

Novell Storage Services™ File System

www.novell.com

May 14, 2005

ADMINISTRATION GUIDE FOR
NETWARE® 6.5



Novell
®

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.

You may not use, export, or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Copyright © 2005 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 at <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

Novell Storage Services File System Administration Guide for NetWare 6.5
[May 14, 2005](#)

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

ConsoleOne is a registered trademark of Novell, Inc. in the United States and other countries.

eDirectory is a trademark of Novell, Inc.

Groupwise is a registered trademark of Novell, Inc. in the United States and other countries.

Hot Fix is a trademark of Novell, Inc.

NetWare is a registered trademark of Novell, Inc. in the United States and other countries.

NetWare Core Protocol and NCP are trademarks of Novell, Inc.

NetWare Loadable Module and NLM are trademarks of Novell, Inc.

Novell is a registered trademark of Novell, Inc. in the United States and other countries.

Novell Client is a trademark of Novell, Inc.

Novell Cluster Services is a trademark of Novell, Inc.

Novell Core Protocol and NCP are trademarks of Novell, Inc.

Novell Directory Services and NDS are registered trademarks of Novell, Inc. in the United States and other countries.

Novell Storage Services is a trademark of Novell, Inc.

Storage Management Services is a trademark of Novell, Inc.

Transaction Tracking System and TTS are trademarks of Novell, Inc.

Third-Party Materials

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

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org>).

Contents

About This Guide	15
1 Overview of NSS	17
Benefits of NSS	17
Understanding NSS	18
Storage Pools	18
NSS Volumes	19
NSS Features	19
Use Less Memory and Gain More Speed	20
Improve Storage Availability	20
Prevent Unauthorized Access	20
Protect Data from Corruption or Loss	21
Maximize Available Space	22
What's Next	22
2 What's New	23
What's New for NetWare 6.5	23
Pool Snapshot	23
Software RAID 1 (Mirroring)	23
Software RAIDs 0 and 5	24
Distributed File Services for Moving or Splitting Volumes	24
NSS Management Utility	24
NSS Sys: Volume Recovery Commands	24
What's Changed for NetWare 6.5	24
CD, DVD, and Macintosh CD Device Support	25
Volume Copy Upgrade	25
Name Caching	26
Mirroring Partitions and Hot Fix	26
CIFS and AFP Protocols	26
Admin Volume	26
What's New for NetWare 6.5 Support Pack 2	26
Encrypted Volume Support	26
Multiple Device Selection in NSSMU	27
CD and DVD Image Files as NSS Volumes	27
What's New for NetWare 6.5 Support Pack 3	27
Storage Plug-in for Novell iManager 2.5	27
Partition Information	27
Deleting Pool Snapshots	27
3 Management Utilities for NSS	29
Novell iManager Storage Plug-In	29
Prerequisites for Using the Storage, Archive Versioning, CIFS, and Clustering iManager Plug-Ins	30
Downloading and Installing Plug-In Updates	31
Accessing Novell iManager	34
Accessing NSS Storage Management Role and Tasks	34
Selecting a Server to Manage	35

Understanding iManager Storage Management Tasks	36
NSSMU	41
NSS Command Line Management	43
Novell NetStorage	43
Accessing NetStorage	43
Configuring File System Trustees, Trustee Rights, and Attributes	44
Purging and Salvaging Deleted Files	44
Browsing Directories and Files	44
Novell Remote Manager.	44
Novell Client for Windows 2000/XP	45
Trustee Rights Utility	45
ConsoleOne	45
Virtual File Services and Scripts.	46
4 Planning for NSS Storage Solutions	47
Prerequisites	47
Security Considerations	47
Using Encrypted Volume Support	47
Preventing Encrypted Data from Exposure in a Core Dump.	48
Using Data Shredding to Prevent Unauthorized Access to Purged Deleted Files.	48
Protecting the Admin Volume and Files.cmd	48
Understanding Security Equivalence Vectors for NSS Users	48
Controlling File System Access for NSS Volumes.	48
Coexistence and Migration Issues.	49
Compatibility with Operating Systems and Services	49
Compatibility Issues for the Storage, Archive Versioning, CIFS, and Clustering iManager Plug-Ins	49
Upgrading to NetWare 6.5 from NetWare 6.0 and Earlier	50
Comparison of NSS and NetWare Traditional File Systems.	50
Planning for Your Storage Needs	50
Devices	51
Software RAID Devices	51
Multiple I/O Paths	51
Free Space	51
NSS Pools and Volumes.	51
NSS Encrypted Volumes	52
Storage Objects in eDirectory	52
Naming NSS Storage Objects.	52
What's Next	54
5 Managing Devices	55
Understanding Devices	55
Viewing Devices on a Server	56
Viewing Details for a Device.	57
Scanning for Devices	58
Initializing a Disk.	59
Sharing Devices	60
Planning for Device Sharing	60
Configuring the Device's Share State	61
Viewing Partitions on a Device	61
Viewing Pools on a Device	62
What's Next	63
6 Managing Partitions	65
Understanding Partitions	65
Creating NSS Partitions	67
Viewing a List of Partitions	67

Viewing Partitions on a Device	67
Viewing Partitions in a Software RAID Device	68
Viewing Partitions in an NSS Pool	68
Viewing Details for a Partition	69
Labeling a Partition	69
Deleting a Partition	69
Deleting NSS Partitions in an Software RAID Device	69
Deleting NSS Partitions in a Pool	70
Deleting Cluster Services Partitions.	70
Deleting an iSCSI Partition	71
7 Managing Software RAID Devices	73
Understanding Software RAID Devices	73
Planning for a Software RAID Device	75
General Guidelines for Software RAID Devices	75
Guidelines for Software RAID 1 Devices	76
Drive Restrictions for NSS Software RAID Devices.	76
Choosing a Software RAID Solution	76
Determining the Partition Size	77
Determining the Number of Partitions.	78
Determining the Stripe Size for RAID 0 and RAID 5	79
Viewing Software RAID Devices on a Server.	79
Viewing Details of a Software RAID Device	80
Creating a Software RAID Device Using iManager.	82
Renaming a Software RAID Device	83
Increasing the Size of a Software RAID Device	83
Restripping a Software RAID 0 or 5 Device	85
Replacing a Failed Segment in a Software RAID.	85
Deleting a Software RAID Device	87
Viewing Pools on a Software RAID Device.	88
Viewing Partitions on a Software RAID Device	88
Deleting Partitions on a Software RAID Device	89
Managing Software RAID Devices with NSSMU	89
Creating Software RAID Devices with NSSMU.	90
Mirroring an Existing Pool with NSSMU	91
Creating a Software RAID 10 with NSSMU.	91
Creating a Software RAID 15 with NSSMU.	92
Creating a RAID 1 Mirror to Duplicate Data	93
8 Managing Multiple Connection Paths to Devices	95
Planning Your Multiple Connection Path Solution	95
Configuring the Primary Path and Priorities for Failover Connection Paths	96
Viewing Connection Path Details.	97
Setting a Connection Path as Up or Down	97
Setting the Primary Path for a Device to Its Default Path.	98
Resetting the Server Registry with Default Priority Settings for a Device	98
Managing Multiple Paths with Server Console Commands	99
9 Managing NSS Pools	101
Creating Pools with iManager	101
Viewing Pools on a Server	104
Viewing Pool Details	105
Viewing Partition Information for a Pool	106
Viewing Volume Information for a Pool.	106
Viewing Device Information for a Pool	107
Renaming a Pool	107

Increasing the Size of a Pool	108
Activating and Deactivating Pools	109
Deleting a Pool	109
Verifying and Rebuilding NSS Pools and Volumes	110
Viewing and Salvaging Deleted NSS Volumes in a Pool	111
Updating eDirectory Pool Objects	112
Preventing Pools from Activating on Multiple Servers	113
Managing MSAP Using Server Console Commands	113
What's Next	114
10 Managing NSS Pool Snapshots	115
Benefits of Pool Snapshots	115
How the Pool Snapshot Works	116
Understanding Key Concepts for Pool Snapshots	117
Creating a Pool Snapshot	117
Naming Pool Snapshots	117
Choosing the Stored-on Pool	118
Maintaining the Stored-on Pool	118
Activating Pool Snapshots	119
Deleting Pool Snapshots	119
Managing Pool Snapshots Using iManager	120
Creating a New Pool Snapshot	120
Viewing Pool Snapshot Details	122
Renaming a Pool Snapshot	123
Activating and Deactivating a Pool Snapshot	123
Moving an Active Pool Snapshot Offline	124
Deleting a Pool Snapshot	125
Managing Pool Snapshots Using Commands	126
11 Managing NSS Volumes	127
Understanding NSS Volumes	128
Understanding Volume Attributes	128
Encryption	129
Data Shredding	129
Compression	129
Data Migration	129
Directory Quotas	129
User Space Quotas	130
Salvage Files	130
Read Ahead Blocks in Volumes	130
Flush Files Immediately	130
User-Level Transaction Model	130
File-Level Snapshot	130
Modified File List	131
Backup	131
Configuring Nonencrypted NSS Volumes with iManager	131
Configuring Encrypted NSS Volumes with NSSMU	133
Updating eDirectory Volume Objects	133
Viewing the Details of a Volume	134
Viewing Properties of a Volume	134
Modifying Attributes of an NSS Volume	136
Renaming an NSS Volume	136
Activating and Deactivating an NSS Volume	137
Activating and Deactivating CDs and DVDs as NSS Volumes	137
Activating and Deactivating CD and DVD Image Files as NSS Volumes	138
Activating and Deactivating DOS Partitions as NSS Volumes	139

Mounting and Dismounting an NSS Volume	139
Mounting a USB Floppy Disk as a Local FAT Volume	139
Deleting an NSS Volume	140
Verifying and Rebuilding NSS Pools and Volumes	141
Mounting the Volume to Repair Journaled Errors.	141
Verifying the Pool to Repair Inconsistent Data Blocks	142
Restoring the Data from Backup	142
Rebuilding the Pool	142
Error and Log Files	142
Controlling Access to the Admin Volume and Files.cmd File.	142
Assigning Volume Rights with Trustees.xml (NetWare)	143
Restricting Access to Files.cmd (NetWare)	145
Using Data Shredding to Prevent Access to Deleted Files.	146
Setting the Data Shredding Attribute When You Create a Volume	146
Setting the Data Shredding Attribute for an Existing Volume	147
Disabling Data Shredding for an Existing Volume	147
Configuring Read Ahead Blocks Parameters.	148
Using the Flush Files Immediately Attribute to Protect Against Possible Data Corruption on System Failure	148
Setting the Flush Files Immediately Attribute When You Create a Volume.	148
Setting the Flush Files Immediately Attribute for an Existing Volume.	149
Enabling the Flush Files Immediately Attribute for All Volumes on a Server	149
Using the Transaction Tracking System for Application-Based Transaction Rollback	150
Using the File-Level Snapshot Attribute to Enable the Backup of Open Files	151
Understanding File-Level Snapshots	151
How the File Snapshot Attribute Works	151
Sizing the Volume to Accommodate File Snapshots	152
Assessing I/O Overhead for File Snapshots	153
Configuring Volumes with the File Snapshot Attribute	153
Configuring Backup Software to Use File Snapshots	156
Restoring Volumes from Backup Media.	156
Configuring the NSS Volume Salvage Area	156
Setting the Purge Delay for the Salvage Area	157
Setting the Low and High Watermarks for Purging the Salvage Area	157
Viewing, Salvaging, or Purging Deleted NSS Volumes.	157
Salvaging or Purging Deleted Files	159
Salvaging or Purging Deleted Files with NetStorage	159
Salvaging or Purging Deleted Files with the Novell Client	160
Salvaging or Purging Deleted Files with Novell Remote Manager	160
Understanding Space Quotas	160
Managing NSS Volume Quotas	161
Managing Directory Quotas	163
Setting the Directory Quotas Attribute for an NSS Volume	163
Novell NetStorage.	164
Novell Client.	164
Novell Remote Manager for NetWare.	165
Managing User Space Quotas	166
Setting the User Space Quotas Attribute for an NSS Volume	166
Viewing User Space Quotas	167
Configuring User Space Quotas	168
Modifying a User Quota	169
Deleting a User Quota	169
What's Next.	169
12 Managing Encrypted NSS Volumes	171
Understanding Encrypted Volume Support.	171

Encryption Method	171
How EVS Works	172
Guidelines for Using Encrypted Volumes	172
Creating an Encrypted Volume	172
Using Encrypted Volumes in a Server Cluster	173
Archiving Files from an Encrypted Volume	174
Using Direct I/O on an Encrypted Volume.	174
Managing Encrypted Volumes with NSS Commands	174
Removing Encrypted Volumes	175
What's Next	176
13 Using Compression to Conserve Storage Space on NSS Volumes	177
Understanding File Compression	177
Compression Settings	178
Compression and Decompression Processes	178
Compression Criteria	178
Decompression Criteria	179
Compression and Storage Backup	179
Planning for File Compression	180
Inactivity Determines Which Files Are Eligible for Background Compression	180
Some Files Do Not Compress Well	180
Some Volumes Are Not Good Candidates for Compression	181
Decompression Activity Depends on Available Space	181
Immediate Compression Impacts CPU Performance	181
Files Remain Compressed during Backup and Restore	181
If Set, the Compression Attribute Persists for the Life of the Volume	181
How to Monitor Compression Activity	181
Configuring Compression Parameters for a Server	182
Understanding Compression Parameters	182
Setting Compression Parameters with Monitor	184
Setting Compression Parameters with Novell Remote Manager	184
Setting Compression Parameters with the Set Command.	184
Configuring a Volume for Compression	184
Enabling Compression for a New Volume	185
Enabling Compression for an Existing Volume	185
Suspending Compression for Volumes or Files	186
Disabling Compression for a Volume	186
Restoring Data to a Uncompressed Volume	186
Configuring Compression Attributes for Directories and Files.	186
Using the Flag Command	187
Setting Compression Attributes for a Directory	187
Setting Compression Attributes for a File	188
Viewing Compression Status for Files and Directories	188
Using NSS Commands to Configure and Monitor Compression	188
Copying Compressed Files between Volumes with the Ncopy Command	189
Viewing the File Attributes with the Ndir Command	189
Repairing Compressed Volumes with the Compxfix Utility	189
14 Using Distributed File Services for Moving and Splitting NetWare 6.x NSS Volumes	191
Understanding DFS	191
Volume Location Database	192
DFS Junctions	192
Move Volume Jobs	192
Split Volume Jobs	192
Original and New Volumes.	193
Prerequisites and Guidelines for DFS	193

Prerequisites for Creating and Using DFS Junctions	193
Guidelines for Creating DFS Junctions Manually	194
Guidelines for Original Volumes and New Volumes	194
Guidelines for Managing Move Volume or Split Volume Jobs	195
Guidelines for Files in Nearline Storage	195
Creating a DFS Management Context for NCP	195
Enabling DFS Junction Support for CIFS Clients	196
Creating a DFS Junction Manually with ConsoleOne	197
Viewing a DFS Junction	197
Deleting a DFS Junction Manually with ConsoleOne.	198
Managing the Volume Location Database Service	198
VLDB Commands	198
VLDB Management Service in ConsoleOne	199
Moving Volumes with iManager	199
Splitting Volumes with iManager	201
Managing Move or Split Jobs.	203
Viewing the Status of Move or Split Jobs	204
Pausing a Move or Split Job	205
Resuming a Move or Split Job	205
Rescheduling a Move or Split Job	206
Viewing Files Skipped by a Move or Split Job	206
Deleting a Move or Split Job	207
Finishing a Move or Split Job	207
15 Monitoring the NSS File System Status	209
Monitoring Status of NSS Devices, Pools, and Volumes with iManager	209
Monitoring Compression and Salvage Statistics	209
Monitoring Quotas and Space Usage for NSS Pools and Volumes	212
Monitoring File System Parameters	214
Monitoring NSS File System Parameters with Novell Remote Manager	214
Monitoring NSS File System Parameters with Novell NetStorage	214
Monitoring Server Status with the Monitor Utility	214
Monitoring Server Status with Novell Remote Manger	215
16 Using NSS Server Console Commands	217
Online Help Commands	217
Status Commands	218
NSS Startup Commands	219
Issuing NSS Startup Commands while NetWare Boots.	219
Making NSS Startup Commands Persist through a Server Reboot.	219
Startup Commands	219
Maintenance Commands	220
System Volume Recovery Commands	221
Volume Compression Commands	222
Volume Purge Delay Commands.	222
Performance Tuning Commands	223
Cache Balancing Commands.	223
Other NSS Commands	224
Commands for Mounting CDs and DVDs as NSS Volumes	226
Commands for CD and DVD Image Files as NSS Volumes	227
DOS FAT Commands	227
Multiple Server Activation Prevention Commands	227
Multipath Connection Failover Commands	228
Pool Snapshot Commands	229
NSS File System Rights Utility	230

17 Configuring the System Cache to Fine-Tune NSS Performance	231
Do I Need to Tune NSS?	231
Adjusting NSS Parameters	231
Important NSS Tuning Guidelines	232
Start with These Parameters.	232
Setting the Cache Balance	232
Setting the Cache Buffers	235
Setting the Closed File Cache Size	237
Setting the File/Buffer Flush Timer	237
Setting the Name Cache	238
18 Troubleshooting NSS	239
Tuning NSS Volumes for GroupWise Servers.	239
Cannot See Volumes and Devices	239
NSS Does Not Recognize a Device	240
Cannot Create an NSS Pool or Volume.	240
Cannot Create an NSS Volume	240
File Compression Is Not Working	240
Software RAID 1 Fails to Recognize a Replacement Device	240
Problems Moving NetWare 6.5 NSS Pools to NetWare 6.0 Servers	241
Problems Following DFS Junctions in Windows 2000/XP Releases	241
19 Managing File System Access to Directories and Files	243
Understanding File Systems.	243
Directory Structures	244
Directory Path	245
Root Directory	245
Fake Root Directory	245
Directory Map Objects	246
Drive Map	247
Planning Your Directory Structure.	248
Organizing Directory Structures Based on Access Requirements.	248
Managing Directory Structures for Network Applications	249
Designing Application Directory Structures	249
Designing Data Directory Structures.	251
Designing Home or User Directory Structures.	251
Configuring and Managing Directories	252
Creating a Directory	252
Viewing Directory and File Information	253
Copying or Moving Directories and Files	254
Creating a Fake Root Directory with the Map Root Command	254
Disabling the Default Use of Map as Map Root in Login Scripts.	254
Creating and Configuring a Directory Map Object	255
Mapping Network Drives.	257
Understanding Access and Usage Control for Directories and Files	259
eDirectory Objects and Security Equivalence	260
File System Trustee Rights	260
The Connection Manager for NetWare	264
Novell Client	265
Understanding Directory and File Attributes for NSS Volumes or NetWare Traditional Volumes	265
Configuring File System Trustees, Trustee Rights, Inherited Rights Filters, and Attributes for Directories and Files.	267
Tools for Managing File System Trustees and Attributes	267
Generating a Server Security Report	268
Viewing a File System Trustee Report for a Volume	269
Managing File System Trustees, Trustee Rights, and Inherited Rights Filters	269
Managing Attributes for Directories and Files	273

Trustee Rights Utility for Linux	276
Trustee Rights Utility for NetWare	278
Attributes Utility for Linux	280
FLAG	282
20 Managing Hard Links	283
Understanding Hard Links	283
Creating a Hard Link	284
Deleting a Hard Link	284
A Upgrading NetWare 5 Volumes to NetWare 6.x NSS Volumes Using Volume Copy Upgrade	285
Copying and Upgrading Legacy Volumes with Volume Copy Upgrade	285
Understanding Volume Copy Upgrade	285
Using VCU from the Command Line	287
Using VCU from a Java Application.	288
After the Volume Copy or Volume Upgrade.	291
Upgrading Legacy NSS Volumes.	291
Upgrading Legacy NSS Volumes in Clusters.	292
B Comparison of NSS and NetWare Traditional File Systems	293
Comparison of Features for NSS and Traditional File Systems	293
SET Parameters Shared by NSS and Traditional File Systems	297
SET Parameters for the NSS File System	298
SET Parameters for the Traditional File System	299
Comparison of Directory and File Attributes	300
C NSS Nomenclature	303
D Documentation Updates	305
May 14, 2005	305
Management Tools for NSS	305
Securing Access to NSS Volumes and Files	306
February 28, 2005	306
What's New	306
Management Tools for NSS	306
Planning for NSS Storage Solutions	307
Managing Devices	307
Managing Software RAID Devices	307
Managing NSS Pool Snapshots	308
Managing NSS Volumes	308
Monitoring the NSS File System Status.	308
Troubleshooting NSS	309
Managing Hard Links	309
Managing File System Access to Directories and Files.	309
Comparison of NSS and NetWare Traditional File Systems	309
August 8, 2004	309
Managing Partitions.	309
Configuring and Managing Directories and Files	309
July 2, 2004.	310
Overview of NSS	310
Management Utilities for NSS.	311
Configuring and Managing NSS Volumes	311
Using NSS Server Console Commands	311
Configuring and Managing Directories and Files	311
May 17, 2004	311
Overview of NSS	312
Management Utilities for NSS.	312

Managing Devices	312
Configuring and Managing NSS Pools.	312
Using NSS Pool Snapshots to Support Data Backup and Restore Services	313
Configuring and Managing NSS Volumes	313
Managing Encrypted NSS Volumes	313
Using Compression to Conserve Storage Space on NSS Volumes.	313
Using Distributed File Services for Moving and Splitting NSS Volumes.	313
Monitoring the Status of the NSS File System.	313
Using NSS Console Commands.	314
Appendix A: Upgrading to NSS Volumes in Clusters	314
Appendix C: Documentation Updates	314

About This Guide

This documentation describes how to use the Novell® Storage Services™ (NSS) File System to configure, activate, and maintain large volumes and numerous files without disrupting the work of users.

This guide is intended for network administrators and is divided into the following sections:

- ◆ [Chapter 1, “Overview of NSS,” on page 17](#)
- ◆ [Chapter 2, “What’s New,” on page 23](#)
- ◆ [Chapter 3, “Management Utilities for NSS,” on page 29](#)
- ◆ [Chapter 4, “Planning for NSS Storage Solutions,” on page 47](#)
- ◆ [Chapter 5, “Managing Devices,” on page 55](#)
- ◆ [Chapter 6, “Managing Partitions,” on page 65](#)
- ◆ [Chapter 7, “Managing Software RAID Devices,” on page 73](#)
- ◆ [Chapter 8, “Managing Multiple Connection Paths to Devices,” on page 95](#)
- ◆ [Chapter 9, “Managing NSS Pools,” on page 101](#)
- ◆ [Chapter 10, “Managing NSS Pool Snapshots,” on page 115](#)
- ◆ [Chapter 11, “Managing NSS Volumes,” on page 127](#)
- ◆ [Chapter 12, “Managing Encrypted NSS Volumes,” on page 171](#)
- ◆ [Chapter 13, “Using Compression to Conserve Storage Space on NSS Volumes,” on page 177](#)
- ◆ [Chapter 14, “Using Distributed File Services for Moving and Splitting NetWare 6.x NSS Volumes,” on page 191](#)
- ◆ [Chapter 15, “Monitoring the NSS File System Status,” on page 209](#)
- ◆ [Chapter 16, “Using NSS Server Console Commands,” on page 217](#)
- ◆ [Chapter 17, “Configuring the System Cache to Fine-Tune NSS Performance,” on page 231](#)
- ◆ [Chapter 18, “Troubleshooting NSS,” on page 239](#)
- ◆ [Chapter 19, “Managing File System Access to Directories and Files,” on page 243](#)
- ◆ [Chapter 20, “Managing Hard Links,” on page 283](#)
- ◆ [Appendix A, “Upgrading NetWare 5 Volumes to NetWare 6.x NSS Volumes Using Volume Copy Upgrade,” on page 285](#)
- ◆ [Appendix B, “Comparison of NSS and NetWare Traditional File Systems,” on page 293](#)
- ◆ [Appendix C, “NSS Nomenclature,” on page 303](#)
- ◆ [Appendix D, “Documentation Updates,” on page 305](#)

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.

User Comments

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment 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 *Novell Storage Services Administration Guide*, see the latest *NetWare* (<http://www.novell.com/documentation/lg/nw65/index.html>) documentation.

Additional Documentation

For documentation on storage media, see the *NetWare 6.5 Server Disks and Storage Devices Administration Guide*.

For documentation on configuring the NetWare Traditional File System, see the *NetWare 6.5 Traditional File System Administration Guide*.

For information about file access protocols, see the *NetWare 6.5 Native File Access Protocols Guide*.

Novell Archive and Version Services captures interval-based versions of files on specified volumes and manages access to file versions to allow users to restore lost, modified, or deleted files from an archive database of file versions. For information, see the *Novell Archive and Version Services 2.0 Administration Guide for NetWare 6.5* and the *Novell Archive and Version Services 2.0 User Guide for NetWare 6.5*.

For documentation on iManager 2.0, see the *Novell iManager 2.0.x Administration Guide*.

For documentation on iManager 2.5, see the *Novell iManager 2.5 Administration Guide*.

1

Overview of NSS

The Novell® Storage Services™ (NSS) File System is the default file system for NetWare® 6 and later. Its many features and capabilities include visibility, a trustee access control model, multiple simultaneous namespace support, native Unicode*, user and directory quotas, rich file attributes, multiple data stream support, event file lists, and a file salvage sub-system. These features can help you effectively manage your shared file storage for any size of organization, scaling management of the system for even the largest of organizations with hundreds of thousands of employees.

This section discusses the following:

- ◆ “[Benefits of NSS](#)” on page 17
- ◆ “[Understanding NSS](#)” on page 18
- ◆ “[NSS Features](#)” on page 19
- ◆ “[What’s Next](#)” on page 22

Benefits of NSS

Files are at the heart of every company, large or small. Whether your network spans continents or a few cubicles, your files become the foundation of your business. No one can afford unreliable file service, especially when the files you manage are continually growing and requiring more and more storage space.

Businesses today demand more storage space and faster and easier access to data. To meet the demands, you need a file system that can scale to a growing business, is easily maintained, and is better protected against corruption. NSS provides a variety of features that can be combined to provide a robust and reliable solution for your business.

NSS provides the following benefits:

- ◆ A journaling file system that lets you create bigger volumes that activate (mount) quicker, store more data, and better resist corruption
- ◆ An unlimited number of NSS volumes per NetWare partition
- ◆ Software RAID 0 (striping), 1 (mirroring), 5 (striping with parity), 10 (mirroring RAID 0 devices), and 15 (mirroring RAID 5 devices)
- ◆ Multiple server activation prevention (MSAP) to help protect pools from being concurrently activated by multiple servers that do not share a cluster relationship
- ◆ An NSS volume in a pool of storage that spans multiple storage devices
- ◆ Up to trillions of files in a single directory
- ◆ Faster access to data, regardless of file size or volume size
- ◆ Lower memory requirements: 1 MB of RAM can activate an NSS volume

- ◆ Directory space restrictions
- ◆ User space restrictions
- ◆ Salvage support for deleted volumes and files
- ◆ Multiple I/O path support
- ◆ Pool snapshots that capture point-in-time versions of files in the pool
- ◆ Encrypted volume support to meet the legal standard of making data inaccessible to software that circumvents normal access control, such as if the media were stolen
- ◆ Transaction Tracking System™ (TTS™)
- ◆ CDs and DVDs automatically activated as NSS volumes
- ◆ CD and DVD image files activated as NSS volumes
- ◆ Novell Distributed File Services that allow you to move and split volumes to better manage storage growth
- ◆ Novell Archive and Version Services that allow you to archive interval-based versions of user files and make them available to users for individual retrieval. For information, see the *Novell Archive and Version Services 2.0 Administration Guide for NetWare 6.5*.

Understanding NSS

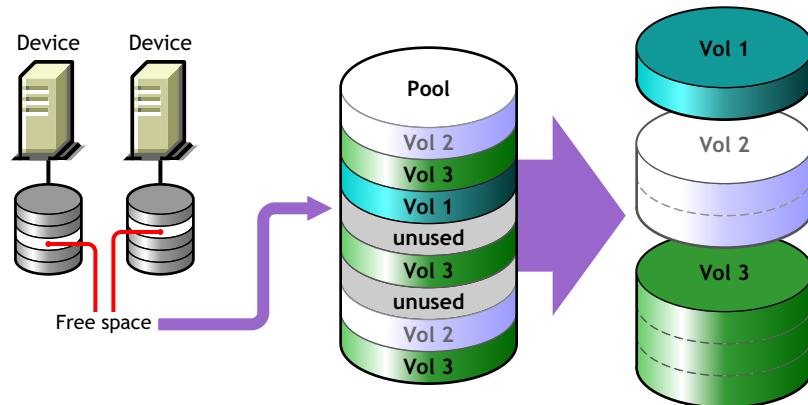
NSS is a 64-bit file system that can manage a virtually unlimited number of file objects. On each physical storage device, NSS abstracts up to four physical NetWare partitions to make them appear as contiguous free space. NSS recognizes physical and logical devices up to 2 TB in size from which you can create any number of virtual storage resources, called pools. You can choose space from at least four devices of up to 2 TB each to create a pool with a maximum pool size of 8 TB. A pool can contain an unlimited number of volumes. If the pool spans devices, the volumes automatically span the devices. A single volume can contain up to 8 trillion files and grow to 8 TB in size, depending on the size of the pool and space consumed by other volumes in the pool.

Storage Pools

During the NetWare installation, NSS automatically creates a system pool (sys) and an NSS volume (sys:) that can grow to the size of the pool. We recommend that you reserve the system pool and volume for operating system software and extensions. Create additional pools to effectively store applications, files, and databases.

You create additional storage pools by assigning areas of free space obtained from one or more of a server's storage devices. You can create one or more NSS volumes from the space in the storage pool. [Figure 1 on page 19](#) shows how NSS uses free space on multiple devices to create a storage pool.

Figure 1 NSS Pool Architecture



NSS Volumes

The logical volumes you create on NSS storage pools are called NSS volumes. You can specify a maximum storage quota for the volume, or allow the volume to grow dynamically to the size of its pool. You can add any number of volumes to a storage pool.

Because there is no limit to the number of volumes you can create, it is possible that the combined size of all the volumes taken together is larger than the storage pool itself. NSS refers to this process as “overbooking.” If you overbook space in the pool, the individual administrative size of a volume cannot exceed the size of the storage pool.

NSS allocates space from the pools to the volumes only as needed. Typically, user consumption of a volume’s available space ebbs and flows; it is quite unlikely that users concurrently consume volumes at 100% of their available capacity. Each volume consumes the space it needs as it needs it. By overbooking space, NSS provides a flexible and cost effective way to accommodate expanding storage needs.

For example, suppose you have a 300 GB storage pool. From this storage pool, you create two NSS volumes of 200 GB. You can define two 200 GB NSS volumes out of a storage pool of only 300 GB, if you feel comfortable that the NSS volumes will not both exceed 75 percent capacity (150 GB) and therefore, exceed the overall size of the storage pool. If one NSS volume does reach 150 GB, but the other volume stays under 100 GB, your overbooking plan worked.

