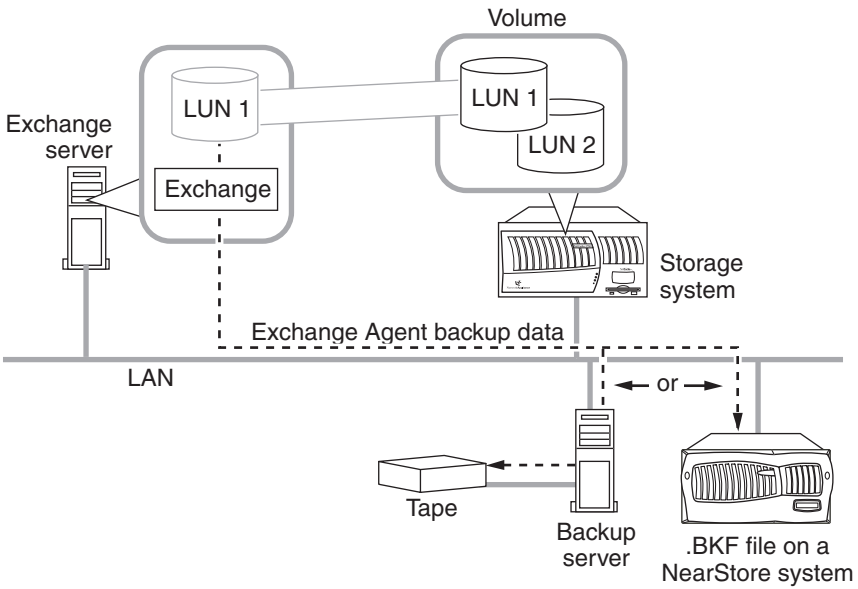
The following topics discuss archiving Exchange backups using the Exchange Backup Agent in a SnapManager environment:

- "About this method" on page 311
- "Usage example" on page 312

About this method

When you use Exchange backups to archive your SnapManager backups, you use NTBackup (which, in turn, uses the Exchange Backup Agent) to create a copy backup of your Exchange databases. In this case, the Exchange data itself is captured and archived. Because SnapManager is not used to create the backup, it also is not used to perform the restore, so the SnapInfo directory does not need to be archived for this method.

This archive method is represented by the following diagram:



Archiving using Exchange backup

Attention

You must use a copy or differential backup for this method. Performing any other type of backup causes your existing SnapManager backups to become unusable for an up-to-the-minute restore.

Advantages: The advantage of this approach is that the procedures and tools used for this method are probably familiar and available to you.

Disadvantages: The disadvantage of this approach is that no SnapManager backups can be initiated while this method is in use.

Usage example

The following script launches NTBackup and tells it to perform a copy-type backup through the Exchange backup agent.

Before you can use this script, you need to use the NTBackup GUI to create a `.BKS` file that contains the storage groups you want to back up.

This script assumes that it is being run on the computer running Exchange and SnapManager.

Example script:

```
REM Launch NTBackup

ntbackup backup "@c:\MyConfig.BKS" /M copy
```

Note

Although this archive method does not use SnapManager backups, it can be invoked using the Run Command After Operation feature. For more information about the Run Command After Operation feature, see "Using Run Command After Operation to archive automatically" on page 313.

Using Run Command After Operation to archive automatically

SnapManager includes the ability to automatically run your own program or script after a backup or database verification operation finishes successfully. This feature, called Run Command After Operation, is typically used to automatically archive a backup. See the following topics for more information:

- "How you can launch your own program or script" on page 313
- "Command arguments pass information to your program or script" on page 314
- "Specifying the command to be run after the operation succeeds" on page 315
- "Running a script from a UNC path on a Windows Server 2003 system" on page 319

Attention

Make sure that you archive all components of a backup set together. For more information, see "SnapManager backup sets" on page 300.

How you can launch your own program or script

When you start or schedule a SnapManager backup or database verification operation, you can specify that SnapManager automatically run a command after the operation finishes successfully. If you choose this option, you will be prompted to specify the following information:

1. The host system from which the command is to be run
2. The full path of the command that you want SnapManager to run after the backup or database verification finishes successfully
3. Any parameters that are to be passed to the command

   Because the command is invoked from within the context of a specific backup or database verification, you can pass the command information about the components of that operation.

   In your script, any occurrence of the text string `%1` corresponds to the first parameter passed; the text string `%2` corresponds to the second parameter, and so on.

Command arguments pass information to your program or script

The Run Command After Operation feature supports the following variables, which can pass operation-specific information to your program or script.

Variable	Description

`$ExchSnapshot`	Expands to the name of an Exchange database Snapshot copy. Examples:
	`exchsnap__winsrvr3__01-31-2006_15.03.09`
	`exchsnap__winsrvr3__recent`
	Note
	The number of database Snapshot copies in a SnapManager backup set depends on the number of volumes used to store the storage groups included in the backup.

`$InfoSnapshot`	Expands to the name of a SnapInfo directory Snapshot copy. Examples:
	`eloginfo__winsrvr2__01-31-2006_15.03.09`
	`eloginfo__winsrvr2__recent`

`$SnapInfoName`	Expands to the name of the SnapInfo directory. Examples:
	`WINSRVR3__01-23-2006_16.21.07__Daily`
	`WINSRVR3__recent`
	Note
	If you use this variable, you must also provide the correct path to the directory.

`$SnapInfoPath`	Expands to the name of the SnapInfo subdirectory. Example: `I:\SME_SnapInfo\EXCH__WINSRVR3\SG__First Storage Group\WINSRVR5_01-06-2006_11.52.36`

The `$SnapInfoPath` variable is automatically enclosed within double quotes so that the actual path name can contain spaces without affecting the script invocation on the Windows command line. If you do not want the double quotes to appear in your command line, remove them from the Command Arguments field in the Run Command After Operation dialog box.

Specifying the command to be run after the operation succeeds

While specifying a SnapManager backup or verification operation, you can use the Run Command After Operation dialog box to specify the details of the command you want to run after the backup or verification operation finishes.

Note

You can specify default values for the command arguments so that you do not have to enter the command information each time you initiate a backup or verification. For details, see "Managing the Run Command After Operation default settings" on page 358.

Procedure: To run a command or invoke a batch file after backup or verification, complete the following steps.

Step	Action	
1	Open the Run Command After Operation dialog box.	
	From the...	**Do this...**
	Backup and Verification tab	**1.** Specify a database backup or a verification of the databases and transaction logs in the most recent backups. **2.** Select the Run Command After Operation option. **3.** Click Backup Now or Verify Now.
	Backup Wizard	**1.** Step through the wizard screens to specify a full database backup, a transaction log only backup, or a database verification. **2.** In the Run a Command After the Operation screen, select the option labeled "Yes, run a command after this operation", and then click Next.
	Result: The Run Command After Operation dialog box appears and displays the current default settings.	
2	In the "Specify a computer where..." box, enter or browse to the name of the host on which your program or script resides.	

Step	Action
3	In the “Specify the full path...” box, browse to your program or script. **Note** If the script is stored on a network share, use the UNC path rather than the network drive letter to specify the script’s location. If SnapManager is installed on a Windows Server 2003 system, then add the network location to Internet Explorer's list of trusted sites, otherwise the command could fail silently

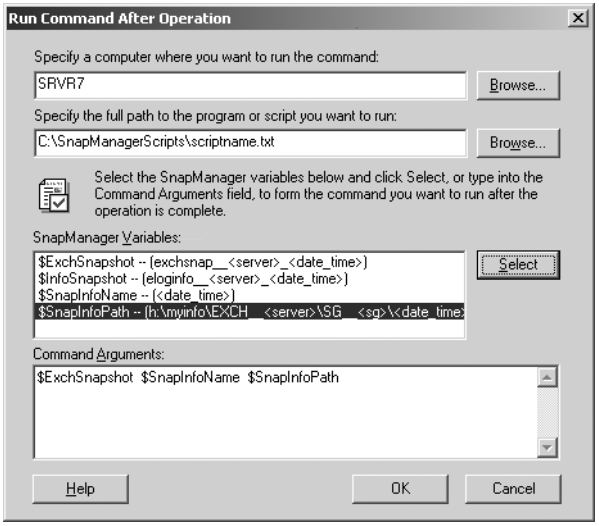
Step	Action
4	Form the command input string in the Command Arguments box. You can do this using any combination of the following methods: ◆ To enter text directly into the Command Arguments box, click in the box and type the desired text. ◆ To enter a SnapManager variable into the Command Arguments box, do the following: **a.** If necessary, click in the Command Arguments box to position the cursor. **b.** In the SnapManager Variables list, select the variable you want to enter. For more information, see "Command arguments pass information to your program or script" on page 314. **c.** Click Select. **Notes:** ◆ The `$SnapInfoPath` variable is automatically enclosed within double quotes so that the actual path name can contain spaces without affecting the script invocation on the Windows command line. If you do not want the double quotes to appear in your command line, remove them from the Command Arguments field in the Run Command After Operation dialog box. ◆ If more than one Snapshot copy exists for this operation, you must include that Snapshot copy type's variable name once for every Snapshot copy. If you do not, you cannot create a complete archive. For details, see "Command arguments pass information to your program or script" on page 314.
5	Repeat Step 4 as needed until the Command Arguments box contains the arguments you want to pass to your program or script.

Step	Action
6	Click OK to apply your changes, close the Run Command After Operation dialog box, and return to the backup or verification setup process. **Result:** After when the backup or verification finishes successfully, the command you specified, with the Snapshot copy and SnapInfo information for this backup operation inserted, runs automatically.

Example: Suppose you want to run the script `C:\SnapManager Scripts\scriptname.txt` with the following parameters:

- Name of the database Snapshot copy
- Name of the specific SnapInfo directory
- NTFS path to the SnapInfo directory

The corresponding Run Command After Operation dialog box would look like this:



For more examples, see "Using NDMP or dump to archive SnapManager backups" on page 304 and "Using a Windows backup utility to archive SnapManager backups" on page 308.

Running a script from a UNC path on a Windows Server 2003 system

If SnapManager is installed on a Windows Server 2003 system, then attempting to launch a script from a UNC (Uniform Naming Convention) path might cause SnapManager to hang. If this occurs, the log file shows no indication of the failure other than it is missing the last line of text: "The specified command has been launched successfully."

Windows Server 2003 ships with Internet Explorer's Enhanced Internet Explorer Security Configuration enabled. This setting is restrictive and prevents batch files located on a network share from running. The network location will need to be added to Internet Explorer's list of trusted sites.

To run a script from a UNC path on a Windows Server 2003 system, complete the following steps.

Step	Action
1	Log in to the Windows Server 2003 system that will be running the script. ◆ This system can be the same system that is running SnapManager, or it can be a different server. ◆ You must log on using the same user account that SnapManager is configured to use. For more information, see "Understanding SnapManager COM server identity account requirements" on page 20.
2	Launch Internet Explorer.
3	In the menu bar, select Tools > Internet Options. **Result:** The Internet Options dialog box appears.
4	In the Internet Options dialog box, do the following: **a.** Select the Security tab. **b.** In the Security tab, select the Local intranet icon, and then click Sites. **Result:** The Local Intranet dialog box appears.

Step	Action
5	In the Local Intranet dialog box, do the following: **a.** In the "Add this Web site to the zone" box, enter the host name of the machine from where the script will be launched. **b.** Click Add. **Result:** The host name is added to the Web Sites list.
6	Click Close to close the Local Intranet dialog box.
7	Click OK to close the Internet Options dialog box.
8	To verify your changes, browse to the network location where the script resides and launch the script. **Result:** The script should now run normally without security prompts. **Note** Although the script should run, it might actually fail to complete properly because the SnapManager variables are not be passed to the script in this test.

Note

These security settings are specific to each user account on each machine. You will need to repeat this procedure for on all machines that might be used to run scripts and for all users that might launch the script on each machine. You will also need to repeat these steps if you start using a different user account to run SnapManager.

