

Dynamic Storage Technology 1.0 Administration Guide

Novell® Open Enterprise Server

2 SP1

March 3, 2009

www.novell.com



Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2007–2009 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the [Novell Legal Patents Web page \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see [the Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide	11
1 Overview of Dynamic Storage Technology	13
1.1 Understanding Dynamic Storage Technology	13
1.2 Benefits of Dynamic Storage Technology	15
1.2.1 Transparent File Access to End Users	15
1.2.2 Policy-Based Migration between Primary and Secondary Storage Areas	16
1.2.3 Faster and Smaller Backups of Important Data	16
1.2.4 Faster Disaster Recovery	16
1.2.5 More Efficient Use of Expensive Storage	16
1.2.6 Fast Storage for Active Data and Slower, Less Expensive Storage for Old Data	16
1.2.7 Migrating Files from an Existing Secondary Volume	17
1.2.8 Access to the Secondary Storage Area without the Performance Penalties Seen in HSM Solutions	17
1.3 Shadowing Scenarios	17
1.3.1 Existing Volume as Primary with an Empty Volume as Secondary	17
1.3.2 Empty Volume as Primary with an Existing Volume as Secondary	18
1.4 DST Policy Scenarios	18
1.4.1 Place Seldom-Used Files in the Secondary Area	19
1.4.2 Place Unimportant Files in the Secondary Area	19
1.4.3 Migrate Selected Files to Another Volume	19
1.4.4 Migrate Files from Existing Volumes	19
1.5 DST Components	19
1.5.1 NCP Engine	20
1.5.2 ShadowFS	20
1.5.3 Policy Engine	20
1.6 Management Tools	20
1.7 What's Next	20
2 What's New for Dynamic Storage Technology	21
2.1 What's New (OES 2 SP1Linux)	21
2.1.1 iSCSI Block Storage Devices	21
2.2 What's New (OES 2 Linux)	21
3 Planning Your Dynamic Storage Technology Solution	23
3.1 Guidelines for Configuring and Using Dynamic Storage Technology	23
3.1.1 Operating System	23
3.1.2 Storage Devices	23
3.1.3 iSCSI Block Storage Devices	25
3.1.4 Remote Server-to-Server Connections	26
3.1.5 File Systems	26
3.1.6 User Access and Authentication	26
3.1.7 File Access Protocols	26
3.1.8 ShadowFS and FUSE	28
3.2 Guidelines for DST Shadow Volumes	28
3.2.1 Guidelines for Using Shadow Volumes	28
3.2.2 Caveats for Shadow Volumes	28
3.2.3 Number of Shadow Volumes per Server	29

3.2.4	Access Files via the Primary Volume	29
3.2.5	Virus Checking Utilities for Shadow Volumes	29
3.2.6	File Management Utilities for Shadow Volumes	30
3.2.7	Trustee Management for Shadow Volumes	30
3.2.8	Backup and Restore for Shadow Volumes	30
3.3	Guidelines for Using NSS Volumes in DST Shadow Volumes.	31
3.3.1	DST Support for NSS Media Formats	31
3.3.2	DST Support for NSS Volume Attributes	31
3.3.3	DST Support for NSS Features and Actions	33
3.3.4	DST Support for NSS File System Trustees and Attributes	34
3.3.5	DST Support for NSS Volume, Directory, and User Quotas	34
3.3.6	Using NSS Volumes in Clustered DST Shadow Volumes.	35
3.4	Guidelines for Using Shadow Volumes in Clusters with Novell Cluster Services for Linux . . .	36
3.5	Guidelines for Using Novell Distributed File Services with DST Shadow Volumes	36

4 Installing and Configuring Dynamic Storage Technology 39

4.1	Installation Requirements for Dynamic Storage Technology	39
4.1.1	NCP Server and Dynamic Storage Technology	40
4.1.2	Novell Storage Services	40
4.1.3	Novell eDirectory 8.8.2	40
4.1.4	Novell Samba	40
4.1.5	Linux User Management	40
4.1.6	Novell Cluster Services for Linux.	41
4.1.7	SLP	41
4.1.8	Novell Remote Manager for Linux	41
4.1.9	Novell iManager 2.7 for Linux	41
4.1.10	FUSE	42
4.1.11	OpenWBEM.	42
4.1.12	Other OES 2 Linux Services	42
4.2	Installing NCP Server and Dynamic Storage Technology	42
4.2.1	Installing on a New OES 2 Linux Server	42
4.2.2	Installing on an Existing OES 2 Linux Server	44
4.2.3	Configuring Global Policies for DST	45
4.3	Installing NCP Server and Dynamic Storage Technology on Nodes in a Novell Cluster Services for Linux Cluster.	45
4.4	Configuring a Global Policy that Replicates Branches of the Primary File Tree in the Shadow File Tree	46
4.5	Configuring Global Policies for Shifting Files from the Shadow File Tree to the Primary File Tree	47
4.5.1	Understanding Shift Parameters	47
4.5.2	Configuring a Global Policy for Shifting Modified Shadow Files	49
4.5.3	Configuring a Global Policy for Shifting Accessed Shadow Files	50
4.5.4	Configuring a Global Policy for the Days Since Last Access.	50
4.5.5	Using the SET Command to Set Global Policies.	51
4.6	Configuring Global Policies for Resolving Instances of Duplicate Files.	51
4.6.1	Understanding Conflict Resolution for Duplicate Files.	51
4.6.2	Configuring Actions to Resolve Duplicate Files Conflicts	54
4.6.3	Enabling or Disabling Broadcast Messages for Duplicate Files Conflicts	54
4.6.4	Resolving Instances of Duplicate Files in the /_DUPLICATE_FILES Directory	55
4.7	Configuring a Global Policy to Automatically Load ShadowFS at Boot Time.	56
4.8	Restarting the Novell NCP/NSS IPC (ncp2nss) Daemon.	56
4.9	Restarting the Novell eDirectory (ndsd) Daemon.	57

5	Installing and Configuring Shadow File System (ShadowFS) for CIFS/Samba Users	59
5.1	Understanding ShadowFS	59
5.2	Prerequisites for Using ShadowFS	60
5.3	Preparing Your System for Using ShadowFS	60
5.4	Installing ShadowFS and FUSE	61
5.5	Setting Rights to ShadowFS Shares	62
5.6	Creating a Samba Share	63
5.7	Adding a User to Samba	63
5.8	Connecting Users to the Share	64
5.9	Testing Shadow Volume Policies	64
5.10	Enabling or Disabling ShadowFS to Load at Boot Time	65
5.10.1	Verifying ShadowFS Commands in the init.d Script	65
5.10.2	Loading ShadowFS and FUSE at Boot Time	65
5.11	Starting and Stopping ShadowFS Manually	65
5.11.1	Starting FUSE and ShadowFS	66
5.11.2	Starting FUSE and ShadowFS with novell-shadowfs	66
5.11.3	Stopping Shadowfs	66
5.12	Configuring Trustee Rights for CIFS/Samba Users	67
6	Using Dynamic Storage Technology in a Virtual Environment	69
7	Management Tools for Dynamic Storage Technology	71
7.1	Dynamic Storage Technology Tasks in Novell Remote Manager for Linux	71
7.1.1	Accessing Novell Remote Manager	71
7.1.2	Starting, Stopping, or Restarting Novell Remote Manager on Linux	72
7.1.3	Quick Reference for Dynamic Storage Technology Options	72
7.1.4	Quick Reference for NCP Server Options	73
7.1.5	Quick Reference for DST Global Policy Settings	74
7.1.6	Shadow Volume Inventory	74
7.2	NCP Console (NCPCON) Commands	75
7.3	Management Tools for NSS Volumes	75
7.3.1	Storage Plug-In to Novell iManager 2.7	75
7.3.2	Files and Folders Plug-In to Novell iManager 2.7	75
7.3.3	NSS Management Utility (NSSMU)	75
7.4	Management Tools for Clustering	75
8	Managing DST Shadow Volumes for NSS Volumes	77
8.1	Understanding DST Shadow Volumes	77
8.1.1	DST Shadow Volumes	77
8.1.2	DST Shadow Volumes Management Tasks	78
8.1.3	Dynamic Storage Technology Policies	82
8.2	Creating NSS Volumes to Use in the DST Shadow Volume Pair	82
8.2.1	Requirements for NSS Volumes	83
8.2.2	Preparing Devices for NSS Volumes	83
8.2.3	Creating an NSS Pool	84
8.2.4	Creating and Configuring Unencrypted NSS Volumes	87
8.3	Configuring the NCP/NSS Bindings for an NSS Volume	90
8.3.1	Understanding the NCP/NSS Bindings Parameter	90
8.3.2	Enabling the NCP/NSS Bindings for an NSS Volume	91
8.3.3	Disabling the NCP/NSS Bindings for an NSS Volume	92

8.3.4	Enabling or Disabling NCP/NSS Bindings by Editing the /etc/opt/novell/ncp2nss.conf File	93
8.4	Creating a DST Shadow Volume with NSS Volumes	94
8.4.1	Prerequisites for DST Shadow Volumes	94
8.4.2	Preparing the NSS Volumes for Use in a DST Shadow Volume	95
8.4.3	Creating a DST Shadow Volume with Unshared NSS Volumes	96
8.5	Mounting and Dismounting DST Shadow Volumes	99
8.6	Viewing Volume Information	100
8.7	Removing a DST Shadow Volume	100
8.7.1	Preparing to Remove a Shadow Volume	100
8.7.2	Removing the Shadow Volume Relationship by Using Novell Remote Manager for Linux	101
8.7.3	Removing a Shadow Volume by Editing Configuration Files	103
8.8	Viewing File Events in the Shadow Volume's Audit Log	104
8.9	Backing Up DST Shadow Volumes	104
8.9.1	Planning Your Backup Solution	105
8.9.2	Planning Your Restore Solution	105
8.9.3	Using the /etc/NCPVolumes XML File for Backup	107
8.9.4	Configuring the Backup Attribute for NSS Volumes	107
8.9.5	Configuring Backup for Trustee Information on NSS Volumes on Linux	107
9	Managing Policies for Shadow Volumes	109
9.1	Understanding Shadow Volume Policy Options	109
9.1.1	Last Executed	109
9.1.2	Description	110
9.1.3	Start Time	110
9.1.4	End Time	110
9.1.5	Start Day	110
9.1.6	Frequency	110
9.1.7	Command Status	111
9.1.8	Volume Selection	112
9.1.9	Volume Operations	112
9.1.10	Subdirectory Restrictions	112
9.1.11	Search Criteria	113
9.2	Creating a Shadow Volume Policy	115
9.2.1	Prerequisite	115
9.2.2	Guidelines for Shadow Volume Policies	115
9.2.3	Creating a Shadow Volume Policy	115
9.3	Modifying a Shadow Volume Policy	117
9.4	Viewing DST Policies and Policy Status	117
9.5	Deleting a Shadow Volume Policy	118
10	Monitoring DST Shadow Volumes	119
10.1	Understanding the Shadow Volume Inventory	119
10.1.1	Inventory Summary	119
10.1.2	Available Space Trends	120
10.1.3	Graphical Profiles	121
10.1.4	Tabular Profiles	124
10.1.5	Inventory Detail Reports	125
10.1.6	Custom Shadow Volume Options	125
10.2	Accessing the Shadow Volume Inventory	127
10.3	Viewing Statistics for the Shadow Volume	127
10.4	Using Inventory Detail Reports to Move, Copy, or Delete Files on the Shadow Volume	128
10.5	Generating a Custom Inventory Report	128

11	Configuring DST Shadow Volumes with Novell Cluster Services for Linux	133
11.1	Planning for Shadow Volumes in a Cluster Environment	133
11.1.1	Prerequisites for Using Shadow Volumes in a Cluster	133
11.1.2	Guidelines for Load Scripts for the Cluster Resource for the Shadow Volume Pair	135
11.2	Preparing the Nodes to Support DST in a Cluster Environment	136
11.3	Preparing the NSS Volumes for Use in a Clustered Shadow Volume	136
11.4	Configuring the Cluster Load Script for Shadow Volumes Based on NSS Volumes	136
11.4.1	Creating a Shadow Volume in the Load Script	136
11.4.2	Overview of Cluster Resource Setup	137
11.4.3	Viewing or Modifying Cluster Load and Unload Scripts	138
11.4.4	Configuring the Load and Unload Scripts for a Shadow Volume	140
11.5	Configuring Shadow Volume Policies for the Clustered Shadow Volume	144
11.6	Removing a Clustered DST Shadow Volume	144
11.6.1	Preparing to Remove a Shadow Volume	144
11.6.2	Removing the Shadow Volume Relationship	145
12	Troubleshooting for Dynamic Storage Technology	151
12.1	My NCP server information has the setting: LOCAL_CODE_PAGE CP437. Why isn't it using UTF-8?	151
12.2	A File Is Listed Twice in a Directory	151
12.3	Users Cannot See Some Files and Directories	151
12.4	Cross-Protocol Locking Stops Working	152
13	Security Considerations	153
13.1	Client Access	153
13.2	Linux-Enabled eDirectory Users	153
13.3	Using File System Trustees and Rights	153
13.4	Server-to-Server Access	154
13.5	Hidden Directories and Files	154
13.5.1	Trustee Database	154
13.5.2	Available Space Trends	154
13.6	Shadow Volumes Audit Logs	154
13.7	Shadow File System Audit Logs	155
13.8	NCP Server Auditing and Log Files	155
13.9	Use Secure Remote Connections	155
A	Commands and Utilities for Dynamic Storage Technology	157
A.1	Using NCPCON for DST Commands	157
A.1.1	Interactive Mode	157
A.1.2	Command Line Mode	157
A.1.3	Scripting Mode	158
A.2	DST Commands for NCPCON	158
A.3	DST Commands for NCPCON for Use with Novell Cluster Services for Linux Clusters	162
A.3.1	Scenario 1: Primary NSS and Shadow NSS	162
A.3.2	Scenario 2: Primary Non-NSS and Shadow Non-NSS (Not supported in the initial release.)	162
A.3.3	Scenario 3: Primary Non-NSS and Shadow NSS (Not supported in the initial release.)	163
A.3.4	Scenario 4: Primary NSS and Shadow Non-NSS (Not supported in the initial release.)	163
A.4	Configuring Global DST Policies by Using the SET Command	163

A.4.1	Understanding DST Parameters for the SET Command	164
A.4.2	Using Novell Remote Manager to Configure DST Parameters for the SET Command	165
A.4.3	Using the ncpcon set Command to Configure DST Parameters	166
A.5	DST Commands for /etc/opt/novell/ncpserv.conf	167
A.6	DST Commands for /etc/opt/novell/shadowfs.conf	168
A.7	DST EXCLUDE_VOLUME Command for /etc/opt/novell/ncp2nss.conf	169
A.8	DST Shadow Volume Information in /etc/NCPVolumes	169
A.9	DST ShadowFS Volume Information in /etc/mtab.shadowfs	169

B RPM Files for Dynamic Storage Technology 171

C Documentation Updates 173

C.1	March 3, 2009	173
C.1.1	Configuring DST Shadow Volumes with Novell Cluster Services for Linux	173
C.2	February 13, 2009	174
C.2.1	Configuring DST Shadow Volumes with Novell Cluster Services for Linux	174
C.2.2	Installing and Configuring Dynamic Storage Technology	174
C.2.3	Managing DST Shadow Volumes for NSS Volumes	175
C.3	January 13, 2009	175
C.3.1	Management Tools for Dynamic Storage Technology	175
C.3.2	Managing DST Shadow Volumes for NSS Volumes	175
C.4	December 2008 (OES 2 SP1 Linux)	175
C.4.1	Configuring DST Shadow Volumes with Novell Cluster Services for Linux	176
C.4.2	Installing and Configuring Dynamic Storage Technology	176
C.4.3	Installing and Configuring Shadow File System (ShadowFS) for CIFS/Samba Users	176
C.4.4	Managing DST Shadow Volumes for NSS Volumes	176
C.4.5	Planning Your Dynamic Storage Technology Solution	177
C.4.6	Using DST to Migrate Data on Demand from NetWare to OES 2 Linux	177
C.5	May 30, 2008	177
C.5.1	Managing Policies for Shadow Volumes	178
C.6	May 5, 2008	178
C.6.1	Commands and Utilities for Dynamic Storage Technology	178
C.6.2	Installing and Configuring Dynamic Storage Technology	178
C.6.3	Installing and Configuring Shadow File System (ShadowFS) for CIFS/Samba Users	178
C.6.4	Managing DST Shadow Volumes for NSS Volumes	179
C.7	January 7, 2008	179
C.7.1	Managing DST Shadow Volumes for NSS Volumes	179
C.8	December 7, 2007	179
C.8.1	Planning Your Dynamic Storage Technology Solution	179
C.8.2	Using DST to Migrate Data on Demand from NetWare to OES 2 Linux	180
C.9	November 16, 2007	180
C.9.1	Installing and Configuring Shadow File System (ShadowFS) for CIFS/Samba Users	180

About This Guide

This guide describes how to install, configure, and manage the Dynamic Storage Technology for Novell® Open Enterprise Server (OES) 2 Linux.

- ♦ Chapter 1, “Overview of Dynamic Storage Technology,” on page 13
- ♦ Chapter 2, “What’s New for Dynamic Storage Technology,” on page 21
- ♦ Chapter 3, “Planning Your Dynamic Storage Technology Solution,” on page 23
- ♦ Chapter 4, “Installing and Configuring Dynamic Storage Technology,” on page 39
- ♦ Chapter 5, “Installing and Configuring Shadow File System (ShadowFS) for CIFS/Samba Users,” on page 59
- ♦ Chapter 6, “Using Dynamic Storage Technology in a Virtual Environment,” on page 69
- ♦ Chapter 7, “Management Tools for Dynamic Storage Technology,” on page 71
- ♦ Chapter 8, “Managing DST Shadow Volumes for NSS Volumes,” on page 77
- ♦ Chapter 9, “Managing Policies for Shadow Volumes,” on page 109
- ♦ Chapter 10, “Monitoring DST Shadow Volumes,” on page 119
- ♦ Chapter 11, “Configuring DST Shadow Volumes with Novell Cluster Services for Linux,” on page 133
- ♦ Chapter 12, “Troubleshooting for Dynamic Storage Technology,” on page 151
- ♦ Chapter 13, “Security Considerations,” on page 153
- ♦ Appendix A, “Commands and Utilities for Dynamic Storage Technology,” on page 157
- ♦ Appendix B, “RPM Files for Dynamic Storage Technology,” on page 171

Audience

This guide is intended for storage services administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *Dynamic Storage Technology Administration Guide*, see the [Novell Open Enterprise Server 2 documentation Web site](http://www.novell.com/documentation/oes2/) (<http://www.novell.com/documentation/oes2/>).

Additional Documentation

For documentation on Novell Storage Services™ (NSS) volumes, see the *OES 2 SPI: NSS File System Administration Guide*.

For documentation on NCP™ (NetWare® Core Protocol™) Server and NCP volumes for Linux* POSIX* file systems, see the *OES 2 SP1: NCP Server for Linux Administration Guide*.

For documentation on other OES 2 products, see the [Novell Open Enterprise Server 2 documentation Web site](http://www.novell.com/documentation/oes2/) (<http://www.novell.com/documentation/oes2/>).

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux or UNIX*, should use forward slashes as required by your software.

Overview of Dynamic Storage Technology

1

Dynamic Storage Technology (DST) for Novell® Open Enterprise Server (OES) 2 Linux is an information life-cycle management technology that uses a policy-based approach for relocating data between two Novell Storage Services™ (NSS) volumes located on different devices, and transparently provides a unified view of the file tree to users. You specify policies that classify data to be moved by its frequency of use, filename, file type, and file size. Policy enforcement is automated with scheduled and on-demand runs of the policies. DST allows you to seamlessly tier storage between high-performance and lower-performance devices. For example, you can establish policies that keep frequently-used mission-critical data on high-performance devices, and move rarely accessed less-essential data to lower-performance devices. Backup can be performed separately on the two volumes, which allows for different backup schedules.

Dynamic Storage Technology enables you to manage data more efficiently for the enterprise--and in doing so, the enterprise can potentially realize significant cost savings in storage management.

This section provides an overview of Dynamic Storage Technology and its components.

- [Section 1.1, “Understanding Dynamic Storage Technology,” on page 13](#)
- [Section 1.2, “Benefits of Dynamic Storage Technology,” on page 15](#)
- [Section 1.3, “Shadowing Scenarios,” on page 17](#)
- [Section 1.4, “DST Policy Scenarios,” on page 18](#)
- [Section 1.5, “DST Components,” on page 19](#)
- [Section 1.6, “Management Tools,” on page 20](#)
- [Section 1.7, “What’s Next,” on page 20](#)

1.1 Understanding Dynamic Storage Technology

NCP™ (NetWare® Core Protocol™) Server is a service that allows you to define NCP volumes as share points on Linux POSIX file systems. Novell Storage Services volumes are automatically mounted as NCP volumes. Each NCP volume exports the subdirectory structure located from its root on down. This is called the volume’s directory tree structure, or *primary file tree*.

Dynamic Storage Technology (DST) for OES 2 Linux is a new feature of NCP Server that allows you to specify a shadow relationship between two volumes, which forms a *shadow volume pair*. The secondary directory tree structure, or *shadow file tree*, shadows the primary file tree.

IMPORTANT: In the initial release of DST, only NSS volumes are supported for DST shadow volume pairs.

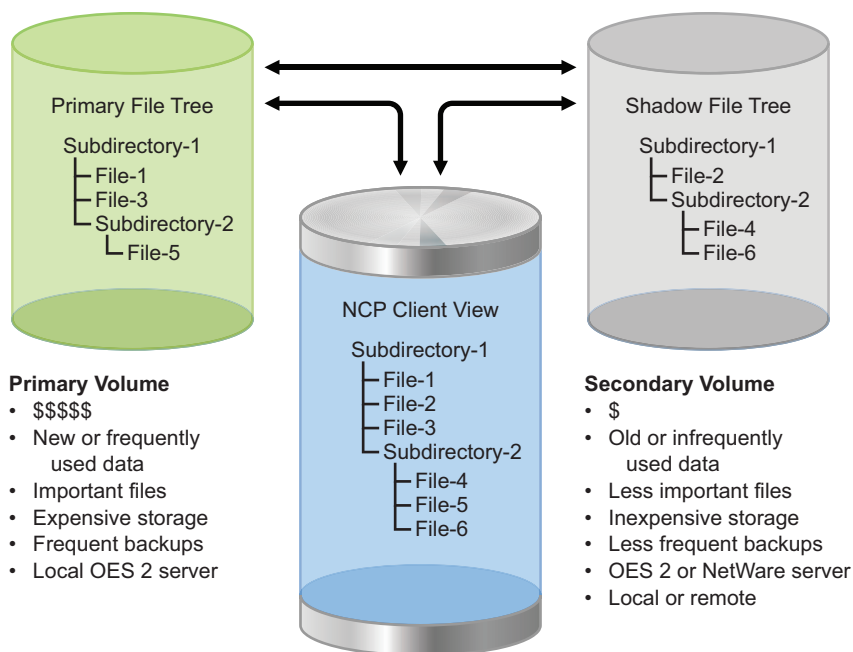
DST presents a unified view to users of the subdirectory trees on each volume, as illustrated in [Figure 1-1](#). The primary file tree and secondary file tree have the same directory structure so that each subdirectory appears in both locations as data is moved between the two volumes. The primary

tree and the secondary tree are overlaid to create one virtual volume tree that is transparently presented to the users. NCP client and CIFS/Samba users are not aware of the actual physical location of the files.

Users access files by connecting to the primary volume. All file operations (such as read, write, rename, delete, and so on) can be performed whether the file actually resides on the primary or secondary location. DST executes the transaction transparently for the user. In general, transactions are executed wherever the file resides. Any file that requires a normal user-level action (copy, delete, and so on) is moved back to the primary for the action to take place, which simplifies the auditing requirements. Some transactions, such as a directory rename, occur in both file trees.

An example of the unified view of the shadow volume is shown in **Figure 1-1**. When an NCP client lists files for Subdirectory-1, the user sees File-1, File-2, and File-3. File-1 and File-3 are stored in the primary file tree. File-2 is stored in the shadow file tree.

Figure 1-1 User View of the File System Directory



Only NCP clients and CIFS/Samba clients see the unified view of the file tree. Applications that directly access the local Linux file system see the primary file tree and the shadow file tree as independent subdirectories. Thus, backup tools can apply one backup policy to the primary file tree and a different backup policy to the shadow file tree. The only operations that take place on the secondary volume are backup, or “remove and archive.” The secondary volume is hidden to everyone but the backup administrators and the IT staff until the shadow relationship is removed, at which point, the volume once again functions independently and normally.

When a client creates new files, the files are automatically stored in the primary file tree. When files in the shadow file tree are modified, a configurable option allows the files to be moved to the primary file tree (default), or left in the shadow file tree. For example, if your policy is to place newer files in the primary file tree and to place older files in the shadow file tree, you want an older file in the secondary file tree to move to primary file tree if the file’s content is modified. On the

other hand, if you are placing files of one type (such as .doc and .ppt) in the primary area and files of a different type (such as .mp3 and .jpg) in the secondary area, you want files to stay where they are whenever they are modified.

When a new subdirectory is created, it is created in the primary file tree. A configurable option allows the necessary branches of the tree to be created in the shadow file tree as policies are enforced to move files to the secondary area (the default), or to be created immediately in the secondary area and files moved later as policies are enforced. Performance is better when the branches are created only as needed.

When a subdirectory is deleted, it is deleted in both areas. When a subdirectory is renamed, it is renamed in both areas. Unified file and directory management happens automatically so that the areas remain synchronized and have the same directory structure.

The primary area and the secondary area can each be located anywhere in the logical Linux subdirectory tree available to the server. For example, the default location for NSS volumes is in the /media/nss/ directory, but DST can handle any mount point that you specify for your NSS volumes.

The primary volume and secondary volume must use the same file system, such as NSS volumes. The primary and secondary volumes can be located on a local, Fibre Channel, or iSCSI block storage device. Clustering is supported for Fibre Channel and iSCSI devices. The device types and performance can differ, with the secondary volume typically being on the device with lesser performance.

1.2 Benefits of Dynamic Storage Technology

Shadow volumes have many benefits:

- ♦ [Section 1.2.1, “Transparent File Access to End Users,” on page 15](#)
- ♦ [Section 1.2.2, “Policy-Based Migration between Primary and Secondary Storage Areas,” on page 16](#)
- ♦ [Section 1.2.3, “Faster and Smaller Backups of Important Data,” on page 16](#)
- ♦ [Section 1.2.4, “Faster Disaster Recovery,” on page 16](#)
- ♦ [Section 1.2.5, “More Efficient Use of Expensive Storage,” on page 16](#)
- ♦ [Section 1.2.6, “Fast Storage for Active Data and Slower, Less Expensive Storage for Old Data,” on page 16](#)
- ♦ [Section 1.2.7, “Migrating Files from an Existing Secondary Volume,” on page 17](#)
- ♦ [Section 1.2.8, “Access to the Secondary Storage Area without the Performance Penalties Seen in HSM Solutions,” on page 17](#)

1.2.1 Transparent File Access to End Users

The users’ view of the data is unified for NCP clients. With ShadowFS, the view is also transparent for CIFS/Samba clients. Because shadow volumes present a merged view of the file trees, the end user’s files are in the same logical place regardless of their physical location. This allows the administrator to manage the data without disrupting the end user’s view of the files.

1.2.2 Policy-Based Migration between Primary and Secondary Storage Areas

DST provides policy-based control of the direction that you want to move data between devices. You can set up policies that migrate data by type, date, or directory in either direction. You can set policies so that data stored on the secondary storage volume can be accessed without demigrating it.

1.2.3 Faster and Smaller Backups of Important Data

Backup policies can differ for the primary storage volume and the secondary storage volume. The server administrator can partition the volume's data into two categories:

- ♦ Important data that needs to be maintained on quality storage and backed up frequently
- ♦ Less important data that can be stored on less expensive storage and backed up less frequently

Analyzing the inventory of a volume's data shows that a large portion of its data is seldom used. Having a shadow volume allows the server administrator to spend more on the most important data and spend less on the less important data. The important data, which is stored on the primary area, can be backed up nightly. The less important data, which is stored in the secondary area, can be backed up weekly or even monthly. Getting the less important data out of the way enables the backups of your important data to run more quickly and efficiently. Partitioning your data in this way can significantly lower the cost of backups by reducing both labor and tape requirements.

1.2.4 Faster Disaster Recovery

Start by locating your most important files on the primary area. Then, during a disaster recovery, the server administrator can restore the primary area first. This restores the critical files first, and leaves the recovery of the less important secondary area until later. The users can continue working while files they probably do not need immediately are being restored. Also, other fault-tolerant replication solutions like snapshots can be used for the primary area without wasting money on files that do not require the same level of fault tolerance.

1.2.5 More Efficient Use of Expensive Storage

Policies can be used to partition files based on file age, owner, type, size, and so on. You can move the less important files to from a higher quality storage array to a lesser quality storage, thus reserving the higher-cost storage for your most important files. For example, you can configure the primary area on block-based SCSI storage devices in a Fibre Channel SAN-based hardware RAID array or storage array, and configure the secondary area on a lesser quality storage array using slower devices like SATA. This allows you to get more use out of your Fibre Channel storage solution, and keep it from filling up with unimportant files. You can store more data on your server with a lower overall cost per gigabyte.

1.2.6 Fast Storage for Active Data and Slower, Less Expensive Storage for Old Data

Storage media can differ for the primary storage volume and the secondary storage volume. Storage costs can be reduced by allowing data that is used infrequently to be stored on lower-cost storage. Locate the primary area on storage drives that are faster and higher quality. Then locate the secondary area on less expensive storage drives. Files that the users are currently working on can be

located on the high-performance drives. The files that have not been modified for a long time can be moved to the lower-performance drives to free up space on the high-performance drives. In this way, you can locate a large amount of your data on less expensive, lower-performance storage drives, while your users still get high-quality performance because their active files are located on the high-performance storage drives.

1.2.7 Migrating Files from an Existing Secondary Volume

You can start with an empty primary NSS volume, and have the shadow area be an existing volume. The combined view initially presented by the NCP Engine is equivalent to the secondary volume. You can define a policy to move files to the primary as they are modified or accessed. As users access their data through the new primary volume, the files they use are automatically migrated to the new server. This migration-on-demand approach migrates the data gradually, freeing the IT department from spending off-hours time migrating the data with the server offline.

1.2.8 Access to the Secondary Storage Area without the Performance Penalties Seen in HSM Solutions

With HSM (hierarchical storage management) solutions, files are migrated from the primary storage to a secondary storage device, and a copy of the file's metadata (stub file) is left behind in the volume's directory tree. If the file is ever accessed again, it needs to be migrated back to the primary storage before it is available.

In contrast, DST shadow volumes can access files directly regardless of which area (primary or secondary) they are in, and without de-migrating them. If a user searches through all the files on a shadow volume, the files are searched without needing to move them to the primary area. Also, shadow volume backups are faster because there are no HSM metadata stub files for the backup software to scan. The backup software need not be HSM aware.

1.3 Shadowing Scenarios

The flow of data between the primary storage area and the secondary storage area can take place two ways.

- ♦ [Section 1.3.1, “Existing Volume as Primary with an Empty Volume as Secondary,” on page 17](#)
- ♦ [Section 1.3.2, “Empty Volume as Primary with an Existing Volume as Secondary,” on page 18](#)

1.3.1 Existing Volume as Primary with an Empty Volume as Secondary

In this scenario, all data currently exists on an NSS volume that you want to make the primary volume. You create a new volume to use as the secondary storage, then define a shadow volume for the two NSS volumes.

The volume contains information that is seldom used and rarely changes, and you want to move the little used data to a location where it can be accessed but backed up less frequently. This decreases the time it takes to backup or restore the data you use the most.

Configure a policy that governs what data moves to the secondary storage area. Data is returned to the primary area based on a policy of usage or file type. For example, if the user simply views the data in a file, then the data does not move. If the user modifies the file, then the file is moved back to the primary volume. Users are not aware of where the data are physically stored because they see a unified view of both volumes.

1.3.2 Empty Volume as Primary with an Existing Volume as Secondary

You have an existing volume on older storage and want to move the data to new storage arrays. You create a new volume on a storage device in a Fibre Channel SAN solution. You define a shadow volume that uses the empty device as the primary area, and the existing volume as the secondary area.

Configure a policy wherein the data moves to the primary volume based upon usage. Data gradually flows to the primary volume as it is used. In this way, there is a natural background migration of data from the existing volume to the new volume. The new volume gradually grows, and the relationship between the primary and shadow volume is as if the primary had been populated first.

For example, suppose you have an existing pool that spans multiple LUNs, and contains multiple volumes. The current best practice is to use a separate LUN for each pool, and a single volume per pool. You create a new pool on a new larger LUN (or fewer larger LUNs), then create a single NSS volume in the pool. You might need to rename the old and new NSS volumes if users need to access the data via known paths, because after the shadow volume is created, users access data via the new volume. Repeat this process so that you have one new empty volume for each of the old volumes on the pool. As the new and old volumes are ready, you create a DST shadow volume with the new volume as the primary storage area and an existing volume from the old pool as the secondary storage area.

To begin de-migrating the data, configure the global policies to shift data from the secondary storage area to the primary storage area whenever they are accessed or modified. You can also configure individual shadow volume policies or use inventory reports to shift data on schedule or on-demand based on age, filenames, file types, or file size. De-migration occurs with the storage online and accessible to end users; they are not aware of where the data is actually stored.

When you have moved all the data from the old NSS volume to the new one, you can remove the shadow volume, then delete the empty old NSS volume from the old pool. When the old pool has had all its volumes deleted, you can delete the old pool, which frees that storage for use in other volumes. Users are not aware that the volumes are on a new pool. They see only the volume by its name.

1.4 DST Policy Scenarios

DST policies control how data flows between the primary storage area and the secondary storage.

- ♦ [Section 1.4.1, “Place Seldom-Used Files in the Secondary Area,” on page 19](#)
- ♦ [Section 1.4.2, “Place Unimportant Files in the Secondary Area,” on page 19](#)
- ♦ [Section 1.4.3, “Migrate Selected Files to Another Volume,” on page 19](#)
- ♦ [Section 1.4.4, “Migrate Files from Existing Volumes,” on page 19](#)

1.4.1 Place Seldom-Used Files in the Secondary Area

Create a DST policy that locates and moves files that have not been modified or accessed for a period of time, such as 6 months, to the secondary area. Continue doing regular nightly backups of the primary area, but back up the shadow area once every 2 weeks.

Schedule the policy to run monthly to check for additional files that now meet the usage criteria, and move them to the shadow area. Let this policy be enforced before backing up the secondary area.

1.4.2 Place Unimportant Files in the Secondary Area

Create a policy that locates and moves less important files types to the secondary area. This could include *.jpg, *.mp3, *.wma, *.mpeg, *.iso, *.zip, *.cab, and so on. By default, files in the secondary area are moved back to the primary area if they are modified. You should disable the SHIFT_MODIFIED_SHADOW_FILES parameter to turn off this auto-move feature. The SHIFT_ACCESSED_SHADOW_FILES parameter is disabled by default so that files are not moved when accessed. These settings are global settings that apply to all shadow volumes on a given server. In this way, the desired file types stay in the secondary area after they are moved there.

Continue doing regular nightly backups of the primary area, but back up the shadow area only once every 2 weeks. Run the policy monthly to move any additional files to the secondary area before backing up the secondary area.

1.4.3 Migrate Selected Files to Another Volume

After using a shadow volume for awhile, you want to split the volumes so they can be used separately. Use the Shadow Volume Inventory page in Novell Remote Manager for Linux to view statistics on files and usage for the shadow volume. At the bottom of the page, use the form to move selected files from the secondary area to the primary area, or vice versa. Repeat as necessary until the files are placed as desired in the two storage areas. Remove the shadow volume relationship, which allows each volume to function independently again.

1.4.4 Migrate Files from Existing Volumes

You want to migrate volumes from old storage devices to new ones. Create a new NSS volume on the OES 2 Linux server with the same attributes as an existing volume. Create a shadow volume that uses the new volume as primary, and the old volume as secondary. Set up global policies for shifting files between primary and secondary areas as desired. The clients log in to the new volume instead of the old one. Their files from the old server appear to reside on the new server's volume. As files are accessed or modified, the files are automatically migrated on demand to the new volume. This eliminates the need to take the old volume offline to transfer its files to the new storage location.

1.5 DST Components

There are four main components for Dynamic Storage Technology.

- ♦ [Section 1.5.1, “NCP Engine,” on page 20](#)
- ♦ [Section 1.5.2, “ShadowFS,” on page 20](#)
- ♦ [Section 1.5.3, “Policy Engine,” on page 20](#)

1.5.1 NCP Engine

The NCP Engine provides support for NCP clients and the main file copy engine. It supports the Shadow Volume system for NCP file access. Shadow Volume allows users of the volume to see a unified file-tree view of the primary file tree and shadow file tree.

1.5.2 ShadowFS

The Shadow File System (ShadowFS) allows Linux applications, such as Samba Server, to see the combined view of the shadow volume. It allows CIFS/Samba users of the volume to see a unified file-tree view of the primary file tree and shadow file tree.

ShadowFS uses FUSE (File Systems in User Space) to create a local mount point for each NCP shadow volume in `/media/shadowfs/shadow_volume_name`. FUSE is an open source software package included in OES 2 Linux that is installed automatically when you install DST.

Backup utilities can optionally use this Linux-based unified view when restoring data to the shadow volume. For information, see [Section 8.9.2, “Planning Your Restore Solution,” on page 105](#).

1.5.3 Policy Engine

The DST policy engine allows you to create, manage, and enforce policies for a shadow. There are two types of policies:

- ♦ **Global:** The policy applies to every mounted Shadow volume on the server. If global policies are set for a server where volumes are in a clustered pool, these policies must be set on every node in the cluster. For information about setting global policies, see [Chapter 4, “Installing and Configuring Dynamic Storage Technology,” on page 39](#).
- ♦ **Volume:** The policy applies only to a specified volume. Volume policies can be used for local or shared volumes. They should be used when volumes are in a clustered pool so that the policy easily follows the volume when the cluster resource fails over. For information, see [Chapter 9, “Managing Policies for Shadow Volumes,” on page 109](#).

1.6 Management Tools

Dynamic Storage Technology shadow volumes, global policies, and shadow volume policies can be managed in Novell Remote Manager for Linux. For information about using Novell Remote Manager, see [Chapter 7, “Management Tools for Dynamic Storage Technology,” on page 71](#).

DST shadow volumes can be created and removed with commands by using the NCP Console (NCPCON, `npccon (8)`) utility. For information, see [Appendix A, “Commands and Utilities for Dynamic Storage Technology,” on page 157](#).

1.7 What’s Next

For information about installing NCP Server, Dynamic Storage Technology, and NSS, see [Chapter 4, “Installing and Configuring Dynamic Storage Technology,” on page 39](#).

For information about planning your DST solution, see [Chapter 3, “Planning Your Dynamic Storage Technology Solution,” on page 23](#).

What's New for Dynamic Storage Technology

2

This section describes enhancements and additions to the Dynamic Storage Technology for Novell® Open Enterprise Server (OES) 2 Linux.

- ♦ [Section 2.1, “What’s New \(OES 2 SP1Linux\),” on page 21](#)
- ♦ [Section 2.2, “What’s New \(OES 2 Linux\),” on page 21](#)

2.1 What's New (OES 2 SP1Linux)

This section describes capabilities for Dynamic Storage Technology in OES 2 SP1 that have been added since the initial release of OES 2.

- ♦ [Section 2.1.1, “iSCSI Block Storage Devices,” on page 21](#)

2.1.1 iSCSI Block Storage Devices

DST supports using iSCSI block storage devices running on OES servers for the primary and secondary storage areas for NSS volumes. They can also be used for clustered DST shadow volume pairs. For guidelines, see [Section 3.1.3, “iSCSI Block Storage Devices,” on page 25](#).

2.2 What's New (OES 2 Linux)

This is an initial release of Dynamic Storage Technology 1.0.

Planning Your Dynamic Storage Technology Solution

3

This section describes guidelines for using Dynamic Storage Technology (DST) on Novell® Open Enterprise Server (OES) 2 Linux servers.

- ♦ [Section 3.1, “Guidelines for Configuring and Using Dynamic Storage Technology,” on page 23](#)
- ♦ [Section 3.2, “Guidelines for DST Shadow Volumes,” on page 28](#)
- ♦ [Section 3.3, “Guidelines for Using NSS Volumes in DST Shadow Volumes,” on page 31](#)
- ♦ [Section 3.4, “Guidelines for Using Shadow Volumes in Clusters with Novell Cluster Services for Linux,” on page 36](#)
- ♦ [Section 3.5, “Guidelines for Using Novell Distributed File Services with DST Shadow Volumes,” on page 36](#)

3.1 Guidelines for Configuring and Using Dynamic Storage Technology

- ♦ [Section 3.1.1, “Operating System,” on page 23](#)
- ♦ [Section 3.1.2, “Storage Devices,” on page 23](#)
- ♦ [Section 3.1.3, “iSCSI Block Storage Devices,” on page 25](#)
- ♦ [Section 3.1.4, “Remote Server-to-Server Connections,” on page 26](#)
- ♦ [Section 3.1.5, “File Systems,” on page 26](#)
- ♦ [Section 3.1.6, “User Access and Authentication,” on page 26](#)
- ♦ [Section 3.1.7, “File Access Protocols,” on page 26](#)
- ♦ [Section 3.1.8, “ShadowFS and FUSE,” on page 28](#)

3.1.1 Operating System

The Dynamic Storage Technology services and NetWare® Core Protocol™ (NCP™) Server for Linux run only on an OES 2 Linux server. DST supports 32-bit and 64-bit processors. DST supports any number of processors; you are limited only by what OES 2 Linux supports.

