

SnapManager® 1.0 for Lotus® Domino Installation and System Administration Guide

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

Part number 215-02377
December 2002

Copyright and trademark information

Copyright information

Copyright © 1994—2003 Network Appliance, Inc. All rights reserved. Printed in the U.S.A.

No part of this book 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 and purchase of this product do 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 and the Network Appliance design are registered trademarks of Network Appliance, Inc. in the United States, Canada, and the European Union. Network Appliance is a registered trademark of Network Appliance, Inc. in Monaco and a trademark of Network Appliance, Inc. in the United States and Canada. FAServer is a registered trademark of Network Appliance, Inc. in the United States and the European Union. NetCache is a registered trademark of Network Appliance, Inc. in the European Union and Japan, and a trademark of Network Appliance, Inc. in the United States. SnapCopy is a registered trademark of Network Appliance, Inc. in the European Union and a trademark of Network Appliance, Inc. in the United States. WAFL is a registered trademark of Network Appliance, Inc. in the United States, the European Union, and Canada. FilerView, SecureShare, SnapManager, SnapMirror and SnapRestore are registered trademarks of Network Appliance, Inc. in the United States. Data ONTAP is a trademark of Network Appliance, Inc. in the United States and Canada. Snapshot is a trademark of Network Appliance, Inc. in the United States and the European Union. NetApp—the Network Appliance Company is a registered trademark of Network Appliance, Inc. in the United States and other countries. ApplianceWatch, BareMetal, Center-to-Edge, ContentDirector,

DataFabric, MultiStore, NearStore, SecureAdmin, Serving Data by Design, Smart SAN, SnapCache, SnapDrive, SnapVault, Vfiler, and Web Filer are trademarks of Network Appliance, Inc. in the United States.

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

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

Table of Contents

	Preface	i
Chapter 1	Understanding SnapManager	1
	SnapManager overview.	2
	Domino server configurations with SnapManager.	6
	How SnapManager works	11
	What SnapManager Configurator does	12
	What SnapManager Backup does	13
	What SnapManager Restore does	15
Chapter 2	Installing and Configuring SnapManager	17
	Preparing to install SnapManager	18
	Verifying system requirements.	20
	Backing up system resources.	22
	Assessing volume size	23
	Preparing to install SnapManager	25
	Installing SnapManager.	27
	Performing the basic installation process	28
	Installing SnapManager on a Domino cluster	32
	Migrating Domino servers using SnapManager	33
	Configuring E-mail, Syslog, and Autosupport notification	39
	Uninstalling and reinstalling SnapManager	40
	SnapManager command-line interface	41
Chapter 3	Backing Up Domino Data Directories	43
	Using SnapManager Backup	44
	Deleting snapshots	46
	Use of SnapManager Backup with other types of backup	47
Chapter 4	Restoring with SnapManager Restore	49
	SnapManager Restore tasks	50
	Guidelines for restoring SnapManager backups	51

	SnapManager Restore options	53
Chapter 5	Archiving to Other Types of Media	55
	About archiving.	56
	Archiving snapshots to offline media.	58
Chapter 6	Recovery from Archive	61
	Supporting documentation	62
	Understanding disaster recovery	63
	Preparing to recover using snapshots from archived media	64
	Restoring the Data directory from archived media	65
	Recovery scenarios	66
	Using backup archives to restore a failed filer volume	67
	Failure of both the filer and the Domino server	68
Chapter 7	SnapManager Reports	69
	What SnapManager reports contain	70
	Index	73

Preface

About this guide This guide describes how to install SnapManager® for Lotus® Domino and use its online backup and restore features. This guide does not explain how to migrate, backup, and restore Domino servers. For this information, you must see the *SnapManager for Lotus Domino Online Help*.

This guide does not explain how to install, configure, and use the SnapDrive™ features that enable you to create and connect to virtual disks, which you must do before you use SnapManager. For this information and details about how to configure filer volumes and enable filer access, see the *SnapDrive 2.0 Installation and Administration Guide*.

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 who possess a working knowledge of Lotus Domino and Windows® 2000. The discussion assumes familiarity with the following topics:

- ◆ Lotus Domino server administration
- ◆ Lotus Notes administration
- ◆ Network functions and operations
- ◆ Basic concepts for moving data over a network
- ◆ Your operating system, network, and Network Appliance™ storage appliance, such as a filer
- ◆ NFS and CIFS protocols, as used for file sharing and file transfers

Is this the right guide for you? Use the following table to determine which documents to read.

If you are...	Read...
Installing filers in an Ethernet environment	The document <i>Data ONTAP™ Product Documentation</i> , which is delivered with the filer.
Installing filers in a Fibre Channel environment	The document <i>Data ONTAP 6.3 SAN System Administrator's Guide</i> , which is delivered with the filer.

If you are...	Read...
Installing SnapManager on a Windows 2000 system that is connected to a filer and you plan to use Fibre Channel Protocol (FCP) as the protocol for your virtual disk	This document. <i>The NetApp Fibre Channel Protocol HBA on Windows Installation and Setup Guide 1.0.</i> If SnapDrive is not already installed, read the following guides in this order before you install it: ◆ <i>The NetApp Fibre Channel Protocol HBA on Windows Installation and Setup Guide 1.0.</i> ◆ <i>The SnapDrive 2.0 Installation and Administration Guide.</i>
Installing SnapManager in a Windows 2000 system that is connected to a filer and you plan to use VLD as the protocol for your virtual disk	This document. If SnapDrive is not already installed, read the <i>SnapDrive 2.0 Installation and Administration Guide</i> first.

Typographic conventions

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

Convention	Type of information
<i>Italic type</i>	Words or characters that require special attention. Placeholders for information you must supply. For example, if the guide says to enter the <code>arp -d hostname</code> command, you enter the characters “arp -d” followed by the actual name of the host. Book titles in cross-references.
Monospaced font	Command and daemon names. Information displayed on the system console or other computer monitors. The contents of files.

Convention	Type of information
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.

Terminology

This guide uses the following terminology:

- ◆ *Database Instance ID (DBIID)* is a value that is located in the database header and that associates the database with specific entries in the transaction log.
- ◆ *Domino Data directory* refers to the directory on the Domino server that houses all the Domino databases. Each Domino server or partition server has a Data directory.
- ◆ *File system* refers to the native Windows 2000 file system supported by SnapManager using NTFS.
- ◆ *Filer* refers to all NetApp® storage appliances.
- ◆ *notes.ini* file is a settings file that includes setup selections, the default server ID, the default user ID, Name and Address books, and most program runtime variables the Domino server and Lotus Notes Client. The location of the Domino Data directory is specified in the *notes.ini* file.
- ◆ *Partitioned server* is a single computer configured to run an unlimited number of instances of the Domino server program. Using partitioned servers reduces hardware expenses and minimizes server administration. Each partitioned server picks up its own *notes.ini* location from the Domino server.
- ◆ *Volume* refers to a functional unit of storage exported from a filer. A single filer volume might store multiple virtual disks belonging to different Lotus Domino servers.
- ◆ *Virtual Disk* is a SnapDrive component that enables filers to interface with the Windows 2000 operating system. There are two types of virtual disks:
 - ❖ *Virtualized Local Disk (VLD)* refers to a specific file corresponding to a specific volume on a filer managed by SnapDrive in an Ethernet environment. Within the Windows 2000 operating system environment, a VLD appears as if it were a locally attached disk.
 - ❖ *Logical Unit Number (LUN)* refers to a storage target device created by SnapDrive that resides in a storage target (filer) in a Fibre Channel environment. Within the Windows 2000 operating system, the LUN appears as if it were a local disk.

SnapManager® for Lotus® Domino enables you to use multiple virtual disks (VLDs or LUNs) in the same filer volume.

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.

Caution

A caution contains instructions that keep you from damaging equipment, crashing your system, or losing data.

About this chapter This chapter explains how SnapManager® for Lotus® Domino works.

Topics in this chapter This chapter discusses the following topics:

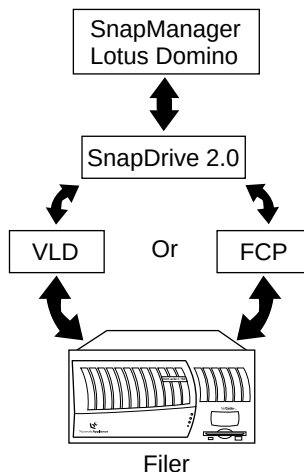
- ◆ “SnapManager overview” on page 2
- ◆ “How SnapManager works” on page 11

SnapManager overview

What SnapManager does

SnapManager is the data management tool that integrates Network Appliance SnapDrive 2.0 technology to provide a data management solution for Lotus Domino databases. It dramatically boosts the availability, scalability, and reliability of Domino servers. SnapManager provides near-instantaneous hot backup and rapid restoration of Domino servers by building on the online Snapshot™ technology from Network Appliance.

The following figure illustrates the relationship between Network Appliance filers, SnapDrive 2.0, and SnapManager for Lotus Domino.



How SnapManager and SnapDrive work together

The SnapDrive software integrates with the Microsoft® NTFS Volume Manager to enable use of filers as virtual disks for data storage in the Windows 2000 environment. SnapDrive provides the underlying layer of support for SnapManager. As such, it is transparent to the SnapManager application.

When to use SnapManager: When both SnapDrive and SnapManager are installed on your server, you must use SnapManager for all snapshots and related operations. For example, you use SnapManager to establish your Domino Data directory on virtual disks on a filer and to back up and restore virtual disks on the filer. In this case, SnapDrive is used to create, connect, and expand the virtual disk that hosts the Domino server.

If you do not use SnapManager to migrate your Domino Data directory and transaction logs to virtual disks and then back them up, the correct information required by SnapManager is not available to restore the Data directory.