Suppose you expect one of the volumes might exceed its share of the pool. You can overbook the pool by creating one NSS volume with a quota of 200 GB and a second NSS volume that can grow to the size of the pool. As the combined size nears the size of the pool, you can extend the size of the pool to allow more space for the larger, expanding volume. Your overbooking plan works because you built in the opportunity to expand the pool and volume, according to your business needs.

NSS Features

NSS helps improve the scalability, flexibility, and availability of your storage devices. This section describes specific NSS features that will help you do the following:

- ◆ “Use Less Memory and Gain More Speed” on page 20
- ◆ “Improve Storage Availability” on page 20

- ◆ “[Prevent Unauthorized Access](#)” on page 20
- ◆ “[Protect Data from Corruption or Loss](#)” on page 21
- ◆ “[Maximize Available Space](#)” on page 22

Use Less Memory and Gain More Speed

NSS requires only about 1 MB of server memory to activate a volume, independent of the number of files it contains. With NSS, you can activate up to 256 NSS volumes concurrently per server, up to the available server memory.

Whenever you activate an NSS volume, it takes only seconds to mount a volume instead of minutes. NSS uses a journaling file system and does not need to scan the entire file system to create a directory entry table (DET) to load the volume. NSS loads a file’s metadata into the memory *only* when you access the file.

NSS reads the file system journal only if server goes down abnormally. Instead of slowly searching the volume for errors, NSS reads the journal to identify any incomplete transactions. It either completes the transaction or backs it out. This results in less server down time and is beneficial for applications such as mail services.

Improve Storage Availability

NSS provides three key features to improve I/O performance and provide fault tolerant access to your data:

- ◆ Multiple I/O paths support for adapters

Use multiple channels to connect the server to local media or a storage area network. For information, see “[Managing Multiple Connection Paths to Devices](#)” on page 95.

- ◆ Software RAIDs 0, 1, 5, 10, and 15

Use software RAID devices to improve performance and availability. For information, see “[Managing Software RAID Devices](#)” on page 73.

- ◆ Shared-disk cluster storage

Make devices shareable for use in a cluster. For information, see “[Sharing Devices](#)” on page 60.

- ◆ Multiple name space support

NSS provides full support for DOS, Windows*, UNIX, and Macintosh* file naming simultaneously.

- ◆ Rich file metadata support

NSS provides full support for all file attributes and multiple data streams for DOS, Windows, UNIX, and Macintosh simultaneously.

Prevent Unauthorized Access

NSS includes the following features to help prevent access to data that circumvents normal access control:

- ◆ Encrypted Volume Support

Encrypt data volumes, meeting U.S. Government security standards. For information, see “[Managing Encrypted NSS Volumes](#)” on page 171.

- ◆ Data shredding (up to 7 times) for deleted files

Erase files completely, meeting U.S. Government security standards. For information, see “[Using Data Shredding to Prevent Access to Deleted Files](#)” on page 146.

- ◆ Multiple server access prevention for pools

Multiple Server Access Prevention ensures data integrity by preventing unauthorized access to shared media in a storage area network. For information, see “[Preventing Pools from Activating on Multiple Servers](#)” on page 113.

- ◆ Trustee model for access control on NSS volumes

NSS uses the Novell Trustee Model to greatly simplify access control management in the file system. It restricts visibility of data structures so that users only see subdirectories they have rights to see, not the whole tree like all other file systems.

For information about the Novell Trustee Model and NSS file system rights, see “[Security: Granting Trustee Rights to Directories and Files](#)” in the *NetWare 6.5 Traditional File System Administration Guide*.

Protect Data from Corruption or Loss

NSS includes the following features to help ensure that the most current copy of your data is recoverable:

- ◆ [Pool snapshots to provide point-in-time views of data](#)

- ◆ [Immediate data saves](#)

- ◆ [Transaction Tracking System \(TTS\)](#) to roll back uncompleted transactions

- ◆ Pool snapshots to provide point-in-time views of data

Back up files from snapshots of data so that all files, including open ones, can be backed up. For information, see “[Managing NSS Pool Snapshots](#)” on page 115.

- ◆ Immediate data saves

On file closure, write data from memory to the file immediately instead of waiting for the next scheduled write to disk. For information, see “[Using the Flush Files Immediately Attribute to Protect Against Possible Data Corruption on System Failure](#)” on page 148.

- ◆ Transaction tracking support for user applications

Monitor application transactions and roll back uncompleted application transactions after a system failure. For information, see “[Using the Transaction Tracking System for Application-Based Transaction Rollback](#)” on page 150.

- ◆ File-level snapshots to allow backup of files that are not open exclusively

Back up files from snapshots of data so that all files, including open ones, can be backed up. For information, see “[Using the File-Level Snapshot Attribute to Enable the Backup of Open Files](#)” on page 151.

- ◆ Salvage file subsystem

Recover files that were deleted by applications or from the terminal/console commands. For information, see “[Salvaging or Purging Deleted Files](#)” on page 159.

Maximize Available Space

NSS includes the following features to help you maximize your available space:

- ◆ File compression

Compress inactive files, according to preset parameters, to conserve space in a volume. For information, see “[Using Compression to Conserve Storage Space on NSS Volumes](#)” on page 177.

- ◆ Volume space restrictions

Limit the amount of space a volume can consume in its pool. For information, see “[Managing NSS Volume Quotas](#)” on page 161.

- ◆ Directory space restrictions

Limit the amount of space a subdirectory can consume, regardless of broader volume and user constraints. For information, see “[Managing Directory Quotas](#)” on page 163.

- ◆ User space restrictions

Limit the amount of space a user’s data can consume, regardless of broader directory or volume constraints. For information, see “[Managing User Space Quotas](#)” on page 166.

What’s Next

See “[What’s New](#)” on page 23 to learn about new and modified features in this release of NSS.

Review the following sections before designing and implementing your storage solution:

- ◆ “[Management Utilities for NSS](#)” on page 29
- ◆ “[Planning for NSS Storage Solutions](#)” on page 47

Use the following table to determine where to go next.

To Manage:	Go Here:
Storage devices	Managing Devices
Software RAID devices	Managing Software RAID Devices
Multiple I/O paths between the server and storage media	Managing Multiple Connection Paths to Devices
Pools	Managing NSS Pools
Pool snapshots	Managing NSS Pool Snapshots
Volumes	Managing NSS Volumes
Encrypted volumes	Managing Encrypted NSS Volumes
Volume compression	Using Compression to Conserve Storage Space on NSS Volumes
Distributed file services	Using Distributed File Services for Moving and Splitting NetWare 6.x NSS Volumes

2

What's New

This section discusses additions and modifications to the Novell® Storage Services™ File System.

- ◆ “What’s New for NetWare 6.5” on page 23
- ◆ “What’s Changed for NetWare 6.5” on page 24
- ◆ “What’s New for NetWare 6.5 Support Pack 2” on page 26
- ◆ “What’s New for NetWare 6.5 Support Pack 3” on page 27

What’s New for NetWare 6.5

The following features have been added or improved for NetWare 6.5 as compared to NetWare 6.0:

- ◆ “Pool Snapshot” on page 23
- ◆ “Software RAID 1 (Mirroring)” on page 23
- ◆ “Software RAID 0 and 5” on page 24
- ◆ “Distributed File Services for Moving or Splitting Volumes” on page 24
- ◆ “NSS Management Utility” on page 24
- ◆ “NSS Sys: Volume Recovery Commands” on page 24

Pool Snapshot

A pool snapshot is another way to keep a consistent copy of your data for backup purposes. A snapshot captures a point-in-time metadata copy of a specified pool. You can back up snapshots more frequently than the entire volume. For information, see “[Managing NSS Pool Snapshots](#)” on page 115.

Software RAID 1 (Mirroring)

Software RAID 1 is a technique for mirroring data on two to four storage devices. In NetWare 6.5, NSS requires lower amounts of memory to mirror large partitions. RAID 1 now uses the same amount of memory to mirror partitions, regardless of its size.

In the event of a server failure, you no longer need to remirror all the partitions because RAID 1 automatically tracks and remirrors any blocks that were in the process of being written to when the server crashed. Also, if the server crashes during a mirroring process, when the server comes back up, the mirroring process resumes where it left off.

Additional RAID 1 benefits:

- ♦ Multiprocessor enabled
- ♦ Re-mirrors only those partitions that are out of sync
- ♦ Mirrors partitions that had no previous mirror

Create software RAID devices using the Web-based iManager utility or the console-based NSS Management Utility (NSSMU). For more information, see [“Managing Software RAID Devices” on page 73](#).

Software RAIDs 0 and 5

NetWare 6.5 supports two data striping techniques for software RAIDs: RAID 0 and RAID 5. Both striping methods improve disk I/O. RAID 5 also maintains parity information for disk fault tolerance. RAID 0 provides slightly faster I/O performance than RAID 5 because it does not have the overhead of the parity maintenance.

Software RAID 5 improves I/O speeds and data protection by striping data to multiple partitions and interleaving parity. Parity information makes it possible to reconstruct lost data if a single member device is lost. The parity partition can reconstruct only one lost partition at a time.

For more information, see [“Managing Software RAID Devices” on page 73](#).

Distributed File Services for Moving or Splitting Volumes

In NetWare 6.5, Distributed File Services (DFS) allows you to move NetWare 6.x volumes and split NetWare 6.x NSS volumes to a destination NetWare 6.x NSS volume. The ability to efficiently reorganize storage makes it easier to get rid of old hardware or free up disk space. For information, see [“Using Distributed File Services for Moving and Splitting NetWare 6.x NSS Volumes” on page 191](#).

NSS Management Utility

The NSS Management Utility (nssmu.nlm) is loaded from the command line of the server console and gives you limited creation and management of the following NSS components: devices (including software RAIDs and iSCSI), partitions, pools, and volumes. This utility is not meant to replace iManager or any other Web-based management utility. However, this utility is the only management tool that can access your server if you accidentally delete or rename the sys: volume.

For information, see [“NSSMU” on page 41](#).

NSS Sys: Volume Recovery Commands

New NSS sys: recovery commands give you additional control over your sys: volume.

For more information, see [“System Volume Recovery Commands” on page 221](#).

What's Changed for NetWare 6.5

The following NSS features behave differently as compared to NSS in NetWare 6.0:

- ♦ [“CD, DVD, and Macintosh CD Device Support” on page 25](#)
- ♦ [“Volume Copy Upgrade” on page 25](#)

- ◆ “Name Caching” on page 26
- ◆ “Mirroring Partitions and Hot Fix” on page 26
- ◆ “CIFS and AFP Protocols” on page 26
- ◆ “Admin Volume” on page 26

CD, DVD, and Macintosh CD Device Support

The new cddvd.nss module replaces cdrom.nlm and cd9660.nss for CD support, udf.nss for DVD support, and cdhfs.nss for Macintosh* CD support. When you load cddvd.nss, it uses the same set of switches (UpdateCDToNDS, LoginUpdateToNDS, LeaveCDInNDS, and LockCDMediaIn) that were used in the previous commands.

Cddvd.nss loads format in the order of DVD, CD, and HFS. It provides the LoadISOVolumeFirst switch to allow CDs to be loaded first.

For more information, see “Activating and Deactivating CDs and DVDs as NSS Volumes” on [page 137](#).

Volume Copy Upgrade

The Volume Copy Upgrade utility allows you to convert NetWare 5.1 NSS or Traditional volumes to NSS volumes for use with NetWare 6.5. The following changes have been made to Volume Copy Upgrade (vcu.nlm):

- ◆ A new file, called irf.out (Inherited Rights Filter), is now created by vcu.nlm. This file contains information about whether the Inherited Rights Filters were moved correctly during a volume copy or restore. Mismatches will be preceded by three asterisks (***).

The irf.out file is stored in the same location as errors.out (at the root directory of the destination volume).

- ◆ You can now use vcu.nlm to copy and restore NSS volumes.

With previous versions, you could use vcu.nlm to copy only Traditional volumes to NSS volumes.

- ◆ You can now run vcu.nlm from a Windows* client.
- ◆ The optional input of dsContainer, dsPoolName, and dsVolName has been deleted.
- ◆ The /i switch has been deleted.

For a listing of available switches and their functionality: At the server console, enter

vcu /h

- ◆ The /m switch has been added.

This switch lets users rename a volume’s default eDirectory™ object.

For more information on how to use vcu.nlm to copy volume data from Traditional or NSS volumes to NSS pools, see [Appendix A, “Upgrading NetWare 5 Volumes to NetWare 6.x NSS Volumes Using Volume Copy Upgrade,” on page 285](#).

Name Caching

The /NSS NameCachSize= command is no longer a startup command; it can be modified at any time. You can now specify the maximum number of entries the system can use in the cache. Additionally, the size of the cache has now been automated; the cache automatically resizes itself during set intervals based on the file system usage.

Mirroring Partitions and Hot Fix

Hot Fix™ is not supported in NetWare 6.5 and later because the function is provided in modern hardware at the device level. You no longer need to specify a Hot Fix space in order to create a software RAID 1 device.

CIFS and AFP Protocols

In NetWare 6.5, the CIFS and AFP protocols are installed by default when you install your NetWare 6.5 server. Additionally, these protocols can access only NSS pools and volumes. For information, see the *NetWare 6.5 Native File Access Protocols Guide*

Admin Volume

A new file called files.cmd was added to the Admin volume (_admin:\manage_nss\files\files.cmd). Applications like NetStorage and other end-user browser-based tools use this file to communicate with the file server. The files.cmd file is a virtual file and generates dynamic information that lets users see and modify their files through a browser.

Every user on the file server has access to this file and thus inherits the following default rights: Read, Write, and Scan. This also means that the Admin volume is now visible to end users. In previous versions of NetWare, this was not the case. End users cannot delete this file nor modify its properties.

If you want to restrict access to this file or the Admin volume, you must do so by modifying a configuration file called trustees.xml. For more information, see “[Assigning Volume Rights with Trustees.xml \(NetWare\)](#)” on page 143.

For more information on virtual files, see the [Virtual File Services for NetWare \(http://developer.novell.com/ndk/doc/vfs/index.html?page=/ndk/doc/vfs/vfs_enu/data/h5ubo7tt.html\)](http://developer.novell.com/ndk/doc/vfs/index.html?page=/ndk/doc/vfs/vfs_enu/data/h5ubo7tt.html) in the NDK documentation.

What's New for NetWare 6.5 Support Pack 2

The following features have been added for NetWare 6.5 Support Pack 2:

- ♦ “[Encrypted Volume Support](#)” on page 26
- ♦ “[Multiple Device Selection in NSSMU](#)” on page 27
- ♦ “[CD and DVD Image Files as NSS Volumes](#)” on page 27

Encrypted Volume Support

Encrypted NSS volumes meet the legal standard of making data inaccessible to software that circumvents normal access control, such as if the media were stolen. NetWare 6.5 Support Pack 2

provides optional Encrypted Volume Support (EVS) for newly created NSS volumes. You cannot encrypt the sys: volume. For information, see “[Managing Encrypted NSS Volumes](#)” on page 171.

Multiple Device Selection in NSSMU

In NetWare 6.5 Support Pack 2, NSSMU allows you to select one or more devices for Initialize or Share actions. For information, see “[NSSMU](#)” on page 41.

CD and DVD Image Files as NSS Volumes

In NetWare 6.5 Support Pack 2, the cddvd.nss module allows you to activate CD and DVD image files as NSS volumes. For information, see “[Activating and Deactivating CD and DVD Image Files as NSS Volumes](#)” on page 138.

What’s New for NetWare 6.5 Support Pack 3

The following features and capabilities have been added for NetWare 6.5 Support Pack 3:

- ◆ “[Storage Plug-in for Novell iManager 2.5](#)” on page 27
- ◆ “[Partition Information](#)” on page 27
- ◆ “[Deleting Pool Snapshots](#)” on page 27

Storage Plug-in for Novell iManager 2.5

The Storage plug-in was updated for compatibility with Novell iManager 2.5. For information, see “[Novell iManager Storage Plug-In](#)” on page 29.

Partition Information

You can now view details about partitions on the Partitions Management page in iManager. For information, see “[Managing Partitions](#)” on page 65.

Deleting Pool Snapshots

The rules and process for deleting pool snapshots has changed. When a snapshot is deleted, Media Manager automatically zeroes out all the blocks that it used. It no longer turns on shredding for the internal volume when creating a snapshot. For information, see “[Deleting a Pool Snapshot](#)” on page 125.

3

Management Utilities for NSS

This section discusses various tools for managing your Novell® Storage Services™ storage solution:

- ◆ “Novell iManager Storage Plug-In” on page 29
- ◆ “NSSMU” on page 41
- ◆ “NSS Command Line Management” on page 43
- ◆ “Novell NetStorage” on page 43
- ◆ “Novell Remote Manager” on page 44
- ◆ “Novell Client for Windows 2000/XP” on page 45
- ◆ “Trustee Rights Utility” on page 45
- ◆ “ConsoleOne” on page 45
- ◆ “Virtual File Services and Scripts” on page 46

NOTE: Legacy NetWare® tools, such as NWADMIN and NWCONFIG, might not be compatible with some of the NSS features.

NSS also supports third-party tools on both kernels for advanced data protection and management, virus scanning, and traditional archive and backup solutions.

Novell iManager Storage Plug-In

Novell iManager is a Web browser-based tool used for configuring, managing, and administering Novell eDirectory™ objects on your network. For NetWare 6.5 and later, the iManager Storage plug-in is the primary tool used to manage NSS.

Novell iManager gives you the ability to assign specific tasks or responsibilities to user accounts and to present the user with only the tools (with the accompanying rights) necessary to perform those sets of tasks. For more information, see the *Novell iManager 2.5 Administration Guide*.

This section discusses the following:

- ◆ “Prerequisites for Using the Storage, Archive Versioning, CIFS, and Clustering iManager Plug-Ins” on page 30
- ◆ “Downloading and Installing Plug-In Updates” on page 31
- ◆ “Accessing Novell iManager” on page 34
- ◆ “Accessing NSS Storage Management Role and Tasks” on page 34
- ◆ “Selecting a Server to Manage” on page 35
- ◆ “Understanding iManager Storage Management Tasks” on page 36

Prerequisites for Using the Storage, Archive Versioning, CIFS, and Clustering iManager Plug-Ins

The requirements in this section apply to the following storage-related plug-ins for iManager:

- ◆ Storage plug-in
- ◆ Archive Versioning plug-in
- ◆ CIFS plug-in
- ◆ Clustering plug-in

Web Browser Language Setting

The iManager plug-in might not operate properly if the highest priority Language setting for your Web browser is set to a language other than one of the supported languages. To avoid problems, in your Web browser, click Tools > Options > Languages, and then set the first language preference in the list to a supported language.

Protocols

The following table provides information about the protocols needed to use iManager to manage storage in a heterogenous environment with NetWare 6.5 servers and Novell Open Enterprise Server (OES) servers for NetWare and Linux platforms. A protocol annotated with an asterisk is the default and is configured automatically on the servers. The protocols you use must be loaded and running on both the iManager server and the target server you want to manage.

iManager Server		Target Server		
		OES Linux	OES NetWare	NetWare 6.5 SP3
OES Linux	* WBEM	* WBEM	WBEM (Start WBEM.)	
	CIFS	CIFS	CIFS	CIFS (Field Patch 2B)
OES NetWare	* WBEM	* WBEM	WBEM (Start WBEM.)	
		NCP	* NCP	* NCP
NetWare 6.5 SP3	* WBEM	* WBEM	WBEM (Start WBEM.)	
		NCP	* NCP	* NCP
NetWare 6.5 SP2	CIFS	CIFS	CIFS	CIFS (Field Patch 2B)
	Not available	* NCP	* NCP	* NCP

WBEM

Where WBEM is the default protocol, WBEM is loaded and runs automatically when you start the server. Otherwise, you must start WBEM to use the protocol.

To start WBEM: At the server console, enter

openwbem

If you receive file protocol errors, it might be because WBEM is not running.

For information about installing WBEM, see “Setting Up OpenWBEM” (<http://www.novell.com/documentation/oes/cimom/data/bv3wjre.html>) in the *OpenWBEM Services Administration Guide for OES* (<http://www.novell.com/documentation/oes/cimom/data/front.html>).

CIFS

Where it is available, CIFS must be configured before you can use it. An additional CIFS setup requirement for Field Patch 2B is noted where it is required. For information, see the *NetWare 6.5 Native File Access Protocols Guide*.

NCP

NCP™ is the default protocol when the iManager server and target server is NetWare 6.5 SP3 or SP2.

Downloading and Installing Plug-In Updates

This section contains the instructions for downloading and installing updates to the Storage plug-in for iManager 2.x. However, it can be generalized and applied to updates for the following:

- ♦ **NSS (nssmgmt.npm):** Contains the Storage plug-in for managing NSS on NetWare 6.5 Support Pack 3, OES NetWare, and OES Linux.

This file also contains the CIFS plug-in, which is used to manage CIFS services for end users of data stored on your NetWare 6.0 and later servers. For information about CIFS, see the *NetWare 6.5 Native File Access Protocols Guide*.

- ♦ **Archive Versioning (arkmgmt.npm):** Contains the Archive Versioning plug-in for managing Novell Archive and Version Services for NetWare 6.5 and OES NetWare.

For information, see *Novell Archive and Version Services 2.0 Administration Guide for NetWare 6.5*.

- ♦ **Cluster Services (ncsmgmt.npm):** Contains the Clustering plug-in for managing Novell Cluster Services™.

For information, see the *Novell Cluster Services 1.7 Administration Guide*.

Downloading the Plug-In

- 1 Click the Download button, log in, and review the download agreement.

If you haven't registered yet, you can register for free.

- 2 On the system where Novell iManager is installed, download the NPM file.

NOTE: When downloading this iManager plug-in, the browser might rename the downloaded file by adding a .zip extension (i.e. pluginname.npm.zip). If this occurs, you can either install the .zip file in iManager or you can rename the file and install it. Any plug-in with the additional .zip extension can still be installed with iManager without any additional steps.

- 3 You can leave the NPM in the downloaded location, or move it to the iManager packages location.

Installing the Plug-In for iManager 2.5 When RBS Is Not Configured

If you do not have Role-based Services (RBS) configured for Novell eDirectory™, install the NPM file as follows:

- 1 Download the NPM update file.

For information, see “[Downloading the Plug-In](#)” on page 31.

- 2 In a Web browser, log in to iManager on the system where you downloaded the file.
- 3 Click the Configure icon (person seated behind a desk).
- 4 Under Module Installation, click Available Novell Plug-In Modules.
- 5 If the Storage and CIFS plug-ins (nssmgmt.npm file) do not appear in the list, click New, browse to select the nssmgmt.npm file, then click OK.

You are returned to the Available Novell Plug-in Modules page.

- 6 Select the Storage and CIFS plug-ins (nssmgmt.npm file) from the list of available modules, then click Install.

This install takes a few minutes. You should receive a message confirming a successful install.

- 7 Click OK to dismiss the message, then close iManager.
- 8 Restart Tomcat4, using one of the following methods:

Platform	Restart Command
NetWare 6.5 or later	<p>Enter</p> <p>TC4STOP</p> <p>Wait at least one minute, then enter</p> <p>TOMCAT4</p>
OES Linux	<p>Enter</p> <p>/etc/init.d/novell-tomcat4 stop</p> <p>Wait at least one minute, then enter</p> <p>/etc/init.d/novell-tomcat4 start</p>
Windows*	Stop and start the Tomcat service.
Solaris*	<p>Enter</p> <p>/etc/init.d/imgr stop</p> <p>Wait at least one minute, then enter</p> <p>/etc/init.d/imgr start</p>
HP*-UX*	<p>Enter</p> <p>/opt/hpws/tomcat/bin/shutdown.sh</p> <p>Wait at least one minute, then enter</p> <p>/opt/hpws/tomcat/bin/startup.sh</p>

- 9 Tomcat sometimes requires several minutes to fully initialize. Wait at least 5 minutes before trying to log into iManager.

For more information, see “[Downloading and Installing an NPM](#)” in the *Novell iManager 2.5 Installation Guide*.

Installing a Plug-In When RBS Is Configured

If you are running iManager in Assigned Mode and have RBS configured for eDirectory, complete the following steps to install the NPM file.

IMPORTANT: To re-install an existing plug-in, you must first delete the rbsModule object for that plug-in from eDirectory, using the Module Configuration > Delete RBS Module task.

- 1 Download the NPM update file.

For information, see [“Downloading the Plug-In” on page 31](#).

- 2 In a Web browser, log in to iManager as an RBS Collection Owner on the system where you downloaded the NPM file.

- 3 Click the Configure icon (person seated behind a desk).

- 4 Under Module Installation, click Available Novell Plug-In Modules.

- 5 If the Storage and CIFS plug-ins (nssmgmt.npm file) do not appear in the list, click New, browse to select the nssmgmt.npm file, then click OK.

You are returned to the Available Novell Plug-in Modules page.

- 6 Select the Storage and CIFS plug-ins (nssmgmt.npm file) from the list of available modules, then click Install.

This install takes a few minutes. You should receive a message confirming a successful install.

- 7 Click OK to dismiss the message, then close iManager.

- 8 Restart Tomcat4, using one of the following methods:

Platform	Restart Command
NetWare 6.5 or later	Enter TC4STOP Wait at least one minute, then enter TOMCAT4
OES Linux	Enter /etc/init.d/novell-tomcat4 stop Wait at least one minute, then enter /etc/init.d/novell-tomcat4 start
Windows*	Stop and start the Tomcat service.
Solaris*	Enter /etc/init.d/imgt stop Wait at least one minute, then enter /etc/init.d/imgt start

Platform	Restart Command
HP*-UX*	<p>Enter</p> <pre>/opt/hpws/tomcat/bin/shutdown.sh</pre> <p>Wait at least one minute, then enter</p> <pre>/opt/hpws/tomcat/bin/startup.sh</pre>

- 9 Tomcat sometimes requires several minutes to fully initialize. Wait at least 5 minutes before trying to log into iManager.
- 10 After Tomcat initializes, in a Web browser, log in to iManager as a Collection Owner again.
- 11 Click the Configure icon.
- 12 Under Role-Based Services, select RBS Configuration.

The table on the 2.x Collections tabbed page displays modules ready to update.
- 13 Locate the collection where you want to install the plug-in, then click its Out-of-Date number.

The Storage and CIFS plug-ins (nssmgmt.npm) should be displayed under Modules Not Yet Installed column.
- 14 Select the plug-ins.
- 15 Click Update.
- 16 Wait for the Completed message, then click OK to continue.

The Storage role and CIFS role should appear on the Roles and Tasks pane.

Accessing Novell iManager

- 1 Launch a Web browser.
- 2 Click File > Open, then enter

`http://server-IP-address/nps/iManager.html`

Replace *server-IP-address* with the actual server DNS name or IP address. For example:

`http://192.168.1.1/nps/iManager.html`

The iManager Login page opens.

- 3 Log in, using your administrator username and password, to the eDirectory tree that contains the server you want to manage.

In Novell iManager, you can access only the roles and tasks you are authorized to manage. For full access to all available Novell iManager features, you must log in as Supervisor of the tree.

Accessing NSS Storage Management Role and Tasks

- 1 Access iManager, then log in to the eDirectory tree where the server you want to manage resides.

For information, see “[Accessing Novell iManager](#)” on page 34.
- 2 In Roles and Tasks, click Storage.

Figure 2 The iManager NSS Storage Management Role and Tasks



The Storage role expands to reveal its main tasks and opens the main page to the Devices task.

As you work in the Storage plug-in, use the navigation links at the top of the page, referred to as “breadcrumbs,” to return to pages you recently visited, or use the links in Roles and Tasks. If you use the Refresh and Back features of your Web browser to navigate, iManager returns you to the initial page you encountered after login.

- 3 To activate the options on the selected page, select a server to manage.

For information, see “[Selecting a Server to Manage](#)” on page 35.

- 4 Continue with Device management, or click one of the other tasks to access its associated management options:

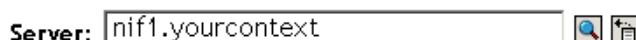
- ◆ Pools
- ◆ Volumes
- ◆ Volume Job Control
- ◆ Partitions
- ◆ Software RAIDS
- ◆ Devices
- ◆ Scan for Devices

For information about Storage tasks, see “[Understanding iManager Storage Management Tasks](#)” on page 36.

Selecting a Server to Manage

Before you can access the management options on a selected Storage task page, you must select a server to manage that is in the same Novell eDirectory tree where you are currently logged in.

Figure 3 The Server Selection Field



Use one of the following methods to select a server in the tree you are logged in to:

- ◆ Type the eDirectory distinguished server name for the server you want to manage, then click Apply. For example: svr1.novell.
- ◆ Click the Search icon to open the eDirectory Object Selector. Browse or search the list to locate the server you want to manage, then click the server name.
- ◆ Click the Object History icon to select a server you have recently managed.

Wait for iManager to retrieve information about that server and display the appropriate information to the task page you are in.

Understanding iManager Storage Management Tasks

The NSS file storage and management system provides an easy, reliable, and secure way to organize, consolidate, and manage data for your enterprise. To organize storage in ways that make sense to users, you can create virtual devices, storage pools, and volumes that abstract the physical storage devices in a mixed-media environment.

Use the Novell iManager Storage plug-in to manage the NSS file system for your server. In iManager, the Storage Management role comprises six key tasks:

- ◆ “Pools” on page 36
- ◆ “Volumes” on page 37
- ◆ “Volume Job Control” on page 38
- ◆ “Partitions” on page 38
- ◆ “Software RAIDs” on page 39
- ◆ “Devices” on page 40
- ◆ “Scan for Devices” on page 40

Pools

You can create and manage storage pools to efficiently use all free space. Enable the pool snapshot feature to preserve point-in-time views of data pools and to support data recovery and backup.

Use the following table to find information about subtasks available from the Pools task.

Subtask	Description	Reference
Pools	A list of all pools on the selected server.	Viewing Pools on a Server
Details	View information about a selected pool.	Viewing Pool Details
New	Create a new pool on the selected server.	Creating Pools with iManager
Delete	Delete a selected pool and all of its volumes and their data.	Deleting a Pool
Rename	Rename a selected pool.	Renaming a Pool
Activate	Mount and activate a selected deactive or unmounted pool.	Activating and Deactivating Pools
Deactivate	Deactivate a selected active pool.	Activating and Deactivating Pools
Increase Size	Add more partitions from available devices to expand the size of a pool.	Increasing the Size of a Pool
Snapshot	Opens the Pool Snapshot Management page where you can create and manage pool snapshots.	Managing NSS Pool Snapshots

Subtask	Description	Reference
Update eDirectory	If a storage object is not recognized automatically, update eDirectory objects to force recognition.	Updating eDirectory Pool Objects
Deleted Volume	View and salvage deleted volumes in a pool.	Viewing and Salvaging Deleted NSS Volumes in a Pool
Offline	For a pool snapshot that is online as an active pool, take it offline. This does not delete the pool snapshot.	Moving an Active Pool Snapshot Offline
Partitions	View a list of the partitions comprising the pool's storage space.	Viewing Partition Information for a Pool
Volumes	View a list of all volumes on a selected pool.	Viewing Volume Information for a Pool
Devices	View a list of the devices that contribute space to a selected pool.	Viewing Device Information for a Pool

Volumes

You can create and manage NSS volumes, including their key attributes.

Use the following table to find information about subtasks available from the Volumes task.