3.1.2 Storage Devices

Block storage devices used for the primary and secondary storage can (and usually do) have different performance characteristics where the secondary storage area is slower and less expensive. Both the primary and secondary devices must be attached to the OES 2 Linux server where you are creating and managing DST shadow volume pairs.

Typically, both the primary and secondary storage devices reside in storage arrays in a Fibre Channel storage area network (SAN). You can also use block storage devices in an iSCSI SAN where the targets are running on OES servers. You can use Fibre Channel and iSCSI block storage devices in the same shadow volume pair.

Table 3-1 summarizes the supported device types and whether the device type can be used for clustered solutions.

Table 3-1 *Supported Devices for Primary and Secondary Storage Areas*

OES 2 Linux Server	Primary Location	Secondary Location	Cluster Support	Caveats
Server-based storage	Yes	Yes	No	No known issues.
Direct-attached storage	Yes	Yes	No	No known issues.
Fibre Channel storage	Yes	Yes	Yes	For additional cluster guidelines, see “Guidelines for Using Shadow Volumes in Clusters with Novell Cluster Services for Linux” on page 36.
iSCSI target storage devices	Yes	Yes	Yes	For additional iSCSI guidelines, see Section 3.1.3, “iSCSI Block Storage Devices,” on page 25.

Both the Novell Storage Services™ (NSS) and Novell Cluster Services for Linux require that devices must be able to be managed by the Enterprise Volume Management System (EVMS). When you create an NSS pool on OES 2 Linux, the NSS management tools automatically configure the device for use with EVMS. If you create a pool on a shared device, an EVMS Cluster Segment Manager and a NetWare Segment Manager is added to the device. For information, see [“EVMS Requirements”](#) in the *OES 2 SP1: NSS File System Administration Guide*.

Make sure that you consider device requirements imposed by other components that you use with Dynamic Storage Technology. For information, see the references in [Table 3-2](#) that pertain to your particular storage solution.

Table 3-2 *Requirements for Devices*

Device Requirements	Reference
OES 2 Linux	“Server Hardware” in the <i>OES2 SP1: Linux Installation Guide</i>
Novell Storage Services™ (NSS) on Linux	“Devices” in the <i>OES 2 SP1: NSS File System Administration Guide</i>
NSS on Linux running in a virtual environment	“Guidelines for Using NSS in a Xen Virtualization Environment” in the <i>OES 2 SP1: NSS File System Administration Guide</i>
Novell Cluster Services for Linux	“Shared Disk System Requirements” in the <i>OES 2 SP1: NSS File System Administration Guide</i>
iSCSI initiator software on OES 2 Linux	“Configuring iSCSI Initiator” in the <i>SLES 10 SP2 Installation and Administration Guide</i>
iSCSI target software on NetWare 6.5 SP7	“iSCSI Target Requirements” in the <i>OES 2 SP 1: iSCSI 1.1.3 for NetWare Administration Guide</i>
iSCSI target software on OES 2 Linux	“Setting Up an iSCSI Target” in the <i>SLES 10 SP2 Installation and Administration Guide</i>

3.1.3 iSCSI Block Storage Devices

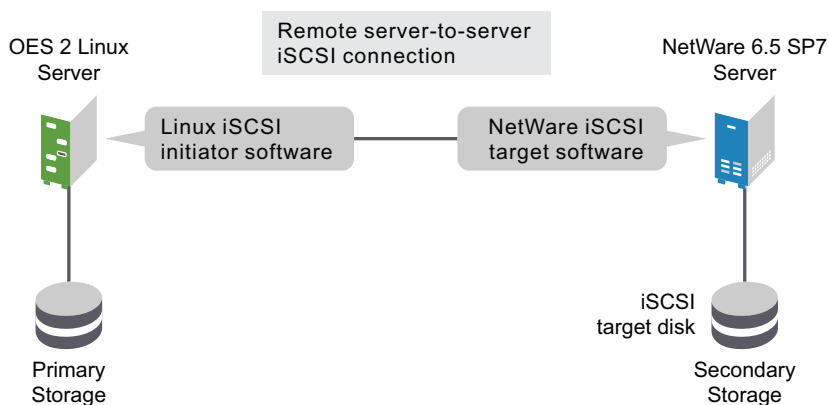
Dynamic Storage Technology supports using target iSCSI block storage devices to store the primary and secondary volumes in a shadow volume pair. Any iSCSI block storage device should work in a shadow volume pair, providing that it is compatible with the Linux iSCSI initiator software running on the OES 2 Linux server where you create and manage the shadow volume pair. However, only iSCSI targets running on the following OES servers (or later versions) have been tested and are supported:

- ♦ OES 2 Linux
- ♦ OES 2 NetWare (NetWare 6.5 SP7)
- ♦ OES 1 SP2 Linux

IMPORTANT: Third-party iSCSI solutions have not been tested, so are not supported.

For example, [Figure 3-1](#) illustrates a NetWare 6.5 SP7 server as the iSCSI target server that connects to the OES 2 Linux server via the Linux iSCSI initiator software.

Figure 3-1 NetWare 6.5 to OES 2 Linux



For information about setting up iSCSI target devices on OES servers, see the following:

- ♦ “[Setting Up an iSCSI Target](#)” in the *SLES 10 SP2 Installation and Administration Guide*
- ♦ “[Configuring iSCSI Targets](#)” in the *OES 2 SP 1: iSCSI 1.1.3 for NetWare Administration Guide*

The iSCSI targets must be connected to the Linux iSCSI initiator software running on the OES 2 Linux server where you are creating DST shadow volumes. For information, see the following resources:

- ♦ “[Configuring iSCSI Initiator](#)” in the *SLES 10 SP2 Installation and Administration Guide*
- ♦ “[Accessing iSCSI Targets on NetWare Servers from Linux Initiators](#)” in the *OES 2 SP 1: iSCSI 1.1.3 for NetWare Administration Guide*

IMPORTANT: OES 2 Linux does not support running iSCSI target software and initiator software on the same server.

3.1.4 Remote Server-to-Server Connections

Remote server-to-server connections to NSS volumes are not supported for NCP, Samba, and NFS protocols.

3.1.5 File Systems

Dynamic Storage Technology supports shadow volumes based only on Novell Storage Services volumes. Both the primary storage location and the secondary storage location must be existing NSS volumes. For more information, see [Section 3.3, “Guidelines for Using NSS Volumes in DST Shadow Volumes,” on page 31](#).

IMPORTANT: Mixing file systems for the primary and secondary areas in a given DST shadow volume pair is not supported.

3.1.6 User Access and Authentication

Users access data in the DST shadow volume by connecting to the primary storage location. All file access is controlled using the Novell trustee model, which requires users to authenticate via Novell eDirectory™ 8.8.2. All users (except the `root` user) of the shadow volume must have User objects defined in eDirectory. For information about configuring eDirectory users, see the [Novell eDirectory 8.8 Administration Guide](#).

The `root` user of the OES 2 Linux server is the only local user who has direct access to the volumes.

3.1.7 File Access Protocols

DST supports user access via NCP and CIFS/Samba protocols. You can use both NCP and CIFS/Samba in the same DST environment. Users can share files accessible through both protocols and utilize a multi-protocol file locking feature of NCP Server (cross-protocol locks) to ensure that shared files are not corrupted by either protocol. Primary lock identification comes from the Samba system.

IMPORTANT: Users access all data via the primary storage location of the shadow volume. They should never connect directly to the secondary storage area.

When DST is used, performance is slightly reduced, depending on the file access protocol being used. With NCP, aggregate performance is reduced by less than 10%. With CIFS/Samba, aggregate performance is reduced by up to 48%.

See the following sections for more information about each protocol:

- ♦ [“NCP Users” on page 27](#)
- ♦ [“CIFS/Samba Users” on page 27](#)
- ♦ [“Novell AFP \(Not Supported\)” on page 27](#)
- ♦ [“Novell CIFS \(Not Supported\)” on page 27](#)
- ♦ [“Other Protocols \(Not Supported\)” on page 28](#)

NCP Users

The DST Shadow Volumes engine supports access for NCP client users. Users access data via the primary storage server, using the Novell Client™ or other NCP clients. For information about configuring NCP Server for the OES 2 Linux server, see the *OES 2 SP1: NCP Server for Linux Administration Guide*.

See the following resources for the latest release of the Novell Client, which provides NCP access for users on Linux and Windows clients:

- ♦ [Novell Client 2.0 for Linux documentation Web site \(http://www.novell.com/documentation/linux_client/index.html\)](http://www.novell.com/documentation/linux_client/index.html)
- ♦ [Novell Client 1.0 SP1 for Vista* documentation Web site \(http://www.novell.com/documentation/vista_client/index.html\)](http://www.novell.com/documentation/vista_client/index.html)
- ♦ [Novell Client 4.91 SP5 for Windows XP/2003 documentation Web site \(http://www.novell.com/documentation/noclienu/index.html\)](http://www.novell.com/documentation/noclienu/index.html)

Only NCP client versions that are configured to receive broadcast messages are eligible to receive the duplicate file conflict messages. For information, see **Section 4.6.3, “Enabling or Disabling Broadcast Messages for Duplicate Files Conflicts,”** on page 54.

NetStorage for Linux has limited use for accessing files on shadow volumes. The user can see, read, and write files, and is unaware whether a specific file is on the primary volume or the shadow volume. However, certain management functions such as getting file properties, setting trustees, and salvaging files, work only if the files are on the primary volume, but do not work if the files are on the secondary volume.

CIFS/Samba Users

The DST Shadow File Systems (ShadowFS) engine supports access for CIFS/Samba users. In order to access the server via Samba, CIFS/Samba users must also be Linux-enabled users of the Linux server. Use the Linux User Management (LUM) plug-in to iManager to Linux-enable users. Samba must also be LUM enabled. Enable the cross-protocol file locking parameter for NCP Server if you are also giving access to NCP users.

For information, see the following:

- ♦ *OES2 SP1: Samba Administration Guide*
- ♦ *OES 2 SP1: Novell Linux User Management Technology Guide*

Novell AFP (Not Supported)

Novell AFP (Apple Filing Protocol*) for OES 2 SP1 Linux has not been tested in use for NSS volumes in a DST configuration, so it is not supported for DST in the OES 2 SP1 Linux release. Novell AFP supports cross-protocol file locking.

Novell CIFS (Not Supported)

Novell CIFS for OES 2 SP1 Linux has not been tested in use for NSS volumes in a DST configuration, so it is not supported for DST in the OES 2 SP1 Linux release. Novell CIFS does not support cross-protocol file locking in OES 2 SP1 Linux.

Other Protocols (Not Supported)

User access to shadow volumes via other protocols (such as HTTP, FTP, NFS, and others) is not supported.

3.1.8 ShadowFS and FUSE

The Shadow File System (ShadowFS) must be running when you have CIFS/Samba users of the shadow volume. It resolves the tree information from the two storage areas into a single, unified view of the shadow volume tree.

When ShadowFS is running, it automatically creates a shadow file system directory for each of the shadow volumes, not just the ones where you plan to allow CIFS/Samba access. CIFS/Samba users see only those volumes where they have file system trustee rights.

ShadowFS requires FUSE (File System in User Space) to be installed and running.

3.2 Guidelines for DST Shadow Volumes

Consider the guidelines in this section when planning your shadow volumes.

- ♦ [Section 3.2.1, “Guidelines for Using Shadow Volumes,” on page 28](#)
- ♦ [Section 3.2.2, “Caveats for Shadow Volumes,” on page 28](#)
- ♦ [Section 3.2.3, “Number of Shadow Volumes per Server,” on page 29](#)
- ♦ [Section 3.2.4, “Access Files via the Primary Volume,” on page 29](#)
- ♦ [Section 3.2.5, “Virus Checking Utilities for Shadow Volumes,” on page 29](#)
- ♦ [Section 3.2.6, “File Management Utilities for Shadow Volumes,” on page 30](#)
- ♦ [Section 3.2.7, “Trustee Management for Shadow Volumes,” on page 30](#)
- ♦ [Section 3.2.8, “Backup and Restore for Shadow Volumes,” on page 30](#)

3.2.1 Guidelines for Using Shadow Volumes

DST shadow volumes are intended for use with data volumes. Consider the following additional guidelines when planning your shadow volumes:

- ♦ Do not put system files and application files on DST shadow volumes.
- ♦ You cannot create a DST shadow volume for the `_ADMIN` volume.
- ♦ Make sure to exclude directories that contain databases such as those for Novell GroupWise® and MySQL. Rebuild situations might occur because of the additional latency related to the DST handling, or if the secondary storage area becomes unavailable for any reason.

3.2.2 Caveats for Shadow Volumes

- ♦ When using NSS volumes in the shadow volume, both the primary volume and the secondary volume must exist before you define the shadow volume.
- ♦ While a file is moved from one area to the other, the file is locked so that clients cannot access it during relocation.

- ♦ A file cannot be moved between the areas if the file is open. When the administrator attempts to relocate a file from one area to the other, by policy or through an immediate execution, that relocation request fails if a user has the file open; only files that are not in use might be moved.
- ♦ New files are automatically created on the primary volume.
- ♦ When you rename a folder on the primary location, the name is changed on the primary location and the secondary location.
- ♦ When you rename a folder on the secondary location by accessing the folder through NCP or CIFS/Samba, the name is changed on the primary location and the secondary location.
- ♦ If you rename a folder by directly accessing the folder on the secondary location, the new name is not modified on the primary location. It becomes a different folder in the secondary file tree. It contains the files that were stored in it at that location at the time when you renamed it. The files appear to have disappeared from existing folder.

IMPORTANT: To avoid this problem, do not modify or rename files and folders on the secondary volume by directly accessing them. Use only NCP or CIFS/Samba to access them via the primary volume, which uses the unified file tree view.

3.2.3 Number of Shadow Volumes per Server

The supported limit for Shadow Volumes is 32 volumes on a physical server and 16 volumes on a virtual server.

The supported limit for ShadowFS is 32 volumes on a physical server and 16 volumes on a virtual server.

IMPORTANT: This constraint is imposed because of a known defect in FUSE (File System in User Space). A patch for FUSE is planned after the initial release of OES 2 to extend the number of supported ShadowFS volumes.

3.2.4 Access Files via the Primary Volume

Changes made to files and directories directly on the secondary storage server while it is defined and running as a shadow volume do not synchronize to the primary server. Instead, they become two different folders or files.

IMPORTANT: Do not rename or modify files or directories directly on the secondary storage location.

3.2.5 Virus Checking Utilities for Shadow Volumes

You can continue use of existing virus checking utilities that currently execute successfully against the designated file systems on the primary volume. DST is transparent to this operation. Because the only access to the secondary volume is through the primary volume, there is no need for a virus checking operation on the secondary volume unless the shadow volume is removed, allowing the volume to act independently again.

3.2.6 File Management Utilities for Shadow Volumes

You can continue use of existing file management utilities that currently execute successfully against the designated file systems. DST is transparent to this operation. All file management operations currently available to NSS users through Novell iManager 2.7, NSSMU, and Novell Remote Manager for Linux function transparently for shadow volumes. File operations and the location of the file are transparent to the NCP and CIFS clients.

3.2.7 Trustee Management for Shadow Volumes

When the NCP protocol is used conjunction with the NSS file system, all native NCP functionality (security, rights, trustees, salvage, directory quotas, and so on) are preserved in a DST environment. This configuration requires the use of eDirectory 8.8.2. No functionality is lost, and no management patterns are changed.

When you deploy DST in a CIFS/Samba operational environment, use of the CIFS protocol in conjunction with the NSS file system presents native CIFS functionality for security, rights, and so on. The conversion of CIFS ACLs (access control lists) to NSS ACLs based on the POSIX definitions is based on code resident in Samba and is not supported for modification by Novell. This configuration requires the use of eDirectory 8.8.2 in the OES 2 server environment.

IMPORTANT: The CIFS support of ACLs is offered as-is, and is not modified to take advantage of the expanded management features of NSS file systems.

3.2.8 Backup and Restore for Shadow Volumes

Applications that directly access the local Linux file system see the primary file tree and the shadow file tree as independent subdirectories. Thus, backup tools can apply one backup policy to the primary file tree and a different backup policy to the shadow file tree. The only operations that take place on the secondary volume are backup, or “remove and archive.”

Using shadow volumes allows backups of important data to be made faster and more frequently because you can apply different backup policies for the primary volume and secondary volume. For example, the server administrator can partition the volume’s data into two categories:

- ♦ Important data that needs to be maintained on quality storage and backed up frequently.
- ♦ Less important data that can be stored on less expensive storage and backed up less frequently.

An analysis or inventory of a volume’s data shows that a large portion of it is seldom used. Having a shadow volume allows the server administrator to spend more on the most important data and spend less on the less important data. The frequently used data can be backed up nightly. The seldom-used data can be backed up weekly or monthly. Getting the less important data out of the way enables the backups of your important data to run more quickly and efficiently. Partitioning your data in this way can significantly reduce the cost of hosting it.

Because the most important files are located in the primary storage area, disaster recovery can be faster, too. The server administrator can restore the critical files by restoring the primary storage area first, then restore the secondary storage area. This gets the files that users need most to them quickly, and they do not need to wait while files they do not usually need are restored. In addition, more fault tolerant replication solutions can be deployed for the primary storage area where it matters most.

3.3 Guidelines for Using NSS Volumes in DST Shadow Volumes

Dynamic Storage Technology supports shadow volumes created with unencrypted Novell Storage Services volumes. Consider the guidelines and caveats in this section when planning your shadow volume solution.

- ♦ [Section 3.3.1, “DST Support for NSS Media Formats,” on page 31](#)
- ♦ [Section 3.3.2, “DST Support for NSS Volume Attributes,” on page 31](#)
- ♦ [Section 3.3.3, “DST Support for NSS Features and Actions,” on page 33](#)
- ♦ [Section 3.3.4, “DST Support for NSS File System Trustees and Attributes,” on page 34](#)
- ♦ [Section 3.3.5, “DST Support for NSS Volume, Directory, and User Quotas,” on page 34](#)
- ♦ [Section 3.3.6, “Using NSS Volumes in Clustered DST Shadow Volumes,” on page 35](#)

3.3.1 DST Support for NSS Media Formats

The NSS media format used by the primary and secondary volume must be the same. For information about media formats supported for NSS on OES 2 Linux and later, see [“Upgrading the NSS Media Format”](#) in the *OES 2 SPI: NSS File System Administration Guide*.

3.3.2 DST Support for NSS Volume Attributes

Make sure you enable the same NSS volume attributes on both volumes in the shadow relationship to ensure a consistent user experience. For example, if Salvage is enabled for the primary volume but not for the secondary volume, files that are deleted when they reside on the secondary volume are purged immediately, and are not available for salvage.

[Table 3-3](#) describes which NSS volume attributes are supported for use with Dynamic Storage Technology, and any caveats to consider when using them. For information about the volume attributes, see [“Volume Attributes”](#) in the *OES 2 SPI: NSS File System Administration Guide*.

Table 3-3 *DST Support for NSS Volume Attributes*

NSS Volume Attribute	Supported	Caveats
Allow mount point to be renamed	No	DST does not track the renaming of NSS volumes or their mount points. Before you rename or modify the mount point for an NSS volume, you must remove the shadow volume definition. Afterwards, you can re-create the shadow volume.
Backup	Yes	The Linux file system sees both volumes, so you back up each volume separately.

NSS Volume Attribute	Supported	Caveats
Compression	Yes	<p>You can set compression on one or both volumes.</p> <p>Compressed files are uncompressed when they are moved from the primary volume to secondary volume, and vice versa. In order for the move to occur, there must be sufficient space on the source volume to allow both the uncompressed and compressed copies of the file to coexist until the move is completed. There must also be sufficient space on the destination volume for the uncompressed file to be stored. The file is re-compressed according to the compression schedule and settings in the destination volume.</p>
Data Shredding	Yes	For security compliance reasons, you should set this attribute on both volumes if you use it.
Directory Quotas	Yes	Set a directory quota for a directory only on the primary volume. For more information, see Section 3.3.5, “DST Support for NSS Volume, Directory, and User Quotas,” on page 34.
File-level Snapshot	Yes	No known issues.
Flush Files Immediately	Yes	No known issues.
Lookup Namespace	Yes	In OES 2 SP1 and later, the default Lookup Namespace for NSS on Linux is Long, which treats filenames as case insensitive. In prior versions, the default name space is UNIX. Using the Long name space helps improve performance because NetWare and Windows treat filenames as case insensitive. This is especially important when files are to be accessed through the CIFS/Samba protocol.
Migration (to near-line HSM storage)	No	DST should not be used in combination with HSM storage solutions.
Modified File List (Use Event File List APIs instead.)	No	<p>By default, modified files are moved back to the primary location. If you disable the Shift Modified Files parameter, modified files might also be located on the secondary location.</p> <p>Modified File List is rarely used. It has been replaced by the Event File List APIs that provide more information than the Modified File List. For information, see “Using the Event File List to Refine the Backup” in the <i>OES 2 SP1: NSS File System Administration Guide</i>.</p>
Salvage	Yes	<p>Deleted files on a NSS volume that are salvageable remain salvageable after that volume is used in a shadow volume pair.</p> <p>Duplicate deleted folders might be presented when using Salvage (undelete) and Purge options for folders. You must restore the folders in order to see which one contains the deleted files (on the primary volume), and which is empty (on the secondary volume).</p>
User Space Quotas	Yes	Set up the user space quotas separately on each of the volumes. For more information, see Section 3.3.5, “DST Support for NSS Volume, Directory, and User Quotas,” on page 34.
User-level Transaction Model	No	NSS does not support the NetWare Transaction Tracking System™ for NSS volumes on Linux.

3.3.3 DST Support for NSS Features and Actions

Table 3-4 describes caveats for using the NSS volume features and actions when working with DST shadow volumes.

Table 3-4 *Caveats for NSS Features and Actions*

NSS Feature	Supported	Caveats
Novell Archive and Version Services	Yes	File versions can be archived only for files located on the primary volume of the DST shadow volume. You cannot set up archive jobs for the secondary volume.
Novell Distributed File Services	Yes	Some limitations apply. For information, see Section 3.5, “Guidelines for Using Novell Distributed File Services with DST Shadow Volumes,” on page 36.
Encryption	No	DST does not support shadow volumes using encrypted NSS volumes. Configuring DST with encrypted NSS volumes causes the volumes to hang on mount. They cannot be remounted until you remove the shadow volume relationship.
Hard links	No	DST does not support hard links on NSS volumes used in a shadow volume. if a file is a hard link, and the hard-linked file is moved between the primary and the secondary area, the move is really a copy and has the effect of breaking the hard link and creating an additional version of the file that is not linked to the other ones.
Media format for enhanced hard links	Yes	The media format that supports enhanced hard links is supported, but the hard links themselves are not.
Multiple Server Activation Prevention	Yes	Each pool enforces this separately.
Pool low-space warnings and watermarks	Yes	You must set the pool-level watermarks for low-space warnings separately for the primary pool and the secondary pool. IMPORTANT: NSS does not have a volume-level low-space-warning feature. However, you can take advantage of the NCP Server global parameters for managing low-space warnings for NCP volumes on NSS, Ext3, and Reiser file systems. For information, see “ NCP Volumes Low-Space Warning ” in the <i>OES 2 SP1: NCP Server for Linux Administration Guide</i> .
Pool snapshots	Yes	Take pool snapshots separately for the primary and secondary pools. IMPORTANT: For NSS on Linux, pool snapshots are not supported for clustered pools. If the primary volume is configured to contain the most frequently used data, pool snapshots of the primary pool have a higher percentage of changed data than does the secondary pool.

NSS Feature	Supported	Caveats
Renaming a volume's mount point	No	Renaming a volume's mount point breaks the shadow volume. If you need to rename a volume's mount point, remove the shadow, rename the volume's mount point, then create the shadow volume again.
Renaming a volume	No	Renaming a volume breaks the shadow volume. If you need to rename a volume, remove the shadow, rename the volume, then create the shadow volume again.
Resizing (growing) a pool	Yes	No known issues.
Sharing a pool and its volumes in a cluster	Yes	When using NSS volumes in shared pools, you must manage both pools' resources in the same cluster load and unload scripts. For information, see Section 3.3.6, "Using NSS Volumes in Clustered DST Shadow Volumes," on page 35 and Section 3.4, "Guidelines for Using Shadow Volumes in Clusters with Novell Cluster Services for Linux," on page 36 .
Volume quotas	Yes	Set the volume quotas separately for each volume. For more information, see Section 3.3.5, "DST Support for NSS Volume, Directory, and User Quotas," on page 34 .

3.3.4 DST Support for NSS File System Trustees and Attributes

Authentication and file access is controlled by the trustee settings on the primary volume of the DST shadow volume pair. Users do not have direct access to the secondary volume.

Explicit trustee settings for files and folders are stored in both volumes.

Inherited trustee rights are calculated and enforced based on the trustee settings for the folders and files on the primary volume.

File system attributes are enforced by the NSS file system. For NSS on Linux, the Read Only, Read/Write, Execute, and Hidden attributes are available.

3.3.5 DST Support for NSS Volume, Directory, and User Quotas

DST supports using volume, directory, and user quotas features of NSS volumes. However, DST does not have a unified quota system for the two volumes that manages quotas for the combined primary and secondary volumes in a shadow volume pair.

- ♦ ["NSS Volume Quotas" on page 34](#)
- ♦ ["NSS Directory Quotas" on page 35](#)
- ♦ ["NSS User Quotas" on page 35](#)

NSS Volume Quotas

Volume quotas specify how big a volume can grow within a NSS pool. You can set a volume quota on the primary volume, secondary volume, or both volumes in the shadow volume pair. Each quota is enforced independently of the other.

Users of the shadow volume pair can map drives only to the primary volume. They are not aware of the existence of the secondary volume. Users see only the volume quota status for the primary volume. The volume quota information is not presented with a total space usage across both volumes. Users can actually store up to the quota amount set on each of the volumes, where each limit is enforced separately.

When the user has data stored on both the primary and secondary volume, the user sees the amount of space used only on the primary volume, which does not accurately reflect the total of space used on the two volumes.

The administrator can check the combined space available on the shadow volume pair and on each volume separately by using Novell Remote Manager for Linux.

NSS Directory Quotas

Directory quotas are set on specific directories and specify how much data can reside in that specific directory. You can set a directory quota only on the primary volume. When a secondary volume is in a shadow volume pair, the directory quotas set on it are not enforced. The directory quota is enforced only for the space consumed on the primary volume.

The users can store up to the directory quota amount for the directory on the primary volume, and an unlimited amount up to the maximum volume size on the secondary volume.

Users see only the directory quota status for the primary volume. The directory quota information is not presented with a total for the directory across both volumes.

NSS User Quotas

User quotas are set on specific users and specify how much data a user can store on a specific volume. You can set a user quota for a user on the primary volume, secondary volume, or both volumes in the shadow volume pair. Quotas on each volume are enforced independently of the other.

Users see only the user quota status for the primary volume. The user quota information is not presented with a total space usage across both volumes. Users can actually store up to the user quota amount set on each of the volumes, where each limit is enforced separately.

3.3.6 Using NSS Volumes in Clustered DST Shadow Volumes

NSS supports sharing NSS pools and their volumes in OES 2 Linux clusters with Novell Cluster Services for Linux.

The nature of shadow volumes is that the two member NSS volumes reside on separate devices that have differing performance characteristics. In a clustered shadow volume, the two NSS volumes are in different clustered NSS pools, and the pools are on different shared devices. You must cluster the resources on each device separately, then manage them together in the same cluster load script and the same cluster unload script. In this way, the clustered DST shadow volume is failed over as a single logical resource to the destination node, and the devices, pools, and volumes are mounted in the correct sequence.

For general clustering guidelines, see [Section 3.4, “Guidelines for Using Shadow Volumes in Clusters with Novell Cluster Services for Linux,”](#) on page 36.

3.4 Guidelines for Using Shadow Volumes in Clusters with Novell Cluster Services for Linux

DST supports using DST shadow volumes in a cluster with Novell Cluster Services for Linux for clusters of up to 16 nodes. Clustering is supported for NSS volumes on shared Fibre Channel and iSCSI devices. Users can access files via NCP or CIFS/Samba.

Both the primary storage location and the secondary storage location must be clustered. Because it is the nature of the two locations to be on separate devices, you create the two clustered resources separately. However, the two clustered resources must be managed in the same cluster load script and unload script so they can be failed over together between nodes.

The following caveats apply:

- ♦ All nodes where you plan to fail over the shadow volume must be running OES 2 Linux. The nodes must have the same configuration of file systems, access protocols, and so on.
- ♦ DST and the NCP Server services are not cluster aware. They must be installed and configured separately on each node in the cluster.
- ♦ Global policies for DST must have the same settings on each node in the server. To manage a global DST policy for a given node, open Novell Remote Manager for Linux by using the IP address of the node, not the cluster resource. For information about configuring DST global policies, the [Chapter 4, “Installing and Configuring Dynamic Storage Technology,” on page 39](#).
- ♦ To manage shadow volume policies in a cluster, open Novell Remote Manager for Linux by using the IP address of the cluster resource. You can also open Novell Remote Manager by using the IP address of the physical node where the cluster resource is currently mounted if you know which node it is on.
- ♦ At any given time, the primary volume and the secondary volume in the DST shadow volume must be located on the same OES 2 Linux node in the cluster.
- ♦ The shadow volume’s policies are failed over along with the shadow volume.

For clustering issues for NSS volumes, see [Section 3.3.6, “Using NSS Volumes in Clustered DST Shadow Volumes,” on page 35](#).

3.5 Guidelines for Using Novell Distributed File Services with DST Shadow Volumes

Novell Distributed File Services can be used with DST shadow volumes in the limited configurations shown in [Table 3-5](#). DFS is installed automatically as part of the NSS file system.

Table 3-5 *DST Support for Novell DFS Features*

Novell DFS Features	Primary NSS Volume	Secondary NSS Volume	Clustered Shadow Volumes	File Access Protocol
Junctions	Yes	No	No	NCP only Samba does not support DFS junctions for NSS volumes on Linux.

Novell DFS Features	Primary NSS Volume	Secondary NSS Volume	Clustered Shadow Volumes	File Access Protocol
Junction targets	Yes	No	No	NCP or CIFS/ Samba
Move/split volumes	No	No	No	Not applicable

When using DST shadow volumes in combination with Novell DFS junctions, consider the following caveats:

- ♦ Junctions are broken when they reside on secondary NSS volumes. If you use a new volume as the primary area and an existing volume as the secondary area, you must delete junctions on the existing NSS volume before you create the shadow volume, and recreate them on the primary volume after you create the shadow volume.
- ♦ If you use a new volume as the primary area and an existing volume as the secondary area, and the existing volume is the target of an existing junction, the junctions pointing to it are broken when you create the shadow volume pair. You must create a new junction that points to the same location on the primary volume of that shadow relationship. After the new junction is working, delete the junction that points to the secondary volume.
- ♦ Do not create a shadow relationship for an NSS volume if a DFS move volume or split volume job is in progress.
- ♦ You must remove the shadow volume before you start a DFS move or split volume job.

Installing and Configuring Dynamic Storage Technology

4

This section describes installation requirements and how to install and configure Dynamic Storage Technology on Novell® Open Enterprise Server (OES) 2 Linux.

- ♦ [Section 4.1, “Installation Requirements for Dynamic Storage Technology,” on page 39](#)
- ♦ [Section 4.2, “Installing NCP Server and Dynamic Storage Technology,” on page 42](#)
- ♦ [Section 4.3, “Installing NCP Server and Dynamic Storage Technology on Nodes in a Novell Cluster Services for Linux Cluster,” on page 45](#)
- ♦ [Section 4.4, “Configuring a Global Policy that Replicates Branches of the Primary File Tree in the Shadow File Tree,” on page 46](#)
- ♦ [Section 4.5, “Configuring Global Policies for Shifting Files from the Shadow File Tree to the Primary File Tree,” on page 47](#)
- ♦ [Section 4.6, “Configuring Global Policies for Resolving Instances of Duplicate Files,” on page 51](#)
- ♦ [Section 4.7, “Configuring a Global Policy to Automatically Load ShadowFS at Boot Time,” on page 56](#)
- ♦ [Section 4.8, “Restarting the Novell NCP/NSS IPC \(ncp2nss\) Daemon,” on page 56](#)
- ♦ [Section 4.9, “Restarting the Novell eDirectory \(ndsd\) Daemon,” on page 57](#)

4.1 Installation Requirements for Dynamic Storage Technology

Make sure your system satisfies the required software and configuration settings that are specified in this section.

- ♦ [Section 4.1.1, “NCP Server and Dynamic Storage Technology,” on page 40](#)
- ♦ [Section 4.1.2, “Novell Storage Services,” on page 40](#)
- ♦ [Section 4.1.3, “Novell eDirectory 8.8.2,” on page 40](#)
- ♦ [Section 4.1.4, “Novell Samba,” on page 40](#)
- ♦ [Section 4.1.5, “Linux User Management,” on page 40](#)
- ♦ [Section 4.1.6, “Novell Cluster Services for Linux,” on page 41](#)
- ♦ [Section 4.1.7, “SLP,” on page 41](#)
- ♦ [Section 4.1.8, “Novell Remote Manager for Linux,” on page 41](#)
- ♦ [Section 4.1.9, “Novell iManager 2.7 for Linux,” on page 41](#)
- ♦ [Section 4.1.10, “FUSE,” on page 42](#)
- ♦ [Section 4.1.11, “OpenWBEM,” on page 42](#)
- ♦ [Section 4.1.12, “Other OES 2 Linux Services,” on page 42](#)

4.1.1 NCP Server and Dynamic Storage Technology

Dynamic Storage Technology is a component of the NetWare® Core Protocol™ (NCP™) Server. NCP Server for Linux provides the NCP services for NSS volumes on Linux and for NCP volumes on Linux POSIX file systems. NCP Server must be installed and running in order for DST to work. DST is automatically enabled when NCP server is running and enabled, even if there are no shadow volumes currently defined. There is no way to turn DST off in Novell Remote Manager for Linux or in the YaST Runlevel Editor.

For information about managing NCP Server for Linux, see the *OES 2 SP1: NCP Server for Linux Administration Guide*.

4.1.2 Novell Storage Services

In order to use Novell Storage Services™ (NSS) in Dynamic Storage Technology shadow volumes, you must install and configure Novell Storage Services and any other OES 2 services that are required by NSS for Linux. For information about installing NSS, see “[Installing and Configuring Novell Storage Services](#)” in the *OES 2 SP1: NSS File System Administration Guide*.

In its initial release, Dynamic Storage Technology supports only NSS volumes being used as shadow volumes. If you plan to use DST, you need to install NSS when you install NCP Server and Dynamic Storage Technology.

IMPORTANT: Some restrictions apply. For information, see [Section 3.3, “Guidelines for Using NSS Volumes in DST Shadow Volumes,”](#) on page 31.

4.1.3 Novell eDirectory 8.8.2

Dynamic Storage Technology requires that access to data be restricted to users with User objects defined in Novell eDirectory™ 8.8.2. For information about configuring eDirectory and users, see the *Novell eDirectory 8.8 Administration Guide*.

IMPORTANT: The server’s `root` user is the only local user who can access data without authenticating in eDirectory.

4.1.4 Novell Samba

When using Samba to provide file access for CIFS/Samba users, you must install and configure Novell Samba, then configure users for CIFS/Samba access. For information about configuring Samba services, see the *OES2 SP1: Samba Administration Guide*.

4.1.5 Linux User Management

Linux User Management is selected and installed automatically when you install NCP Server and Dynamic Storage Technology. CIFS/Samba users must be Linux-enabled with Linux User Management. For information about Linux-enabling users with Linux User Management, see the *OES 2 SP1: Novell Linux User Management Technology Guide*.

4.1.6 Novell Cluster Services for Linux

NCP Server and Dynamic Storage Technology support the sharing of shadow volumes in clusters with Novell Cluster Services 1.8.4 for Linux (and later versions). NCP Server and DST are not clustered, and must be installed and configured on each OES 2 Linux node in the cluster where you plan to fail over DST shadow volumes.

For information about configuring shadow volumes in cluster resources, see [Chapter 11, “Configuring DST Shadow Volumes with Novell Cluster Services for Linux,”](#) on page 133.

For information about installing and managing Novell Cluster Services for Linux, see *OES 2 SPI: Novell Cluster Services 1.8.5 for Linux Administration Guide*.

4.1.7 SLP

SLP (Service Location Protocol) is a required component for Dynamic Storage Technology when you place the shadow volume (that is, the primary and secondary NSS volumes) on cluster resources on Novell Cluster Services clusters. NCP requires SLP for the `ncpcon bind` and `ncpcon unbind` commands in the cluster load and unload scripts.

SLP is not automatically installed when you select Novell Cluster Services. SLP is installed with Novell eDirectory during the OES 2 Linux install. You can enable and configure SLP on the *eDirectory Configuration - NTP & SLP* page. For information, see “[Specifying SLP Configuration Options](#)” in the *OES2 SPI: Linux Installation Guide*.

When the SLP daemon (`slpd`) is not installed and running on a cluster node, any cluster resource that contains the `ncpcon bind` command goes comatose when it is migrated or failed over to the node because the bind cannot be executed without SLP.

4.1.8 Novell Remote Manager for Linux

Novell Remote Manager for Linux is required for managing NCP Server services, NCP volumes, and Dynamic Storage Technology. It is installed as a default component when you install NCP Server and Dynamic Storage Technology.

For information about managing Novell Remote Manager and using its other features, see the *OES 2 SPI: Novell Remote Manager for Linux Administration Guide*. For information about management options for DST, see [Section 7.1, “Dynamic Storage Technology Tasks in Novell Remote Manager for Linux,”](#) on page 71.

4.1.9 Novell iManager 2.7 for Linux

Novell iManager 2.7 for Linux is required for managing eDirectory users, Samba services, Universal Password, Linux User Management, Novell Storage Services, and Novell Cluster Services for Linux. It is not necessary to install iManager on every server, but it must be installed somewhere on the network. For information about installing and using Novell iManager, see the *Novell iManager 2.7 Installation Guide*.

4.1.10 FUSE

The Shadow File System uses FUSE (File Systems in User Space) to create a local mount point that presents a unified file system view of a shadow volume for CIFS/Samba users. FUSE is an open source software package that is delivered in OES 2 Linux, and is installed automatically when you install Dynamic Storage Technology.

4.1.11 OpenWBEM

In OES 2 Linux, OpenWBEM is a PAM-enabled Linux utility that must be enabled and running on the OES 2 Linux server when managing services with Novell Remote Manager for Linux and Novell iManager. During the install, make sure you enable OpenWBEM (the default) when configuring Linux services. For information, see “[Services in OES 2 Linux That Require LUM-Enabled Access](#)” in the *OES 2 SP1: Planning and Implementation Guide*.

4.1.12 Other OES 2 Linux Services

Make sure to install and configure additional OES 2 Linux services that might be required by each of the other services mentioned in this section. Refer to the individual guides for those services for information about how to install and manage them.

4.2 Installing NCP Server and Dynamic Storage Technology

- ♦ [Section 4.2.1, “Installing on a New OES 2 Linux Server,” on page 42](#)
- ♦ [Section 4.2.2, “Installing on an Existing OES 2 Linux Server,” on page 44](#)
- ♦ [Section 4.2.3, “Configuring Global Policies for DST,” on page 45](#)

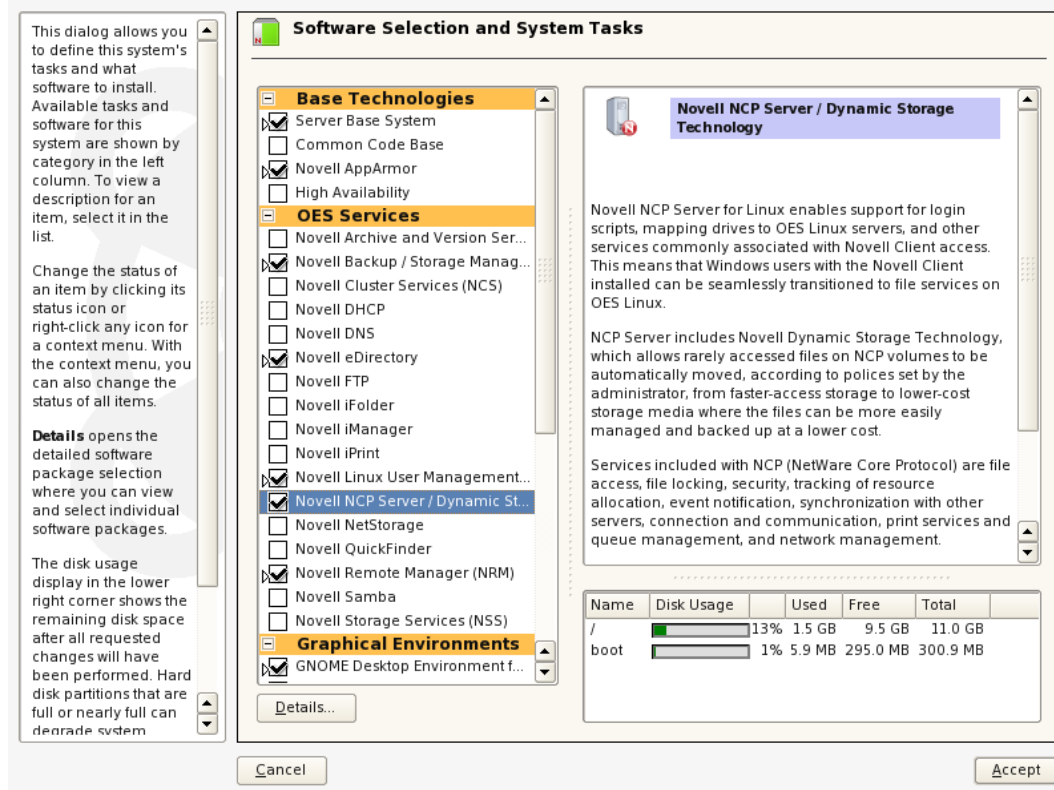
4.2.1 Installing on a New OES 2 Linux Server

NCP Server for Linux and Dynamic Storage Technology can be installed during the OES 2 Linux installation. For general install instructions, see the *OES2 SP1: Linux Installation Guide*.