Managing SnapManager Reports 15

This section describes how to use and manage the reports that SnapManager automatically creates for every operation performed. The following topics are covered:

- "Understanding SnapManager reports" on page 322
- "Deleting SnapManager reports" on page 323
- "Printing SnapManager reports" on page 324

Related topics:

- "Uninstalling SnapManager" on page 55
- "Managing the report directory options" on page 372

Attention

You must run SnapManager from the system console, not from a Terminal Services client. Do not use Terminal Services for any type of SnapManager administration, because you might miss critical information that is displayed only in pop-up boxes at the system console.

Understanding SnapManager reports

SnapManager reports list step-by-step details for every SnapManager operation you perform, the final status of the operation, and error messages for any errors encountered during the operation.

The SnapManager Reports tab provides four folders, which contain the reports for each of these operation types:

Note

There could be other folders if you are running SnapManager in a Windows cluster or you have a previous version of SnapManager Reports.

- Backup
- Config
- Delete Snapshot
- Miscellaneous
- Restore

About changing the report directory

You can use the Options > Report Directory Setting menu to change the directory where your SnapManager reports are stored. You might want to do this if you find that you have limited space in the original report directory.

If you change the path, you can no longer see the reports created before the path was changed, but they are still accessible. You can look at them by changing the Report Directory Setting back to the original setting and selecting Refresh from the View menu.

Locating the report directory in a Windows cluster

By default, the report directory is in the disk where SnapManager is installed. In a Windows cluster, however, this does not allow the report directory to be shared between the nodes in the cluster, and you cannot see the same reports from different nodes. To avoid this problem, you can use the Options menu to move the report directory to a disk that belongs to the same group as your Exchange virtual server. This needs to be performed from every SnapManager node.

Attention

Do not use a disk that contains Exchange or SnapManager data for the report directory; it is restored from Snapshot copy when you perform a SnapManager Restore.

Deleting SnapManager reports

To delete any of the reports from the Reports folders, complete the following steps.

Step	Action
1	Click the SnapManager Reports tab in the SnapManager main window.
2	Expand the appropriate folder in the left column of the Report tree.
3	Right-click the folder or individual report that you want to delete and select Delete Report.
4	Click the dialog box that appears, prompting for whether you want to delete the report. **Result:** The report is deleted.

Printing SnapManager reports

SnapManager for Microsoft Exchange provides the following two ways to print reports:

- Directly to the printer from within the displayed report on the right pane using the context menu
- From within Notepad

Printing a displayed report to the printer

To send a displayed report to the printer, complete the following steps.

Step	Action
1	Click the SnapManager Reports tab in the SnapManager main window.
2	Expand the appropriate reports folder and select the report you want to print.
3	Right-click anywhere within the displayed report in the right pane and select Print.

Printing a report using Notepad

To print a report using Notepad, complete the following steps.

Step	Action
1	Click the SnapManager Reports tab in the SnapManager main window.
2	Expand the appropriate report folder.
3	Right-click the report name in the folder pane and select Open with Notepad.
4	From within Notepad, select the Print option on the File menu.

SnapManager Command-Line Reference A

This section details the SnapManager 3.2 for Microsoft Exchange operations you can execute using the SnapManager command-line functionality. This allows you to create scripts to invoke SnapManager functionality without having to use the SnapManager Graphical User Interface (GUI).

Guidelines for using the commands

Observe the following guidelines when using the SnapManager command-line tool:

- All parameters and options are case-insensitive. So using the option “-Daily” will achieve the same results as using “-daily”.
- Some of the options must be invoked in a particular order. For best results, use the order given in the synopsis for all options.
- When a parameter value string contains spaces, be sure to enclose it in double quotes. For example, use **`“First Storage Group”`** rather than **`First Storage Group`**.
- When a parameter has a variable number of input values, it is preceded by a parameter named “count,” which you use to indicate how many values will be included in the parameter. If you specify a number different than the number of values included in the parameter, the command fails.

snapbackup

Name

snapbackup — Command for accessing SnapManager backup functionality.

Description

This command enables you to initiate a backup or verification job, with all of the options available through the SnapManager GUI.

Syntax for backup operation

snapbackup *target_exchange_server_name*
-b *number_of_storage_groups storage_group_1* [**,** *storage_group_2...*]
[**-u**]
[**-daily** | **-weekly**]
[**-m**]
[**-k**]
[**-t**]
[**-p** *throttling_value*]
[{**-c** *verification_server number_of_backup_sets* | **-nc**}
[**-mp** [**-mpdir** *mount_point_directory_path*]]]
[**-d** *number_of_backup_sets_or_days* [**-rd**]]
[**-r** *run_cmd_path* \ "*run_cmd_args* \ " [**-a** *run_cmd_server*]]

Syntax for verification-only operations

snapbackup *exchange_server_name_in_backup_set*
-s *number_of_storage_groups_in_backup_set storage_group_1*
[**,** *storage_group_2...*]
-c *verification_server number_of_backup_sets_to_verify*
[**-mp** [**-mpdir** *mount_point_directory_path*]]
[**-daily** | **-weekly** | **-all**]
[**-m**] [**-a** *run_cmd_server* **-r** *run_cmd_path run_cmd_args*]
[**-p** *throttling_value*]
[**-r** *run_cmd_path* \ "*run_cmd_args* \ " [**-a** *run_cmd_server*]]

Options

The options shown in the synopsis for this command are described in the following table:

Option	Description
-v	Verbose output. The -v option informs SnapBackup to display verbose information regarding the backup job. This is useful for seeing how the backup job runs and what error might have occurred.
-b	Backup operation Denotes this as a backup operation and specifies the list of Storage group to be backup. The list is always preceded by the count, specifying the number Storage Groups in the list.
-s	Verify only operation. Denotes this as a verify only operation and specifies the list of Storage group to be verified. The list is always preceded by the count, specifying the number Storage Groups in the list.
-d	Number of backups to retain. Used for backup operations to specify the number of backups to retain after the delete phase.
-rd	Use day base backup deletion retention. Denotes that the deletion of backups is to be based on an "older than number of days" policy. This option used in conjunction with the "-d" option will specify the number of days after which a backup is to be deleted. Absence of this option denotes a deletion policy of based on retained backup count.
-nc	No verification of database at end of backup operation. Denotes that the verification phase of a backup operation is to be skipped.
-c	Verification server and number of Snapshots. Specifies the host to be used as the verification server for the verification phase of a backup operation. If the verification server is followed by a number, then this is a verification operation and the number specifies how many backup are to be verified.

Option	Description
-daily	Mark as member of "Daily Management Group." Denotes that the backup or verify are to be flagged as being a part of the "Daily Management Group."
-weekly	Mark as member of "Weekly Management Group." Denotes that the backup or verify are to be flagged as being a part of the "Weekly Management Group."
-all	Mark as member of "All Backup Management Group." Denotes that this verify operation is part of all and any backup management group.
-u	Use Unique naming convention. Denotes that the backup to be created are to be named using the Unique naming convention. The most recent backup is to be named using the date and time instead of the string "recent". Absents of this option causes the most recent backup to be named using the Generic naming convention, where backups are named using the word "_recent."
-m	Do not update SnapMirror after backup operation. Suppresses the SnapMirror replication phase of a backup operation. SnapMirror updates specified volume to reflect incremental updates on a source volume. If a SnapManager volume is enable for SnapMirror usage and this option is not specified, then at the end of a backup operation, the SnapMirror destination will be update from the source volume.
-k	Do not retain up-to-minute restore ability. The logs are not to be deleted for any backups deleted as part of this backup operation. This will retain the up-to-the-minute restore ability for older backups that remain after the delete phase of a backup operation.
-t	Do not backup truncated logs. During the backup operation, skip the backing up of log which will be truncated. This option can be used to conserve space on the LUN containing the backed up Exchange logs.

Option	Description
-mpdir	Use specified mount point directory. Specify which mount point directory a snapshot will be mounted to during database verification
-mp	Mount Snapshot to a directory. Mount snapshots in a default NTFS directory during database verification. This option is also effective when there are no available drive letters to mount snapshots.
-r	Run specified command with arguments after backup operation. Specifies the complete path and arguments for the command to be run after the backup or verify operation is complete
-a	Run command on specified server Specifies the server where the command is to be run after the backup or verify operation is complete.
-p	Verification Throttling Specifies the throttling values to be used for the verify operation.

Dependencies

The `-c` and `-nc` options are mutually exclusive

The `-daily`, `-weekly`, and `-all` options are mutually exclusive.

Required options

Either the `-s` or the `-b` option are required, but they are mutually exclusive.

Default behavior:

Database and log verification: The running of verification after a backup operation is the default. The -nc option will suppress the behavior. The `-c` option will override the verification server specified in the SnapManager GUI.

Management group: The default option is Standard, where backups are marked with standard backup management group specification.

Backup retention: Backup retention defaults to the “In excess of” policy, where backups are deleted base on backup count. The `-rd` option will override this option and set the policy to one based on date.

Backup naming: The naming of backups defaults to the Unique naming policy where the most recent backup is named using the text string `_recent`.

Examples of use

The following examples show a few of the ways the `snapbackup` command can be invoked. It is assumed that these operations are invoked from the SnapManager directory

Backup Example #1:

```
snapbackup EXCHSRVR3 -b 2 "First Storage Group", "Second Storage
Group" -nc
```

This command creates a new backup of two storage groups on EXCHSRVR3 in the Standard backup management group (the default), using the unique naming convention (the backup will be named using the date-time stamp). No verification or command after operation is performed, and no older backups are deleted.

Backup Example #2:

```
snapbackup EXCHSRVR3 -b 2 "First Storage Group", "Second Storage
Group" -c SRVR7 -d 3 -daily -m
```

This command creates a new backup in the Daily backup management group. The backup is verified on SRVR7, and all older Daily backups are deleted except for the three most recent ones. No SnapMirror mirror replication is initiated after the backup, even if the volume is a SnapMirror source volume.

Backup Example #3:

```
snapbackup EXCHSRVR3 -b 1 "First Storage Group" -nc -d 4 -weekly -u
-k -a SRVR3 -r "C:\SnapManager Scripts\scriptname.txt"
"$ExchSnapshot $SnapInfoPath"
```

This command creates a new Weekly backup of only the First Storage Group, using the unique naming convention, while deleting all older Weekly backups except for the 4 most recent ones. The up-to-the-minute restore ability is retained for any older backups that remain after the deletions. After the backup is complete, it is archived using the run command after operation capability.

Verification Example #1:

```
snapbackup EXCHSRVR3 -c SRVR6 3 -s 2 "First Storage Group", "Second
Storage Group" -all
```

This command verifies the last 3 backups, in any backup management group, that contains both First Storage Group and Second Storage Group. The server SRVR6 is used to perform the verification.