Subtask	Description	Reference
Volumes	View a list of volumes on the selected server.	Managing NSS Volumes
Details	View information about a selected volume.	Viewing the Details of a Volume
New	Create a new nonencrypted volume.	Configuring Nonencrypted NSS Volumes with iManager
Delete	Delete a selected volume and all of its contents.	Deleting an NSS Volume
Rename	Rename a selected volume.	Renaming an NSS Volume
Activate	Mount and activate a deactive or unmounted volume.	Activating and Deactivating an NSS Volume
Deactivate	Deactivate an active volume.	Activating and Deactivating an NSS Volume
Mount	Mount an unmounted volume. (A volume must be mounted to view its details.)	Mounting and Dismounting an NSS Volume
Dismount	Dismount a mounted volume.	Mounting and Dismounting an NSS Volume
Move	Move a selected volume to reorganize and redistribute storage on the same server (or to other servers) in response to changing business needs.	Moving Volumes with iManager

Subtask	Description	Reference
Split	Split a selected volume to reorganize and redistribute storage on the same server (or to other servers) in response to changing business needs.	Splitting Volumes with iManager
Properties	View or set attributes for a volume. View usage statistics for a volume.	Viewing Properties of a Volume
User Quotas	View and manage user quotas.	Managing User Space Quotas
Offline	Take a selected snapshot volume offline, where it remains active in the background.	Moving an Active Pool Snapshot Offline
Update eDirectory	If a storage object is not recognized automatically, update eDirectory objects to force recognition.	Updating eDirectory Volume Objects

Volume Job Control

You can use NSS Distributed File Services to move an NSS volume to a different pool. You can also use DFS to split part of a volume, including all data beneath a specified directory in a volume's file structure, to a new volume in a different pool.

Use the following table to find information about subtasks available from the Move/Split Job Control task.

Subtask	Description	Reference
Create a Move / Split Job	Move or split an NSS volume.	Prerequisites and Guidelines for DFS
Move / Split Job Report	After creating a move volume or split volume job, view the job's status report.	Managing Move or Split Jobs
Pause	Pause active move and split jobs.	Pausing a Move or Split Job
Resume	Resume previously paused move and split jobs.	Resuming a Move or Split Job
Reschedule	Reschedule pending move and split jobs.	Rescheduling a Move or Split Job
Delete	Cancel and delete pending move and split jobs.	Deleting a Move or Split Job
Finish	Manually force a job completion to occur for a selected move or split job that cannot complete without manual intervention. Typically, this occurs if files are open during the move or split process and cannot be copied to the new location.	Finishing a Move or Split Job

Partitions

NSS creates and deletes partitions for you when you work with software RAIDS and pools in iManager and NSSMU. To delete partitions manually, use the NSSMU Partitions page.

Use the following table to find information about subtasks available from the Partitions task.

Subtask	Description	Reference
Partitions	View a list of partitions on the selected server.	Viewing a List of Partitions
Details	View information about a selected partition.	Viewing Details for a Partition
Label	Add a label to a selected partition.	Labeling a Partition

Software RAIDs

You can create and manage software RAID devices to improve storage performance and reliability. For NetWare, you can create software RAIDs 0, 1, 5. You can combine RAIDs to create RAIDs 10 and 15. You must use NSSMU to create a software RAID 10 or 15 device.

Use the following table to find information about subtasks available from the Software RAIDs task.

Subtask	Description	Reference
Software RAIDs	View a list of software RAID devices on the selected server.	Viewing Software RAID Devices on a Server
Details	View the details of a selected software RAID device.	Viewing Details of a Software RAID Device
New	Create a new software RAID 0, 1, or 5 device for the selected server.	Creating a Software RAID Device Using iManager
Rename	Rename a selected software RAID device.	Renaming a Software RAID Device
Increase Size	Expand an existing software RAID device by adding a partition to the RAID (up to the limit for that type of RAID). If there are no devices available, the button is disabled. Each partition you add must reside on a different device. You can only add partitions that match the shared state of current member devices. They must be all local or all shared; you cannot mix them.	Increasing the Size of a Software RAID Device
Restripe	Complete a restriping process for a RAID 0 or RAID 5 device that has been paused.	Restriping a Software RAID 0 or 5 Device
Delete	Delete the selected software RAID device and remove the RAID relationship between member partitions and the underlying storage structures. All data on the member partitions is lost.	Deleting a Software RAID Device
Pools	Create and manage software RAID devices.	Viewing Pools on a Software RAID Device
Partitions	View details about partitions in the RAID. In some cases, you can also delete a partition to repair a RAID.	Viewing Partitions on a Software RAID Device

Devices

You can configure, mount, and maintain a wide selection of storage devices, including direct-attached-storage devices, network-attached storage devices, networked storage devices in a Fibre Channel or iSCSI storage area network (SAN), and hardware device arrays.

Use the following table to find information about subtasks available from the Devices task.

Subtask	Description	Reference
Devices	A list of all local and external devices available on the selected server.	Viewing Devices on a Server
Details	View information about a selected device.	Viewing Details for a Device
Initialize Disk	Initialize the selected device by erasing its partition table and effectively destroying all its data.	Initializing a Disk
Multipath	For network configurations with multiple paths between network devices, opens the Multipath page where you can set the primary path and path failover priorities for fault tolerance of connections between host bus adapters and storage devices. You can also bring paths up and down.	Managing Multiple Connection Paths to Devices
Set Default Path	Sets the connection to selected device to its user-defined default primary path.	Setting the Primary Path for a Device to Its Default Path
Reset Registry	Resets the multipath priority settings for a selected device in the server registry to its user-defined defaults.	Resetting the Server Registry with Default Priority Settings for a Device
Shareable for Clustering	Enable device sharing to support high-availability server clusters.	Sharing Devices
Pools	View a list of pools on a device.	Viewing Pools on a Device
Partitions	View information about partitions configured on a device.	Viewing Partitions on a Device

Scan for Devices

You can scan for devices not found automatically by the Media Manager.

Use the following table to find information about subtasks available from the Scan for Devices task.

Subtask	Description	Reference
Scan (Continue)	After you select a server to manage, scan for devices added since you booted the server.	Scanning for Devices

NSSMU

The Novell Storage Services Management Utility (NSSMU) is a console-based utility for managing NSS storage media on a server. NSSMU is the interface you use to set up your basic NSS storage solution during the NetWare installation. For example, you must use NSSMU to create the sys pool and sys: volume. NSSMU allows limited creation and management of the following NSS components: devices (including software RAIDs 0, 1, 5, 10, and 15), partitions (NSS and iSCSI), pools, and volumes.

To set up iSCSI partitions, use the Partitions option in NSSMU. You must have iSCSI target software loaded to make your server into an iSCSI disk server. You cannot create iSCSI devices during the initial installation. For information, see the *iSCSI 1.1.3 Administration Guide for NetWare 6.5*.

For NetWare 6.5 Support Pack 2, you can use NSSMU and Novell Remote Manager to create encrypted volumes. Encryption is an optional volume attribute, available only at volume-creation time. An encrypted volume meets the legal standard of making data inaccessible to software that circumvents normal access control, such as if the media were stolen. You cannot create encrypted volumes during the installation. The sys: volume is not eligible for encryption.

IMPORTANT: NSSMU is not meant to replace iManager or any other NetWare file system management utilities. However, it is the only management tool that can access your server if you accidentally delete or rename the sys: volume.

Load the NSSMU module (nssmu.nlm) from the command line of the server console by entering
nssmu

The following table identifies key functions available in NSSMU for NetWare.

Management Options	Function Keys	Description
Device Management	F1 = Help F2 = Scan for devices F3 = Initialize device (not for sys:) F4 = Multipath (available only if there are multiple paths for the device) F5 = Select/Deselect one or more devices for Initialize or Share actions F6 = Share (Sharable/Not sharable for clustering) F9 = Refresh details of the device Enter = Show partitions	Use this menu option to initialize and maintain a wide selection of physical storage devices and software RAID devices available to this server. Use the RAID Devices option to create and expand software RAID-0, RAID-1, and RAID-5 devices.

Management Options	Function Keys	Description	
Pool Management	Ins = Create a pool Del = Delete a pool F3 = Expand a pool (add partitions) F5 = Refresh details of the pool F6 = Rename a pool F7 = Activate/Deactivate pools F8 = More (list more options) F9 = Show/Hide deleted volumes F10 = List devices (that a pool resides on) Alt+F8 = Update NDS/eDirectory Enter = Show volumes (on a server or pool)	Use this menu option to create, delete, rename, and expand NSS storage pools to efficiently use all free space in the available devices.	
Volume Management	Ins = Create an encrypted or unencrypted volume Del = Delete a volume F3 = Rename a volume F5 = Refresh details of the volume F6 = Deactivate/Activate an encrypted or unencrypted volume. If encrypted, the volume prompts for a password on the first activate after a system boot or reboot. F7 = Dismount/Mount a volume F8 = More (list more options) Alt+F8 = Update NDS/eDirectory Enter = Properties (set volume properties)	Use this menu option to create, delete, rename, activate/deactivate, and mount/dismount volumes and to set volume attributes.	To store data in encrypted format, enable the encryption attribute at the time you create a volume. The encryption setting persists for the life of the volume. The encryption password can be up to 16 standard ASCII characters, with a suggested minimum of 6. The password generates a 128-bit NICI key for encryption. Supply the password on the first volume activate after a system boot or reboot.
Software RAID Management	Ins = Create a Software RAID (0, 1, or 5) Del = Delete a software RAID device F3 = Expand a RAID device (add partitions) F5 = Refresh details of the software RAID device F6 = Restripe (resume restriping for paused RAID 0/5) F8 = Show pools (list pools on selected RAID 0 or 5; for RAID 1, its single member pool appears in device details) Enter = Show partitions (list member partitions for selected device)	A software RAID device emulates a hardware RAID device. RAID devices combine partitioned space on multiple physical devices into a single virtual device that you manage like any device. Each member device contributes an equal amount of space and only a single partition to the RAID.	You can also create a software RAID 10 device by mirroring a pool on software RAID 0 devices, which must have no physical drives in common. Create a pool on one of the RAID 0 devices, then mirror the pool on up to three software RAID 0 devices, totalling up to four partitions for the RAID 10 device.

Management Options	Function Keys	Description
Partitions	Ins = Create an NSS or an iSCSI partition Del = Delete an NSS or an iSCSI partition F3 = Mirror (create a software RAID-1 device) F5 = Refresh details of the partition Enter =Show volumes	Use this option to create and manage NSS partitions and iSCSI partitions. To create iSCSI partitions, the server must run iSCSI target software and be the server you plan to make your iSCSI disk server.

NSS Command Line Management

All NSS commands can be issued from the NetWare server console. Use the server console to monitor NSS activity through console messages.

To view NSS commands and options, at the NetWare server console command prompt, enter
nss /help

For information, see [Chapter 16, “Using NSS Server Console Commands,” on page 217](#).

Novell NetStorage

Novell NetStorage provides a Web-based interface to access directories and files on your NSS volumes on NetWare. You can also manage file system trustees, file system trustee rights, and directory and file attributes for the NSS file system on NetWare.

For information about NetStorage, see the [NetWare 6.5 NetStorage Administration Guide](#).

Accessing NetStorage

To access NetStorage, launch your Web browser and open it to the following location:

`http://192.168.1.1/oneNet/NetStorage`

Replace `192.168.1.1` with the actual DNS name or IP address of your NetStorage server or the IP address for Apache-based services. If Apache-based services use a port other than 80, you must also specify that port number with the URL. For example, if the port number is 51080, the URL would be in the form

`http://192.168.1.1:51080/oneNet/NetStorage`

The date and time on the workstation being used to access NetStorage should be reasonably close (within a few hours) to the date and time on the server running NetStorage to avoid conflicts.

NetStorage uses Novell eDirectory for authentication. Log in with your administrator username and password to manage file system access for directories and files on NSS volumes. You can also log in as any username with equivalent rights to the administrator. This limitation does not apply if you have created a Storage Location object using SSH (Secure Shell).

Configuring File System Trustees, Trustee Rights, and Attributes

Using NetStorage, you can set file system trustees, trustee rights, and attributes for directories and files on NSS volumes. Click the NetWare Info tab to view or modify NSS directory or file attributes. Click the NetWare Rights tab to view or modify NSS file system trustee rights.

For information about file system trustees, trustee rights, and attributes for directories and files on NSS Volumes, see “[Security: Granting Trustee Rights to Directories and Files](#)” in the *NetWare 6.5 Traditional File System Administration Guide*.

Purging and Salvaging Deleted Files

Using NetStorage, you can purge and possibly undelete, or *salvage*, NSS files that were previously deleted. For information, see “[Salvaging or Purging Deleted Files](#)” on page 159.

Browsing Directories and Files

Administrators and users can use NetStorage to browse directories and files in an NSS volume.

Novell Remote Manager

Novell Remote Manager for NetWare provides most of the functionality of the Monitor utility and other functionality from server-console-based utilities. It is the primary management tool for NetWare Traditional File System volumes.

NRM for NetWare also supports some common tasks for managing NSS pools and volumes. For example, you can configure devices, NSS pools, and NSS encrypted or nonencrypted volumes. However, these tasks are best managed with iManager. For NSS, NRM for NetWare is more commonly used to manage file system trustees, file system trustee rights, and attributes for directories and files in your NSS file system.

You can also use Novell Remote Manager to monitor your server’s health, change the configuration of your server, or perform diagnostic and debugging tasks.

To access NRM:

- 1 From your Web browser, enter

`https://server-ip-address:8009`

Replace *server-ip-address* with the IP address or DNS name of the server you want to manage.

The NRM login page opens.

- 2 Type your username and password.
- 3 Click OK.

NRM opens in your Web browser.

For information on accessing, understanding the layout, and configuring server storage parameters through Novell Remote Manager, see the *NetWare 6.5 Novell Remote Manager Administration Guide for NetWare*.

Novell Client for Windows 2000/XP

In combination with NCP Server, the Novell Client™ for Windows 2000/XP supports the following:

- ◆ Management of file system trustees, trustee rights, and inherited rights filters for directories and files on NSS volumes
- ◆ Purge and salvage of deleted files on NSS volumes, if the volume is configured to support it
- ◆ Drive mapping for NSS volumes
- ◆ Login scripts for automatic drive mapping on login

For information, see the *Novell Client for Windows Installation and Administration Guide*.

Trustee Rights Utility

The NSS Trustee Rights Utility (RIGHTS) for NetWare allows you to specify file system trustee rights for directories and files in the NSS file system. For information, see “**RIGHTS**” in the *NetWare 6.5 Utilities Reference*.

ConsoleOne

ConsoleOne is a Java* application that runs on the server or a workstation. In NetWare 6.5, use ConsoleOne to manage the Distributed File Services Management Context and Junctioning functions, including the following options:

- ◆ Create one or more DFS management contexts where servers can host the Volume Location Database (VLDB).
- ◆ Create, maintain, and monitor active VLDB services to locate and transparently redirect traffic to volumes.
- ◆ Optionally create and manage DFS junctions. When you use iManager’s Storage plug-in to move or split NSS volumes, it automatically creates the necessary DFS junctions.

Loading ConsoleOne

To use ConsoleOne on a client workstation, you need to load ConsoleOne 1.3 or later, then copy the NSS .jar files from your server to your client workstation.

- 1 Copy these three NSS .jar files to your local lib directory:

```
public\mgmt\consoleone\1.3\lib\nssadmin.jar  
public\mgmt\consoleone\1.3\lib\nssc1lib.jar  
public\mgmt\consoleone\1.3\lib\nssjavalib.jar
```

- 2 Copy these two .jar files to your local resources directory:

```
public\mgmt\consoleone\1.3\resources\nssadminres.jar  
public\mgmt\consoleone\1.3\resources\nssc1libres.jar
```

- 3 Copy the following .jar file to your local snap-ins directory:

```
public\mgmt\consoleone\1.3\snapins\nssadminreg.jar
```

Managing DFS from ConsoleOne

- 1 Open ConsoleOne.
- 2 Open the tree you want to work with.
- 3 Right-click the server object you want.
- 4 Click Properties.

This opens the ConsoleOne interface, where you can access the snap-ins for managing NSS. The NSS configuration features for DFS are in the media snap-in.

For more information, see the *ConsoleOne 1.3.x User Guide*.

ConsoleOne for NetWare 6.0 and Earlier

For NetWare 6.0 and earlier, ConsoleOne is the primary utility used to configure and maintain partitions, storage pools, and volumes for the NSS and Traditional file systems.

Virtual File Services and Scripts

Virtual File Services (VFS) provides methods that allow you to manage services such as NSS using standard file system functions. Using VFS and a scripting or GUI-based interface, you can view the status and statistics for your system and change the system parameters.

NSS provides a special administration volume, known as the admin volume (named as _admin), that exists on each server. This volume uses no disk space and is created at startup time. Using VFS and the services provided by files that are created on the admin volume, you can potentially control all server management functions.

For more information and instructions, see [Virtual File Services for NetWare \(\[http://developer.novell.com/ndk/doc/vfs/index.html?vfs_enu/data/h5ubo7tt.html\]\(http://developer.novell.com/ndk/doc/vfs/index.html?vfs_enu/data/h5ubo7tt.html\)\)](http://developer.novell.com/ndk/doc/vfs/index.html?vfs_enu/data/h5ubo7tt.html) in the Novell Developers Kit (NDK) documentation.

4

Planning for NSS Storage Solutions

This section describes the following:

- ◆ “Prerequisites” on page 47
- ◆ “Security Considerations” on page 47
- ◆ “Coexistence and Migration Issues” on page 49
- ◆ “Planning for Your Storage Needs” on page 50
- ◆ “Storage Objects in eDirectory” on page 52
- ◆ “Naming NSS Storage Objects” on page 52
- ◆ “What’s Next” on page 54

Prerequisites

- A server running NetWare® 6.5
- At least 10 MB free space on the server storage for each NSS volume you plan to create, up to the combined space you want to allocate to NSS volumes
- One or more devices, each up to 2 TB in size

Security Considerations

This section discusses the following security issues for NSS:

- ◆ “Using Encrypted Volume Support” on page 47
- ◆ “Preventing Encrypted Data from Exposure in a Core Dump” on page 48
- ◆ “Using Data Shredding to Prevent Unauthorized Access to Purged Deleted Files” on page 48
- ◆ “Protecting the Admin Volume and Files.cmd” on page 48
- ◆ “Understanding Security Equivalence Vectors for NSS Users” on page 48
- ◆ “Controlling File System Access for NSS Volumes” on page 48

Using Encrypted Volume Support

Encrypted volume support to meet the legal standard of making data inaccessible to software that circumvents normal access control (such as if the media were stolen) is available for NetWare 6.5 Support Pack 2 and later. For information, see “Managing Encrypted NSS Volumes” on page 171.

Preventing Encrypted Data from Exposure in a Core Dump

When a core dump occurs for an encrypted NSS volume, data from the encrypted volume might be included in the core dump as nonencrypted data dumped from cache memory. To prevent encrypted data exposure in the dump, when prompted to select writing all of memory in the core dump or to exclude NSS cache, select to exclude cache during a core dump.

Using Data Shredding to Prevent Unauthorized Access to Purged Deleted Files

If the Data Shredding attribute for an NSS volume is disabled, unauthorized access to purged deleted files is possible. An individual can extend a file, LSEEK to the end of the existing file data, then read the data. This returns the decrypted leftover data that is in the block.

To secure this vulnerability, make sure to enable the Data Shredding attribute for an NSS volume by specifying a value of 1 to 7 times for the Data Shredding attribute. A value of 0 disables Data Shredding.

For information, see “[Using Data Shredding to Prevent Access to Deleted Files](#)” on page 146.

Protecting the Admin Volume and Files.cmd

The _admin:\manage_nss\files.cmd file is visible to users, but they cannot delete this file nor modify its properties. You should set trustee rights to prevent users from seeing this volume. For information, see “[Restricting Access to Files.cmd \(NetWare\)](#)” on page 145.

Understanding Security Equivalence Vectors for NSS Users

When a user authenticates to the network, the system calculates the user's Security Equivalence Vector (SEV) based on information in the user's profile in Novell eDirectory. Whenever a user connects to the NSS file system, NetWare retrieves the user's SEV from eDirectory and maintains it as part of the connection structure for the user's session. NSS automatically retrieves the user's SEV from the connection structure. NSS validates the user's SEV against the file system trustee rights of the directory and file the user is attempting to access.

Controlling File System Access for NSS Volumes

To ensure that users have the appropriate effective rights to resources, you can make explicit file system trustee assignments, grant security equivalences, and filter inherited rights. To simplify the assignment of rights, you can create Group and Organizational Role objects in Novell eDirectory, then assign users to the groups and roles. For information, see the [Novell eDirectory 8.7.3 Administration Guide](#).

You can control how a file or directory is used by setting its file system attributes. For information, see the following:

- “[Comparison of Directory and File Attributes](#)” on page 300
- “[Managing Attributes for Directories and Files](#)” in the [NetWare 6.5 Traditional File System Administration Guide](#)

Coexistence and Migration Issues

This section discusses the following coexistence and migration issues for NSS:

- ◆ “Compatibility with Operating Systems and Services” on page 49
- ◆ “Compatibility Issues for the Storage, Archive Versioning, CIFS, and Clustering iManager Plug-Ins” on page 49
- ◆ “Upgrading to NetWare 6.5 from NetWare 6.0 and Earlier” on page 50
- ◆ “Comparison of NSS and NetWare Traditional File Systems” on page 50

Compatibility with Operating Systems and Services

The following table summarizes the compatibility of NSS with network operating system versions, directory services versions, and dependencies on other products or services.

NetWare Operating System	NetWare 6.5 SP3 or later
Directory Services	Novell eDirectory™ 8.7.3 or later
Dependencies	NCP™ or Native File Access Protocols (AFP, CIFS, NFS)

Compatibility Issues for the Storage, Archive Versioning, CIFS, and Clustering iManager Plug-Ins

The requirements in this section apply to the following storage-related plug-ins for iManager:

- ◆ Storage plug-in
- ◆ Archive Versioning plug-in
- ◆ CIFS plug-in
- ◆ Clustering plug-in

Web Browser Language Setting

The iManager plug-in might not operate properly if the highest priority Language setting for your Web browser is set to a language other than one of the supported languages. To avoid problems, in your Web browser, click Tools > Options > Languages, and then set the first language preference in the list to a supported language.

Protocols

The following table provides information about the protocols needed to use iManager to manage storage in a heterogenous environment. A protocol annotated with an asterisk is the default and is configured automatically on the servers. The protocols you use must be loaded and running on both the iManager server and the target server you want to manage.

iManager Server		Target Server		
	OES Linux	OES NetWare	NetWare 6.5 SP3	NetWare 6.5 SP2
OES Linux	* WBEM	* WBEM	WBEM (Start WBEM.)	
	CIFS	CIFS	CIFS	CIFS (Field Patch 2B)

iManager Server		Target Server	
OES NetWare	* WBEM	* WBEM	WBEM (Start WBEM.)
		NCP	* NCP
	CIFS	CIFS	CIFS (Field Patch 2B)
NetWare 6.5 SP3	* WBEM	* WBEM	WBEM (Start WBEM.)
		NCP	* NCP
	CIFS	CIFS	CIFS (Field Patch 2B)
NetWare 6.5 SP2	Not available	* NCP	* NCP

WBEM

Where WBEM is the default protocol, WBEM is loaded and runs automatically when you start the server. Otherwise, you must start WBEM to use the protocol.

To start WBEM: At the server console, enter

`openwbem`

If you receive file protocol errors, it might be because WBEM is not running.

CIFS

Where it is available, CIFS must be configured before you can use it. An additional CIFS setup requirement for Field Patch 2B is noted where it is required. For information, see the *NetWare 6.5 Native File Access Protocols Guide*.

NCP

NCP is the default protocol when the iManager server and target server are both NetWare 6.5 SP3 or NetWare 6.5 SP2.

Upgrading to NetWare 6.5 from NetWare 6.0 and Earlier

Use Volume Copy Upgrade to upgrade NetWare 6.0 or earlier NSS and NetWare Traditional volumes to NetWare 6.5 NSS volumes. For information, see “[Upgrading NetWare 5 Volumes to NetWare 6.x NSS Volumes Using Volume Copy Upgrade](#)” on page 285.

Comparison of NSS and NetWare Traditional File Systems

For a comparison of the NSS and NetWare Traditional file systems, see “[Comparison of NSS and NetWare Traditional File Systems](#)” on page 293.

Planning for Your Storage Needs

Before you begin to subdivide, or carve, your physical disks, you should consider what your storage needs are and how you can effectively manage and divide your storage space to best meet your needs. Use the following guidelines when planning how to implement your storage solution:

- ◆ “[Devices](#)” on page 51
- ◆ “[Software RAID Devices](#)” on page 51

- ◆ “[Multiple I/O Paths](#)” on page 51
- ◆ “[Free Space](#)” on page 51
- ◆ “[NSS Pools and Volumes](#)” on page 51
- ◆ “[NSS Encrypted Volumes](#)” on page 52

Devices

NSS recognizes devices up to 2 TB in size. If you have physical or logical devices larger than 2 TB in size, you must carve them into smaller logical devices.

Storage devices can be local to the server, such as a system hard drive, or external to the server, such as with direct-attached storage or in a Fibre Channel or iSCSI storage area network (SAN).

A local hard drive typically hosts the system software and can optionally host applications and user data. The operating system is stored on the system hard drive in the NSS sys pool and sys: volume.

NSS supports server clusters built with Novell Cluster Services™. Both local and SAN storage devices can be shared between the servers, depending on network connections. For information, see the [Novell Cluster Services 1.7 Administration Guide](#).

Software RAID Devices

NSS supports software RAID devices 0, 1, 5, 10, and 15. Use NSSMU to create RAID 10 or 15 devices.

If you use hardware RAID devices, software RAID devices are unnecessary. You can use both hardware and software RAID devices on the same server.

For more information, see “[Managing Software RAID Devices](#)” on page 73.

Multiple I/O Paths

NSS supports multiple I/O paths for fault-tolerant connections between the server and its storage devices. For information, see “[Managing Multiple Connection Paths to Devices](#)” on page 95

Free Space

Understanding how much free space you will need from each device helps you during the disk carving phase of the NSS configuration.

To maximize the performance benefits of software RAID devices, partitions used for the RAID should come from different disks. For software RAID 1 devices, the mirrored partitions can share no disks in common.

For information about space availability on devices, see “[Viewing Details for a Device](#)” on page 57.

NSS Pools and Volumes

NSS is the primary storage file system on NetWare. The sys pool and sys: volume should be reserved for your system software. Create separate pools for applications and user data.

When creating a pool, assign up to 2 TB from free space for each partition. Use at least 4 partitions of up to 2 TB each to create the maximum-sized pool of 8 TB. To grow a pool, add more partitions of space, up to the limits.

Pools can contain space from multiple devices, using various amounts of free space from each. Pools can use multiple partitions from the same device.

To mirror pools, each pool must use partitions from different devices; mirrored pools can have no devices in common.

Pools can contain multiple volumes, but a volume belongs to only one pool.

When creating a volume, assign it a fixed administrative quota or allow the volume to grow dynamically to the size of the pool. Any given volume's quota cannot exceed the size of the pool.

Pools can be overbooked. If a pool contains multiple volumes, the cumulative administrative maximum sizes of all volumes can exceed the pool size, using the overbooking feature, although real total size is bound by physical limitations. Because space is allocated to volumes as needed, a volume might not reach its quota.

NSS Encrypted Volumes

Encrypted Volume Support is available only in NetWare 6.5 Support Pack 2 or later. Create encrypted volumes only after you verify a successful system install or upgrade. For information, see “[Managing Encrypted NSS Volumes](#)” on page 171.

Storage Objects in eDirectory

When you create a logical pool or volume on a server, a Storage object is automatically created in Novell eDirectory™. By default, the name of the Storage object is the server's name with an underscore and the object's name appended (for example, *myserver_sys*). A Storage object represents a logical or physical object on a server, whether it is a writable disk, a CD, or other storage medium.

For more information about Novell eDirectory, see “[Object Classes and Properties](#)” in the *Novell eDirectory 8.7.3 Administration Guide*.

Naming NSS Storage Objects

Storage object names must be unique on a server. If the server is part of a cluster, then all pools and volumes must have unique names across all servers in the cluster, whether they are in shared relationships or not.

Case Insensitive Naming Convention

NSS storage object names are case insensitive. Names such as AURORA, Aurora, and aurora are the same. NSS saves pool, volume, and software RAID device names in uppercase. NSS saves names and labels in uppercase. For example, if you enter vol2 as the name, it is saved as VOL2.

Number of Characters Allowed

- ◆ Device, pool, and volume names consist of at least 2 characters, but not more than 15 characters
- ◆ Software RAID 0 and 5 device names consist of 2 to 128 characters.

- ◆ RAID 1 device names consist of 2 to 80 characters.
- ◆ Partition labels consist of 2 to 128 characters.
- ◆ The encryption password for encrypted NSS volumes on NetWare can be up to 16 standard ASCII characters, with a suggested minimum of 6. The password generates a 128-bit NICI key for encryption.

Conventions for Valid Names

Valid storage object names use the following conventions:

- ◆ Contain only valid characters:
ABCDEFGHIJKLMNPQRSTUVWXYZ0123456789_!@#\$%&()
- ◆ Cannot contain spaces
- ◆ Cannot begin or end with the underscore (_)
- ◆ Cannot contain multiple contiguous underscores (_)
- ◆ Cannot be one of these reserved names:

ALL
AUX
CLOCK
COM1
COM2
COM3
COM4
CON
LPT1
LPT2
LPT3
NETQ
NSS_ADMIN
NUL
PIPE
PRN
SYS

Other Guidelines

- ◆ Because the commercial “at” character (@) is an element of electronic mail addresses such as code@engineer.com, it might cause confusion and possible problems in a storage object name. A Web browser or other application could mistake it for an e-mail address. We recommend that you do not use the commercial “at” character in storage object names.
- ◆ The percent character (%) might cause problems if it is passed in a format string to an application routine that uses it to delineate parameters. For example, if a volume name that contains the percent character, such as store%sales, is passed to an (s)printf routine, the

(s)printf routine might look for parameters that are not there and crash. We recommend that you do not use the percent character in storage object names.

What's Next

You can now create logical devices for your file systems. Continue with the next section, [“Managing Devices” on page 55](#).

5 Managing Devices

Novell® Storage Services™ is the default file system for NetWare® 6 and later. The Web-browser-based iManager Storage plug-in is the primary storage management interface for NSS. For information about iManager, see the *Novell iManager 2.5 Administration Guide*.

You can also use the console-based NSS Management Utility (NSSMU) to manage your NSS file system. You can create pools, volumes, iSCSI partitions for iSCSI disk servers, software RAID devices, and other NSS management functions.

You must use the NSSMU interface to create iSCSI disk partitions for an iSCSI disk server. An iSCSI disk server requires iSCSI target software. For information about managing and using iSCSI devices, see the *iSCSI 1.1.3 Administration Guide for NetWare 6.5*.