When to use SnapDrive: SnapDrive manages virtual disks on a filer, making these disks available as ordinary local disks on the Windows 2000 host server. This allows the server to interact with the virtual disks as if they were directly attached, physical disks. You can use SnapDrive to create and manage virtual disks—to create and change the size of virtual disks and to connect and disconnect virtual disks. For information about how to perform these tasks using SnapDrive, see the *SnapDrive 2.0 Installation and Administration Guide*.

SnapManager modules

SnapManager consists of the following modules:

Domino server add-in: The server add-in module is deployed on the same physical machine as the Domino server. The server module uses the Domino server API for add-ins. The server module is responsible for managing all backup and restore activity.

Client interface: The client interface is the user interface portion of SnapManager for Lotus Domino. The client interface enables you to manage and schedule snapshots and restores against a properly configured Domino server. The client interface communicates with the server on a Windows 2000 socket, which uses a TCP/IP protocol. This enables you to manage and schedule snapshots and restores from any machine that has a network connection to the server.

How SnapManager works with other backup methods

Because backups reside on disk instead of tape, SnapManager technology should be employed as a complement to conventional backup processes.

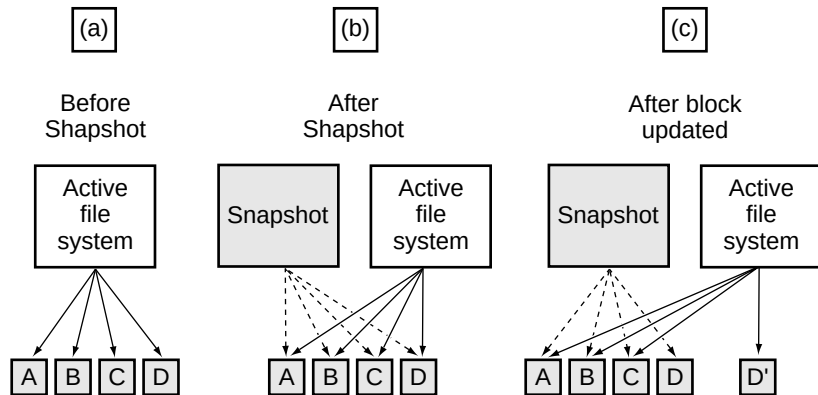
SnapManager backups are not intended to replace periodic disaster recovery measures. NDMP or Dump are the most efficient methods for creating archives of the virtual disk drive files.

How SnapManager works with snapshots used as backups

A snapshot is a point-in-time, read-only copy of a Domino Data directory stored on a filer volume. SnapManager Backup uses snapshot functionality to create real-time, online, read-only copies of the Domino Data directory. Snapshots enable you to restore your Domino Data directory rapidly if you encounter data corruption or other problems.

The following figure provides an example of how snapshots work.

How Snapshots work



Example: Suppose you take a snapshot of a file named file.txt that spans four disk blocks in the active file system. Initially, the snapshot 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 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. 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, plus the one new block. The snapshot 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; deleting file.txt from the active file system does not free any disk space until the snapshot is deleted.

How SnapManager safeguards data

Under SnapManager, the Domino Data directory and transaction logs reside on a virtual disk created on the filer and formatted with the New Technology File System (NTFS). The virtual disk can be either a Virtualized Local Disk (VLD), or a Logical Unit Number (LUN), which uses Fibre Channel Protocol (FCP). A VLD is used to store data on a filer in an Ethernet environment. A LUN is a storage target device in a Fibre Channel environment.

To the filer, a virtual disk is one big file. Filers use battery-protected nonvolatile RAM (NVRAM) to protect incoming file system I/O operations. The contents of NVRAM are flushed to disk at regular intervals—more frequently if the NVRAM fills up, even during periods of inactivity. This ensures that the file system is always in a consistent state. The filer’s WAFL® file system guarantees that the contents of NVRAM are always written to disk, even during a power failure.

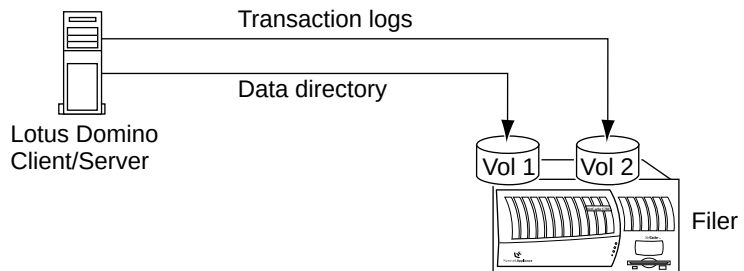
Domino server configurations with SnapManager

Domino server configurations

The illustrations in this section show the various ways you can place the data on your Domino server on filer volumes.

Single Domino server and multiple filer volumes

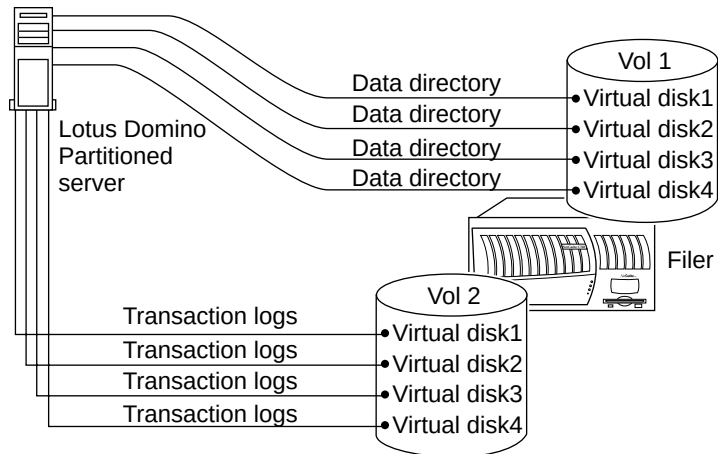
The following figure shows an example configuration of a Domino server and filer volumes created for the Data directory and transaction logs.



Each server's Data directory on separate filer volume.
Each server's transaction logs on separate filer volume.

Domino partitioned servers and one filer volume

The following illustration shows multiple Domino partition servers with virtual disks contained on the same volume.

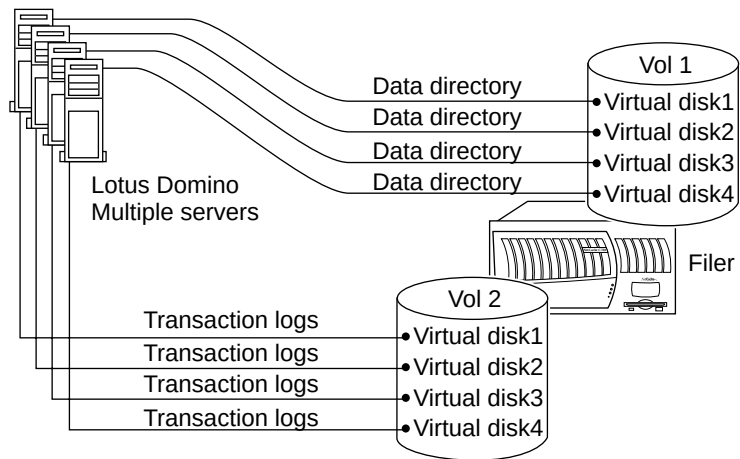


Each partition server's Data directory on a separate virtual disk within the same filer volume.

Each partition server's transaction logs on a separate virtual disk within the same filer volume.

Multiple Domino servers and two filer volumes

The following illustration shows multiple Domino servers with virtual disks contained on the same volume.

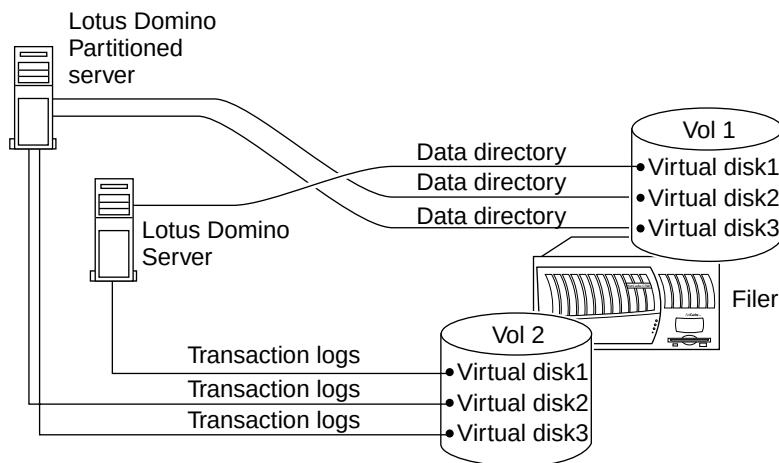


Each server's Data directory on a separate virtual disk within the same filer volume.

Each server's transaction logs on a separate virtual disk within the same filer volume.

Domino partitioned server in a mixed environment with a single Domino server

The following illustration shows a Domino partitioned server with virtual disks contained on the same volume as the virtual disks of a single Domino server.

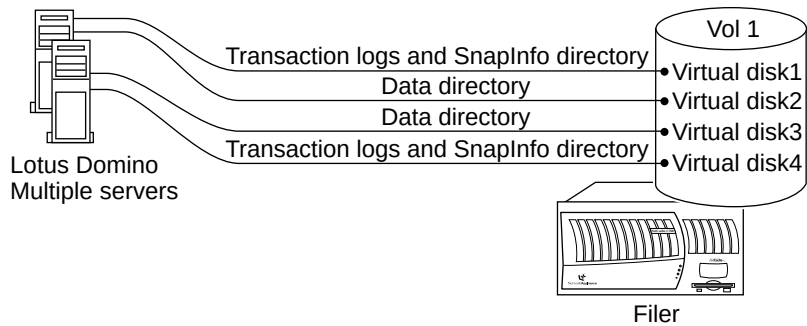


Example of a single server's Data directory residing on a Virtual disk within the same filer volume as the virtual disk of a partitioned server.