Standard backups with remote verification using mount points (unique naming convention):

```
"C:\Program Files\NetApp\SnapManager for Exchange\SnapBackup.exe"
"PRODSERVER"  -b 4 "SG2" "First Storage Group" "SG3" "SG4" -c
"VERSERVER" -u -m -mpdir "C:\Program Files\NetApp\SnapManager for
Exchange\SnapMgrMountPoint" -mp
```

Standard backups with local verification using drive letters if available (generic naming convention):

```
"C:\Program Files\NetApp\SnapManager for Exchange\SnapBackup.exe"
"PRODSERVER"  -b 4 "SG2" "First Storage Group" "SG3" "SG4" -c
"PRODSERVER" -m -mpdir "C:\Program Files\NetApp\SnapManager for
Exchange\SnapMgrMountPoint"
```

Daily backups without verification using unique naming convention:

```
"C:\Program Files\NetApp\SnapManager for Exchange\SnapBackup.exe"
"PRODSERVER"  -b 4 "SG2" "First Storage Group" "SG3" "SG4" -nc -u -
m -Daily
```

Weekly backups without verification using generic naming convention:

```
"C:\Program Files\NetApp\SnapManager for Exchange\SnapBackup.exe"
"PRODSERVER"  -b 4 "SG2" "First Storage Group" "SG3" "SG4" -nc -m -
Weekly
```

Standard backup with remote verification using mount points (unique naming convention), performing run command and snapmirror operations after backup:

```
"C:\Program Files\NetApp\SnapManager for Exchange\SnapBackup.exe"
"PRODSERVER"  -b 4 "SG2" "First Storage Group" "SG3" "SG4" -c
"VERSERVER" -u -mpdir "C:\Program Files\NetApp\SnapManager for
Exchange\SnapMgrMountPoint" -mp -a "PRODSERVER" -r
"C:\afterbackup.vbs" "$ExchSnapshot $InfoSnapshot $SnapInfoName
\"$SnapInfoPath\""
```

Verification only operation of 5 most recent backup sets (All backup management groups):

```
"C:\Program Files\NetApp\SnapManager for Exchange\SnapBackup.exe"
"PRODSERVER" -c "VERSERVER" 5 -s 4 "SG2" "First Storage Group"
"SG3" "SG4" -m -All -mpdir "C:\Program Files\NetApp\SnapManager for
Exchange\SnapMgrMountPoint" -mp
```

Standard backups (unique naming convention) with remote verification using mount points, ese throttling of 150, delete backups day based in excess of 7 days :

```
<SnapBackup.exe "PRODSERV" -d 7.000000 -b 4 "First Storage Group"
"SG2" "SG3" "SG4" -c "VERSERV" -u -m -rd -p 150 -mpdir "C:\Program
Files\NetApp\SnapManager for Exchange\SnapMgrMountPoint">
```

Standard backups (unique naming convention) with remote verification using mount points, no ese throttling , delete backups day based in excess of 7 days:

```
<SnapBackup.exe "PRODSERV" -d 7.000000 -b 4 "First Storage Group"
"SG2" "SG3" "SG4" -c "VERSERV" -u -m -rd -mpdir "C:\Program
Files\NetApp\SnapManager for Exchange\SnapMgrMountPoint">
```

Standard backups (unique naming convention) with remote verification using mount points, ese throttling of 150 milli seconds, delete backups day based in excess of 7 days:

```
"C:\Program Files\NetApp\SnapManager for Exchange\SnapBackup.exe"
"PRODSERV" -d 7.000000 -b 4 "First Storage Group" "SG2" "SG3" "SG4"
-c "VERSERV" -u -m -rd -p 150 -mpdir "C:\Program
Files\NetApp\SnapManager for Exchange\SnapMgrMountPoint"
```

Standard backups (unique naming convention) with remote verification using mount points, no ese throttling , delete backups day based in excess of 7 days:

```
"C:\Program Files\NetApp\SnapManager for Exchange\SnapBackup.exe"
"PRODSERV" -d 7.000000 -b 4 "First Storage Group" "SG2" "SG3" "SG4"
-c "VERSERV" -u -m -rd -mpdir "C:\Program Files\NetApp\SnapManager
for Exchange\SnapMgrMountPoint"
```

Configuring SnapManager Application Settings B

This section describes SnapManager application settings that can be configured or changed at any time after SnapManager has been installed. The following topics are covered:

- "Overview of SnapManager application settings" on page 336
- "Connecting to a different Exchange server" on page 338
- "Changing the Exchange user account" on page 340
- "Enabling or disabling database migration back to local disks" on page 341
- Managing the database verification settings
  - "Selecting the database verification server" on page 342
  - "Selecting the Snapshot copy access method for database verification" on page 346
  - "Configuring Eseutil throttling for database verification" on page 348
  - "Overriding database verification during restore" on page 354
- "Managing the backup setting" on page 357
- "Managing the Run Command After Operation default settings" on page 358
- "Managing fractional space reservation" on page 360
- "Managing the report directory options" on page 372
- "Managing the event notification options" on page 374

Attention

You must run SnapManager from the system console, not from a Terminal Services client. Do not use Terminal Services for any type of SnapManager administration, because you might miss critical information that is displayed only in pop-up boxes at the system console.

This section **does not** describe the following topics:

- Settings that can be configured only with the Configuration Wizard
- Settings that are specific to the context of a particular backup or a database verification operation

This information is described in other, related topics in this guide.

Related topics:

- "Settings configurable only with the Configuration Wizard" on page 116
- Chapter 9, "Backing Up Databases with SnapManager," on page 163
- Chapter 10, "Restoring Databases with SnapManager," on page 183

Overview of SnapManager application settings

The following table lists SnapManager application settings that can be configured or changed at any time after SnapManager has been installed. Shaded rows indicate settings that can also be configured using the Configuration Wizard.

Application setting	How the setting can be accessed
Exchange server to manage[1]	Action menu
Exchange user account	Options menu
Migrate databases to local disk	Options menu
Database verification settings[2] ◆ Verification server ◆ Override for restore ◆ Eseutil throttling ◆ Mount point	◆ Options menu ◆ Backup Wizard ◆ Restore Wizard
Backup settings	◆ Options menu ◆ Backup Wizard ◆ Backup and Verification tab
Run Command After Operation[3] default settings	◆ Options menu ◆ Within the context of a backup or database verification operation: ❖ Backup Wizard ❖ Backup and Verification tab
Fractional space reservation policy settings ◆ Current status ◆ Policy settings	Options menu
Report directory options	Options menu
Event notification settings ◆ Email ◆ Logging	◆ Configuration Wizard ◆ Options menu

1. The first time you start SnapManager, the application automatically opens this dialog box to prompt you for this setting. See Chapter 4, "Starting SnapManager for the First Time," on page 63.
2. From the Configuration Wizard, you can specify only the verification server. In order to access other verification settings (Override Verification, Eseutil Throttling, and Access LUN in Snapshot Copy), you must open the Verification Settings dialog box.
3. When the Run Command After Operation dialog box is opened from the Options menu, only the default settings can be viewed or configured. See "Managing the Run Command After Operation default settings" on page 358. However, from within the context of a specific operation, the default settings are presented and then can be modified for this operation only. As an option, the default settings can be updated. See "Using Run Command After Operation to archive automatically" on page 313.

Connecting to a different Exchange server

Use the Connect to Exchange Server dialog box to connect to the Exchange server you want to manage and specify the security authentication method to be used to establish the connection.

- "About the Connect to Exchange Server dialog box" on page 338
- "Connecting to a different Exchange server" on page 338

About the Connect to Exchange Server dialog box

Use the Connect to Exchange Server dialog box to connect to a specific Exchange server. When you specify or change the Exchange server specified in this dialog box, SnapManager immediately connects to that server. This setting remains in effect, specifying the default Exchange server, until or unless you change it.

When you start SnapManager, the Connect to Exchange Server dialog box opens automatically if a **default Exchange server** has not yet been specified. You cannot proceed to use SnapManager until you successfully connect to an Exchange server. Thereafter, whenever the SnapManager application is started, it automatically connects to the default Exchange server using the default security authentication method.

If at a later time you want to manage a **different Exchange server**, explicitly open the Connect to Exchange Server dialog box to connect to the remote Exchange server using an Exchange server account that belongs to the `Administrators` group on that machine.

Connecting to a different Exchange server

To connect to a different Exchange server, complete the following steps.

Step	Action
1	Open the Connect to Exchange Server dialog box. ◆ If the default Exchange server has not yet been specified, SnapManager automatically opens the dialog box when you start SnapManager. In this case, the Exchange Server box is empty. ◆ If SnapManager is already connected to the default Exchange server, open the dialog box explicitly. To do this, go to the menu bar and select Action > Connect to Another Exchange Server. In this case, the Exchange Server box displays the name of the currently connected Exchange server and the Exchange release and build numbers.
2	In the Exchange Server box, specify the Exchange server you want to manage.
3	Click OK. **Result:** The Connect to Exchange Server dialog box closes, and SnapManager connects to the specified Exchange server using the specified security authentication method. **Note** Whenever you connect to an Exchange server, SnapManager checks that the Exchange server is running the supported versions of Exchange and SnapDrive. These checkpoints are described within the procedure described in "Starting SnapManager and connecting to the default server" on page 64.
4	If, instead of connecting to the specified Exchange server, SnapManager displays an error message regarding the Exchange server or SnapDrive version on that Exchange server, do the following: **a.** Refer to "Windows host system requirements" on page 24 to determine which software components you need to update on the Exchange server. **b.** Close the SnapManager application. **c.** Upgrade the software on the Exchange server as needed. **d.** Restart SnapManager.

Changing the Exchange user account

You can change the SnapManager server process account used to run SnapManager backup and restore operations.

To change the SnapManager server process account used to run SnapManager backup and restore operations, complete the following steps.

Step	Action
1	Open the Local SnapManager Server Properties dialog box. There are two ways to do this: ◆ From the SnapManager main window, go to the menu bar and select Options > Run SnapManager As. ◆ From the Connect to Exchange Server dialog box, click Change. **Result:** The Local SnapManager Server Properties dialog box appears and displays the name of the current SnapManager account for this Exchange server.
2	Select the SnapManager server process account that you want to use to run SnapManager on this system: ◆ If you want to change the SnapManager server process account on this instance, select the "The launching user" option. ◆ If you want to make SnapManager accessible from a remote Exchange server or within an MSCS environment, select the "This user" option. This option is selected by default.
3	If you select the "This user" option, also do the following: **a.** Either enter the user account in the User box in *DomainName\UserName* format or click Browse to select the domain and user name. **b.** In the Password and the Confirm Password boxes, enter the password for this user account.
4	Click OK. This change will not take effect until you exit this SnapManager session and any currently running SnapManager jobs have completed. After you start a new SnapManager session, any SnapManager operations, such as backup and restore, will run under this newly specified account.

Enabling or disabling database migration back to local disks

The primary function of the Configuration Wizard is to migrate Exchange databases to Data ONTAP LUNs so that the databases can be backed up and restored using SnapManager. If you choose to stop using SnapManager as your data management tool, you can also use the Configuration Wizard to migrate your databases back to local disks. However, by default, the Where to Move databases screen of the Configuration Wizard does not list any local drives unless you explicitly enable the“migrate databases to local disks” feature.

Related topics:

- “Configuring the Exchange data store” on page 118
- “Moving databases using the Configuration Wizard” on page 126
- “Moving transaction logs using the Configuration Wizard” on page 128

To enable or disable the ability to migrate databases from Data ONTAP LUNs back to local disks, complete the following steps.

Step	Action	
1	Open the Configuration Wizard Option Settings dialog box. To do this, select Options > Configuration Wizard Option.	
2	View the current state of the “migrate databases to local disks” feature by noting whether the “Enable databases and transaction logs to be migrated back to local disk” option is enabled.	
	If...	**Then...**
	The option is selected	The migrate-back-to-local-disk feature is *enabled*.
	The option is not selected	The migrate-back-to-local-disk feature is *disabled*.
3	If you want to change the state of this option, click to select or deselect it. **Note** If you enable this option, it is reset the next time you start the SnapManager application.	
4	Click OK to close the dialog box.	

Selecting the database verification server

Verification of the databases in a backup set can be done on the production Exchange server (the Windows host system running the Exchange server used to service the end users) or on a remote verification system (a different Exchange server with Exchange management tools installed).

Running database verification on a production Exchange server is CPU-intensive for the Windows host and also involves a substantial amount of activity on the storage system. SnapManager offers three methods for managing database verification load:

- Deferred verification
- Remote verification
- Verification throttling

The three options for managing database verification load, which can be used separately or in any combination, are described in "Managing database verification load" on page 146.

Note

Both deferred verification and remote verification manage database verification load by separating database verification from the backup operation. Verification throttling manages database verification load by slowing down the verification throughput rate.

This topic provides detailed information about **remote verification**. For more information about remote verification, see the following topics:

- "Remote verification prerequisites" on page 343
- "How remote verification works" on page 343
- "Viewing or changing the verification server" on page 344

Note

When you change the database verification server, this change does not affect any database backup (with verification) or database verification-only jobs that are already scheduled. You will need to recreate the scheduled backup jobs.

Related topics:

- "How SnapManager checks database integrity in backup sets" on page 145
- "Selecting the Snapshot copy access method for database verification" on page 346
- "Configuring Eseutil throttling for database verification" on page 348
- "Overriding database verification during restore" on page 354

Remote verification prerequisites

The following paragraphs describe the prerequisites for using a remote verification server.