This section describes the following:

- ◆ “Understanding Devices” on page 55
- ◆ “Viewing Devices on a Server” on page 56
- ◆ “Viewing Details for a Device” on page 57
- ◆ “Scanning for Devices” on page 58
- ◆ “Initializing a Disk” on page 59
- ◆ “Sharing Devices” on page 60
- ◆ “Viewing Partitions on a Device” on page 61
- ◆ “Viewing Pools on a Device” on page 63
- ◆ “What’s Next” on page 63

Understanding Devices

A device is the physical or virtual storage media available to a server. Physical devices include direct attached storage devices (such as server disks, disk arrays, hardware RAID (redundant arrays of independent disks) devices, and SAN (storage area network) devices. Virtual devices include software RAID devices and iSCSI devices. The following table discusses the management methods to use with NSS for different types of devices.

Type of Device	Management Method
Physical device	To manage physical devices: In iManager, click Storage > Devices.

Type of Device	Management Method
Software RAID device	<p>To create and manage software RAID devices: In iManager, click Storage > Software RAIDs. For information, see “Managing Software RAID Devices” on page 73.</p> <p>After creating the device, you can add pools and volumes as you would for a physical device.</p> <p>To create a software RAID 10 device, use NSSMU. For information, see “Creating a Software RAID 10 with NSSMU” on page 91.</p> <p>To create a software RAID 15 device, use NSSMU. For information, see “Creating a Software RAID 15 with NSSMU” on page 92.</p>
iSCSI device	<p>An iSCSI disk server requires iSCSI target software. To create and manage iSCSI partitions for an iSCSI disk server: At the server console, enter</p> <p><code>nssmu</code></p> <p>In NSSMU, click Partition Management > Insert (Create), then allocate space to the partition.</p> <p>For information about using NSSMU, see “NSSMU” on page 41.</p> <p>To access iSCSI storage devices for a file and print server, you first must connect to an iSCSI disk server. This requires iSCSI initiator software. After connecting, you can view the devices on the disk server in the Devices list and add NSS pools and volumes as you would with any device.</p> <p>For information about managing and using iSCSI devices, see the iSCSI 1.1.3 Administration Guide for NetWare 6.5.</p>

Viewing Devices on a Server

1 In iManager, click Storage > Devices.

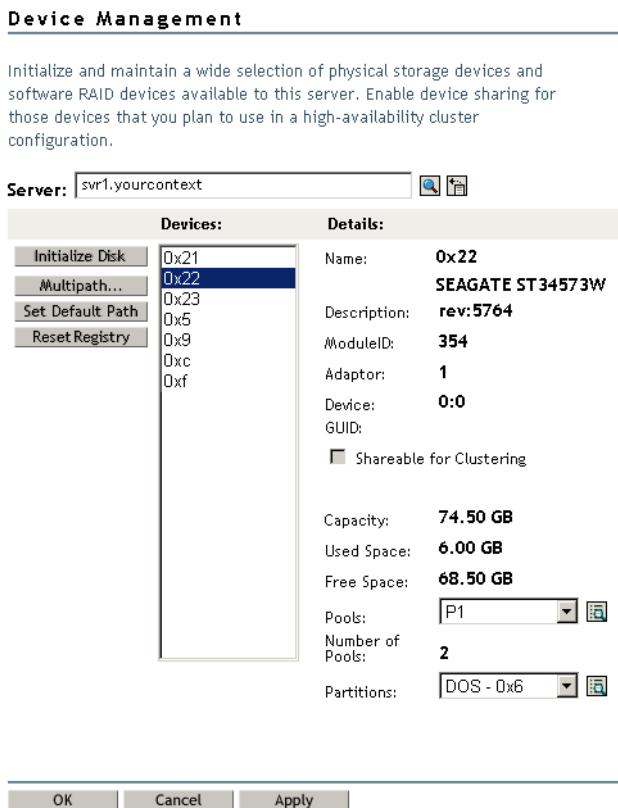
For instructions, see [“Accessing NSS Storage Management Role and Tasks” on page 34](#).

2 Select a server to manage.

For instructions, see [“Selecting a Server to Manage” on page 35](#).

A list of devices appears in the Devices list. Depending on the number of devices, this can take a few seconds. Avoid clicking again in the page until it refreshes and displays the Devices list.

For an overview of the subtasks available from this page, see [“Devices” on page 40](#).



Viewing Details for a Device

The Details field in the Devices Management page displays information about each device in the Devices list, as described in the following table.

Device Detail	Description
Name	The device name assigned by NetWare.
Description	The physical description of the storage object. This is the physical device identification. For software RAIDs, the description might be RAID0, RAID1, or RAID5.
Module ID	The Novell driver identification number for the module, which indicates what type of driver you are using.
Adapter	The sequential number registered for the adapter. The number indicates which drive is on which adapter.
Device	<p>The server address of the selected device.</p> <p>For a SCSI device, the first number is the SCSI ID number and the second number is the Logical Unit Number (LUN), which is commonly used for backup tape drives.</p> <p>For an IDE device, the first number is the channel number and the second number indicates if the device is a master (0) or a slave (1).</p>

Device Detail	Description
GUID	The Global Unique Identifier (GUID) number that NSS assigns to the storage object. This number is necessary so your file system can locate the specific device.
Shareable for Clustering	The attribute of a device that indicates whether the selected device can be shared by multiple computers in a cluster solution.
Capacity	The total available storage space of the selected device.
Used Space	The amount of space on the device that is currently in use by partitions, including NSS partitions, Traditional NetWare partitions, and non-NetWare partitions such as DOS partitions.
Free Space	The total amount of space on the device that is currently not in use.
Pools	The drop-down list shows all pools that exist on this device. To view a pool's details or to manage a pool, select the pool from the list, then click the View Details icon to go to the Pool Management page for that pool.
Number of Pools	The total number of pools that use this device.
Partitions	The drop-down list shows all partitions that exist on this device. To view a partition's details, select the partition from the list, then click the View Details icon to go to the Partition Information page for that partition.
Mirror Status	For a RAID1 device, this field shows its status: <ul style="list-style-type: none"> ♦ In Sync: The mirror group is fully synchronized. ♦ Partial Sync: The mirror group is only partially synchronized. ♦ Not Mirrored: The device is not mirrored (only one partition).

To view a device's details:

1 In iManager, click Storage > Devices.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of devices appears in the Devices list. Wait for the page to load before moving to the next step.

3 Select a device to view its details.

The page must refresh to display the details, which might take several seconds.

Scanning for Devices

NetWare typically recognizes all devices on reboot or after you create them. If you add devices to a server and NetWare does not automatically detect them, you might need to scan for devices.

1 In iManager, click Storage > Scan for Devices.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

The browser opens to the Scan Devices page.

[Storage Management](#) ▶ [Scan for Devices](#)

Scan for Devices



Scan for devices attached to this server, if not found automatically by the media manager. Scanning can take several minutes to complete. Allow an elapsed time of about 30 seconds for each adapter, depending on the number of devices on the adapter.

Server:

[Continue](#) [Cancel](#)

After iManager connects to the server, it scans for devices and displays them in the Devices list. The scan can take several seconds, depending on the number of adapters and disks on your systems. Click Cancel at any time to back out of the process.

3 View the list of devices.

This list is only viewable; there are no actions to make from this page.

4 When you are done:

- ♦ Click Continue to go to the Storage Management main page.
- ♦ Click Storage > Devices in Roles and Tasks to manage the devices.

Initializing a Disk

On the Devices Management page, the Initialize Disk option initializes the selected device and completely removes all the partitions it contains. All the data stored on the device will be lost. If the device contains a partition of an NSS pool, a Traditional volume, or a software RAID device, the Initialize command also deletes data on all of the partitions of the entire pool, volume, or device, even if they reside on separate devices.

WARNING: Do not initialize the device that contains your sys: volume. Initializing the sys: volume destroys the operating system and all the data in it.

This option is disabled (dimmed) if the selected device contains any of the following:

- ♦ System pool or sys: volume
- ♦ DOS partition
- ♦ Software RAID 1 (mirrored) device

It can also be disabled if there is no space available based on each partition’s size, or if you already have the maximum number of partitions allocated in a software RAID device.

To initialize a disk:

- 1 In iManager, click Storage > Devices.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of devices appears in the Devices list.

- 3 In the Devices list, select a device.

- 4 Click Initialize Disk.

Sharing Devices

Storage devices that exist in a storage area network (SAN) can be shared by multiple servers in a cluster. For more information about clustering, see the [Novell Cluster Services 1.7 Administration Guide](#).

IMPORTANT: The system hardware does not specify disk drives to come up automatically as Shareable for Clustering or Not Shareable for Clustering. You must manually set this value for each device, according to the configuration of your storage system.

Making a device shareable enables device sharing for those devices in high-availability clusters that you want to be part of a shared-disk storage solution. If the Shareable for Clustering option is enabled (selected), the selected storage device can be shared by multiple computers in a cluster.

Shareable for Clustering

Marking a device as shareable for clustering sets all of the pools on this device to shareable. If any of these pools span multiple devices, you must make sure that each device is set to the same share state as this one, or the device can become unusable.

If this device is a member of a software RAID device, marking a device as shareable for clustering also sets all the other member devices as shareable for clustering.

Planning for Device Sharing

- Do not assign a device as Shareable for Clustering if it is not capable of being shareable.
- If you create a pool that spans multiple storage devices, each of the member devices in that pool must either be marked as Shareable for Clustering or as Not Shareable for Clustering.
- The system pool and all of its member devices cannot be marked as Shareable for Clustering.
- Devices that contain Traditional partitions and volumes cannot be marked as Shareable for Clustering.
- If you assign partitions to a software RAID device, all the devices for those member partitions must either be marked as Shareable for Clustering or as Not Shareable for Clustering.

Configuring the Device's Share State

- 1 In iManager, click Storage > Devices.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of devices appears in the Devices list.

- 3 In the Devices list, select a device.

After the page refreshes, information about the selected device appears in the Devices list.

- 4 Depending on the current state of the device:

- ◆ To set a device's share state to On, select the Shareable for Clustering check box, then click Apply or click OK.
- ◆ To set a device's share state to Off, deselect the Shareable for Clustering check box, then click Apply or click OK.

If you click Apply, iManager saves the change and remains on the device page. If you click OK, iManager saves the change and takes you to the main Storage Management page. If you do not click Apply or OK, the setting is not implemented; the device remains not shareable.

Viewing Partitions on a Device

In NetWare 6.5 and later, NSS abstracts all partition creation and deletion in iManager; there are no actions to perform on partitions. For information about partitions, see “[Managing Partitions](#)” on page 65.

To view a list of partitions:

- 1 In iManager, click Storage > Devices.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

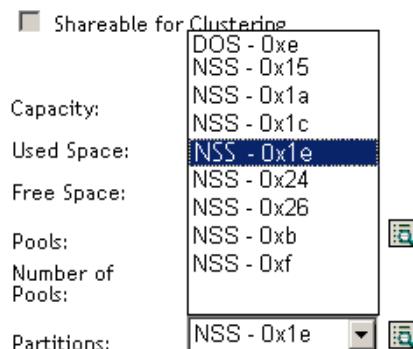
- 2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of devices appears in the Devices list.

- 3 In the Devices list, select a device.

- 4 In the Details area, click the arrow on the Partitions drop-down list to expand it.



5 Select a partition, then click View Details.

This opens the Partition Management page. It displays a list of all the partitions that currently exist on the selected device.

Partitions on: 0x2						
Details						
	ID	Type	Status	Device Name	Pool Name	Size
<input type="checkbox"/>	0x6	DOS	In Use	0x2		2.00 GB
<input type="checkbox"/>	0x8	NSS	In Use	0x2	SYS	3.91 GB
<input type="checkbox"/>	0x11	NSS	In Use	0x2	ARK_POOL	2.79 GB
<input type="checkbox"/>	0x14	Virtual Device	In Use	0x2		100.02 MB
<input type="checkbox"/>	0x17	NSS	In Use	0x2	TEST	95.37 MB
<input type="checkbox"/>	0x20	Virtual Device	In Use	0x2		500.02 MB
<input type="checkbox"/>	0x28	Unknown	In Use	0x2		30.00 GB
<input type="checkbox"/>	0x2b	NSS	In Use	0x2	VOL4	4.66 GB

To view details about a partition:

1 In iManager, click Storage > Devices.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of devices appears in the Devices list.

3 In the Devices list, select a device.

4 In the Details area, click the arrow on the Partitions drop-down list to expand it.

5 Select a partition, then click View Details.

This opens the Partition Management page. It displays a list of all the partitions that currently exist on the selected device.

6 Select a partition from the Partitions list, then click Details to view its details.

Viewing Pools on a Device

1 In iManager, click Storage > Devices.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of devices appears in the Devices list.

3 In the Devices list, select a device.

4 In the Details area, click the arrow on the Pools drop-down list to expand it.



- 5 Select a pool, then click **View Details**.

This opens the Pool Management page where you can view the details of the pool and manage it. See [on page 102](#) for a sample Pool Management page.

For information about pool management, see [“Managing NSS Pools” on page 101](#).

What's Next

You can create software RAID devices to use for pools. For information, see [“Managing Software RAID Devices” on page 73](#).

If your server provides multiple I/O paths between the server and its storage devices, configure the primary path and path priorities for I/O failover for each device. For information, see [“Managing Multiple Connection Paths to Devices” on page 95](#). When you are done, continue with creating pools on your devices.

You can now create pools of storage on the devices you created. For information, see [“Managing NSS Pools” on page 101](#).

6 Managing Partitions

Novell® Storage Services™ automatically manages partitions you use to build software RAID devices and NSS pools, whether you create them in the Storage plug-in for iManager or the NSS Management Utility.

This section discusses the following:

- ◆ “Understanding Partitions” on page 65
- ◆ “Creating NSS Partitions” on page 67
- ◆ “Viewing a List of Partitions” on page 67
- ◆ “Viewing Details for a Partition” on page 69
- ◆ “Labeling a Partition” on page 69
- ◆ “Deleting a Partition” on page 70

Understanding Partitions

A partition is a logical division of a physical hard drive. In NetWare 6.5 and later, NSS abstracts all partition creation and deletion in iManager through the Pools page and Software RAIDs page. When you create NSS pools or NSS software RAID devices, NSS creates the NSS partitions on the devices you specify. You can view and label partitions from the iManager Partitions page.

Partitions on a Device

In iManager, the Partition Information page shows a list of partitions for a selected device. Select a device to view information about the partition in the Details area.

Storage Management > Devices > Partitions

Partition Management

Server: SVR1.novell

Partitions on: 0x2

ID	Type	Status	Device Name	Pool Name	Size
0x6	DOS	In Use	0x2		2.00 GB
0x8	NSS	In Use	0x2	SYS	3.91 GB
0x11	NSS	In Use	0x2	ARK_POOL	2.79 GB
0x14	Virtual Device	In Use	0x2		100.02 MB
0x17	NSS	In Use	0x2	TEST	95.37 MB
0x20	Virtual Device	In Use	0x2		500.02 MB
0x28	Unknown	In Use	0x2		30.00 GB
0x2b	NSS	In Use	0x2	VOL4	4.66 GB

OK

Types of Partitions

The following table shows the types of partitions in a NetWare storage system.

Partition Type	Description
Cluster Service	A partition that NetWare uses to monitor cluster connectivity and services; it appears only in shared devices in the cluster.
DOS	A conventional DOS partition that NetWare uses for installing and upgrading NetWare on the server.
iSCSI	A partition in a target disk server in an iSCSI storage area network; it appears as an iSCSI device to file servers with iSCSI initiator software.
NSS	The primary partition type for NSS file systems.
System Configuration	A vendor-specific partition for maintaining metadata about the server configuration.
Traditional	A partition type found in NetWare systems with legacy NetWare traditional file systems. These might exist in a mixed NetWare environment.
Unknown	An partition type that is unknown to the current operating system.
Upgrade Traditional	An NSS partition in mid-upgrade state between different versions of NetWare.
Virtual Device	A partition that serves as a partition in a software RAID 0 or RAID 5 device.

Partition Details

You can view the following information about partitions:

The following table shows the types of partitions in a NetWare storage system.

Partition Type	Description
DOS	A conventional DOS partition that NetWare uses for installing and upgrading NetWare on the server.
System Configuration	A vendor-specific partition for maintaining metadata about the server configuration.
NSS	The primary partition type for NSS file systems.
Traditional	A partition type found in NetWare systems earlier than NetWare 5. These might exist in a mixed NetWare environment.
Upgrade Traditional	An NSS partition in mid-upgrade state between different versions of NetWare.
Virtual Device	A partition that serves as a partition in a software RAID 0 or RAID 5 device.
iSCSI	A partition in a target disk server in an iSCSI storage area network; it appears as an iSCSI device to file servers with iSCSI initiator software.
Cluster Service	A partition that NetWare uses to monitor cluster connectivity and services; it appears only in shared devices in the cluster.

Creating NSS Partitions

You can view the details of an NSS partition, but NSS abstracts the creation of partitions for pools and software RAID devices.

Use the Software RAID options to create a new software RAID device and to manage its partitions. For information, see “[Creating a Software RAID Device Using iManager](#)” on page 82.

Use the Pools option to create a new pool and to manage its partitions. For information, see “[Creating Pools with iManager](#)” on page 101.

Use the Novell Cluster Services management interface to create a new Cluster Services partition. For information, see the *Novell Cluster Services 1.7 Administration Guide*.

Use NSSMU to create an iSCSI device and to manage its partitions. For information, see the *iSCSI 1.1.3 Administration Guide for NetWare 6.5*.

Viewing a List of Partitions

In iManager, you must access partitions through a related task, such as the following:

- ◆ “[Viewing Partitions on a Device](#)” on page 67
- ◆ “[Viewing Partitions in a Software RAID Device](#)” on page 68
- ◆ “[Viewing Partitions in an NSS Pool](#)” on page 69

Viewing Partitions on a Device

1 In iManager, click Storage > Devices.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

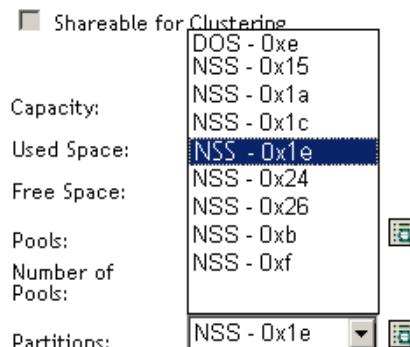
2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of devices appears in the Devices list.

3 In the Devices list, select a device.

4 In the Details area, click the arrow on the Partitions drop-down list to expand it.



5 To view details for the partitions, click the View Partition Details icon.

This opens the Partition Management page. It displays a list of all the partitions that currently exist on the selected device.

Server:

Partitions on: 0x2

Details						
	ID	Type	Status	Device Name	Pool Name	Size
<input type="checkbox"/>	0x6	DOS	In Use	0x2		2.00 GB
<input type="checkbox"/>	0x8	NSS	In Use	0x2	SYS	3.91 GB
<input type="checkbox"/>	0x11	NSS	In Use	0x2	ARK_POOL	2.79 GB
<input type="checkbox"/>	0x14	Virtual Device	In Use	0x2		100.02 MB
<input type="checkbox"/>	0x17	NSS	In Use	0x2	TEST	95.37 MB
<input type="checkbox"/>	0x20	Virtual Device	In Use	0x2		500.02 MB
<input type="checkbox"/>	0x28	Unknown	In Use	0x2		30.00 GB
<input type="checkbox"/>	0x2b	NSS	In Use	0x2	VOL4	4.66 GB

OK

Viewing Partitions in a Software RAID Device

1 In iManager, click Storage > Software RAID.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of devices appears in the Software RAIDs list.

3 In the Software RAIDs list, select a device.

Wait for the page to refresh before continuing.

4 In the Details area, click the arrow on the Partitions drop-down list to expand it.

5 To view details about partitions, click the View Partition Details icon.

This opens the Partition Management page. It displays a list of all the partitions that currently exist on the selected device.

6 Select a partition from the Partitions list, then click Details to view more information.

Viewing Partitions in an NSS Pool

Although NSS abstracts the partitions underlying the pool structure, you can view information about those partitions.

1 In iManager, click Storage > Pools.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of pools appears in the Pools list.

3 Select the pool you want to manage.

Wait for the page to refresh and display the details. The pool must be active to see partition details.

- 4 (Conditional) If the pool is deactive, make sure the pool is selected, then click **Activate**.
After the page refreshes, the **Partitions** drop-down list is available.
- 5 Click on the arrow next to the **Partitions** drop-down list to expand the list.
- 6 To view details about the partitions, click the **View Partition Details** icon.
A Partition Management page opens where you can view details about the pool's partitions.
- 7 Select a partition from the **Partitions** list, then click **Details** to view more information.

Viewing Details for a Partition

- 1 From the **Partitions Management** page, select a partition.
- 2 Click **Details** to view the **Partition Information** page.

For information about the details, see [“Understanding Partitions” on page 65](#).

Labeling a Partition

Partition labels are optional, but if you use them, the label must be unique on a server. If the server is part of a cluster, then partition labels must have unique names across all servers in the cluster, whether they are in shared relationships or not. Partition labels can have 2 to 128 characters.

- 1 On the **Partitions Management** page, select the partition, then click **Edit**.
- 2 Type the new label.
- 3 Click **OK**.

Deleting a Partition

Deleting a partition results in data loss. The Storage plug-in to iManager does not allow you to delete partitions from the **Partitions** page because it abstracts all partition management. Instead, go to the management page of the storage structure that is using the partition to access its partitions and delete them. NSSMU allows you to delete any NSS or NetWare-related partition directly from the **Partitions** page. Use a third-party management tool to delete non-NetWare partitions.

This section discusses the following:

- ◆ [“Deleting NSS Partitions in an Software RAID Device” on page 70](#)
- ◆ [“Deleting NSS Partitions in a Pool” on page 71](#)
- ◆ [“Deleting Cluster Services Partitions” on page 71](#)
- ◆ [“Deleting an iSCSI Partition” on page 71](#)

Deleting NSS Partitions in an Software RAID Device

For software RAID devices, use the **Software RAIDs** page to access and delete its partitions.

You can delete all but one partition of a RAID 1 (mirror) and only one partition at a time for a RAID 5. To delete this partition, use the **Software RAIDs** page to delete its RAID. For information, see [“Replacing a Failed Segment in a Software RAID” on page 85](#).

To delete partitions for a RAID 0, use the **Software RAIDs** page to delete its RAID.

To delete all of the partitions in a software RAID device, you must delete the software RAID itself. For information, see “[Deleting a Software RAID Device](#)” on page 87.

Deleting Partitions with iManager

To delete a single partition in a software RAID 1 or RAID 5 device:

- 1 In iManager, click Storage > Software RAIDs.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 Select a server to view a list of its software RAID devices.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

- 3 Select the software RAID 1 or RAID 5 device you want to manage.

Wait for the page to refresh and display the details.

- 4 Click the View Partition Details icon to open the Partitions Management page for the selected software RAID.

- 5 Select a partition to delete.

- 6 Click Delete to delete the partition and its contents.

Deleting Partitions with NSSMU

- 1 In NSSMU, select Partitions.

- 2 Select the partition you want to delete.

- 3 Click Delete to delete the partition and its contents, then click OK to confirm deletion.

Deleting NSS Partitions in a Pool

You cannot shrink the size of a pool by deleting its partitions. Use the Pools page to delete the pool. For information, see “[Deleting a Pool](#)” on page 109.

Deleting Cluster Services Partitions

The Cluster Services partition is a small partition used by Novell Cluster Services™ to pass status information between cluster nodes. Deleting a Cluster Services partition disrupts services for the cluster. If you have a cluster on your server, you should not delete this partition unless it is corrupted and you plan to rebuild it. If you have deleted your cluster and no longer use Novell Cluster Services, the partition can be deleted safely.

If you delete this partition in error, you can rebuild it with Cluster Services console commands. For information, see “[Novell Cluster Services Console Commands](#)” in the *Novell Cluster Services 1.7 Administration Guide*.

- 1 In iManager, click Storage > Partitions.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 Select a server to view a list of its partitions.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

- 3 Select the Cluster Services partition you want to delete.

- 4 Click Delete to delete the partition and its contents, then click OK to confirm deletion.

Deleting an iSCSI Partition

Deleting an iSCSI partition deletes the NSS partitions on the iSCSI partition, destroys all data in the NSS partitions, and makes the iSCSI target inaccessible to the iSCSI initiators. After deletion, servers (cluster or otherwise) no longer have access to the shared storage in your storage area network that was previously made available by the iSCSI target.

WARNING: Do not delete an iSCSI partition unless it is your intention to get rid of your shared storage, data and all.

If you are not sure about which partitions to delete, you should delete the iSCSI target directly from its management interface.

- 1 In iManager, click Storage > Partitions.

For instructions, see [“Accessing NSS Storage Management Role and Tasks” on page 34](#).

- 2 Select a server to view a list of its partitions.

For instructions, see [“Selecting a Server to Manage” on page 35](#).

- 3 Select the iSCSI partition you want to delete.

- 4 Click Delete to delete the partition and its contents, then click OK to confirm deletion.

7

Managing Software RAID Devices

RAID devices can help improve your storage availability and performance by enhancing data fault tolerance and I/O performance. In NetWare® 6.5, Novell Storage Services™ supports software RAID devices: 0, 1, 5, 10, and 15.

This section discusses the following:

- ◆ “Understanding Software RAID Devices” on page 73
- ◆ “Planning for a Software RAID Device” on page 75
- ◆ “Viewing Software RAID Devices on a Server” on page 79
- ◆ “Viewing Details of a Software RAID Device” on page 80
- ◆ “Creating a Software RAID Device Using iManager” on page 82
- ◆ “Renaming a Software RAID Device” on page 83
- ◆ “Increasing the Size of a Software RAID Device” on page 83
- ◆ “Restriping a Software RAID 0 or 5 Device” on page 85
- ◆ “Replacing a Failed Segment in a Software RAID” on page 85
- ◆ “Deleting a Software RAID Device” on page 87
- ◆ “Viewing Pools on a Software RAID Device” on page 88
- ◆ “Viewing Partitions on a Software RAID Device” on page 88
- ◆ “Deleting Partitions on a Software RAID Device” on page 89
- ◆ “Managing Software RAID Devices with NSSMU” on page 89
- ◆ “Creating Software RAID Devices with NSSMU” on page 90
- ◆ “Mirroring an Existing Pool with NSSMU” on page 91
- ◆ “Creating a Software RAID 10 with NSSMU” on page 91
- ◆ “Creating a Software RAID 15 with NSSMU” on page 92
- ◆ “Creating a RAID 1 Mirror to Duplicate Data” on page 93

Understanding Software RAID Devices

A software RAID is a configuration for storage devices that emulates a hardware RAID device. A software RAID combines partitioned space from multiple physical devices into a single virtual device that you manage like any device. Each member device contributes an equal amount of space to the RAID. You can create partitions, pools, and volumes on a RAID device, just as you would with any physical storage device. Unlike hardware RAID devices, software RAIDs use standard host adapters and do not require any special RAID hardware.

The following table describes the software RAID devices supported by NSS:

Type of RAID	Number of Segments	Purpose	Advantages	Disadvantages
RAID 0	2 to 14	Data striping	<p>Improves I/O performance for both reads and writes, which occur concurrently in parallel to its member devices.</p>	<p>Does not provide data redundancy for data fault tolerance.</p> <p>If a single disk fails, the data cannot be recovered. You must re-create the RAID 0 and restore its volumes from a backup copy before you can use it again.</p>
RAID 1	2 to 4	Data mirroring	<p>Provides full data redundancy for failover and instant recovery.</p> <p>Improves read performance.</p> <p>Equivalent write performance is possible with a duplex connection, which provides a separate channel for each member disk.</p>	<p>To achieve the best I/O performance, it requires separate channels for each member disk; otherwise, write performance decreases slightly.</p> <p>Each mirror must be on a separate device; it can share no disks in common.</p> <p>Can be a member of only one pool.</p>
RAID 5	3 to 14	Data striping with parity	<p>Provides limited data recovery for one member disk at a time. If a single drive in the RAID fails, its volumes and pools remain active, but with degraded performance because the RAID must use parity to reconstruct the missing data. You must remove the failed segment, replace the disk, add the new segment, and restripe the data to reconstruct the data on the replacement drive.</p> <p>Improves read performance if all drives are present and working properly. If a drive fails, read performance is reduced because of parity reads and data reconstruction.</p>	<p>Read responses are the same only if data happens to be in cache when called; otherwise it is slightly reduced for parity checking.</p> <p>I/O performance for writes is reduced because it takes time to calculate and write parity to disk. The more writes to the drive, the greater is the burden to CPU.</p> <p>If multiple disks fail, the data cannot be recovered. You must re-create the RAID 5 and restore its volumes from a backup copy before you can use it again.</p>
RAID 10	2 to 4 RAID 0 devices	Mirroring RAID 0 devices	<p>Provides full data redundancy for failover and instant recovery.</p> <p>Improves I/O performance for both reads and writes, but is slower than an unmirrored RAID 0 device.</p>	<p>Requires separate channels for each member disk to achieve best I/O performance.</p> <p>RAID 0 devices that you mirror can share no disks in common.</p> <p>If a single disk fails, you must recreate the RAID 0 and remirror the entire device. The data is restored through mirroring.</p>

Type of RAID	Number of Segments	Purpose	Advantages	Disadvantages
RAID 15	2 to 4 RAID 5 devices	Mirroring RAID 5 devices	<p>Provides full data redundancy for failover and instant recovery.</p> <p>If a single data disk fails, the RAID 5 device remains up and mirrored. Its performance is degraded until you replace the failed disk.</p> <p>It can handle multiple disk failures, depending on the number of failures and which disks fail.</p>	<p>Requires separate channels for each member disk to achieve best I/O performance.</p> <p>RAID 5 devices that you mirror can share no disks in common.</p> <p>If multiple data disks fail concurrently on the same segment or if the parity disk fails, you must remove the damaged segment from the mirror, re-create the RAID 5, and then mirror the RAID 5. The data synchronizes with the mirrors.</p>

Planning for a Software RAID Device

Before you create your software RAID device, you must evaluate your storage requirements and determine which RAID solution best fits your performance and fault tolerance needs.

This section discusses the following:

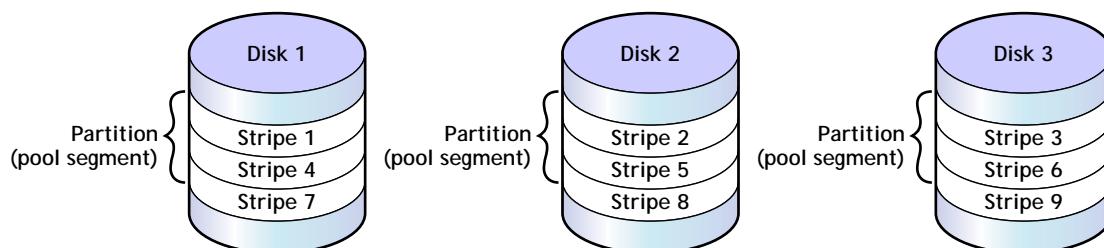
- ◆ [General Guidelines for Software RAID Devices \(page 75\)](#)
- ◆ [Guidelines for Software RAID 1 Devices \(page 76\)](#)
- ◆ [Choosing a Software RAID Solution \(page 76\)](#)
- ◆ [Determining the Number of Partitions \(page 78\)](#)
- ◆ [Determining the Partition Size \(page 77\)](#)
- ◆ [Determining the Stripe Size for RAID 0 and RAID 5 \(page 79\)](#)

General Guidelines for Software RAID Devices

To set up a RAID device, you allocate free space from any of your physical storage devices. NSS transparently presents the allocated free space as virtual partitions that represent NSS-managed physical partition areas on the participating drives. These partitions are the basic elements of a software RAID device. How you allocate each of the partitions to pools depends on the nature of the pools (shared or not shared for clustering) and the type of RAID device it is.