Example of a single server's Transaction logs residing on a Virtual disk within the same filer volume as the Virtual disk of a partitioned server.

Multiple Domino servers on the same filer volume

The following figure shows a filer volume containing virtual disks containing the Data directories of multiple servers residing on the same filer volume as the virtual disks for the transaction logs and their corresponding SnapInfo subdirectories.



Each server's Data directory and transaction logs on different virtual disks within the same volume.

How SnapManager works

SnapManager components

SnapManager enables you to migrate your Domino Data directory and transaction logs and move them to virtual disks on a filer volume. You use SnapManager Configurator for this purpose. After you migrate your Domino server's data to virtual disks, you can use the SnapManager Backup and Restore features to back up snapshots of the Domino Data directory and transaction logs.

For details about virtual disks, see the *SnapDrive 2.0 Installation and Administration Guide*.

This section describes the following components:

- ◆ SnapManager Configurator
- ◆ SnapManager Backup
- ◆ SnapManager Restore

For detailed information

For details about how each of the SnapManager components work, see the following topics:

- ◆ “What SnapManager Configurator does” on page 12
- ◆ “What SnapManager Backup does” on page 13
- ◆ “What SnapManager Restore does” on page 15

What SnapManager Configurator does

How the SnapManager Configurator works

SnapManager Configurator is a wizard-based component of SnapManager that moves your Domino Data directory and transaction log files to the virtual disks you configured with SnapDrive.

SnapManager Configurator copies the Domino Data directory and transaction logs so that they are placed in the correct location for proper functionality of the SnapManager Backup and Restore processes. The SnapManager Configurator can migrate data in the following ways:

- ◆ From local disk to virtual disk
- ◆ From CIFS shares to virtual disk

Note

Before you migrate your Domino server to virtual disks, you must make sure that your Domino server is down. When you migrate your Domino server Data directories and transaction logs to virtual disk, you must restart your Domino server in order to complete the migration process.

Rules for storing Domino Data directory and transaction log files

Adhere to the following rules for storing the Data directory and transaction log files:

Note

These rules are enforced by SnapManager Configurator.

- ◆ Each server must have its own virtual disk for storing the Domino Data directory.
- ◆ Domino transaction logs and SnapInfo directory cannot reside on the same virtual disks as their corresponding Data directory.
You must store Domino Data directory and transaction log files on separate virtual disks; this enables SnapManager Restore to use the filer's SnapRestore™ feature.
- ◆ A single filer volume can store multiple virtual disks from various Domino servers.
- ◆ Do not install system files on filer volumes containing your virtual disks used for your Domino Data directory or transaction logs.

What SnapManager Backup does

Functions it performs

SnapManager Backup performs a full online backup of the Domino server's Data directory and transaction logs. SnapManager Backup uses snapshot functionality to create real-time, online, read-only copies of the Domino Data directory. After the Data directory is safely backed up, SnapManager archives the available transaction log files to the SnapInfo directory.

In the context of SnapManager Backup, each volume is viewed as a discrete entity. Although backups are performed at the Data directory level (all databases in a server are backed up at once)—the entire content of the volume, including all its virtual disks, is captured in the snapshot.

How it works

When using SnapManager Backup, snapshots are prefaced by placing the Domino server in backup mode. This is initiated with a call to the Domino backup API. After a backup is initiated, a snapshot of the virtual disk that the data resides on is issued. While the backup progresses, pre-snapshot images are accumulated for each Data directory and archived along with the snapshot to restore the snapshot properly.

Using SnapManager Backup, you can back up the Data directory and transaction logs belonging to a Domino server at once. They are then placed together as one data set on their respective, separate virtual disks. For each Domino server, the backup includes the databases in the Domino Data directory, the transaction logs, and SnapInfo files belonging to the Data directory.

Data directory backups

When you select a Domino Data directory for backup, all databases composing the Data directory are automatically selected for backup.

Data organization in SnapManager backup sets

The SnapInfo subdirectory contains the information about each backup set created by SnapManager Backup. A subdirectory under the SnapInfo directory is created for each backup set. Each backup-set subdirectory contains the transaction logs backed up as part of that snapshot as well as the recovery information for that specific snapshot.

Every time a SnapManager backup is created, a new backup-set subdirectory is created under the SnapInfo directory and is populated with the appropriate information and data. A complete backup set consists of this SnapInfo subdirectory and the corresponding snapshot of the virtual disk drives that store the Domino Data directory and transaction logs. The SnapInfo subdirectories can reside on the same virtual disk as the transaction log files, but not on the same virtual disk with the Domino Data directory.

What SnapManager Restore does

How it works

SnapManager Restore restores the Domino server’s selected snapshot. The entire virtual disk containing the selected Domino server’s Data directory and transaction logs is restored from the backup.

What happens when you perform a SnapManager Restore

When you perform a SnapManager Restore, the following events occur in sequential order:

Stage	Process
1	SnapManager restores the Data directory residing in the chosen snapshot to the active file system.
2	The transaction logs are restored from snapshot.
3	The archived logs are copied back into the transaction log directory.
4	The Domino server needs to be restarted.
5	If you are doing an Up-to-the-Minute Restore, the transaction logs are played forward.

Types of restore

SnapManager Restore provides the following types of restore:

- ◆ Up-to-the-minute—In this type of restore, all the transaction logs are played forward into the restored Data directory. 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.
- ◆ Point-in-time—In this type of restore, only the transaction logs that existed at the time the selected snapshot was created are played forward into the restored database because you are restoring to the instant the backup was taken.

After a point-in-time restore is executed, all previously existing snapshots are not available for up-to-the-minute restores. You can use these existing

snapshots for point-in-time restores only. New snapshots will be available for up-to-the-minute restores.

About this chapter This chapter provides information you need to install SnapManager for Domino. It also explains how to configure SnapManager after you install it.

Topics in this chapter This chapter discusses the following topics:

- ◆ “Preparing to install SnapManager” on page 18
- ◆ “Installing SnapManager” on page 27
- ◆ “Migrating Domino servers using SnapManager” on page 33
- ◆ “Configuring E-mail, Syslog, and Autosupport notification” on page 39
- ◆ “Uninstalling and reinstalling SnapManager” on page 40
- ◆ “SnapManager command-line interface” on page 41

Preparing to install SnapManager

Before you install SnapManager

Installing and configuring SnapManager are the final steps you take in the process that includes tasks to safeguard your current system resources and prepare your hardware and software for SnapManager. Before you begin installing SnapManager, ensure that you complete these prerequisite tasks.

For SnapManager to function properly, you must complete the stages of this process in the following order.

Step	Action
1	Verify your system requirements. For details, see “Verifying system requirements” on page 20.
2	Back up system resources. For details, see “Backing up system resources” on page 22.
3	Assess your volume space requirements. For details about how to evaluate your space requirements, see the <i>SnapDrive 2.0 Installation and Administration Guide</i> .
4	Configure your filer. For details, see the <i>SnapDrive 2.0 Installation and Administration Guide</i> .
5	Configure your Windows 2000 system. For details, see the Microsoft documentation.
6	If an earlier version of SnapDrive prior to SnapDrive 2.0 is installed on the system, remove (uninstall) the software from the system before you install the new software: For details about removing SnapDrive, see the <i>SnapDrive 2.0 Installation and Administration Guide</i> .

Step	Action
7	Install SnapDrive 2.0. SnapDrive is installed before SnapManager. Caution_____ Do not begin the SnapManager installation process unless you installed SnapDrive and already created two or more dedicated virtual disks to hold the Domino Data directory, transaction log files, and SnapInfo directory. The SnapInfo directory and the transaction log files can be housed on the same virtual disk. _____ Note_____ For remote administration using SnapManager, you do not need to install SnapDrive on the remote machine. See “SnapManager remote administration” on page 26 for details. _____ For details, see the <i>SnapDrive 2.0 Installation and Administration Guide</i>.

For detailed information

For details about resource requirements, safeguards, and prerequisite tasks, see the following sections:

- ◆ “Verifying system requirements” on page 20
- ◆ “Backing up system resources” on page 22
- ◆ “Assessing volume size” on page 23
- ◆ “Preparing to install SnapManager” on page 25

Verifying system requirements

System requirements

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

Host system requirements	Description
SnapDrive 2.0	The host system used to run SnapManager for Domino must meet the SnapDrive 2.0 hardware and software system requirements. See the <i>SnapDrive 2.0 Installation and Administration Guide</i> for complete details about the following system requirements: ◆ operating system ◆ hardware platform ◆ network For information about remote administration systems that do not require SnapDrive, see “SnapManager remote administration” on page 26.
Operating system	One of the following operating systems is required: ◆ Windows 2000 Server with Service Pack 2 or Service Pack 3 ◆ Windows 2000 Advanced Server with Service Pack 2 or Service Pack 3 It is recommended that Post-SP2 hot fix 306185 be applied to machines running SnapDrive on Windows 2000 with Service Pack 2 applied. Read the Microsoft Q article 306185 at http://www.microsoft.com for information about the required registry change for this hot fix. The registry change must also be applied for Windows 2000 Service Pack 3.
Lotus Domino server	SnapManager for Lotus Domino supports Lotus Domino 5.0.11.

Requirements for a remote administration

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

- ◆ SnapManager must be installed.

Note

You need to install, but not configure, SnapManager. Use the same account you use for access from the production server for the account to be used for access to the filer.