Windows host requirements: Remote verification is performed using the same mechanisms used for local verification, except that the verification is performed on a different host than the one that initiated the backup. This is why you need SnapDrive and SnapManager installed on your remote verification server, as well as connectivity to the storage system (FCP or iSCSI). The requirements for a remote verification server are described in "Requirements for a remote verification server" on page 27.

LUN requirements: If you use a remote verification server to verify the databases in multiple databases in a single job, an additional LUN is required. For more information, see "Verifying multiple backup sets using a remote verification server" on page 146.

Verification server designation: To designate a remote verification server, see "Viewing or changing the verification server" on page 344.

How remote verification works

The following list of steps outline the process followed for remote verification.

1. The SnapManager backup with verification (or verification only) is initiated on the primary SnapManager host, which is configured to run verifications on the remote verification server.
2. The primary SnapManager host contacts the remote verification server and initiates the verification job.
3. The remote verification server uses SnapDrive to connect to a LUN backed by the Snapshot copy containing the databases to be verified.
4. The remote verification server performs the database verification on the LUN backed by Snapshot copy.
5. When the remote verification server completes the verification, it sends the results back to the primary SnapManager host.

Note

Whether you run verification remotely or locally, the verification is performed on a LUN backed by Snapshot copy. If you take a Snapshot copy of the same volume while a LUN backed by Snapshot copy exists, you create a "busy Snapshot copy," which might cause problems when you attempt to delete some Snapshot copies. For this reason, you must be careful not to schedule backups while a verification is in progress.

Viewing or changing the verification server

To view or change the verification server, complete the following steps *from the production Exchange server.*

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td>1</td><td colspan="2">Connect to the production Exchange server, and then open the Database Verification Settings dialog box.</td></tr>
<tr><td></td><td>From the...</td><td>Do this...</td></tr>
<tr><td></td><td>SnapManager menu bar</td><td>Select Options > Database Verification Settings.</td></tr>
<tr><td></td><td>Backup Wizard</td><td>Go to the Verify the Databases and Transaction Logs in this Backup screen, and then click Verification Settings.</td></tr>
<tr><td></td><td>Restore Wizard</td><td>Go to the Verify Database Integrity in the Selected Backup screen (displayed only if you choose to restore from an unverified backup, and then click Verification Settings.</td></tr>
<tr><td></td><td colspan="2">Result: The Database Verification Settings dialog box appears. The Verification Server tab is active by default and displays the host name of the current verification server.</td></tr>
<tr><td>2</td><td colspan="2">In the Verification Server box, type or browse to the Exchange server you want to use as the database verification server.

Note
If you plan to specify a remote verification server, ensure that the server is set up properly, as described in “Requirements for a remote verification server” on page 27.</td></tr>
</table>

Step	Action
3	Click OK. **Result:** The Verification Settings dialog box closes. **Note** Until you change these settings, database verification is run from the Exchange server you selected. It does not necessarily run on the system from which you opened the Database Verification Settings dialog box. It does not affect any database verification jobs that are already scheduled.

Selecting the Snapshot copy access method for database verification

Use the Access LUN in Snapshot tab to specify how SnapManager is to access database backup Snapshot copies during database integrity verification.

Related topics:

- "Selecting the database verification server" on page 342
- "Configuring Eseutil throttling for database verification" on page 348
- "Overriding database verification during restore" on page 354

To specify which method is to be used to access database backup Snapshot copies during database integrity verification, complete the following steps.

Step	Action	
1	Access the Access LUN in Snapshot tab.	
	From the...	**Do this...**
	Configuration Wizard	Go to the Database Verification Server screen, and then click Advanced.
	SnapManager menu bar	Select Options > Database Verification Settings, and then select the Access LUN in Snapshot tab.
	Backup Wizard	Go to the Verify the Databases and Transaction Logs in this Backup screen, click Verification Settings, and then select the Access LUN in Snapshot tab.
	Restore Wizard	Go to the Verify Database Integrity in the Selected Backup screen (displayed only if you choose to restore from an unverified backup, click Verification Settings, and then select the Access LUN in Snapshot tab.

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td>2</td><td colspan="2">Assign either a drive letter or directory path to access the backup Snapshot copy as a mounted LUN.</td></tr>
<tr><td></td><td>If you want to...</td><td>Then...</td></tr>
<tr><td></td><td>Mount the Snapshot copy on the next available drive letter</td><td>Select the “Automatically assign available drive letter” option.</td></tr>
<tr><td></td><td>Mount the Snapshot copy on a specific NTFS mount point</td><td>Do the following:
a. Select the “Mount in an empty NTFS directory” option.
b. Enter or browse to the directory path of an NTFS mount point.
Note
This mount point will be used if SnapManager is configured to use drive letters but runs out of available drive letters.</td></tr>
<tr><td>3</td><td colspan="2">Click OK.
Result: The Verification Settings dialog box closes.</td></tr>
</table>

Configuring Eseutil throttling for database verification

When installed with Exchange 2003 SP2, SnapManager supports the ability to throttle the database checksum verification rate. For more information, see the following topics:

- "About database verification load" on page 348
- "Requirements for using the Eseutil throttling option" on page 348
- "How the database verification throttling feature works" on page 349
- "The effect of using different throttling values" on page 349
- "Choosing the sleep interval" on page 349
- "Configuring the throttling option" on page 352
- "Entries in the SnapManager backup and verification report" on page 353

Related topics:

- "Selecting the database verification server" on page 342
- "Selecting the Snapshot copy access method for database verification" on page 346
- "Overriding database verification during restore" on page 354

About database verification load

Database verification can place a significant load on both the Exchange server and the storage system. For this reason, verification can degrade Exchange Server response, particularly during peak work hours. With SnapManager 3.1 and earlier releases, there are two options for distributing this load by separating database verification database backup operations: **deferred database verification** and **remote database verification**.

SnapManager 3.2 supports a third option for managing database verification, that you can combine with either or both of the existing options, to reduce the load even further. When installed with Microsoft Exchange 2003 SP2, SnapManager 3.2 supports the ability to throttle Eseutil (the Microsoft Exchange consistency checker utility) in database checksum verification mode.

Requirements for using the Eseutil throttling option

This Eseutil throttling feature was first introduced with Exchange 2003 SP2, and SnapManager 3.2 provides a configuration option for configuring this feature.

Note

Attempting to use the throttling feature with earlier versions of SnapManager or Exchange will have no effect.

How the database verification throttling feature works

Exchange 2003 SP2 added a feature to `Eseutil.exe`, the Microsoft Exchange consistency checker utility, that can insert a one-second pause after a given number of I/O operations during the database physical consistency verification.

The effect of using different throttling values

`Eseutil.exe` reads 512 KB for each database checksum verification I/O operation. Therefore, when configuring the throttling value, the maximum throughput rate for database checksum verification is decreased to the following:

512 KB per I/O × *x* I/Os per second = 512 × *x* KB/second

To decrease the maximum throughput rate, decrease the number of I/O operations (*x*) that elapse between one-second pauses. The following examples illustrate the effect of using throttling values of 100, 150, 200, and 250 for *x*.

Number of I/O operations (*x*) between one-second pauses	**Maximum possible database verification speed**	
	Calculation	**Maximum speed**
100	512 KB/IO × 100 IO/sec = 51,200 KB/sec	50 MB/sec
150	512 KB/IO × 150 IO/sec = 76,800 KB/sec	75 MB/sec
200	512 KB/IO × 100 IO/sec = 102,400 KB/sec	100 MB/sec
250	512 KB/IO × 250 IO/sec = 128,000 KB/sec	125 MB sec

Note

Decreasing the `Eseutil.exe` database verification throughput causes the database checksum verification to take longer to complete. This also means that a backup job that is configured with verification will also take longer to complete. However, decreasing verification throughput does not cause a backup job without verification configured to take any longer to complete.

Choosing the sleep interval

Calculate the appropriate sleep interval value to use *for each Exchange server.* This entails monitoring the read and write performance of the LUNs on which the Exchange databases reside and then adjusting the verification throttle setting so that the average and peak physical disk performance is below the maximum values determined by Microsoft.

To calculate the Eseutil throttling value for a specific Exchange server, complete the following steps.

Step	Action
1	Launch the Windows Performance Monitor utility (also known as "Perfmon") on the machine that is the Exchange server.
2	Add the following Perfmon counters for each Data ONTAP LUN that contains an Exchange database: ◆ PhysicalDisk\Average Disk sec/Read ◆ PhysicalDisk\Average Disk sec/Write **Note** Monitor the LUNs containing the live Exchange databases, not the LUN in Snapshot copy that is mounted and verified by the verification process.
3	Monitor these pairs of values while a SnapManager verification job or a backup job with verification is in progress. Follow these guidelines: ◆ To monitor the SnapManager progress, watch the Backup Status window that is displayed during a manually launched backup job. ◆ If monitoring a backup with verification job, be sure to monitor the counters during the *verification portion* of the job. ◆ Multiple databases on the same Exchange server are verified sequentially, so be sure to monitor the counters for *all* of the database verifications. ◆ Monitor the counters during the busiest time of day that a verification or backup with verification job might occur.
4	The throttle setting is global, so select the reading from the database that exhibits the worst performance (highest readings).

Step	Action
5	Compare the measured values to the maximum values recommended by Microsoft. **PhysicalDisk\Average Disk sec/Read:** The average physical disk performance times determined by Microsoft are as follows: ◆ Average read time should be below 20 ms. ◆ Maximum peak read time should be below 50 ms. **PhysicalDisk\Average Disk sec/Write:** The maximum physical disk performance times determined by Microsoft are as follows: ◆ Average write time should be below 20 ms. ◆ Maximum peak write time should be below 50 ms. **Note** These values are good guidelines during **peak** Exchange usage hours. During **off-peak** Exchange hours, higher latencies may be acceptable.
6	If the measured values exceed the maximum values recommended by Microsoft, adjust the throttle setting to decrease the verification throughput rate.

Configuring the throttling option

To configure database verification throttling, complete the following steps on every Windows host system that will be performing database verification and is running Exchange 2003 SP2.

Note

You can configure the throttling option on *all* systems involving database verification, but the throttling feature of `Eseutil` is only supported by Exchange 2003 SP2.

Step	Action	
1	Open the Verification Settings dialog box.	
	From the...	**Do this...**
	SnapManager menu bar	Select Options > Database Verification Settings.
	Backup Wizard	Go to the Verify the Databases and Transaction Logs in this Backup screen, and then click Verification Settings.
	Restore Wizard	Go to the Verify Database Integrity in the Selected Backup screen (displayed only if you choose to restore from an unverified backup, and then click Verification Settings.
2	Select the Eseutil Throttling tab.	
3	Select or deselect the "Throttle Eseutil database checksum verification" option to enable or disable the Eseutil throttling feature. **Note** The "Throttle Eseutil database checksum verification" option is accessible only if the verification server is installed with Microsoft Exchange 2003 SP2. **Result:** If you enabled the Eseutil throttling feature, the "Pause for 1 second after *x* I/O operations" box displays the current sleep interval. The default value is 150. If you disabled the feature, the box is grayed out and inaccessible.	

Step	Action
4	If you enabled the Eseutil throttling feature, enter a positive integer value in the "Pause for 1 second after *x* I/O operations" box. The default value is 150. Enter the number I/O operations to complete before pausing for one-second during the database physical consistency check. Refer to the formula and example calculations in "The effect of using different throttling values" on page 349. It has been observed that using a value in the range of 100 to 250 is suitable for most environments.
5	Click OK.

Entries in the SnapManager backup and verification report

Before each database verification, the SnapManager backup and verification report indicates whether the feature is enabled:

- If the feature is enabled, the report includes the following entry:
  `ESEUTIL throttling feature is enabled.`
- If the feature is not enabled, the report includes the following entries:
  `ESEUTIL throttling feature is disabled.`
  `ESEUTIL output will show the throttling parameter.`

Overriding database verification during restore

You are strongly advised to restore only from verified backups. By default, SnapManager does not allow you to select an unverified backup as the source of the restore operation. However, if a verified backup is not available when you need to restore and you cannot wait for a verification to complete before restoring, you can override the verification requirement and restore directly from an unverified backup. For more information, see the following topics:

- "Configuring the database verification override option" on page 354
- "Entry in the SnapManager restore report" on page 356

Attention

If you must restore from an unverified backup, it is best to perform an up-to-the-minute restore. This way, if you discover later that the backup was corrupted, you can restore from another backup to recover.