- 1 During the YaST install, on the *Install Settings* page, click *Software* to view details.
- 2 Select *Novell NCP Server / Dynamic Storage Technology* from the *OES Services* options.

When you select *Novell NCP Server / Dynamic Storage Technology*, the following additional *OES Services* options are automatically selected:

- ♦ *Novell Backup / Storage Management Services*
- ♦ *Novell eDirectory*
- ♦ *Novell Linux User Management*
- ♦ *Novell Remote Manager (NRM) for Linux*



- 3 Select *Novell Storage Services* from the *OES Services* options.

IMPORTANT: In its initial release, DST shadow volumes are supported only for Novell Storage Services volumes.

- 4 (Optional) Select *Novell iManager* from the *OES Services* options.

You must install Novell iManager somewhere in your network, but it is not necessary to install it on every server.

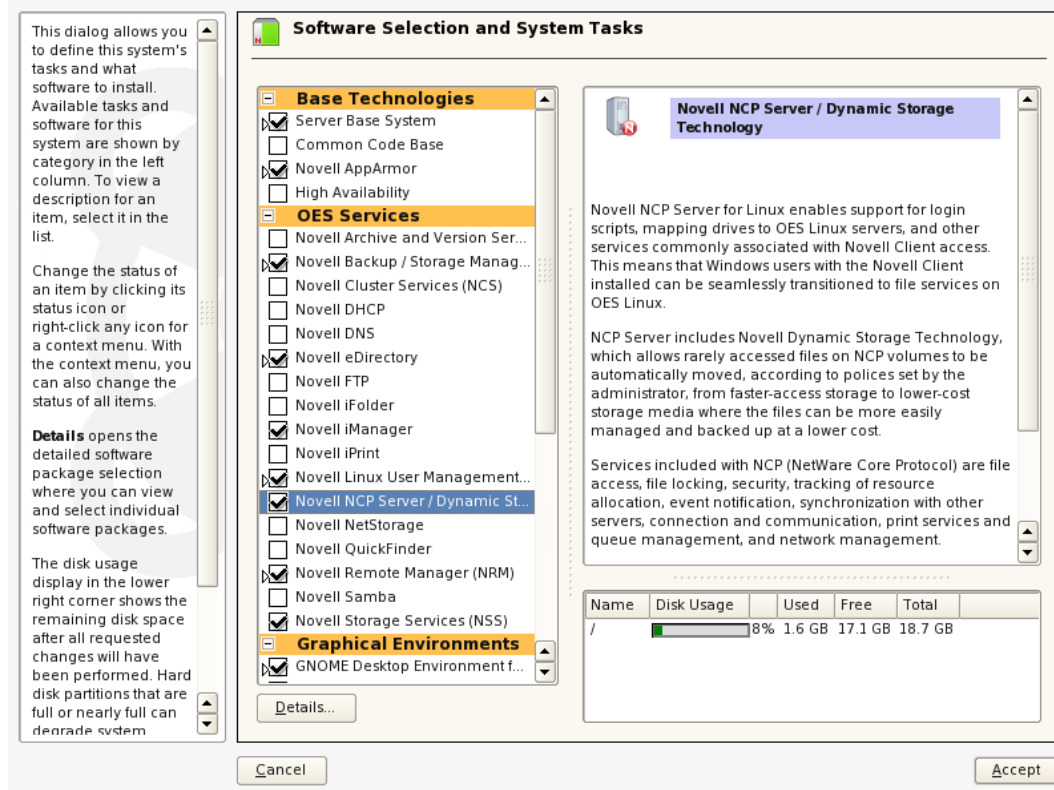
- 5 If you plan to configure DST shadow volumes on a cluster node, select *Novell Cluster Services (NCS)* from the *OES Services* options.

For detailed information about configuring cluster settings during the install for Novell Cluster Services for Linux, see “[Installing and Configuring Novell Cluster Services](#)” in the *OES 2 SPI: Novell Cluster Services 1.8.5 for Linux Administration Guide*.

- 6 If you plan to provide access to DST shadow volumes for CIFS/Samba users, select *Novell Samba* from the *OES Services* options.

For detailed information about configuring Samba services during the install

- 7 Click *Accept* to continue with the installation.



4.2.2 Installing on an Existing OES 2 Linux Server

You can install NCP Server and Dynamic Storage Technology at any time after the initial OES 2 Linux install. Make sure to select the following options, just as you would for a new install:

- ♦ *Novell Backup / Storage Management Services*
- ♦ *Novell eDirectory*
- ♦ *Novell Cluster Services (NCS)* (This is required only when installing DST on a cluster node.)
- ♦ *Novell iManager* (If it is not installed on this server, you must install iManager 2.7 somewhere in the network.)
- ♦ *Novell Linux User Management*
- ♦ *Novell NCP Server / Dynamic Storage Technology*
- ♦ *Novell Remote Manager (NRM) for Linux*
- ♦ *Novell Samba* (This is required only for CIFS/Samba users.)
- ♦ *Novell Storage Services*

For general instructions for installing and configuring OES 2 components on an existing OES 2 Linux server, see “[Installing or Configuring OES 2 Services on an Existing OES 2 SP1 Linux or SLES 10 SP2 Server](#)” in the *OES2 SP1: Linux Installation Guide*.

4.2.3 Configuring Global Policies for DST

- 1 Configure global policies for DST. Global policies apply to all DST shadow volumes on the server.

For information about DST global policies, see the following:

- ♦ [Section 4.4, “Configuring a Global Policy that Replicates Branches of the Primary File Tree in the Shadow File Tree,” on page 46](#)
- ♦ [Section 4.5, “Configuring Global Policies for Shifting Files from the Shadow File Tree to the Primary File Tree,” on page 47](#)
- ♦ [Section 4.6, “Configuring Global Policies for Resolving Instances of Duplicate Files,” on page 51](#)
- ♦ [Section 4.7, “Configuring a Global Policy to Automatically Load ShadowFS at Boot Time,” on page 56](#)

4.3 Installing NCP Server and Dynamic Storage Technology on Nodes in a Novell Cluster Services for Linux Cluster

NCP Server and Dynamic Storage Technology software are not cluster aware. They must be installed on every OES 2 Linux node in the cluster where you plan to migrate or fail over the cluster resource that contains shadow volumes. You do not cluster NCP Server or DST services.

- 1 For each node in the OES 2 Linux cluster, install NCP Server and Dynamic Storage Technology along with Novell Cluster Services for Linux.

For information, see [Section 4.2, “Installing NCP Server and Dynamic Storage Technology,” on page 42](#).

For detailed information about installing Novell Cluster Services for Linux, see “[Installing and Configuring Novell Cluster Services](#)” in the *OES 2 SP1: Novell Cluster Services 1.8.5 for Linux Administration Guide*.

- 2 On each node in the OES 2 Linux cluster, configure the DST global policies with the same settings. Global policies apply to all DST shadow volumes on the server.

IMPORTANT: Whenever you modify global policies on a given node in the cluster, you must make those same changes on the other nodes.

For information about DST global policies, see the following:

- ♦ [Section 4.4, “Configuring a Global Policy that Replicates Branches of the Primary File Tree in the Shadow File Tree,” on page 46](#)
- ♦ [Section 4.5, “Configuring Global Policies for Shifting Files from the Shadow File Tree to the Primary File Tree,” on page 47](#)

- ♦ [Section 4.6, “Configuring Global Policies for Resolving Instances of Duplicate Files,” on page 51](#)
 - ♦ [Section 4.7, “Configuring a Global Policy to Automatically Load ShadowFS at Boot Time,” on page 56](#)
- 3 Set up the shadow volume and its volume-level policies on the first node in the cluster, then copy its DST information to all nodes in the cluster where you want to fail over the cluster resource.
- For information, see [Chapter 11, “Configuring DST Shadow Volumes with Novell Cluster Services for Linux,” on page 133](#).

4.4 Configuring a Global Policy that Replicates Branches of the Primary File Tree in the Shadow File Tree

When a new subdirectory is created, the folder is created in the primary file tree. A configurable option called *Replicate Primary Tree to Shadow* determines whether a matching path is automatically created at that time, or later when a policy is enforced that actually moves data in the folder to the secondary location. By default, the branches are not created in the shadow file tree until they are needed. Performance is better when the branches are created only as needed.

IMPORTANT: If you use shadow volumes in a cluster, make sure to set the same global policies on each OES 2 Linux node in the cluster.

Valid settings for the Replicate Primary Tree to Shadow are:

- ♦ **Disabled (0, default):** Branches of the primary file tree are replicated to the shadow file tree as needed when data is moved from the primary storage area to the secondary storage area.
- ♦ **Enabled (1):** Branches of the primary file tree are replicated to the shadow file tree immediately as they are created on the primary file tree, even if they do not currently contain data in the secondary storage location. Paths in the primary file tree and secondary file tree are the same at all times.

To configure the Replicate Primary Tree to Shadow parameter:

- 1 Log in as the `root` user to Novell Remote Manager.
- 2 Select *Manage NCP Services > Manage Server* to view the *Server Parameter Information*.
- 3 Click the link for the `REPLICATE_PRIMARY_TREE_TO_SHADOW` setting.
- 4 In *New Value*, do one of the following:
 - ♦ **Disable Immediate Path Replication:** Type 0 to replicate paths in the shadow file tree as they are needed when the data is actually moved to the secondary storage area.
 - ♦ **Allow Immediate Path Replication:** Type 1 to replicate all paths in the shadow file tree immediately as they are created on the primary file tree.
- 5 Click *Change*.
- 6 On the *Server Parameter Information* page, verify that the new setting is displayed for the `REPLICATE_PRIMARY_TREE_TO_SHADOW` parameter.

For information about using the SET command to modify this global policy, see [Section A.4, “Configuring Global DST Policies by Using the SET Command,”](#) on page 163.

4.5 Configuring Global Policies for Shifting Files from the Shadow File Tree to the Primary File Tree

You can configure global policies for how files in the shadow file tree are migrated to the primary volume. By default, files are shifted back to the primary if they are modified, but not if they are accessed.

- ♦ [Section 4.5.1, “Understanding Shift Parameters,”](#) on page 47
- ♦ [Section 4.5.2, “Configuring a Global Policy for Shifting Modified Shadow Files,”](#) on page 49
- ♦ [Section 4.5.3, “Configuring a Global Policy for Shifting Accessed Shadow Files,”](#) on page 50
- ♦ [Section 4.5.4, “Configuring a Global Policy for the Days Since Last Access,”](#) on page 50
- ♦ [Section 4.5.5, “Using the SET Command to Set Global Policies,”](#) on page 51

4.5.1 Understanding Shift Parameters

You can control how files are shifted from the secondary storage area to the primary storage area by configuring three shift parameters:

- ♦ Shift Modified Shadow Files
- ♦ Shift Accessed Shadow Files
- ♦ Shift Days Since Last Access

IMPORTANT: If you use shadow volumes in a cluster, make sure to set the same global policies on each OES 2 Linux node in the cluster.

This section describes the parameters, and recommends combinations of the policies to achieve different goals.

- ♦ [“Shift Modified Shadow Files”](#) on page 47
- ♦ [“Shift Accessed Shadow Files”](#) on page 48
- ♦ [“Shift Days Since Last Access”](#) on page 48
- ♦ [“Use Cases for Shifting Shadow Files”](#) on page 49

Shift Modified Shadow Files

When files in the shadow file tree are modified, a configurable global policy called *Shift Modified Shadow Files* allows the files to be moved to the primary file tree (default), or kept in the shadow file tree. When this parameter is enabled, the file is automatically moved back to the primary storage area when the file is closed. This global policy applies to all DST shadow volumes on a given server.

Valid settings for the Shift Modified Shadow Files are:

- ♦ **Disabled (0):** When a file that resides on the secondary storage area is modified, it remains on the secondary storage area.
- ♦ **Enabled (1, default):** If a file that resides on the secondary storage area is modified, it is automatically shifted to the primary storage area after it is closed. The file remains on the primary storage area until a policy is enforced that shifts it to the secondary storage area.

For example, if your policy is to place newer files in the primary file tree and to place older files in the shadow file tree, you want an older file in the secondary file tree to move to primary file tree if the file's content is modified. The Shift Modified Shadow Files parameter is enabled by default, so this is the default behavior.

On the other hand, if you are placing files of one type (such as .doc and .ppt) in the primary area and files of a different type (such as .mp3 and .jpg) in the secondary area, you want files to stay where they are whenever they are modified. In this case, you want to disable the Shift Modified Shadow Files parameter.

Shift Accessed Shadow Files

When files in the shadow file tree are accessed (but not changed), a configurable global policy called *Shift Accessed Shadow Files* allows the files to be left in the shadow file tree (default), or to be moved to the primary file tree. When this parameter is enabled, a file is shifted if it is accessed as read-only a second time during a specified period of time. The file is automatically moved back to the primary area when the file is closed. By default, the period of time is 1 day. Use the Shift Days Since Last Access parameter to specify the period of time. This global policy applies to all DST shadow volumes on a given server.

Valid settings for the Shift Accessed Shadow Files are:

- ♦ **Disabled (0, default):** When a file that resides on the secondary storage area is accessed twice in the specified period, it remains on the secondary storage area.
- ♦ **Enabled (1):** If a file that resides on the secondary storage area is accessed twice in the specified period, it is automatically shifted to the primary storage area after it is closed. The file remains on the primary storage area until a policy is enforced that shifts it to the secondary storage area.

For example, if you are placing files that are changing in the primary area and files that are not changing in the secondary area, you want files to stay where they are whenever they are accessed but not changed. The Shift Accessed Shadow Files parameter is disabled by default, so this is the default behavior.

On the other hand, if your policy is to place in-use files in the primary file tree and to place unused files in the shadow file tree, you want an in-use file in the secondary file tree to move to primary file tree if the file is accessed, whether it changes or not. In this case, you want to enable the Shift Accessed Shadow Files parameter.

Shift Days Since Last Access

The Shift Days Since Last Access parameter specifies the number of days to use when determining if a file should be moved back to the primary storage area. When it is used with `SHIFT_ACCESSSED_SHADOW_FILES`, the parameter sets the time when files are migrated back to the primary storage area after the second access within the specified elapsed time.

Valid settings for the Shift Accessed Shadow Files are:

- ♦ **Disabled (0):** Files are not shifted on access.
- ♦ **Number of Days (1 to 365):** If a file that resides on the secondary storage area is accessed twice in the specified period, it is automatically shifted to the primary storage area after it is closed. The default is 1 day.

Use Cases for Shifting Shadow Files

Table 4-1 describes use cases for shifting files based on the global policies.

Table 4-1 *Shift Behaviors for Files in the Shadow File Tree*

	Don't Shift Modified Shadow File to Primary	Shift Modified Shadow File to Primary (Default)
Don't Shift Accessed Shadow File to Primary (Default)	<p>Files can be modified or accessed without being shifted to the primary file tree.</p> <p>For example, you can separate files by file type, with the less important files in the secondary area. Thereafter, the files remain where you moved them. You can periodically apply volume-level policies that move file types from the primary to the secondary.</p> <p>Back up the primary area more frequently because it contains the most important file types.</p>	<p>Modified files are shifted to the primary file tree, but accessed files are not. This is the default combination.</p> <p>Separate files so that recently modified files are located in the primary area. Older files remain in the secondary area.</p> <p>Back up the primary area more frequently because it contains all of the recently changed files.</p>
Shift Accessed Shadow File to Primary	<p>Files are shifted when they are accessed twice in a specified period, but not when they are modified.</p> <p>No use case exists for this combination.</p>	<p>Files are shifted when they are modified, or if they are accessed twice in a specified period.</p> <p>This is desirable for migration-on-demand solutions that move data gradually from an old volume to a new, higher-performance location.</p> <p>Unchanged, seldom-used files are available to users, but do not require frequent backups.</p>

4.5.2 Configuring a Global Policy for Shifting Modified Shadow Files

To configure the Shift Modified Shadow Files parameter:

- 1 Log in as the `root` user to Novell Remote Manager.
- 2 Select *Manage NCP Services > Manage Server* to view the *Server Parameter Information*.

- 3 Click the link for the `SHIFT_MODIFIED_SHADOW_FILES` setting.
- 4 In *New Value*, do one of the following:
 - ♦ **Disable Modified Files from Shifting to Primary:** Type 0 to keep files on the secondary storage area when they are modified.
 - ♦ **Allow Modified Files to Shift to Primary:** Type 1 to shift files on the secondary storage area to the primary storage area when they are modified. This is the default.
- 5 Click *Change*.
- 6 On the *Server Parameter Information* page, verify that the new setting is displayed for the `SHIFT_MODIFIED_SHADOW_FILES` parameter.

4.5.3 Configuring a Global Policy for Shifting Accessed Shadow Files

To configure the Shift Accessed Shadow Files parameter:

- 1 Log in as the `root` user to Novell Remote Manager.
- 2 Select *Manage NCP Services > Manage Server* to view the *Server Parameter Information*.
- 3 Click the link for the `SHIFT_ACCESSED_SHADOW_FILES` setting.
- 4 In *New Value*, do one of the following:
 - ♦ **Disable Accessed Files from Shifting to Primary:** Type 0 to keep files on the secondary storage area when they are accessed. This is the default.
 - ♦ **Allow Accessed Files to Shift to Primary:** Type 1 to shift files on the secondary storage area to the primary storage area when they are accessed twice during a specified period.
- 5 Click *Change*.
- 6 On the *Server Parameter Information* page, verify that the new setting is displayed for the `SHIFT_ACCESSED_SHADOW_FILES` parameter.

4.5.4 Configuring a Global Policy for the Days Since Last Access

To configure the Shift Days Since Last Access parameter:

- 1 Log in as the `root` user to Novell Remote Manager.
- 2 Select *Manage NCP Services > Manage Server* to view the *Server Parameter Information*.
- 3 Click the link for the `SHIFT_DAYS_SINCE_LAST_ACCESS` setting.
- 4 In *New Value*, do one of the following:
 - ♦ **Disable:** Type 0 to disable this parameter.
 - ♦ **Number of Days:** Type an integer value from 1 to 365 (in days) that specifies the number of days to wait for a second access of a shadow file. If the second access occurs during this period, the file can be moved if the `SHIFT_ACCESSED_SHADOW_FILES` parameter is also enabled.
- 5 Click *Change*.
- 6 On the *Server Parameter Information* page, verify that the new setting is displayed for the `SHIFT_DAYS_SINCE_LAST_ACCESS` parameter.

4.5.5 Using the SET Command to Set Global Policies

For information about using the SET command to modify these global policies, see [Section A.4, “Configuring Global DST Policies by Using the SET Command,”](#) on page 163.

4.6 Configuring Global Policies for Resolving Instances of Duplicate Files

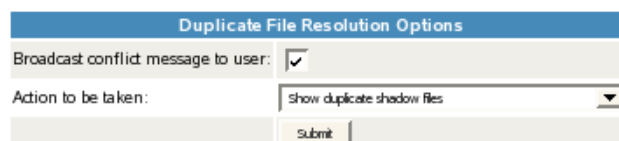
Global DST policies apply to all DST shadow volume pairs on a given server. You might want to change the default policies for how duplicate files are resolved for DST shadow volumes to suit your needs.

- ♦ [Section 4.6.1, “Understanding Conflict Resolution for Duplicate Files,”](#) on page 51
- ♦ [Section 4.6.2, “Configuring Actions to Resolve Duplicate Files Conflicts,”](#) on page 54
- ♦ [Section 4.6.3, “Enabling or Disabling Broadcast Messages for Duplicate Files Conflicts,”](#) on page 54
- ♦ [Section 4.6.4, “Resolving Instances of Duplicate Files in the /._DUPLICATE_FILES Directory,”](#) on page 55

4.6.1 Understanding Conflict Resolution for Duplicate Files

The Duplicate File Resolution policies are designed to handle the case where files with the same name are located in matching subdirectories in both the primary storage location and the secondary storage location. Duplicate files typically are caused by restoring instances of the same file to both the primary storage location and the secondary storage location. If you back up the primary volume more frequently than the secondary volume, the instance of the file that is restored on the primary storage area should be the most current of the two files.

Figure 4-1 Duplicate File Resolution Options (Defaults)



Duplicate File Resolution Options	
Broadcast conflict message to user:	<input checked="" type="checkbox"/>
Action to be taken:	Show duplicate shadow files
<input type="button" value="Submit"/>	

IMPORTANT: If you use shadow volumes in a cluster, make sure to set the same global policies on each OES 2 Linux node in the cluster.

The following global policies can be set to govern handling of duplicate files for all shadow volumes on the server:

- ♦ [“Handling Instances of Duplicate Files”](#) on page 52
- ♦ [“Broadcasting Conflict Messages to NCP Users”](#) on page 53
- ♦ [“Recommended Policy Settings for Duplicate Files Conflict Resolution”](#) on page 53

Handling Instances of Duplicate Files

Table 4-3 describes the options for handling duplicate instances of files. For information about configuring the *Actions to be taken* parameter, see Section 4.6.2, “Configuring Actions to Resolve Duplicate Files Conflicts,” on page 54.

Table 4-2 *Actions for Duplicate File Resolution*

Parameter Options	User View	Resolution
Show duplicate shadow files (default)	The filename appears twice in directory listings.	The administrator or user manually renames one of the files so the system can tell them apart. The user should then determine whether or not to delete one of the instances, and which instance to delete.
Hide duplicate shadow files	Only one instance of the filename is displayed in the directory listings. Client file operations are directed to the instance located on the primary area. If the client deletes the file, the instance in the primary area is deleted, and the instance in the secondary area is then visible.	The users are not aware that a conflict exists. However, the user might see files randomly reappear after they delete a file.
Rename duplicate shadow files	Automatically renames the duplicate file located on the secondary area by adding a unique extension to the name.	Both instances of the file (the file on the primary area and the renamed file on the secondary area) appear in directory listings. The user needs to be informed that such instances might occur so the user can determine which file instance to keep.
Delete duplicate files from the shadow area	Automatically deletes duplicate files located on the secondary storage area.	The users are not aware that a conflict exists. Because duplicate files are typically caused by restoring instances of the same file to both the primary and secondary areas, the instance located on the primary area should be the most current of the two.

Parameter Options	User View	Resolution
Move duplicate shadow files to / ._DUPLICATE_FILES	Causes the duplicate file located on the secondary storage area to be moved to the / ._DUPLICATE_FILES directory at the root of the secondary volume. If there is a filename conflict in the destination directory, then a unique extension is also added to the filename.	The users are not aware that a conflict exists. This option is less risky than automatically deleting duplicate files. It might require occasional cleanup work to be performed in the /._DUPLICATE_FILES directory.

Broadcasting Conflict Messages to NCP Users

DST leverages the broadcast message capability of NCP Server for Linux. You can choose not to broadcast messages when duplicate files are discovered by disabling the broadcast option in DST. If the option is enabled, the messages are received only by client versions that support broadcast messages, and only if the client itself has broadcast messages enabled.

If the option is enabled, whenever duplicate file conflicts occur, a message is broadcast by default to NCP users of the file.

There are two prerequisites for using broadcast messages:

- ♦ **NCP Server:** NCP Server must be configured to support broadcast messages by setting the Disable Broadcast parameter for the SET command to 0 (disabled).
- ♦ **Novell Client:** The Novell Client™ version being used by the NCP users must be capable of receiving broadcast messages, and the client must be configured to receive broadcast messages. The broadcast message capability is called Send Message in the Novell Client. In OES 2 SP1, the Send Message feature is available in the Novell Client 4.91 SP4 for Windows XP/2003, the Novell Client 1.0 SP1 for Vista, and the Novell Client 2.0 for Linux.

For information about configuring the *Broadcast Conflict Messages to Users* parameter, see [Section 4.6.3, “Enabling or Disabling Broadcast Messages for Duplicate Files Conflicts,” on page 54](#).

Recommended Policy Settings for Duplicate Files Conflict Resolution

The settings for broadcasting messages and handling files are configured separately. [Table 4-3](#) summarizes recommendations for combining the two. However, if users are CIFS/Samba users who cannot receive broadcast messages, or if the version of the Novell Client that is in use does not support receiving broadcast messages, you should simply disable broadcast, and select an action that makes sense in your environment.

For information, see [“Handling Instances of Duplicate Files” on page 52](#).

Table 4-3 *Recommended Global Policies for Duplicate Files Resolution*

Action to be Taken	Broadcast Conflict Messages to Users
Show duplicate shadow files (default)	Enable broadcast (default)
Hide duplicate shadow files	Disable broadcast

Action to be Taken	Broadcast Conflict Messages to Users
Rename duplicate shadow files	Optionally enable broadcast
Delete duplicate files from the shadow area	Disable broadcast
Move duplicate shadow files to / ._DUPLICATE_FILES	Disable broadcast

4.6.2 Configuring Actions to Resolve Duplicate Files Conflicts

By default, the *Actions to be taken* parameter is set to show duplicate shadow files to the user. For information about the other options, see [“Handling Instances of Duplicate Files” on page 52](#).

For information about using the SET command to modify this global policy, see [Section A.4, “Configuring Global DST Policies by Using the SET Command,” on page 163](#).

- 1 In Novell Remote Manager for Linux, select *View File System*, then select *Dynamic Storage Technology Options*.
- 2 In the *Duplicate File Resolution Options* area, view the current setting for *Actions to be taken*.

- 3 From the *Actions to be taken* drop-down list, select one of the following options:
 - ♦ *Show duplicate shadow files* (default)
 - ♦ *Hide duplicate shadow files*
 - ♦ *Rename duplicate shadow files*
 - ♦ *Delete duplicate files from shadow area*
 - ♦ *Move duplicate shadow files to / ._DUPLICATE_FILES*
- 4 In the *Duplicate File Resolution Options* area, click *Submit* to save and apply the change.

4.6.3 Enabling or Disabling Broadcast Messages for Duplicate Files Conflicts

When *Broadcast Conflict Messages to Users* is enabled (the default setting), a message is broadcast to NCP users of the file when duplicate instances of the file occur on the primary storage location and secondary storage location. For information, see [“Broadcasting Conflict Messages to NCP Users” on page 53](#) and [“Recommended Policy Settings for Duplicate Files Conflict Resolution” on page 53](#).

IMPORTANT: In order for users to be able to receive the duplicate-file-conflict messages, NCP Server must be configured to support broadcast messages and the Novell clients must be configured to receive broadcast messages. For instructions, see [“Enabling or Disabling Broadcast Message Support” in the OES 2 SP1: NCP Server for Linux Administration Guide](#).

For information about using the SET command to modify this global policy, see [Section A.4, “Configuring Global DST Policies by Using the SET Command,”](#) on page 163.

- 1 In Novell Remote Manager for Linux, select *View File System*, then select *Dynamic Storage Technology Options*.
- 2 In the *Duplicate File Resolution Options* area, enable or disable *Broadcast Conflict Messages to Users* by selecting or deselecting the check box next to it. It is enabled by default.

- 3 In the *Duplicate File Resolution Options* area, click *Submit* to save and apply the change.
- 4 If you enabled Broadcast Conflict Messages, make sure that NCP Server is configured to support broadcast messages by verifying that the Disable Broadcast (DISABLE_BROADCAST) parameter for the SET command is disabled.
 - 4a In Novell Remote Manager for Linux, select *Manage NCP Services*, then select *Manage Server*.
 - 4b In the *Set Parameter Information* table, locate the DISABLE_BROADCAST parameter, then view the current value of the parameter. By default, the parameter is disabled (set to 0), which means that NCP Server supports broadcast messages.

DISABLE_BROADCAST	0
-------------------	-------------------

- 4c If the DISABLE_BROADCAST parameter is enabled (set to 1), click the link for the value in the *Parameter Value* column to open a page where you can change the value.

DISABLE_BROADCAST	1
-------------------	-------------------

- 4d In *New Value*, type 0, then click *Change* to save and apply the settings that disable the DISABLE_BROADCAST parameter, which enables broadcasting for NCP Server.

IMPORTANT: Messages are received only by logged-in users who are using Novell Client versions that are capable of receiving broadcast messages, and that are configured to receive them.

4.6.4 Resolving Instances of Duplicate Files in the / ._DUPLICATE_FILES Directory

If you enable *Move duplicate shadow files to / ._DUPLICATE_FILES* as the action to be taken when duplicate file conflicts occur, it might require occasional cleanup work to be performed in the / ._DUPLICATE_FILES directory.

4.7 Configuring a Global Policy to Automatically Load ShadowFS at Boot Time

ShadowFS and FUSE must be running in order for Samba/CIFS users to see a unified view of the shadow volume tree. By default, ShadowFS and FUSE are installed when you install NCP Server and Dynamic Storage Technology. They are not started unless you start them manually, or you set a global policy for *ShadowFS Configuration* that starts them at boot time. For information about using and managing ShadowFS, see [Chapter 5, “Installing and Configuring Shadow File System \(ShadowFS\) for CIFS/Samba Users,”](#) on page 59.

IMPORTANT: If you use shadow volumes in a cluster, make sure to set the same global policies on each OES 2 Linux node in the cluster.

- 1 In Novell Remote Manager for Linux, select *View File System*, then select *Dynamic Storage Technology Options*.
- 2 In the *ShadowFS Configuration* area, view the current setting for *Load ShadowFS at Boot Time*.



- 3 Enable or disable *Load ShadowFS at Boot Time* by selecting or deselecting the check box.
- 4 In the *ShadowFS Configuration* area, click *Submit* to save and apply the change.

4.8 Restarting the Novell NCP/NSS IPC (ncp2nss) Daemon

If NSS is installed, NCP Server runs the Novell NCP/NSS IPC (`/etc/init.d/ncp2nss`) daemon in order to synchronize its settings with NSS. When you modify NCP Server settings by using Novell Remote Manager for Linux, NCP Server automatically restarts `ncp2nss` so that the new settings are immediately synchronized with NSS. If you modify values for any of the DST global parameters for NCP Server by directly editing the `/etc/opt/novell/ncpserv.conf` file, you must manually restart `ncp2nss`.

- 1 On the OES 2 Linux server, open a terminal console, then log in as the `root` user.
- 2 At the terminal console prompt, enter
- 3 If `ncp2nss` restarts successfully, the following messages are displayed in the terminal console:

```
Shutting down Novell NCP/NSS IPC daemon...
```

```
Exited
```

```
Starting the Novell NCP/NSS IPC daemon.
```


4.9 Restarting the Novell eDirectory (ndsd) Daemon

When you modify NCP Server settings by using Novell Remote Manager for Linux, NCP Server automatically restarts the Novell eDirectory daemon to apply the new settings. If you modify values for any of the DST global parameters for NCP Server by directly editing the `/etc/opt/novell/ncpserv.conf` file, you must restart the Novell eDirectory daemon to make the changes go into effect.

Use the following steps to stop and start `ndsd` when a single instance is running. For information about stopping and starting `ndsd` when you are running multiple instances of it on the same server, see “[Managing Multiple Instances](#)” in the *Novell eDirectory 8.8 What*.

IMPORTANT: Restarting or stopping `ndsd` automatically disconnects all user connections and does not warn users before the connection is broken. Users can reconnect to the server after the service starts.

- 1 Use one of the following commands to stop `ndsd`:

```
rcndsd stop
```

```
/etc/init.d/ndsd stop
```

- 2 Use one of the following commands to start `ndsd`:

```
rcndsd start
```

```
/etc/init.d/ndsd start
```


Installing and Configuring Shadow File System (ShadowFS) for CIFS/Samba Users

This section describes how to provide a unified view of the Dynamic Storage Technology (DST) shadow volume for your CIFS/Samba users by using the Shadow File System (ShadowFS) component.

- ♦ [Section 5.1, “Understanding ShadowFS,” on page 59](#)
- ♦ [Section 5.2, “Prerequisites for Using ShadowFS,” on page 60](#)
- ♦ [Section 5.3, “Preparing Your System for Using ShadowFS,” on page 60](#)
- ♦ [Section 5.4, “Installing ShadowFS and FUSE,” on page 61](#)
- ♦ [Section 5.5, “Setting Rights to ShadowFS Shares,” on page 62](#)
- ♦ [Section 5.6, “Creating a Samba Share,” on page 63](#)
- ♦ [Section 5.7, “Adding a User to Samba,” on page 63](#)
- ♦ [Section 5.8, “Connecting Users to the Share,” on page 64](#)
- ♦ [Section 5.9, “Testing Shadow Volume Policies,” on page 64](#)
- ♦ [Section 5.10, “Enabling or Disabling ShadowFS to Load at Boot Time,” on page 65](#)
- ♦ [Section 5.11, “Starting and Stopping ShadowFS Manually,” on page 65](#)
- ♦ [Section 5.12, “Configuring Trustee Rights for CIFS/Samba Users,” on page 67](#)

5.1 Understanding ShadowFS

ShadowFS provides a virtual view of the shadow volume, and allows users to access the primary storage area by using the CIFS/Samba protocol instead of the NetWare® Core Protocol™ (NCP™).

IMPORTANT: Performance for CIFS/Samba clients to access data via ShadowFS is slower than what NCP clients see.

The ShadowFS technology was implemented on the FUSE (File Systems in Userspace) virtual file system. FUSE is an open source software package that is delivered in OES 2 Linux, and is installed automatically when you install Dynamic Storage Technology.

When ShadowFS loads, it checks the `/etc/NCPVolumes` file to see what NCP shadow volumes exist, then it automatically creates a local mount point in `/media/shadowfs/volumename` that presents a unified file tree that includes both volumes. This local mount point allows Samba and other local applications (including backup utilities) to see the same combined view that NCP clients see when they access a shadow volume. Each instance of ShadowFS runs as a separate process.

The ShadowFS configuration file is `/etc/opt/novell/shadowfs.conf`.

The ShadowFS log file is `/var/opt/novell/log/shadowfs.log`.

5.2 Prerequisites for Using ShadowFS

- ❑ Before using ShadowFS, make sure that the following services have been installed and configured:

- ♦ NCP Server and Dynamic Storage Technology
- ♦ Novell® eDirectory™
- ♦ Novell Samba
- ♦ Linux User Management
- ♦ FUSE
- ♦ Novell Remote Manager for Linux
- ♦ Novell iManager for Linux

For information about these services, see [Section 4.1, “Installation Requirements for Dynamic Storage Technology,” on page 39](#).

- ❑ There must be at least one functional shadow volume on the server that is mounted in NCP. For information, see [Section 8.4, “Creating a DST Shadow Volume with NSS Volumes,” on page 94](#).

5.3 Preparing Your System for Using ShadowFS

Prepare your system for using ShadowFS:

- 1 Verify that Samba services are functioning properly:

- ♦ Samba server is running.
- ♦ Shares can be created.
- ♦ Users can access Samba shares.

Use the Samba plug-in for iManager to configure and verify Samba services. In iManager, go to the *File Protocols > Samba > General* page with the server selected.

- 2 Linux-enable users with Linux User Management.

Users must be Linux-enabled through Linux User Management in order to access data via CIFS/Samba.

The users must be members of a primary group that is Linux-enabled on the target server or workstation object where both the Primary Group ID and Primary Group Name are assigned to the user. This is the primary group that is later assigned rights to the Samba share. Only primary groups can be assigned as the Directory group for the Samba share.

Use the Linux User Management plug-in for iManager to Linux-enable users. To verify Linux-enabled users, go to the *Modify User > Linux Profile > General* page with the server selected. Make sure that the values match to the users' Group Assignment.

IMPORTANT: You must Linux-enable users before adding a Samba Password policy assignment for the Samba server. If you attempt to add a user to a group, and the user is not already Linux-enabled, you cannot continue.

- 3 Make sure users have a Samba Password policy assignment at the eDirectory user, group or container level.
- 4 Make sure users have a Universal Password.

Users must have a Universal Password set in order for Samba to work properly.

5 Linux-enable the group with Linux User Management.

You must assign a Unix Workstation object for the group. To verify, use iManager, to go to the *Modify Group > Linux Profile > General* page, confirm that the *Enable Linux Profile* option is enabled, and confirm that a *Unix Workstation* object is assigned and has a Group ID.

NOTE: For the purposes of testing, you can PAM-enable services on the server, so that test users can SSH into the server and validate access to directory paths to shares, and so on. For information about configuring SSH for a user, see *SSH Services on OES 2 Linux* in the *OES 2 SPI: Planning and Implementation Guide*.

5.4 Installing ShadowFS and FUSE

ShadowFS and FUSE are installed automatically when you install Dynamic Storage Technology. The following instructions are provided in case you need to install it manually.

- 1 Open YaST as the `root` user.
- 2 In YaST, select *Software Management*.
- 3 In *Software Management*, search for *shadow* to find the `novell-shadowFS` package.
- 4 Select *novell-shadowFS*, click *Install*, click *Accept* to install it, then when prompted, accept its dependencies (such as FUSE).
- 5 Load FUSE by entering the following at a terminal console as the `root` user:

```
cd /opt/novell/ncpserv/sbin
modprobe fuse
```

There is no command line feedback to indicate if the command is successful.

- 6 Start ShadowFS by entering the following at a terminal console as the `root` user:

```
/opt/novell/ncpserv/sbin ./shadowfs
```

IMPORTANT: Make sure you run only a single instance of `shadowfs` at a time. Avoid entering the command multiple times.

For example, if the primary storage location is an NSS volume named `VOL1` and the secondary storage location is an NSS volume named `ARCVOL`, the output would look similar to this:

```
SHIFT_ON_MODIFY: 1
SHIFT_ON_ACCESS: 0
SHIFT_DAYS_SINCE_LAST_ACCESS: 1
Primary Tree 0: /media/nss/VOL1
Shadow Tree 0: /media/nss/ARCVOL
shadowfs root 0: /media/shadowfs/VOL1
```

Loading ShadowFS creates the ShadowFS root volume `/media/shadowfs/VOL1` where it creates the ShadowFS volumes. If multiple NCP volumes have shadow volumes, each of them are shadowed with ShadowFS and are reported. You cannot control whether to shadow only one or some of them.

5.5 Setting Rights to ShadowFS Shares

Grant POSIX rights for users so they can access files on the ShadowFS volume via the CIFS/Samba protocol. Rights are granted based on need. You set rights so that users can read, write, and execute in the ShadowFS volume's root location in the `/media/shadowfs` directory. Do not set POSIX rights to the actual NCP shares for the primary and secondary volumes.

- 1 Open a terminal console, then log in as the `root` user.
- 2 Go to the ShadowFS volume root location of `/media/shadowfs` by entering the following at the terminal prompt:

```
cd /media/shadowfs
```

- 3 Set directory ownership for the group-level access to the ShadowFS volume root by entering the following:

```
chown :groupname shadowfs_volumename
```

For example, if the *groupname* is `marketing` and the *shadowfs_volumename* is `USERS`, enter

```
chown :marketing USERS
```

- 4 Set POSIX rights for the directory group by entering the following:

```
chmod mode shadowfs_volumename
```

For example, to grant POSIX read, write, and execute permissions for the user and group levels, and to set read and execute only for the others (world) level, set the *mode* to `775` by entering:

```
chmod 775 USERS
```

You are setting directory rights for `/media/shadowfs/USERS` as `drwxrwxr-x`.

- 5 Visually verify POSIX rights by entering

```
ll
```

Continuing the example, the results should look like this:

```
drwxrwxr-x  3 root marketing  80 May 16 15:48 USERS
```

- 6 Verify that the CIFS/Samba user can access the ShadowFS volume and can create directories.

6a Decide which user identity you want to use to test the setup. For example, you could assign the admin user as a user of the CIFS/Samba group, or use iManager to create a temporary user identity for a test user in the group.

6b Use iManager to make sure the test user is Linux-enabled with Linux User Management, and grant the user SSH rights for accessing the server.

For information about configuring SSH for a user, see “[SSH Services on OES 2 Linux](#)” in the *OES 2 SP1: Planning and Implementation Guide*.

6c Use iManager to set eDirectory permissions on the volume or path for the test user.

6d Use Secure Shell (SSH) to log in to the volume as a user in the group.

For example, `ssh` to the server and log in:

```
ssh username@server.context.com
```

```
password:*****
```

- 6e** Go to the ShadowFS volume location by entering

```
cd /media/shadowfs/USERS
```

The user should be able to `cd` to and see the directory. If not, recheck the preceding steps to make sure you followed the steps correctly.

- 6f** As the user, create a directory. For example, enter

```
mkdir username
```

If the directory `/media/shadowfs/USERS/username` is created, the rights are working as expected.

5.6 Creating a Samba Share

Create a Samba share that points to the newly created ShadowFS root, so that users can access it. Rights need not be set at the Primary and Shadow volumes themselves, unless they are not visible or accessible to the user or group assignment.

- 1** Log in to iManager as the administrator user.
- 2** In iManager, click *File Protocols > Samba > Shares*.
- 3** Select a server to manage.
- 4** On the *Shares* page, click *New*.
- 5** Specify the following information:
 - ♦ **Share name:** Specify a share name that does not conflict with existing shares that are defined in the `smb.conf` file. To continue earlier examples in this section, `USERS` has been used, so the Samba share name must differ. For example, `usertest`.
 - ♦ **Path:** Specify the context-sensitive path of the ShadowFS root location for the `USERS` volume, such as `/media/shadowfs/USERS`.
 - ♦ **Comment:** Specify a description of the share, such as “User file storage for Windows users.”
 - ♦ **Inherit ACLs:** Enable this option to allow POSIX inheritance of access control lists and rights.
- 6** Click *Finish* to create the Samba share.

If the share is created successfully, it is listed on the *Shares* page.

5.7 Adding a User to Samba

If Linux-enabled users who need access are not already added to Samba, add them to the Samba server.