- ◆ Lotus Notes must be installed on the remote system.
- ◆ The appropriate virtual disk driver must be installed.

Caution

Do not try to connect the Domino server's virtual disks to the remote verification server.

Things to remember: If, for some reason, you have trouble setting up your remote administration server, check the following:

- ◆ The DNS server is consistent. If the DNS server is not consistent, try using the server's IP address in place of the remote server's hostname.
- ◆ Make sure that the Domino server services have started on the remote server.

Filer license requirements

The following requirements must be met in order to run SnapManager.

- ◆ The filer must have either the VLD or FCP license enabled, depending on which protocol you are using for your virtual disks.
- ◆ SnapRestore™ must be licensed on the filer.

Account requirements

To run SnapManager, the SnapManager user account that the SnapManager service runs under must have administrative access on the Domino server. This is usually addressed by making the user a member of the administrator's group. For convenience, this account can be the same one that SnapDrive runs under.

Note

A filer administrator must perform and verify the configuration.

Backing up system resources

Backing up system resources

Before you install SnapManager, Network Appliance strongly recommends that you back up your system resources using your current backup tool or another industry standard backup utility.

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

Step	Action
1	Back up the operating system installation on the Domino server, including the system state.
2	Back up your Domino data, transaction log files, notes.ini file, and server ID.
3	Back up the boot and system drives, and the registry.
4	Use an industry standard backup tool to create and maintain a current emergency repair disk (ERD).

Assessing volume size

SnapDrive storage requirements

In addition to the space required for your virtual disks, SnapDrive requires space to store data that has changed between snapshots and the active file system of the virtual disk. It also requires space to store metadata. Allowing for this additional space ensures that taking multiple snapshots does not encroach on the virtual disk files in the volume.

When you create filer volumes to hold virtual disks, you must take into account the following SnapDrive requirements:

- ◆ To create snapshots, the volume storing the virtual disk must be at least twice the size of that virtual disk.

By extension, a filer volume must have at least twice the capacity of all the virtual disks it contains.

- ◆ The volume must have enough free space for the number of snapshots you intend to keep online.

In sizing volumes, take into account how many day's worth of snapshots will be online at the same time.

The first snapshot lock uses disk space equal to the virtual disk file size itself (thus, double the requirement). Additional snapshots add to this.

Virtual disk size calculations for the Data directory

To ensure that you create volumes to meet these SnapDrive requirements, you must calculate the potential size of your virtual disks. The following formula works best to calculate Domino Data directory size for a Domino mail server:

$$\text{Data directory size} = (\text{mail files} * \text{mailbox quota}) * 2 + \text{deleted item cache} + \text{NAB (Name and Address Book)}$$

Example: Given these requirements, the following parameters can be expressed by the formula shown after them:

- ◆ 1,000 users with 100 MB quotas for mail files
- ◆ Double the space for the first snapshot
- ◆ The deleted item cache is 10%

$$(((1000 * 100 \text{ MB}) * 2) * 1.10) = \text{about } 220 \text{ GB} + \text{NAB}$$

SnapManager storage requirements for transaction logs

SnapManager Backup backs up transaction logs that were not committed to the Domino Data directory at the time of the backup. It also saves copies of the transaction logs committed to the Data directory to be purged from the active file system during the backup. The number of logs that accumulates between backups vary from server to server, but is dependent on the amount of transactions and E-mails sent and received. Each Domino transaction log consumes 64 MB of space.

Estimating the amount of space required for transaction logs

You can determine how much disk space is required for your Domino Data directory transaction logs by first estimating the number of transaction logs that are generated on your server.

To estimate how many transaction logs are generated, note the number of transaction logs that accumulate in the transaction log directory immediately before a backup. Use that number to estimate how much disk space you need. (You should do this over a period of several days and use the maximum number).

The following formula works best for calculating virtual disk size required for a transaction log drive:

virtual disk size = ((number of transaction logs generated per day * 64 MB) * (number of snapshots to keep online + 1 for the active file system))

Example: Given the following parameters, at least 6 GB of virtual disk drive is required to accommodate the transaction logs for the example Domino databases. This is expressed by the formula following the parameters:

- ◆ The server generates 5 transaction logs in one day.
- ◆ Each transaction log is 64 MB.
- ◆ There is about 1 GB of transaction logs at the end of the day.
- ◆ The plan is to keep five days' of SnapManager backups online at the same time.

$((5 * 64 \text{ MB}) * (5+1)) = 1920 \text{ MB}$ or about 1.2 GB

Preparing to install SnapManager

Preparing to install SnapManager

SnapManager requirements

Before you install SnapManager on your Windows 2000 server, you must complete the following tasks.

Task	Process	
1	If...	Then...
	You plan to run SnapManager for Domino locally	Continue with Step 2.
	You plan to run SnapManager for Domino remotely	Read “SnapManager remote administration” on page 26 and determine your installation requirements. Then install the required software.
2	If...	Then...
	You plan to use SnapManager for Domino, and SnapDrive is not already installed	You must install SnapDrive. See the <i>SnapDrive 2.0 Installation and Administration Guide</i> for details about configuring the filer for SnapDrive (and SnapManager) and installing and configuring SnapDrive.
	You plan to use SnapManager for Domino, and SnapDrive is already installed	Follow the instructions in “Installing the SnapManager software” on page 28.

Task	Process
3	Make sure that you understand all the installation and configuration steps needed to make SnapManager work in your particular environment. Read one of the following sections, before you continue with the process: ◆ “Installing the SnapManager software” on page 28 ◆ “Installing SnapManager on a Domino cluster” on page 32

Domino server configuration

Prior to installing SnapManager for Domino, your Domino server must archived logging enabled. Circular logging is not supported in SnapManager for Domino and should be disabled. If you disable transaction logging on the Domino server and the change is not recognized by Domino, try restarting the server until circular logging is disabled.

SnapManager remote administration

You can configure a system for remote administration of the Domino server running SnapManager. In this case, you do not need to install SnapDrive (or a VLD driver or an HBA driver) on the remote machine. You can only use SnapManager remote administration for taking snapshots and performing restores. You cannot use SnapDrive remote administration for configuring SnapManager.

Note

When using SnapManager for Domino in a remote administration environment, you must install Lotus Notes on your remote system, otherwise you will be unable to remotely administer SnapManager for Domino.

Installing SnapManager

About this section This section discusses how to install SnapManager depending on your configuration. Although the overall installation processes you follow differ for each of the configurations (installing in a cluster, installing on a single server), the steps you complete to install the SnapManager software are the same in all cases. For this reason, this section describes the set of installation steps once; each of the three configuration processes refers to that set of steps.

Topics in this section This section describes the following processes.

Installation section	When to use
“Performing the basic installation process” on page 28	If you want to install SnapManager on a single (as opposed to a Domino cluster) system. In this case, both of the following conditions must be true: ◆ Your Domino server is <i>not</i> clustered; ◆ You are <i>not</i> in the process of creating a cluster to run Domino and SnapManager.
“Installing SnapManager on a Domino cluster” on page 32	If you want to install SnapManager on a Domino cluster.

Performing the basic installation process

About this section

This section explains how to install and configure SnapManager on a single system. Follow the instructions in this section if both of the following are true:

- ◆ Your Domino server is *not* clustered
- ◆ You are *not* in the process of creating a cluster to run Domino and SnapManager

Installing the SnapManager software

To install SnapManager, complete the following steps.

Step	Action	
1	Install the software from CD-ROM or download it. Caution _____ Network Appliance recommends that you not use Terminal Services for any type of SnapManager administration because you might miss critical information. _____	
2	If...	Then...
	You are obtaining the software from the network	Download the SnapManager package and save it on the Domino server. Then, launch the SnapManager installation package by browsing to the location of the Setup.exe file, and double-clicking it. Result: The InstallShield Wizard Welcome screen appears.
2	You are installing the software from CD-ROM	Browse to the location of the SnapManager installation package and double-click Setup.exe. Result: The InstallShield Wizard Welcome screen appears.

Step	Action						
3	Click Next. Result: The License Agreement window appears.						
4	Read the License Agreement. If you accept the agreement, click the “I accept....” radio button, then click Next. Result: The Customer Information window appears.						
5	In the Customer Information window, enter ◆ Your user name, in the User Name field ◆ The name of your company or organization, in the Organization field ◆ Who you are installing SnapManager for (your personal use, or anyone who uses the local machine).  Result: The Setup window appears.						
6	In the Setup window, decide whether you want a custom or complete installation of SnapManager. <table><tr><th>If...</th><th>Then...</th></tr><tr><td>You choose a complete install</td><td>Select the Complete Install button and continue to Step 8.</td></tr><tr><td>You choose a custom install</td><td>Select the Custom Install button and continue to Step 7.</td></tr></table>	If...	Then...	You choose a complete install	Select the Complete Install button and continue to Step 8.	You choose a custom install	Select the Custom Install button and continue to Step 7.
If...	Then...						
You choose a complete install	Select the Complete Install button and continue to Step 8.						
You choose a custom install	Select the Custom Install button and continue to Step 7.						

Step	Action
7	In the Custom Setup window, select the client installation and verify that the directory listed for the location of the installation is correct, then click Next. Continue to Step 9. Note— The Custom Setup is traditionally used for remote administration, where you would only want to install the Domino client, but you could also install the Domino client and server for a local configuration.
8	Accept the default location for the files shown in the Destination Folder window. Make a note of the location of the installation.
9	Click the Install button if you are satisfied with your previous specifications. Otherwise, click Back to review or change them. Result: After you click Install, the program proceeds with the installation. After the installation program is completed, the InstallShield Wizard Completed window appears.
10	Click Finish to exit the InstallShield Wizard.
11	To begin configuring SnapManager, see “Migrating Domino servers using SnapManager” on page 33 for details. To migrate the Data directories of multiple partition servers using SnapManager, see the <i>SnapManager® for Lotus® Domino Online Help</i>.