Related topics:

- "Selecting the database verification server" on page 342
- "Selecting the Snapshot copy access method for database verification" on page 346
- "Configuring Eseutil throttling for database verification" on page 348

Configuring the database verification override option

By default SnapManager Restore requires that you restore only from verified backups. To override this requirement until you exit the SnapManager application, complete the following steps.

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Open the Verification Settings dialog box:
From the SnapManager menu bar, select Options > Database Verification Settings.
From the Backup Wizard, go to the Verify the Databases and Transaction Logs in this Backup screen, and then click Verification Settings.
From the Restore Wizard, go to the Verify the Database Integrity in this Backup screen (displayed only if you choose to restore from an unverified backup), and then click Verification Settings.
<table>
<tr><th>From the...</th><th>Do this...</th></tr>
<tr><td>SnapManager menu bar</td><td>Select Options > Database Verification Settings.</td></tr>
<tr><td>Backup Wizard</td><td>Go to the Verify the Databases and Transaction Logs in this Backup screen, and then click Verification Settings.</td></tr>
<tr><td>Restore Wizard</td><td>Go to the Verify Database Integrity in the Selected Backup screen (displayed only if you choose to restore from an unverified backup, and then click Verification Settings.</td></tr>
</table></td></tr>
<tr><td>2</td><td>Select the Override Verification tab.</td></tr>
<tr><td>3</td><td>Configure the Override Database Verification Requirement for Restore option:
If you must restore from an unverified backup, select the option.
Otherwise, deselect the option or leave it deselected.
Note
If you enable this option, it is reset the next time you start the SnapManager application.</td></tr>
</table>

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>4</td><td>If a message box appears, do the following:

a. Heed the warning in the message box:

<pre>WARNING: An unverified backup may contain an image of an Exchange database that is physically corrupt. If the backup contains physical database corruption, this corruption will persist in the restored database.

Are you sure that you want to enable this option?</pre>b. If want to enable the option, click OK; otherwise, click No.

Result: The message box closes.</td></tr>
<tr><td>5</td><td>To close the dialog box and apply your change, click OK.

Note
If you are using the Restore Wizard, selecting this option causes the “Verify the database integrity of this backup prior to restoring it” option to become accessible so that you can disable it.

<table><tr><th>If...</th><th>Then...</th></tr><tr><td>The override option is disabled (the default and recommended setting)</td><td>You cannot select an unverified backup as the source of the restore operation.</td></tr><tr><td>The override option is enabled (not recommended)</td><td>If you select an unverified backup as the source of the restore operation, you are given the option to proceed with the restore operation.

Note
This option is reset when you exit SnapManager.</td></tr></table></td></tr>
</table>

Entry in the SnapManager restore report

Before each database verification, the SnapManager restore report indicates if this option is enabled. If the feature is enabled, the report includes the following warning:

```
Database verification before restore was overridden.
```

Managing the backup setting

This topic describes how to specify the naming convention you want used to form database backup Snapshot copy names and SnapInfo directory Snapshot copy names.

To set the backup naming convention option, complete the following steps.

Step	Action
1	Access the backup naming convention option: ◆ From the SnapManager menu bar, select Options > Backup Setting. ◆ From the Backup Wizard, go to the Backup Naming Convention screen.
2	Select the naming convention you want used to form database backup Snapshot copy names and SnapInfo directory Snapshot copy names: ◆ If you want the most recent backup to be identified by the Snapshot copy name that includes the string `recent`, select the Use Generic option. This option is selected by default. ◆ If you want all Snapshot copy names, even for the most recent backup, to contain the Snapshot copy creation date and time, select the Use Unique option. This is the Snapshot copy naming convention used by SnapManager for Microsoft Exchange releases *prior to release 3.0*. For more detailed information, see "SnapManager Snapshot copy naming conventions" on page 142.
3	Click OK. **Result:** SnapManager will apply the selected naming convention to all subsequent backup operations.

Managing the Run Command After Operation default settings

You can configure default values that you want used to prepopulate the Run Command After Operation dialog box when it is opened from either the Backup and Verification tab or the Backup Wizard.

Related topics:

- "Using a Windows backup utility to archive SnapManager backups" on page 308
- "Using Run Command After Operation to archive automatically" on page 313

To use the Run Command After Operation dialog box to configure default settings, complete the following steps.

Step	Action
1	Open the Run Command After Operation dialog box from the Option menu. To do this, select Options > Default Run Command After Operation.
2	In the "Specify a computer where..." box, enter or browse to the name of the host on which your program or script resides.
3	In the "Specify the full path..." box, browse to your program or script.

Step	Action
4	Form the command input string in the Command Arguments box. You can do this using any combination of the following methods: ◆ To enter text directly into the Command Arguments box, click in the box and type the desired text. ◆ To enter a SnapManager variable into the Command Arguments box, do the following: **a.** If necessary, click in the Command Arguments box to position the cursor. **b.** In the SnapManager Variables list, select the variable you want to enter. For more information, see "Command arguments pass information to your program or script" on page 314. **c.** Click Select. **Note** The `$SnapInfoPath` variable is automatically enclosed within double quotes so that the actual path name can contain spaces without affecting the script invocation on the Windows command line. If you do not want the double quotes to appear in your command line, remove them from the Command Arguments field in the Run Command After Operation dialog box.
5	Repeat Step 4 as needed until the Command Arguments box contains the arguments you want to pass to your program or script.
6	Click OK to apply your changes and close the Run Command After Operation dialog box. **Result:** SnapManager verifies that the specified program exists on the specified system. Whenever the Run Command After Operation dialog box is opened from either the Backup and Verification tab or the Backup Wizard, the boxes will be prepopulated with the values you specified as default settings. **Note** SnapManager does not run the command at this time.

Managing fractional space reservation

This topic summarizes Data ONTAP fractional space reservation and describes how to configure SnapManager fractional space reservation policies:

- "About fractional space reservation" on page 360
- "What can happen with a fractional-space-reserved volume" on page 361
- "Fractional space reservation policies manage Exchange data" on page 362
- "About the default fractional space reservation policy" on page 364
- "Viewing fractional space reservation status" on page 365
- "Configuring fractional space reservation policies" on page 367

About fractional space reservation

The following paragraphs summarize space reservation and fractional space reservation as supported by Data ONTAP 7.1 or greater. For more detailed information about these features, see the *Data ONTAP Block Access Management Guide for iSCSI and FCP* for release 7.1 or later.

Space reservation: When you create a LUN on a storage system volume, Data ONTAP reserves enough space in the traditional or flexible volume so that write operations to those LUNs do not fail due of a lack of disk space on the storage system. Other operations, such as taking a Snapshot copy or the creation of new LUNs, can occur only if there is enough available unreserved space; these operations are restricted from using reserved space.

SnapDrive creates and manages LUNs with space reservation enabled. That is, additional space on the storage system volume is automatically reserved for overwriting blocks that belong to a LUN. By default this additional space is equal to 100 percent of the total size of all space-reserved LUNs in the storage system volume. If space reservation is disabled, write operations to a LUN might fail due to insufficient disk space in the storage system volume and the host application may terminate, report I/O errors, or experience unexpected behavior.

Fractional space reservation: With fractional reserve, the amount of space reserved for overwrites is set to less than 100 percent of the total size of all space-reserved LUNs in a traditional volume or a flexible volume that has the guarantee option set to `volume` rather than file. The space that is preallocated for space reservation is reduced to that percentage. Fractional reserve is generally used for volumes with LUNs that store data with a **low rate of change**.

While space reservation is enabled at the LUN level, fractional overwrite reserve amounts are configured at the volume level; that is, fractional space reservation does not control how the total amount of space reserved for overwrites in a volume is applied to individual LUNs in that volume.

What can happen with a fractional-space-reserved volume

When a LUN is fully space reserved, write operations to that LUN are guaranteed against failure caused by an out-of-space condition due to Snapshot copy disk space consumption. When the overwrite reserve for a volume is set to less than 100 percent, however, write operations to the LUNs on that volume are no longer guaranteed when the storage system volume runs low in free disk space due to Snapshot copy space consumption.

Attention

If a storage system volume runs out of overwrite reserve space, write operations to a LUN on that volume will fail and the host application may terminate, report I/O errors, or exhibit unexpected behavior.

Data ONTAP provides two space management tools tor ensure that a fractionally space-reserved volume does not run out of overwrite reserve: automatic FlexVol expansion and automatic Snapshot copy deletion from FlexVol volumes. These features, summarized in the following paragraphs, monitor the reserved space and take action if the free space becomes scarce. For more detailed information, see the *Data ONTAP Block Access Management Guide for iSCSI and FCP* for release 7.1 or later.

Automatic expansion of flexible volumes: Data ONTAP can automatically expand the volume that is used to store Snapshot copy data, provided the volume is a flexible volume with the guarantee option set to `volume`. When the flexible volume is nearly full, Data ONTAP automatically expands the volume into the space preallocated for it in the aggregate. The automatic Snapshot copy deletion and FlexVol expansion features can be enabled separately, or together with one policy to be applied before the other. When fractional-space-reserved volumes hold LUNs that store Exchange database files, however, only the automatic FlexVol expansion feature can be used, if needed.

Automatic deletion of Snapshot copies from flexible volumes: Data ONTAP can automatically delete one or more Snapshot copies on the volume, provided the Data ONTAP Snapshot copy autodeletion policy is enabled and set to trigger when the overwrite reserve is nearly full on the volume. If the trigger condition is detected, the oldest or newest Snapshot copies are deleted until a configured percentage of the volume is free space. Note that this Data ONTAP feature is not designed specifically to support backup and restore operations on Exchange databases:

- The options for selecting Snapshot copies to be deleted do not have visibility to the automatic backup Snapshot copy deletion criteria configured in SnapManager.
- Exchange administrators want to retain at least one online backup for each database at all times.

If the Data ONTAP Snapshot copy autodelete policy is enabled for a volume that stores SnapManager backup set components, either disable the policy or configure it so that it does not delete the SnapManager backup set components. For more information, see "Viewing fractional space reservation status" on page 365.

Fractional space reservation policies manage Exchange data

In a SnapManager environment in which Exchange data is stored on LUNs in a fractional space-reserved storage system volume, the Exchange administrator needs to avoid an out-of-space condition on the volume in a way that allows explicit or implicit Exchange-aware control over the deletion of Exchange backup set components. To address this need, SnapManager provides its own space management tool for monitoring overwrite reserve utilization on the volumes. If overwrite reserve space runs low for a fractional space-reserved volume, SnapManager can take action to prevent the overwrite reserve from becoming fully depleted. Specifically, SnapManager can **delete Exchange backup sets** or **dismount Exchange databases** (or both), triggered when the overwrite reserve utilization for the volume reaches specific thresholds specified in the fractional space reservation policy.

Note

If SnapManager e-mail notification is enabled, SnapManager sends SMTP e-mail after a SnapManager fractional space reservation policy event finishes.

Automatic deletion of Exchange backups: SnapManager provides for the automatic deletion of backups of LUNs that store Exchange data. When enabled, this component of the SnapManager fractional reservation policy serves as the Exchange-aware replacement for or adjunct to the Data ONTAP Snapshot copy deletion feature. If the level of overwrite reserve utilization on the volume reaches a threshold specified by the policy, automatic backup deletion is triggered and SnapManager deletes Exchange backups as follows:

- Delete the oldest backup Snapshot copies first.
- Retain the specified number total backup Snapshot copies on the volume.
- Retain the most recent backup of any database (if it resides on the volume).
- Retain any backups of databases no longer in existence.

Choose the backup retention level based on your SnapManager backup creation and verification schedule. If Snapshot copy deletion triggers, enough backup Snapshot copies should be retained so that *at least one verified backup* remains on the volume. Due to these Exchange-aware features, the automatic deletion of Snapshot copies does not necessarily prevent an out-of-space condition on the volume.