As an example, the RAID 0 device shown below consists of three RAID partitions. It stripes data across three physical drives. The stripes are written and read in the order designated.

Figure 4 Striping Data on a Software RAID 0 Device



Consider the following general guidelines when creating a software RAID device:

- Each partition in the RAID configuration should come from a different device. NSS lets you obtain RAID partitions from the same device, but this severely impedes the performance of your file system.
- Do not use space from a drive that contains your system partition.
- You can use any combination of IDE or SCSI devices in a software RAID device. Make sure these devices have similar performance characteristics; otherwise, your performance might decrease.
- In a clustered solution using Novell Cluster Services™, for software RAIDs 0 or 5 on shared disks:
 - You can have only one pool associated with that RAID device.
 - You must create an NSS pool and volume on that RAID device from the same server node before the pool can be migrated to other nodes in the cluster.

Guidelines for Software RAID 1 Devices

The following is a list of requirements for mirroring partitions with software RAID 1 devices:

- Mirrored partitions must have the same partition type: NSS partitions to NSS partitions and Traditional partitions to Traditional partitions.
- Mirrored partitions should be set up on devices that have similar performance thresholds.
- You can mirror only partitions, each from its own NetWare partition. If a storage pool spans multiple devices, each of the individual partitions that make up that pool can be mirrored independently. All of the pool's partitions must be mirrored in order for the data in that pool to be fault tolerant.
- You cannot combine mirror groups (existing groups with multiple mirrored partitions). A mirror group is expanded by adding a partition from your free space but not by adding an existing mirror group to the current group.
- All of the devices that participate in a mirror must be marked a shared or not shared for clustering for each mirror group.
- Avoid setting up multiple mirror groups on a single device. Such configuration heavily degrades the performance of the file system.
- To mirror software RAID 0 devices, the member devices must have no drives in common.

Drive Restrictions for NSS Software RAID Devices

When you create or expand an NSS software RAID device, do not use space from the drive that contains your system partition. In a worst-case scenario, you might need to reinitialize a drive if the partition in the RAID failed.

WARNING: Reinitializing a drive destroys its contents.

Choosing a Software RAID Solution

When choosing a software RAID solution, determine whether you need to address file system performance, data fault tolerance, or both. The following tables highlights the key data fault tolerance, performance, and configuration issues associated with each RAID type.

Requirement	RAID 0	RAID 1	RAID 5	RAID 10	RAID 15
Data fault-tolerance	No	Redundancy	Parity	Redundancy	Redundancy and parity
Read I/O performance	Best improved (parallel reads)	Improved if parallel channels to each mirror	Improved, if all segments are present and working properly	Improved, with RAID 0 read advantage	Improved if parallel channels to each mirror, with RAID 5 read advantage
Write I/O performance	Best improved (parallel writes)	Same if parallel channels; otherwise, slightly decreased	Somewhat decreased by parity calculation	Slightly improved, depending on channel configuration	Somewhat decreased, depending on channel configuration and parity calculations
Valid names	2 to 128 characters	2 to 80 characters	2 to 128 characters	2 to 80 characters	2 to 80 characters
Number of segments	2 to 14	2 to 4	3 to 14	2 to 4 software RAID 0 devices	2 to 4 software RAID 5 devices
Maximum segment size	1 TB, if 2 segments	2 TB for each mirror	1 TB, if 3 segments (2 for data and 1 for parity)	2 TB for each mirror	2 TB for each mirror
Maximum device size	2 TB	2 TB	2 TB	2 TB	2 TB

Determining the Partition Size

The space that a member device contributes to a software RAID is called a partition or segment. Each physical device should contribute only one partition to the RAID; otherwise, it negates the benefits of the RAID. A software RAID device can contain only one partition per device. All member partitions in a software RAID device must be the same size.

The size of physical and logical devices used for NSS and Traditional file systems cannot exceed 2 terabytes (TB). Therefore, the maximum partition size is 1 TB for software RAID 0 and 5 devices and 2 TB for software RAID 1. For information, see [“Choosing a Software RAID Solution” on page 76](#).

The capacity of the RAID device depends on the RAID type and the number of member partitions:

- ◆ **RAID 0:** Capacity equals the number of partitions times the partition size.
- ◆ **RAID 1:** Capacity equals one partition size.
- ◆ **RAID 5:** Capacity equals the number of partitions minus one, times the partition size.
- ◆ **RAID 10:** Capacity equals one partition size of space taken from the RAID 0; it is not limited to the partition size of partitions in the RAID 0 itself.
- ◆ **RAID 15:** Capacity equals one partition size of space taken from the RAID 5; it is not limited to the partition size of partitions in the RAID 5 itself.

For example, the following table shows the maximum size of partitions needed to create a software RAID device of up to 2 TB.

Maximum Segment Size					
Number of Segments	RAID 0	RAID 1	RAID 5	RAID 10	RAID 15
2	1 TB (1000000 MB)	2 TB (where each mirrored element is a 2 TB device)	Not applicable	2 TB (where each mirrored element is a 2 TB RAID 0)	Not applicable
3	666666 MB	2 TB (2000000 MB)	1 TB (1000000 MB)	2 TB	2 TB (where each mirrored element is a 2 TB RAID 5)
4	500000 MB	2 TB	666666 MB	2 TB	2 TB
5	400000 MB	Not applicable	500000 MB	Not applicable	Not applicable
6	333333 MB	Not applicable	400000 MB	Not applicable	Not applicable
7	285714 MB	Not applicable	333333 MB	Not applicable	Not applicable
8	250000 MB	Not applicable	285714 MB	Not applicable	Not applicable
9	222222 MB	Not applicable	250000 MB	Not applicable	Not applicable
10	200000 MB	Not applicable	222222 MB	Not applicable	Not applicable
11	181818 MB	Not applicable	200000 MB	Not applicable	Not applicable
12	166666 MB	Not applicable	181818 MB	Not applicable	Not applicable
13	153846 MB	Not applicable	166666 MB	Not applicable	Not applicable
14	142857 MB	Not applicable	153846 MB	Not applicable	Not applicable
Maximum device size	2 TB	2 TB	2TB	2 TB	2 TB

Determining the Number of Partitions

Each software RAID device comprises multiple partitions. You must specify at least the minimum number of partitions to create the type of RAID you choose. The maximum number of partitions is limited by the maximum number supported by that RAID type and the maximum device size (2 TB) for NSS and Traditional file systems.

After you set up the software RAID device, you can increase its size by adding segments. In iManager, click Storage > Software RAID Management > Increase Size, and then add segments up to the maximum number of segments for each type of RAID, or until you reach the maximum device size of 2 TB.

You cannot remove segments in a RAID device to decrease its size. In general, to reduce the size of a RAID device: Back up its data, delete the RAID, re-create the RAID with a smaller segment size or fewer segments, and then restore its data from the backup copy.

For some RAIDs, you can replace a failed partition by removing the segment from the RAID, replacing the failed disk, and then adding a segment to the RAID to replace the failed one. For information, see [“Replacing a Failed Segment in a Software RAID” on page 85](#).

Determining the Stripe Size for RAID 0 and RAID 5

In RAID 0 and RAID 5 configurations, NSS writes data to each member device in turn. The maximum amount of data (in KB) committed to each write to a partition is called a stripe. Striping is unrelated to file block sizes that you might set on your storage device.

Set the stripe size in increments of powers of two, between 4 KB and 256 KB (4, 16, 32, 64, 128, 256). The default stripe size is 64 KB.

To maximize performance of the RAID, set the stripe size to correspond with your typical data write requirements. In general, use smaller stripe sizes for data servers and medium-to-large sizes for file servers. For most implementations, 64 KB provides the best performance.

Viewing Software RAID Devices on a Server

Use the Software RAIDs task in the iManager Storage plug-in to create and manage your software RAID devices.

- 1 In iManager, click Storage > Software RAID Management.

For instructions, see [“Accessing NSS Storage Management Role and Tasks” on page 34](#).

- 2 Select a server in the Novell eDirectory™ tree you are logged in to.

For instructions, see [“Selecting a Server to Manage” on page 35](#).

A list of software RAID devices appears in the Software RAIDs list. Depending on the number of devices, this can take a few seconds. Avoid clicking again in the page until it refreshes and displays the Software RAIDs list.

For an overview of the subtasks available from this page, see [“Software RAIDs” on page 39](#).

Software RAID Management



Create and manage software RAID devices. RAID 0, 1 and 5 can improve read and write performance. RAID 1 and 5 also improve reliability. RAID 0 uses data striping on two to fourteen devices. RAID 1 uses data mirroring with two to four mirrored redundant devices. RAID 5 uses data striping with interleaved parity across three to fourteen devices.

Server: nif1.yourcontext

The screenshot shows a software interface for managing RAID devices. On the left, a sidebar lists actions: New..., Delete, Rename..., Increase size..., and Restripe. The main area is divided into two sections: 'Software RAIDs:' and 'Details:'. The 'Software RAIDs:' section contains a list of devices with their IDs: 0x13, 0x20, and 0x26. The device '0x26' is selected and highlighted with a blue background. The 'Details:' section provides the following information for the selected RAID 0 device:

Detail	Value
Name:	0x26
Device:	
Description:	RAID0
ModuleID:	
Adaptor:	
GUID:	
Share State:	Not Sharable for Clustering
Capacity:	100.00 MB
Used Space:	16.00 KB
Free Space:	99.98 MB
Pools:	<input style="width: 150px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px; margin-right: 10px;" type="button" value="..."/> <input style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px;" type="button" value="Edit"/>
Number of Pools:	0
Type:	RAID 0
Stripe Size (KB):	64.00 KB
Segment Size:	50.00 MB
Segments:	<input style="width: 150px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px; margin-right: 10px;" type="button" value="0x25"/> <input style="border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px;" type="button" value="Edit"/>
Number of Segments:	2
Status:	In Sync

Viewing Details of a Software RAID Device

You can view the following information about a selected software RAID device:

Software RAID Device Detail Description	
Name	The device name assigned by NetWare. This is the Device ID from the list box.
Device	The RAID type and the number of member devices.
Description	The physical description of the storage object. This is the administrator-provided name on creation or on rename. If no name is provided, NetWare provides a default name.

Software RAID Device Detail	Description
Module ID	The Novell driver identification number for the module, which indicates what type of driver you are using.
Adapter	The sequential number registered for the adapter, which indicates which drive is on which adapter.
GUID	The Global Unique Identifier number that NSS assigns to the storage object. This number is necessary so your file system can locate the specific device.
Share State	Shareable for Clustering or Not Shareable for Clustering. The share state can be modified on the Devices Management page. If you assign partitions to a software RAID device, all the devices for those member partitions must either be marked as Shareable for Clustering or as Not Shareable for Clustering.
Capacity	The total storage capacity of the device that is reserved for data storage. For a RAID 0, the storage capacity is equal to the sum of its partitions. For RAID 1, the storage capacity is equal to a single partition size; the duplicate partitions are mirrors. For RAID 5, the storage capacity is equal to the sum of its partitions minus one partition for parity.
Used Space	The amount of space on the device that is currently in use by NSS partitions.
Free Space	The total amount of space on the device that is currently not in use.
Partitions	Lists the member partitions of the selected software RAID device in a drop-down list. To view a partition's details, select the partition in the drop-down list, then click the View Details icon.
Partition Size	The size (in MB) of partitioned space per drive.
Stripe Size	The maximum size (in KB) of a data write, as configured for a RAID 0 or RAID 5 device.
Number of Partitions	The total number of partitions in the selected software RAID device.
Status	Shows the status of a RAID 1 (mirrored) device's partitions: In Sync or Out of Sync.

1 In iManager, click Storage > Software RAID Management.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server in the eDirectory tree you are logged in to.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

This opens the Software RAIDs Management page.

The Software RAIDs list displays the virtual RAID devices on the selected server. The list might include any RAID 0, RAID 1, or RAID 5 devices that you created. It does not list any hardware RAID devices in this list; they are listed in the Devices page.

3 Select a virtual storage device in the Software RAIDs list to view information about that device.

Creating a Software RAID Device Using iManager

1 In iManager, click Storage > Software RAID Management.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server in the eDirectory tree you are logged in to.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

3 Click New.

This opens a wizard that steps you through the process.

4 **Device Type and Name:** Specify the type of RAID device you want to create and name the RAID, then click.

If you do not provide a name, NSS creates a unique name for the device. For information about choosing names, see “[Naming NSS Storage Objects](#)” on page 52.

This opens the Devices and Space page.

Used Size (MB)	Storage	Available Size (MB)
<input type="checkbox"/> 0	0x3-1	19234
<input checked="" type="checkbox"/> 19999	0x3-2	80000
<input checked="" type="checkbox"/> 19999	0x4-1	80000
<input checked="" type="checkbox"/> 19999	0x5-1	80000

5 **Devices and Space:** Select devices and the amount of space to use from each, then click Next.

5a In the Partition Size field, type the amount of space in MB to use from each physical device.

NSS identifies devices that have enough free space to meet the partition-size requirements and are eligible for inclusion in the RAID. For information, see “[Determining the Partition Size](#)” on page 77.

If the amount you specify exceeds the amount of free space available on a minimum number of physical devices, the RAID creation fails and returns an error message.

5b Select the check box next to each of the storage devices you want to obtain space from.

You can obtain space from multiple devices. Select only devices that have enough space available to meet your needs.

If a device’s available space is smaller than the specified partition size, it is disabled (dimmed) so that you cannot select it.

A single physical device can offer multiple free space areas in the list. After you select a device, all other free space on that device is disabled for that RAID. Each device should contribute only one partition to the RAID; otherwise, it defeats the purpose of improved performance and data protection that a RAID affords..

If the server has both local and shared devices, the partitions of a RAID can reside only on shared devices or only on local devices. If you select the check box next to a local storage device, the shared devices are dimmed so that you cannot select them. If you select the box next to a shared storage device, the local devices are dimmed.

Only devices that have free space appear in the list. If no devices are listed, there is no space available to create a software RAID device. Cancel the wizard, add more devices to the server or free up space on existing devices, then return to the Software RAID Management page to create a RAID device.

5c Click Next

6 (Conditional) Stripe Size: If this is a RAID 0 or 5 device, set the stripe size. For information, see [“Determining the Stripe Size for RAID 0 and RAID 5” on page 79](#).

7 Click Finish. (Or click Cancel at any time to back out of the process.)

NSS creates the software RAID device, then opens to the Software RAID Management task. Your newly created RAID device appears in the Software RAID Devices list.

After you create the RAID, manage it as you would a physical device in terms of using it for pools and volumes. For information on configuring an NSS file system on your RAID, see [Chapter 9, “Managing NSS Pools,” on page 101](#).

Renaming a Software RAID Device

1 In iManager, click Storage > Software RAID Management.

For instructions, see [“Accessing NSS Storage Management Role and Tasks” on page 34](#).

2 Select a server in the eDirectory tree you are logged in to.

For instructions, see [“Selecting a Server to Manage” on page 35](#).

3 Click Rename.

This opens a dialog where you can enter the new name.

4 Type the new name.

For information about choosing names, see [“Naming NSS Storage Objects” on page 52](#).

5 Click OK. (Or click Cancel at any time to back out of the process.)

NSS renames the software RAID device, then opens to the Software RAID Management task. Your newly renamed software RAID device appears in the Software RAID Devices list.

Increasing the Size of a Software RAID Device

You can increase the capacity of an existing software RAID 0, 1 or 5 device by adding partitions, up to the maximum number for the type of RAID. However, you cannot decrease the size of a partition after the device is created.

To add partitions to an existing software RAID:

1 In iManager, click Storage > Software RAID Management.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server in the eDirectory tree you are logged in to.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

3 Make sure that there is no I/O for the volumes on the RAID device by deactivating the volume.

3a Click Volumes.

3b Select the volumes in the RAID device you want to expand.

3c Click Deactivate.

4 Select a device in the Software RAID Devices list.

If the device contains the maximum number of partitions, the Increase Size option is dimmed. You cannot expand the RAID. Do not proceed.

5 Click Increase Size.

This opens the Expand a RAID wizard to let you choose from available free space on devices that are not already members in the RAID and that contain enough free space to meet the RAID’s current partition size.

6 Do one of the following:

- ◆ If there are no devices available, you cannot expand the RAID. Proceed to [Step 7](#).
- ◆ If the RAID already contains the maximum number of partitions, the Increase Size option is dimmed. You cannot expand the RAID. Proceed to [Step 7](#).
- ◆ Select the check box next to each of the storage devices you want to obtain space from.

The partition size is predetermined by the existing RAID. The partition you choose must be the same size as other partitions comprising the device.

Stripe size is fixed at its current value for the duration of the expansion. If you want to change the stripe size, restripe after the expansion.

You can choose multiple partitions up to the maximum for the type of RAID it is. For information, see “[Determining the Number of Partitions](#)” on page 78 and “[Determining the Partition Size](#)” on page 77.

7 Click Finish.

After you add a partition, the RAID’s data is restriped across both existing and new partitions. During the restriping, the RAID’s capacity does not include the added partition. After the restriping is complete, the RAID’s capacity includes the added partition.

Remirroring and Restriping Temporarily Impacts System Performance

For software RAID 1 devices, the additional mirror begins to collect data immediately. Performance is slightly impacted, but data is available.

For software RAID 0 or RAID 5 devices, the system automatically begins restriping the disks to accommodate the partition you just added. This severely impacts performance until the striping is complete. The capacity of the RAID is not updated until the restriping is done. If the restriping process is interrupted before it completes, it begins automatically on system reboot.

Restriping a Software RAID 0 or 5 Device

In general, there are three reasons for restriping a software RAID 0 and 5 device:

- ♦ **Partition Replacement:** If a partition fails, you must replace it. Restriping recovers the data in a single lost data partition in a RAID 5 by using parity and other data to recreate missing data. However, the data must be restriped from a backup tape if a partition fails in a RAID 0.
- ♦ **RAID Expansion:** If you expand a RAID 1 or 5 device, the RAID restripes the data across all members.
- ♦ **RAID Stripe Size:** If you increase or decrease the stripe size of a RAID 1 or 5 device, the RAID restripes the data across all members. This happens infrequently, unless you are measuring performance with different striping sizes to determine which best fits your operational needs.

If the restriping process is interrupted, the RAID recognizes that when the system reboots, and automatically continues the restriping process. You can also use iManager to pause and resume a restriping process.

To manually resume or pause the Restripe process:

- 1 In iManager, click Storage > Software RAID Management.

For instructions, see [“Accessing NSS Storage Management Role and Tasks” on page 34](#).

- 2 Select a server in the eDirectory tree you are logged in to.

For instructions, see [“Selecting a Server to Manage” on page 35](#).

- 3 Make sure that there is no I/O for the volumes on the RAID device by deactivating the volume.

3a Click Volumes.

3b Select the volumes in the RAID device you want to expand.

3c Click Deactivate.

- 4 Select a device in the Software RAID Devices list.

Wait for the page to refresh before continuing.

- 5 Click Restripe.

The restriping process begins or pauses immediately. Restriping severely degrades I/O performance until the restriping is complete.

Replacing a Failed Segment in a Software RAID

For some RAIDs, you can replace a failed segment by removing the segment from the RAID, replacing the failed disk, and then adding a segment to the RAID to replace the failed one. The following table provides recommended actions for each RAID type.

Software RAID	Remove Segments	Recommended Action
RAID 0	Not allowed	If one or more disks in a RAID 0 fails, all data is lost on that device. You must re-create the RAID and restore its data from a backup copy.

Software RAID	Remove Segments	Recommended Action
RAID 1	All but one mirrored segment	<p>The last segment of a RAID 1 device is the primary device that contains the data. You can use NSSMU Partitions option to remove mirrored segments to free up the related space on those segments, but the data on the last remaining segment is no longer mirrored.</p> <p>If a disk fails in one of the segments, all of its data is lost on that segment. The remaining mirrors continue to operate normally. Remove the segment, replace the failed disk, and then add the segment as an element in the mirror. The data is synchronized over time until it is fully mirrored on the new segment.</p>
RAID 5 (NetWare only)	One data segment at a time	<p>You can temporarily remove one segment at a time in a RAID 5 device to replace a failed data disk.</p> <p>For example, you can replace a single failed data disk while the system is still operational. Use the NSSMU Partitions option to remove the failed segment, replace the failed disk, add a segment to the RAID 5, and then restripe the RAID. The parity is used during restriping to restore the missing data. Read and write performance is degraded on the failed segment until the data is recovered because of parity-related reads and calculations.</p> <p>If multiple data segments fail concurrently or if the parity segment fails, all data is lost on that device. You must delete the RAID 5 and re-create it with good disks. Recover its data from a backup copy.</p>
RAID 10	All but one mirrored segment; cannot remove disks from the underlying RAID 0	<p>The last segment of a RAID 10 is a RAID 0 device that contains the original data. If one or more disk fails in one of the mirrored segments, all data is lost on that segment. The remaining mirrors continue to operate normally. Remove the failed RAID 0 from the RAID 10. Delete the RAID 0, replace the failed disks, re-create the RAID 0, and then add the RAID 0 segment as an element in the mirror. The data is synchronized over time until it is fully mirrored on the repaired RAID 0 segment.</p>
RAID 15 (NetWare only)	All but one mirrored segment; can safely remove one segment at a time per segment	<p>The last segment of a RAID 15 is a RAID 5 device that contains the original data. If a single data segment fails in a RAID 5 that is an element in a RAID 15, repair the RAID 5 while it is operational, as you would with any RAID 5 device.</p> <p>If multiple disks in a mirrored segment fail concurrently or if the parity segment fails, all data is lost on that segment. The remaining mirrors continue to operate normally. Remove the failed RAID 5 from the RAID 15. Delete the RAID 5, replace the failed disks, re-create the RAID 5, and then add the repaired RAID 5 as a segment in the RAID 15. The data is synchronized over time until it is fully mirrored on the repaired RAID 5 segment.</p>

A Segment Fails in a RAID 0

If a segment fails in a RAID 0, you must delete the software RAID 0 device, create a new RAID 0 device, then copy your data to the RAID from backup media. For information, see [“Deleting a Software RAID Device” on page 87](#).

A Segment Fails in a RAID 1

- 1 From the command console, enter `nssmu`.
- 2 From the NSSMU main menu, select Software RAIDs.
- 3 Remove the bad segment.

3a Select the software RAID 1 device that you want to manage.

- 3b Press Enter to show its member segments. The bad segment should show a status of Bad - Unavailable Partition.
- 3c Select the bad segment, then press Delete.
- 4 Expand the RAID with a replacement segment.
 - 4a Select the software RAID 1 device that you want to manage.
 - 4b Press F3 to increase the size of the RAID.
 - 4c From the list of available devices, select the device you want to use for the new segment. The segment size defaults to the size of existing partitions in the RAID 1.
 - 4d Select OK twice.
- 5 The data begins mirroring automatically and continues until the segment is 100% mirrored.

A Single Data Segment Fails in a RAID 5

To replace a single failed data segment in a software RAID 5:

- 1 From the command console, enter **nssmu**.
- 2 From the NSSMU main menu, select Software RAIDs.
- 3 Remove the bad segment.
 - 3a Select the software RAID 5 device that you want to manage.
 - 3b Press Enter to show its member segments. The bad segment should show a status of Bad - Unavailable Partition.
 - 3c Select the bad segment, then press Delete.
- 4 Expand the RAID with a replacement segment.
 - 4a Select the software RAID 5 device that you want to manage.
 - 4b Press F3 to increase the size of the RAID.
 - 4c From the list of available devices, select the device you want to use for the new segment. The partition size defaults to the size of existing partitions in the RAID 5.
 - 4d Select OK twice.
- 5 The restriping should begin automatically. If it does not, from the Software RAIDs page, select the RAID 5 device, then press F6 to Restripe.

Multiple Segments Fail in a RAID 5

If two or more segments fail concurrently in a RAID 5 or if the parity partition fails, you must delete the software RAID 5 device, create a new RAID 5 device, then copy your data to the RAID from backup media. For information, see [“Deleting a Software RAID Device” on page 87](#).

Deleting a Software RAID Device

If you delete a software RAID device, it ends the RAID relationship, and it destroys the NSS file structure on member partitions. All data is lost. Make sure to back up your data or move it to another location before deleting the software RAID device.

- 1 In iManager, click Storage > Software RAID Management.

For instructions, see [“Accessing NSS Storage Management Role and Tasks” on page 34](#).

- 2 Select a server in the eDirectory tree you are logged in to.
For instructions, see “[Selecting a Server to Manage](#)” on page 35.
- 3 Make sure that there is no I/O for the volumes on the RAID device by deactivating the volume.
 - 3a Click Volumes.
 - 3b Select the volumes in the RAID device you want to expand.
 - 3c Click Deactivate.
- 4 Select a device in the Software RAID Devices list.
- 5 Click Delete.

Viewing Pools on a Software RAID Device

- 1 In iManager, click Storage > Software RAIDs.
For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.
- 2 Select a server to manage.
For instructions, see “[Selecting a Server to Manage](#)” on page 35.
A list of devices appears in the Software RAIDs list.
- 3 In the Software RAIDs list, select a RAID device.
- 4 In the Details area, click the arrow on the Pools drop-down list to expand it.



- 5 Select a pool, then click View Details.
This opens the Pool Management page where you can view the details of the pool and manage it.
For information about pool management, see “[Managing NSS Pools](#)” on page 101.

Viewing Partitions on a Software RAID Device

- 1 In iManager, click Storage > Software RAID.
For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.
- 2 Select a server to manage.
For instructions, see “[Selecting a Server to Manage](#)” on page 35.
A list of devices appears in the Software RAIDs list.
- 3 In the Software RAIDs list, select a device.
Wait for the page to refresh before continuing.
- 4 In the Details area, click the arrow on the Partitions drop-down list to expand it.

- 5 Select a partition, then click View Details.

This opens the Partition Management page. It displays a list of all the partitions that currently exist on the selected device.

- 6 Select a partition from the Partitions list, then click Details to view its details.

Deleting Partitions on a Software RAID Device

You can delete all but one partition of a RAID 1 (mirror) and only one partition at a time for a RAID 5. To delete a RAID 1 partition, you must delete its RAID.

- 1 In iManager, click Storage > Software RAID.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of devices appears in the Software RAIDs list.

- 3 Make sure that there is no I/O for the volumes on the RAID device by deactivating the volume.

3a Click Volumes.

3b Select the volumes in the RAID device you want to expand.

3c Click Deactivate.

- 4 In the Software RAIDs list, select a device.

Wait for the page to refresh before continuing.

- 5 Click the Partitions View Details icon.

This opens the Partition Management page. It displays a list of all the partitions that currently exist on the selected device.

- 6 Select a partition from the Partitions list, click Delete, then click OK.

Managing Software RAID Devices with NSSMU

The following table lists the keystrokes that enable you to view, expand, stripe, create, and delete a RAID device:

Keystroke	Description
Enter	Shows the RAID partitions associated with the selected RAID device.
F3	Expands a RAID device by adding more partitions from another storage device. You should not place more than one RAID partition on a disk; this will severely impede the performance of your file system.

Keystroke	Description
F6	<p>Restripes or remirrors a RAID device.</p> <p>Make sure all partitions have been added to your RAID device before restriping a device.</p> <p>The file system performance might slow down during the restriping/ remirroring process.</p>
F8	Show pools (list pools on selected RAID 0 or 5; for RAID 1, its single member pool appears in device details)
Ins	Creates a software RAID (0, 1, or 5)
Del	<p>Deletes an entire RAID device.</p> <p>When you delete a RAID device, all partitions, volumes, and pools associated with that device are also deleted.</p>
F5	Refreshes the display.

Creating Software RAID Devices with NSSMU

1 (Conditional) If you are creating a RAID 1 device, review the “[Guidelines for Software RAID 1 Devices](#)” on page 76 before continuing.

2 Do one of the following:

- ♦ (RAID 1 only) To create a RAID 1 device for an existing pool, select Partitions from the NSS main menu, select the existing partition you want to create the RAID 1 device on, press F3 to select the partitioned free space you want to include in your RAID 1 device, then press Enter to create the RAID device (the partition is automatically mirrored when added to the RAID device).
- ♦ To create a new RAID device from partitioned free space or to expand RAID devices, select RAID Devices from the NSSMU main menu.

3 Press Insert (Ins) to create a new device.

4 Select the RAID type (RAID 0, 1, or 5), then press Enter.

5 Enter the stripe size, then press Enter.

64 KB is the default size and typically provides the best performance if you are using NSS volumes.

6 Select the partitions that you want to mirror or add by using the arrow keys, then pressing Enter.

IMPORTANT: If no partitions appear, it is an indication that either there are no partitions large enough or there are no free partitions.

When you press Enter, the partition appears in the Partition Partitions Included in RAID window. The following table lists the number of partitions that you can include in a RAID device:

RAID Type	Number of partitions
RAID 0	Maximum of 14

RAID Type	Number of partitions
RAID 1	Maximum of 4
RAID 5	Minimum of 3 (one of which is used as the parity) and a maximum of 14

IMPORTANT: After a partition is selected from a device, other free partitions associated with that device might not appear. This prevents you from adding more than one partition from a single physical device, and consequently, helps ensure the optimum performance of your file system.

- 7 Press F3 to initialize and create the RAID device.

After the RAID device is created, the device ID will appear in the RAID Devices window. This window is viewed from the RAID Devices NSSMU main menu.

Mirroring an Existing Pool with NSSMU

- 1 Before you begin, review the “[Guidelines for Software RAID 1 Devices](#)” on page 76.
- 2 In NSSMU, select Partitions from the NSSMU main menu.
- 3 From the list of existing partitions, select the NSS partition for the pool you want to mirror.
- 4 Press F3 to create the RAID 1 device and mirror the partition where the pool resides.
- 5 From the available devices, select up to three additional devices that you want to use as a segment, then press Enter.

The space assigned is the same size as the existing partition. The segments must reside on different devices. If no partitions appear, it is an indication that either there are no partitions large enough or no free space exists on other devices.

- 6 To confirm the RAID 1 device, select RAID Devices from the NSSMU main menu. The RAID 1 device ID appears in the RAID Devices window.

Creating a Software RAID 10 with NSSMU

If you want to mirror your software RAID 0 devices to create a RAID 10, you must use NSSMU to mirror the partition used by the pool on a RAID 0 device. The following procedure describes how to create the RAID 10 in NSSMU. You can also create the RAID 0 devices and an NSS pool on one of the devices in iManager, then switch to NSSMU to mirror the pool’s partition..

- 1 In NSSMU, create a software RAID 0 device with 2 to 14 segments.

For information, see “[Creating a Software RAID Device Using iManager](#)” on page 82.

- 2 Repeat Step 1 one to three times to create 2 to 4 RAID 0 devices.

The RAID 0 devices you use to create the mirror must have no drives in common. Each drive you use to create the RAIDs can belong to only one of the RAID 0 devices.