Installing SnapManager on Domino partitioned servers

When you configure Lotus Domino you have the option to configure multiple partition servers. If you choose to configure multiple Domino partitioned servers running on the same Windows 2000 server, you only have to install one instance of SnapManager for Domino. See the procedure “Installing the SnapManager software” on page 28 for instructions about how to install SnapManager.

When installing SnapManager on multiple partition servers, adhere to the following rules:

- ◆ You must create a virtual disk for each Data directory on each partitioned server.
- ◆ You must create a virtual disk for the transaction logs on each partitioned server.
- ◆ You can create a virtual disk for the SnapInfo directory for the partitioned servers, but you may also place your SnapInfo directory on the same virtual disk as the transaction log files.

Installing SnapManager on a Domino cluster

About this section This section explains how to install SnapManager on a Domino cluster. Because Domino clustering uses real-time replication across all nodes, it is not necessary to install SnapManager on every node of your cluster.

If SnapManager is installed on node 1 of your cluster, and node 1 goes down, it is recommended that you have SnapManager installed on another node in your cluster for data management. After node 1 is brought back up and the rest of your nodes replicate data back to node 1, you can once again use node 1 as your primary data management node.

Considerations when installing SnapManager on a cluster

When installing SnapManager on a Domino cluster, consider the following:

- ◆ SnapManager for Domino supports a six node Domino cluster.
- ◆ Install SnapManager for Domino on at least two nodes of your cluster.
- ◆ Lotus Domino runs in Active + Active mode only.
- ◆ Lotus Domino clustering uses instantaneous replication of nodes.

Installing SnapManager on a cluster

To install SnapManager into a Domino cluster, complete the following steps.

Step	Action
1	Install SnapManager on node 1. See “Installing the SnapManager software” on page 28 for directions.
2	Migrate your Lotus Domino Data directory using SnapManager Configurator Wizard. See the <i>SnapManager for Lotus Domino Online Help</i> for details.
3	Install SnapManager on the second node of your choosing. Caution ————— Do not migrate the Data directory using the second node. The Data directory has already been migrated to virtual disks.

Migrating Domino servers using SnapManager

Migrating your data

This section discusses how to migrate your data from your Domino servers to virtual disk. This section also explains how to move your data back to your Domino server should the need arise to do so.

Requirements to configure SnapManager with a Domino server

To migrate your Domino server information to virtual disks, consider the following requirements:

- ◆ Before you can migrate Domino server, you must use SnapDrive to create the following virtual disks:
 - ❖ One virtual disk for the Domino Data directory
 - ❖ For each Domino Data directory, one virtual disk for the transactions logs and SnapInfo directory
- ◆ You must run the SnapManager Configurator wizard before SnapManager Backup.
- ◆ You must not store anything (including system paging files) on the virtual disks used for the Domino Data directory and transaction logs except what the Configurator puts there.
- ◆ You must not rename the shortcut directory on partitioned servers because when you migrate your Data directory, the shortcut does not recognize the new location even though the migration was successful.
- ◆ Before migrating your Data directories and transaction logs to virtual disks using the Configurator, the logdir field in the server document on the Domino server must have the full path name identified, not the default logdir folder that Domino admin client places there. This is critical because the log directories cannot be migrated when only the relative path is placed in the logdir field of the server document.

Migrating databases to virtual disks using SnapManager

To migrate your Domino databases to virtual disks, complete the following steps.

Note

Any time you use SnapManager Configurator to move data from one drive to another, backups taken prior to the move become invalid. After you migrate to a new virtual disk, take an immediate snapshot.

Step	Action
1	In the Windows 2000 user interface, choose Start > Programs > SnapManager for Domino. Caution _____ Run SnapManager from the system console, not from a Terminal Services client. Network Appliance recommends that you not use Terminal Services for any type of SnapManager administration as you may miss critical information contained in pop-up dialog boxes that might not appear. Result: The SnapManager for Lotus Domino Welcome screen appears.
2	Select the Configurator Wizard button.
3	At the Configurator Wizard Welcome screen, click Next.
4	In the Where to Move Databases screen, select the Domino Data directory you want to migrate to a virtual disk.
5	From the virtual disk list, select the virtual disk to which you want to move your Domino Data directory, click the move (<=>) button, and then click Next. Result: The Where to move transaction logs screen appears.
6	In the Where to Move Transaction Logs screen, select the transaction log files you want to move and the virtual disk to which you want to move them to, click the <=> button, and then click Next. Result: The Where to put SnapInfo files screen appears.
7	In the Where to put SnapInfo files screen, type in or browse to the virtual disk drive letter you want your SnapInfo files to be moved to. Note _____ The virtual disk you use for your SnapInfo file can also be the same virtual disk you use for your transaction logs. Result: The Configurator displays a summary of the configuration.

Step	Action
8	If the configuration summary is satisfactory, click Finish to display a list of tasks the Configurator performs, based on the configuration information you specified.
9	Click Start Now to migrate your databases, their logs, and the SnapInfo files to the virtual disks you specified.
10	After the migration is complete, restart your Domino server to make sure that the migration was successful.
11	Back up your database immediately. Note _____ Any time you use SnapManager Configurator to move data from one drive to another, backups taken prior to the move become invalid. After you migrate to a new virtual disk, take an immediate snapshot.

Migrating databases back to local disk

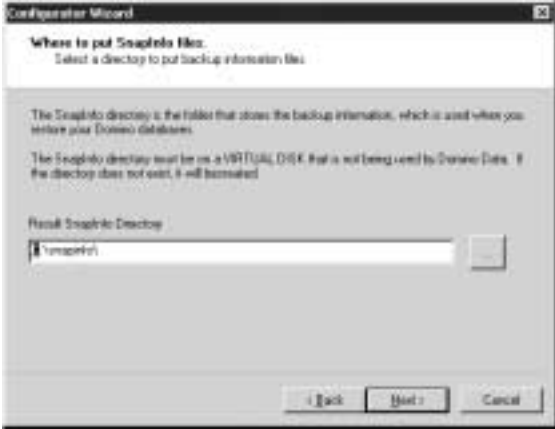
If, for any reason, you choose not to use SnapManager as your data management tool, you need to migrate your databases back to local disk.

To migrate your databases back to local disk, complete the following steps.

Step	Action
1	In the Windows 2000 interface, choose Start > Run.
2	At the dialog box, type regedit.
3	In the regedit file, navigate to the Lotus Domino directory.

Step	Action
4	In the right window pane, look for network paths other than paths pointing to local disk. For example: Your local drive letter is C: and you want to move all of your data off virtual disk and your local disk. Edit all instances of virtual drive letters to the local drive letter. Change: D:\Lotus\Domino\Data to: C:\Lotus\Domino\Data
5	After you finish with the Domino directory, navigate to the 5.0 directory under the Domino directory.
6	Look for network paths other than paths pointing to local disk and edit them to point to local disk.
7	Close regedit.
8	Launch the Domino server.
9	Launch Lotus Notes from the Program menu.
10	In Lotus Notes, open the Address Book.
11	Select File > Databases > Open.
12	In the Open Database dialog box, from the pull-down menu, choose the server to which you want to migrate your databases.
13	After you choose your server, select your server's address book and click Open.
14	After your address book opens, double-click the server highlighted in the right-hand window of the Address Book window.
15	In the upper left-hand corner of the window, select Edit Server.
16	Click the Transaction Logging tab.

Step	Action
17	Change the drive letter of the log path from the virtual disk drive letter to the drive letter of the local drive. 
18	Click Save and Close.
19	Exit Lotus Notes.
20	Quit from the Domino server.
21	From Windows Explorer, navigate to the Domino directory and open the notes.ini file.
22	Manually change all drive letters listed in the notes.ini file to the local drive letter, then save and close the file. Note If you have multiple partitioned servers, you must modify multiple notes.ini files in order for the migration from virtual disk back to local disk to take place.
23	Open SnapManager for Lotus Domino
24	Click the Configurator Button.

Step	Action
25	Click Next until you arrive at the Where to Put SnapInfo files window. 
26	Change the drive letter of the Result SnapInfo Directory back to the drive letter of the local disk, and then click Next.
27	Click Finish and then Start Now.
28	Once the migration is complete, exit out of SnapManager for Domino.
29	Relaunch the Domino server.
30	At the prompt, enter the following command: <pre>show server</pre> This verifies that the changes took effect.

Configuring E-mail, Syslog, and Autosupport notification

Enabling Autosupport notification on your filer

To enable Autosupport notification on your filer, you must set up the notification through the SnapDrive add-in Windows 2000 Management Console. This will set up filer Autosupport for your virtual disks.

SnapDrive enables you to set up e-mail notification and enable filer auto support in the event of a SnapDrive message or filer error. When you set up notification settings, you can specify the following information:

- ◆ Whether or not to send e-mail notification, and where to send it
- ◆ What types of messages to report
- ◆ Whether to allow a subset of events to be posted to the filer's autosupport.

Note

The Autosupport daemon monitors the filer's operations and sends automatic messages to Network Appliance Technical Support to alert technical support to potential filer problems. If necessary, Network Appliance 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 filer. For additional information, see the *Data ONTAP 6.3 SAN System Administrator's Guide*.

To use SnapDrive to enable Autosupport for your virtual disks, see the *SnapDrive 2.0 Installation and Administration Guide*.

Uninstalling and reinstalling SnapManager

Uninstalling SnapManager

To uninstall SnapManager and all its components, complete the following steps.