- 1** Log in to iManager as the administrator user.
- 2** In iManager, click *File Protocols > Samba > Shares*.
- 3** Select a server to manage, then click the *Users* tab.
- 4** On the *Shares > Users* page, click *Add*, then locate and select the users you want to add to Samba.

If a user is added successfully, the username is listed on the *Users* page. The user should be listed with the default Samba user group *hostname-W-SambaUserGroup* and with the primary Linux-enabled user group to which the user was added earlier.

Users are automatically added to *hostname-W-SambaUserGroup* when they are added as Samba users via the Samba Management plug-in for iManager. If a user is already a member of another Linux-enabled group, adding the user to Samba adds the Samba group as the user's primary group.

If the user's previous primary group gave the user specific access to PAM-enabled services, the user likely loses those access rights, because the default Samba group gives users no rights to any PAM-enabled services. If this occurs, you can remove the user from the default Samba user group and reassign the user back to his or her previous primary group. This is done by modifying the user's properties.

- 5 If you need to modify a user's properties, go to *User > Modify > Linux Profile*, and change the *Primary Group Name* back to the previous group name. This also changes the *Primary Group ID*.
- 6 If you encounter problems with Samba, you can start, stop, or restart the Samba server from the *File Protocols > Samba > Shares > General* page.

5.8 Connecting Users to the Share

At this point, the Samba share users should be able to attach to server from a Windows client or other CIFS/SMB client. The procedure in this section explains the steps for a Windows client.

- 1 Using Windows XP, open *My Network Places*.
- 2 Select *Add Network Place*, then click *Next*.
- 3 Select *Choose another network location*, then click *Next*.
- 4 Type the location as `\\servername\Samba_sharename` (such as `\\svr1\usertest`), then click *Next*.

Connecting to the server can take a few seconds to minutes, depending on network speed, discovery of server and share, and so on.

- 5 When prompted, enter your username (DN only, not FDN) and password.
- 6 Specify the name of this network place, or use the default place name, then click *Next*.
- 7 Enable *Open this network place when I click Finish*, then click *Finish*.

If the connection is good, an Explorer window opens for the mapped location.

- 8 Make sure the rights are working by creating a new folder (right-click, then select *New > Folder*).

If the user can create a folder, rights are working.

5.9 Testing Shadow Volume Policies

If you are not familiar with policies on shadow volumes, you should test them against a test data set to understand how to use them to your advantage.

Add files of several different types to the new share, then either create a DST policy to move the files, or do an inventory to search for specific file types, then move them to the shadow.

SSH in as the user, or root, and look at the primary, shadow, and shadowfs root paths to see if things are where you expect them to be.

5.10 Enabling or Disabling ShadowFS to Load at Boot Time

By default, ShadowFS and FUSE are not started unless you start them manually. You can set a global policy for *ShadowFS Configuration* that starts them at boot time.

IMPORTANT: If you use shadow volumes in a cluster, make sure to set the same global policies on each OES 2 Linux node in the cluster.

- ♦ [Section 5.10.1, “Verifying ShadowFS Commands in the init.d Script,” on page 65](#)
- ♦ [Section 5.10.2, “Loading ShadowFS and FUSE at Boot Time,” on page 65](#)

5.10.1 Verifying ShadowFS Commands in the init.d Script

In *ShadowFS Configuration* on the Dynamic Storage Technology page, you can enable the *Load ShadowFS at Boot Time* check box to execute the `init.d` script. This puts the commands `shadowfs` and `fuse` startup commands in the boot sequence.

You can verify that the commands are available by viewing the script in a text editor. The following lines should be in the `init.d` script:

```
modprobe fuse
/opt/novell/ncpserv/sbin/shadowfs
```

5.10.2 Loading ShadowFS and FUSE at Boot Time

- 1 In Novell Remote Manager for Linux, select *View File System*, then select *Dynamic Storage Technology Options*.
- 2 In the *ShadowFS Configuration* area, view the current setting for *Load ShadowFS at Boot Time*.



This command executes the `init.d` script, which puts the necessary commands in the boot sequence.

- 3 Enable or disable *Load ShadowFS at Boot Time* by selecting or deselecting the check box.
- 4 In the *ShadowFS Configuration* area, click *Submit* to save and apply the change.

5.11 Starting and Stopping ShadowFS Manually

FUSE and ShadowFS are required when users are accessing NSS volumes via Samba/CIFS. If FUSE or ShadowFS stop running, you must start them manually. Only one instance of `shadowfs` should be running at a time.

5.11.1 Starting FUSE and ShadowFS

- 1 On the server, open a terminal console, then log in as the `root` user.
- 2 At the terminal console prompt, start FUSE by entering

```
cd /opt/novell/ncpserv/sbin
modprobe fuse
```

There is no command line feedback to indicate if the command is successful.

- 3 At the terminal console prompt, start ShadowFS by entering

```
/opt/novell/ncpserv/sbin ./shadowfs
```

The output identifies the primary volume, secondary volume, and the shadowfs volume.

For example, if the primary storage location is an NSS volume named `VOL1` and the secondary storage location is an NSS volume named `ARCVOL`, the output would look similar to this:

```
SHIFT_ON_MODIFY: 1
SHIFT_ON_ACCESS: 0
SHIFT_DAYS_SINCE_LAST_ACCESS: 1
Primary Tree 0: /media/nss/VOL1
Shadow Tree 0: /media/nss/ARCVOL
shadowfs root 0: /media/shadowfs/VOL1
```

Loading ShadowFS creates the ShadowFS root volume `/media/shadowfs/VOL1` where it creates the ShadowFS volumes. If multiple NCP volumes have shadow volumes, each of them are shadowed with ShadowFS and are reported. You cannot control whether to shadow only one or some of them.

5.11.2 Starting FUSE and ShadowFS with novell-shadowfs

- 1 On the server, open a terminal console, then log in as the `root` user.
- 2 At the terminal console prompt, start FUSE and ShadowFS by entering

```
/etc/init.d/novell-shadowfs start
```

5.11.3 Stopping Shadowfs

- 1 On the server, open a terminal console, then log in as the `root` user.
- 2 At the terminal console prompt, stop the shadowfs process by entering

```
/etc/init.d/novell-shadowfs stop
```

If the process does not stop, you need to kill the process. Enter

```
killall shadowfs
```

5.12 Configuring Trustee Rights for CIFS/Samba Users

When using ShadowFS to provide a unified view to CIFS/Samba users, access is still controlled by the Novell trustee model for user access. You must use NCP rights management tools to set trustees, just as you do for NCP clients. You must use the Files and Folders plug-in to iManager 2.7, the Novell Client, or the `ncpcon rights` command to set trustees, trustee rights, and inherited rights filters for files and folders.

Using Dynamic Storage Technology in a Virtual Environment

Dynamic Storage Technology (DST) for Novell® Open Enterprise Server (OES) 2 Linux works similarly on a native hardware environment as on a virtual machine, with the following caveats:

- ♦ DST supports up to 16 shadow volumes and up to 16 ShadowFS volumes in a virtualized guest server environment.
- ♦ DST is not supported for use in the virtualization host server environment.

Xen* limits for the number of devices assigned to a virtual machine:

- ♦ **Para-virtualized:** 16 devices
- ♦ **Fully virtualized:** 4 devices

To get started with virtualization, see *SUSE Linux Enterprise Server 10 SP2: Virtualization with Xen* (http://www.novell.com/documentation/sles10/xen_admin/data/bookinfo.html)

For information on setting up NetWare on a Xen-based virtual guest server, see “**Installing and Managing OES 2 SP1 NetWare on a Xen-based VM Host Server**” in the *OES 2 SP1: NetWare Installation Guide*.

For information on setting up OES 2 Linux on a Xen-based virtual guest server, see “**Installing, Upgrading, or Updating OES 2 SP1 Linux on a Xen-based Virtual Machine**” in the *OES2 SP1: Linux Installation Guide*.

Management Tools for Dynamic Storage Technology

7

This section provides an overview of the management tools for Dynamic Storage Technology (DST) in Novell® Open Enterprise Server (OES) 2 Linux.

- [Section 7.1, “Dynamic Storage Technology Tasks in Novell Remote Manager for Linux,” on page 71](#)
- [Section 7.2, “NCP Console \(NCPCON\) Commands,” on page 75](#)
- [Section 7.3, “Management Tools for NSS Volumes,” on page 75](#)
- [Section 7.4, “Management Tools for Clustering,” on page 75](#)

7.1 Dynamic Storage Technology Tasks in Novell Remote Manager for Linux

The volume options allow you to create a shadow volume or add a volume shadow to an existing NetWare® Core Protocol™ (NCP™) volume. You can also remove a shadow from an NCP volume.

- [Section 7.1.1, “Accessing Novell Remote Manager,” on page 71](#)
- [Section 7.1.2, “Starting, Stopping, or Restarting Novell Remote Manager on Linux,” on page 72](#)
- [Section 7.1.3, “Quick Reference for Dynamic Storage Technology Options,” on page 72](#)
- [Section 7.1.4, “Quick Reference for NCP Server Options,” on page 73](#)
- [Section 7.1.5, “Quick Reference for DST Global Policy Settings,” on page 74](#)
- [Section 7.1.6, “Shadow Volume Inventory,” on page 74](#)

7.1.1 Accessing Novell Remote Manager

- 1 In a Web browser, go to the URL of the server that you want to manage.

For example, enter the following in the address (URL) field:

`http://server_IP_address:8008` or `other_configured_port_number`

For example:

`http://192.168.123.11:8008`

`https://192.168.123.11:8009`

- 2 Log in to Novell Remote Manager as the `root` user of the server or as the Novell eDirectory™ administrator user who has sufficient rights to manage the server.

The `root` user logs in as a local user of the server, not through eDirectory. If eDirectory, Linux User Management, or PAM are not working, the `root` user can still log in to NRM to manage the server. The `root` user can always log in directly to the server to manage it.

NRM is PAM-enabled, so any Linux-enabled user can log in. Depending on the user's trustee rights for the server, the user gets access only to the tasks the user has rights to perform.

7.1.2 Starting, Stopping, or Restarting Novell Remote Manager on Linux

Novell Remote Manager on Linux is installed and runs by default. If it hangs, you can use the `/etc/init.d/novell-httpstkd` script to get status or to stop, start, or restart `httpstkd`. For the latest information about `httpstkd`, see “Starting or Stopping HTTPSTKD” in the *OES 2 SP1: Novell Remote Manager for Linux Administration Guide*.

- 1 Open a terminal console, then log in as the `root` user.
- 2 At the terminal console prompt, enter the command for the task you need to perform:

Task	Command
Status	<code>rcnovell-httpstkd status</code>
Start	<code>rcnovell-httpstkd start</code>
Stop	<code>rcnovell-httpstkd stop</code>
Restart	<code>rcnovell-httpstkd restart</code>

7.1.3 Quick Reference for Dynamic Storage Technology Options

Table 7-1 describes the management tasks available for *View File Systems > Dynamic Storage Technology Options* task in Novell Remote Manager for Linux.

Table 7-1 *View File Systems > Dynamic Storage Technology Options*

Subtasks	Management Tasks
Volume Information	<p>View a list of NCP volumes and NSS volumes on the server.</p> <p>Click the <i>Add Shadow</i> link next to an NSS volume to view share information, where you can create a shadow volume. (NCP volumes are not supported as shadow volumes in the initial release.)</p> <p>Click the <i>Inventory</i> link next to a shadow volume to view an inventory report for both the primary and secondary volumes.</p> <p>Click the <i>View Log</i> link next to an NSS volume to download a copy of the audit log for the selected volume.</p>
Add Shadow link	<p>This option takes you to the Share Information page. Scroll down to the <i>Volume Tasks</i> area to find the <i>Add Shadow Volume</i> task.</p> <p>The Share Information page and Add Shadow Volume page do not distinguish or validate whether the volumes you choose are actually supported file systems and available combinations.</p> <hr/> <p>WARNING: NSS volumes must already exist when you create the shadow volume. The <i>Create if not present</i> option is available for future support of NCP volumes on Linux file systems. Do not use this option for NSS volumes.</p>

Subtasks	Management Tasks
Inventory link	View statistics and graphical trend displays for the volume's files and directories. For a DST shadow volume, the report includes information for both the primary storage area (primary area) and the secondary storage area (shadow area).
Volume Information (Info icon)	<p>NCP share information, such as the Linux file system path for the volume, file system type, NCP volume ID, status, capacity, and cache statistics.</p> <p>Open files listed for each NCP connection.</p> <p>Add a shadow volume for the NCP volume.</p> <p>For unmounted DST shadow volumes, click the <i>Info</i> icon to access the dialog to remove the shadow volume relationship. This removes the entry in the <code>ncpserv.conf</code> file, but does not delete the volume itself.</p> <p>To unmount a shadow volume, click <i>Manage NCP Services > Manage Shares</i>, then click <i>Unmount</i> option next to the shadow volume.</p>
Dynamic Storage Technology Policies	<p>Create a new policy.</p> <p>View a list of existing policies.</p> <p>Click the <i>Policy Name</i> link to modify or delete the policy.</p>
Duplicate File Resolution Options	Set a global policy for how to handle duplicate files.
ShadowFS Configuration	Set a global policy for whether to automatically start FUSE and Shadow File System at boot time.

7.1.4 Quick Reference for NCP Server Options

Table 7-2 describes the DST tasks available for the *Manage NCP Services > Manage Shares* task in Novell Remote Manager for Linux. For a complete list of NCP Server management tasks, see “Quick Reference for the NCP Server Plug-In for Novell Remote Manager for Linux” in the *OES 2 SPI: NCP Server for Linux Administration Guide*.

Table 7-2 *Manage NCP Services > Manage Shares*

Subtasks	Management Tasks
NCP/NSS Bindings	In the <i>Configuration</i> area, click <i>NCP/NSS Bindings</i> to view a list of NSS volumes on the server. Set the <i>NCP Available</i> setting to No for NSS volumes that you want to use as secondary storage locations for DST shadow volumes.
Mount/Unmount	Mount or unmount the primary volume for a shadow volume. The primary volume must be unmounted in order to access the Remove Shadow Volumes task.

Subtasks	Management Tasks
Info > Remove Shadow Volume	For unmounted DST shadow volumes, click the <i>Info</i> icon to access the dialog to remove the shadow volume relationship. This removes the entry in the <code>ncpserv.conf</code> file, but does not delete the two volumes and their data.

7.1.5 Quick Reference for DST Global Policy Settings

Table 7-3 describes the DST parameters available for the *Manage NCP Services > Manage Server* task in Novell Remote Manager for Linux. For descriptions of the parameters, see [Section A.4.1, “Understanding DST Parameters for the SET Command,”](#) on page 164.

Table 7-3 *Manage NCP Services > Manage Server > Server Parameter Information*

Parameter Name	Default Value	Valid Values
SHIFT_MODIFIED_SHADOW_FILES	1	0 - Disable 1 - Allow
SHIFT_ACCESSED_SHADOW_FILES	0	0 - Disable 1 - Allow
SHIFT_DAYS_SINCE_LAST_ACCESS	1	0 - Disable 1 to 365 (in days)
DUPLICATE_SHADOW_FILE_ACTION	0	0 - Show duplicate shadow files (default) 1 - Hide duplicate shadow files 2 - Rename duplicate shadow files 3 - Delete duplicate files from shadow area 4 - Move duplicate shadow files to / . _DUPLICATE_FILES
DUPLICATE_SHADOW_FILE_BROADCAST	1	0 - Disable 1 - Allow
REPLICATE_PRIMARY_TREE_TO_SHADOW	0	0 - Disable 1 - Allow

7.1.6 Shadow Volume Inventory

The volume inventory feature detects shadow volumes and displays information from the primary and secondary volumes. The complete inventory profile displays three categories of information: combined areas, primary area, and shadow area. With Novell Remote Manager’s shadow volume

inventory, you can also select files that meet specific criteria (such as files that have not been accessed for two years, files that have not been modified in a year, all .mp3 files, and so on). Use the inventory information to profile each area's files and move them as needed.

7.2 NCP Console (NCPCON) Commands

You can optionally use the NCP Console (NCPCON, `ncpcon (8)` command) to manage Dynamic Storage Technology from a terminal console. For information, see [Section A.1, “Using NCPCON for DST Commands,” on page 157](#).

7.3 Management Tools for NSS Volumes

- ♦ [Section 7.3.1, “Storage Plug-In to Novell iManager 2.7,” on page 75](#)
- ♦ [Section 7.3.2, “Files and Folders Plug-In to Novell iManager 2.7,” on page 75](#)
- ♦ [Section 7.3.3, “NSS Management Utility \(NSSMU\),” on page 75](#)

7.3.1 Storage Plug-In to Novell iManager 2.7

Use the Storage plug-in to iManager to create and manage Novell Storage Services (NSS) volumes that you use as DST shadow volumes. For information, see [“Novell iManager and Storage-Related Plug-Ins” in the *OES 2 SPI: NSS File System Administration Guide*](#).

7.3.2 Files and Folders Plug-In to Novell iManager 2.7

Use the Files and Folders plug-in to iManager to manage file system trustees, trustee rights, and inherited rights filters for files and directories on NSS volumes that you use as DST shadow volumes. You can also set file ownership, directory quotas, and file system attributes. For information, see [“Files and Folders Plug-In Quick Reference” in the *OES 2 SPI: NSS File System Administration Guide*](#).

7.3.3 NSS Management Utility (NSSMU)

You can also use the NSS Management Utility (NSSMU, `nssmu (8)` command) to create and manage NSS volumes that you use in DST shadow volumes. For information, see [“NSSMU for Linux Quick Reference” in the *OES 2 SPI: NSS File System Administration Guide*](#).

7.4 Management Tools for Clustering

Use the Clustering plug-in to Novell iManager 2.7 to create and manage the cluster resources, load scripts, and unload scripts for clustered NSS pools that contain the NSS volumes you use as DST shadow volumes. For information, see [“Creating Cluster Resources” in the *OES 2 SPI: Novell Cluster Services 1.8.5 for Linux Administration Guide*](#).

Managing DST Shadow Volumes for NSS Volumes

8

Dynamic Storage Technology (DST) supports shadow volume pairs with two Novell® Storage Services™ (NSS) volumes on Novell Open Enterprise Server (OES) 2 Linux. This section describes how to create and manage shadow volume pairs with NSS volumes.

- ♦ [Section 8.1, “Understanding DST Shadow Volumes,” on page 77](#)
- ♦ [Section 8.2, “Creating NSS Volumes to Use in the DST Shadow Volume Pair,” on page 82](#)
- ♦ [Section 8.3, “Configuring the NCP/NSS Bindings for an NSS Volume,” on page 90](#)
- ♦ [Section 8.4, “Creating a DST Shadow Volume with NSS Volumes,” on page 94](#)
- ♦ [Section 8.5, “Mounting and Dismounting DST Shadow Volumes,” on page 99](#)
- ♦ [Section 8.6, “Viewing Volume Information,” on page 100](#)
- ♦ [Section 8.7, “Removing a DST Shadow Volume,” on page 100](#)
- ♦ [Section 8.8, “Viewing File Events in the Shadow Volume’s Audit Log,” on page 104](#)
- ♦ [Section 8.9, “Backing Up DST Shadow Volumes,” on page 104](#)

8.1 Understanding DST Shadow Volumes

Dynamic Storage Technology lets you optimize the use of your storage by automatically moving data to storage best optimized for the data type or frequency of use. You can create one or more policies to manage and optimize the use of your storage.

- ♦ [Section 8.1.1, “DST Shadow Volumes,” on page 77](#)
- ♦ [Section 8.1.2, “DST Shadow Volumes Management Tasks,” on page 78](#)
- ♦ [Section 8.1.3, “Dynamic Storage Technology Policies,” on page 82](#)

8.1.1 DST Shadow Volumes

The DST shadow volume is a virtual NCP™ (NetWare® Core Protocol™) volume that consists of a primary storage area and a secondary storage area. In the initial release of DST, the primary and secondary areas use existing NSS volumes, where the secondary volume is typically empty when you define the DST relationship. Shadow volumes are known by their primary volume name. The primary file tree and the secondary file tree for the shadow volume share the same directory structure. Each subdirectory appears in both the primary file tree and the secondary file tree.

NOTE: In the Dynamic Storage Technology interface in Novell Remote Manager for Linux, you will see the terms “shadow” and “secondary” used interchangeably for the secondary storage area. The interface also refers to the primary volume as being “shadowed” when it is the primary volume in a DST shadow volume. Future changes are planned to resolve terminology inconsistencies.

New directories are created in the primary file tree. A configurable global policy called *Replicate Primary Tree to Shadow* determines when the directory path is created in the shadow file tree:

- ♦ At the time when the directory is created in the primary file tree
- ♦ Only as needed at the time when files are moved based on policy enforcement

Performance is better when the branches are created only as needed. For information about setting the *Replicate Primary Tree to Shadow* parameter, see [Section 4.4, “Configuring a Global Policy that Replicates Branches of the Primary File Tree in the Shadow File Tree,”](#) on page 46.

A file can be located in either the primary file tree or the shadow file tree. When an NCP client accesses a shadow volume, the client sees a unified view of the files that reside in both areas as if they were one tree because the primary file tree and the shadow file tree are overlaid to create one virtual volume tree view, as shown in [Figure 1-1, “User View of the File System Directory,”](#) on page 14. When a CIFS/Samba user accesses a shadow volume, the unified view is provided by the ShadowFS component of DST.

8.1.2 DST Shadow Volumes Management Tasks

The Dynamic Storage Technology Options page (shown in [Figure 8-1](#)) in Novell Remote Manager for Linux is the main page for configuring global policies for all DST shadow volumes, creating and managing DST shadow volumes, and configuring shadow volume policies. For information about configuring global policies for DST, see [Chapter 4, “Installing and Configuring Dynamic Storage Technology,”](#) on page 39.

Figure 8-1 View File System > Dynamic Storage Technology Options

Dynamic Storage Technology Options ?

Dynamic Storage Technology allows you optimize the use of your storage by automatically moving data to storage best optimized for the data type or frequency of use. You can create one or more policies to manage, and optimize the use of your storage.

Volume Information	
Volume Name	Shadow Status
VOL1	Add Shadow Inventory
_ADMIN	No Shadow Inventory
SYS	Add Shadow Inventory

No Dynamic Storage Technology policies defined.

[Create a new policy](#)

Duplicate File Resolution Options

Broadcast conflict message to user: ☒

Action to be taken: [Show duplicate shadow files](#)

[Submit](#)

ShadowFS Configuration

☐ Load ShadowFS At Boot Time

[Submit](#)

Use the Dynamic Storage Technology Options page to perform the following task for managing shadow volumes:

- ♦ “[Viewing the Volume Information Report](#)” on page 79

- ♦ “Viewing the Volume Share Information for a Given Volume” on page 79
- ♦ “Viewing the Shadow Status of a Volume” on page 81
- ♦ “Adding a Shadow” on page 81
- ♦ “Managing NCP Shares” on page 82
- ♦ “Generating the Shadow Volume Inventory” on page 82
- ♦ “Viewing the Audit Log” on page 82

Viewing the Volume Information Report

On the Dynamic Storage Technology Options page in Novell Remote Manager for Linux, the *Volume Information* report contains information about all NCP volumes on the server. NSS volumes are by default NCP volumes. NCP volumes can also be NCP shares define for Linux POSIX file systems such as Ext3 or Reiser.

IMPORTANT: In its initial release, DST supports shadow volumes only for NCP volumes on the NSS file system.

The Volume Information report includes both NSS volumes and NCP volumes on Linux POSIX file systems, as shown in [Figure 8-2](#). The report does not distinguish between the underlying file systems for the NCP volumes. In the initial release of DST, make sure you create shadows only for NCP volumes based on the NSS file system. You can identify whether a volume is an NSS volume by clicking the *Information* icon next to the volume name, then view its underlying file system type. For information about the other details available, see “Viewing the Volume Share Information for a Given Volume” on page 79.

Figure 8-2 Volume Information Report

Dynamic Storage Technology Options ?		
Dynamic Storage Technology allows you optimize the use of your storage by automatically moving data to storage best optimized for the data type or frequency of use. You can create one or more policies to manage, and optimize the use of your storage.		
Volume Information		
Volume Name	Shadow Status	
NCPVOL1		Add Shadow Inventory
VOL1	Shadowed	Inventory View Log
_ADMIN	No Shadow	Inventory
SYS		Add Shadow Inventory

Viewing the Volume Share Information for a Given Volume

The Share Information page displays details about the NCP volume, such as its Linux file system path, the file system path of its shadow area (if it is shadowed), the file system type, and capacity.

Figure 8-3 NSP Volume Share Information

VOL1 Share Information

Information		
Description	Value	
File system path	/media/nss/VOL1	
File system shadow path	/media/nss/ARCVOL	
File system type	NSS	
NCP volume ID	2	
Status	mounted, online, NSS, salvageable	
Capacity	488.51 MB	
Local cache	Parameter	Value
	trustee count	0
	cached files	9
	evicted files	0
	cached folders	7
	cache retrieved	59
	cache retrieved locked	7
Pool name	POOL1	
Pool attributes	2833362296	
GUID	5f63e720-6afb-01dc-80-00-ac7e4c66ba5f	

Table 8-1 describes each of the reported parameters on the Share Information page:

Table 8-1 NCP Volume Share Information

Parameter	Description
File System Path	The mount point of the selected volume.
File System Shadow Path	If the selected volume is shadowed, this is the mount point of its secondary storage area.
File System Type	The underlying file system type, such as NSS, Reiser, or Ext3.
NCP Volume ID	The unique identifier given to the volume by the NCP engine. Values range between 0 and 254 (up to 255 volumes mounted concurrently).
Status	Reports the status of the selected volume, such as if it is mounted and online or offline for the NCP engine. For NSS volumes, it also shows which attributes are enabled, such as user quotas, directory quotas, and salvage.
Capacity	The total amount of space allocated to the volume.
Advanced Information	<p>Click <i>View</i> to reveal the following information:</p> <p>Local Cache: Shows the current status of cache parameters, such as trustee count, cached files, evicted files, cached folders, cache retrieved, and cache retrieved locked.</p> <p>Pool Name: For NSS, the name of the NSS pool where the volume resides.</p> <p>Pool Attributes: For NSS, the attribute identifier for the volume's pool.</p> <p>GUID: The Novell eDirectory™ globally unique identifier for the selected volume.</p>

Parameter	Description
Open Files	<p>Reports the connection number (station) of the NCP client connection, the typeless fully distinguished eDirectory username (such as username.context) who opened the connection, and the files that are currently open for that connection.</p> <p>You manage NCP connections to the primary storage area of the DST shadow volume. Users do not connect directly to the secondary storage area. To manage connections, go to the <i>Manage NCP Services</i> role, then click <i>Manage Connections</i>.</p>

Viewing the Shadow Status of a Volume

In the *Volume Information* report, the *Shadow Status* column displays whether or not a volume has a shadow. There are three states:

Table 8-2 *Shadow Status in the Volume Information Report*

Shadow State	Description
No Shadow	The NSS _ADMIN volume cannot be shadowed, and displays a status of No Shadow.
Add Shadow	<p>The volume is an NSS volume or an NCP volume that is eligible for shadowing. You must separately verify that the volume satisfies the guidelines and caveats that are specified in Chapter 3, “Planning Your Dynamic Storage Technology Solution,” on page 23.</p> <p>IMPORTANT: In the initial release of DST, you should select the Add Shadow link only for NCP volumes where the underlying file system is the NSS file system.</p>
Shadowed	The volume is the primary volume in a DST shadow volume. To identify the secondary storage area for this volume, click the <i>Information</i> icon next to the volume name to go to the Share Information page, then view the File System Shadow Path.

Adding a Shadow

In order to create a DST shadow volume, you need two existing NSS volumes that meet the guidelines and caveats specified in [Chapter 3, “Planning Your Dynamic Storage Technology Solution,”](#) on page 23. In the *Volume Information* report, an unshadowed NSS volume has an *Add Shadow* status. Identify two NSS volumes with the *Add Shadow* status, then determine which volume you want to use for the secondary area. For NSS volumes, the secondary storage area must be disabled for being automatically mounted and available for NCP Server. After you turn off its NCP/NSS bindings, the secondary NSS volume no longer appears in the Volume information report, and is ready to be used as the secondary volume. For information, see [Section 8.3, “Configuring the NCP/NSS Bindings for an NSS Volume,”](#) on page 90.

Click the *Add Shadow* link for the primary volume to go to the Volume Share Information page, then click *Add Shadow Volume* in the *Volume Tasks* area. This takes you to an area where you can set up the shadow relationship between the primary and secondary volumes. For information, see [Section 8.4, “Creating a DST Shadow Volume with NSS Volumes,”](#) on page 94.

Managing NCP Shares

In Novell Remote Manager for Linux, an NCP share is the mount point on an Ext3 or Reiser volume that you want to define as an NCP volume. An NSS volume is automatically mounted or unmounted as an NCP share, or you can mount or unmount the NSS volume by using Novell Remote Manager for Linux. You can create, modify, and delete NSS volumes only by using the NSS management tools.

Click *Share Management Home* to go directly to *Manage NCP Services > Manage Shares*, where you can mount or unmount NCP volumes and NSS volumes from the NCP Server. For information, see [Section 8.5, “Mounting and Dismounting DST Shadow Volumes,” on page 99](#).

Generating the Shadow Volume Inventory

To generate an inventory of the files located on a volume, select the *Inventory* link next to the volume. The Inventory page allows you to move specific file types between a volume’s primary and shadow (secondary) areas. For information, see [Chapter 10, “Monitoring DST Shadow Volumes,” on page 119](#).

Viewing the Audit Log

For volumes with a *Shadow Status* of *Shadowed*, all moves between the primary and shadow storage areas are logged to the shadow volume’s audit file. In the Volume Information report, click the *View Log* link to view an XML log file containing audit events for that volume. For information, see [Section 8.8, “Viewing File Events in the Shadow Volume’s Audit Log,” on page 104](#).

8.1.3 Dynamic Storage Technology Policies

Shadow Volume policies manage how files are distributed across the shadow volume’s primary and shadow areas. A Shadow Volume policy allows you to specify when the policy is enforced (one time, hourly, daily, weekly, and so on), which volumes the policy applies to, which direction files are moved (primary to shadow or shadow to primary), and which files are moved (file type, modify date, access date, size, and so on). Multiple policies can be applied to the same volumes and multiple policies can be scheduled to run concurrently.

For information about creating or modifying Dynamic Storage Technology Policies, see [Chapter 9, “Managing Policies for Shadow Volumes,” on page 109](#).

8.2 Creating NSS Volumes to Use in the DST Shadow Volume Pair

In its initial release, DST shadow volumes can be created using only NSS volumes. At least one of the two NSS volumes that you use in the shadow volume pair must be a new volume. This section describes the essentials for creating the NSS volumes. For complete information, see the [OES 2 SP1: NSS File System Administration Guide](#).

- ♦ [Section 8.2.1, “Requirements for NSS Volumes,” on page 83](#)
- ♦ [Section 8.2.2, “Preparing Devices for NSS Volumes,” on page 83](#)
- ♦ [Section 8.2.3, “Creating an NSS Pool,” on page 84](#)
- ♦ [Section 8.2.4, “Creating and Configuring Unencrypted NSS Volumes,” on page 87](#)

8.2.1 Requirements for NSS Volumes

Before you can create a DST shadow volume, you need two existing NSS volumes that have the same configuration of attributes and features. [Table 8-3](#) identifies key NSS requirements for NSS volumes that you use in the DST shadow volume:

Table 8-3 Requirements for the Primary and Secondary Storage Areas

NSS Requirements	Caveats
Devices must be attached to the OES 2 Linux server	The device type, performance characteristics, size, and storage subsystem can differ for the primary and secondary storage locations. For information about supported devices, see Section 3.1.2, “Storage Devices,” on page 23 and Section 3.1.3, “iSCSI Block Storage Devices,” on page 25.
Devices must be able to be managed by EVMS	When you create an NSS pool on OES 2 Linux, the NSS management tools automatically configure the device for use with EVMS. If the pool you create is not clustered, an EVMS NetWare Segment Manager is added to the device. If the pool is clustered, an EVMS Cluster Segment Manager is added. For information, see “EVMS Requirements” in the OES 2 SP1: NSS File System Administration Guide .
Pools' share state must be the same	Typically, the two NSS volumes exist in different pools. The share state of each pool must be the same: <ul style="list-style-type: none">◆ Both pools are unshared with a share state of Not Shareable for Clustering.◆ Both pools are shared with a share state of Shareable for Clustering, and are clustered with Novell Cluster Services™ for Linux.
Volume attributes and features	Both volumes must be configured with the same attributes and features. Some limitations apply. For guidelines and caveats for working with NSS volumes in shadow volumes, see in Section 3.3, “Guidelines for Using NSS Volumes in DST Shadow Volumes,” on page 31.

8.2.2 Preparing Devices for NSS Volumes

[Table 8-4](#) provides a quick reference for the tasks needed to prepare devices for NSS volumes. Perform the tasks in the order presented as they apply to your planned storage solution and the current state of your system. For details related to any step, see the referenced sections in the [OES 2 SP1: NSS File System Administration Guide](#), except as otherwise noted.

IMPORTANT: Perform only those tasks that apply for your storage needs.

Table 8-4 Task Quick Reference for Preparing to Create an NSS Volume on OES 2 Linux


Task	Description	Unshared	Shared
Use third-party tools to carve disks to sizes between 20 MB and 2 TB.	NSS recognizes devices up to 2 TB in size. You can combine multiple devices to create a single NSS pool up to 8 TB in size.	Required	Required


Task	Description	Unshared	Shared
If you plan to cluster the pools, make sure you have installed Novell Cluster Services for Linux and that it is running.	Novell Cluster Services for Linux must be installed before you can create shared NSS pools. For information, see “ Installing and Configuring Novell Cluster Services ” in the <i>OES 2 SP1: Novell Cluster Services 1.8.5 for Linux Administration Guide</i> .	Not used	Required for sharing
If the SAN solution provides multiple paths between the device and the server’s HBA, configure multipathing for the device.	Use multipath management tools from the hardware vendor, third-party tools, or Linux multipath tools to resolve the multiple I/O paths into a single multipath device that represents the actual device. For information about using Linux multipath management tools, see “ Managing Multipath I/O for Devices ” (http://www.novell.com/documentation/sles10/stor_evms/data/multipathing.html) in the <i>SUSE® Linux Enterprise Server 10 Storage Administration Guide</i> (http://www.novell.com/documentation/sles10/stor_evms/data/bookinfo.html).	As needed	As needed
If the disk has not already been initialized, initialize the disk.	<p>A newly added device must be initialized in order for its free space to be available for creating NSS pools. You cannot initialize the device that contains the operating system. Do not initialize devices that contain data you want to keep, whether the data is stored in NSS file systems or Linux file systems.</p> <hr/> <p>WARNING: The initialization process destroys all data on the disk.</p> <hr/> <p>For information, see “Initializing a Disk”.</p>	New devices	New devices
Enable sharing for clustered devices.	<p>If you plan to cluster the pool, set the device’s share state to Shareable for Clustering. Do this for all devices that you want to contribute space to the pool. If a device is marked as sharable for clustering, all partitions on that device are automatically sharable.</p> <p>For information, see “Sharing Devices for NSS Pools”.</p>	Not used	Required for sharing

8.2.3 Creating an NSS Pool

- 1 In iManager, click *Storage > Pools*.
- 2 Click the browser to locate and select the OES 2 Linux server you want to manage.
- 3 Click *New* to open the *New Pool Wizard* to guide you through the pool creation process.
- 4 Specify a name for the new storage pool, then click *Next*.
NSS changes your entry to all capitals when it creates the pool.
- 5 Specify the following pool configuration settings:

Parameter	Description
Devices	Select the check box next to one or more of the available devices you want to use in the pool.
Used Size	<p>For each selected device, specify the amount of space in megabytes (MB) to add to the pool, up to the amount of free space available for that device.</p> <p>To update the <i>Total Pool Size</i> as you enter each device's <i>Used Size</i>, click anywhere within the Wizard dialog box.</p> <p>Devices appear in the list only if they are able to be managed by EVMS, are 2 TB or less in size, were previously initiated for NSS, and have free space available. The pool itself can be up to 8 TB and uses space from one or any number of devices. Any given device can contribute only up to 2 TB, of course.</p>
Cluster Enable on Creation	If the selected device is shareable, the <i>Cluster Enable on Creation</i> check box is automatically selected so the pool can be shared in a cluster configuration with Novell Cluster Services for Linux. Deselect the check box if you do not want to cluster-enable this pool for sharing.
Mount on Creation	Select <i>Mount on Creation</i> to mount the device automatically after it is created. This parameter is enabled by default.

New Pool 

 **Select device and space**

Name: **nifpool**

A pool can be created on one or more storage objects. Select the storage objects for the pool and determine what amount of the available storage space will be used for the pool.

Used Size (MB)	Device ID	Device Name	Free Size (MB)	Type
<input checked="" type="checkbox"/> 59999	0x13	R5_nifb	59999	Shared
<input checked="" type="checkbox"/> 59999	0x20	R5_nifa	59999	Shared
<input checked="" type="checkbox"/> 59999	0x26	R5_nifc	59999	Shared
<input type="checkbox"/> 0	0x3	[V312-A0-D0:0] WD1GTL WDE4360-1807A3 rev:1.80	1340	Local
<input type="checkbox"/> 0	0x4	[V312-A0-D1:0] SEAGATE ST31230N rev:0300	309	Local
<input type="checkbox"/> 0	0x5	[V312-A0-D2:0] HP 2.13 GB #A2 rev:0180	881	Shared

Total Pool Size (MB): 179999

☒ Cluster Enable on Creation

☒ Activate On Creation

<< Back Finish Cancel

6 Do one of the following:

- ♦ **Not Clustered:** Click *Finish*. You are done; continue with [Section 8.2.4, “Creating and Configuring Unencrypted NSS Volumes,” on page 87](#).
- ♦ **Clustered:** If the *Cluster Enable on Creation* check box is selected, click *Next* to specify cluster parameters for the pool. Continue to the next step.

7 Specify the *Cluster Information*:

New Pool

Cluster Information

Name: **NIFPOOL**

Shared Pool Clustering Parameters:

Virtual Server Name:

CIFS Server Name:

IP Address:

Advertising Protocols:

☒ NCP

☐ CIFS

☐ AFP

<< Back Finish Cancel

Fill in the following shared pool clustering parameters:

- ♦ **Virtual Server Name:** The name assigned to the virtual server that represents the shared pool in the cluster.

When you cluster-enable a pool, a virtual Server object is automatically created in Novell eDirectory and given the name of the Cluster object plus the name of the cluster-enabled pool. For example, if the cluster name is `cluster1` and the cluster-enabled pool name is `pool1`, then the default virtual server name is `cluster1_pool1_server`. You can edit the field to change the default virtual server name.

- ♦ **CIFS Virtual Server Name:** The name assigned by Novell CIFS to the virtual server for handling CIFS (Common Internet File System) requests. This is the name of the server as it appears in a Windows system.

IMPORTANT: Novell CIFS for OES 2 SP1 Linux has not been tested with DST.

For OES 2 Linux, Windows network access is via Samba. In order to give CIFS/Samba access to users, you must install Novell Samba and configure users for Samba access. For information about configuring Samba services, see the *OES2 SP1: Samba Administration Guide*.

- ♦ **IP Address:** The IP address that you want to assign the virtual server.

Each cluster-enabled NSS pool requires its own IP address. The IP address is used to provide access and failover capability to the cluster-enabled pool (virtual server). The IP address you assign to the pool remains assigned to the pool no matter which server node in the cluster that the pool is active.

IMPORTANT: The IP address for the virtual server must be in the same IP subnet as the server nodes in the cluster where you plan to use it.

To specify an IP address, tab between the different entries; no dot is required in the fields. For example, if the IP address is `192.168.1.1`, type

`192 168 1 1`

- ♦ **Advertising Protocols:** Protocols that give users native file access to data.

Specify the advertising protocol by selecting the check boxes of the protocols you want to enable for data requests to this shared pool.

- ♦ NetWare Core Protocol (NCP) is the Novell networking protocol used by the Novell Client™ and other NCP clients. It is selected by default and is required by NSS, even if your users are accessing the clustered NSS volumes via CIFS/Samba.

Selecting NCP causes commands to be added to the pool-resource load and unload scripts to activate the NCP protocol on the cluster. This lets you ensure that the cluster-enabled pool you are creating is highly available to all NCP clients.

- ♦ CIFS is the Windows networking protocol. Novell CIFS is available on NetWare and on OES 2 SP1 Linux. Use Linux Samba instead. Samba is not configured in this interface.

IMPORTANT: Novell CIFS for OES 2 SP1 Linux has not been tested with DST. Although NSS supports using Novell CIFS for Linux, DST does not support using it with shadow volume pairs.

- ♦ Apple* Filing Protocol (AFP) is the Macintosh networking protocol. Novell AFP is available on NetWare and on OES 2 SP1 Linux.

IMPORTANT: Novell AFP for OES 2 SP1 Linux has not been tested with DST. Although NSS supports using Novell AFP for Linux, DST does not support using it with shadow volume pairs.

8 Click *Finish*.

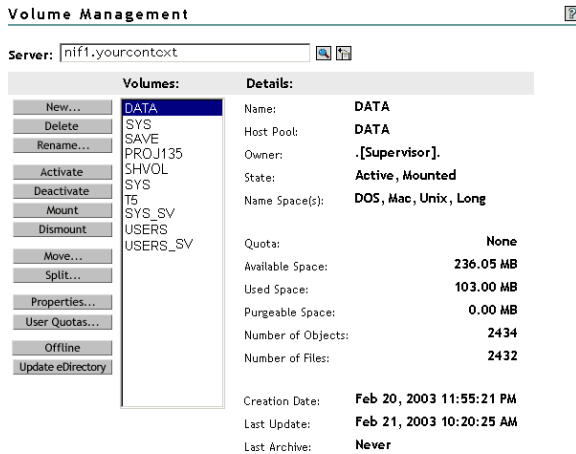
8.2.4 Creating and Configuring Unencrypted NSS Volumes

This section describes how to create an unencrypted volume with iManager. Before you begin, make sure you understand the guidelines and caveats specified in [Section 3.3, “Guidelines for Using NSS Volumes in DST Shadow Volumes,” on page 31](#).