- 3 In NSSMU, create a pool on one of the RAID 0 devices.
 - 3a In NSSMU, select Pools from the NSSMU main menu.
 - 3b Press Insert (Ins) to create a pool.
 - 3c From the list of available devices, select one of the RAID 0 devices.
 - 3d Assign all of the available space to the pool, then press Enter.

- 4 Create a RAID 1 device to mirror the pool.
 - 4a In NSSMU, select Partitions from the NSSMU main menu.
 - 4b Select the NSS partition for the pool you want to mirror.
 - 4c Press F3 to create the RAID 1 device and mirror the partition.
 - 4d From the available devices, select one to three of the remaining RAID 0 devices you created above, then press Enter.
 - 4e Press F3 to initialize and create the RAID 1 (mirror) device.

After the RAID device is created, the device ID appears in the RAID Devices window. This window is viewed from the RAID Devices NSSMU main menu. The RAID is a RAID 10.

Creating a Software RAID 15 with NSSMU

If you want to mirror your software RAID 5 devices for your NetWare server, you must use NSSMU for NetWare to mirror the partition used by the pool on a RAID 5 device. The following procedure describes how to create the RAID 15 in NSSMU. You can also create the RAID 5 devices and an NSS pool on one of the RAID 5 devices in the Storage plug-in for iManager, then switch to NSSMU to mirror the pool's partition.

- 1 In NSSMU, create a software RAID 5 device with 3 to 14 segments.

For information, see “[Creating Software RAID Devices with NSSMU](#)” on page 90.

- 2 Repeat Step 1 one to three times to create 2 to 4 RAID 5 devices.

The RAID 5 devices you use to create the mirror must have no drives in common. Each drive you use to create the RAIDs can belong to only one of the RAID 5 devices.

- 3 In NSSMU, create a pool on one of the RAID 5 devices.

3a In NSSMU, select Pools from the NSSMU main menu.

3b Press Insert (Ins) to create a pool.

3c From the list of available devices, select one of the RAID 5 devices.

3d Assign all of the available space to the pool, then press Enter.

- 4 Create a RAID 1 device to mirror the pool.

4a In NSSMU, select Partitions from the NSSMU main menu.

4b Select the NSS partition for the pool you want to mirror.

4c Press F3 to create the RAID 1 device and mirror the partition.

4d From the available devices, select one to three of the remaining RAID 5 devices you created above, then press Enter.

4e Press F3 to initialize and create the RAID 1 (mirror) device.

After the RAID device is created, the device ID appears in the RAID Devices window. This window is viewed from the RAID Devices NSSMU main menu. The RAID is a RAID 15.

Creating a RAID 1 Mirror to Duplicate Data

You can create a RAID 1 mirror to duplicate data on a new device, such as to duplicate data on a new storage array.

- 1 Set up the RAID 1 mirror between the initial storage element and new storage element.

For information, see [“Creating a Software RAID Device Using iManager” on page 82](#).

- 2 Let the RAID create a duplicate of the data on the mirror.

- 3 (Optional) If you want to retain the data on the initial storage element and use the element elsewhere, remove the disk it is on from the server.

WARNING: If you leave the disk attached to the server while deleting the element from the RAID, its data is destroyed.

- 4 Use NSSMU or iManager to delete the initial storage element from the mirror, leaving only the new storage element active on the server as a single-element mirror.

The RAID 1 group remains in Media Manager, using only 1 KB of memory. The new array performs normally, without performance degradation and without consuming additional resources.

WARNING: Leave the RAID 1 group active because deleting the RAID 1 group deletes all of its member partitions and destroys the data on them.

In iManager and from the command line, the new array reports that it is Not Mirrored. In NSSMU, the new array reports that it is In-Sync and 100% remirrored, even though there is only a single element.

8

Managing Multiple Connection Paths to Devices

Novell® Storage Services™ supports multipathing, a fault-tolerant and high-availability storage solution. NSS enables you to dynamically manage multiple, redundant connection paths between a server and its external storage devices, according to priorities you set. A single path serves as the primary, active interconnect; the other paths serve as failover paths. In the event of a failure in the active interconnect, NSS automatically and dynamically recovers to another available failover path. This feature is only available if you have multiple interconnect paths in your server-to-storage configuration.

This section discusses the following:

- ◆ “Planning Your Multiple Connection Path Solution” on page 95
- ◆ “Configuring the Primary Path and Priorities for Failover Connection Paths” on page 96
- ◆ “Viewing Connection Path Details” on page 97
- ◆ “Setting a Connection Path as Up or Down” on page 97
- ◆ “Setting the Primary Path for a Device to Its Default Path” on page 98
- ◆ “Resetting the Server Registry with Default Priority Settings for a Device” on page 98
- ◆ “Managing Multiple Paths with Server Console Commands” on page 99

Planning Your Multiple Connection Path Solution

Connection failures can occur if an adapter, cable, or switch in the path between the server and the storage device fails for any reason. For example, if you have two adapters in a server pointing to the same device and the adapter in the primary path fails, the connection between the server and the device fails. The multipath connection feature automatically fails over to the secondary path, using the second adapter and its related path to continue communications. The failover is transparent to users and applications.

To achieve the desired availability, your storage solution can implement one or more host bus adapters in the server and multiple adapters in a SAN. These adapters can interconnect with cables from the server to the device, with cables from each set of adapters to the same switch, or with cables from each set of adapters homed to different switches in your SAN. NSS multipathing is interoperable with third-party storage products such as SANs and hardware RAIDs.

NSS automatically identifies multiple connection paths and randomly selects one path to serve as the primary, active interconnect. You can specify path priorities to control which path serves as the primary path and to set up the failover sequence of the alternate available paths. NSS multipath support enables you to dynamically manage multiple paths according to the priorities you set.

In the event of a failure in the active interconnect, NSS automatically and dynamically recovers to another available failover path. The path with the highest priority of the paths that are available (up) becomes the primary path. The paths not selected remain as failover device paths for the new primary path.

Set a path's priority to determine its position in the failover sequence of the alternate available paths. The default priority is zero (0), which is no priority. Assign a value between 1 (highest priority) to 4 million (lowest priority).

The NLM™ programs needed to take advantage of multipath support (mm.nlm and nwpa.nlm) are installed and loaded when you install NetWare® 6 and later. You can manage multipathing using the browser-based iManager Storage plug-in, NSS Management Utility (NSSMU), or server console commands.

Configuring the Primary Path and Priorities for Failover Connection Paths

You can configure multiple connection paths for a selected device by implementing designs such as the following:

- ◆ Configure the server with multiple host bus adapters for connection to external devices.
- ◆ Use a storage device with multiple interconnects for connection to one or more host bus adapters.
- ◆ Interconnect a server's multiple host bus adapters to storage devices through one or more intermediate network devices, such as a Fibre Channel switch.

Typically, multipath solutions involve storage area network interconnects, but other solutions are possible with external SCSI devices.

To set the primary path and set priorities for failover:

- 1 In iManager, click Storage > Devices.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of devices appears in the Devices list.

- 3 Select a device to manage.

Wait for the page to refresh before continuing.

- 4 Click Multipath.

This opens the Multipath page. All of the paths available between the selected server and the selected device appear in the Failover Device Paths list.

- 5 Select a path to manage.

Wait for the page to refresh before continuing.

- 6 Do one or both of the following:

- ◆ **Select Path:** Click Select Path to make the selected path the primary path between the server and the external storage device. If the selected path is already specified as the primary path, this option is dimmed.
- ◆ **Priority:** Click Priority to set the priority for the selected path. In the Multipath Priority dialog box, enter a valid priority range of 1 to 4 million, where 1 is the highest priority and 4 million is the lowest. The default value of 0 (zero) is no priority.

Viewing Connection Path Details

You can view the following information in the Failover Device Path details:

Failover Device Path Detail	Description
Device Name	The device name assigned by NetWare.
Path Name	The path name assigned by NetWare.
Adapter ID	The ID assigned to the host bus adapter in the server that is a component of the selected interconnect.
Port	The port address for the storage device that is a component of the selected interconnect.
Priority	The integer value you set for the failover path.
Status	<p>The state of the path.</p> <ul style="list-style-type: none">♦ Available: A path is marked as Up if it is available, or Down if it is not.♦ Selected: Only one path serves as the primary path at any given time. The selected path is the primary path.

1 In iManager, click Storage > Devices.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of devices appears in the Devices list.

3 Select a device to manage.

Wait for the page to refresh before continuing.

4 Click Multipath.

This opens the Multipath page. All of the paths available between the selected server and the selected device appear in the Failover Device Paths list.

5 Select a path to manage.

When the page refreshes, the path’s details appear in the Details area.

Setting a Connection Path as Up or Down

When a path’s status is Up, it is available to serve as the primary path or as a failover path between the server and the storage device. A connection path’s status might be Down because a component along the path has failed. You might specify a functioning path as Down to perform maintenance on components in a path.

You can also designate a path as Down if you want to remove the path from consideration as a failover path. For example, if multiple adapters in the server are connected to a target hardware device consisting of multiple devices, NSS would see multiple paths to the devices through each adapter. You might want to allocate which adapter serves which device. To accomplish this, you could down the paths you want the server to ignore.

1 In iManager, click Storage > Devices.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of devices appears in the Devices list

3 Select a device to manage.

Wait for the page to refresh before continuing.

4 Click Multipath.

This opens the Multipath page. All of the paths available between the selected server and the selected device appear in the Failover Device Paths list.

5 Select a path to manage.

Wait for the page to refresh before continuing.

6 Select one of the following:

- **Up:** Make the path available to be selected as the primary path or as one of the failover device paths. If the selected path is already up, this option is dimmed.
- **Down:** Make the path unavailable to be selected as the primary path or as one of the failover device paths. If the selected path is already down, this option is dimmed.

Setting the Primary Path for a Device to Its Default Path

The Set Default Path option resets the connection paths to selected devices to their user-defined default primary paths. For example, after an automatic failover, you can reset the device to use its default primary connection path for current connectivity.

1 In iManager, click Storage > Devices.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of devices appears in the Devices list.

3 In the Devices list, select one or more devices that you want to manage.

4 Click Set Default Path.

The action affects only those devices that actually have multiple paths available.

Resetting the Server Registry with Default Priority Settings for a Device

The Reset Registry option resets the values for path priorities in the registry to their user-defined default values for selected devices. For example, after an automatic failover, you can reset the device to use its default connection priorities for future failovers.

1 In iManager, click Storage > Devices.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of devices appears in the Devices list.

3 In the Devices list, select one or more devices that you want to manage.

4 Click Reset Registry.

The action affect only those devices that actually have multiple paths available.

Managing Multiple Paths with Server Console Commands

When you use the server console to assign multiple paths, you can also assign a priority level to each path, according to which paths you want used first and last. The lower the number, the higher the priority. This number determines which path to take; if the current path fails, the path with the next highest priority is used. Multiple paths can have the same priority level. These values are persistent and they are stored in the registry.

The following commands are available from the server console.

Media Manager Multipath I/O Console Command	Description
list failover devices <i>device_id</i>	<p>This command lists all of the failover devices. It also lists all the paths associated with each device, their assigned priorities, and the path that is selected.</p> <p>To list the paths associated with all the devices on the server, enter the command without specifying the <i>device_id</i>.</p> <p>To list the paths associated with a given device, enter the command followed by the <i>device_id</i>.</p> <p>For example, to see the paths associated with a device with <i>device_id</i> 0x12, enter the following at the server console</p> <pre>list failover devices 0x12</pre> <p>The list provides output similar to the following results:</p> <pre>Ox12 [V132-A1-D2:20] ABC DEVICE rev:5678 Up 11 [V132-A1-D2:20] ABC DEVICE rev:5678 Priority = 1 selected Up 26 [V132-A1-D2:20] ABC DEVICE rev:5678 Priority = 2</pre> <p>In this example, two paths are assigned to device Ox12. Number 11 is <i>Up</i>, and it has been assigned the highest priority of 1. The word <i>Up</i> simply means that this path is available for use. The word <i>selected</i> means that any disk requests that are trying to reach the Ox12 device automatically go through the 11 path, because it is set as the primary path. In this example, you could use the <code>mm set failover path</code> command to override the priorities and make the number 26 path to be the primary path used.</p>
mm set failover priority <i>pathid</i> = <i>number</i>	This command sets the priority level for the selected path. The <i>pathid</i> must be a valid path ID. The <i>number</i> is the priority to set for the selected path. The number must be a decimal integer value between 1 and 4 million, with 1 being the highest priority and 4 million being the lowest priority.

Media Manager Multipath I/O Console Command	Description
mm set failover priority <i>pathid</i> = <i>number</i> /insert	The /insert option inserts the specified path with its specified priority. For example, if you have four existing paths that are assigned the priorities of 1, 2, 3, and 4, and you enter a new path followed by a number 2 and the /insert option, then the paths that were previously assigned to 2, 3, and 4 priority are bumped to priority 3, 4, and 5 in order to accommodate the new path that has been assigned priority 2.
mm set failover state <i>pathid</i> =up /setpath	<p>This command sets the state of the specified path to Up. The <i>pathid</i> must be a valid path ID.</p> <p>If the Up option is followed by the /setpath option, NSS automatically selects the highest priority path from among all the paths that are in the Up state, including the new path.</p>
mm set failover state <i>pathid</i> =down /setpath	<p>This command enables you to designate a path to be in the Down state so you can perform preventative maintenance or reroute cables on a good, functional path. If the path is bad, NSS automatically moves the path to a Down state.</p> <p>If the Down option is followed by the /setpath option, NSS automatically selects the highest priority path from among the other paths that are currently in the Up state.</p>
mm set failover path <i>pathid</i>	This command activates the selected path as <i>selected</i> , which means it serves as the primary path. The <i>pathid</i> must be a valid path that is currently in the Up state. The priority of a path remains static regardless of whether a path is considered up or down or whether a path is selected or not selected as the primary path.
mm restore failover path <i>device_id</i>	This command forces the device to reselect the highest priority path that is online. The <i>deviceid</i> must be a valid device ID.
mm reset failover registry	This command resets the multipath settings in the operating system registry.

9

Managing NSS Pools

Novell® Storage Services™ uses storage pools to efficiently acquire and use all free space available on devices. A pool is an area of storage that consists of space, called a *partition*, obtained from one or more of the storage devices available on a server. The amount of space that each storage device contributes can differ for each member device.

Use the iManager Storage plug-in to configure and manage NSS pools. For information about iManager, see the *Novell iManager 2.0.x Administration Guide*.

You can also use the console-based NSS Management Utility to configure and manage NSS pools. For information, see “[NSSMU](#)” on page 41.

This section describes how to configure and manage NSS pools by completing the following tasks:

- ◆ “[Creating Pools with iManager](#)” on page 101
- ◆ “[Viewing Pools on a Server](#)” on page 104
- ◆ “[Viewing Pool Details](#)” on page 105
- ◆ “[Viewing Partition Information for a Pool](#)” on page 106
- ◆ “[Viewing Volume Information for a Pool](#)” on page 106
- ◆ “[Viewing Device Information for a Pool](#)” on page 107
- ◆ “[Renaming a Pool](#)” on page 107
- ◆ “[Increasing the Size of a Pool](#)” on page 108
- ◆ “[Activating and Deactivating Pools](#)” on page 109
- ◆ “[Deleting a Pool](#)” on page 109
- ◆ “[Verifying and Rebuilding NSS Pools and Volumes](#)” on page 110
- ◆ “[Viewing and Salvaging Deleted NSS Volumes in a Pool](#)” on page 111
- ◆ “[Updating eDirectory Pool Objects](#)” on page 112
- ◆ “[Preventing Pools from Activating on Multiple Servers](#)” on page 113
- ◆ “[What’s Next](#)” on page 114

For information about pool snapshots, see “[Managing NSS Pool Snapshots](#)” on page 115.

Creating Pools with iManager

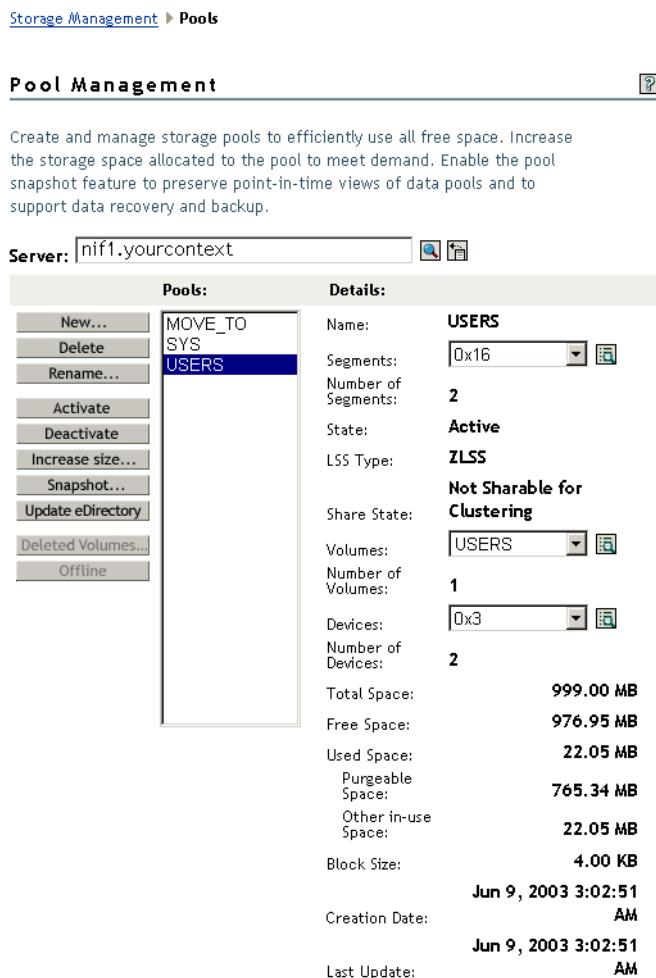
- 1 In iManager, click Storage > Pools.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of pools appears in the Pools list.



The screenshot shows the 'Pool Management' interface with the 'Details' tab selected. The 'Server' dropdown is set to 'nif1.yourcontext'. The 'Pools' list on the left shows 'MOVE_TO' and 'SYS' as options, with 'USERS' currently selected. The 'Details' tab displays the following information for the 'USERS' pool:

Details:
Name: USERS
Segments: 0x16
Number of Segments: 2
State: Active
LSS Type: TLSS
Share State: Not Sharable for Clustering
Volumes: USERS
Number of Volumes: 1
Devices: 0x3
Number of Devices: 2
Total Space: 999.00 MB
Free Space: 976.95 MB
Used Space: 22.05 MB
Purgeable Space: 765.34 MB
Other in-use Space: 22.05 MB
Block Size: 4.00 KB
Creation Date: Jun 9, 2003 3:02:51 AM
Last Update: Jun 9, 2003 3:02:51 AM

3 To create a new pool, click **New**.

The New Pool wizard opens to guide you through the process.

4 Specify a name for the new storage pool, then click **Next**.

For guidelines about naming pools, see “[Naming NSS Storage Objects](#)” on page 52.

5 Select the devices you want to use and the amount of space to use from each device.

In the **Used Size** field, type the amount of space in megabytes (MB) to add, up to the amount of free space available for that device. If any entry exceeds a device's available space, the pool expansion fails and returns an error message.

The size of a given storage partition cannot exceed 2 terabytes (TB). If you want to create an 8 TB pool or volume, you must use at least four partitions when you create the pool.

The **Total Pool Size** is the sum of the partitions you define plus the current pool size. Initially, the **Total Pool Size** field displays the current size of the pool. To update the **Total Pool Size** as you enter values in the **Used Size** field, click anywhere within the wizard dialog box.

You can obtain space from one or more of the devices listed. Only devices that have free space appear in the list. If no devices are listed, there is no space available to increase the size of the

pool. Cancel the wizard, add more devices to the server or free up space on existing devices, then return to the Pool Management page to increase the size of this pool.

6 Specify if you want to activate the device and if you want to cluster-enable shared devices by doing the following:

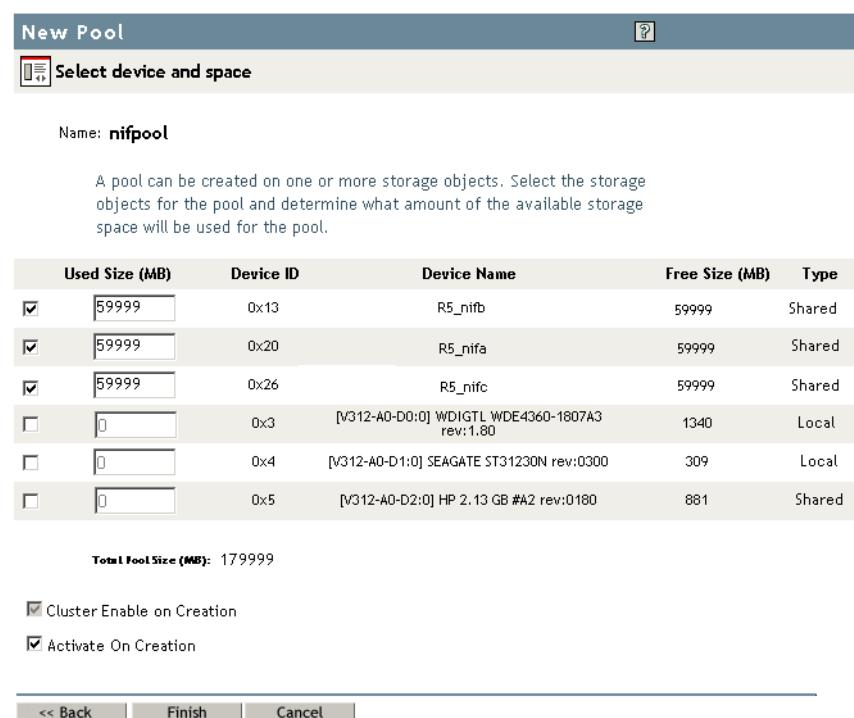
- ♦ **Local:** The Create Pool dialog box appears with the Activate on Creation check box automatically selected. Deselect the box if you do not want to activate this pool on creation.

If the partition that you selected is *not* shareable for clustering (local), click Finish.

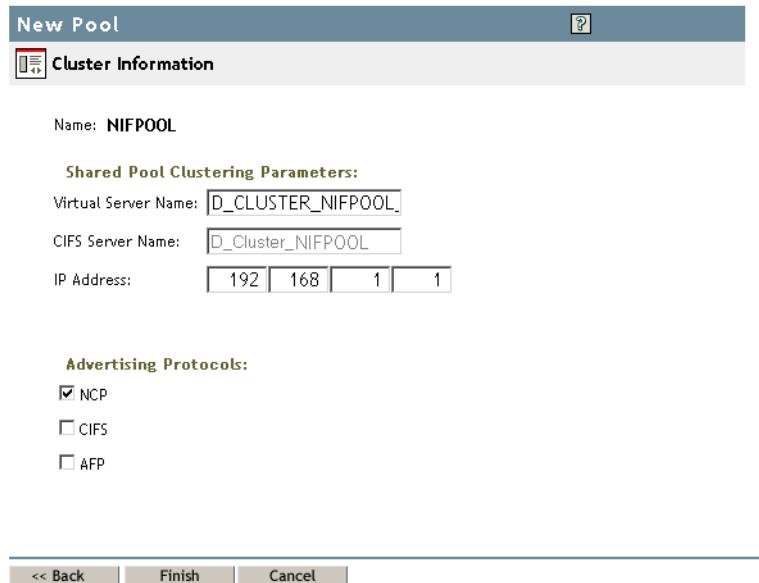
- ♦ **Shared:** If the partition that you selected *is* shareable, the Create Pool dialog box appears with the Activate on Creation and Cluster Enable on Creation check boxes selected.

Deselect the Activate on Creation check box if you do not want to activate this pool on creation.

If you want to cluster-enable the pool, click Next; otherwise, deselect the box, then click Next.



7 (Conditional) If the Cluster Enable on Creation check box is selected, an additional page appears to enable you to specify the cluster information.



Fill in the following shared pool clustering parameters:

- ◆ **Virtual Server Name:** The name assigned by NetWare® to the virtual server that represents the shared pool in the cluster.
- ◆ **CIFS Virtual Server Name:** The name assigned by NetWare 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.
- ◆ **IP Address:** The IP address that you want to assign the virtual server.

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 one or more advertising protocols 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.
- ◆ CIFS is the Windows networking protocol
- ◆ Apple* File Protocol (AFP) is the Macintosh networking protocol.

8 Click Finish.

Viewing Pools on a Server

1 In iManager, click Storage > Pools.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

When the page refreshes, a list of pools appears in the Pools list. Depending on the number of pools, this can take a few seconds. Avoid clicking again in the page until it refreshes and displays the Pools list. See [Viewing Pools on a Server](#) for a sample Pool Management page.

Viewing Pool Details

The Details area of the Pool Management page displays information about a selected pool in the pools list, as described in the following table.

Device Detail	Description
Name	The descriptive pool name assigned by the administrator.
Partitions	A list of all of the partitions that are part of the selected pool. To view information about any of the partitions, select the partition in the drop-down list, then click the View Details icon.
Number of Partitions	The total number of partitions currently assigned to the selected pool.
State	The current state of the selected pool: Active or Deactive. Active pools are available to the users; deactivate pools are not available to users.
LSS Type	The type of Loadable Storage System, such as ZLSS, CDDVD, or DOSFAT.
Share State	Shows whether the selected pool is on a device that is Shareable for Clustering or Not Shareable for Clustering. The system pool cannot reside on a device that is sharable for clustering. Use the Device Management page to set this device attribute.
Volumes	A list of all existing volumes residing in the selected pool. To view information about any of the volumes or to manage any of the volumes, select the volume in the drop-down list, then click the View Details icon. You can also select a pool, then click Volumes in Roles and Tasks.
Number of Volumes	The total number of volumes residing in the selected pool.
Devices	A list of all the devices contributing space to the selected pool.
Number of Devices	The total number of devices currently assigned to the selected pool.
Total Space	The total amount of space assigned to the selected pool.
Free Space	The total amount of space that is currently not in use on the selected pool. <ul style="list-style-type: none">◆ Purgeable Space: The total amount of space in the selected pool that is currently in use as a salvage area or partitioned space that is not yet otherwise assigned.◆ Other In-Use Space: The total amount of space in the selected pool that is currently in use and cannot be easily deleted without destroying data.
Block Size	The maximum amount of data committed to a single write. Possible sizes include 4, 8, 16, 32, or 64 KB. The default setting for NSS is 4 KB.
Creation Date	The time stamp (date and time) that the pool was created.
Last Update	The time stamp (date and time) that the pool was last modified by a management action.

Procedure

1 In iManager, click Storage > Pools.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of pools appears in the Pools list.

3 Select a pool to view its details.

Wait for the page to refresh and display the pool’s details.

4 (Conditional) The pool must be active to display its details. If the Details field is empty, select the pool, then click Activate.

When the page refreshes, you can view the pool’s details.

Viewing Partition Information for a Pool

Although NSS abstracts the partitions underlying the pool structure, you can view information about those partitions.

1 In iManager, click Storage > Pools.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of pools appears in the Pools list.

3 Select the pool you want to manage.

Wait for the page to refresh and display the details. The pool must be active to see partition details.

4 (Conditional) If the pool is inactive, make sure the pool is selected, then click Activate.

After the page refreshes, the Partitions drop-down list is available.

5 Click on the arrow next to the Partitions drop-down list to expand the list.

6 To view details about a partition, select the partition, then click View Details.

A Partition Information page opens where you can view details about the partition.

Viewing Volume Information for a Pool

1 In iManager, click Storage > Pools.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of pools appears in the Pools list.

3 From the Pool Management page, select a pool.

Wait for the page to refresh and display the details in the Details area.

4 To view the volumes in the pool, use one of these methods:

♦ In the Details area, click the arrow on the Volumes drop-down list.

To view details for a volume in the list: Select the volume, then click View Details. The Volume Management page opens with the server and volume preselected.

- ♦ Click Storage > Volumes in Roles and Tasks.

The Volume Management page opens with the server preselected. To view details for a volume in the Volumes list: Select the volume, then wait for the page to refresh.

For information about Volume management, see “[Managing NSS Volumes](#)” on page 127.

Viewing Device Information for a Pool

- 1 In iManager, click Storage > Pools.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of pools appears in the Pools list.

- 3 From the Pool Management page, select a pool.

Wait for the page to refresh and display the pool’s details in the Details area.

- 4 To view the list, in the Details area, click the arrow on the Devices drop-down list.

- 5 (Optional) To view details for a device in the list: Select the device, then click View Details.

The Device Management page opens with the server and device preselected. Wait for the page to refresh to view the device’s details.

For information about device management, see “[Managing Devices](#)” on page 55.

Renaming a Pool

The Rename option on the Pool Management page lets you to modify the name of the selected pool. For example, you might want to assign a pool name that relates to a department name change.

- 1 In iManager, click Storage > Pools.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of pools appears in the Pools list.

- 3 Select the pool that you want to rename.

Wait for the page to refresh and display the details.

- 4 Click Rename.

This opens the Rename a Pool wizard that guides you through the process.

- 5 Specify a name, then click Finish.

If the name is valid and unique, the pool is successfully renamed.

If not, you receive an error, and you must repeat the process. For information about valid pool names, see “[Naming NSS Storage Objects](#)” on page 52.

- 6 (Conditional) If the Pool Management page does not automatically update to show the new name for the pool, in Roles and Tasks, click Pools to refresh the current page.

Increasing the Size of a Pool

Using the Increase Size option on the Pool Management page expands the storage capacity of a selected pool by adding new partitions. You can increase the size of your storage pools, but you cannot reduce their size.

- 1 In iManager, click Storage > Pools.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

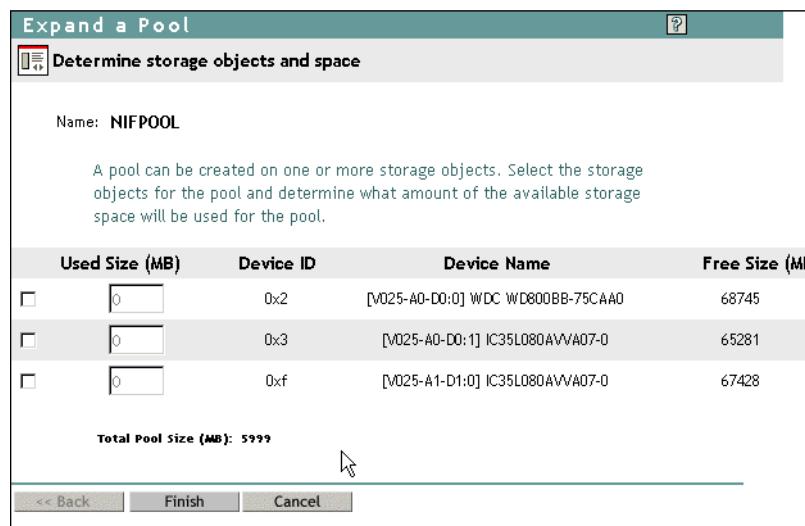
A list of pools appears in the Pools list.

- 3 Select the pool that you want to expand.

Wait for the page to refresh. It displays the pool's details and enables management options.

- 4 Click Increase Size.

This opens an Expand a Pool wizard that guides you through the process of adding partitions from available devices.



- 5 Select the devices you want to use and the amount of space to use from each device.