Step	Description
1	Make sure that your Domino server and your Notes client are not running.
1	Use SnapManager to move your Data directory and transaction logs from the virtual disks onto a local disk. See the <i>SnapManager for Lotus Domino Online Help</i> for more information.
2	Disconnect your virtual disks. See the <i>SnapDrive 2.0 Installation and Administration Guide</i> for details.
3	In the Windows 2000 Control Panel, click Add/Remove Programs, and choose SnapManager for Domino. If you are removing a previous version of SnapManager, select it from the Control Panel.
4	Click Remove.
5	After you remove SnapManager for Domino from your computer, click Close.

Reinstalling SnapManager for Domino

To reinstall SnapManager for Domino, you do not need to remove the existing copy of the same version of the program, if it is already installed. In this case, the InstallShield Wizard enables you to choose to remove or repair the existing software.

SnapManager command-line interface

Operations you can perform from the command-line interface

SnapManager contains the command-line interface, `smd.exe`, for automating SnapManager operations. You can use the `smd.exe` utility to automate the following operations:

- ◆ Backup
- ◆ Restore
- ◆ Point-in-time restore
- ◆ Delete

Note

You cannot use the SnapManager command-line interface for remote administration.

Commands for automated operations

To use the automated operations, you must first open a command-line prompt on your Windows system and navigate to the directory where SnapManager is installed. You can use the following parameters in conjunction with the `smd.exe` command.

- ◆ The `<Pn>` parameter indicates the number of the partition server or serve on which you want to perform the operation.
- ◆ The `<N>` parameter indicates a numerical value, either the number of snapshots, or a particular server number.
- ◆ The `<del>` parameter can only be used with the backup command and a number must be specified for the number of backups to delete in excess of.
- ◆ The `<--p>` parameter can only be used for point-in-time restores.

The following table lists the automated operations, their functionality, and their command-line syntax.

Operation
- -backup creates a new snapshot. smd - -backup=[<P1>] Example: smd - -backup=1 takes a snapshot of either partition server 1 or a single server. Note You can use <n> for more than one partitioned server by differentiating partition servers with a colon. For example, 1:2:3, where 1:2:3 are partitioned servers 1, 2, and 3.
- -del deletes an existing snapshot. smd - -backup=<Pn> - -del=<N> Example: smd - -backup=1 - -del=3 deletes all backups on partition server 1 in excess of 3.
- -restore restores an existing snapshot. smd - -restore=<Pn> - -snapshot=<N> Example: smd - -restore=1 - -snapshot=1 restores the most recent backup for a single Domino server.
- -restore restores an existing snapshot. smd - -restore=<Pn> - -snapshot=<N> Example: smd - -restore=2 - -snapshot=3 restores the most recent backup for the partition server 2.
- -p restores an existing snapshot to a Point-in-Time restore. smd - -restore=<n> - -snapshot=<n> - -p Example: smd - -restore=1 - -snapshot=3 - -p executes a point-in-time restore for partition server 1 or a single server.

About this chapter This chapter describes how to back up the Domino Data directory with SnapManager Backup. For information about how SnapManager Backup works, see “What SnapManager Backup does” on page 13.

Topics in this chapter This chapter discusses the following topics:

- ◆ “Using SnapManager Backup” on page 44
- ◆ “Deleting snapshots” on page 46
- ◆ “Use of SnapManager Backup with other types of backup” on page 47

Using SnapManager Backup

Ways to access SnapManager Backup

You can access SnapManager Backup in two ways:

- ◆ From the SnapManager Backup Wizard in the SnapManager interface
- ◆ From the SnapManager Backup tab in the SnapManager interface

Requirements for running SnapManager Backup

To run SnapManager Backup

- ◆ You must have administrator rights on the Domino server.
- ◆ You must have administrator rights on the filer.

Caution

In some instances of Domino server 5.0.11, you might get a notice that nlogasio.exe is launched in a DOS console window reporting Transaction Logging messages similar to the following:

“Found archived extent ##### to rename, not in active array.”
and/or

“Could not find available archived extent.”

When this error is generated new extents are being created and archived ones are not being reused. Closing the window might result in a server crash.

This console does not affect the server as long as the window is open. Closing the DOS window can place the server in a hang condition.

- ◆ SnapManager online backups should not be scheduled during the same time as a scheduled Domino compact (ncompact.exe). Databases that are being compacted cause the online backup process to fail. Please check your Domino server's program documents, and the notes.ini to ensure that both events do not occur at the same time.

Backing up the Data directory for the first time

At the end of the Data directory and transaction log migration process, SnapManager prompts you to restart your Domino server to commit the changes in the migration path to your Domino server. Network Appliance recommends that you take an immediate snapshot of the Domino Data directory after you verify that the migration was successful.

Managing the snapshot limit during backups

The maximum number of snapshots you can keep online is 31. SnapManager Backup fails if you already saved 31 snapshots of the Data directory on disk (that is, if you have completed 31 SnapManager Backups and does not remove any of the resulting snapshots). Snapshots not created by SnapManager also factor into the snapshot count.

You can specify the number of snapshots to retain using the “Delete Oldest Snapshots in Excess Of #” field. When the “Delete Oldest Snapshots in Excess Of #” field is enabled, SnapManager Backup deletes older snapshots that exceed the number you want to preserve.

Note

If you reach the snapshot limit of 31 on the filer volume, there is no way to delete the snapshot through SnapManager. In this case only, delete the snapshot either through the filer console or using SnapDrive.

Note

In an online Domino environment, snapshots should only be taken using the SnapManager application. Taking snapshots from the filer console or SnapDrive is not supported and results in an inconsistent snapshot image of the online Data directory and transaction logs. However, you can use SnapDrive or the filer console to take snapshots of Domino Data directory and transaction logs that are offline.

Frequency of backups

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

Deleting snapshots

How to delete a snapshot

Network Appliance recommends that you manage the number of snapshots stored using automatic snapshot deletion.

You can manage the number of snapshots stored and delete older snapshots automatically using the “Delete Oldest Snapshots in Excess Of” feature in the SnapManager Backup window.

Management of snapshots using automatic deletion

When you use the SnapManager Backup feature to immediately back up a Data directory or schedule a Data directory for backup at a later time, you can also specify the number of snapshots of the backup to be retained.

To do so, you use the Delete Oldest Snapshots in Excess Of field. When the Delete Oldest Snapshots in Excess Of field is enabled, SnapManager Backup deletes older snapshots that exceed the number you specify. It deletes only snapshots that have the prefix “dominosnap” (on the Data directory volume).

SnapManager deletes the oldest snapshot only after it backs up the Data directory in the backup set that satisfies the criteria for triggering deletion—that is, the data set whose snapshot addition exceeds the maximum number. This type of deletion occurs automatically after you configure the option. This method of snapshot deletion is the recommended one.

Use of SnapManager Backup with other types of backup

Guidelines for integrating SnapManager Backup

The following guidelines help you integrate SnapManager Backup with other types of backup:

- ◆ Do not mix SnapManager backups with backups performed by other third-party Domino applications. Disable other backup programs, such as the Windows Backup Agent. After you implement SnapManager, use only SnapManager Backup for backups.
- ◆ Continue to create offline archives. Always archive the most recent snapshot. The latest snapshot is specially named: it is always called *DominoSnap__Win2Kservername__Dominoserver_Recent*, where *Dominoservername* is the name of the Domino server.
- ◆ Always include the SnapInfo directory that correlates to the backup set you are archiving as part of the archive.

Archived media creation and retrieval

For details about creating archives, see “Archiving to Other Types of Media” on page 55. For details about restoring archived Data directories, see “Preparing to recover using snapshots from archived media” on page 64.

About this chapter This chapter describes how to recover data from a SnapManager backup set with SnapManager Restore.

Topics in this chapter This chapter discusses the following topics:

- ◆ “SnapManager Restore tasks” on page 50
- ◆ “Guidelines for restoring SnapManager backups” on page 51
- ◆ “SnapManager Restore options” on page 53

SnapManager Restore tasks

Restore tasks you can perform

You can use SnapManager Restore to do the following tasks:

- ◆ Restore the Data directory from a SnapManager backup set in either of the following ways (see “SnapManager Restore options” on page 53):
 - ❖ A point-in-time restore
 - ❖ An up-to-the-minute restore
- ◆ Perform a restore from archive

Checklist when preparing to restore

Before a SnapManager Restore can take place, you must manually shut down Domino server.

Before performing any of the restore operations, check all the following:

- ◆ Make sure that all Explorer windows are closed on the Domino server where SnapManager is running.
- ◆ If you are running Domino partitioned servers and you want to do a restore on one partition, you must shut down all partitions prior to implementing the restore.
- ◆ If you want to do a restore to the primary node on a Domino cluster, you must shut down that node prior to implementing the restore.

Guidelines for restoring SnapManager backups

Guidelines before restoring snapshots

Follow these general guidelines before you restore a SnapManager backup set:

Caution

Do not perform a SnapManager Restore with your Domino servers running. Performing a restore with your Domino servers running causes database corruption.

- ◆ Before you implement any restore process, take a snapshot of the file system you are restoring. That way, in the unlikely event that something catastrophic happens during a restore, you have a recent snapshot of the file system prior to the restore.
- ◆ If you want to roll forward all the transactions up to the most current time, use an up-to-the-minute restore.

Note

If you do anything to change a Database Instance ID (DBIID), you need to take an immediate backup after you change the DBIID, or you cannot do an up-to-the-minute restore. This is because when you change a DBIID for any reason, the corresponding transaction log IDs are not updated unless you take an immediate snapshot of the Data directory. For example, running `compact -j` would be a scenario where the DBIID changes.