SnapManager execute based on the policy for the volume that exceeds the thresholds, not other volumes that could exist in the same backup set.

For example, suppose you have an Exchange server the has backup that span multiple volumes and with the following automatic deletion thresholds configured:

- Volume 1: Delete all but 2 Snapshot copies if 20% overwrite reserve utilization is exceeded.
- Volume 2: Delete all but 5 Snapshot copies if 20% overwrite reserve utilization is exceeded.
- Volume 3: Delete all but 10 Snapshot copies if 20% overwrite reserve utilization R is exceeded.

If the 20% overwrite reserve utilization threshold for Volume 1 is exceeded, SnapManager deletes all but two Snapshot copies, regardless of the policies for Volumes 2 and 3. If the 20% overwrite reserve utilization threshold for Volume 2 is exceeded, SnapManager deletes all but five Snapshot copies., regardless of the policies for Volumes 1 and 3.

Set the same number of backup sets to delete on exchange database and logs LUN residing on storage system volumes. If there is a mismatch in this number, SnapManager attempts to delete backup sets based on the the fractional reserve policy settings.

Automatic dismounting of Exchange databases: SnapManager provides for the automatic dismounting of Exchange databases in space-reserved LUNs, triggered if overwrite reserve utilization on the volume reaches the threshold specified by the fractional space reservation policy. This effectively stops Exchange write operations to LUNs in a storage system volume where overwrite reserve space is nearly full. This second component of the fractional space reservation policy is a last resort action that prevents further consumption of overwrite reserve. Therefore, it is always enabled.

When both components of a fractional space reservation policy are enabled, the **dismounting of Exchange databases** must be triggered at a *higher level of overwrite reserve utilization* than is used to trigger the **deletion of Exchange backup Snapshot copies**. This causes SnapManager to first use backup set deletion to free up some overwrite reserve. If this is not sufficient, dismounting the affected database prevents further consumption of overwrite reserve.

Attention

If another host or client continues to write data to the affected volume, the overwrite reserve space may still run out and the storage system volume will go offline. For this reason, it is recommended that dedicated volumes are used for Exchange data.

Fractional space reservation policy settings: The following table summarizes the fractional space reservation policy by listing each setting, along with its factory default value and its configurable values.

SnapManager fractional space reservation policy setting	Factory default value	Configurable values
Deletion of Exchange backup Snapshot copies		
Status:	Enabled	Enabled or disabled [1]
Trigger on overwrite reserve utilization:	70%	1% – 99% [2]
Number of Snapshot copies to retain:	5	1 – 256
Dismounting of Exchange databases		
Status:	Always enabled [1]	
Trigger on overwrite reserve utilization:	90%	1% – 99% [2]

[1] Enabling automatic deletion of Exchange backup Snapshot copies does not necessarily prevent an out-of-space condition on the volume. Therefore, database dismounting is always enabled.

[2] Enabling automatic deletion of Exchange backup Snapshot copies does not necessarily prevent an out-of-space condition on the volume. Therefore, if Snapshot copy deletion is enabled, it must be configured to trigger *prior to* database dismounting.

About the default fractional space reservation policy

The default fractional space reservation policy is automatically enabled for any traditional or flexible storage system volume that has overwrite reserve set to less than 100 percent and contains LUNs that store Exchange database files, Exchange transaction log files, or SnapManager SnapInfo directories.

Default policy with default settings: You can use the default policy as-is, allowing the factory default values to be applied to every storage system volume that contains fractional-space-reserved LUNs.

Default policy with customized settings: Optionally, you can customize the default policy that is applied to all storage system volume that contains fractional-space-reserved LUNs.

Volume-specific policies: Optionally, you can override the default policy for any particular volume that contains fractional-space-reserved LUNs, by applying a custom policy.

Viewing fractional space reservation status

In the Fractional Space Reservation Settings dialog box, use the Current Settings tab to view the current space consumption in the storage system volumes that contain LUNs that store Exchange data or SnapInfo directories.

Drive Letter or Mount Point: *A SnapManager configuration setting for the LUN.* The drive letter or NTFS mount point on which the LUN is mounted.

Fractional Reserve (%): The amount of space reserved for overwrites on the storage system volume that contains this LUN. Expressed as a percentage of the total size of all space-reserved LUNs in the volume.

Backup Autodelete Trigger (%): *A SnapManager fractional space reservation policy setting for the storage system volume that contains the LUN.* The percentage of overwrite reserve utilization that triggers automatic deletion of Exchange backup sets.

Disable Database Trigger (%): *A SnapManager fractional space reservation policy setting for the storage system volume that contains the LUN.* The percentage of overwrite reserve utilization that triggers automatic disabling of Exchange databases.

Used Reserve: For the storage system volume that contains this LUN, the amount of overwrite reserve **in use**. Expressed in two ways: as a percentage of the total size of all space-reserved LUNs in the volume and in megabytes.

Available Reserve (MB): For the storage system volume that contains this LUN, the amount of overwrite reserve **available**.

Snapshot Autodelete: For the storage system volume that contains this LUN, the state of the Data ONTAP Snapshot copy autodeletion feature: enabled or disabled. If this LUN stores Exchange data files and is contained in a storage system volume for which the Data ONTAP Snapshot copy autodeletion feature is enabled, disable this feature on that volume or ensure that it is configured so that it will not delete SnapManager backup set components.

To view the current space consumption information about each LUN, complete the following steps.

Step	Action
1	In the SnapManager main window, select Options > Fractional Space Reservation Settings.

Step	Action
2	In the Current Settings tab, note the space consumption status for each LUN that stores Exchange data or SnapInfo directories. ◆ The following columns displays SnapManager configuration information: ❖ Drive Letter or Mount Point ❖ Backup Autodelete Trigger (%) ❖ Disable Database Trigger (%) **Note** The SnapManager fractional space reservation policy triggers (listed above) are not applicable to fully space-reserved LUNs. ◆ The following columns displays the fractional overwrite reserve settings and status: ❖ Fractional Reserve (%) ❖ Used Reserve (%) ❖ Used Reserve (MB) ❖ Available Reserve (MB) ❖ Snapshot Autodelete **Note** If Fractional Overwrite Reserve (%) is 100, the LUN is contained in a fully space-reserved volume rather than a fractionally space-reserved volume. The information displayed in this tab automatically refreshes every 60 seconds. **Note** Only the Drive Letter or Mount Point column displays LUN-specific information. All other columns in this tab display information that applies across the storage system volume that contains the LUN.

Step	Action
3	If the Snapshot Autodelete column is `Enabled`, investigate the cause and take preventive action if necessary. **Attention** If the Storage Snapshot Autodelete column is `Enabled`, the LUN is contained in a FlexVol™ volume that has overwrite reserve set to less than 100 percent and that also has the Data ONTAP automatic Snapshot copy deletion feature enabled and configured to trigger when the overwrite reserve is nearly full. If Exchange data or SnapManager SnapInfo directories are stored on LUNs contained in a volume with these characteristics, the Data ONTAP Snapshot copy autodeletion policy might delete Exchange backup set components. If the Storage Snapshot Autodelete column is `Enabled`, take one of the following actions on the volume: ◆ Disable the Data ONTAP Snapshot copy autodelete feature. ◆ Ensure that the Data ONTAP Snapshot copy autodelete feature is configured in such a way that it will not delete Exchange backup set components. For details about the `snap autodelete` storage system command, see the *Data ONTAP™ Block Access Management Guide for iSCSI and FCP* for release 7.1 or later. **Note** The SnapManager fractional space reservation policy includes a separate, Exchange-aware autodeletion feature. For details, see "Automatic deletion of Exchange backups" on page 362 and "Configuring fractional space reservation policies" on page 367. The SnapManager autodeletion feature can be used in place of or in conjunction with the Data ONTAP autodeletion feature; you can also choose to disable the SnapManager autodeletion feature.
4	To close the dialog box, click **OK**.

Configuring fractional space reservation policies

In the Fractional Space Reservation Settings dialog box, use the Policy Settings tab to view or customize the default policy and to configure custom policies for individual fractional-space-reserved LUNs.

The default fractional space reservation policy and its factory default settings are described in "About the default fractional space reservation policy" on page 364.

Note

SnapManager automatically applies the default policy to every storage system volume that contains fractional-space-reserved LUNs that store Exchange database files or SnapInfo directories. Therefore, your storage is protected from an out-of-space condition, without requiring you to explicitly enable or configure any fractional space reservation policies.

To configure the fractional space reservation policy, complete the following steps.

<table>
<tr><th>Step</th><th colspan="2">Action</th></tr>
<tr><td>1</td><td colspan="2">In the SnapManager main window, select Options > Fractional Space Reservation Settings.</td></tr>
<tr><td>2</td><td colspan="2">Select the Policy Settings tab.</td></tr>
<tr><td colspan="3">Choose to specify either the default policy or a volume-specific policy</td></tr>
<tr><td>3</td><td colspan="2">In the left navigation tree, select the scope of the policy you want to view or change in the main panel on the right-hand side of the tab:</td></tr>
<tr><td></td><td>If you want to view or change...</td><td>Then do this...</td></tr>
<tr><td></td><td>The default policy</td><td>In the navigation tree, select Default Policy.</td></tr>
<tr><td></td><td>A volume-specific policy</td><td>In the navigation tree, select the storage system and then the volume.</td></tr>
</table>

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td colspan="2">Disable or configure automatic deletion of Exchange backup Snapshot copies</td></tr>
<tr><td>4</td><td>Use the “Automatically delete backup sets” panel to disable, enable, or configure automatic deletion of Exchange backup Snapshot copies in fractional-space-reserved LUNs on the volume.

Note
Although automatic deletion of Exchange backup Snapshot copies does not necessarily prevent an out-of-space condition on the volume, it is recommended that this feature be enabled for every volume that contains fractional-space-reserved LUNs that store Exchange data.

For more information, see “Automatic deletion of Exchange backups” on page 362.
<table>
<tr><th>If you want to...</th><th>Then do this...</th></tr>
<tr><td>Enable automatic deletion of Exchange backup Snapshot copies</td><td>Select the “Delete backups that include LUNs which have less than 100% overwrite reservation” option, and then skip ahead to Step 7.</td></tr>
<tr><td>Disable automatic deletion of Exchange backup Snapshot copies</td><td>De-select the “Delete backups that include LUNs which have less than 100% overwrite reservation” option, and then proceed to Step 5.</td></tr>
</table>
Note
Data ONTAP includes a separate Snapshot copy autodeletion feature. For details, see “Viewing fractional space reservation status” on page 365. The SnapManager autodeletion feature can be used in place of or in conjunction with the Data ONTAP autodeletion feature.</td></tr>
</table>

Step	Action
5	In the “Trigger point for overwrite reserve utilization” field, enter the level of overwrite reserve utilization (in percentage of total reserve) that is to trigger deletion of Exchange backup Snapshot copies. The value must be a non-negative integer that is less than the “Trigger point for overwrite reserve utilization” value in the “Automatic dismount of databases” panel.
6	In the “Number of most recent backup sets to retain” field, enter the number of backup set to be retained if automatic backup set deletion is triggered. The value must be an integer from 1 through 256 and should be based on the backup creation and verification schedule. For more information, see “Automatic deletion of Exchange backups” on page 362.
Configure automatic dismounting of Exchange databases	
7	Use the “Automatically dismount databases” panel to configure automatic dismounting of Exchange databases in fraction-space-reserved LUNs on the volume. **Note** Because automatic deletion of Exchange backup Snapshot copies does not necessarily prevent an out-of-space condition on the volume, SnapManager does not allow you to disable dismounting of databases for any fractional space reservation policy. In the “Trigger point for overwrite reserve utilization” field, enter the level of overwrite reserve utilization (in percentage of total reserve) that is to trigger dismounting of Exchange databases. The value must be an integer from 0 through 99. **Note** If Snapshot copy autodeletion is enabled, SnapManager requires that this threshold be set to a higher level than the threshold that triggers automatic Snapshot copy deletion. This ensures that Snapshot copy autodeletion is triggered first. For more information, see “Automatic dismounting of Exchange databases” on page 363.