IMPORTANT: Shadow volumes are not supported for encrypted NSS volumes.

- 1 In iManager, click *Storage > Volumes*.
- 2 Select a server to manage.

A list of existing NSS volumes appears in the *Volumes* list, as illustrated in the following figure.



3 To create a new volume, click *New* to open the New Volume Wizard to guide you through the process.

4 Specify a name for the new volume.

If the name you provide is not unique, you receive an error message. NSS volume names are case insensitive. The letters you enter are capitalized when the volume is created.

5 Do one of the following:

- ♦ Select an existing pool from the list where you want the new volume to reside.
- ♦ If no pools exist, click *New Pool*, create a pool to use, select the pool.
- ♦ If existing pools do not have sufficient space for the volume you want to create, click *Cancel* to close the wizard. You must add more segments of free space to the pool, then return to the Volumes page to create the new volume.
- ♦ If no pools exist and no space is available to create one, click *Cancel* to close the Wizard. You must add more devices to the server or free up space on existing pools, then return to the Volumes page to create the new volume.

6 Specify the size of the volume:

- ♦ **No Volume Quota:** Select *Allow Volume Quota to Grow to the Pool Size* if you want the volume to expand to the size of the pool. This is the default.
Pools can be overbooked; each volume can potentially grow to the size of the pool. NSS allocates space as it is needed.
- ♦ **Volume Quota:** Deselect *Allow Volume Quota to Grow to the Pool Size*, then type a *Volume Quota* size in MB for the volume if you want to limit the size of the volume. Valid values are 10 MB to the size of the pool.

7 On the Attribute Information page under the *Attributes* section, set the attributes for the new volume you are creating. The *Backup* and *Salvage* attributes are selected by default.

For information about volume attributes, see “[Understanding Volume Properties](#)” in the *OES 2 SP1: NSS File System Administration Guide*.

For guidelines and caveats about using different attributes with Dynamic Storage Technology, see [Table 3-3, “DST Support for NSS Volume Attributes,”](#) on page 31.

New Volume ?

Attribute information

Select the desired attributes for the volume. Once set, Compression persists for the life of the volume. For Linux, specify the mount point's path, such as /mnt/nss/volumes/volumename. Enable the mount point to be renamed to allow updates to the volume name or its path.

Attributes

☒ Backup ☐ Migration

☐ Compression ☐ Modified File List(MFL)

☐ Data Shredding ☒ Salvage

Number of shredding cycles:

☐ Directory Quotas ☐ Snapshot

☐ Flush Files Immediately ☐ User Space Quotas

☐ User-level Transaction Model

On Creation

☒ Activate ☒ Mount

File Information

Mount Point: Lookup Namespace:

☐ Allow Mount Point to be Renamed ☐ DOS

☒ Long

☐ Mac

☐ Unix

<< Back Finish Cancel

8 On the *Attribute Information* page under the *On Creation* section, set the following preferences:

- ♦ **Activate:** Activates logical volumes as soon as you create them.
- ♦ **Mount:** Mounts logical volumes as soon as you create them.

9 On the *Attribute Information* page under *File Information*, specify the following parameters:

- ♦ **Mount Point (Linux):** For a Linux server, specify the mount point for the NSS volume, such as /media/nss/VOLA.

The default mount path for NSS volumes on Linux is /media/nss/*volumename*, where *volumename* is the name of the volume.

- ♦ **Allow Mount Point to Be Renamed (Linux):** For a Linux server, select this option if you want to allow the mount point to be renamed after it has been created.

IMPORTANT: DST does not support renaming mount points.

Renaming a mount point means that you can specify another path as the mount point, such as /media/uservols/*volumename*, but the volume would continue to be associated with the same Volume object in eDirectory.

- ♦ **Lookup Name Space:** Select the name space to use when you mount the volume. The name spaces are UNIX, Long, DOS, or Macintosh. For Linux, the default name space is UNIX.

The recommended name space setting is Long. This setting ensures that filenames are case insensitive whether the volume is mounted on a Linux server or NetWare server. It also improves performance, especially if you expect to store millions of files on the volume.

10 Click *Finish*.

11 (Linux) If you enabled the *Directory Quotas* attribute, restart NCP2NSS by entering at a terminal prompt:

```
/etc/init.d/ncp2nss restart
```

8.3 Configuring the NCP/NSS Bindings for an NSS Volume

- ♦ Section 8.3.1, “Understanding the NCP/NSS Bindings Parameter,” on page 90
- ♦ Section 8.3.2, “Enabling the NCP/NSS Bindings for an NSS Volume,” on page 91
- ♦ Section 8.3.3, “Disabling the NCP/NSS Bindings for an NSS Volume,” on page 92
- ♦ Section 8.3.4, “Enabling or Disabling NCP/NSS Bindings by Editing the /etc/opt/novell/ncp2nss.conf File,” on page 93

8.3.1 Understanding the NCP/NSS Bindings Parameter

NSS volumes are automatically mounted by default on system restart in NSS, then in NCP Server. This is the desired behavior for all independent NSS volumes that are not in shadow volumes, and for NSS volumes that you use as primary storage locations in a DST shadow volumes. When an NSS volume is used as the secondary storage area in a DST shadow volume, you want the NSS volume to be mounted in NSS, but not in NCP Server. This allows DST to control access to the secondary storage area via the primary storage area. Files in the secondary storage area cannot be directly accessed by users.

The NCP/NSS Bindings parameter for an NSS volume governs whether the volume is automatically mounted on system restart in NCP Server. When the parameter is enabled, the NSS volume is automatically mounted for NCP Server. When it is disabled, the NSS volume is not mounted for NCP Server. The NCP/NSS Bindings parameter is enabled by default, making the volume NCP accessible.

In the NCP/NSS Bindings dialog, NSS volumes are enabled by default to be *NCP Accessible*, and have a setting of *Yes*.

NCP / NSS Bindings ?

Warning:
When a NSS Volume is changed to be not accessible via NCP, it will be dismounted immediately as a NCP share point

Available NSS volumes		
NCP Accessible	Volume Name	Mount point
Yes: <input checked="" type="radio"/> No: <input type="radio"/> <small>Save Selection</small>	VOL1	/media/nss/VOL1
Yes: <input checked="" type="radio"/> No: <input type="radio"/> <small>Save Selection</small>	ARCVOL	/media/nss/ARCVOL

Share Management Home

For example, if you plan to create a DST shadow volume that uses VOL1 as the primary storage location and ARCVOL as the secondary storage location, set *NCP Accessible* to *Yes* for VOL1, and set it to *No* for ARCVOL.

Warning:

When a NSS Volume is changed to be not accessible via NCP, it will be dismounted immediately as a NCP share point

Available NSS volumes		
NCP Accessible	Volume Name	Mount point
Yes: <input type="radio"/> No: <input checked="" type="radio"/> <input type="button" value="Save Selection"/>	ARCVOL	/media/nss/ARCVOL
Yes: <input checked="" type="radio"/> No: <input type="radio"/> <input type="button" value="Save Selection"/>	VOL1	/media/nss/VOL1

After you remove a shadow volume, the NCP/NSS Bindings parameter for the NSS volume that was used as the secondary storage area remains disabled until you enable it. You must enable the bindings and mount the volume in order to enable users to access the now independent volume.

8.3.2 Enabling the NCP/NSS Bindings for an NSS Volume

The volume's NCP/NSS Bindings parameter must be enabled for NSS volumes that you use as primary storage locations in a DST shadow volumes, and for all independent NSS volumes that are not in shadow volumes. This is the default.

- 1 In Novell Remote Manager for Linux, select *Manage NCP Services* > *Manage Shares*.

Configuration

- 2 In the *Configuration* area of the NCP Shares page, click *NCP/NSS Bindings* to open the NCP/NSS Bindings page.
- 3 In the *Available NSS Volumes* list, locate the NSS volume that you want to enable.

Available NSS volumes		
NCP Accessible	Volume Name	Mount point
Yes: <input type="radio"/> No: <input checked="" type="radio"/> <input type="button" value="Save Selection"/>	ARCVOL	/media/nss/ARCVOL
Yes: <input checked="" type="radio"/> No: <input type="radio"/> <input type="button" value="Save Selection"/>	VOL1	/media/nss/VOL1

- 4 If the volume's *NCP Accessible* setting is *No*, click *Yes* to make the NSS volume accessible to NCP so that the volume is automatically mounted in NCP after it is mounted in NSS.

Available NSS volumes		
NCP Accessible	Volume Name	Mount point
Yes: <input checked="" type="radio"/> No: <input type="radio"/> Save Selection	VOL1	/media/nss/VOL1
Yes: <input checked="" type="radio"/> No: <input type="radio"/> Save Selection	ARCVOL	/media/nss/ARCVOL

- 5 Beneath the volume's setting for *NCP Accessible*, click *Save Selection* to save and apply the new setting.
- 6 Verify that the NSS volume is available for NCP by selecting *Manage NCP Services > Manage Shares* to view a list of active volumes.
If the NSS/NCP bindings are enabled, the NSS volume appears in the *Volume Information* list, and a *Mount* button is displayed next to it.
- 7 If you want users to be able to access the volume at this time, click *Mount*.
When the volume is successfully mounted, the volume's name is hyperlinked, and an *Unmount* button is displayed next to it.

8.3.3 Disabling the NCP/NSS Bindings for an NSS Volume

The volume's NCP/NSS Bindings parameter must be disabled for NSS volumes that you use as secondary storage locations in a DST shadow volumes.

- 1 In Novell Remote Manager for Linux, select *Manage NCP Services > Manage Shares*.
- 2 In the *Configuration* area of the NCP Shares page, click *NCP/NSS Bindings*.

Configuration
Create new share
Delete existing share
NCP/NSS Bindings

- 3 In the *Available NSS Volumes* list, locate the NSS volume that you want to disable.
- 4 In the *NCP Accessible* column, click *No* to make the NSS volume not accessible to NCP so that it is not mounted in NCP after it is mounted in NSS.

Available NSS volumes		
NCP Accessible	Volume Name	Mount point
Yes: <input type="radio"/> No: <input checked="" type="radio"/> Save Selection	ARCVOL	/media/nss/ARCVOL
Yes: <input checked="" type="radio"/> No: <input type="radio"/> Save Selection	VOL1	/media/nss/VOL1

- 5 Beneath the volume's setting for *NCP Accessible*, click *Save Selection* to save and apply the new setting.
- 6 Verify that the NSS volume is not available for NCP by selecting *Manage NCP Services > Manage Shares* to view a list of active volumes.
If the NCP/NSS bindings were successfully disabled, the NSS volume should not appear in the *Volume Information* list.

8.3.4 Enabling or Disabling NCP/NSS Bindings by Editing the /etc/opt/novell/ncp2nss.conf File

When the NCP/NSS bindings parameter is disabled for a volume, NCP Server adds an `EXCLUDE_VOLUME` entry to the `/etc/opt/novell/ncp2nss.conf` file. You can manually disable or enable the NSS volume's NCP/NSS bindings parameter by adding or removing this entry from the file, then restarting the NCP2NSS daemon.

- 1 Open the `/etc/opt/novell/ncp2nss.conf` configuration file in a text editor.
- 2 Do one of the following:
 - ♦ **Disable the NCP/NSS Binding:** Add an `EXCLUDE_VOLUME` for the volume you plan to use as secondary NSS volume in order to exclude the volume from being automatically mounted for NCP Server.

```
EXCLUDE_VOLUME nss_volumename
```

Replace `nss_volumename` with the name of the NSS volume. For example, to disable the bindings for the NSS volume named `ARCVOL:`, add the following line. Note that you do not include the colon after the volume name.

```
EXCLUDE_VOLUME ARCVOL
```

- ♦ **Enable the NCP/NSS Binding:** Locate the `EXCLUDE_VOLUME` entry for the NSS volume, then remove that line from the file.
- 3 Save the file.
 - 4 Restart the Novell eDirectory daemon by entering the following commands:

```
rcnssd stop
```

```
rcnssd start
```

- 5 Restart the NCP/NSS IPC daemon to synchronize the changes you made to the `/etc/opt/novell/ncp2nss.conf` file.
 - 5a At the terminal console prompt, enter

```
/etc/init.d/ncp2nss restart
```

- 5b If the NCP/NSS IPC daemon restarts successfully, the following messages are displayed in the terminal console:

```
Shutting down Novell NCP/NSS IPC daemon...
```

```
Exited
```

```
Starting the Novell NCP/NSS IPC daemon.
```

8.4 Creating a DST Shadow Volume with NSS Volumes

- ♦ [Section 8.4.1, “Prerequisites for DST Shadow Volumes,” on page 94](#)
- ♦ [Section 8.4.2, “Preparing the NSS Volumes for Use in a DST Shadow Volume,” on page 95](#)
- ♦ [Section 8.4.3, “Creating a DST Shadow Volume with Unshared NSS Volumes,” on page 96](#)

8.4.1 Prerequisites for DST Shadow Volumes

Before you configure shadow volumes on the server, make sure you have completed the following prerequisites.

- ♦ [“Prerequisites for Global Policies” on page 94](#)
- ♦ [“Prerequisites for Creating a DST Shadow Volume with NSS Volumes” on page 94](#)

Prerequisites for Global Policies

Before you configure shadow volumes on the server, make sure you configure global policies for DST. Global policies govern the behavior of DST, and apply to all shadow volumes on a given server. For information, see the references listed in [Table 8-5](#).

Table 8-5 *Global Policies*

Global Policy Parameter	For Information
REPLICATE_PRIMARY_TREE_TO_SHADOW	Section 4.4, “Configuring a Global Policy that Replicates Branches of the Primary File Tree in the Shadow File Tree,” on page 46
SHIFT_MODIFIED_SHADOW_FILE	Section 4.5, “Configuring Global Policies for Shifting Files from the Shadow File Tree to the Primary File Tree,” on page 47
SHIFT_ACCESSED_SHADOW_FILE	
SHIFT_DAYS_SINCE_LAST_ACCESS	
DUPLICATE_SHADOW_FILE_ACTION	Section 4.6, “Configuring Global Policies for Resolving Instances of Duplicate Files,” on page 51
DUPLICATE_SHADOW_FILE_BROADCAST	

Prerequisites for Creating a DST Shadow Volume with NSS Volumes

- ❑ NSS must be installed and running.
- ❑ Two existing NSS pools:
 - ♦ The primary pool (the pool that contains the NSS volume that you plan to use as the primary storage area) should be on the higher-performance device.
 - ♦ The NSS pool to be used for the primary storage area must be on a device that satisfies the guidelines specified in [Section 3.1.2, “Storage Devices,” on page 23](#). It cannot be on a device that is attached to the OES 2 Linux server via a remote server-to-server connection.

- ♦ The NSS pool to be used for the secondary storage area must be on a device that satisfies the guidelines specified in [Section 3.1.2, “Storage Devices,” on page 23](#).
- ♦ The NSS pools can be old or new.

For information about creating a new NSS pool, see [Section 8.2.3, “Creating an NSS Pool,” on page 84](#).

❑ Two existing NSS volumes:

- ♦ The volumes must reside in separate pools, where the volume to be used as the primary volume is in the pool on the higher-performance device.
- ♦ The volumes must be configured with the same NSS attributes and features. For information, see [Section 3.3, “Guidelines for Using NSS Volumes in DST Shadow Volumes,” on page 31](#).
- ♦ The NSS volumes can be two new volumes, or an old volume and a new volume.

You should not use two old volumes, unless you temporarily remove a shadow volume relationship, then use the same volumes when you configure the shadow volume again. This situation is typical of using shadow volumes in a cluster, where no user access occurs on the two volumes before they are paired again after failing over to another node in the cluster.

For information about creating a new NSS volume, see [Section 8.2, “Creating NSS Volumes to Use in the DST Shadow Volume Pair,” on page 82](#).

8.4.2 Preparing the NSS Volumes for Use in a DST Shadow Volume

For all NCP volumes (NSS and non-NSS), the trustee information is obtained at volume mount time from the `._NETWARE/.trustee_database.xml` file. For an NSS volume, the Linux path to the file is `/media/nss/volumename/._NETWARE/.trustee_database.xml`.

The first time that you create and mount a given shadow volume, the trustee information on the primary volume is copied to the same location on the secondary volume. While the shadow relationship exists, all trustee changes are copied to both locations in order to keep the copies of the trustee information synchronized. When you remove a shadow volume, each volume has a complete copy of the trustee information.

This is not a problem for scenarios where the secondary volume is a new empty volume. However, for scenarios where the primary volume is the new volume and the secondary volume is an old volume, the old trustee information gets overwritten. To avoid losing the trustee information, copy the trustee file from the old volume to the new empty volume.

If the volume that you want to use as the secondary volume is an old volume, do the following to preserve the existing trustee information before you create the shadow volume:

- 1 In Novell Remote Manager, log in as the `root` user.
- 2 Select *Manage NCP Services > Manage Shares* to view a list of active volumes.
- 3 Dismount the NSS volumes from NCP Server that you want to use as the primary volume and secondary volume by selecting the *Unmount* button next to each volume.

If the NSS volume that you plan to use as the secondary volume has its NCP/NSS bindings disabled, it is already dismounted from NCP Server. For information, see [Section 8.3, “Configuring the NCP/NSS Bindings for an NSS Volume,” on page 90](#).

- 4 Open a terminal console as the `root` user, then copy the trustee file from the secondary volume location to the primary volume location by entering the following at a terminal console prompt:

```
cp /media/nss/secondary_volumename/._NETWARE/.trustee_database.xml /media/nss/primary_volumename/._NETWARE/.trustee_database.xml
```

IMPORTANT: You must rename or delete the `/media/nss/primary_volumename/._NETWARE/.trustee_database.xml` file on the primary volume before you can copy the `.trustee_database.xml` file from the secondary volume to that location.

- 5 Select *Manage NCP Services > Manage Shares* to view a list of active volumes.
- 6 Mount the primary volume and secondary volume for NCP Server by selecting the *Mount* button next to each volume.
- 7 At the terminal console prompt, enter the following command to synchronize the NSS trustee information that is now on the primary volume with NCP Server:

```
ncpcon nss sync=primary_volumename
```

- 8 Continue with creating the DST shadow volume for the two volumes. For information, see [Section 8.4.3, “Creating a DST Shadow Volume with Unshared NSS Volumes,” on page 96.](#)

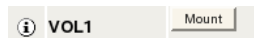
8.4.3 Creating a DST Shadow Volume with Unshared NSS Volumes

The procedure in this section describes how to use two unshared NSS volumes to create an unshared DST shadow volume.

IMPORTANT: For information about using shared NSS volumes to create a shared DST shadow volume in a cluster environment, see [Chapter 11, “Configuring DST Shadow Volumes with Novell Cluster Services for Linux,” on page 133.](#)

As an example, the procedure in this section uses `VOL1` for the primary storage area, and `ARCVOL` as the secondary storage area. Make sure to substitute the actual names of the NSS volumes you are using in each of the steps.

- 1 In Novell Remote Manager for Linux, log in as the `root` user.
- 2 Select *View File System > Dynamic Storage Technology Options* to view a list of mounted volumes.
- 3 On the Dynamic Storage Technology page, make sure that the NSS volume that you want to use as the primary volume appears in the *Volume Information* list with a status of *Add Shadow*. If it is not listed, the NSS volume might be unmounted, or its NCP/NSS bindings might be disabled.
 - 3a Select *Manage NCP Services > Manage Shares* to view a list of active volumes.
 - 3b If the NSS volume is in the list but it is not mounted, the volume’s name is not hyperlinked and a *Mount* button is located next to it.



To mount the volume, click the *Mount* button next to the volume name. Continue with the [Step 4](#).

- 3c** If the NSS volume does not appear in the list of active volumes, click *NCP/NSS Bindings* to view the *Available NSS Volumes* list. If the NSS volume is in the list, verify that its NCP/NSS Bindings parameter is enabled.

If the *NCP Accessible* value is set to No, the volume's NCP/NSS binding is disabled.

To enable the NCP/NSS bindings for the NSS volume, select *Yes* in the *NCP Accessible* column for the NSS volume, then click *Save Selection* to save and apply the change.

Select *Manage NCP Services > Manage Shares* to view the *Volume Information* list, then click the *Mount* button next to the volume name to mount it.

- 3d** If the volume does not appear in the list of active volumes, and it does not appear on the NCP/NSS Bindings page in the Available NSS Volumes list, the volume probably is not mounted in NSS.

Exit Novell Remote Manager, then use NSSMU or the storage plug-in for Novell iManager to mount the volume in NSS.

- 4** In Novell Remote Manager on the Dynamic Storage Technology page, if the NSS volume that you want to use as the secondary volume is listed in the *Volume Information* list, you must disable its *NCP/NSS Binding*, which also dismounts the volume from NCP Server.

For example, if the volume ARCVOL is the NSS volume planned for the secondary volume, it should not appear in the list of available volumes.

Volume Information		
Volume Name	Shadow Status	
① ARCVOL	Add Shadow	Inventory
① VOL1	Add Shadow	Inventory
① _ADMIN	No Shadow	Inventory
① SYS	Add Shadow	Inventory

To disable the NCP/NSS bindings for the NSS volume, select *Manage NCP Services > Manage Shares*, click *NCP/NSS Bindings*, select *No* in the *NCP Accessible* column for the NSS volume, then click *Save Selection* to save and apply the change.

Available NSS volumes		
NCP Accessible	Volume Name	Mount point
Yes: <input type="radio"/> No: <input checked="" type="radio"/> Save Selection	ARCVOL	/media/nss/ARCVOL
Yes: <input checked="" type="radio"/> No: <input type="radio"/> Save Selection	VOL1	/media/nss/VOL1

On the Dynamic Storage Technology page, the ARCVOL is no longer listed.

- 5** Use one of the following methods to go to the volume's Share Information page of the NSS volume that you want to use as the primary storage area.
- ♦ Select *View File System > Dynamic Storage Technology Options* to go to the Dynamic Storage Options page, then click the *Add Shadow* link next to the volume name of the NSS volume.

For example, click the *Add Shadow* link for VOL1.

Volume Information		
Volume Name	Shadow Status	
① VOL1	Add Shadow	Inventory
① _ADMIN	No Shadow	Inventory
① SYS	Add Shadow	Inventory

- ♦ Select *Manage NCP Services > Manage Shares* to open the Manage Shares page, then click the *Information* (i) icon next to the volume name of the NSS volume.



- 6 On the volume's Share Information page, scroll down to the *Volume Tasks* area, then click *Add Shadow Volume*.



- 7 Specify the following information for the secondary storage area for the DST shadow volume, then click *Create* to define the shadow volume.

Create Shadow for Volume VOL1 ?

Shadow Path:

☐ Create if not present

- ♦ **Shadow Path:** Type the Linux path for the NSS volume that you want to use as the secondary storage area. The default Linux path where NSS volumes are mounted is `/media/nss/volumename`.
For example, to specify the NSS volume named ARCVOL as the secondary storage area, type `/media/nss/ARCVOL` in the *Shadow Path* field.
- ♦ **Create If Not Present:** For NSS volumes, the volume must already exist. Make sure this option is deselected (not checked) when shadowing NSS volumes.

IMPORTANT: In OES 2 SP1 and earlier release of DST, this option is a placeholder for future capabilities to support shadow volumes for NCP volumes on Ext3 and Reiser.

- 8 On the volume's Share Information page, make sure the *File System Shadow Path* information shows the shadow path you specified in **Step 7**.

Information	
Description	Value
File system path	/media/nss/VOL1
File system shadow path	/media/nss/ARCVOL
File system type	NSS
NCP volume ID	2
Status	mounted, online, NSS, salvageable
Capacity	488.51 MB
Advanced Information	View

- 9 Select *View File System > Dynamic Storage Technology Options* to go to the Dynamic Storage Options page, then verify that the *Shadow Status* for the volume is set to *Shadowed* and the *View Log* link is available.

Volume Information		
Volume Name	Shadow Status	
① VOL1	Shadowed	Inventory View Log
① _ADMIN	No Shadow	Inventory
① SYS	Add Shadow	Inventory

All moves between the primary storage area and the secondary storage area are logged as events to the shadow volume's audit log. An audit log for a given DST shadow volume is located in the `._NETWARE` directory located at the root of the primary volume. For NSS volumes, the default file path for the log is `/media/nss/volumename/._NETWARE/volumename.audit.log`.

For example, if the primary area is named VOL1, the audit file is `/media/nss/VOL1/._NETWARE/VOL1.audit.log`.

- 10 Select *View File System > Dynamic Storage Technology Options* to go to the Dynamic Storage Options page, then create one or multiple shadow volume policies for the shadow volume.

Shadow volume policies can be configured to shift files by the time since the file was last modified, accessed, or changed; by filenames; by file types; or by file size. You can schedule policies to run automatically, or you can run them on-demand.

For information about creating and scheduling shadow volume policies, see [Chapter 9, "Managing Policies for Shadow Volumes,"](#) on page 109.

- 11 (Optional) You can shift selected data on-demand by running customized inventory reports, then using the inventory detail reports to move selected files to either volume by the time since the file was last modified, accessed, or changed; by filenames; by file types; or by file size. For information, see [Section 10.4, "Using Inventory Detail Reports to Move, Copy, or Delete Files on the Shadow Volume,"](#) on page 128.
- 12 If you plan to grant access to the shadow volume for CIFS/Samba users, configure ShadowFS and FUSE. For information, see [Chapter 5, "Installing and Configuring Shadow File System \(ShadowFS\) for CIFS/Samba Users,"](#) on page 59.

8.5 Mounting and Dismounting DST Shadow Volumes

To mount or dismount the DST shadow volume for NCP Server, you mount or dismount the primary storage area.

To mount a shadow volume:

- 1 In Novell Remote Manager, click *Manage NCP Services > Manage Shares*, then click the *Mount* button next to the volume name of the primary storage area for the DST shadow volume you want to mount.



To dismount a shadow volume:

- 1 In Novell Remote Manager, click *Manage NCP Services > Manage Shares*, then click the *Unmount* button next to the volume name of the primary storage area for the DST shadow volume you want to dismount.



8.6 Viewing Volume Information

You can quickly get name and path information for the member volumes in the DST shadow volume by entering the following at the server command prompt:

```
ncpcon volume data
```

8.7 Removing a DST Shadow Volume

Removing a DST shadow volume simply removes the relationship between the primary and secondary storage area. It does not remove the underlying volumes themselves. The files remain on whichever storage area they are on at the time when you remove the shadow relationship.

- ♦ [Section 8.7.1, “Preparing to Remove a Shadow Volume,” on page 100](#)
- ♦ [Section 8.7.2, “Removing the Shadow Volume Relationship by Using Novell Remote Manager for Linux,” on page 101](#)
- ♦ [Section 8.7.3, “Removing a Shadow Volume by Editing Configuration Files,” on page 103](#)

8.7.1 Preparing to Remove a Shadow Volume

Before you remove a shadow volume relationship, make sure that you shift data between the two volumes that make up the shadow volume, according to where you want the data to reside after the DST shadow volume relationship is removed. In order for the data to be shifted to the primary storage area or to the secondary storage area, it is up to you to make that happen.

- 1 In Novell Remote Manager for Linux, log in as the `root` user.
- 2 Select *View File System > Dynamic Storage Technology Options*, locate the volume in the list, then click the *Inventory* link next to it.

View the volume inventory for the shadow volume to determine the space in use and the available space for both the primary and the secondary areas of the shadow volume. Make sure there is sufficient free space available in either location for the data that you plan to move to that location.

- 3 Use any combination of the following techniques to shift data between the two areas:
 - ♦ **Shadow Volume Policies:** Run an existing shadow volume policy by using the *Execute Now* option in the *Frequency* area of the policy. You can also create a new shadow volume policy that moves specific data, and run the policy by using the *One Time* and *Execute Now* options in the *Frequency* area of the policy.

For information about configuring policies to move data between the primary and secondary areas, see [Chapter 9, “Managing Policies for Shadow Volumes,”](#) on page 109.
 - ♦ **Inventories:** Use the detailed inventory reports or customized inventories to move specific files to either area.

For information about using the volume customized inventory options to move data between the primary and secondary areas, see [Section 10.5, “Generating a Custom Inventory Report,”](#) on page 128.

8.7.2 Removing the Shadow Volume Relationship by Using Novell Remote Manager for Linux

- 1 In Novell Remote Manager for Linux, log in as the `root` user.
- 2 Select *Manage NCP Services* > *Manage Shares* to go to the NCP Shares page.
- 3 Make sure that you know which NSS volume is being used as the secondary volume so that you can manage it independently later.
 - 3a On the NCP Shares page, locate the primary NSS volume in the *Active Shares* list, then click the *Information* icon next to the share name.
 - 3b On the primary volume’s Share Information page, view the volume information in the *File System Shadow Path*.

In the following example, ARCVOL is an NSS volume that is the secondary storage area in the shadow volume.

File system path	/media/nss/VOL1
File system shadow path	/media/nss/ARCVOL

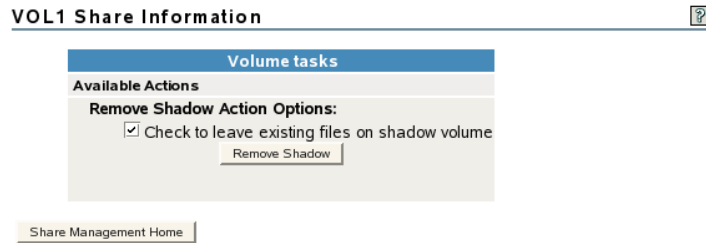
- 4 On the NCP Shares page, locate the primary NSS volume in the *Active Shares* list, then click the *Unmount* button next to the share name.



- 5 On the Manage Shares page, click the *Information* (i) icon next to the volume name of the NSS volume to access the *Remove Shadow Action Options*.



- 6 On the volume’s Share Information page, select *Check to leave existing files on the shadow volume*.



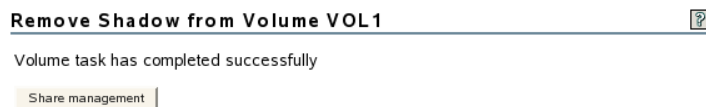
When you enable *Check to leave existing files on the shadow volume*, the data that currently resides on each volume remains where it is, so that the data on the secondary storage area is not shifted back to the primary volume.

The *Check to leave existing files on the shadow volume* option is deselected by default. When this option is disabled and you click *Remove Shadow*, all of the data that currently resides on the secondary volume is moved back to the primary storage location before the secondary volume is again available as an individual volume. It takes time to move the data back to the primary, depending on how much data there is to move.

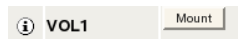
IMPORTANT: In the OES 2 SP1 release for DST, if you disable the *Check to leave existing files on the shadow volume*, the shadow volume is not removed. DST does not remove the shadow relationship until you enable the option to keep data where it is.

7 Click *Remove Shadow*.

After the shadow volume is removed, the page refreshes to report a successful removal.



8 Select *Share Management* to go to the NCP Shares page, locate the volume that was the primary volume in the *Active Shares* list, then click the *Mount* button next to it.



9 Verify that the shadow volume was removed by using one of the following methods:

- ♦ Select *View File System > Dynamic Storage Technology Options* to go to the Dynamic Storage Options page. The former primary volume now has an *Add Shadow* link next to it instead of a *Shadowed* link.

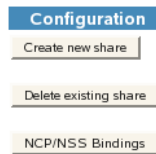
Volume Information		
Volume Name	Shadow Status	
① VOL1	Add Shadow	Inventory
① _ADMIN	No Shadow	Inventory
① SYS	Add Shadow	Inventory

- ♦ Select *Manage NCP Services > Manage Shares*, then click the *Information* icon next to the former primary volume's name. The *File System Shadow Path* field displays n/a (not applicable).

File system path `/media/nss/VOL1`
 File system shadow path `n/a`

- 10 (Optional) Mount the volume that was used as the secondary volume (for example, ARCVOL) as an independent volume.

10a In the *Configuration* area of the NCP Shares page, click *NCP/NSS Bindings*.



- 10b In the *Available NSS Volumes* list, locate the former secondary volume (such as ARCVOL), click *Yes*, then click *Save Selection*.



The volume is mounted automatically, and now appears again in the *Active Shares* list on the NCP Shares page.

Active Shares		
Info	Share name (volume name)	Tasks
SYS		Unmount
_ADMIN		
VOL1		Unmount
ARCVOL		Unmount

8.7.3 Removing a Shadow Volume by Editing Configuration Files

- 1 Open a terminal console, then log in as the `root` user.
- 2 Edit the `/etc/opt/novell/ncpserv.conf` file to remove the following entry for your volume, then save your changes.

```
SHADOW_VOLUME shadow_volume_name
```

- 3 Stop and restart the eDirectory `ndsd` daemon for the changes to take effect by entering

```
/etc/init.d/ndsd stop
```

```
/etc/init.d/ndsd start
```

- 4 Verify that the secondary NSS volume is available for mounting in NCP by checking that there is no longer an `EXCLUDE` entry for the volume in the `/etc/opt/novell/ncp2nss.conf` file.

If necessary, edit the `/etc/opt/novell/ncp2nss.conf` file to remove the following entry for it:

```
EXCLUDE_VOLUME nss_volumename
```

An entry is automatically removed from the `/etc/opt/novell/ncp2nss.conf` file by using Novell Remote Manager for Linux to set the *Manage NCP Services > Manage Shares > NCP/NSS Bindings > NCP Accessible* option to Yes for the NSS volume. For instructions, see [Section 8.3, “Configuring the NCP/NSS Bindings for an NSS Volume,” on page 90](#).

- 5 Restart the NCP/NSS IPC daemon to synchronize the changes you made to the `/etc/opt/novell/ncp2nss.conf` file.

5a At the terminal console prompt, enter

```
/etc/init.d/ncp2nss restart
```

- 5b** If `ncp2nss` restarts successfully, the following messages are displayed in the terminal console:

```
Shutting down Novell NCP/NSS IPC daemon...
```

```
Exited
```

```
Starting the Novell NCP/NSS IPC daemon.
```

8.8 Viewing File Events in the Shadow Volume's Audit Log

All moves between the primary storage area and the secondary storage area are logged as events to the shadow volume's audit log. An audit log for a given DST shadow volume is located in the `._NETWARE` directory located at the root of the primary volume. For NSS volumes, the default file path for the log is `/media/nss/volumename/._NETWARE/volumename.audit.log`.

For example, if the primary area is named `VOL1`, the audit file is `/media/nss/VOL1/._NETWARE/VOL1.audit.log`.

- 1 In Novell Remote Manager for Linux, log in as the `root` user.
- 2 Select *View File System > Dynamic Storage Technology Options*, locate the volume in the list, then click the *View Log* link next to it.

Volume Information		
Volume Name	Shadow Status	
① VOL1	Shadowed	Inventory View Log
① _ADMIN	No Shadow	Inventory
① SYS	Add Shadow	Inventory

- 3 When prompted, select whether to view the file in a text editor, or to save a copy to your local computer. (The “local computer” is the computer where you are running the Web browser for accessing the server via Novell Remote Manager.)

8.9 Backing Up DST Shadow Volumes

- ♦ [Section 8.9.1, “Planning Your Backup Solution,” on page 105](#)
- ♦ [Section 8.9.2, “Planning Your Restore Solution,” on page 105](#)
- ♦ [Section 8.9.3, “Using the /etc/NCPVolumes XML File for Backup,” on page 107](#)

- ♦ [Section 8.9.4, “Configuring the Backup Attribute for NSS Volumes,” on page 107](#)
- ♦ [Section 8.9.5, “Configuring Backup for Trustee Information on NSS Volumes on Linux,” on page 107](#)

8.9.1 Planning Your Backup Solution

Applications that directly access the local Linux file system see the primary file tree and the secondary file tree as independent subdirectories. The backup utility does not see the unified view of the file tree that the end user sees. Thus, backup tools can apply one backup policy to the primary file tree and a different backup policy to the secondary file tree. The only operations that take place on the secondary volume are backup, or “remove and archive”. Using shadow volumes allows backups of important data to be made faster and more frequently because you can apply different backup policies for the primary volume and secondary volume.

For example, the server administrator can partition the volume’s data into two categories:

- ♦ Important data that needs to be maintained on quality storage and backed up frequently.
- ♦ Less important data that can be stored on less expensive storage and backed up less frequently.

An analysis or inventory of a volume’s data shows that a large portion of it is seldom used. Having a shadow volume allows the server administrator to spend more on the most important data and spend less on the less important data. The frequently used data can be backed up nightly. The seldom-used data can be backed up weekly or monthly.

Getting the less important data out of the way enables the backups of your important data to run more quickly and efficiently. Partitioning your data in this way can significantly reduce the cost of hosting it.

Because the most important files are located in the primary storage area, disaster recovery can be faster, too. The server administrator can restore the critical files by restoring the primary storage area first, then restore the secondary storage area. This quickly gets the files they need most to users, and they do not need to wait while files they do not usually need are restored. In addition, more fault tolerant replication solutions can be deployed for the primary storage area where it matters most.

8.9.2 Planning Your Restore Solution

You can restore the data separately to each volume by using the backups you made of each area. If ShadowFS is running, you can also restore the data by using the ShadowFS local mount point in `/media/shadowfs/volumename` that presents a unified file tree that includes both volumes. The advantages and disadvantages of each restore option are described in [Table 8-6](#).

Table 8-6 *Comparison of Restore Options for DST Shadow Volumes*

Restore Option	Advantages	Disadvantages
Restore to the primary file tree and secondary file tree	<p>Files are copied directly to the primary volume and secondary volume, so there is no need for the information to be transferred again through policies.</p> <p>There is no performance hit when you restore directly to each volume like there is when restoring to the ShadowFS file tree.</p> <p>The restoration size is not an issue because you are restoring to the proper volume rather than through the ShadowFS file tree view.</p>	<p>Potential conflicts might occur by restoring duplicate versions of the file on each of the volumes. The duplicate files are resolved by DST global policies instead of being resolved by the backup software. By default, the duplicate files are allowed to coexist, and a conflict message is broadcast to users. For information about duplicate file resolution, see Section 4.6, “Configuring Global Policies for Resolving Instances of Duplicate Files,” on page 51.</p> <p>When restoring partial data, you need to know whether the most recent version of the data is located on the backup for the primary volume or the secondary volume.</p>
Restore to the ShadowFS file tree in <code>/media/shadowfs/volumename</code>	<p>The backup software sees both volumes through the unified file tree view. You can restore the primary volume, secondary volume, or both volumes through this view, and let any duplicates be handled by your backup software.</p> <p>Whether the data is on the backup for the primary volume or the backup for the secondary volume, if both are restored, the users’ data is restored.</p>	<p>The FUSE technology used by ShadowFS is slower than using the NCP view, but the backup software cannot see the NCP view.</p> <p>All files restored through the ShadowFS file tree view are copied to the primary volume. The data that you restore from the backup for the secondary volume is not returned to the secondary volume until you run policies or use inventory scans to move the data back to the secondary volume.</p> <p>Because all data is restored to the primary volume when you restore through the ShadowFS file tree view, it is possible to run out of space. The primary volume must be large enough to accommodate holding both volumes worth of data unless you restore in phases—that is, restore some directories, then shift data to the secondary, then restore more directories.</p>

8.9.3 Using the /etc/NCPVolumes XML File for Backup

By using the `/etc/NCPVolumes` XML file, a backup utility can easily locate each mounted NCP volume and find its primary and shadow file trees. The file contains an entry for each mounted volume. It lists the volume's name and the path for the volume's primary file tree (PRIMARY_ROOT). If the volume is a shadow volume, it also shows the path for the shadow file tree (SHADOW_ROOT).

For example, the following XML entry defines the DST shadow volume named VOL1. The volumes are NSS volumes, with VOL1 as the primary storage location, and ARCVOL as the secondary storage location.

```
<VOLUME>

  <NAME>VOL1</NAME>

  <PRIMARY_ROOT>/media/nss/VOL1</PRIMARY_ROOT>

  <SHADOW_ROOT>/media/nss/ARCVOL</SHADOW_ROOT>

</VOLUME>
```

8.9.4 Configuring the Backup Attribute for NSS Volumes

The Backup attribute must be enabled on the NSS volumes if you use the Novell Storage Management Services™ tools for backup of NSS volumes. The attribute is enabled by default when you create a new NSS volume.

To enable the Backup attribute for an existing NSS volume:

- 1 In iManager, click *Storage > Volumes*.
- 2 Select a server to manage to view a list of the NSS volumes on it.
- 3 In the *Volumes* list, select the volume that you want manage, then wait for the page to refresh to show the volume's details.
- 4 Click *Properties* to view the settings for the volume attributes.
- 5 On the Attributes tab, select the *Backup* attribute, then click *Apply*.

8.9.5 Configuring Backup for Trustee Information on NSS Volumes on Linux

If you plan to use a backup utility with DST, you might need to add an NSS attribute that allows for the backing up and restoring of file system trustee assignments, trustee rights, and inherited rights filters. NSS provides the `nss /ListXattrNWMetadata` switch to enable this capability. For information, see “[ListXattrNWmetadata Option](#)” in the *OES 2 SPI: NSS File System Administration Guide*.

Managing Policies for Shadow Volumes

9

This section describes how to configure and manage Dynamic Storage Technology policies for shadow volumes on a Novell® Open Enterprise Server (OES) 2 Linux server.

- ♦ [Section 9.1, “Understanding Shadow Volume Policy Options,” on page 109](#)
- ♦ [Section 9.2, “Creating a Shadow Volume Policy,” on page 115](#)
- ♦ [Section 9.3, “Modifying a Shadow Volume Policy,” on page 117](#)
- ♦ [Section 9.4, “Viewing DST Policies and Policy Status,” on page 117](#)
- ♦ [Section 9.5, “Deleting a Shadow Volume Policy,” on page 118](#)

For information about setting global policies for DST on the server, see [Chapter 4, “Installing and Configuring Dynamic Storage Technology,” on page 39](#).