- ◆ If you want to recover the Data directory as it was at a particular point in time, for example the point in time when the most recent backup was created, use a point-in-time restore.
- ◆ If you are recovering a snapshot from an offline archive, you can only do a point-in-time restore. That is, you can recover the Data directory only to the state it was in at the time the backup set was created.

For example, if you created a backup set a week ago, archived it to tape last night, and restored it this morning, the Domino Data directory after the restore this morning is in the same state it was in a week ago. For additional information, see “Archiving to Other Types of Media” on page 55.

Guidelines when restoring a snapshot

When you use SnapManager to restore a virtual disk on a volume containing multiple virtual disks, SnapManager does not rename the snapshot of that volume used for the backup after it performs the restore. Also, it does not rename the related SnapInfo directory.

If you use SnapManager to restore a backup that is not the most recent one, that backup's sequential backup sets are still available for future restore.

SnapManager Restore uses the Domino recovery process to play forward transaction logs into the restored Data directory. Before allowing a restore operation to proceed, SnapManager checks that the selected backup set was verified through the use of Domino APIs. (See "Data organization in SnapManager backup sets" on page 13.)

Follow these guidelines when restoring a SnapManager backup set:

- ◆ Store the Domino Data directory on a separate virtual disk from the one storing the Data directory.
This method of storage brings the disk back to the state it was in at the time the snapshot was taken.
- ◆ You should always restore from the most recent snapshot, *DominoSnap__Win2Kservername__Domino server_Recent*, where *Domino server* is the host name of the Domino server.
- ◆ If you renamed the Domino database since the backup was made, you cannot recover it from a backup taken before the database was renamed.
 - ❖ If you rename a database, make sure that you back it up as soon as possible.
 - ❖ If you must recover a database from a backup taken before the database was renamed, rename the database back to its old name, then recover it from the backup.
 - ❖ If you use a snapshot that is not the most recent snapshot to do a point-in-time restore, all snapshots taken prior to the one you restored become point-in-time restorable only.

SnapManager Restore options

SnapManager Restore operating conditions

You can use SnapManager Restore if SnapRestore is licensed on the filer that contains your virtual disks.

SnapManager Restore options

You can use SnapManager Restore to do either of the following types of restore:

- ◆ An up-to-the-minute restore (recommended)
- ◆ 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 Data directory, from the time the backup set was created up to the most current time, are played forward and applied to the Data directory.

For example, if you run SnapManager Backup every lunchtime, and on Wednesday at 4 p.m. you decide to restore the backup set from Tuesday lunchtime, SnapManager Restore restores that backup set. Then, all the transaction logs are played forward and applied to the restored Data directory, 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.

Note

For an up-to-the-minute restore to work, all the archived transaction logs that are needed must be in the SnapInfo subdirectory, which is taken care of by SnapManager. SnapManager archives the transaction logs in the SnapInfo folder at the time of backup. Network Appliance does not recommend that you perform an up-to-the-minute restore with a snapshot that is not the most recent snapshot because the archived transaction log files would not be consistent with the transaction logs in the active file system.

Note

If you do anything to change a DBIID, you need to take an immediate backup after you change the DBIID, or you cannot do an up-to-the-minute restore. This is because when you change a DBIID for any reason, the corresponding transaction log IDs are not updated unless you take an immediate snapshot of the Data directory. For example, running `compact -j` is a scenario where the DBIID changes.

Point-in-time restore: In this type of restore, no transaction logs are played forward because you restored to the instant the backup was taken.

After a point-in-time restore is executed, all existing snapshots are not restorable for up-to-the-minute restores. You can use these existing snapshots for point-in-time restores only. New backups will be available for up-to-the-minute restores.

You can use this method to restore the Data directory up to a snapshot where you think corruption occurred.

After a point-in-time restore of a snapshot that is not the most recent one, all backup sets prior to the chosen backup set become point-in-time restorable only.

About this chapter

This chapter provides guidelines and direction explaining how to create archives of snapshots containing the Domino Data directory backed up by SnapManager for archiving to some other type of media.

Topics in this chapter

This chapter discusses the following topic:

- ◆ “About archiving” on page 56
- ◆ “Archiving snapshots to offline media” on page 58

About archiving

About archiving SnapManager backup sets

SnapManager Backup sets consist of three components—the snapshots of the virtual disk drives that store the Domino Data directory, the snapshot of the transaction log files, and the SnapInfo subdirectory that is created as part of the backup operation. You must create an archive of all these components together.

Due to the potential size difference between the SnapInfo directory and the virtual disk that it resides on, it might be more efficient to back up only the SnapInfo directory directly from the Domino server rather than backing up the entire virtual disk from the filer.

If you use the filer's dump command or NDMP, do the following:

- ◆ Take a snapshot of the virtual disks that you do not plan to archive immediately prior to archiving.
- ◆ Back up the virtual disk file corresponding to the drive letter where the SnapInfo directory is located as well as the virtual disk files associated with the drive letters that correspond to the Data directory and transaction logs.

Guidelines for archiving

Follow these guidelines when creating archives:

- ◆ Create an archive of the most recent backup set: Domino server Data directory, transaction logs, and SnapInfo directory.

The most recent snapshot in the filer's virtual disk drive volume that stores the Domino Data directory is always named */dominosnap_win2kservername_Dominoservername_recent*, where *Dominoservername* is the name of the Domino server from which the snapshot was taken.

Follow these guidelines about how to create the archive:

- ◆ Backup files must have the following absolute path names when using the NDMP or Dump-based archive method:
/vol/virtual_disk_volume_name/snapshot/virtual_disk_filename/snapshot_name/virtual_disk_filename/virtual_disk_volume_name is the name of the volume on which the database resides.
snapshot_name is the name of snapshot you want to archive. It should be *Dominoservername__recent*.
- ◆ Backup files must have the following absolute path names when using the CIFS-based archive method:

To back up a virtual disk file directly from the filer, use the following path:

`\\filename\sharename\~snapshot\snapshot_name\
virtual_disk_filename`

filename is the filer's host name.

sharename is the name that was used to share the volume. (This can be any name, not necessarily the volume name, which is suggested as a convenience.)

~snapshot

snapshotname is the name of the snapshot.

virtual_disk_filename is the name of the file (such as *file.vld* or *file.lun*).

Using archive media for disaster recovery

The combination of SnapManager for Domino and archives of SnapManager backup sets using media such as the NetApp NearStore™ product provide a solid disaster recovery solution for Domino information store data. (A complete disaster recovery backup strategy must also include system level backups of the Domino server.)

Problems using tape as the archive media

Proper scheduling of SnapManager Backup requires consideration of the archive media solution's backup speed. Scheduling conflicts can occur if tape is used as the archive media. The best strategy for SnapManager and tape archive schedules is to consider the tape backup strategy required to meet Service Level Agreements, the desired total number of SnapManager backups per day, and Domino client activity schedule. Then devise a schedule that does not encroach on the time necessary to complete tape archive.

Archiving snapshots to offline media

Archiving Manager backups

Offline archiving of virtual disks to archive media, such as NearStore technology or other media, is a good way to protect and retain data by using an alternate storage method. It is a good practice to back up snapshots to offline media kept in offsite storage for use in disaster recovery.

A backup consists of the snapshots of the virtual disk drives that store the data files. NDMP or Dump are the most efficient methods for creating archives of the virtual disk drive files.

Backing up the virtual disk file

Using any popular Windows backup software package or the dump command on the filer, back up the virtual disk file itself from a snapshot.

It is important to back up a virtual disk file that is in a snapshot that was created by SnapManager. Because virtual disks from multiple hosts can be stored on the same filer volume, only virtual disks that belong to the host that created the SnapManager snapshot are consistent. All virtual disks within that snapshot that belong to other hosts are not consistent. For this reason, it is recommended that you dedicate your filer volumes to individual hosts.

As part of the snapshot process, the file system (NTFS) is flushed to disk and the disk image in the snapshot is in a consistent state. This cannot be ensured if the snapshot was created outside the control of SnapManager (that is, at the filer console, using SnapDrive, or using the FilerView® interface, or rsh), or if the virtual disk file in the active file system is backed up.

Restoring archived VLDs

Restore the virtual disk file from your archive media to the active file system. After the file is restored, use the SnapDrive management interface to connect to the virtual disk file using its original drive letter. For more information about how to perform a recovery from offline archive, see your backup application software documentation or the *Data ONTAP 6.3 Data Protection Guide* if you are using the dump or NDMP command.

Restoring archived LUNs

If you are using the NDMP or dump command, or the CIFS option, restoring LUN-type virtual disk files is identical to restoring VLD-type virtual disk files. Where the process might differ is if the LUN environment is leveraging FC-AL-based backups. For more information about LUN backups, see the *Data ONTAP 6.3 SAN System Administrator's Guide*.

About this chapter This chapter discusses how you can restore Domino Data directories from their archived snapshots.

Topics in this chapter This chapter discusses the following topics:

- ◆ “Supporting documentation” on page 62
- ◆ “Understanding disaster recovery” on page 63
- ◆ “Preparing to recover using snapshots from archived media” on page 64
- ◆ “Restoring the Data directory from archived media” on page 65
- ◆ “Recovery scenarios” on page 66

Supporting documentation

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 virtual disks, see the *SnapDrive 2.0 Installation and Administration Guide*.
- ◆ For information about your specific version of Data ONTAP, see the appropriate *Data ONTAP System Administrator's Guide*.
- ◆ For detailed information describing how to prepare for loss of a Domino environment in the event of disaster, see the documentation entitled, *Administering the Domino System Volumes 1 and 2* published by Lotus at www.lotus.com.
- ◆ This document also describes how to reconstruct the environment after the disaster.
- ◆ Microsoft Windows 2000 documentation

Understanding disaster recovery

Domino environment recovery processes

Recovery from catastrophic loss of a Lotus Domino environment that integrates use of the SnapManager for Lotus Domino software and filers can be divided into the following two main processes:

- ◆ Recovering the Lotus Domino server
- ◆ Recovering the Lotus Domino Data directory

SnapManager backs up the Domino Data directory (and not the Domino server).