In the Used Space field, type the amount of space in megabytes (MB) to add, up to the amount of Free Space available for that device. If any entry exceeds a device's available space, the pool expansion fails and returns an error message.

Software RAID 1 (mirrored) devices can contain only one pool per device. If you select a RAID-1 device to add a partition to your pool, NSS automatically allocates all of the available space to the pool.

The Total Pool Size is the sum of the partitions you define plus the current pool size. Initially, the Total Pool Size field displays the current size of the pool. To update the Total Pool Size as you enter values in the Used Size, click anywhere within the wizard dialog box.

You can obtain space from one or more of the devices listed. Only devices that have free space appear in the list. If no devices are listed, there is no space available to increase the size of the

pool. Cancel the wizard, add more devices to the server or free up space on existing devices, then return to the Pool Management page to increase the size of this pool.

- 6 Click Finish, or click Cancel at any time to back out of the process.

Activating and Deactivating Pools

You might need to temporarily restrict user access to a pool. Instead of bringing down the server, you only need to deactivate the specific pool.

The Activate option on the Pool Management page makes the selected pools and all the volumes in them available for user access. The Deactivate option on the Pool Management page takes the selected pools and all the volumes in them temporarily unavailable to users. It does not destroy volumes in the pools, nor does it destroy the data contained in the volumes.

To change the state of a pool:

- 1 In iManager, Storage > Pools.

For instructions, see [“Accessing NSS Storage Management Role and Tasks” on page 34](#).

- 2 Select a server to manage.

For instructions, see [“Selecting a Server to Manage” on page 35](#).

A list of pools appears in the Pools list.

- 3 Select the pool that you want to activate or deactivate.

Wait for the page to refresh. It displays the pool’s details and enables management options. The State field shows whether the device is Active or Deactive.

- 4 Depending on the pool’s current state, to change the state of the pool:

- ♦ Click Activate.
- ♦ Click Deactivate.

Deleting a Pool

You might need to delete an NSS pool to create more free space for other pools. After you delete a pool, ownership of the space for the pool is removed and the free space becomes available. You can assign this space to other NSS pools, as desired, to increase their size.

IMPORTANT: If you delete a pool, you cannot restore any of the volumes in that pool.

The Delete option on the Pool Management page removes one or more selected pools from the server, including all member partitions and the data on them.

WARNING: Deleting a pool destroys all volumes in the pool and destroys all the data in them. These volumes cannot be restored.

You cannot delete a system pool using iManager. Deleting a system pool removes the operating system. You need to reinstall NetWare to delete a system pool. However, if the system pool you want to delete does not contain the active operating system (for example, a remnant on a previously used disk), you can rename the pool, then delete it.

Deleting a pool removes the ownership of the space it occupied, freeing the space for reassignment. If the pools you want to delete are active, deactivate them before you delete them.

- 1 In iManager, Storage > Pools.

For instructions, see [“Accessing NSS Storage Management Role and Tasks” on page 34](#).

2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of pools appears in the Pools list.

3 Select one or more pools that you want to delete.

Wait for the page to refresh. It displays the pool’s details and enables its management options.

4 Click Delete.

5 Click Yes to confirm the deletion, or click No to cancel the deletion.

WARNING: If you click Yes, the pool and all the volumes and data on it are immediately destroyed.

Verifying and Rebuilding NSS Pools and Volumes

Volume errors are typically transactions left unfinished during a system crash of some kind. Most volume errors get fixed automatically during volume mount. If the errors persist, NSS uses the Verify and Rebuild utilities to resolve any problems.

IMPORTANT: The Verify and Rebuild utilities are not the same as the Vrepair command (used to rebuild Traditional volumes).

NSS allows you to temporarily deactivate individual storage pools to fix volume problems instead of bringing down the server. However, when you deactivate a storage pool, users do not have access to any of the volumes in that pool.

Verify fixes NSS pools and volumes by searching for inconsistent data blocks or other errors. This utility indicates if there are persistent problems with the file system that require you to use the Rebuild utility.

Rebuild verifies and uses the existing leaves of an object tree to rebuild all the other trees in the system. You need to deactivate a pool before you run Rebuild so users cannot access the volumes you are rebuilding. When you deactivate a storage pool, all the volumes in the pool automatically deactivate.

WARNING: You should use Rebuild only as a last resort to recover the file system after data corruption. Data loss might occur during a rebuild.

When you use the Verify and Rebuild utilities, a log file of errors and transactions, *volume_name.rlf*, is generated at the root of the DOS drive. The error log, *sys:pool_name.vlf*, contains information about data that has been lost or recovered. You can check the error file whenever an NSS volume does not come up in active mode after a rebuild.

Every time you rebuild a particular pool and volume, the previous error file is overwritten. If you want to keep old error files, move them to another location.

1 (Optional) Verify the pool with a read-only assessment of volume problems.

1a At the server console, enter

```
nss /poolverify
```

1b Select the pool name from the displayed list.

1c Review any errors onscreen or in the *volume_name.rlf* file, located at the root of the DOS drive.

2 To run Rebuild, enter the following command at the server console:

```
nss /poolrebuild=poolname
```

Replace *poolname* with the name of the pool you want to rebuild.

This verifies and accounts for all blocks in the system. Rebuilding can take several minutes to several hours, depending on the size of the pool.

3 For each volume, do one of the following:

- ♦ **Volume with Errors:** If a volume has errors, its error messages are reported onscreen and in the Rebuild and Verify Log. The volume remains in maintenance mode. Read the *volume_name.rlf* file at the root of the DOS drive on your server for information about the errors and transactions. Read the *sys:pool_name.vlf* file for information about data that has been lost or recovered.
- ♦ **Volume without Errors:** If a volume has no errors, it automatically reverts to the active state. Mount the volume.

Viewing and Salvaging Deleted NSS Volumes in a Pool

If you delete a volume, NSS removes it from the pool. However, during a specified amount of time, called the Purge Delay time, you can review and restore the volumes you have deleted. After the purge delay time elapses, NSS automatically removes volumes from the system and you can no longer access them. You can also manually purge any volumes you have deleted.

During the Purge Delay time (by default, four days after a volume is deleted), you can manually purge deleted volumes, view the volume contents, transfer files from the deleted volume to other volumes, or salvage the entire volume, if desired.

You can also change the Purge Delay time to extend or reduce the time for the automatic purging cycle. The Purge Delay time command can be changed by adding a line in the autoexec.ncf file. The default value for the Purge Delay is 345600 seconds, which is four days. Specify the time in seconds. See [“Setting the Purge Delay for the Salvage Area” on page 157](#).

The Deleted Volumes option on the Pools page opens separate Deleted Volumes page where you can purge or salvage the deleted volumes for the pool. This option is only available if the selected pool has deleted volumes on it.

WARNING: If you delete an entire pool, all the volumes are deleted with it. You cannot restore a pool or any deleted volumes.

To manage the deleted volumes in a pool:

1 In iManager, click Storage > Pools.

For instructions, see [“Accessing NSS Storage Management Role and Tasks” on page 34](#).

2 Select a server to manage.

For instructions, see [“Selecting a Server to Manage” on page 35](#).

A list of pools appears in the Pools list.

3 Select the pool that you want to manage.

Wait for the page to refresh. It displays the pool’s details and enables its management options. The Deleted Volumes option is active only when there are deleted volumes in the list.

4 Click Deleted Volumes.

This opens the Deleted Volumes page.

Deleted Volumes:		Details:
Purge	PROJ46	Pool: PROJ46
Pause Purge	PROJ135	Volume was deleted: Jun 9, 2003 4:19:07 PM
Restart Purge	SHVOL	Scheduled Purge Time: Jun 13, 2003 4:19:07 PM
Salvage...	TEMP30	Current deletion state: Salvageable
TEMP60	TEMP90	
TEMP90		
Close		

5 Select a volume from the Deleted Volumes list.

Wait for the page to refresh and display the selected volume's details.

- ◆ **Pool:** The pool name.
- ◆ **Volume Was Deleted:** The time stamp when the volume was deleted.
- ◆ **Scheduled Purge Time:** The time that the Purge Delay expires for this deleted volume and the purging process is scheduled to begin.
- ◆ **Current Deletion State:** The deleted volume can be salvageable, purging, or paused.

6 Select one or more volumes, then perform one or more of these actions:

- ◆ **Purge:** Immediately begins the process of purging the selected volumes and their contents.
- ◆ **Pause Purge/Restart Purge:** Pause Purge stops the volume purging process for selected volumes. Restart Purge purges the selected volumes.
- ◆ **Salvage:** Begins the restore process for deleted volumes you selected.

If you salvage a volume, you need to assign a new name to that volume. A wizard opens to allow you to name the salvaged volume.

The volume salvage process can slow the server response time, so you might want to do this when there is less server activity.

- ◆ **Close:** Closes the Deleted Volumes page.

Updating eDirectory Pool Objects

On the Pool Management page, the Update eDirectory option adds or updates the Novell eDirectory™ pool object at the same context level as the server. NSS searches for the object. If the pool object exists, NSS prompts you with two options: delete and replace the existing object, or retain the existing object. If the pool object does not exist, NSS adds the object to the context level.

Use this option to update eDirectory after you have modified a pool's parameters or renamed it.

1 In iManager, click Storage > Pools.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of pools appears in the Pools list.

3 Select the pool you want to update.

Wait for the page to refresh. It displays the pool’s details and enables its management options.

4 Click **Update eDirectory**.

Preventing Pools from Activating on Multiple Servers

If enabled, the pool Multiple Server Activation Prevention (MSAP) prevents some accidental activations of a pool on more than one server at a time. It does not catch all multiple activations. You should never purposely attempt to activate a pool on two servers at the same time. MSAP is not meant as a replacement of clustering software that controls shared pools.

MSAP protects pools on systems that do not have clustering installed but are attached to a shared disk by accident. For example, a pool might not be marked with the Shareable for Clustering attribute, but it exists on shared disks seen by multiple servers.

Pool MSAP also protects against dangerous conflicts that can occur if you disable the Shareable for Clustering flag in order to force an activation of a shared pool, or if you use `override=shared` when activating a pool. If MSAP detects a conflict, it deactivates the pool before massive corruption occurs.

If you unload Novell Cluster Services™ NLM™ software, or if you are not running it, pool MSAP provides an extra level of protection. The clustering software watches pools that are marked with the Shareable for Clustering attribute; MSAP detects conflicting connection from multiple servers and prevents corruption of pools even on devices that are marked as Not Shareable for Clustering.

In some cases, the MSAP software causes pools to take up to 30 seconds to activate. This delay might occur on the next pool activation after the Server ID or the Cluster ID changes for a given server pool. The Server ID changes if the registry is corrupted. The Cluster ID changes if the Cluster eDirectory object ID is lost.

If MSAP is enabled, all active NSS pools are read every 14 seconds. If your storage media are not shared between multiple servers such as in a SAN, you can clear the `zpool_feature_msap` bit. You should not clear this bit if your pools are on physically shared storage media.

If a pool can be accessed by older servers not running the Support Pack with the MSAP software, then multiple pool activations can still occur.

IMPORTANT: MSAP does not protect against partition conflicts for pools. It does not prevent multiple servers from creating a pool in the same partition.

Managing MSAP Using Server Console Commands

The management file for pool MSAP is `_admin\manage_nss\pool\poolname\zIss\msap.xml`. One file exists for each pool. The `msap.xml` file contains MSAP statistics for the pool. The MSAP attribute is displayed in the `enabledAttributes` field of the `poolinfo.xml` management file.

For `manage.cmd`, the pool operation `getPoolInfo` returns the MSAP tag (`<msap>`) in the `supportedAttributes` tag (`<supportedAttributes>`) and the `enabledAttributes` tag (`<enabledAttributes>`).

For APIs, the pool feature `zpool_feature_msap` can be viewed and controlled using the `zGetInfo` and `zModifyInfo` commands.

Use the following table understand MSAP console commands.

MSAP Console Command	Description
<code>nss /msapserver</code>	Enables MSAP for all the pools on the server. By default, MSAP is enabled for every pool on the server. We recommend that you never disable MSAP.
<code>nss /nomsapserver</code>	Disables MSAP for all the pools on the server. This command remains in effect only until the server is next rebooted. We recommend that you never disable MSAP.
<code>nss /msaprebuild</code>	Rebuilds a corrupt MSAP block. Before issuing the command to rebuild, you must deactivate the pool because a corrupt MSAP prevents a pool from going into Maintenance state. Rebuilding an MSAP block does not give the rebuilder ownership of the pool.
<code>nss /poolmsap=poolname</code>	Enables MSAP for a given pool on the server. MSAP is enabled the next time the pool is activated. (Enter the command, deactivate the pool, then activate the pool. MSAP is now enabled.)
<code>nss /nopoolmsap=poolname</code>	Disables MSAP for a given pool. Use the command when the pool is activated. MSAP will be disabled the next time the pool is activated. (Enter the command, deactivate the pool, then activate the pool. MSAP is now disabled.)
<code>nss /pools</code>	Displays the message “Multi-use detect” for pools that have MSAP enabled.

What's Next

You can now create volumes in the NSS pools you created. For information, see [Chapter 11, “Managing NSS Volumes,” on page 127](#).

10

Managing NSS Pool Snapshots

In NetWare® 6.5, Novell Storage Services™ supports pool snapshots to improve backup and restore services. A pool snapshot is a metadata copy of a storage data pool that preserves a point-in-time view of a data pool. When you back up a pool from its pool snapshot, your backup can capture every file in the pool, even those that are in use at the time. You can create, manage, and delete a pool snapshot for any pool on your server.

A pool snapshot also supports file recovery. After you take a snapshot, you can activate it at a later time to access the original pool's data as it existed at the time of the snapshot. Both the pool and its snapshots can be active and available concurrently. You access data on the active pool snapshot just as you would any other pool, even while data is changing on the original pool you snapped.

When pool snapshots are active, server performance can decrease slightly because the number of disk writes increases, depending on the volatility of your data and the number of pool snapshots that are active.

This section discusses the following:

- ◆ [“Benefits of Pool Snapshots” on page 115](#)
- ◆ [“How the Pool Snapshot Works” on page 116](#)
- ◆ [“Understanding Key Concepts for Pool Snapshots” on page 117](#)
- ◆ [“Managing Pool Snapshots Using iManager” on page 120](#)
- ◆ [“Managing Pool Snapshots Using Commands” on page 126](#)

Benefits of Pool Snapshots

Pool snapshots save time and preserve data. They provide an instant copy of a pool that can help expedite routine maintenance procedures to back up, archive, and protect data on that pool. Because traditional methods of duplicating large amounts of data can be expensive and time-consuming, the efficiency of snapshots can be an important benefit for your enterprise. You can make snapshots as frequently as needed to meet your data availability and resilience requirements.

You can use pool snapshots in a variety of ways to enhance your current storage infrastructure, including the following scenarios.

Supporting Backup Operations

A pool snapshot facilitates non-disruptive backups because the snapshot becomes the source of the backup. As contrasted to a traditional, full-data copy of the pool, the metadata copy only takes a moment to create and occurs transparently to the user. With traditional backups, applications might be shut down throughout the backup routine. In comparison, the pool snapshot process makes the original pool available with almost imperceptible delay.

Archiving Data

You can archive pool snapshots to capture a history of the changes made to the original data pool.

Restoring Data

Pool snapshots can serve as a source for restoring information. Two common reasons to restore information are user error and application errors.

- A user might inadvertently make changes to a file that need to be reversed. Files can become corrupted or deleted. The pool snapshot provides a quick and easy way to locate and reinstate selected files.
- An application might be infected by a virus or be corrupted by other problems, causing the application to store erroneous data throughout the pool. With a pool snapshot, you can easily effect a rollback of all or part of the original pool to a point in time before the virus or problem was known to exist in the system.

Re-Creating Operational and Development Environments

You can also write to the pool snapshot, just as you would any pool. You can work with and modify the snapshot version of the data. For example, in a software development environment, engineers might want to repeat builds and tests of data within a given snap.

Testing and Training

Snapshots can provide a convenient source for testing and training environments and for data mining purposes.

How the Pool Snapshot Works

The pool snapshot function uses copy-on-write technology to enable the instantaneous block-level snapshot of a pool, while requiring only a fraction of the storage space of the original data pool. A pool snapshot does not save an exact copy of the original data pool. Instead, the snapshot is a metadata-based copy that stores only the blocks of data that change subsequent to the instant of the snap. The snapshot combines the metadata and stored block data with the unchanged data on the original pool to provide a virtual image of an exact copy of the data at the instant the snapshot was taken, plus any end-user modifications made to that snap.

Before the snapshot can occur, the snapshot function must render the original pool quiescent by briefly halting all data transaction activity when current transactions complete. It temporarily prevents new writes to the pool and flushes the file system cache to make the pool current with existing writes. Any open files are seen by the snapshot feature as being closed after these outstanding writes occur. Then, it snaps the now-stable pool, and allows data transaction activity to resume.

The quiescence process provides a transactionally consistent image at the instant the snapshot is made. Because the snapshot is consistent, it is not necessary to check the consistency of the file system or database when you activate the snapshot for access.

After the snap, the snapshot function continues to track the transaction activity in the original pool. It determines which blocks in the original pool will change as data writes are made to the original pool. It suspends the write activity while it copies the original block data to the designated pool where it stores the pool snapshot, referred to as the “stored-on pool.” Then it allows a write to that block in the original pool. This keeps the snapshot metadata consistent in time with the exact instant the snapshot was taken.

As the original pool changes, the snapshot can grow to the size of the stored-on pool. The average disk space requirements for a pool snapshot are 10 percent to 20 percent of the original pool size. The actual space depends on how many writes are made to the original volume and the time period that the snapshot exists before it is archived or deleted. Currently, a combination of up to 500 snapshots can exist on any given stored-on pool. The more snapshots you must traverse to find data, the longer it takes to retrieve the data, and the slower the perceived response time to the user.

Understanding Key Concepts for Pool Snapshots

This section discusses the following topics:

- ◆ [“Creating a Pool Snapshot” on page 117](#)
- ◆ [“Naming Pool Snapshots” on page 117](#)
- ◆ [“Choosing the Stored-on Pool” on page 118](#)
- ◆ [“Maintaining the Stored-on Pool” on page 118](#)
- ◆ [“Activating Pool Snapshots” on page 119](#)
- ◆ [“Deleting Pool Snapshots” on page 119](#)

Creating a Pool Snapshot

Create a pool snapshot when you want to capture a point-in-time view of a active data pool. Both the original pool and the stored-on pool must be active when you make the snapshot. For instructions on creating a pool snapshot, see [“Creating a New Pool Snapshot” on page 120](#).

Naming Pool Snapshots

You name a pool snapshot at the time you order the snap. Specify a unique snapshot name for each snapshot. Because the snapshot name also serves as the snap’s pool name when active, the name you give it should be unique among snapshots and among pools. The combination of snapshot name and time stamp when the snapshot was taken can help you identify the version of a data pool you want to access when a pool snapshot is active.

We recommend that you apply a naming convention for snaps. This is particularly important if you plan to create a series of snapshots for multiple pools. The snapshot name is generally a modified version of the original pool’s name to support easy identification of all snaps for any given pool.

IMPORTANT: The snapshot name can be 2 to 16 characters.

Default Naming Scheme

For example, by default, NSS adds a letter and number designator to the original pool name, such as “_Sn”. The “S” indicates that it is a snap. The “n” represents an incremental number of snaps taken for this pool. In this scenario, snapshot names might be PoolA_S1, PoolA_S2, and so on for snaps of PoolA. If you delete older snaps and reuse the lower sequence numbers, a simple sort by snapshot name can be confusing. Be sure to verify the time stamp on the pool when you work with pools that conform to this naming convention.

Example of an Alternate Naming Scheme

For some scenarios, it might be desirable to adopt more meaningful and sortable naming conventions. Currently, you can sort by snapshot name only, not by time stamp. If you create multiple snaps of a pool each day, consider using a logical naming convention that identifies both

the pool name and a combination of the date and an approximate 24-hour-clock time of the snap. For example, use a modified version of the pool name and add “_Syyymddttt”. Snapshot names for snaps of PoolA might be PA_S0210300600, PA_S0210301800, PA_S0210310600, PA_S0210311800, and so on. Of course, the time stamp shows the exact time that the snapshot was taken, because there is a slight delay between ordering a snapshot and the instant of the snapshot itself.

Considerations for Naming

It is also important to consider the names of existing pool snapshots and your snap-naming conventions when you name new data pools. If an active data pool and a deactive pool snapshot share the same name, a conflict occurs when you try to activate a pool snapshot or another regular pool with the same name. To resolve the conflict, the media manager dynamically modifies the snapshot name of the pool snapshot with an *n* (sequential number). This makes the snapshot name unique with respect to the active pool list during the time that the pool snapshot is active and functioning as a pool.

Choosing the Stored-on Pool

The stored-on pool is the active data pool where you want to store the pool snapshot. All pool snapshots for any given original pool must reside on the same stored-on pool. As noted previously, a combination of up to 500 snapshots can exist on any given stored-on pool.

When you create a pool’s first snapshot, you select the stored-on pool for the first and any subsequent snapshots. Typically, you can select the pool itself or a different pool to be the stored-on pool, given that the pool you choose is active and has sufficient space available. There are two exceptions:

- ♦ If the original pool is a shared pool, you must select the original pool as the stored-on pool, and this pool must be active and have sufficient space available.
- ♦ If the original pool is a non-shared pool, you cannot select a shared pool as the stored-on pool.

In general, you can achieve better performance by selecting a data pool located on a different disk than the pool you want to snap.

When creating your first NSS pool-level snapshot for a pool, we highly recommend that the destination pool specified for the snapshot data is different than the source pool you are snapshotting. The exception to this is clustering, where the destination pool for the snapshot data must be the same as the source pool you are snapshotting.

If the destination pool that stores the snapshot data runs out of space, it causes write errors to happen on the pool(s) being snapshot. Please allow ample space for snapshots to grow over time when sizing the snapshot’s destination pool. The amount of space required depends on the number of snapshots, the snapshot retention policy, and the turnover rate for data in the source pool.

Maintaining the Stored-on Pool

If the stored-on pool and the original pool are the same, the status of any given pool snapshot is closely tied to the operational status of the pool. However, if they are not the same, you need to consider how the status of each pool affects the other, and how they affect the status of the pool snapshot.

You can deactivate the original pool, as needed, without adversely impacting the pool snapshot or the status of the stored-on pool. If the original pool is deactive, there are no active transactions for the pool snapshot function to process. If the stored-on pool hosts only the snapshots made for that

deactivated original pool, it can be safely deactivated for the duration. Re-activate the stored-on pool first when bringing the pools back into service.

IMPORTANT: If you need to deactivate a stored-on pool, you must first deactivate each of the original pools that correspond to the families of pool snapshots stored on it.

In contrast, deactivating the stored-on pool first can cause the ungraceful deactivation of the corresponding original pool. Each pool snapshot must be able to dynamically expand its storage footprint in the stored-on pool, because its metadata grows in response to changes in the original pool. Dynamic allocation is not possible when its stored-on pool is deactive. For brief outages, it is possible that any given pool snapshot residing in that stored-on pool has sufficient space available to accept new metadata, depending on the frequency of writes to its corresponding original pool. However, if you deactivate a stored-on pool, it increases the likelihood that one of the pool snapshots it hosts will run out of space. This causes the ungraceful deactivation of the corresponding original pool.

IMPORTANT: The stored-on pool should remain active as long as it hosts any pool snapshots. You can deactivate it safely only after all original pools are deactivated, and for the duration of their deactivation. Activate the stored-on pool before re-activating any of the original pools.

Activating Pool Snapshots

You activate a pool snapshot whenever you want to access the data on it, such as for data retrieval, data modification, and data backup. After the pool snapshot is active, it appears by its user-assigned snapshot name in the pool list. Treat it as you would any pool to manage the pool and to activate and mount its volumes.

The names of volumes on the pool snapshot are a modified version of the volumes on the original pool. Generally, an “_SV” (snapshot volume) is added to the volumes’ names. When you deactivate the pool snapshot, any snapshot volumes on it are automatically deactivated, and its snapshot name is no longer listed in the pool list.

Deleting Pool Snapshots

You delete a pool snapshot when you no longer need it, or if you want to make room to add other snapshots to its stored-on pool. If you create a pool snapshot and specify its stored-on pool as the same pool where its original data resides, and more than one pool snapshot exists when you are ready to delete a snapshot, delete its oldest snapshot in a first created, first deleted sequence.

Users can access the snapshot for reads and writes when the snapshot is activated as a pool, just as they would any pool. Because any given pool snapshot can rotate into an archived status or be deleted, you need to be aware if the snapshot is in use before you delete it.

In NetWare 6.5 SP3 and later, when a snapshot is deleted, Media Manager automatically zeroes out all the blocks that it used. It no longer turns on shredding for the internal volume when creating a snapshot. You can apply the system shredding feature to a snapshot pool by entering

```
mm snap shred snapname = on
```

Replace *snapname* with the unique name of the pool snapshot. Shredding occurs only in the internal volume of the pool where you are storing the snapshot.

If you turn on snapshot shredding for a snapshot, you can have only one snapshot at a time for its original pool. When you delete the snapshot, do not create another snapshot until the system has had enough time to complete the shredding process. Depending on the size of the snap, allow more time for larger amounts of data to shred. The typical delay time is a few minutes.

If any pool snapshot was created on this pool prior to the NetWare 6.5 SP3 release, shredding is already turned on. You can turn shredding off by entering

```
mm snap shred snapname = off
```

Replace *snapshotname* with the unique name of the pool snapshot. Shredding is turned off only in the internal volume of the pool where you are storing the snapshot. It does not affect other snapshots.

If the system goes down during the delete, the zeroing process does not continue after the system restarts. Some nonzeroed data blocks might remain. If it is important that all snapped data be removed from the system, you can turn on shredding, with the limitations as noted above.

If shredding is turned on, the delete process zeroes out the data, and then starts shredding the blocks where data was stored. If the system goes down during the delete, the zeroing process does not continue after the system restarts, but the shredding automatically continues after the system restarts.

Managing Pool Snapshots Using iManager

This section discusses the following management tasks:

- ♦ [Creating a New Pool Snapshot](#)
- ♦ [Viewing Pool Snapshot Details](#)
- ♦ [Renaming a Pool Snapshot](#)
- ♦ [Activating and Deactivating a Pool Snapshot](#)
- ♦ [Moving an Active Pool Snapshot Offline](#)
- ♦ [Deleting a Pool Snapshot](#)

Creating a New Pool Snapshot

- 1 In iManager, click Storage > Pools.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 In the server field on the Pool Management task, select a server to manage.

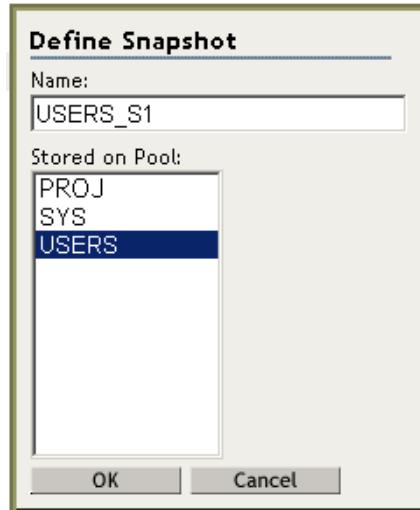
For instructions, see “[Selecting a Server to Manage](#)” on page 35.

- 3 In the Pools list, select the active pool that you want to be the original pool to be snapped, then click Snapshot.

Both the original pool and the stored-on pool must be active when you make the snap. The original pool and stored-on pool can be the same. To activate a pool, select the pool, then click Activate.

IMPORTANT: If the selected pool is a pool snapshot, this option is not available. You cannot take a pool snapshot of a snapshot.

- 4 In the Define Snapshot dialog box, name the snapshot and specify its stored-on pool.



4a Name the snapshot.

By default, the name is the name of the original pool, appended with *_Sn*, where *n* represents a number. You can change this name, but it should be something that you can easily relate to the original pool and the sequence in which the snapshot was taken. By default, *_SV* is added to volume names to indicate the storage object is a volume in a pool snapshot.

For example, if your original pool is named users, its default snapshot name is users_s1.

You can change the default name, if desired. For information about naming considerations, see [“Naming Pool Snapshots” on page 117](#).

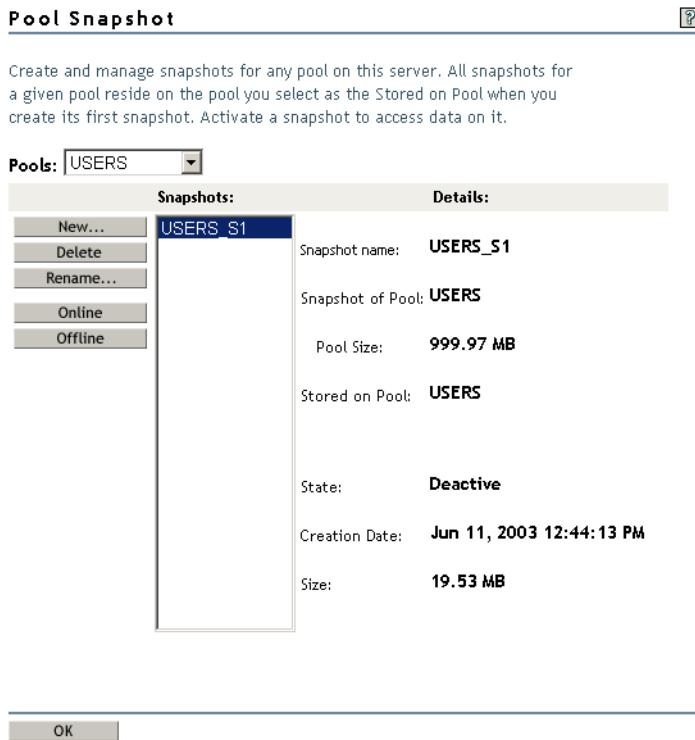
4b Select the stored-on pool from the list of pools available on the selected server.

By default, NSS specifies the stored-on pool to be the same as the original pool. You can choose any of the pools on the server.

IMPORTANT: After you specify a stored-on pool, that pool is the default stored-on pool for all subsequent snapshots made of the original pool. To modify the stored-on pool associated with an original pool, you must delete all existing snapshots for the original pool, then begin again to create a new pool.

4c Click OK to create the snapshot, or click Cancel to back out of the process.

5 After NSS creates the pool snapshot, NSS opens to the Pool Snapshot Management page so that you can further manage the snapshot. The Snapshots list contains the newly created snapshot.



Viewing Pool Snapshot Details

In iManager, you can view the following details about a pool snapshot.

Snapshot Details	Description
Snap Name	The descriptive pool snapshot name assigned by the administrator.
Snapshot of Pool	The name of the original pool that was snapped.
Pool Size	The total size allocated for the pool snapshot.
Stored-On Pool	The pool where the snapshot metadata resides. This can be the same as the original pool. The current default in iManager is that the stored-on pool and the original pool are the same. If you want to store snapshots on a different pool, you must use the command line interface. For instructions, see "Managing Pool Snapshots Using Commands" on page 126 .
State	The current state of the selected pool: Show or Hide. If you show pool snapshots (Online), they appear in the pool list. If you hide pool snapshots (Offline), they do not appear in the pools list.
Creation Date	The time stamp that shows the date and time the original pool was snapped.
Size	The current size of the pool snapshot. The pool's snapshot can continue to add metadata for the snapshot until it reaches the size allocated.