9.1 Understanding Shadow Volume Policy Options

Shadow Volume policies manage how files are distributed across the shadow volume’s primary and secondary areas. A Shadow Volume policy allows you to specify when the policy is enforced (one time, hourly, daily, weekly, and so on), which volumes the policy applies to, which direction files are moved (primary area to its secondary area, or secondary area to its primary area), and which files are moved (by filename, file type, time stamps, or file size).

DST policies are configured in Novell Remote Manager for Linux. DST provides the following policy options:

- ♦ [Section 9.1.1, “Last Executed,” on page 109](#)
- ♦ [Section 9.1.2, “Description,” on page 110](#)
- ♦ [Section 9.1.3, “Start Time,” on page 110](#)
- ♦ [Section 9.1.4, “End Time,” on page 110](#)
- ♦ [Section 9.1.5, “Start Day,” on page 110](#)
- ♦ [Section 9.1.6, “Frequency,” on page 110](#)
- ♦ [Section 9.1.7, “Command Status,” on page 111](#)
- ♦ [Section 9.1.8, “Volume Selection,” on page 112](#)
- ♦ [Section 9.1.9, “Volume Operations,” on page 112](#)
- ♦ [Section 9.1.10, “Subdirectory Restrictions,” on page 112](#)
- ♦ [Section 9.1.11, “Search Criteria,” on page 113](#)

9.1.1 Last Executed

For an existing policy, the *Last Executed* parameter reports the last time the policy was run successfully. This parameter is not configurable.

9.1.2 Description

Description is the user-defined name for the policy. It should be descriptive of the policy it represents, and meaningful to the administrator. This name appears in the *Dynamic Storage Technology Policies* table on the main *Dynamic Storage Technology Options* page.

Description (required):

9.1.3 Start Time

Start Time specifies the time of day to begin a run to enforce the policy. For hourly policies, the policy enforcement begins at the selected minutes past each hour. Time is specified based on a 24-hour clock. For example, 18:00 (6:00 p.m.) is the default start time.

Start Time: :

9.1.4 End Time

End Time specifies the time of day to stop work on an enforcement run. Specifying an end time for a scheduled run allows you to prevent the policy enforcement from happening during busy work hours. Time is specified based on a 24-hour clock. For example, 07:00 (7:00 a.m.) is the default end time.

End Time: :

If the policy enforcement process is still running when the end time is reached, the policy's queued work is paused until the next scheduled run. When the policy run begins at its next scheduled time, it continues with the queued work, and adds new work to the end of the queue.

9.1.5 Start Day

For policies that run weekly, *Start Day* specifies the day of the week to enforce the policy. You can specify only one day of the week for a given policy. Options are *Saturday* (default), *Sunday*, *Monday*, *Tuesday*, *Wednesday*, *Thursday*, or *Friday*.

Start Day: (for weekly commands)
 (for one time or monthly commands)

For policies that are run one time or monthly, *Start Day* specifies the month and day of the month when the policy is scheduled to be enforced.

9.1.6 Frequency

Frequency specifies how often the policy is enforced when the *Command Status* is set to *Active*.

Table 9-1 describes each frequency option. The *Execute Now* option can be selected or deselected in combination with any one of the scheduled frequency options.

Frequency:

☐ One Time

☐ Hourly

☐ Daily

☒ Weekly

☐ Monthly

☐ Execute now

Table 9-1 Frequency Options for DST Policies

Option	Description
<i>One Time</i>	Whenever the policy's <i>Command Status</i> is set to <i>Active</i> , the policy runs one time, then changes the <i>Command Status</i> to <i>Inactive</i> . You can activate the policy to run again by changing its status.
<i>Hourly</i>	The policy enforcement process runs once each hour. It begins at the number of minutes past the hour specified by the <i>Start Time</i> . The process continues until it is done, or until the number of minutes past the hour specified by the <i>End Time</i> . Unfinished work is queued until the next run.
<i>Daily</i>	The policy enforcement process runs once each day. It begins at the time specified by the <i>Start Time</i> . The process continues until it is done, or until the time specified by the <i>End Time</i> . Unfinished work is queued until the next run.
<i>Weekly</i> (default)	The policy enforcement process runs once each week. It begins on the day of the week specified by the <i>Start Day</i> . The process continues until it is done, or until the time specified by the <i>End Time</i> . Unfinished work is queued until the next run.
<i>Monthly</i>	The policy enforcement process runs once each month. It begins on the month and day specified by the <i>Start Day</i> , then it runs every month afterwards on that day of the month. The process continues until it is done, or until the time specified by the <i>End Time</i> . Unfinished work is queued until the next run.
<i>Execute Now</i>	Select this option to run the policy now, in addition to its regularly scheduled runs. The policy enforcement process is initiated within a few minutes after the policy's <i>Command Status</i> is set to <i>Active</i> and saved (submitted). The process continues until it is done, or until the time specified by the <i>End Time</i> . Unfinished work is queued until the next run.

9.1.7 Command Status

Command Status governs whether a policy is actively enforced or inactive. Inactive policies can be changed back to active. New policies can be created and set to inactive without running them. Options are *Active* (default) and *Inactive*.

Command Status:

☒ Active

☐ Inactive

9.1.8 Volume Selection

Volume Selection allows you to specify the shadow volumes affected by a given policy. You can select one or multiple shadow volumes from a drop-down list of existing shadowed volumes, or select *All Shadowed Volumes*. You can have multiple policies associated with a given shadow volume. A given policy can apply to multiple shadow volumes.

Volume Selection:

All Shadowed Volumes ▼

When working with DST shadow volumes in a cluster, you should create separate policies for the shadow volumes that exist in a given cluster resource. A given policy can apply to multiple shadow volumes in the cluster resource. You can have multiple policies associated with a given shadow volume in the cluster resource.

9.1.9 Volume Operations

Volume Operations specifies the direction the files are moved between the primary storage location (primary area) and the secondary storage location (shadow area).

Volume Operations:

☒ Move selected files from primary area to shadow area.

☐ Move selected files from shadow area to primary area.

Table 9-2 *Volume Operations for a Policy*

Option	Description
<i>Move selected files from primary area to shadow area</i> (default)	When the policy is enforced, all files on the primary storage location that meet all of the search criteria are moved from the primary storage location to the secondary storage location.
<i>Move selected files from shadow area to primary area</i>	When the policy is enforced, all files on the secondary storage location that meet all of the search criteria are moved from the secondary storage location to the primary storage location.

9.1.10 Subdirectory Restrictions

In the *Subdirectory Restrictions* area, you specify the *Scope* and *Path* information that determines whether the policy applies to everything in a volume, to only to a specified subdirectory (and its contents), or to all directories but the one specified. Specify the path relative to the root of the DST volume, and not to the root of the server. For example, enter `subdir1/subdir2`.

Subdirectory Restriction:

Scope: None ▼

Path:

Table 9-3 describes the options for *Scope*:

Table 9-3 *Subdirectory Restrictions for the Scope of a Policy*

Option	Description
<i>None</i> (default)	The policy is enforced for all subdirectories in the volume. Do not specify a path.
<i>Apply only in subdirectory</i>	The policy is enforced only for a specified subdirectory and its contents. You must specify the Linux path to the directory on the primary volume. For example: /media/nss/VOL1/project_abc/videos
<i>Exclude subdirectory</i>	The policy is enforced for all subdirectories in the volume, except for the specified subdirectory and its contents. You must specify the Linux path to the directory on the primary volume. For example: /media/nss/VOL1/project_abc/contracts

9.1.11 Search Criteria

Files must match all of the specified criteria in order to be moved between the primary storage location and secondary storage location. Criteria options include filename or extension, time stamp, and file size. The conditions are combined (and-ed) together, which means that all conditions must be true for a file before it is queued for moving to the other location. Specify any of the following search criteria:

- ♦ “Search Pattern” on page 113
- ♦ “Time Stamp Restrictions” on page 113
- ♦ “File Size Restriction” on page 114

Search Pattern

Search Pattern allows you to set criteria based on the filename or extension. You can specify characters and wildcards to search by filename. You can specify files by types by specifying a wildcard and an extension, such as *.mp3. The default entry is *.* , which applies the policy to all filenames and all file types.

Search Pattern:

Time Stamp Restrictions

Time Stamp Restrictions identifies which of the time stamps to use when applying the policy.

Time Stamp Restrictions:

Time Stamp:

☐ Last Modified Time

☐ Last Accessed Time

☐ Last Changed Time

Time from now:

Direction:

Days:

Weeks:

Months:

Years:

The time stamp types are:

- ♦ **Last Time Modified:** Time of last content modification for the selected file.
- ♦ **Last Time Accessed:** Time of last access.
- ♦ **Last Time Changed:** Time of last file status change.

The default is no time restriction (all Time Stamp options are deselected), so the default policy applies the policy for all existing files.

These time stamps are defined by POSIX and supported by Linux. Many operations change more than one time stamp. NCP can modify the access time and the modify time, but cannot control whether the change time is reset. The Last Time Changed value is controlled automatically. For example, if you copy a file from one location to another, NCP preserves the access and modify times, but the change time is reset because the file's path changed. That is, it had a status change but the file was not opened for access and its data was not modified.

You must also specify the specific time period to use in *Time from Now*. Direction options are *Greater than* and *Less than*. Specify a direction, then select one of the time periods described in [Table 9-4](#).

Table 9-4 Time Periods for the Time Stamp Restrictions in a Policy

Option	Description
<i>Days</i>	Specify 0 to 14 days. 0 days (the default) disables the option.
<i>Weeks</i>	Specify 0 to 10 weeks. 0 weeks (the default) disables the option.
<i>Months</i>	Specify 0 to 24 months. 0 months (the default) disables the option.
<i>Years</i>	Specify 0 to 24 years. 0 years (the default) disables the option.

For example, you can select all files that have a modified time greater than 6 months by selecting *Last Time Modified* in the *Time Stamp* field, *Greater than* for the *Direction* field, and 6 in the *Months* field.

File Size Restriction

Specifies the range of file sizes to search. *Direction* specifies to look for files that are greater than or less than the specified size in KB. Specify a value of 0 KB to disable the file size restriction. The default is no size restriction, which applies the policy for files of all sizes.

File Size Restriction:

Direction:

Size (KB):

9.2 Creating a Shadow Volume Policy

- Section 9.2.1, “Prerequisite,” on page 115
- Section 9.2.2, “Guidelines for Shadow Volume Policies,” on page 115
- Section 9.2.3, “Creating a Shadow Volume Policy,” on page 115

9.2.1 Prerequisite

In order to configure policies that apply only to a specific shadow volume, the shadow volume must already be defined.

9.2.2 Guidelines for Shadow Volume Policies

- For each Dynamic Storage Technology shadow volume, you must establish at least one policy that controls how files are migrated from the primary storage area to the secondary storage area of the shadow volume, or vice versa.
- Any given shadow volume policy is best kept to a simple goal. Complex combinations of rules in a single policy can lead to confusion on how they are executed.
- You can have multiple policies associated with a given shadow volume.
- A given policy can apply to multiple shadow volumes.
- Multiple policies can be scheduled to be run concurrently.

9.2.3 Creating a Shadow Volume Policy

- 1 In Novell Remote Manager for Linux, select *View File System*, then select *Dynamic Storage Technology Options* to open the Dynamic Storage Technology Options page.

Initially, no policies are defined, so you do not see a policy report.

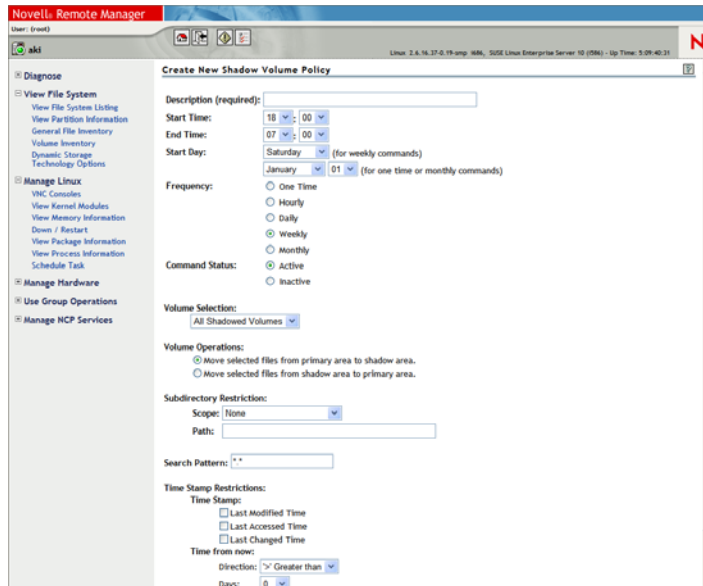
No Dynamic Storage Technology policies defined.

[Create a new policy](#)

After one or more policies are defined, the policies are reported in a table.

Dynamic Storage Technology Policies			
Name	Volume	Last Executed	Total Files Moved
ProjectABC Exclude contracts	All Shadowed Volumes	Not executed	0
Create a new policy			

- 2 Beneath the list of *Dynamic Storage Technology Policies*, click *Create a New Policy* to open a page where you can configure a new storage policy.



- 3 On the *Create New Shadow Volume Policy* page, specify a name for the policy in the *Description* field.

The name should be descriptive of the policy it represents, and meaningful to the administrator.

For example, suppose you plan to create a policy for a shadow volume used by Project ABC, and exclude the path to the `contracts` directory. You might name the policy *Project ABC Exclude contracts*.

- 4 On the *Create New Shadow Volume Policy* page, configure policy settings.

For information about policy options, see [Section 9.1, “Understanding Shadow Volume Policy Options,”](#) on page 109.

- 5 Specify the *Command Status* as *Active* or *Inactive*.

A policy’s state must be active in order for it to run.

- 6 If you want the policy changes to be enforced sooner than the next scheduled run, make sure to select *Execute Now* in the *Frequency* area.

The process is triggered for a run within a few minutes after you save (submit) the policy.

- 7 Click *Submit* (at the bottom of the page) in order to save the policy, and to schedule it if it is Active.

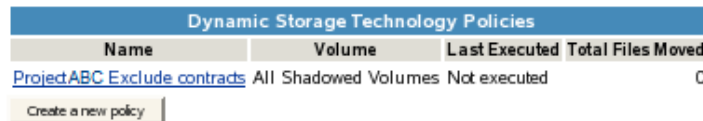
The new policy is listed in the *Dynamic Storage Technology Policies* report on the Dynamic Storage Technology Options page.

Dynamic Storage Technology Policies			
Name	Volume	Last Executed	Total Files Moved
ProjectABC Exclude contracts	All Shadowed Volumes	Not executed	0
Create a new policy			

9.3 Modifying a Shadow Volume Policy

You can modify a shadow volume policy at any time. For example, if the planned migration activity for a policy is not completed in the allowed time, you can adjust the policy run times and frequency until it meets your workload needs. Modified policies take effect the next time the policy is run, and do not affect currently running processes.

- 1 In Novell Remote Manager for Linux, select *View File System*, then select *Dynamic Storage Technology Options* to open the Dynamic Storage Technology Options page.



Dynamic Storage Technology Policies			
Name	Volume	Last Executed	Total Files Moved
ProjectABC Exclude contracts	All Shadowed Volumes	Not executed	0

Create a new policy

- 2 In the list of *Dynamic Storage Technology Policies*, click the *Name* link for the policy in order to view and modify the individual settings for the policy.
- 3 On the View/Edit Shadow Volume Policy page, view and modify the policy settings.
For information about policy settings, see [Section 9.1, “Understanding Shadow Volume Policy Options,” on page 109](#).
- 4 Specify the *Command Status* as *Active* or *Inactive*.
A policy’s state must be active in order for it to run.
- 5 If you want the policy changes to be enforced sooner than the next scheduled run, make sure to select *Execute Now* in the *Frequency* area.
If the policy is not currently running, the policy runs within a few minutes after you click *Submit* in [Step 6](#).
If the policy is currently running, the updated policy does not run until the current run stops. That means the updated policy process is triggered for a run within a few minutes after the currently running process completes or reaches the previously set *End Time*.
- 6 If you make any changes, you must click *Submit* (at the bottom of the page) in order for the changes to take effect at the next scheduled run.

9.4 Viewing DST Policies and Policy Status

After you create DST policies, the Dynamic Storage Technology Policies table reports a list of policies, and information such as the shadow volumes to which the policy applies, when the policy was last executed, and the total number of files moved in the last run for that policy.

- 1 In Novell Remote Manager for Linux, select *View File System*, then select *Dynamic Storage Technology Options* to open the Dynamic Storage Technology Options page.

Initially, no policies are defined.



No Dynamic Storage Technology policies defined.
Create a new policy

After one or more policies are defined, the policies are reported in a table.

Dynamic Storage Technology Policies			
Name	Volume	Last Executed	Total Files Moved
ProjectABC Exclude contracts	All Shadowed Volumes	Not executed	0
Create a new policy			

- 2 View the following summary of information about all current policies on the server:

Parameter	Description
Name	The administrator-defined description of the policy. You specify the name in the <i>Description</i> field in the policy form.
Volumes	A list of shadow volumes to which the policy applies. These are specified in <i>Volume Selection</i> field of the policy form.
Last Executed	The time the policy was last enforced.
Total Files Moved	The number of files moved between the primary storage location and the secondary storage location the last time the policy ran.

- 3 Click the *Name* link for the policy to view or modify the individual settings for the policy.
- 4 On the View/Edit Shadow Volume Policy page, view or modify the policy settings.
For information about policy settings, see [Section 9.1, “Understanding Shadow Volume Policy Options,” on page 109](#).
- 5 If you make any changes, you must click *Submit* (at the bottom of the page) in order for the changes to take effect.

9.5 Deleting a Shadow Volume Policy

You can delete a shadow volume policy at any time. If a policy is currently running, the policy is deleted after the process completes its run or reaches the previously set End Time.

- 1 In Novell Remote Manager for Linux, select *View File System*, then select *Dynamic Storage Technology Options* to open the Dynamic Storage Technology Options page.

Dynamic Storage Technology Policies			
Name	Volume	Last Executed	Total Files Moved
ProjectABC Exclude contracts	All Shadowed Volumes	Not executed	0
Create a new policy			

- 2 In the list of *Dynamic Storage Technology Policies*, click the *Name* link for the policy in order to view and delete the policy.
- 3 On the View/Edit Shadow Volume Policy page, scroll to the bottom of the page, then click *Delete*.

If the policy is not currently running, it is deleted immediately.

If the policy is currently running, it is deleted after the process stops.

Monitoring DST Shadow Volumes

10

In Novell® Remote Manager for Linux, you can view reports for the DST shadow volume, with statistics and information about files in the primary file tree and secondary file tree.

- ♦ [Section 10.1, “Understanding the Shadow Volume Inventory,” on page 119](#)
- ♦ [Section 10.2, “Accessing the Shadow Volume Inventory,” on page 127](#)
- ♦ [Section 10.3, “Viewing Statistics for the Shadow Volume,” on page 127](#)
- ♦ [Section 10.4, “Using Inventory Detail Reports to Move, Copy, or Delete Files on the Shadow Volume,” on page 128](#)
- ♦ [Section 10.5, “Generating a Custom Inventory Report,” on page 128](#)

10.1 Understanding the Shadow Volume Inventory

The inventory reports key statistics about the files in the selected volume, such as files scanned and the available space trends. The inventory reports the following information:

- ♦ [Section 10.1.1, “Inventory Summary,” on page 119](#)
- ♦ [Section 10.1.2, “Available Space Trends,” on page 120](#)
- ♦ [Section 10.1.3, “Graphical Profiles,” on page 121](#)
- ♦ [Section 10.1.4, “Tabular Profiles,” on page 124](#)
- ♦ [Section 10.1.5, “Inventory Detail Reports,” on page 125](#)
- ♦ [Section 10.1.6, “Custom Shadow Volume Options,” on page 125](#)

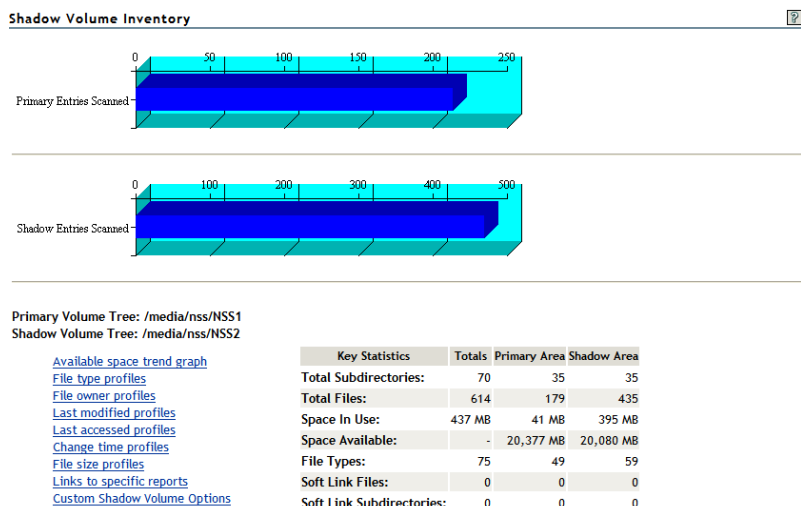
10.1.1 Inventory Summary

The inventory summary reports the number of files scanned on the primary storage area and the secondary storage area. It also reports key statistics for the primary storage area, the secondary storage area, and both areas combined as the shadow volume.

Key Statistics	Description
Total Subdirectories	The total number of subdirectories in the volume.
Total Files	The total number of files in the volume.
Space in Use	The amount of space currently in use in the volume for data and metadata. On NSS volumes where salvage is enabled, the space in use includes space used by deleted files and directories.
Space Available	The amount of free space in the volume.
File Types	The number of different file types in use throughout the entire volume.
Soft Link Files	The NSS file system and NCP Server do not support soft links to files. In the initial release of DST, this is a placeholder for future non-NCP support.

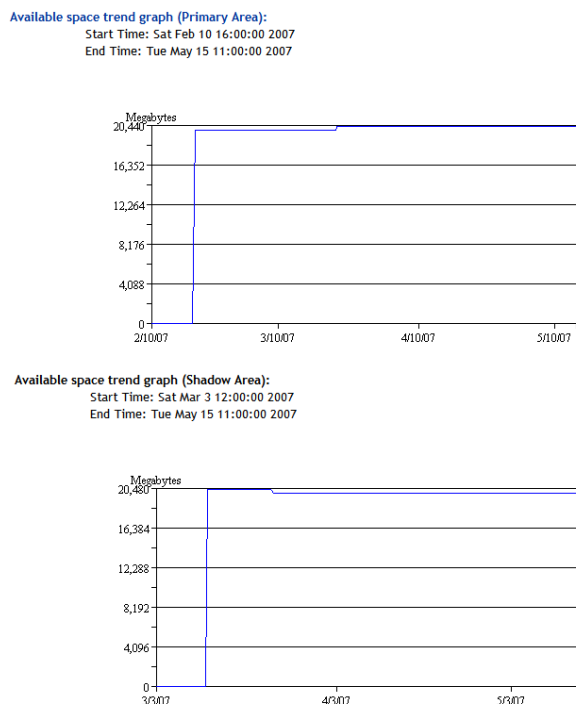
Key Statistics	Description
Soft Link Subdirectories	The NSS file system and NCP Server do not support soft links to subdirectories. In the initial release of DST, this is a placeholder for future non-NCP support.

The following figure is an example of the summary:



10.1.2 Available Space Trends

The *Available Space Trends* report shows the trends for space usage on the primary storage area and the secondary storage area. The following figure is an example of the *Available Space Trend* graphs:



10.1.3 Graphical Profiles

The *Profiles* portion of the inventory report graphically displays information about the shadow volume. Graphical profiles are displayed by size in bytes and file count for the following categories:

- ◆ “File Type Profiles” on page 121
- ◆ “File Owner Profiles” on page 122
- ◆ “Time Stamp Profiles” on page 122
- ◆ “File Size Profiles” on page 123

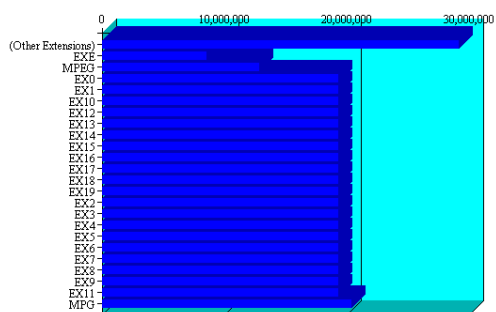
File Type Profiles

File Type Profiles indicates storage space usage by file types that are actually in use on your system, such as LOG, TDF, DAT, XML, EXE, and so on.

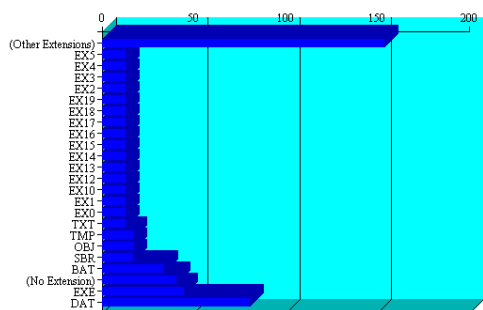
The following figure is an example of the *File Type Profiles* graphs:

File type profiles:
Data Tables:

File Types (By Bytes In Use)



File Types (By File Count)

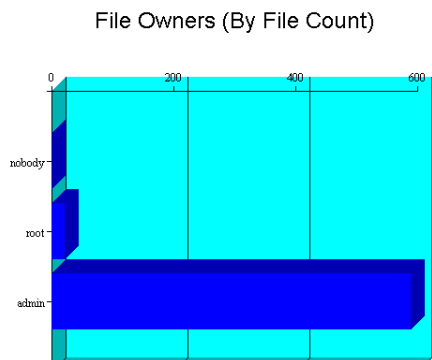
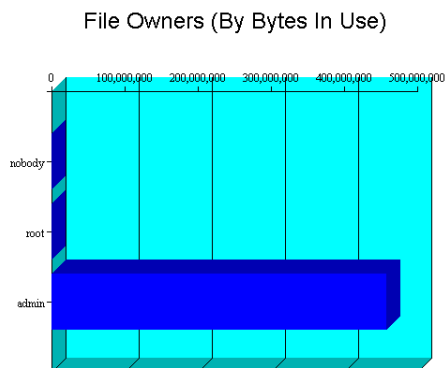


File Owner Profiles

File Owner Profiles indicates storage space usage by the designated owner of the file. It is not unusual in NCP to see the `root` user as the owner of files. For NCP volumes and NSS, file access is governed by the file system trustees assigned to the file, not the file owner. Trustees are users who have User objects defined in Novell eDirectory™, and who have been granted file system rights for the file. NCP tracks ownership via the user's eDirectory GUID.

The following figure is an example of the *File Owner Profiles* graphs.

[File owner profiles:](#)
[Data Tables:](#)



Time Stamp Profiles

Three time stamp profiles are generated:

- ◆ **Files Modified Profiles:** Modified dates indicate the last time someone changed the contents of a file.
- ◆ **Files Accessed Profiles:** Access dates indicate the last time someone accessed a file, but did not change the contents if this differs from the modified date.
- ◆ **Files Changed Profiles:** Change dates indicate the last time someone changed the metadata of a file, but did not change the contents if this differs from the modified date.

Time stamps are grouped by the following time periods:

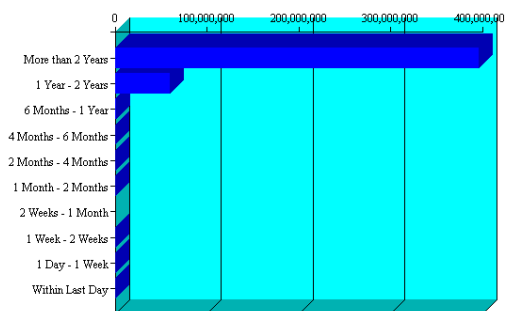
More than 2 years
1 year to 2 years

6 months to 1 year
 4 months to 6 months
 2 months to 4 months
 1 month to 2 months
 2 weeks to 1 month
 1 week to 2 weeks
 1 day to 1 week
 Within last day

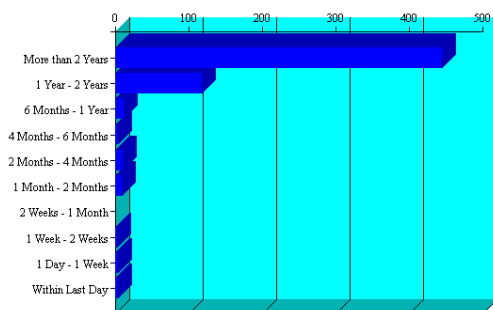
The following figure is an example of the *File Modified Profiles* graphs. Similar graphs are created for *File Accessed Profiles* and *File Changed Profiles*.

[Last modified profiles:](#)
[Data Tables:](#)

Last Modified Times (By Bytes In Use)



Last Modified Times (By File Count)



File Size Profiles

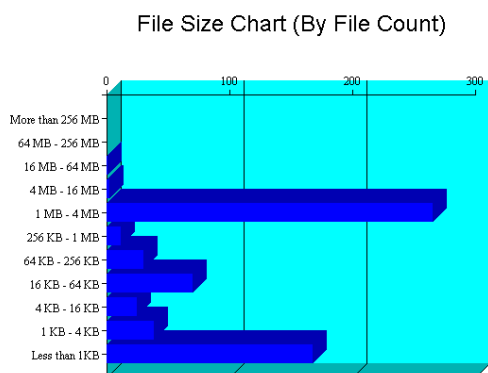
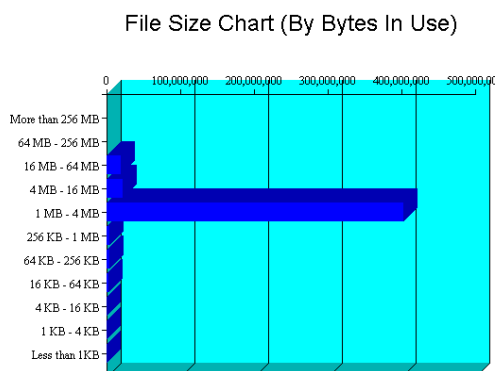
File Size Profiles reports the size of files, grouped by the following size ranges:

More than 256 MB
 64 MB to 256 MB
 16 MB to 64 MB
 4 MB to 16 MB
 1 MB to 4 MB
 256 KB to 1 MB

64 KB to 256 KB
 16 KB to 64 KB
 4 KB to 16 KB
 1 KB to 4 KB
 Less than 1 KB

The following figure is an example of the *File Size Profiles* graphs:

[File size profiles:](#)
[Data Tables:](#)



10.1.4 Tabular Profiles

Statistical data used to create the graphs is also available in tables that report statistics for the primary area, the secondary area, and both areas combined as the shadow volume. The count for file entries for the primary area and shadow (secondary) area are linked to detail reports that list the files matching that particular category and group. From the file lists, you have the option to copy, move, or delete one or multiple files.

For example, the following figure shows a few lines of a file-type information table:

File Extension	Total Space In Use	Total File Count	Primary Space	Primary Files	Shadow Space	Shadow Files
MPG	20,460,496	1	0	0	20,460,496	1
EX0	19,358,676	13	1,335,920	1	18,022,756	12
EX1	19,358,676	13	1,335,920	1	18,022,756	12

10.1.5 Inventory Detail Reports

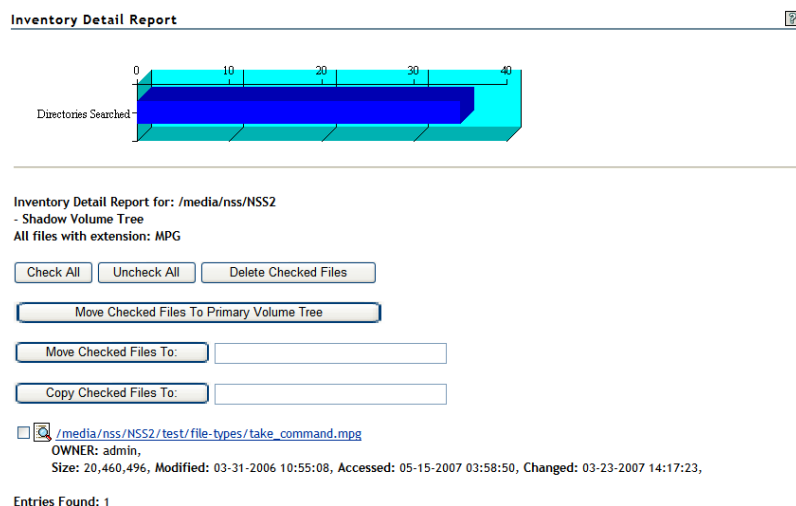
An *Inventory Detail Report* lists all of the files that match a particular category and group for a file count entry in the tabular reports in the shadow volume inventory. You can select one or multiple files in the list, then select one of the following operations to be performed:

- ♦ Move the selected volumes to the other file tree.
- ♦ Move the selected files to a specified path on the server.
- ♦ Copy the selected files to a specified path on the server.
- ♦ Delete the selected files.

The action is performed on the selected files, and a confirmation list is displayed.



The following figure is an example of a detail report for file types that reside on the secondary volume:



10.1.6 Custom Shadow Volume Options

The *Custom Shadow Volume Options* section of the volume inventory allows you to generate reports based on key statistics of interest, and perform actions on them.

- ♦ “Volume Operations” on page 126
- ♦ “Search Patterns” on page 126
- ♦ “File Owner Restrictions” on page 126
- ♦ “Time Stamp Restrictions” on page 126
- ♦ “File Size Restrictions” on page 126

Volume Operations

You can perform one of the following volume operations on the files that match the search criteria you specify:

- ♦ List primary area selected files
- ♦ Move selected files from primary area to shadow area.
- ♦ List shadow area selected files.
- ♦ Move selected files from shadow area to primary area.

Search Patterns

In *Search Patterns*, you can specify wildcards and characters to select files by filenames or extensions.

File Owner Restrictions

In *File Owner Restrictions*, select *None* or a user name. The search applies only to files where the file owner matches the specified owner.

Time Stamp Restrictions

You can specify one or multiple time stamps to consider for the search:

- ♦ Last Modified Time
- ♦ Last Accessed Time
- ♦ Last Changed Time

If no time stamp is selected, time stamps are not considered in the search criteria.

If a time stamp is selected, you can specify one or multiple time ranges to consider for the search:

Within last day

1 day to 1 week

1 week to 2 weeks

2 weeks to 1 month

1 month to 2 months

2 months to 4 months

4 months to 6 months

6 months to 1 year

1 year to 2 years

More than 2 years

File Size Restrictions

You can specify one or multiple ranges of file sizes to consider for the search:

Less than 1 KB

1 KB to 4 KB

4 KB to 16 KB

16 KB to 64 KB

64 KB to 256 KB
256 KB to 1 MB
1 MB to 4 MB
4 MB to 16 MB
16 MB to 64 MB
64 MB to 256 MB
More than 256 MB

10.2 Accessing the Shadow Volume Inventory

- 1 Open Novell Remote Manager for Linux in a Web browser, then log in as the `root` user.
- 2 Use one of the following methods to view the volume inventory:
 - ♦ Select *View File System > Dynamic Storage Technology Options*, locate the volume in the list, then click the *Inventory* link next to it.

Volume Information		
Volume Name	Shadow Status	
① VOL1	Shadowed	Inventory View Log
① _ADMIN	No Shadow	Inventory
① SYS		Add Shadow Inventory

- ♦ Select *View File System > Volume Inventory*, locate the volume in the *NCP Volumes Available for Inventory* list, then click the *Volume* link for the volume.

Volume Inventory		?
NCP Volumes available for Inventory		
Volume	Mount Point	
SYS	(/usr/novell/sys)	
_ADMIN	(/_admin)	
VOL1	(/media/nss/VOL1)	

10.3 Viewing Statistics for the Shadow Volume

- 1 In Novell Remote Manager, access the volume inventory for the shadow volume.
For information, see [Section 10.2, “Accessing the Shadow Volume Inventory,” on page 127](#).
- 2 In the inventory summary area, click a link to go directly to one of the following reports, or scroll to view the reports. For information about each statistical report, see [Section 10.1, “Understanding the Shadow Volume Inventory,” on page 119](#).
 - ♦ Available space trend graph
 - ♦ File type profiles
 - ♦ File owner profiles
 - ♦ Last modified profiles
 - ♦ Last accessed profiles
 - ♦ Change time profiles
 - ♦ File size profiles

- ♦ Links to specific reports
 - ♦ Custom shadow volume options
- 3 Click the *Data Tables* link for a profile to jump directly to the tabular display of the information that was used to generate the graph.

10.4 Using Inventory Detail Reports to Move, Copy, or Delete Files on the Shadow Volume

- 1 In Novell Remote Manager, access the volume inventory for the shadow volume.
For information, see [Section 10.2, “Accessing the Shadow Volume Inventory,” on page 127](#).
- 2 In the summary area, click *Links to Specific Reports*, or scroll down to the *Links to Specific Reports* section to view the tabular reports of information used to generate the profiles.
- 3 Review the following categories to locate the files of interest:
 - ♦ Last modified range
 - ♦ Last accessed range
 - ♦ Change time range
 - ♦ File size range
 - ♦ File owner
 - ♦ File extension
- 4 Click the link of the data entry for the files that you want to manage. Files are grouped by Primary area and by shadow (secondary) area.
- 5 In the *Inventory Detail Report*, select one or multiple files in the list, then do one of the following:
 - ♦ Move the selected volumes to the other file tree (primary or shadow (secondary) file tree).
 - ♦ Move the selected files to a specified path on the server.
 - ♦ Copy the selected files to a specified path on the server.
 - ♦ Delete the selected files.

10.5 Generating a Custom Inventory Report

You can customize the inventory report to limit the search sizes and times reported. The reporting criteria can be combinations of the specific categories described in [Section 10.1.6, “Custom Shadow Volume Options,” on page 125](#).

- 1 In Novell Remote Manager, access the volume inventory for the shadow volume.
For information, see [Section 10.2, “Accessing the Shadow Volume Inventory,” on page 127](#).
- 2 Scroll down to the *Custom Shadow Volume Options* area at the end of the shadow volume inventory.

Custom Shadow Volume Options

Volume Operations:

- ☒ List primary area selected files.
- ☐ Move selected files from primary area to shadow area.
- ☐ List shadow area selected files.
- ☐ Move selected files from shadow area to primary area.

Search Pattern:

File Owner Restriction:

Time Stamp Restrictions:

Time Stamp:

- ☐ Last Modified Time
- ☐ Last Accessed Time
- ☐ Last Changed Time

Range:

- ☐ Within Last Day
- ☐ 1 Day - 1 Week
- ☐ 1 Week - 2 Weeks
- ☐ 2 Weeks - 1 Month
- ☐ 1 Month - 2 Months
- ☐ 2 Months - 4 Months
- ☐ 4 Months - 6 Months
- ☐ 6 Months - 1 Year
- ☐ 1 Year - 2 Years
- ☐ More than 2 Years

File Size Restriction:

- ☐ Less than 1KB
- ☐ 1 KB - 4 KB
- ☐ 4 KB - 16 KB
- ☐ 16 KB - 64 KB
- ☐ 64 KB - 256 KB
- ☐ 256 KB - 1 MB
- ☐ 1 MB - 4 MB
- ☐ 4 MB - 16 MB
- ☐ 16 MB - 64 MB
- ☐ 64 MB - 256 MB
- ☐ More than 256 MB

3 In *Volume Operations*, select one of the following actions to perform on the files that meet the search criteria you specify for the scan in later steps.

- ♦ List primary area selected files
- ♦ Move selected files from primary area to shadow area.
- ♦ List shadow area selected files.
- ♦ Move selected files from shadow area to primary area.

4 In *Search Patterns*, specify wildcards and characters to select files by filename or extension. The default is **.**, which does not restrict the search to specific filenames or extensions; all files are considered.

5 (Optional) In *File Owner Restrictions*, select *None*, or select a username from the drop-down list.

If *None* is selected, file ownership is not considered for the search. If a username is specified, the search applies only to files where the file owner matches the specified owner.

6 (Optional) In *Time Stamp*, specify one or multiple time stamps to be searched. If none are selected, the time stamps are not considered when searching.

- ♦ Last Modified Time

- ♦ Last Accessed Time
 - ♦ Last Changed Time
- 7** In *Range*, if you specified a time stamp restriction, specify one or multiple ranges to be searched.
- Within last day
 1 day to 1 week
 1 week to 2 weeks
 2 weeks to 1 month
 1 month to 2 months
 2 months to 4 months
 4 months to 6 months
 6 months to 1 year
 1 year to 2 years
 More than 2 years
- 8** (Optional) In *File Size Restrictions*, specify one or multiple file sizes to be searched.
- Less than 1 KB
 1 KB to 4 KB
 4 KB to 16 KB
 16 KB to 64 KB
 64 KB to 256 KB
 256 KB to 1 MB
 1 MB to 4 MB
 4 MB to 16 MB
 16 MB to 64 MB
 64 MB to 256 MB
 More than 256 MB
- 9** After you specify the volume operation and search criteria, click *Start Scan*.
- 10** If you chose to list the files, an Inventory Detail Report is generated where you can move, copy, or delete files.
- 10a** Select one or multiple files in the list, then select one of the following actions:
- ♦ *Move the selected volumes to the other file tree.*
 - ♦ *Move the selected files to a specified path on the server.*
 - ♦ *Copy the selected files to a specified path on the server.*
 - ♦ *Delete the selected files.*
- 10b** Click *OK* to confirm the action.
- The action is performed on the selected files, then a confirmation list of the files and the number of files moved is displayed.

Volume Inventory



Moved: /media/nss/ARCVOL/hello~

Total files moved: 1

If you chose to move selected files from one volume to another, the files that meet the search criteria are automatically moved, then a confirmation list of the files and the number of entries moved is displayed.