Preparing for disaster recovery

Preparing for disaster ahead of time is key to recovering from it. The first steps to recovery from catastrophic failure of a Domino database or filer should take place long before the event occurs.

Every environment and site is unique and every company has different requirements, depending on the critical nature of the data stored. Taking these differences into account, consider the following general disaster recovery preparation recommendations:

This guideline holds true for archived data. The archive media, such as a NearStore system, should be located off site.

- ◆ Establish a policy of redundant knowledge by ensuring that more than one person knows how to restore the system. This protects against delayed system recovery.
- ◆ Keep detailed records and logs of changes in printed or other forms of hardcopy.

SnapManager for Lotus Domino, the Domino server, and the filers are dependent on the Microsoft Windows 2000 environment. Before SnapManager can be used, the Windows 2000 environment must be restored. Therefore, it is important that you back up your Microsoft environment so that you can restore to the same state as part of the recovery process:

- ◆ Back up your Domino server.
- ◆ Back up your Windows operating system and any applications running concurrent with the Domino server.

Preparing to recover using snapshots from archived media

Components of SnapManager backup sets

SnapManager backup sets consist of the snapshots of the virtual disks that store the Domino Data directory, transaction log files, and SnapInfo directory that is created as part of the backup operation. All of these components must be archived for you to successfully recover and implement a point-in-time restore.

Type of restore available

Any restore from archive is a point-in-time restore. That is, the Data directory can be recovered only up to the point at which the backup set was created. A point-in-time restore does not include current transactions, so data loss will be incurred. For example, if you created a backup set a week ago, archived it to tape last night, and restored it this morning from archive, the Domino Data directory after the restore this morning are in the same state they were in a week ago.

Rules and guidelines for restoring

Before you restore a database from an archive, make sure that you understand the following:

- ◆ The virtual disk files from the archive must be restored into the active file system of the filer's volume.
- ◆ The drive letter assigned to the virtual disk that is restored must be the same drive letter that was used when the archive was created. For additional information, see "Guidelines for archiving" on page 56.
- ◆ The transaction logs files that you restore from archive can be located on its own virtual disk or on the same virtual disk as the SnapInfo directory.
- ◆ You cannot recover a virtual disk or transaction logs files into a read-only file system, such as a snapshot.

Restoring the Data directory from archived media

Restoring an archived Data directory

To restore the Domino Data directory and its corresponding transaction logs from an archive of a SnapManager backup set, complete the following steps.

Step	Action
1	Identify and locate the archived backup set that you want to restore. The backup consists of the virtual disk that stores the Domino Data directory for the Domino server to be restored and its corresponding transaction logs files.
2	Shut down the Domino server (or partitioned server) to be restored to local disk.
3	Note the virtual disk letter belonging to the Data directory to be restored from archive.
4	If there is sufficient space on the filer volume, use SnapDrive to manually create a snapshot of the virtual disk to be restored from archive.
5	To restore the virtual disk from archive to its original location on the filer, delete all of the files within the virtual disk. Note _____ You can use the Windows Explore navigational window to delete these files. _____
6	Restore the information on the archived virtual disk on the filer to the existing virtual disk.
7	Start your Domino server.
8	Perform an immediate SnapManager backup.

Recovery scenarios

What the scenarios cover

The first two scenarios in this section pertain to recovery of a Domino Data directory stored on a filer. The third and fourth scenarios include recovery of the Domino server, in addition to the Domino Data directory.

These processes do not address a large-scale disaster in which supporting Windows infrastructure is damaged or lost. Before attempting recovery of the Domino server or the filer, you must recover the supporting infrastructure.

For detailed information

Steps for the following recovery scenarios are explained:

- ◆ “Using backup archives to restore a failed filer volume” on page 67
- ◆ “Failure of both the filer and the Domino server” on page 68

Using backup archives to restore a failed filer volume

About recovery of a filer volume from archives

This scenario explains how to recover virtual disks from a failed filer volume or a failed filer using archived SnapManager backups. Keep in mind that this process performs a point-in-time restore. Any data written to the volume between the time that the most recent (archived) backup was taken and the time of failure is lost.

Recovering a filer volume from archives

To recover a failed filer volume using backup archives, complete the following steps.

Step	Action
1	Ensure that the filer is online and available. See the <i>Data ONTAP System Administrator's Guide</i> for information.
2	Prepare the archive media and the backup application so that they are ready to be used for the recovery.
3	Perform the procedure for archive recovery described in “Restoring the Data directory from archived media” on page 65.
4	Confirm operation of the Domino server.

Failure of both the filer and the Domino server

About recovery of both a failed filer and Domino server

If both the filer and the Domino server fail, in most cases you should recover the filer first so that the data—or the space to recover the data—is available.

Successful recovery of the Domino server depends on the existence of the following components:

- ◆ Recent, usable backups of the Domino server
- ◆ Archives of the SnapManager backup sets containing all the virtual disk files.

Note

For detailed information describing how to prepare for loss of a Domino environment in the event of disaster, see, *Administering the Domino System Volumes 1 and 2*, published by Lotus at www.lotus.com.

Recovering both a failed filer and Domino serve

To recover both the filer and the Domino server, complete the following steps.

Step	Action
1	Recover the filer and bring it online. See the <i>Data ONTAP System Administrator's Guide</i> and the Data Protection Guide for your version of Data ONTAP for instruction.
2	If you created archives of the SnapManager backup sets, complete the steps in “Restoring the Data directory from archived media” on page 65.
3	Confirm operation of the Domino server.

About this chapter This chapter describes how to view SnapManager reports for all your SnapManager operations.

Topics in this chapter This chapter discusses “What SnapManager reports contain” on page 70.

What SnapManager reports contain

Contents of SnapManager Reports

The SnapManager Reports feature contains four folders, which contain the log files for each operation:

- ◆ The Configure folder shows the log files for configuring SnapManager and moving the Data directory from the Domino server onto a virtual disk.
- ◆ The Backup folder lists all the log files for every snapshot taken on every Domino server.
- ◆ The Restore folder lists the log files for every snapshot restore performed on the Domino server.
- ◆ The Delete Snapshot folder lists describes which snapshots were deleted, how many were deleted, and which filer volume the deleted snapshot resided on.

Sample restore report

The following illustration shows a report for a restore.



Log file naming conventions

SnapManager Reports contains reports for all log files, database configurations and migrations, deleted snapshots, backups, and restores. The log files are named in the date and time format *month-day-year_hour.minute.second*, where year is a four-digit number and the hour is expressed in military time.

**Accessing the
SnapManager
Reports utility**

To access the SnapManager Reports utility, complete the following step.

Step	Action
1	Click the Reports tab in the SnapManager interface.

Index

A

archives

- CIFS-based 56
- NDMP 58
- NearStore 57
- offline restores 51
- restoring 65

Autosupport, enabling through SnapDrive 39

B

backing up a renamed database 52

backup

- Dump 3
- frequency of 45
- guidelines for restoring 52
- NDMP 3
- snapshots used as 3

backup sets

- about 56
- data organization 13, 14

C

command-Line Interface, *see* SMD CLI

Configurator, SnapManager 12

D

Database Instant ID, *see* DBIID

databases

- backing up 22
- backing up after renaming 52
- restoring from archive 65

DBIID 51, 54

Domino backup API 13

Domino Data directory iii, 3, 11

- calculating the size of 23
- migrating 12
- rules for storing 12

Domino server

- Partitioned server iii

F

FCP ii, iii, 4

Fibre Channel Protocol, *see* FCP

file system iii

filers

- definition of iii
- safeguarding data 4

L

local disk, migrating back to 35

LUNs 4

LUNs, virtual disk type iii

M

migrating to local disk 35

N

NDMP 3

NearStore, archiving 57

notes.ini file iii

NTFS 4

NVRAM 5

P

Partitioned server iii

point-in-time restores 15

R

reinstallation of SnapManager 40

reports

- accessing 71
- types of 70

restores

- from a snapshot 52
- functions of 15
- of a renamed database 52
- point-in-time 15, 51, 54
- points to note about 64

up-to-the-minute 15, 51, 54

S

SMD CLI parameters

del 41

N 41

--p 41

Pn 41

smd --backup 42

smd --restore 42

SnapDrive

about 2

storage requirements 23

when to use 3

SnapInfo subdirectory 12

rules for storing 12

SnapManager Backup 13

SnapManager

before you install 18

components of 12

how it works 11

installing 17

reinstalling 40

snapInfo files in 34

software requirements for 20

storage requirements for 24

uninstalling 40

when to use 2

SnapManager Backup 13

backing up databases with 44

creating archives with 56

definition of 13

deleting oldest snapshots with 45, 46

example of 4

ways to access 44

what it does 13

with other types of backups 47

SnapManager configuration requirements 33

SnapManager Configurator

definition 12

migrating back to local disk 35

requirements 33

SnapManager Reports

about 70

accessing 71

SnapManager Restore

capabilities of 50

guidelines for using 51

restoring from archive with 65, 67

types of restores 15

using point-in-time restores 53

using up-to-the-minute restores 53

what it does 15

snapshots

about 3

deleting oldest 46

maximum number allowed 45

T

transaction logs 11

migrating 12

rules for storing 12

storage requirements for 24

U

uninstalling SnapManager 40

up-to-the-minute restores 15, 51, 54

V

virtual disks

calculating the size 23

types of iii

Virtualized Local Disk, *see* VLD

VLDs

migrating from 35

safeguarding data 4