Step	Action
Apply the changes to the default or volume-specific policy	
8	To apply your changes and close the dialog box, click **OK**.

Managing the report directory options

Use the SnapManager Report Directory Setting dialog box to configure the location of the SnapManager report files. For more information, see any of the following topics.

- "Default report directory" on page 372
- "Reasons to change the report directory" on page 372
- "Accessing reports created in a previous directory" on page 373
- "Using the Report Directory Setting dialog box" on page 373

Related topics:

- Chapter 4, "Starting SnapManager for the First Time," on page 63
- Chapter 15, "Managing SnapManager Reports," on page 321

Default report directory

By default, the SnapManager reports are stored in a subdirectory named `Report` under the directory in which the SnapManager application is installed. If you installed SnapManager in its default installation directory, then the default report directory path is as follows:

```
C:\Program Files\NetApp\SnapManager for Exchange\Report
```

Reasons to change the report directory

Reasons for changing the location of the SnapManager report directory are described in the following paragraphs.

Limited space: If you find you have limited space in the current report directory, you can change the report directory to a different location that has more available disk space.

Clustered environment: If you are running Exchange and SnapManager in an MSCS cluster, storing the SnapManager reports in the default location (in a directory named `Report` under the SnapManager installation directory) would not allow the report directory to be shared between the nodes in the cluster. Furthermore, you would not see the same reports from different nodes.

To avoid these problems, you can move the report directory to a disk that belongs to the same group as your Exchange virtual server. This needs to be performed from every SnapManager node.

Accessing reports created in a previous directory

If you change the name or location of the SnapManager report directory, you cannot use the SnapManager Reports tab to view or print any reports that were created in that report directory.

However, assuming the previous report directory was not explicitly changed or removed, any reports created in that directory are still accessible. In order to view or print those older reports, you must change the report directory back to its previous location.

Using the Report Directory Setting dialog box

Use the Report Directory Setting dialog box to view and change the directory where your SnapManager reports are stored.

Step	Action	
1	From the SnapManager menu bar, select Options > Report Directory Setting. **Result:** The Report Directory dialog box appears and displays the current location of the report directory.	
2	Specify the new location for the report directory. **Attention** Do not use a disk that contains Exchange or SnapManager data for the report directory; it is restored from Snapshot copy when you perform a SnapManager Restore.	
	If...	**Then...**
	You know the full directory path name	Click in the Report Directory box and modify the path name.
	You prefer to browse to the new location	Click Browse to use a browse dialog box to select the new location.
3	To apply your changes and close the Report Directory Setting dialog box, click OK.	
4	To refresh the information displayed in the SnapManager Reports tab, go the SnapManager menu bar and select View > Refresh.	

Managing the event notification options

You can use either the Configuration Wizard or the Auto Notification Settings dialog box to enable and configure the SnapManager event notification services. See the following topics for more information:

- "About the SnapManager event notification options" on page 374
- "Using the Auto Notification Settings dialog box" on page 375

About the SnapManager event notification options

The following event notification options can be configured from either the Configuration Wizard or from the Auto Notification Settings dialog box.

SnapManager e-mail notification: SnapManager can notify you through e-mail (using SMTP) about the success or failure of the following types of events:

- SnapManager backup
- Database integrity verification
- SnapManager restore
- SnapManager configuration
- SnapManager fractional space reservation policy event execution

This option is disabled by default.

SnapManager syslog event logging: SnapManager events can be posted to the storage system syslog. This option is enabled by default.

AutoSupport notification: If AutoSupport is enabled on both the storage system and SnapManager, technical support receives automatic e-mail notification about any SnapManager events or storage system problems that might occur. This option is enabled by default.

The AutoSupport daemon monitors the storage system's operations and sends automatic messages to technical support to alert them to potential storage system problems. If necessary, technical support contacts you at the e-mail address that you specified to help resolve a potential system problem. The AutoSupport daemon is enabled by default on the storage system. For additional information, see the *System Administration Guide* for your version of Data ONTAP.

Limit AutoSupport notification to failure events: If AutoSupport is enabled on the storage system, you can limit the SnapManager events that are posted to the storage system syslog and AutoSupport (if enabled for SnapManager) to failure events only. The option to limit AutoSupport notification to failure events is enabled by default.

Using the Auto Notification Settings dialog box

To configure automatic event notification settings for SnapManager, complete the following steps.

Step	Action
1	From the SnapManager menu bar, select Options > Notification Settings. **Result:** The Auto Notification Settings dialog box appears. **Note** The Configuration Wizard presents the same options in the Configure Automatic Event Notification screen.
Configure E-mail Notification	
2	Optional. To enable e-mail notification, select the Send Email Notification option. By default, the automatic e-mail notification feature is disabled. **Note** SnapManager relies on and requires an external mail host at your site to send mail. The mail host is a host that runs a mail server that listens on the SMTP port (25).

Step	Action
3	In the four text boxes in the top half of the tab, enter the following information. **SMTP Server:** The host name or the IP address of the SMTP e-mail server or gateway to be used. **From:** The e-mail address of the sender of the notification. By default, the name `SMEAutoSender` is used. To specify a sender other than the default, use one of the following formats: ❖ *SenderAlias*<*SenderName@SenderDomain*.com> ❖ *SenderAlias* ❖ *SenderName@SenderDomain*.com **To:** The e-mail address of the recipient to whom the notification is to be sent. For more than one recipient, use a semicolon (;) to separate the addresses. **Subject:** The text to be appended to the following standard subject line, which is included in all notification messages: `Backup status at` *mm_dd_yyyy-hh.mm.ss* `from` *MachineName* By default, `SnapManager for Exchange` is used for the appended subject string.
4	Click Advanced. **Result:** The Advanced Event Notification Settings dialog box appears.
Configure Advanced E-mail Notification Settings	
5	In the Operation Type panel, select all of the SnapManager operation types for which you want e-mail notifications sent: ◆ Backup & Verification ◆ Restore ◆ Configuration

Step	Action
6	In the E-mail Message Content panel, select one of the following types of body messages to include in the body of the e-mail: ◆ Send operation results summary **Note** If you choose to send the operational results in summary format rather than in verbose format, you can also select the Include SnapManager Operation Report as an Attachment option. ◆ Send verbose operation results
7	Click Apply to commit your settings.
8	Click Advanced to open the Advanced E-mail Notifications Settings dialog box. To configure the SMTP mail notification settings, select either or both of the following two options: ◆ Only send notification when operation fails Specifies that you want e-mail notification sent only when a backup process or a verification process fails (off by default). ◆ Include SnapManager operation report as attachment Specifies that you want the status report to be attached to the e-mail notification (off by default).
9	Click OK to apply your settings and close the Advanced Email Notification Settings dialog box.
10	Click Send a Test Email. **Result:** SnapManager sends the e-mail notification, using the settings you specified, and displays a notification.
Configure Syslog Event Logging and AutoSupport	
11	If you want to enable posting of SnapManager events to the storage system syslog, select the Log SnapManager Events to Storage System Syslog option.
12	If SnapManager is configured to log events to the storage system syslog, you can also enable automatic notification about any SnapManager or storage system problems to technical support. To do this, select the Send AutoSupport Notification option.

Step	Action
13	If you want to limit SnapManager event logging to failure events, select the “On failure only” option.
14	Click OK. **Note** If you are using the Configuration Wizard instead of the Auto Notification Settings dialog box, click Next.

Glossary

backup set

A *SnapManager backup set*, often referred to as a backup set, is the complete set of data required to form a restorable backup or archive: all Exchange data Snapshot copies, all transaction log Snapshot copies, and the SnapInfo directory.

Exchange

In this guide, the term *Exchange* is used to describe Microsoft Exchange 2000 or Microsoft Exchange 2003. Information about a particular version of Exchange will be labeled with the Exchange version number or numbers.

Exchange environment

The Exchange organization and the supporting Windows server environment.

Exchange organization

The entire Exchange deployment (all of the Exchange servers).

file system

The native Windows file system supported by SnapManager using NTFS.

LUN (Logical Unit Number)

A logical unit of storage that can be managed by SnapDrive in a SAN environment. Within the Windows operating system, LUNs appear as locally attached disks. The terms “LUN” and “virtual disk” are synonymous; this document uses the term “LUN”.

SFSR

Single File Snap Restore. An SFSR reverts a single file to the version of that file contained in a particular Snapshot copy. After a file has been restored using SFSR, all user-visible information (data and file attributes) for that file in the active file system are identical to the state contained in the Snapshot copy. SnapManager uses SFSR to restore a LUN to its state when a SnapManager backup was taken.

Snapshot copy

An online, read-only copy of a volume. For more information about Snapshot copies, see “SnapManager and Snapshot copies” on page 10.

storage group

This Microsoft concept refers to a group of one to five databases (information stores) and an associated set of transaction log files, all of which are mounted on the same Exchange server.

storage group set

One or more Exchange storage groups that belong to the same Exchange server and are stored on the same storage system volume.

Storage groups in the same storage group set are displayed in the same color and are all automatically preselected when one is selected to be backed up.

storage system

Any NetAppstorage product that supports FCP (Fibre Channel Protocol) and iSCSI (SCSI over IP).

This guide refers to all NetApp storage products (filers, IBM N series storage systems, and NearStore systems) as storage systems. In other documentation, the terms *filer* and *appliance* have also been used to refer to storage systems.

virtual disk (LUN)

A logical unit of storage that can be managed by SnapDrive in a SAN environment. Within the Windows operating system, LUNs appear as locally attached disks.

volume

A logical unit of data storage on a storage system.

Windows Server environment

A group of Windows servers providing basic services such as Active Directory, DNS, DHCP, and so on. Sometimes also referred to as a *Windows environment*.

Index

Symbols

*__recent Snapshot copy names 144

A

Active/Active cluster disk requirements 43
Active/Passive cluster disk requirements 43
archiving
    about 300
    automatically 313
    backup sets, complete 300
    Exchange backups 311
    individual storage groups 302
    methods 303
    scheduling 302
    using dump 304
    using Exchange backups 311
    using for disaster recovery 226, 233
    using NDMP 304
    using NTBackup 308
    using Run Command After Operation 313
    using Windows backup utility 308
automatic
    backup deletion 151
    mirroring 217

B

backing up
    across LUNs 137
    across volumes 137
    Microsoft environment 227
    system resources 18
    using the Backup tab 167
    using the SnapManager Backup Wizard 165
backup management groups
    changing 182
    overview of 180
    using with SnapManager operations
        full database backup 151
backup sets
    about 141
    components of 141
    data organization of 141
    defined 300, 379
    guidelines for archiving 302
backup sets, SnapManager
    naming convention for 142
backup tools 13
backups
    Action menu deletion of 200
    automatic deletion of 151
    cluster failovers during 173
    deleting automatically 151
    deleting selected 209
    deleting with Action menu 200
    errors when deleting 211
    failovers during 173
    failure of some storage groups during 137
    failures, common 173
    guidelines for restoring 190
    initial 157
    minimum target 136
    move groups during 173
    other methods 13
    overview of 136
    restoring 190
    scheduling 158
    scheduling for archiving 302
    target, minimum 136
    tasks 136
    types of 13
    unique name option for 143
    verification status for 148
    volume-wide 137
    ways to access 164
    when additional preserved 152
before you install or upgrade 16
busy Snapshot copy error 211

C

calculating
    database volume size 104

deleted item cache size 100
single instance sharing ratio 98
transaction log volume size
volume size for multiple disks 106
clusters, Windows
creating and installing 44
creating with SnapManager installation 43
disk requirements for Active/Active 43
disk requirements for Active/Passive 43
Exchange configuration 72
move groups during backups of 173
report directory and 322
restoring 188
SnapManager installation in existing 46
command after operation
default setup 358
running 313
component properties 115
configuration
requirements, about 71
samples 87
Configuration Wizard
description of 6
moving databases using 126
moving transaction logs using 128
overview of 114
using 118
when to use 115
configuring 374
Exchange data store 118
notification settings 374