Volume Inventory

Custom file move from Primary tree to Shadow tree
All files matching selected filter:

Moved: /media/nss/VOL1/dir1/hello
Moved: /media/nss/VOL1/dir2/hello
Moved: /media/nss/VOL1/hello
Moved: /media/nss/VOL1/hello~
Entries Moved: 4

- 11 If you view the inventory chart again after the move, you can see that the files that matched the specified criteria before the move are now reported on the other volume.

Configuring DST Shadow Volumes with Novell Cluster Services for Linux

11

Dynamic Storage Technology shadow volume pairs on Novell® Open Enterprise Server (OES) 2 Linux servers can be configured as cluster resources in a cluster with Novell Cluster Services™ for Linux.

- ♦ [Section 11.1, “Planning for Shadow Volumes in a Cluster Environment,” on page 133](#)
- ♦ [Section 11.2, “Preparing the Nodes to Support DST in a Cluster Environment,” on page 136](#)
- ♦ [Section 11.3, “Preparing the NSS Volumes for Use in a Clustered Shadow Volume,” on page 136](#)
- ♦ [Section 11.4, “Configuring the Cluster Load Script for Shadow Volumes Based on NSS Volumes,” on page 136](#)
- ♦ [Section 11.5, “Configuring Shadow Volume Policies for the Clustered Shadow Volume,” on page 144](#)
- ♦ [Section 11.6, “Removing a Clustered DST Shadow Volume,” on page 144](#)

11.1 Planning for Shadow Volumes in a Cluster Environment

Use the prerequisites and guidelines in this section when planning your cluster solution for Dynamic Storage Technology shadow volumes.

- ♦ [Section 11.1.1, “Prerequisites for Using Shadow Volumes in a Cluster,” on page 133](#)
- ♦ [Section 11.1.2, “Guidelines for Load Scripts for the Cluster Resource for the Shadow Volume Pair,” on page 135](#)

11.1.1 Prerequisites for Using Shadow Volumes in a Cluster

The prerequisites in this section apply for all shadow volume pairs in a cluster:

- ♦ [“Novell Open Enterprise Server 2 Linux” on page 134](#)
- ♦ [“Novell Cluster Services for Linux” on page 134](#)
- ♦ [“NCP Server and Dynamic Storage Technology” on page 134](#)
- ♦ [“Shareable Partitions” on page 134](#)
- ♦ [“File Systems” on page 135](#)
- ♦ [“Remote Volumes” on page 135](#)
- ♦ [“Novell iManager 2.7” on page 135](#)
- ♦ [“Novell Remote Manager for Linux” on page 135](#)

Novell Open Enterprise Server 2 Linux

Dynamic Storage Technology runs only on OES 2 Linux servers. Each node that hosts shadow volumes in the cluster must be running OES 2 Linux. For information about installing and configuring OES 2 Linux, see the *OES2 SP1: Linux Installation Guide*.

Novell Cluster Services for Linux

Dynamic Storage Technology supports Novell Cluster Services for Linux running on OES 2 Linux servers. For information, see “[Installing Novell Cluster Services on OES 2 Linux](#)” in the *OES 2 SP1: Novell Cluster Services 1.8.5 for Linux Administration Guide*.

In a mixed platform cluster, you cannot migrate or fail over the shadow volume’s cluster resource from an OES 2 Linux server to a NetWare[®] server or to an OES 1 Linux server. Make sure that you specify only OES 2 Linux nodes as failover candidates for the shadow volume’s cluster resource.

NCP Server and Dynamic Storage Technology

The NCP™ (NetWare Core Protocol™) Server and the Dynamic Storage Technology software are not cluster aware. They must be installed on every OES 2 Linux node in the cluster where you plan to migrate or fail over the cluster resource that contains shadow volumes. You do not cluster NCP Server or DST services.

Install NCP Server and DST on each cluster node, just as you would for an individual server. Make sure that the same global policies are configured on each node where you want to fail over the cluster resource. For install information, see [Section 4.3, “Installing NCP Server and Dynamic Storage Technology on Nodes in a Novell Cluster Services for Linux Cluster,”](#) on page 45.

Set up the shadow volume and its DST policies on the first node in the cluster, then copy that shadow volume’s configuration information from the `/etc/opt/novell/ncpserv.conf` file and the `/etc/opt/novell/ncp2nss.conf` file to those configuration files on each cluster where you want to fail over the cluster resource. You do not copy the entire files, because each server’s configuration files contain information specific to the server and might also contain definitions for other shadow volumes that reside on or fail over to the server. For instructions, see [Section 11.2, “Preparing the Nodes to Support DST in a Cluster Environment,”](#) on page 136.

When working with DST shadow volumes in a cluster, the individual shadow volume policies need to be able to fail over with the volume. You should create separate individual policies for each shadow volume, or make sure that the policy applies only to the shadow volumes that exist in a given cluster resource. A given policy can apply to multiple shadow volumes in the cluster resource. You can have multiple policies associated with a given shadow volume in the cluster resource.

Shareable Partitions

The primary volume and secondary volume in the shadow pair must each reside on a shareable partition. The devices are used in different cluster resources, but are managed in the same load script and unload script so they can be failed over together.

For information about creating shared NSS disk partitions and pools on Linux, “[Creating NSS Shared Disk Partitions and Pools](#)” in the *OES 2 SP1: Novell Cluster Services 1.8.5 for Linux Administration Guide*.

File Systems

In a cluster environment, Dynamic Storage Technology supports shadow volumes created with pairs of NSS volumes that each reside on a clustered pool. You must create the two NSS volumes on separate shared disks before you create the shadow volume relationship for the two volumes.

The NSS volumes that form the shadow volume must be able to fail over or migrate together. To do this, both volumes must be managed in the same load script and unload script. You create cluster resources for each shared pool, then combine the scripts in the proper order so that secondary resources are available first for the primary resource to use.

When you create an NSS volume by using NSS management tools, NSS automatically creates a Volume object for it. If the volume is unshared, the object is associated with the server where the volume is created. If the volume is in a shared pool, the volume is associated with the virtual cluster server name and IP address for that shared pool.

Remote Volumes

Dynamic Storage Technology does not support using remote volumes in DST shadow volumes in a cluster. The secondary volume must be on the same OES 2 Linux server in order for the resources to be failed over together to other OES 2 Linux nodes in the cluster.

Novell iManager 2.7

You use the NSS plug-in to iManager 2.7 to create clustered pools for the NSS volumes you use in the shadow volume. You use the Clustering plug-in to iManager 2.7 to configure cluster resources, load scripts, and unload scripts.

Novell Remote Manager for Linux

When using Novell Remote Manager for Linux to manage policies for the shadow volume, you typically connect to the IP address of the cluster resource for the primary storage location in the shadow volume. You can also connect to the IP address of the server node where the cluster resource is currently mounted.

11.1.2 Guidelines for Load Scripts for the Cluster Resource for the Shadow Volume Pair

Make sure that your cluster load script allows a wait time after activating the pools and after mounting the NSS volumes on Linux. This ensures that both volumes are properly mounted and available on Linux before you mount the shadow volume for NCP Server. You mount the shadow volume by mounting its primary volume for NCP Server.

For example, you add a `sleep` command with a delay of 10 to 20 seconds after mounting the two NSS volumes in NSS.

```
sleep 10
```

After a failover, if the volumes are not mounting properly in NCP Server, increase the sleep time value until it allows sufficient time for the volumes to be mounted on Linux before continuing.

11.2 Preparing the Nodes to Support DST in a Cluster Environment

The following checklist details the tasks you must perform to prepare your NCP volumes to be shadowed in a cluster on an OES 2 Linux node.

- ❑ Install and configure Novell Cluster Services for Linux on each of the OES 2 Linux servers in the cluster. For information, see the *OES 2 SP1: Novell Cluster Services 1.8.5 for Linux Administration Guide*.
- ❑ Install NCP Server and DST on each node in the cluster, then configure the same DST global policies on each node. For information, see [Chapter 4, “Installing and Configuring Dynamic Storage Technology,”](#) on page 39.
- ❑ If you are configuring access for CIFS/Samba clients, configure ShadowFS and Samba for each node in the cluster.

For information about setting up ShadowFS and Samba, see [Chapter 5, “Installing and Configuring Shadow File System \(ShadowFS\) for CIFS/Samba Users,”](#) on page 59.

For information about configuring Samba, see the *OES2 SP1: Samba Administration Guide*.

11.3 Preparing the NSS Volumes for Use in a Clustered Shadow Volume

- ❑ You need two NSS volumes, each in its own clustered pool. For instructions for creating the clustered pools and the NSS volumes, see [Section 8.2, “Creating NSS Volumes to Use in the DST Shadow Volume Pair,”](#) on page 82.
- ❑ If the NSS volume you want to use as the secondary volume is an old volume, and the volume you want to use as the primary volume is a new volume, you need to copy the trustee information from the old volume to the new volume. For information, see [Section 8.4.2, “Preparing the NSS Volumes for Use in a DST Shadow Volume,”](#) on page 95.

11.4 Configuring the Cluster Load Script for Shadow Volumes Based on NSS Volumes

- [Section 11.4.1, “Creating a Shadow Volume in the Load Script,”](#) on page 136
- [Section 11.4.2, “Overview of Cluster Resource Setup,”](#) on page 137
- [Section 11.4.3, “Viewing or Modifying Cluster Load and Unload Scripts,”](#) on page 138
- [Section 11.4.4, “Configuring the Load and Unload Scripts for a Shadow Volume,”](#) on page 140

11.4.1 Creating a Shadow Volume in the Load Script

In a cluster environment, you configure the shadow volumes in the cluster load script so that it defines the NCP volume as it loads. The clustered shadow volume is not permanently defined in the `/etc/opt/novell/ncpserv.conf` files of each node. It is added to the server's `/etc/opt/novell/ncpserv.conf` file when the system fails over to that node.

```
exit_on_error ncpcon mount volumename=volID,SHADOWVOLUME=shadow_volumename
```


Use this command in a cluster load script when the primary volume is an NSS volume and the secondary volume is an NSS volume. Both NSS volumes must already exist and be mounted in NSS.

Replace *volID* with a value from 0 to 254 as the server volume ID to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource.

For example, the following command mounts the NSS volume named VOL1 with a volume ID of 254. The primary volume is an existing NSS volume named VOL1 (/media/nss/VOL1). The secondary volume is an existing NSS volume named ARCVOL (/media/nss/ARCVOL).

```
exit_on_error ncpcon mount VOL1=254,SHADOWVOLUME=ARCVOL
```

Use the Clustering plug-in for iManager to modify the load scripts. You must combine information from the load scripts for the two clustered resources to create a single load script. This process is described in the following sections.

11.4.2 Overview of Cluster Resource Setup

The cluster load scripts elsewhere in this section assume the following setup for your NSS volumes that you want to use in the clustered shadow volume. Make sure to substitute the actual information from your setup.

Setup	Primary NSS Volume	Secondary NSS Volume
Server name for node 1	server38	server38
Cluster server name for node 1	NCS1	NCS1
Cluster pool name	POOL1	ARCPPOOL1
Clustered resource virtual server name	NCS1_POOL1_SERVER	NCS1_ARCPPOOL1_SERVER
Cluster resource IP address	10.10.10.38 You use the IP address for the primary pool's cluster resource for the shadow volume.	10.10.10.39 You use the secondary IP address only when managing the secondary NSS volume as an independent volume.
NSS volume name	VOL1	ARCVOL1
Volume ID on the cluster node	254	253

IMPORTANT: In the cluster load and unload scripts, the `add_secondary_ipaddress` and `del_secondary_ipaddress` commands refer to the cluster resource's IP address that is "secondary" to the node's actual IP address. It is not related to the DST volume's terminology.

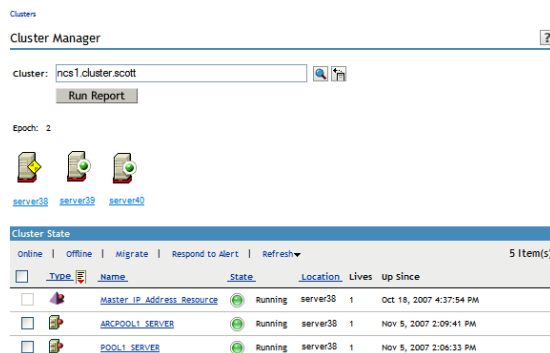
11.4.3 Viewing or Modifying Cluster Load and Unload Scripts

Initially, you have two load scripts and two unload scripts—one pair for each of the clustered NSS pools. You combine these scripts later to create a single load script that manages the two clustered resources so that they fail over together. For information about creating these two cluster resources, see [Section 8.2, “Creating NSS Volumes to Use in the DST Shadow Volume Pair,” on page 82](#).

- ♦ “Viewing Load and Unload Scripts for a Cluster Resource” on page 138
- ♦ “Sample Load and Unload Scripts for the Primary Clustered Resource” on page 139
- ♦ “Sample Load and Unload Scripts for the Secondary Clustered Resource” on page 139

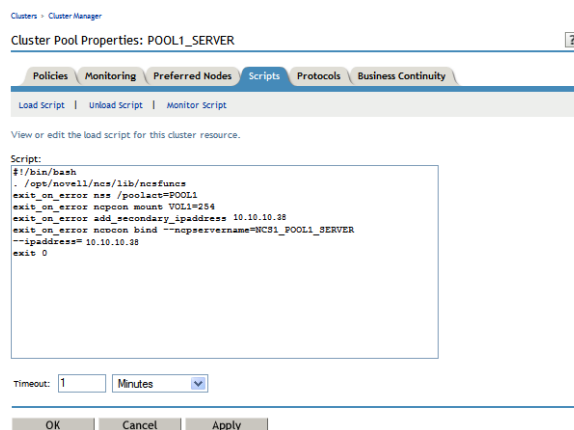
Viewing Load and Unload Scripts for a Cluster Resource

- 1 In iManager, select *Clusters*, then select *Cluster Manager*.
- 2 Click the *Object* browser, then locate and select the cluster server node to view a list of cluster resources.



- 3 Click the *Name* link of the primary cluster resource to go to the Cluster Pool Properties page, then click the *Scripts* tab to go to the Scripts page where you can view or modify the load and unload scripts for the selected cluster resource.

For example, click the *Name* link for POOL1_SERVER, then click *Scripts* to display the load script for the primary clustered pool named POOL1.



To view examples of the default load and unload scripts for the clustered resources, see the following:

- ♦ “Sample Load and Unload Scripts for the Primary Clustered Resource” on page 139
- ♦ “Sample Load and Unload Scripts for the Secondary Clustered Resource” on page 139

Sample Load and Unload Scripts for the Primary Clustered Resource

The load and unload scripts in this section are samples based on the setup in [Section 11.4.2, “Overview of Cluster Resource Setup,”](#) on page 137.

Load Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuns

exit_on_error nss /poolact=POOL1
exit_on_error ncpcon mount VOL1=254

exit_on_error add_secondary_ipaddress 10.10.10.38

exit_on_error ncpcon bind --ncpservername=NCS1_POOL1_SERVER --
ipaddress=10.10.10.38

exit 0
```

Unload Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuns

ignore_error ncpcon unbind --ncpservername=NCS1_POOL1_SERVER --
ipaddress=10.10.10.38

ignore_error del_secondary_ipaddress 10.10.10.38

ignore_error nss /pooldeact=POOL1

exit 0
```

Sample Load and Unload Scripts for the Secondary Clustered Resource

The load and unload scripts in this section are samples based on the setup in [Section 11.4.2, “Overview of Cluster Resource Setup,”](#) on page 137.

Load Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuns

exit_on_error nss /poolact=ARCPPOOL1
exit_on_error ncpcon mount ARCVOL1=253
exit_on_error add_secondary_ipaddress 10.10.10.39

exit_on_error ncpcon bind --ncpservername=NCS1_ARCPPOOL1_SERVER --
ipaddress=10.10.10.39
```

```
exit 0
```

Unload Script

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuns

ignore_error ncpcon unbind --ncpservername=NCS1_ARCPOOL1_SERVER --
ipaddress=10.10.10.39

ignore_error del_secondary_ipaddress 10.10.10.39
ignore_error nss /pooldeact=ARCPOOL1

exit 0
```

11.4.4 Configuring the Load and Unload Scripts for a Shadow Volume

When working with the two volumes as a shadow volume, you must create combined load and unload scripts for the primary cluster pool resource that manages the two clustered resources together. The secondary cluster pool resource appears with a status of offline while it is being managed by the primary scripts.

IMPORTANT: You should not online the secondary cluster pool resource while the pool and its volume is being managed by the primary pool resource.

- 1 Offline the primary and secondary cluster resources.
 - 1a In iManager, select *Clusters*, then select *Cluster Manager*.
 - 1b Click the *Object* browser, then locate and select the cluster server node to view a list of cluster resources.
 - 1c Select the check boxes next to the primary and secondary cluster resources.
 - 1d Click *Offline*.
- 2 Copy information from the secondary load script temporarily into a text file.
 - 2a Click the name link of the secondary cluster resource to view its Cluster Pool Properties page, then click the *Scripts* tab.
 - 2b On the *Scripts > Load Scripts* page, copy the contents of the load script into the temporary text file.
 - 2c On the *Scripts > Unload Scripts* page, copy the contents of the unload script to the temporary text file.
 - 2d Save the temporary files.
 - 2e At the bottom of the Scripts page, click *Cancel* to return to the Cluster Manager page.
- 3 Modify the load script for the primary cluster resource to be used for the shadow volume.
 - 3a Click the name link of the primary cluster resource to view its Cluster Pool Properties page, then click the *Scripts* tab.
 - 3b On the *Scripts > Load Script* page, copy information from the secondary load script into the primary load script.

Use the “[Sample Load Script for a Shadow Volume](#)” on page 143 as a guide for where to add the lines for each of the items.

IMPORTANT: Make sure to activate the secondary pool before activating the primary pool.

- 3c** Add a `sleep` command after the pool activation for the secondary NSS volume.

```
sleep 10
```

Vary the time (in seconds) according to what is needed for your system.

- 3d** Comment out the mount commands for the primary NSS volume and secondary NSS volume by placing a pound sign (#) at the beginning of the line. For example:

```
#exit_on_error ncpcon mount ARCVOL1=253
#exit_on_error ncpcon mount VOL1=254
```

- 3e** Add the mount command for the clustered shadow volume to the primary load script.

```
exit_on_error ncpcon mount VOL1=254,shadowvolume=ARCVOL1
```

- 3f** If you are using shadowfs to provide the unified file tree view for Samba/CIFS users, you must allow time in the load script after mounting the shadow volume to allow shadowfs to become active before continuing. Add a `sleep 10` command after mount command.

For example:

```
exit_on_error ncpcon mount VOL1=254,shadowvolume=ARCVOL1
sleep 10
```

- 3g** If you are loading other items like Samba, rsync, and so on, and you are relying on the shadowfs volume to provide the unified file tree view, you might need to add additional wait time for the shadowfs file system to mount.

Here is one example of the lines to add to the load script before Samba, rsync, and so on:

```
# Wait for shadowfs to start
for (( c=1; c<=10; c++ )) do
  if [ ! -d /media/shadowfs/VOLUME/._NETWARE ]; then sleep 5; fi
done
```

- 3h** Click *Apply* to save your changes.

The changes do not take effect until the cluster resource is online.

- 4** Modify the unload script for the primary cluster resource to be used for the shadow volume.

- 4a** Click the name link of the primary cluster resource to view its Cluster Pool Properties page, click the *Scripts* tab, then click *Unload Script*.

- 4b** On the *Scripts > Unload Script* page, copy information from the secondary unload script into the primary unload script.

Use the “[Sample Unload Script for a DST Shadow Volume](#)” on page 144 as a guide for where to add the lines for each of the items.

IMPORTANT: Make sure to deactivate the primary pool before deactivating the secondary pool.

- 4c** If you are using `shadowfs` to provide a unified file tree view to Samba users, you must unmount the FUSE-mounted file systems that are displayed in the `/media/shadowfs/VOLUME` directory. Add the following line at the end of the unload script:

```
ignore_error fusermount -u /media/shadowfs/VOLUME
```

- 4d** Click *Apply* to save your changes.

5 Online the primary load script.

- 5a** In iManager, select *Clusters*, then select *Cluster Manager*.



- 5b** Click the *Object* browser, then locate and select the cluster server node to view a list of cluster resources.

- 5c** Select the check box next to the primary cluster resource, then click *Online*.

- 5d** Select the cluster node where you want the resource to load (such as `server38`), then click *OK*.

6 Verify that the primary cluster resource is running by going to the *Clusters > Cluster Manager* page.


The primary cluster resource is *Running*. The secondary cluster resource is reported as *Offline* because you are managing that cluster resource through the primary load script.






<input type="checkbox"/>		ARCPPOOL1_SERVER	Offline	1	
<input type="checkbox"/>		POOL1_SERVER	Running	server38	2 Nov 5, 2007 4:11:53 PM




7 Verify that the shadow volume (VOL1) is mounted in NCP and is shadowed.

- 7a** On the first node in the cluster, log in to Novell Remote Manager for Linux as the `root` user.

- 7b** Select *View File Systems*, then verify that the secondary pool `ARCPPOOL1` and the NSS volume `ARCVOL1` are listed under *File Systems*, but the secondary NSS volume is not listed under *NCP Volumes*.

File System Management 

File Systems		
Mounted Device	Mount Location	
 rootfs	/	(95% free)
 udev	/dev	(99% free)
/dev/disk/by-id/scsi-36001c230c175cf000e70368e60a6e6fe-part2 /		
proc	/proc	
sysfs	/sys	
debugfs	/sys/kernel/debug	
devpts	/dev/pts	
securityfs	/sys/kernel/security	
adminfs	/admin	
 admin	/_admin	(100% free)
/dev/evms/POOL1	/opt/novell/nss/mnt/.pools/POOL1	
/dev/evms/ARCPPOOL1	/opt/novell/nss/mnt/.pools/ARCPPOOL1	
 ARCVOL1	/media/nss/ARCVOL1	(99% free)
 VOL1	/media/nss/VOL1	(99% free)

NCP Volumes	
 SYS	/usr/novell/sys
 _ADMIN	/_admin
 VOL1	/media/nss/VOL1

- 7c** Select *View File Systems > Dynamic Storage Technology Options*, then verify that the primary volume is listed under *Volume Information*, and that its status is *Shadowed*.

Dynamic Storage Technology Options

Dynamic Storage Technology allows you optimize the use of your storage by automatically moving data to storage best optimized for the data type or frequency of use. You can create one or more policies to manage, and optimize the use of your storage.

Volume Information		
Volume Name	Shadow Status	
VOL1	Shadowed	Inventory View Log
_ADMIN	No Shadow	Inventory
SYS	Add Shadow	Inventory

No Dynamic Storage Technology policies defined.

[Create a new policy](#)

Duplicate File Resolution Options	
Broadcast conflict message to user:	<input checked="" type="checkbox"/>
Action to be taken:	Show duplicate shadow files
Submit	

ShadowFS Configuration

☐ Load ShadowFS At Boot Time

[Submit](#)

7d Select *Manage NCP Services > Manage Shares*, click NCP/NSS bindings, then verify that the NCP Accessible parameter is turned off for the secondary volume, and turned on for the primary volume.

NCP / NSS Bindings

Warning:
When a NSS Volume is changed to be not accessible via NCP, it will be dismounted immediately as a NCP share point

Available NSS volumes		
NCP Accessible	Volume Name	Mount point
Yes: <input type="radio"/> No: <input checked="" type="radio"/> Save Selection	ARCVOL1	/media/nss/ARCVOL1
Yes: <input checked="" type="radio"/> No: <input type="radio"/> Save Selection	VOL1	/media/nss/VOL1

[Share Management Home](#)

Sample Load Script for a Shadow Volume

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuns

exit_on_error nss /poolact=ARCPool1
sleep 10
exit_on_error nss /poolact=POOL1
sleep 10

#echo -e "/forceactivate=ARCVOL1" > /dev/nsscmd
#echo -e "/forceactivate=VOL1" > /dev/nsscmd

#exit_on_error ncpcon mount ARCVOL1=253
#exit_on_error ncpcon mount VOL1=254

exit_on_error ncpcon mount VOL1=254,shadowvolume=ARCVOL1
exit_on_error add_secondary_ipaddress 10.10.10.38

exit_on_error ncpcon bind --ncpservername=NCS1_POOL1_SERVER --
ipaddress=10.10.10.38

exit 0
```

Sample Unload Script for a DST Shadow Volume

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfuns

ignore_error ncpcon unbind --ncpservername=NCS1_POOL1_SERVER --
ipaddress=10.10.10.38

ignore_error del_secondary_ipaddress 10.10.10.38

ignore_error nss /pooldeact=POOL1
ignore_error nss /pooldeact=ARCPPOOL1

#Deactivating the pools automatically deactivates the NSS volumes on them.

#umount /media/nss/VOL1
#umount /media/nss/ARCVOL1

exit 0
```

11.5 Configuring Shadow Volume Policies for the Clustered Shadow Volume

After the load and unload scripts are created, and the shadow volume is loaded, you are ready to create policies for the shadow volume. Make sure that the policies you create for the clustered shadow volume apply only to the given shadow volume or only to shadow volumes in the same cluster resource.

For information, see [Chapter 9, “Managing Policies for Shadow Volumes,”](#) on page 109.

11.6 Removing a Clustered DST Shadow Volume

Removing a clustered DST shadow volume removes the relationship between the primary and secondary storage area and decouples the load and unload scripts for the clustered pools that contain the two volumes. It does not remove the underlying volumes themselves. The files remain on whichever storage area they are on at the time when you remove the shadow relationship.

- ♦ [Section 11.6.1, “Preparing to Remove a Shadow Volume,”](#) on page 144
- ♦ [Section 11.6.2, “Removing the Shadow Volume Relationship,”](#) on page 145

11.6.1 Preparing to Remove a Shadow Volume

Before you remove a shadow volume relationship, make sure that you shift data between the two volumes that make up the shadow volume, according to where you want the data to reside after the DST shadow volume relationship is removed. In order for the data to be shifted to the primary storage area or to the secondary storage area, it is up to you to make that happen.

- 1 In Novell Remote Manager for Linux, log in as the `root` user.
- 2 Select *View File System > Dynamic Storage Technology Options*, locate the volume in the list, then click the *Inventory* link next to it.

View the volume inventory for the shadow volume to determine the space in use and the available space for both the primary and the secondary areas of the shadow volume. Make sure there is sufficient free space available in either location for the data that you plan to move to that location.

- 3 Use any combination of the following techniques to shift data between the two areas:
 - ♦ **Shadow Volume Policies:** Run an existing shadow volume policy by using the *Execute Now* option in the *Frequency* area of the policy. You can also create a new shadow volume policy that moves specific data, and run the policy by using the *One Time* and *Execute Now* options in the *Frequency* area of the policy.

For information about configuring policies to move data between the primary and secondary areas, see [Chapter 9, “Managing Policies for Shadow Volumes,” on page 109](#).

- ♦ **Inventories:** Use the detailed inventory reports or customized inventories to move specific files to either area.

For information about using the volume customized inventory options to move data between the primary and secondary areas, see [Section 10.5, “Generating a Custom Inventory Report,” on page 128](#).

11.6.2 Removing the Shadow Volume Relationship

- 1 If the cluster pool resource for the shadow volume is not running on the master node, cluster migrate it to the master node.

For information, see “[Cluster Migrating Resources to Different Nodes](#)” in the *OES 2 SPI: Novell Cluster Services 1.8.5 for Linux Administration Guide*.

- 2 Offline the cluster pool resource that is managing the shadow volume.

This unloads the cluster resource and deactivates the cluster pools and their volumes so that the cluster is not controlling them.

For information, see “[Onlining and Offlining \(Loading and Unloading\) Cluster Resources from a Cluster Node](#)” in the *OES 2 SPI: Novell Cluster Services 1.8.5 for Linux Administration Guide*.

- 3 In NSSMU or iManager, activate the shared pools and mount the two volumes.
- 4 In Novell Remote Manager for Linux, log in as the `root` user.
- 5 Select *Manage NCP Services* > *Manage Shares* to go to the NCP Shares page.
- 6 Make sure that you know which NSS volume is being used as the secondary volume so that you can manage it independently later.
 - 6a On the NCP Shares page, locate the primary NSS volume in the *Active Shares* list, then click the *Information* icon next to the share name.

- 6b On the primary volume’s Share Information page, view the volume information in the *File System Shadow Path*.

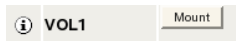
In the following example, ARCVOL is an NSS volume that is the secondary storage area in the shadow volume.

File system path	/media/nss/VOL1
File system shadow path	/media/nss/ARCVOL

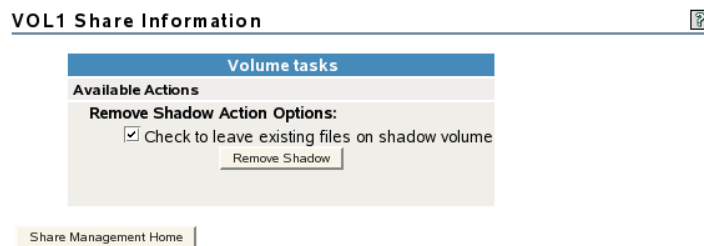
- 7 On the NCP Shares page, locate the primary NSS volume in the *Active Shares* list, then click the *Unmount* button next to the share name.



- 8 On the Manage Shares page, click the *Information* (i) icon next to the volume name of the NSS volume to access the *Remove Shadow Action Options*.



- 9 On the volume's Share Information page, select *Check to leave existing files on the shadow volume*.



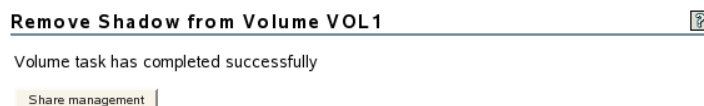
When you enable *Check to leave existing files on the shadow volume*, the data that currently resides on each volume remains where it is, so that the data on the secondary storage area is not shifted back to the primary volume.

The *Check to leave existing files on the shadow volume* option is deselected by default. When this option is disabled and you click *Remove Shadow*, all of the data that currently resides on the secondary volume is moved back to the primary storage location before the secondary volume is again available as an individual volume. It takes time to move the data back to the primary, depending on how much data there is to move.

IMPORTANT: In the OES 2 SP1 release for DST, if you disable the *Check to leave existing files on the shadow volume*, the shadow volume is not removed. DST does not remove the shadow relationship until you enable the option to keep data where it is.

- 10 Click *Remove Shadow*.

After the shadow volume is removed, the page refreshes to report a successful removal.



- 11 Select *Share Management* to go to the NCP Shares page, locate the volume that was the primary volume in the *Active Shares* list, then click the *Mount* button next to it.



12 Verify that the shadow volume was removed by using one of the following methods:

- ♦ Select *View File System > Dynamic Storage Technology Options* to go to the Dynamic Storage Options page. The former primary volume now has an *Add Shadow* link next to it instead of a *Shadowed* link.

Volume Information		
Volume Name	Shadow	Status
① VOL1	Add Shadow	Inventory
① _ADMIN	No Shadow	Inventory
① SYS	Add Shadow	Inventory

- ♦ Select *Manage NCP Services > Manage Shares*, then click the *Information* icon next to the former primary volume's name. The *File System Shadow Path* field displays n/a (not applicable).

File system path	/media/nss/VOL1
File system shadow path	n/a

13 Mount the volume that was used as the secondary volume (for example, ARCVOL) as an independent volume.

13a In the *Configuration* area of the NCP Shares page, click *NCP/NSS Bindings*.

Configuration
Create new share
Delete existing share
NCP/NSS Bindings

13b In the *Available NSS Volumes* list, locate the former secondary volume (such as ARCVOL), click *Yes*, then click *Save Selection*.

Yes: <input checked="" type="radio"/>	No: <input type="radio"/>	ARCVOL	/media/nss/ARCVOL
Save Selection			

The volume is mounted automatically, and now appears again in the *Active Shares* list on the NCP Shares page.

Active Shares		
Info	Share name (volume name)	Tasks
① SYS		Unmount
① _ADMIN		
① VOL1		Unmount
① ARCVOL		Unmount

14 In NSSMU, deactivate the cluster pool resources for both the primary and secondary volumes.

This automatically unmounts the shared volumes. This allows the cluster resources to be managed by their respective cluster resources after you modify the load and unload scripts in the next steps.

- 15** Modify the load script of the cluster pool resource that was managing the clustered shadow volume pair.
- 15a** In iManager, select *Clusters*, then select *Cluster Manager*.
- 15b** Click the *Object* browser, then locate and select the cluster server node to view a list of cluster resources.
- 15c** On the Cluster Manager page, click the name link of the primary cluster resource to view its Cluster Pool Properties page, then click the *Scripts* tab.
- 15d** On the *Scripts > Load Script* page, comment out the activation command for the secondary pool, the sleep command you added for the pool activation, and the mount command for the shadow volume:

```
#exit_on_error nss /poolact=ARCPPOOL1
#sleep 10
#exit on error ncpcon mount VOL1=254,shadowvolume=ARCVOL1
```

- 15e** On the *Scripts > Load Script* page, uncomment the mount command for the primary pool's volume that you commented out when you set up the clustered shadow volume. For example:

```
exit_on_error ncpcon mount VOL1=254
```

- 15f** Click *Apply* to save your changes.

The changes do not take effect until the cluster resource is online.

- 16** Modify the unload script of the cluster pool resource that was managing the clustered shadow volume pair.
- 16a** On the *Scripts > Load Script* page, click the *Unload Script* link.
- 16b** On the *Scripts > Unload Script* page, comment out or remove the deactivation command for the secondary pool:

```
#ignore_error nss /pooldeact=ARCPPOOL1
```

- 16c** Click *Apply* to save your changes.

The changes do not take effect until the cluster resource is online.

- 17** Online the cluster pool resources for the two pools.

- 17a** Select *Clusters*, then select *Cluster Manager* to view the list of cluster resources.

- 17b** Select the check boxes next to the two cluster pool resources, then click *Online*.

IMPORTANT: If you deleted the pool cluster resource for the secondary volume when you merged information from the two scripts into one, you must first cluster enable the shared pool again to create a new cluster pool resource for it, then online it.

- 17c** Select the cluster node where you want the resources to load (such as `server38`), then click *OK*.

- 18** Verify that the cluster resources are running by going to the *Clusters > Cluster Manager* page.

- 19** Verify that the two volumes (VOL1 and ARCVOL1) are mounted independently in NCP.

- 19a** On the first node in the cluster, log in to Novell Remote Manager for Linux as the `root` user.

- 19b** Select *View File Systems*, then verify that the secondary pool ARCPool1 and the NSS volume ARCVOL1 are listed under *NCP Volumes*.
- 19c** Select *View File Systems > Dynamic Storage Technology Options*, then verify that both of the volumes are listed under *Volume Information*, and that they no longer shadowed (the *Add Shadow* link is next to each one).
- 19d** Select *Manage NCP Services > Manage Shares*, click NCP/NSS bindings, then verify that the NCP Accessible parameter is enabled for both of the volumes.

Troubleshooting for Dynamic Storage Technology

12

This section describes issues and possible workarounds for Dynamic Storage Technology (DST) for Novell® Open Enterprise Server (OES) 2 Linux.

- [Section 12.1, “My NCP server information has the setting: LOCAL_CODE_PAGE CP437. Why isn’t it using UTF-8?” on page 151](#)
- [Section 12.2, “A File Is Listed Twice in a Directory,” on page 151](#)
- [Section 12.3, “Users Cannot See Some Files and Directories,” on page 151](#)
- [Section 12.4, “Cross-Protocol Locking Stops Working,” on page 152](#)

12.1 My NCP server information has the setting: LOCAL_CODE_PAGE CP437. Why isn’t it using UTF-8?

All interaction with the Linux file system uses UTF-8. However, for backward compatibility with older Novell Clients, most of the NCPs use a server-defined local code page setting. The more recently defined Case 89 NCPs use UTF-8. We recommend that you configure your client to use them. If all of your clients are using the newer UTF-8 Case 89 NCPs, then there is no need to set the server’s local code page.

12.2 A File Is Listed Twice in a Directory

If a file happens to be located in the same directory on both the primary and secondary storage, the filename is listed twice in the directory listing. However, all file operations are directed to the file on the primary system.

To resolve this problem, you can rename one instance of the file to make both versions of the file available under different names. Then open the files to determine which version to keep.

You can control how DST handles duplicate files by configuring global policies. For information, see [Section 4.6, “Configuring Global Policies for Resolving Instances of Duplicate Files,” on page 51](#).

12.3 Users Cannot See Some Files and Directories

If the secondary storage location becomes unavailable, it appears to users that some of their files and directories are suddenly missing. When the secondary storage location is back online, the files and directories are visible again.

12.4 Cross-Protocol Locking Stops Working

Cross-protocol locking allows Samba/CIFS users and NCP users to concurrently access files by allowing only one user at any time to open the file for write. Multiple users who are accessing via NCP and Samba/CIFS can open a file for read only.

WARNING: Allowing users who access files via different protocols to concurrently open a file for write can lead to data corruption.

NCP Server for Linux provides cross-protocol locking for NCP and Linux Samba/CIFS users. Novell CIFS for Linux does not support cross-protocol locking in OES 2 SP1 Linux.

If cross-protocol locking is enabled for NCP Server for Linux but stops working for DST shadow volume pairs--that is, multiple users can open a file for read and write--it is probably because ShadowFS needs to be restarted. To resolve this problem, stop the shadowfs process, then start shadowfs. For information, see [Section 5.11, “Starting and Stopping ShadowFS Manually,” on page 65](#).

This section describes security issues and recommendations for Dynamic Storage Technology (DST) for Novell® Open Enterprise Server (OES) 2 Linux. It is intended for security administrators or anyone who is using DST and is responsible for the security of the system. It requires a basic understanding of NetWare® Core Protocol™ (NCP™) Server and DST. It also requires the organizational authorization and the administrative rights to carry out the configuration recommendations.

- ♦ [Section 13.1, “Client Access,” on page 153](#)
- ♦ [Section 13.2, “Linux-Enabled eDirectory Users,” on page 153](#)
- ♦ [Section 13.3, “Using File System Trustees and Rights,” on page 153](#)
- ♦ [Section 13.4, “Server-to-Server Access,” on page 154](#)
- ♦ [Section 13.5, “Hidden Directories and Files,” on page 154](#)
- ♦ [Section 13.6, “Shadow Volumes Audit Logs,” on page 154](#)
- ♦ [Section 13.7, “Shadow File System Audit Logs,” on page 155](#)
- ♦ [Section 13.8, “NCP Server Auditing and Log Files,” on page 155](#)
- ♦ [Section 13.9, “Use Secure Remote Connections,” on page 155](#)

13.1 Client Access

NCP clients access the shadow volume through the NCP Engine.

CIFS/Samba clients access data on a shadow volume through the ShadowFS. These users are Linux-enabled through Linux User Management.

Novell AFP and Novell CIFS for OES 2 SP1 Linux have not been tested with DST for the OES 2 SP1 Linux release, so they are not supported.

Other client protocols such as FTP, HTTP, and NFS are not supported.

13.2 Linux-Enabled eDirectory Users

Dynamic Storage Technology requires that all users of the shadow volume be users that have been defined in Novell eDirectory™. For information, see the *Novell eDirectory 8.8 Administration Guide*.

CIFS/Samba users must be enabled for Linux with Linux User Management. This is true for NCP volumes on Linux POSIX file systems (Ext3 and Reiser) and for NSS volumes on Linux and NetWare. The *OES 2 SP1: Novell Linux User Management Technology Guide* describes how to Linux-enable users for an OES 2 Linux server.

13.3 Using File System Trustees and Rights

Dynamic Storage Technology requires that file system access control for data be managed by using the Novell Trustee Model for file system trustees and trustee rights.

For all NCP volumes (NSS and non-NSS), the trustee information is obtained at volume mount time from the `._NETWARE/.trustee_database.xml` file. When trustee changes are made, this trustee database file is updated. Because this file is located on the volume, it follows the volume from node to node as it moves around the cluster.

NCP trustee information is synchronized with the NSS file system. When an NCP user makes a trustee change, the NCP server informs NSS of the change. When NSS changes a trustee assignment, it generates an event that the NCP server listens for so NCP can keep up to date on NSS changes. When DST is involved, events from the secondary NSS volume are also noted, and trustee changes are also synchronized with it.

IMPORTANT: For NCP volumes, make sure that the *Inherit POSIX Permissions* option is disabled (the default setting). When this setting is disabled, the local Linux environment access is restricted to the `root` user and the file owner or creator, which is the most secure configuration. For information, see “[Configuring Inherit POSIX Permissions for an NCP Volume](#)” in the *OES 2 SP1: NCP Server for Linux Administration Guide*.

Rights and trustee management across multiple file systems should all be managed with the NCP tools. There are rights model mapping problems with using a POSIX rights model on NCP volumes, and vice versa.

13.4 Server-to-Server Access

iSCSI is the only protocol supported for server-to-server access that allows a remote volume to be used as a primary or secondary storage area for a shadow volume.

13.5 Hidden Directories and Files

- ♦ [Section 13.5.1, “Trustee Database,” on page 154](#)
- ♦ [Section 13.5.2, “Available Space Trends,” on page 154](#)

13.5.1 Trustee Database

A copy of the trustee database is placed in the `._NETWARE` subdirectory in both the primary tree and the shadow tree.

13.5.2 Available Space Trends

An available space trend data file is placed in the `._NETWARE` subdirectory in both the primary tree and the shadow tree. It is used by the volume inventory option in Novell Remote Manager for Linux.

13.6 Shadow Volumes Audit Logs

An audit log for a DST shadow volume is located in the `._NETWARE` directory located at the root of the primary volume. For NSS volumes, the default file path for the log is `/media/nss/volumename/._NETWARE/volumename.audit.log`. All moves between the primary storage area and the secondary storage area are logged as events to the shadow volume’s audit log.