D

data
configuration plan, creating 94
configuration recommendations 76
configuration rules 74
configuration samples 87
management, supported by SnapManager 4
sizing requirements 93
Data ONTAP
storage system requirement 22
Data ONTAP VSS Hardware Provider 10
database icon colors 165, 167
database verification
throttling Eseutil 348
databases
backing up using Backup Wizard 165
moving with Configuration Wizard 126
per storage group 72
properties 115
remote verification of 148
restoring using Restore tab 194
restoring using Restore Wizard 193
sizing LUNs for 96
verification. *See* verification
DBCC
specifying settings 346
default run command setup 358
deferred
deletion 160
verification 146
deleted item cache, calculating size 100
deleted item retention 160
deleting
backups, automatically 151
backups, individual 209
backups, problems with 211
backups, selected 209
backups, using Action menu 200
reports 323
deletion, deferred 160
disaster recovery
components required 225
documentation about 224
from failed Exchange server 239
from failed storage system and Exchange server 244, 252
from failed storage system volume 238
methods to get data off site 226
preparing for 225
process choices 232
replicating environment 228
restoration guidelines for 231
restoring environment 230
SnapMirror 236
to replicated environment 252
using archives for 233
disk requirements

Active/Active cluster 43
Active/Passive cluster 43
disk size calculation
storage group 96
transaction logs 101
understanding 71
disks, virtual
See also LUNs
types of 380
drive letter limitations 80
`dump` command, storage system
archiving LUNs that contain SnapManager backup sets 4

E

`eloginfo__` SnapInfo Snapshot copies 138, 152, 300, 314
esefile
utility 145
eseutil
Exchange upgrades and 28
utility 145
`Eseutil.exe<DefaultParaFont>`
throttling for database verification 348
`EXCH__*` SnapInfo subdirectory names 142
Exchange
backing up server 227
backup types list 13
data store
configuration recommendations 76
configuration rules 74
configuring 118
database size calculation 96
database volume sizing 104
databases per storage group 72
files not backed up by SnapManager 14
logs, size calculation 101
number of storage groups 72
recovering failed server 239
recovering failed server for 2000/2003 239
recovery processes 230
Recovery Storage Group 72, 186
replicating environment 228
restoring environment 230
storage groups allowed 72
storage rules 74
transaction log volume sizing 105
versions supported 379
virtual servers 72
volume size calculation 106
Windows cluster configuration 72
Windows host system requirements 25
Exchange server
as a remote administration server
other requirements for 26
SnapDrive requirement for 25
verifying host system requirements 24
as a remote verification server
connectivity requirements for 28
verifying host system requirements 24
verifying host system requirements for 24
Exchange servere
as a remote verification server
other requirements for 27
Exchange Storage Manager 159
`exchsnap__` Snapshot copies 138, 152, 300, 314
`exchsnap__*` Snapshot copy names 143

F

failures on backup 137
FCP
LUN access protocol 22, 26
LUN driver 27
file system 379
files
Exchange, not backed up 14

G

guidelines
archiving 302
disaster recovery 231
restore 190

H

how you use SnapManager 7

I

installation directory, SnapManager
    specifying during interactive installation 36
    specifying during unattended installation 40
installation prerequisites 16
installation process
    in existing cluster 46
    preinstallation 16
    stand-alone system 31
    with cluster creation 43
installing SnapManager on a stand-alone system
    Windows host system requirements for 24
installing SnapManager on a standalone system
    in interactive mode 33
    in unattended mode 38
installing SnapManager on a Windows cluster
    Windows host system requirements for 24
interactive mode
    installing SnapManager 33
    uninstalling SnapManager 57
    upgrading SnapManager 51
IP address, setting preferred 22
iSCSI
    LUN access protocol 22, 26
    LUN driver 27

L

license requirements 22
    FCP protocol 22
    iSCSI protocol 22
    SnapMirror 22
    SnapRestore 22
licenses
    storage system requirements 22
    Windows host system requirements 26
licensing
    per server 19
    storage system 19
log files
    verification status for 149
Logical Unit Number. *See LUNs*
logs, Exchange. *See* transaction logs
LUN access protocol 22, 26
LUN driver 27
LUN size 71
LUN size calculation
    storage group 96
    transaction logs 101
LUNs
    backing up multiple 137
    See also virtual disks
    virtual disk type 379

M

management groups. *See* backup management groups
Microsoft environment, backing up 227
Microsoft Exchange
    message tracking 76
Microsoft Exchange. *See* Exchange
Microsoft Volume Shadow Copy Service. *See* VSS
minimum backup target 136
mirroring, automatic 217
MSCS. *See* clusters, Windows

N

NDMP-based backup utility
    archiving LUNs that contain SnapManager backup sets 4
new features 2
notification settings, configuring 374
NTBackup, using to back up system resources 18

O

operating system
    storage system requirements 22
    Windows host system requirements 24
overriding verification 354

P

page zeroing 160
partial backups 137
per server licensing 19
per storage system licensing 19
per-Exchange-server license 26
per-storage system license 26

point-in-time restores 185
preferred IP address, setting 22
preinstallation
    verifying storage system requirements 22
    verifying Windows host system requirements 24
preinstallation process 16
preupgrade process 16
printing reports 324
processes
    installation in existing cluster 46
    installation with cluster creation 43
    preinstallation 16
    restore 184
protocol
    FCP 22, 26
    iSCSI 22, 26
    NDMP 4

R

Recovery Storage Group 72, 186
recovery. *See* disaster recovery
remote administration server 24
    Microsoft Exchange requirement for 25
    other requirments for 26
    SnapDrive requirement for 25
remote administration system requirements 25, 26
remote verification 148
    server, designating 120, 342
remote verification server
    connectivity requirements for 28
    other requirements for 27
    system requirements 24
replicating Exchange environment 228
report directory
    changing 322
    managing in cluster 322
Report directory, SnapManager
    changing the location 373
    default location 372
    option to remove during uninstallation 58, 59
    remote access to 65, 338
reports
    contents of 322
    deleting 323
    printing 324
requirements
    configuration 71
    data sizing 93
    disk, for Active/Active cluster 43
    disk, for Active/Passive cluster 43
    licensing 22
    SnapMirror with SnapManager 215
    storage system 22
    Windows host system 24
restore
    guideline for disaster recovery 231
    See also SnapManager Restore
    Snapshot copies, deleting 205
    type to use 190
    ways to access 192
restoring
    backups, guidelines for 190
    databases
        using Restore tab 194
        using wizard 193
    Exchange environment 230
rolling Snapshot copies 219
`rstrsnap__` Snapshot copies 186
rules
    data configuration 74
    Exchange storage 74
Run Command After Operation
    about 313
    default command 358
    using 313
    variables 314
Run Command After Operation feature
    and generic backup naming (`__recent` suffix) 143
    configuring default values 358
    running a script from a UNC path 319

S

sample configurations 87
scheduling
    backups and verifications 158
    SnapMirror replication 219

server account, SnapManager
in workgroup mode 37, 40
server licensing 19
server-side license. *See* per-Exchange-server license
setting a preferred IP address 22
shadow copies 10
single instance sharing ratio, calculating 98
sizing
database volume 104
Exchange database 96
Exchange transaction logs 101
requirements for data 93
transaction log LUN 101
transaction log volume 105
volume for multiple disks 106
`SMEReportFolder` share 65, 338
SnapDrive
using for SnapMirror replication 220
using with SnapManager 9
when to use 9
Windows host system requirements 25
SnapInfo directory
description of 141
sizing LUN for 102
sizing LUNs for 101
SnapInfo directory, SnapManager
naming conventions for 142
SnapManager
about 4
application overview
command line interface 7
graphical user interface 6
what it does not do 5
where you install and run it 5
backup sets 141, 300, 379
naming convention for 142
block diagrams 8
component properties 115
configuration requirements, about 71
configuring 113
data management functions 4
files not backed up by 14
functions supported 4
how you use 7
installation in existing cluster 46
installation with cluster creation 43
installing or upgrading
option to remove Report directory during uninstall 58, 59
reinstalling 62
storage system requirements for 22
Windows host system requirements for 24
reports 321
SnapDrive, working with 9
stand-alone system installation 31
system overview 8
uninstalling 55
upgrading 48
using with other backup methods 13
variables 314
what it does 4
when to use 9
SnapManager Backup
Backup tab, using 167
command after 313
deferring verification of 146
deleting oldest Snapshot copies with 151
description of 6
initial backup with 157
minimum target 136
overview of 136
remote verification with 27
running command after 313
tasks 136
ways to access 164
what it does 136
when to back up your databases 157
Wizard 165
SnapManager in workgroup mode 37, 40
SnapManager Reports
Report directory
changing the location 373
default location 372
option to remove during uninstall 58, 59
SnapManager Restore
cluster group state during 188
description of 6
guidelines for 190
how it works 184

point-in-time restores 185
process 184
recovery from archives 233
Recovery Storage Group 186
Restore tab, using 194
restoring from archive with 238
restoring in cluster 188
See also restore
Snapshot copies created by 186
type to use 190
types 185
up-to-the-minute restores 185
using 183
ways to access 192
what it does 184
Wizard, using 193
SnapManager system requirements
storage system 22
Windows host system 24
SnapMirror
asynchronous mode 217
automatic mirroring 217
other documentation for 214
overview of 215
recovering Exchange data with 236
replication schedule 219
replication timing control 217
requirements with SnapManager 215
timing control 217
understanding 215
use by SnapManager 217
using for disaster recovery 226
using from within SnapManager 213
using SnapDrive for replication 220
SnapMirror replication of SnapManager backups
storage system license requrements 22
SnapRestore 22
Snapshot copies
about 10
backup Snapshot copies
automatically deleting the oldest 151
naming conventions 142
created by restore 186
creation methods, when to use 11
definition of 380
example 11
how SnapManager uses 10
limit 173
maximum allowed per volume 150
maximum number 12
naming conventions for 300
restore 186
rolling 219
stand-alone system 31
storage group icon colors 165, 167
storage group sets 136, 380
storage groups
archiving individual 302
calculating disk size for 96
definition of 380
maximum in database 72
properties 115
storage requirements 71
storage rules for Exchange 74
storage system
licenses 22
requirements for SnapManager 22
volumes 380
storage system-side license.
See per-storage system license
system requirements
remote administration 25, 26
system requirements for SnapManager
storage system 22
Windows host system 24
system resources, backing up 18

T

transaction logs
calculating disk size for 101
moving with Configuration Wizard 128
sizing LUNs for 101
volume size 105
types of Exchange backups 13

U

unattended mode
installing SnapManager 38
uninstalling SnapManager 59

upgrading SnapManager 52
uninstalling SnapManager 55
before you uninstall 55
in interactive mode 57
in unattended mode 59
option to remove Report directory 58, 59
unique name option for backups 143
upgrading SnapManager 48
in interactive mode 51
in unattended mode 52
Windows host system requirements for 24
up-to-the-minute restores
about 185
using SnapManager 7

V

variables, SnapManager 314
verification
deferred 146
designating remote server 120, 342
importance of 186
overriding 354
overview of 145
remote 148
running 176
scheduling 158, 176
status of backups 148
status of log files 149
utility 145
virtual disks
See also LUNs
types of 380
Volume Shadow Copy Service. *See* VSS
volume size calculation
multiple disks 106
transaction logs 105
understanding 71
volumes
backing up multiple 137
backups and 137
definition of 380
sizing for databases 104
sizing for transaction logs 105
VSS (Microsoft Volume Shadow Copy Service) 10
Hardware Provider requirement 10
how SnapManager uses 10
managing Snapshot copies with 10
vssadmin 10

W

what's new 2
Windows cluster
cluster group state during a restore 188
Windows clusters. *See* clusters, Windows
Windows host system requirements 24, 37, 40
Microsoft Exchange 25
operating system 24
SnapDrive 25
SnapManager licenses 26
Windows operating systems with SnapManager
Windows 2000 Server
Microsoft hotfixes 24
SnapManager requirements 24
Windows Server 2003
Microsoft hotfixes 24
running a script from a UNC path on 319
SnapManager requirements 24
Windows XP theme 68
Windows Server environment 380
Windows XP theme 68
wizards
Backup 165
Configuration 114
Restore 193
workgroup mode, Windows 37, 40

Z

zeroing, page 160