For example, if the primary area is named `VOL1`, the audit file is `/media/nss/VOL1/._NETWARE/VOL1.audit.log`.

13.7 Shadow File System Audit Logs

Audit logs for the Shadow File System are located in the `/var/opt/novell/log/shadowfs.log` file.

13.8 NCP Server Auditing and Log Files

The following log files are located in the `/var/opt/novell/log` directory:

- ♦ `ncpserv.log`
- ♦ `ncp2nss.log`
- ♦ `ncptop.log`

Log files are managed by `logrotate`. For information on usage, see its man page (`man logrotate`).

The control files for `logrotate` are:

- ♦ `/etc/logrotate.d/novell-ncpserv-log`
- ♦ `/etc/logrotate.d/novell-ncpserv-audit`
- ♦ `/etc/logrotate.d/novell-ncp2nss-log`
- ♦ `/etc/logrotate.d/novell-ncp2nss-audit`

By default, the rollover size is 16 MB and 5 compressed copies are kept.

13.9 Use Secure Remote Connections

If the primary storage area or secondary storage area are connected across remote connections, the connection must be secure. For example, use a virtual private network (VPN) or a private WAN connection.

IMPORTANT: iSCSI is the only protocol supported for remote server-to-server connections.

Make sure that authentication, encryption, and data integrity are secure when accessing and transferring data across the network. For example, if sensitive data is written to the primary volume, that data might be written to the secondary volume, depending on shadow policies in place. If there is an anonymous NFS mount for the shadow volume, the data is transferred in the clear over the network, where it might be prone to attacks or capture. In this case, you want to make sure that only authenticated users are able to access the NFS mount and that the connection between the servers is secure.

Commands and Utilities for Dynamic Storage Technology

A

This section describes commands and utilities for Dynamic Storage Technology (DST) for Novell® Open Enterprise Server (OES) 2 for Linux.

- ♦ [Section A.1, “Using NCPCON for DST Commands,” on page 157](#)
- ♦ [Section A.2, “DST Commands for NCPCON,” on page 158](#)
- ♦ [Section A.3, “DST Commands for NCPCON for Use with Novell Cluster Services for Linux Clusters,” on page 162](#)
- ♦ [Section A.4, “Configuring Global DST Policies by Using the SET Command,” on page 163](#)
- ♦ [Section A.5, “DST Commands for /etc/opt/novell/ncpserv.conf,” on page 167](#)
- ♦ [Section A.6, “DST Commands for /etc/opt/novell/shadowfs.conf,” on page 168](#)
- ♦ [Section A.7, “DST EXCLUDE_VOLUME Command for /etc/opt/novell/ncp2nss.conf,” on page 169](#)
- ♦ [Section A.8, “DST Shadow Volume Information in /etc/NCPVolumes,” on page 169](#)
- ♦ [Section A.9, “DST ShadowFS Volume Information in /etc/mtab.shadowfs,” on page 169](#)

A.1 Using NCPCON for DST Commands

The NetWare® Core Protocol™ (NCP™) Console Command (NCPCON) utility provides an interface for issuing NetWare related commands in a Linux environment. You can issue commands via the NCPCON in three modes:

- ♦ [Section A.1.1, “Interactive Mode,” on page 157](#)
- ♦ [Section A.1.2, “Command Line Mode,” on page 157](#)
- ♦ [Section A.1.3, “Scripting Mode,” on page 158](#)

A.1.1 Interactive Mode

Open a terminal console, log in as the `root` user, then enter

```
ncpcon
```

This opens the NCPCON interactive console in the terminal console where you can enter the NCP Server console commands. Enter `exit` to stop interactive mode.

A.1.2 Command Line Mode

For command line mode, issue an NCP Server command at a terminal console prompt by prepending the command with `ncpcon`:

```
ncpcon [command]
```

For example:

```
ncpcon mount sys
```

When using `ncpcon` to issue commands directly from the console command prompt, you must escape the quote character (") by preceding the character with a backslash (\). For example, a `send` command is entered as follows from the console command line prompt:

```
ncpcon send \"hello world\" to all
```

Escaping the quote character is not required when entering the command from the `ncpcon` prompt. For example, the `send` command is entered as followed from the `ncpcon` prompt:

```
send "hello world" to all
```

A.1.3 Scripting Mode

For scripting mode, issue the NCP Server command in the script by prepending the command with `ncpcon`, then placing double-quote marks around the NCP Server command:

```
ncpcon "[command]"
```

For example:

```
ncpcon "mount sys"
```

A.2 DST Commands for NCPCON

The commands in this section can be used only with the NCP Console Command utility. For information, see [Section A.1, “Using NCPCON for DST Commands,” on page 157](#).

`create shadow_volume primary_volumename shadow_path`

Creates a shadow association between an NCP volume and an NCP shadow volume. Specify the volume name for the primary volume and the path of mount location for the NCP shadow volume. Adds the `SHADOW_VOLUME` mount information to the `/etc/opt/novell/ncpserv.conf` file.

By using `ncpcon` to issue the command, you do not need to restart `ndsd` in order for the changes to take effect.

OPTIONS

`/Cluster_Resource`

Causes the shadow volume to be created in NCP, but does not add a shadow volume entry to the `/etc/opt/novell/ncpserv.conf` file. The absence of the entry is desired in order to allow the NCP volume to fail over to other nodes in a Novell Cluster Services™ for Linux cluster.

Use this option in the cluster load script to create a shadow volume for a cluster resource. Because the volume is not defined in `ncpserv.conf`, you do not need the `ncpcon remove shadow_volume` command in the cluster unload script.

Use this option in combination with the `/ID=volume_id` option.

`/ID=volume_id`

Specifies the server volume ID (0 to 254) to use when mounting the shadow volume. Use this option to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource on any node in the cluster.

Use this option in combination with the /Cluster_Resource option.

EXAMPLES

create shadow_volume VOL1 /home/shadows/VOL1

Creates a shadow volume where VOL1 is the primary storage area and /home/shadows/VOL1 is its mount point as a shadow volume.

create shadow_volume /cluster_resource /id=254 VOL1 /home/shadows/VOL1

Creates a shadow volume where VOL1 is the primary storage area and /home/shadows/VOL1 is its mount point as a shadow volume. The shadow volume is created in NCP, but no entry is added to the `ncpserv.conf` file. The server volume ID is 254 on any node in the cluster where it is mounted.

remove shadow_volume [/l] volumename

Removes the shadow association between the primary storage area and secondary storage area. The shadow volume must be dismounted before this operation can be done.

This command removes the SHADOW_VOLUME command from the `/etc/opt/novell/ncpserv.conf` file. If the /l option is specified, it then leaves files where they are on either on the primary and secondary volumes. If the /l option is not specified, it then moves all files from the secondary storage area back to the primary storage area. Make sure that the primary volume has sufficient space to accommodate all the files before you remove the shadow relationship.

Because it is moving files back to the primary, the removal process can take some time, depending on how much data must be moved. After completion, a summary report is created and displayed.

This command can be added to a cluster load script.

EXAMPLES

Issue the following commands from the NCP Console, or prepend the command with `ncpcon` when issuing from a script or at a terminal console prompt.

remove shadow_volume VOL1

Removes the shadow relationship for shadow volume VOL1, and moves all files from the secondary storage area to the primary storage area. You must dismount VOL1 before you issue this command.

remove shadow_volume /l VOL1

Removes the shadow relationship for shadow volume VOL1, and leaves files where they currently are on the secondary storage area and the primary storage area. You must dismount VOL1 before you issue this command.

shadow volumename operation=<lp | ls | mp | ms> [options]

Allows you to list files on the shadow volume, or to move files between the primary storage area and the secondary storage area based on specified criteria. All files on the selected shadow volume that match the criteria are moved. Use the command from within `cron` jobs to automate data partitioning.

OPERATION OPTIONS

lp

List primary files. Lists all files currently residing on the primary storage area.

ls

List shadow files. Lists all files currently residing on the secondary storage area.

mp

Move files to primary. Moves files that match the specified criteria to the primary storage area from the secondary storage area.

ms

Move files to shadow. Moves files that match the specified criteria to the secondary storage area from the primary storage area.

OPTIONS

pattern="searchPattern"

Specifies the file pattern to match against.

owner="username.context"

Specifies the Novell eDirectory username and context of the owner of the files to match against.

uid=uidValue

Specifies the Linux user ID to match against.

time=[time_field]

Specifies which time field to match against, where the *time_field* is:

[m] [a] [c]

- ♦ **m:** Last time modified (content)
- ♦ **a:** Last time accessed
- ♦ **c:** Last time changed (metadata)

range=[time_period]

Specifies which time period to match against, where the *time_period* is:

[a] [b] [c] [d] [e] [f] [g] [h] [i] [j]

- ♦ **a:** Within last day
- ♦ **b:** 1 day to 1 week
- ♦ **c:** 1 week to 2 weeks
- ♦ **d:** 2 weeks to 1 month
- ♦ **e:** 1 month to 2 months
- ♦ **f:** 2 months to 4 months
- ♦ **g:** 4 months to 6 months
- ♦ **h:** 6 months to 1 year
- ♦ **i:** 1 year to 2 years
- ♦ **j:** More than 2 years

size=[size_differential]

Specifies the size differential to match against, where the *size_differential* is:

[a] [b] [c] [d] [e] [f] [g] [h] [i] [j] [k]

- ♦ **a:** Less than 1 KB
- ♦ **b:** 1 KB to 4 KB
- ♦ **c:** 4 KB to 16 KB
- ♦ **d:** 16 KB to 64 KB
- ♦ **e:** 64 KB to 256 KB
- ♦ **f:** 256 KB to 1 MB
- ♦ **g:** 1 MB to 4 MB
- ♦ **h:** 4 MB to 16 MB
- ♦ **i:** 16 MB to 64 MB
- ♦ **j:** 64 MB to 256 MB
- ♦ **k:** More than 256 MB

output="filename"

Outputs the search results to the specified file.

EXAMPLES

shadow VOL1 operation=ls pattern="*.exe"

Lists all files of type EXE that currently reside on the secondary storage area for the shadow volume VOL1.

shadow VOL1 operation=lp size=g

Lists all files of sizes between 1 MB to 4 MB that currently reside on the primary storage area for the shadow volume VOL1.

shadow VOL1 operation=ms range=j

Moves all files on the primary storage area that have not been modified, accessed, or changed in more than two years from the primary storage area to the secondary storage area for the shadow volume VOL1.

shift "volumename:\path\filename" [primary | shadow]

Returns the specified file's location as being on the primary storage area or secondary storage area. Specify the primary or secondary options to move the specified file from its current location to the specified storage area.

OPTIONS

primary

Moves the specified file from the secondary storage area to the primary storage area. The file must be closed when you issue the command; otherwise, the command fails.

shadow

Moves the specified file from the primary storage area to the secondary storage area. The file must be closed when you issue the command; otherwise, the command fails.

EXAMPLES

shift "sys:\textfile.txt"

Shows the specified file's storage area location in the shadow volume as primary (the primary storage area) or shadow (the secondary storage area) for the shadow volume sys.

```
shift "sys:\textfile.txt" primary
```

Moves the specified file's storage area location from the secondary storage area to the primary storage area for the shadow volume `sys`.

```
shift "sys:\textfile.txt" shadow
```

Moves the specified file's storage area location from the primary storage area to the secondary storage area for the shadow volume `sys`.

A.3 DST Commands for NCPCON for Use with Novell Cluster Services for Linux Clusters

NCPCON supports the commands in this section for use with Dynamic Storage Technology in combination with Novell Cluster Services for Linux clusters.

Use the following syntax in cluster load scripts to mount the volume in a cluster. With clustering, no changes are needed to the `ncpserv.conf` file for shadowing. The primary volume information is also not added to the `ncpserv.conf` file.

A.3.1 Scenario 1: Primary NSS and Shadow NSS

```
ncpcon mount volumename=volID,SHADOWVOLUME=shadow_volumename
```

Use this command in a cluster load script when the primary volume is an NSS volume and the secondary volume is an NSS volume. Both NSS volumes must already exist and be mounted in NSS.

Replace `volID` with a value from 0 to 254 as the server volume ID to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource.

EXAMPLE

```
ncpcon mount VOL1=254,SHADOWVOLUME=ARC1
```

Mounts the NSS volume named `VOL1` with a volume ID of 254. The primary volume is an existing NSS volume named `VOL1` (`/media/nss/VOL1`). The secondary volume is an existing NSS volume named `ARC1` (`/media/nss/ARC1`).

A.3.2 Scenario 2: Primary Non-NSS and Shadow Non-NSS (Not supported in the initial release.)

```
ncpcon mount  
volumename=volID,SHADOWPATH=shadowpath,path=primarypath
```

Use this command when the primary volume is a non-NSS volume and the secondary volume is a non-NSS volume.

Replace `volID` with a value from 0 to 254 as the server volume ID to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource.

EXAMPLE

```
ncpcon mount VOL1=254,SHADOWPATH=/media/ncpvolumes/ARC1,path=  
media/ncpvolumes/VOL1
```

Mounts the NCP volume named `VOL1` with a volume ID of 254. The primary volume's path is `/media/ncpvolumes/VOL1`. The secondary volume's path is `/media/ncpvolumes/ARC1`.

A.3.3 Scenario 3: Primary Non-NSS and Shadow NSS (Not supported in the initial release.)

ncpcon mount

volumename=volID,SHADOWVOLUME=shadow_volumename,path=primarypath

Use this command when the primary volume is a non-NSS volume and the secondary volume is an NSS volume. The NSS volume must already exist on the system and be mounted in NSS.

Replace *volID* with a value from 0 to 254 as the server volume ID to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource.

EXAMPLE

ncpcon mount VOL1=254,SHADOWVOLUME=ARC1,path=/media/ncpvolumes/VOL1

Mounts the NCP volume named VOL1 with a volume ID of 254. The primary volume's path is /media/ncpvolumes/VOL1. The secondary volume is an existing NSS volume named ARC1 (mounted at /media/nss/ARC1).

A.3.4 Scenario 4: Primary NSS and Shadow Non-NSS (Not supported in the initial release.)

ncpcon mount volumename=volID,SHADOWPATH=shadowpath

Use this command when the primary volume is an NSS volume and the secondary volume is a non-NSS volume. The NSS volume must already exist on the system and be mounted in NSS.

Replace *volID* with a value from 0 to 254 as the server volume ID to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource.

EXAMPLE

ncpcon mount VOL1=254,SHADOWPATH=/media/ncpvolumes/ARC1

Mounts an NSS volume named VOL1 with a volume ID of 254. The primary volume is an existing NSS volume named VOL1 (/media/nss/VOL1). The secondary volume is an NCP volume named ARC1 that is mounted at /media/ncpvolumes/ARC1.

A.4 Configuring Global DST Policies by Using the SET Command

DST provides several global parameters for the SET command that can be used to customize DST for a given server. These settings control how DST behaves for all shadow volumes on the server. Initially, the parameters and default settings are in force, but the parameters are not explicitly added to the /etc/opt/novell/ncpserv.conf file. After you modify its default setting, an entry for the parameter and its new setting are added to the file. The parameter entry remains in the file even if you modify the setting back to the default.

IMPORTANT: If you use DST shadow volumes in a cluster, make sure to set the same global policies on each OES 2 Linux node in the cluster where you plan to fail over the shared volumes.

- ♦ [Section A.4.1, “Understanding DST Parameters for the SET Command,” on page 164](#)

- ♦ [Section A.4.2, “Using Novell Remote Manager to Configure DST Parameters for the SET Command,” on page 165](#)
- ♦ [Section A.4.3, “Using the ncpcon set Command to Configure DST Parameters,” on page 166](#)

A.4.1 Understanding DST Parameters for the SET Command

Table A-1 lists the DST parameters for the SET command with their default values and valid options.

Table A-1 *Manage NCP Services > Manage Server > Server Parameter Information*

Parameter Name and Description	Default Value	Valid Values
DUPLICATE_SHADOW_FILE_ACTION Controls how duplicate files conflicts are handled. For information, see Section 4.6.1, “Understanding Conflict Resolution for Duplicate Files,” on page 51.	0	0 - Show duplicate shadow files (default) 1 - Hide duplicate shadow files 2 - Rename duplicate shadow files 3 - Delete duplicate files from shadow area 4 - Move duplicate shadow files to /._DUPLICATE_FILES
DUPLICATE_SHADOW_FILE_BROADCAST Controls whether broadcast messages are sent to NCP users whenever duplicate files conflicts occur. For information, see Section 4.6.1, “Understanding Conflict Resolution for Duplicate Files,” on page 51.	1	0 - Disable 1 - Allow
REPLICATE_PRIMARY_TREE_TO_SHADOW Controls how the primary tree is replicated from the primary tree to the shadow tree. By default, it is disabled, and paths are replicated to the secondary storage area when data is actually moved from the primary location to the secondary location. If it is enabled, the entire tree is replicated even if no files in a path have been moved to the secondary storage location. For information, see Section 4.4, “Configuring a Global Policy that Replicates Branches of the Primary File Tree in the Shadow File Tree,” on page 46.	0	0 - Disable 1 - Allow
SHIFT_MODIFIED_SHADOW_FILES Controls whether a file is moved from the shadow file tree to the primary file tree based on its modification time. For information, see “Shift Modified Shadow Files” on page 47.	1	0 - Disable 1 - Allow

Parameter Name and Description	Default Value	Valid Values
SHIFT_ACCESSED_SHADOW_FILES Controls whether a file is moved from the shadow file tree to the primary file tree if it is accessed twice during a specific period of time. Use with SHIFT_DAYS_SINCE_LAST_ACCESS to specify the period of time. For information, see “Shift Accessed Shadow Files” on page 48 .	0	0 - Disable 1 - Allow
SHIFT_DAYS_SINCE_LAST_ACCESS Specifies the number of days to use when determining if a file should be moved back to the primary storage area. When it is used with SHIFT_ACCESSED_SHADOW_FILES , the parameter sets the time when files are migrated back to the primary storage area after the second access within the specified elapsed time.	1	0 - Disable 1 to 365 (in days)

A.4.2 Using Novell Remote Manager to Configure DST Parameters for the SET Command

You can configure the DST parameters for the SET command by using Novell Remote Manager for Linux.

- 1 In Novell Remote Manager for Linux, select *Manage NCP Services*, then select *Manage Server*.
- 2 In the *Set Parameter Information* table, locate the DST parameter you want to configure.
 The following Server Parameters are available. The settings shown are the default values. For information, see [Section A.4.1, “Understanding DST Parameters for the SET Command,” on page 164](#).

DUPLICATE_SHADOW_FILE_ACTION	0
DUPLICATE_SHADOW_FILE_BROADCAST	1
REPLICATE_PRIMARY_TREE_TO_SHADOW	0
SHIFT_ACCESSED_SHADOW_FILES	0
SHIFT_MODIFIED_SHADOW_FILES	1
SHIFT_DAYS_SINCE_LAST_ACCESS	1
- 3 Modify settings by clicking the link for the value in the *Parameter Value* column to open a page where you can change the value.
- 4 In *New Value*, type the value for the parameter, then click *Change* to save and apply the setting.

Current Value	New Value
1	<input type="text" value="0"/> change

[Back](#)

- 5** If you enabled `DUPLICATE_SHADOW_FILE_BROADCAST`, make sure that NCP Server is configured to support broadcast messages by verifying that the Disable Broadcast (`DISABLE_BROADCAST`) parameter for the `SET` command is disabled.

5a In Novell Remote Manager for Linux, select *Manage NCP Services*, then select *Manage Server*.

5b In the *Set Parameter Information* table, locate the `DISABLE_BROADCAST` parameter, then view the current value of the parameter. By default, the parameter is disabled (set to 0), which means that NCP Server supports broadcast messages.

<code>DISABLE_BROADCAST</code>	0
--------------------------------	-------------------

- 5c** If the `DISABLE_BROADCAST` parameter is enabled (set to 1), click the link for the value in the *Parameter Value* column to open a page where you can change the value.

<code>DISABLE_BROADCAST</code>	1
--------------------------------	-------------------

- 5d** In *New Value*, type 0, then click *Change* to save and apply the settings that disable the `DISABLE_BROADCAST` parameter, which enables broadcasting for NCP Server.

IMPORTANT: Messages are received only by logged-in users who are using Novell Client versions that are capable of receiving broadcast messages, and that are configured to receive them.

DISABLE_BROADCAST	
Current Value	New Value
1	<input type="text" value="0"/> change

[Back](#)

A.4.3 Using the `ncpcon set` Command to Configure DST Parameters

- 1 Open a terminal console on the Linux server, then log in as the `root` user.
- 2 At the terminal console prompt, enter

```
ncpcon set parameter_name=value
```

Replace *parameter_name* and *value* with the settings you want to change.

IMPORTANT: Make sure to enter the commands in lowercase.

For example, the following commands set the DST parameters to their default values.

```
ncpcon set duplicate_shadow_file_action=0
```

```
ncpcon set duplicate_shadow_file_broadcast=1
```

```
ncpcon set replicate_primary_tree_to_shadow=0
```

```
ncpcon set shift_modified_shadow_files=1
```

```
ncpcon set shift_accessed_shadow_files=0
```

```
ncpcon set shift_days_since_last_access=1
```

If the `DUPLICATE_SHADOW_FILE_BROADCAST` parameter is enabled, make sure that the `DISABLE_BROADCAST` parameter is disabled in order to allow broadcasting for NCP Server. For example, enter

```
ncpcon set disable_broadcast=0
```

A.5 DST Commands for `/etc/opt/novell/ncpserv.conf`

Use the commands in this section for the NCP Server configuration file (`/etc/opt/novell/ncpserv.conf`). The `ncpserv.conf` file is read only at Novell eDirectory™ startup time. If you modify this file directly, you must restart `nds` in order for the changes to take effect.

SHADOW_VOLUME *volume_name shadow_area_path*

Identifies a volume as having a secondary storage area and specifies the path to that secondary volume. Any NCP volume can have a shadow. The root subdirectory for the shadow area needs to already exist; the rest of the subdirectory tree is automatically created as needed. The volume shadow area is available the next time the volume is mounted.

SHIFT_MODIFIED_SHADOW_FILES *value*

Enables a modified file to be moved from the secondary storage area to the primary storage area. The value can be either 0 (Disabled) or 1 (Allow). The default value is 1. When this parameter is on, and a file that is located in the secondary storage area is modified, the file is automatically moved back to the primary storage area when the file is closed.

SHIFT_ACCESSED_SHADOW_FILES *value*

Enables a file to be moved from the secondary storage area to the primary storage area if it is accessed as read-only a second time during a specified period of time. The value can be either 0 (Disabled) or 1 (Allow). The default value is 0. When this parameter is on, and a file that is located in the shadow area is accessed, if this is the second access within the configured `SHIFT_DAYS_SINCE_LAST_ACCESS`, the file is automatically moved back to the primary area when the file is closed.

SHIFT_DAYS_SINCE_LAST_ACCESS *value*

Specifies the number of days to use when determining if a file should be moved back to the primary storage area. The value may be 0 (Disable), or between 1 and 365 (in days). The default is 1. When it is used with `SHIFT_ACCESSED_SHADOW_FILES`, the parameter sets the time when files are migrated back to the primary storage area after the second access within the specified elapsed time.

DUPLICATE_SHADOW_FILE_ACTION *value*

Controls how duplicate files conflicts are handled. The default is 0.

0 - Show duplicate shadow files (default)

1 - Hide duplicate shadow files

- 2 - Rename duplicate shadow files
- 3 - Delete duplicate files from shadow area
- 4 - Move duplicate shadow files to / `._DUPLICATE_FILES`

DUPLICATE_SHADOW_FILE_BROADCAST *value*

Enables a message to be broadcast to an NCP user when a duplicate copy of a file is located on both the primary volume and the secondary volume. Valid settings are 0 (Disabled) and 1 (Allow). The default is enabled. The Novell Client version in use must support receiving broadcast messages in order for the user to receive the message.

REPLICATE_PRIMARY_TREE_TO_SHADOW *value*

Controls how the primary tree is replicated from the primary tree to the shadow tree. Valid settings are 0 (Disabled) and 1 (Allow). By default, it is disabled, and paths are replicated to the secondary storage area gradually as data is moved from the primary location to the secondary location. If it is enabled, the entire tree is replicated even if no files in a path have been moved to the secondary storage location.

A.6 DST Commands for `/etc/opt/novell/shadowfs.conf`

Use the commands in this section for the Shadow File System configuration file (`/etc/opt/novell/shadowfs.conf`).

SHADOW *root_path primary_area_path shadow_area_path*

Defines a shadow volume for ShadowFS. A shadow volume that is defined by the NCP engine is automatically mounted by ShadowFS and does not need to be defined in this configuration file.

SHIFT_ON_MODIFY *value*

Enables a modified file to be moved from the secondary storage area to the primary storage area. The value can be either 0 (Off) or 1 (On). The default value is 1. When this parameter is on, and a file that is located in the secondary storage area is modified, the file is automatically moved back to the primary area when the file is closed.

SHIFT_ON_ACCESS *value*

Enables a file to be moved from the secondary storage area to the primary storage area if it is accessed a second time during a specified time period. The value can be either 0 (Off) or 1 (On). The default value is 0. When this parameter is on, and a file that is located in the shadow area is accessed, if this is the second access within the configured `SHIFT_DAYS_SINCE_LAST_ACCESS`, the file is automatically moved back to the primary storage area when the file is closed.

SHIFT_DAYS_SINCE_LAST_ACCESS *value*

Specifies the number of days to use when determining if a file should be moved back to the primary storage area. The value may be 0 (Disable), or between 1 and 365 (in days). The default is 1. When it is used with `SHIFT_ON_ACCESS`, the parameter sets the time when files are migrated back to the primary storage area after the second access within the specified elapsed time.

A.7 DST EXCLUDE_VOLUME Command for /etc/opt/novell/ncp2nss.conf

Use the command in this section for the `/etc/opt/novell/ncp2nss.conf` file.

EXCLUDE_VOLUME *nss_volumename*

Prevents the named NSS volume from mounting in NCP Server. Use this command when you want to use the specified NSS volume as the secondary storage area of a DST shadow volume.

An entry is automatically created in the `/etc/opt/novell/ncp2nss.conf` file by using Novell Remote Manager for Linux to set the *Manage NCP Services > Manage Shares > NCP/NSS Bindings > NCP Accessible* option to No for a given NSS volume that you want to use as a secondary storage location in a DST shadow volume. For instructions, see [Section 8.3](#), “Configuring the NCP/NSS Bindings for an NSS Volume,” on page 90.

A.8 DST Shadow Volume Information in /etc/NCPVolumes

The `/etc/NCPVolumes` file is an XML file that contains an entry for each mounted volume. It lists the volume’s name and the path for the volume’s primary file tree (PRIMARY_ROOT). If the volume is a shadow volume, it also shows the path for the shadow file tree (SHADOW_ROOT). Using this data file, a backup utility can easily locate each mounted NCP volume and find its primary and shadow file trees.

For example, the following XML entry defines the DST shadow volume named VOL1:

```
<VOLUME>

  <NAME>VOL1</NAME>

  <PRIMARY_ROOT>/media/nss/VOL1</PRIMARY_ROOT>

  <SHADOW_ROOT>/media/nss/ARCVOL</SHADOW_ROOT>

</VOLUME>
```

A.9 DST ShadowFS Volume Information in /etc/mtab.shadowfs

The `/etc/mtab.shadowfs` file is an XML file that contains an entry for each shadow volume mounted by ShadowFS. It lists the mount point, the path for the primary file tree, and the path for the shadow file tree.

For example, the following XML entry defines the DST shadow volume for ShadowFS named VOL1:

```
<SHADOWFS_MOUNTPOINTS>

  <MOUNTPOINT>

    <PATH>/media/shadowfs/VOL1</PATH>

    <PRIMARY_TREE>/media/nss/VOL1</PRIMARY_TREE>
```

```
<SHADOW_TREE>/media/nss/ARCVOL</SHADOW_TREE>  
  
</MOUNTPOINT>  
  
</SHADOWFS_MOUNTPOINTS>
```

RPM Files for Dynamic Storage Technology

B

The following RPM files are installed for Dynamic Storage Technology for Novell® Open Enterprise Server (OES) 2 Linux.

novell-ncp.i386.rpm

This RPM contains the ncp server shared library (`libncpengine.so`) that runs as part of Novell eDirectory™. This is the piece that handles all client NetWare Core Protocol™ (NCP™) requests.

novell-ncpserv-nrm.i386.rpm

This RPM contains the Novell Remote Manager for Linux plugin provided by the NCP team (`libnrm2ncp.so`).

novell-ncpserv.i386.rpm

This RPM contains `ncpcon` and `ncptop` tools to help administrators manage the NCP Server. It also contains daemons that connect the `ncpserv` engine to other services on the server: `ncp2nss` and `lum2ncp`.

novell-nrm.i386

This RPM contains `httpstk` and the shared library (`libnrm.so`) that creates Novell Remote Manager for Linux as an `httpstk` plug-in. It also contains other files used by Novell Remote Manager.

Documentation Updates

C

This section contains information about documentation content changes made to the *OES 2: Dynamic Storage Technology Administration Guide* since the initial release of Novell® Open Enterprise Server 2. If you are an existing user, review the change entries to readily identify modified content. If you are a new user, simply read the guide in its current state.

Refer to the publication date, which appears on the title page, to determine the release date of this guide. For the most recent version of the *OES 2: Dynamic Storage Technology Administration Guide*, see the [OES 2 documentation Web site \(http://www.novell.com/documentation/oes2/storage.html#b14wnty\)](http://www.novell.com/documentation/oes2/storage.html#b14wnty).

In this section, content changes appear in reverse chronological order, according to the publication date. Within a dated entry, changes are grouped by chapter and sequenced alphabetically. Each change entry provides a link to the related topic and a brief description of the change.

This document was updated on the following dates:

- ♦ [Section C.1, “March 3, 2009,” on page 173](#)
- ♦ [Section C.2, “February 13, 2009,” on page 174](#)
- ♦ [Section C.3, “January 13, 2009,” on page 175](#)
- ♦ [Section C.4, “December 2008 \(OES 2 SP1 Linux\),” on page 175](#)
- ♦ [Section C.5, “May 30, 2008,” on page 177](#)
- ♦ [Section C.6, “May 5, 2008,” on page 178](#)
- ♦ [Section C.7, “January 7, 2008,” on page 179](#)
- ♦ [Section C.8, “December 7, 2007,” on page 179](#)
- ♦ [Section C.9, “November 16, 2007,” on page 180](#)

C.1 March 3, 2009

Updates were made to the following sections. The changes are explained below.

- ♦ [Section C.1.1, “Configuring DST Shadow Volumes with Novell Cluster Services for Linux,” on page 173](#)

C.1.1 Configuring DST Shadow Volumes with Novell Cluster Services for Linux

Location	Change
Step 3g in Section 11.4.4, “Configuring the Load and Unload Scripts for a Shadow Volume,” on page 140	If you are loading other items like Samba, rsync, and so on, and you are relying on the shadowfs volume to provide the unified file tree view, you might need to add additional wait time for the shadowfs file system to mount.

Location	Change
Step 4c in Section 11.4.4, "Configuring the Load and Unload Scripts for a Shadow Volume," on page 140	If you are using <code>shadowfs</code> to provide a unified file tree view to Samba users, you must unmount the FUSE-mounted file systems that are displayed in the <code>/media/shadowfs/VOLUME</code> directory.

C.2 February 13, 2009

Updates were made to the following sections. The changes are explained below.

- Section C.2.1, "Configuring DST Shadow Volumes with Novell Cluster Services for Linux," on page 174
- Section C.2.2, "Installing and Configuring Dynamic Storage Technology," on page 174
- Section C.2.3, "Managing DST Shadow Volumes for NSS Volumes," on page 175

C.2.1 Configuring DST Shadow Volumes with Novell Cluster Services for Linux

Location	Change
Section 11.4.4, "Configuring the Load and Unload Scripts for a Shadow Volume," on page 140	<p>If you are using <code>shadowfs</code> to provide the unified file tree view for Samba/CIFS users, you must allow time in the load script after mounting the shadow volume to allow <code>shadowfs</code> to become active before continuing. Add a <code>sleep 10</code> command after mount command.</p> <p>For example:</p> <pre>exit_on_error ncpcon mount VOL1=254,shadowvolume=ARCVOL1 sleep 10</pre>
Section 11.6, "Removing a Clustered DST Shadow Volume," on page 144	<p>IMPORTANT: In the OES 2 SP1 release for DST, if you disable the <i>Check to leave existing files on the shadow volume</i>, the shadow volume is not removed and an error occurs. DST does not remove the shadow relationship until you enable the option to keep data where it is.</p>

C.2.2 Installing and Configuring Dynamic Storage Technology

Location	Change
Section 4.9, "Restarting the Novell eDirectory (ndsd) Daemon," on page 57	<p>IMPORTANT: Restarting or stopping <code>ndsd</code> automatically disconnects all user connections and does not warn users before the connection is broken. Users can reconnect to the server after the service starts.</p>

C.2.3 Managing DST Shadow Volumes for NSS Volumes

Location	Change
Section 8.7, "Removing a DST Shadow Volume," on page 100	IMPORTANT: In the OES 2 SP1 release for DST, if you disable the <i>Check to leave existing files on the shadow volume</i> , the shadow volume is not removed and an error occurs. DST does not remove the shadow relationship until you enable the option to keep data where it is.

C.3 January 13, 2009

Updates were made to the following sections. The changes are explained below.

- ♦ Section C.3.1, "Management Tools for Dynamic Storage Technology," on page 175
- ♦ Section C.3.2, "Managing DST Shadow Volumes for NSS Volumes," on page 175

C.3.1 Management Tools for Dynamic Storage Technology

Location	Change
Section 7.1.4, "Quick Reference for NCP Server Options," on page 73	Clarified that the mount or unmount options apply to the primary volume of the DST shadow volume pair.

C.3.2 Managing DST Shadow Volumes for NSS Volumes

Location	Change
Section 8.4.2, "Preparing the NSS Volumes for Use in a DST Shadow Volume," on page 95	In Step 4 on page 96 , you must rename or delete the <code>/media/nss/primary_volumename/._NETWARE/.trustee_database.xml</code> file on the primary volume before you can copy the <code>.trustee_database.xml</code> file from the secondary volume to that location.

C.4 December 2008 (OES 2 SP1 Linux)

Updates were made to the following sections. The changes are explained below.

- ♦ Section C.4.1, "Configuring DST Shadow Volumes with Novell Cluster Services for Linux," on page 176
- ♦ Section C.4.2, "Installing and Configuring Dynamic Storage Technology," on page 176
- ♦ Section C.4.3, "Installing and Configuring Shadow File System (ShadowFS) for CIFS/Samba Users," on page 176
- ♦ Section C.4.4, "Managing DST Shadow Volumes for NSS Volumes," on page 176

- Section C.4.5, “Planning Your Dynamic Storage Technology Solution,” on page 177
- Section C.4.6, “Using DST to Migrate Data on Demand from NetWare to OES 2 Linux,” on page 177

C.4.1 Configuring DST Shadow Volumes with Novell Cluster Services for Linux

Location	Change
Section 11.6, “Removing a Clustered DST Shadow Volume,” on page 144	This section is new.

C.4.2 Installing and Configuring Dynamic Storage Technology

Location	Change
Section 4.1.7, “SLP,” on page 41	This section is new.
“Broadcasting Conflict Messages to NCP Users” on page 53	The broadcast message capability is called Send Message in the Novell Client. In OES 2 SP1, the Send Message feature is available in the Novell Client 4.91 SP4 for Windows XP/2003, the Novell Client 1.0 SP1 for Vista, and the Novell Client 2.0 for Linux.

C.4.3 Installing and Configuring Shadow File System (ShadowFS) for CIFS/Samba Users

Location	Change
Section 5.4, “Installing ShadowFS and FUSE,” on page 61	IMPORTANT: Make sure you run only a single instance of shadowfs at a time. Avoid entering the command multiple times.
Section 5.11, “Starting and Stopping ShadowFS Manually,” on page 65	Added information on how to stop shadowfs.

C.4.4 Managing DST Shadow Volumes for NSS Volumes

Location	Change
Section 8.2.3, “Creating an NSS Pool,” on page 84	Novell CIFS for Linux and Novell AFP for Linux are available in OES 2 SP1 Linux. DST has not been tested with these protocols. They are not supported for use with DST shadow volume pairs in OES 2 SP1 Linux.

Location	Change
Section 8.6, "Viewing Volume Information," on page 100	This section is new.

C.4.5 Planning Your Dynamic Storage Technology Solution

Location	Change
Section 3.1.2, "Storage Devices," on page 23	Revised for clarity.
Section 3.1.3, "iSCSI Block Storage Devices," on page 25	Added information about supported configurations.
Section 3.1.4, "Remote Server-to-Server Connections," on page 26	This section is new.
Section 3.1.5, "File Systems," on page 26	IMPORTANT: Mixing file systems for the primary and secondary areas in a given DST shadow volume pair is not supported.
Section 3.3.1, "DST Support for NSS Media Formats," on page 31	This section is new.
Section 3.3.4, "DST Support for NSS File System Trustees and Attributes," on page 34	This section is new.
Section 3.3.5, "DST Support for NSS Volume, Directory, and User Quotas," on page 34	This section is new.

C.4.6 Using DST to Migrate Data on Demand from NetWare to OES 2 Linux

Information in this chapter was revised and moved to [Section 3.1.3, "iSCSI Block Storage Devices,"](#) on page 25.

C.5 May 30, 2008

Updates were made to the following section. The changes are explained below.

- ♦ [Section C.5.1, "Managing Policies for Shadow Volumes,"](#) on page 178

C.5.1 Managing Policies for Shadow Volumes

Location	Change
Section 9.1.10, “Subdirectory Restrictions,” on page 112	Specify the path relative to the root of the DST volume, and not to the root of the server. For example, enter <code>subdir1/subdir2</code> .

C.6 May 5, 2008

Updates were made to the following section. The changes are explained below.

- ♦ Section C.6.1, “Commands and Utilities for Dynamic Storage Technology,” on page 178
- ♦ Section C.6.2, “Installing and Configuring Dynamic Storage Technology,” on page 178
- ♦ Section C.6.3, “Installing and Configuring Shadow File System (ShadowFS) for CIFS/Samba Users,” on page 178
- ♦ Section C.6.4, “Managing DST Shadow Volumes for NSS Volumes,” on page 179

C.6.1 Commands and Utilities for Dynamic Storage Technology

Location	Change
Section A.1.2, “Command Line Mode,” on page 157	You must escape quote characters when using <code>ncpcon</code> to issue commands at the console command prompt.

C.6.2 Installing and Configuring Dynamic Storage Technology

Location	Change
Section 4.1.5, “Linux User Management,” on page 40	Linux User Management is installed by default. Only CIFS/Samba users must be Linux-enabled with Linux User Management.

C.6.3 Installing and Configuring Shadow File System (ShadowFS) for CIFS/Samba Users

Location	Change
Section 5.3, “Preparing Your System for Using ShadowFS,” on page 60	For information about configuring SSH for a user, see “SSH Services on OES 2 Linux” in the <i>OES 2 SP1: Planning and Implementation Guide</i> .
Section 5.5, “Setting Rights to ShadowFS Shares,” on page 62	For information about configuring SSH for a user, see “SSH Services on OES 2 Linux” in the <i>OES 2 SP1: Planning and Implementation Guide</i> .

C.6.4 Managing DST Shadow Volumes for NSS Volumes

Location	Change
Section 8.1.1, “DST Shadow Volumes,” on page 77	NOTE: In the Dynamic Storage Technology interface in Novell Remote Manager for Linux, you will see the terms “shadow” and “secondary” used interchangeably for the secondary storage area. The interface also refers to the primary volume as being “shadowed” when it is the primary volume in a DST shadow volume. Future changes are planned to resolve terminology inconsistencies.

C.7 January 7, 2008

Updates were made to the following section. The changes are explained below.

- ♦ [Section C.7.1, “Managing DST Shadow Volumes for NSS Volumes,” on page 179](#)

C.7.1 Managing DST Shadow Volumes for NSS Volumes

Location	Change
Section 8.3.4, “Enabling or Disabling NCP/NSS Bindings by Editing the /etc/opt/novell/ncp2nss.conf File,” on page 93	When the NCP/NSS bindings parameter is disabled for a volume, NCP Server adds an EXCLUDE_VOLUME entry to the /etc/opt/novell/ncp2nss.conf file.

C.8 December 7, 2007

Updates were made to the following sections. The changes are explained below.

- ♦ [Section C.8.1, “Planning Your Dynamic Storage Technology Solution,” on page 179](#)
- ♦ [Section C.8.2, “Using DST to Migrate Data on Demand from NetWare to OES 2 Linux,” on page 180](#)

C.8.1 Planning Your Dynamic Storage Technology Solution

Location	Change
Section 3.1.3, “iSCSI Block Storage Devices,” on page 25	References were added for information about Linux iSCSI target devices.

C.8.2 Using DST to Migrate Data on Demand from NetWare to OES 2 Linux

Location	Change
Chapter 12, “Using Secondary Volumes on iSCSI Block Storage Devices,” on page 145	You can follow a similar procedure for NSS volumes on any iSCSI target device that is compatible with the Linux iSCSI initiator running on the OES 2 Linux server.

C.9 November 16, 2007

Updates were made to the following section. The changes are explained below.

- ♦ [Section C.9.1, “Installing and Configuring Shadow File System \(ShadowFS\) for CIFS/Samba Users,” on page 180](#)

C.9.1 Installing and Configuring Shadow File System (ShadowFS) for CIFS/Samba Users

The following change was made to this section:

Location	Change
Section 5.5, “Setting Rights to ShadowFS Shares,” on page 62	To test the POSIX rights setup, you need a user who is Linux-enabled with LUM, has SSH permissions for the server, and who has eDirectory rights to the location.