To view details of a pool snapshot:

- 1 In iManager, log on to the tree for the server you want to manage.
- 2 In Roles and Tasks, click Storage > Pool to open the Pool Management task
- 3 Select the server that contains the original pool of the snapshot you want to view.
- 4 In the Pools list, select the original pool of the snapshot you want to view, then click Snapshot.
This opens the Pool Snapshot page.
- 5 Select the snapshot, then view its details in the Details field.
It can take a few seconds for iManager to load the details about the snapshot.

Renaming a Pool Snapshot

You can rename a pool snapshot. For example, you might want to assign a new name for the pool snapshot to correspond to a similar name change to its original pool.

- 1 In iManager, log on to the tree for the server you want to manage.
- 2 In Roles and Tasks, click Storage > Pool to open the Pool Management task
- 3 Select the server that contains the original pool of the snapshot you want to view.
- 4 In the Pools list, select the original pool of the snapshot you want to view, then click Snapshot.
This opens the Pool Snapshot page.
- 5 Select the snapshot in the Snapshots list.
It can take a few seconds for iManager to load the details about the snapshot.
- 6 Click Rename.
This opens the Pool Snapshot Rename wizard. For information about naming conventions in NetWare 6.5, see [“Naming NSS Storage Objects” on page 52](#).
- 7 Specify the new name you want for the pool snapshot.
- 8 Click Finish to accept the new name, or click Cancel to back out of the process.

When the page refreshes, you can see the renamed pool snapshot in the Snapshots list.

Activating and Deactivating a Pool Snapshot

Although the pool snapshot is inactive by default, the snapshot functions are working in the background to capture any changes being made to the original pool. For pool snapshots, Deactive and Active are conditions related to the visibility of the pool snapshot to users as a pool. Active pool snapshots are online; inactive pool snapshots are offline.

To take a pool snapshot offline from the Pool Management page, see [“Moving an Active Pool Snapshot Offline” on page 124](#).

To activate or deactivate a pool snapshot for user access as a pool:

- 1 In iManager, log on to the tree for the server you want to manage.
- 2 In Roles and Tasks, click Storage > Pool to open the Pool Management task
- 3 Select the server that contains the original pool of the snapshot you want to view.
- 4 In the Pools list, select the original pool of the snapshot you want to view, then click Snapshot.
This opens the Pool Snapshot page.

5 Select one or more pool snapshots that you want to manage, then modify the state:

- ◆ **Online** To change the state of the pool from Deactive to Active, click Online.

This makes the selected pool snapshots and all the volumes in them available for user access.

- ◆ **Offline** To change the state of the pool from Active to Deactive, click Offline.

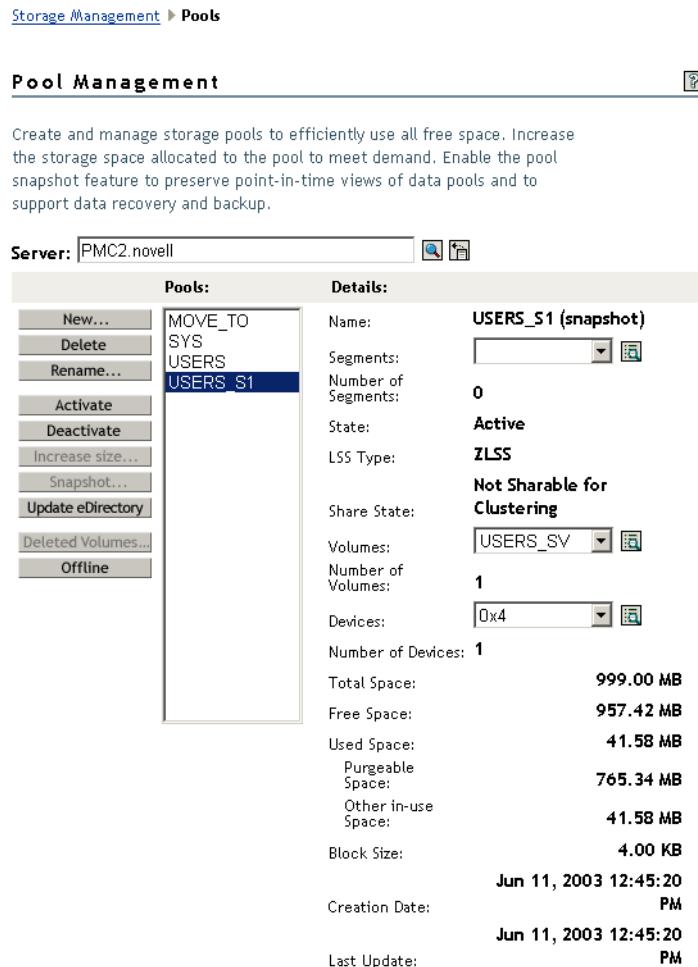
This makes the selected pool snapshots and all the volumes in them temporarily unavailable to users. It does not destroy volumes in the snapshots, nor does it destroy the data contained in the volumes.

Moving an Active Pool Snapshot Offline

When online, pool snapshots appear and function as a regular pool in the Pools list on the Pools Management Page. (See [Figure 5 on page 124](#).)

For information about creating and managing pool snapshots, see [“Benefits of Pool Snapshots” on page 115](#).

Figure 5 Sample Pool Snapshot When Online



To move an active pool snapshot offline:

- 1 In iManager, click Storage > Pools.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of pools appears in the Pools list.

- 3 Select the pool snapshot that you want to move offline.

Wait for the page to refresh. It displays the pool’s details and enables its management options.

- 4 Verify that the pool you selected is the pool snapshot and not the original pool.

If it is a snapshot, in the Details area, the name of the pool should be followed “(snapshot)” and the Offline button is activated.

- 5 Click Offline.

Deleting a Pool Snapshot

Use the Delete option to permanently remove one or more selected pool snapshots from the server. Deleting a pool snapshot removes the ownership of the space it occupied, freeing the space for reassignment.

IMPORTANT: If you create a pool snapshot and specify its stored-on pool as the same pool where its original data resides, and more than one pool snapshot exists when you are ready to delete a snapshot, delete its oldest snapshot in a first created, first deleted sequence.

To delete a pool snapshot:

- 1 In iManager, click Storage > Pools.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of pools appears in the Pools list.

- 3 In the Pools list, select the pool that has a snapshot you want to delete.

Wait for the page to refresh. It displays the pool’s details and enables its management options.

If a pool snapshot is online, it might appear in the Pools list. If the selected pool is a snapshot pool, in the Details area, the name of the pool should be followed “(snapshot)” and the Offline button is activated. If you select a pool snapshot in the Pools list, the page refreshes and enables the Snapshot option.

- 4 Click Snapshot.

If the selected pool has snapshots available or is an online pool snapshot, the Pool Snapshot page opens. If the selected pool has not pool snapshots associated with it, the Snapshot

- 5 On the Pool Snapshot page, select one or more snapshots in the Snapshots list that you want to delete.

Verify that the pool snapshots you selected are the versions you want to delete.

- 6 Click Delete.

- 7 A message requests you to confirm (Yes) or back out of (Cancel) this action.

Modifying the Stored-On Pool

After you specify a stored-on pool, that pool is the default stored-on pool for all subsequent snapshots made of the original pool. To modify the stored-on pool associated with an original pool, you must delete all existing snapshots for the original pool, then begin again to create a new pool.

Managing Pool Snapshots Using Commands

The following table shows the server console commands you can use to manage pool snapshots.

Snapshot Management Commands	Description
<code>mm snap create <i>snappool</i> <i>datapool</i> <i>snapname</i></code>	Creates a pool snapshot.
<code>mm snap activate <i>snapname</i></code>	Activates a pool snapshot.
<code>mm snap deactivate <i>snapname</i></code>	Deactivates a pool snapshot.
<code>mm snap delete <i>snapname</i></code>	Deletes a pool snapshot.
<code>mm snap rename <i>snapname</i> <i>newsnapname</i></code>	Renames the pool as specified
<code>mm snap shred <i>snapname</i> = on</code>	Turns on shredding for the internal volume of the pool where the snapshot is stored. For information, see “ Deleting Pool Snapshots ” on page 119 .
<code>mm snap shred <i>snapname</i> = off</code>	Turns off shredding for the internal volume of the pool where the snapshot is stored. For information, see “ Deleting Pool Snapshots ” on page 119 .
<code>mm snap list</code>	Lists the snapshots on the server.

The following table shows the attribute descriptions for pool snapshot commands.

Attributes for Pool Snapshot Commands	Description
<code>snappool</code>	The unique name of the original data pool that you are snapping; must be 2 to 16 characters.
<code>datapool</code>	The unique name of the stored-on pool for the pool snapshot; must be 2 to 16 characters.
<code>snapname</code>	The unique snapshot name of the pool snapshot, which will be used as its pool name when the pool snapshot is activated; must be 2 to 16 characters.

11

Managing NSS Volumes

Novell® Storage Services™ uses storage volumes to logically organize your data. After creating NSS pools, you can create any number of NSS volumes for each pool, depending on the physical space available.

This section describes how to configure NSS volumes by completing the following tasks:

- ◆ “Understanding NSS Volumes” on page 128
- ◆ “Understanding Volume Attributes” on page 128
- ◆ “Configuring Nonencrypted NSS Volumes with iManager” on page 131
- ◆ “Configuring Encrypted NSS Volumes with NSSMU” on page 133
- ◆ “Updating eDirectory Volume Objects” on page 133
- ◆ “Viewing the Details of a Volume” on page 134
- ◆ “Viewing Properties of a Volume” on page 134
- ◆ “Modifying Attributes of an NSS Volume” on page 137
- ◆ “Renaming an NSS Volume” on page 137
- ◆ “Activating and Deactivating an NSS Volume” on page 138
- ◆ “Activating and Deactivating CDs and DVDs as NSS Volumes” on page 138
- ◆ “Activating and Deactivating CD and DVD Image Files as NSS Volumes” on page 139
- ◆ “Activating and Deactivating DOS Partitions as NSS Volumes” on page 140
- ◆ “Mounting and Dismounting an NSS Volume” on page 140
- ◆ “Mounting a USB Floppy Disk as a Local FAT Volume” on page 140
- ◆ “Deleting an NSS Volume” on page 141
- ◆ “Verifying and Rebuilding NSS Pools and Volumes” on page 142
- ◆ “Controlling Access to the Admin Volume and Files.cmd File” on page 143
- ◆ “Using Data Shredding to Prevent Access to Deleted Files” on page 147
- ◆ “Configuring Read Ahead Blocks Parameters” on page 149
- ◆ “Using the Flush Files Immediately Attribute to Protect Against Possible Data Corruption on System Failure” on page 149
- ◆ “Using the Transaction Tracking System for Application-Based Transaction Rollback” on page 151
- ◆ “Using the File-Level Snapshot Attribute to Enable the Backup of Open Files” on page 152
- ◆ “Configuring the NSS Volume Salvage Area” on page 157

- ◆ “Viewing, Salvaging, or Purging Deleted NSS Volumes” on page 158
- ◆ “Salvaging or Purging Deleted Files” on page 160
- ◆ “Understanding Space Quotas” on page 161
- ◆ “Managing NSS Volume Quotas” on page 162
- ◆ “Managing Directory Quotas” on page 164
- ◆ “Managing User Space Quotas” on page 167
- ◆ “What’s Next” on page 171

Understanding NSS Volumes

NSS volumes are logical storage media that acquire space from pools of storage. When you create a logical volume, you can either assign it a fixed amount of space or allow it to expand to the pool size. To grow a volume, you might need to add new segments to grow the pool first, up to the maximum pool size of 8 TB. On NetWare®, you can also use Novell Distributed File Services Move and Split functions to relocate the volume (or part of a volume) to a new pool on the same or different server in the same tree.

If a pool contains multiple volumes, the cumulative administrative maximum sizes of all volumes can exceed the pool size, using the overbooking feature, although real total size is bound by physical limitations. Because space is allocated to volumes as needed, a volume might not reach its quota. As the overbooked volumes consume the available physical space, you need to add more disk space to the pool to accommodate the growth, or consider moving or splitting volumes to move data to other pools.

For example, suppose you have an 800 MB storage pool with eight volumes set at 100 MB each. The administrative size equals the physical limits. To overbook the pool, you can add volumes, set one or more of the volumes to expand to the pool size, or increase the size of existing volumes, with the understanding that these are administrative maximum sizes, not physical sizes.

NSS recognizes DOS, Macintosh, UNIX, and Long name spaces. Volume names, directory names, and file names in NSS are case insensitive.

After you create NSS pools, use the iManager Storage plug-in to configure NSS storage volumes. For information, see “[Novell iManager Storage Plug-In](#)” on page 29. For information about iManager, see the *Novell iManager 2.5 Administration Guide*.

You can also use the console-based NSS Management Utility to configure and manage NSS volumes. For information about NSSMU, see “[NSSMU](#)” on page 41.

Understanding Volume Attributes

The following volume attributes determine the services and characteristics of an NSS volume:

- ◆ “Encryption” on page 129
- ◆ “Data Shredding” on page 129
- ◆ “Compression” on page 129
- ◆ “Data Migration” on page 129
- ◆ “Directory Quotas” on page 129
- ◆ “User Space Quotas” on page 130

- ◆ “Salvage Files” on page 130
- ◆ “Read Ahead Blocks in Volumes” on page 130
- ◆ “Flush Files Immediately” on page 130
- ◆ “User-Level Transaction Model” on page 130
- ◆ “File-Level Snapshot” on page 130
- ◆ “Modified File List” on page 131
- ◆ “Backup” on page 131

Encryption

Encrypted volume support is provided for NSS volumes in NetWare 6.5 Support Pack 2 and later. The Encryption attribute enables password-protected activation of NSS volumes on NetWare. Encryption is activated at creation time only and persists for the life of the volume. The sys: volume cannot be encrypted.

This attribute is currently not available if you create an NSS volume with iManager; use NSSMU to create an encrypted volume on your NetWare server. For information, see “[Managing Encrypted NSS Volumes](#)” on page 171.

Data Shredding

The Data Shredding attribute allows you to electronically overwrite deleted and purged data areas to prevent unauthorized users from using a disk editor to access purged files. You can specify the number of times (1 to 7) to shred data. A value of 0 (zero) disables data shredding. For information, see “[Using Data Shredding to Prevent Access to Deleted Files](#)” on page 147.

Compression

The Compression attribute activates file compression in NSS volumes. Compression can be activated at creation time only and this choice persists for the life of the volume. Data in the volume might be stored normally or in compressed form, depending on how frequently it is used. Compression parameters can be set at the server level to control compression behavior.

For information about configuring compression parameters, see “[Using Compression to Conserve Storage Space on NSS Volumes](#)” on page 177.

Data Migration

The Data Migration attribute sets a flag that indicates to third-party software that this volume’s data can be migrated to near-line or offline storage media after it is inactive for specified lengths of time. This attribute requires third-party software to take advantage of the capability.

Directory Quotas

The Directory Quotas attribute activates a feature that lets you assign a maximum quota of space a directory can consume. For information about configuring space restrictions, see “[Managing Directory Quotas](#)” on page 164.

User Space Quotas

The User Space Quotas (user space restrictions) attribute enables you assign a maximum quota of space that a user's data can consume across all directories in the volume. For information about configuring space restrictions, see [“Managing User Space Quotas” on page 167](#).

Salvage Files

The Salvage Files attribute enables deleted files to remain on the volume until the Purge Delay time expires or until space is needed on the volume for other data. Until the Purge Delay time expires, the Salvage feature tracks the deleted files and allows the deleted files to be salvaged and restored. If space is needed, the oldest deleted files are purged to clear space.

If the Salvage Files attribute is disabled, deleted files are purged immediately on deletion.

For information, see the following:

- ◆ [“Configuring the NSS Volume Salvage Area” on page 157](#)
- ◆ [“Viewing, Salvaging, or Purging Deleted NSS Volumes” on page 158](#)
- ◆ [“Salvaging or Purging Deleted Files” on page 160](#)

Read Ahead Blocks in Volumes

The Read Ahead Blocks attribute specifies the number of data blocks that NSS reads ahead for any open file on which read operations are ongoing in the specified server.

For information, see [“Configuring Read Ahead Blocks Parameters” on page 149](#)

Flush Files Immediately

The Flush Files Immediately attribute enables NSS to immediately write to disk all data in cache that is pending writes to the file when you close the file. Otherwise, the data in cache must wait until the next write cycle to be written to the disk, putting the information at risk for loss during the interim, for example, if the server failed.

For information, see [“Using the Flush Files Immediately Attribute to Protect Against Possible Data Corruption on System Failure” on page 149](#).

User-Level Transaction Model

The User-Level Transaction Model enables the Transaction Tracking System™ (TTS™) function for this volume. TTS protects database applications by backing out transactions that are incomplete because of a system failure. For information, see [“Using the Transaction Tracking System for Application-Based Transaction Rollback” on page 151](#).

File-Level Snapshot

The File-level Snapshot attribute enables a backup utility to capture the last closed version of a file that is open at the time a backup is in progress. You must manually deactivate the volume, then activate the volume after setting this attribute to let the volume set up the virtual volume for the metadata about file snapshots.

If the File Snapshot attribute is enabled, Novell Storage Management Services™ (SMS) saves the snapshot version of the file to backup media if a file is in use when the backup occurs. Some third-party backup applications also can take advantage of this attribute.

For more information, see “[Using the File-Level Snapshot Attribute to Enable the Backup of Open Files](#)” on page 152.

Modified File List

The Modified File List (MFL) attribute enables NSS to create a list of all files modified since the previous backup. The log is available only through third-party software.

Backup

The Backup attribute sets a flag to indicate to the backup software that the volume contains data you want to back up. Disable this flag if the volume is empty or if backing up the data is unnecessary. This backup flag is independent of the third-party backup system you use; your backup system might not recognize this option, even if you select it.

Configuring Nonencrypted NSS Volumes with iManager

This section describes how to create and configure attributes for a nonencrypted volume. For information on creating encrypted volumes, see “[Managing Encrypted NSS Volumes](#)” on page 171.

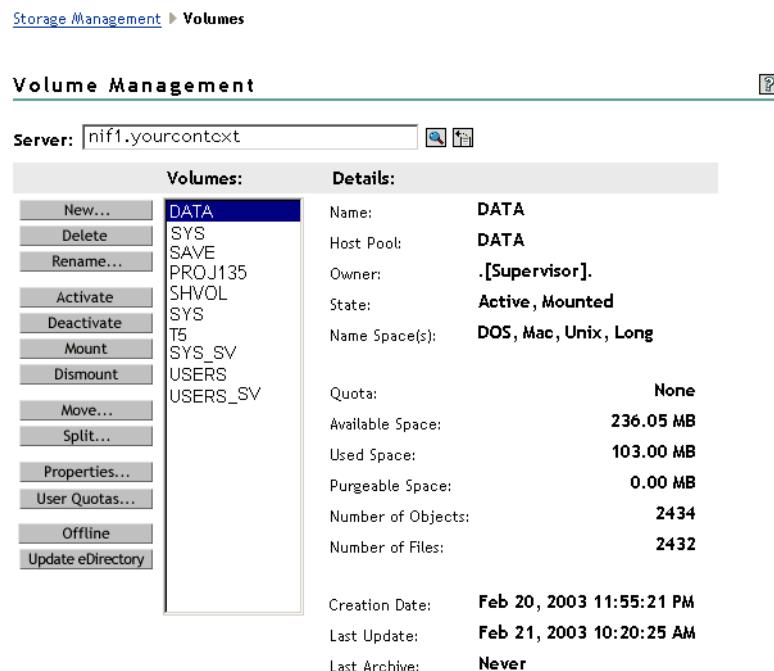
1 In iManager, click Storage > Volumes.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of volumes appears in the Volumes list.



The screenshot shows the iManager Volume Management interface. The top navigation bar includes 'Storage Management' and 'Volumes'. The main window has a 'Volume Management' title bar with a help icon. A sidebar on the left is titled 'Server: nif1.yourcontext' and contains a list of actions: New..., Delete, Rename..., Activate, Deactivate, Mount, Dismount, Move..., Split..., Properties..., User Quotas..., Offline, and Update eDirectory. The main content area is titled 'Volumes' and 'Details:' and lists the following volumes and their details:

Volumes:	Details:
DATA	Name: DATA
SYS	Host Pool: DATA
SAVE	Owner: .[Supervisor].
PROJ135	State: Active, Mounted
SHVOL	Name Space(s): DOS, Mac, Unix, Long
SYS	Quota: None
T5	Available Space: 236.05 MB
SYS_SV	Used Space: 103.00 MB
USERS	Purgeable Space: 0.00 MB
USERS_SV	Number of Objects: 2434
	Number of Files: 2432
	Creation Date: Feb 20, 2003 11:55:21 PM
	Last Update: Feb 21, 2003 10:20:25 AM
	Last Archive: Never

3 To create a new volume, click **New**.

This opens 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. You must click **Cancel** to back out of the wizard, then begin the move process again. For guidelines about naming volumes, see “[Naming NSS Storage Objects](#)” on page 52.

5 Specify the pool on the new location where you want the new volume to reside, then click **Next**.

Only pools that have free space appear in the list. If no pools are listed, there is no space available to create a volume in the existing pools. Cancel the wizard, then add more devices to the server and expand the pool or free up space on existing pools. When you are done, return to the **Volume Management** page to create the new volume.

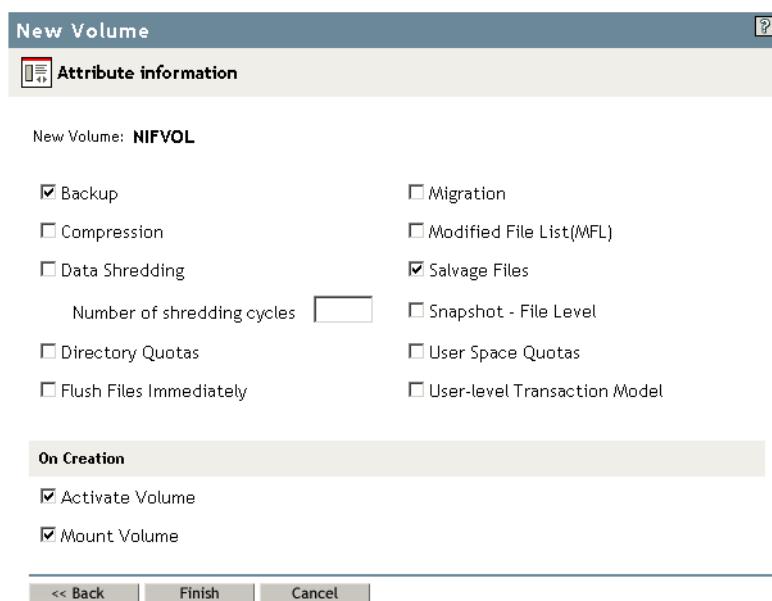
6 Specify the size of the volume:

- ♦ Specify a quota size for the volume if you want to limit the size of the volume.
- ♦ Select **Allow Volume Quota to Grow to the Pool Size** if you want the volume to expand to the size of the pool.

Pools can be overbooked; each volume can potentially grow to the size of the pool. NSS allocates space as it is needed.

7 On the **Volume Attributes** page, set the attributes for the new volume you are creating.

For information, see “[Understanding Volume Attributes](#)” on page 128.



8 In 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 Click **Finish**.

Configuring Encrypted NSS Volumes with NSSMU

In NetWare 6.5 Support Pack 2 and later, NSS Encrypted Volume Support (EVS) allows you to create encrypted NSS volumes using NSSMU. You cannot encrypt the sys: volume. You can create encrypted user data volumes only after the installation or upgrade process. For information, see [“Managing Encrypted NSS Volumes” on page 171](#).

Updating eDirectory Volume Objects

In Novell eDirectory™, each NSS volume is represented by a Volume object. Volume objects are leaf objects that represent a physical or logical volume on the network.

The Volume object's properties contains the following information:

- ◆ The NetWare server where the volume resides
- ◆ The volume name recorded when the volume was initialized on the server (for example, sys:)
- ◆ The volume's owner (login username of the administrator who created it)
- ◆ Space use restrictions for users
- ◆ A description of the volume's use
- ◆ Statistical information on disk space availability, block size, directory entries, name space support, and so on.

Usually, NSS creates the Novell eDirectory Volume object when you create the volume and updates the properties of the volume as needed. The Update eDirectory option on the Volume Management page allows you to add, keep, or replace a Volume object for a selected volume at the same context level as the server.

When you select Update eDirectory, NSS searches for the object.

- 1 In iManager, click Storage > Volumes.

For instructions, see [“Accessing NSS Storage Management Role and Tasks” on page 34](#).

- 2 Select a server to manage.

For instructions, see [“Selecting a Server to Manage” on page 35](#).

A list of volumes appears in the Volumes list.

- 3 Select the volume you want to update.

Wait for the page to refresh and display the details.

- 4 Click Update eDirectory.

Wait while NSS searches for the Volume object in the server context.

- 5 Do one of the following:

- ◆ If the Volume object does not exist, NSS adds the Volume object to the context level. Confirm the addition.
- ◆ If the Volume object exists, NSS prompts you with two options: Delete and Replace the existing object or Retain the existing object. Select one option and confirm your choice.

Viewing the Details of a Volume

- 1 In iManager, click Storage > Volumes.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of volumes appears in the Volumes list.

- 3 In the Volumes list, select a volume that you want manage.

When the page refreshes, the details for the volume appear in the Details area. The volume must be mounted and active for the details to be available.

- 4 To activate the volume, select the volume, then click Activate.

Viewing Properties of a Volume

After you set up and configure NSS volumes, you can view the properties, such as attribute settings, volume statistics, and volume usage.

- 1 In iManager, click Storage > Volumes.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 Select a server to manage.

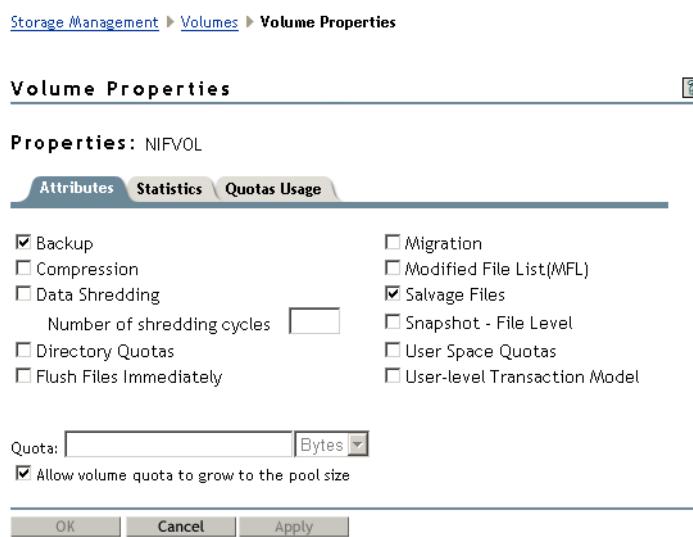
For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of volumes appears in the Volumes list.

- 3 In the Volumes list, select a volume that you want manage.

- 4 Click Properties.

The Properties page has three tabs: Attributes, Statistics, and Volume Quota. It opens by default to the Attributes tab.



Use the Attributes page to view the volume's attribute configuration and the volume quota. For information about modifying attributes, see [“Modifying Attributes of an NSS Volume” on page 137](#).

- 5 Click the Statistics tab to view the current space usage statistics for the selected volume.

[Storage Management](#) ▶ [Volumes](#) ▶ [Volume Properties](#)

Volume Properties ?

Properties: NIFVOL

Attributes **Statistics** **Quotas Usage**

Compression		Salvage	
Compressed Space:	0.00 Bytes	Minimum Keep Seconds:	
Files:		Maximum Keep Seconds:	0
Not Deleted:	0	Low Water Mark:	10
Deleted:	0	High Water Mark:	20
Uncompressed:	0	Next Scheduled Purge	
		Purgeable Space:	0.00 MB
		Unpurgeable Space:	0.00 MB
		Deleted Files:	0
		Oldest Deleted Time:	0

GUID: **A7942770-9C3E-01D7-80-00-1A1A3BF816F4**
 Block Size: **4.00 KB**

Close

- 6 Click the Quotas Usage tab to view the volume and pool space usage for the selected volume.

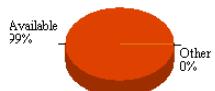
[Storage Management](#) ▶ [Volumes](#) ▶ [Volume Properties](#)

Volume Properties ?

Properties: NIFVOL

Attributes **Statistics** **Quotas Usage**

Volume Usage: NIFVOL **Pool Usage:** NIFPOOL



Available
99%

Other
0%



Free
90%

Used
9%

Quota:	none	Available Space:	89.93 MB
Used Space:	576.00 KB	Free:	89.93 MB
Compressed:	0.00 Bytes	Purgeable:	0.00 MB
Other in-use space:	576.00 KB	Total Space:	99.00 MB
Purgeable Space:	0.00 MB	Used:	9.07 MB
Available Space:	89.93 MB	Booked:	0.00 MB

This pool contains logical volumes with no quotas. They were not used to calculate the booking.

Close

Modifying Attributes of an NSS Volume

After you set up and configure NSS volumes, you can modify most of the attribute settings. Encrypted Volume Support attribute and Compression attribute can be set only at the time the volume is created. If you try to modify those settings, iManager returns an error message. You can also specify a Volume Quota.

- 1 In iManager, click Storage > Volumes.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of volumes appears in the Volumes list.

- 3 In the Volumes list, select a volume that you want manage.

- 4 Click Properties.

The Properties page has three tabs: Attributes, Statistics, and Volume Quota. Use the Attributes page to view or modify the attributes for the selected volume.

- 5 Do one or more of the following:

- ♦ Select or deselect a modifiable attribute, then click Apply.

The Encryption and Compression attributes can be set only at the time the volume is created. If you try to modify those settings, iManager returns an error message.

For information about attributes, see “[Understanding Volume Attributes](#)” on page 128.

- ♦ Specify a volume quota, then click Apply.

Renaming an NSS Volume

You can rename NSS volumes. For example, you might want to change the name of a volume to reflect the department or organization that uses it.

- 1 In iManager, Storage > Volumes.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of volumes appears in the Volumes list.

- 3 In the Volumes list, select a volume.

- 4 Click Rename.

The Rename Volume wizard opens.

- 5 Specify the new name of the volume.

- 6 Click Finish.

After the page refreshes, the volume appears in the Volumes list with its new name.

Activating and Deactivating an NSS Volume

After you set up and configure NSS volumes, you can activate and deactivate volumes to make them available to users and applications. To view details of a volume, it must be active.

1 In iManager, Storage > Volumes.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of volumes appears in the Volumes list.

3 In the Volumes list, select one or more volumes that you want to make active or deactivate.

4 Depending on the state of the volume, click Activate or Deactivate.

After the page refreshes, you can see can see that each volume’s state matches the state you specified.

Activating and Deactivating CDs and DVDs as NSS Volumes

You can activate CDs and DVDs as NSS volumes through the cddvd.nss module. The cddvd.nss module replaces cdrom.nlm and cd9660.nss for CD support, udf.nss for DVD support, and cdhfs.nss for Macintosh* CD support. When you load cddvd.nss, it uses the same set of switches (UpdateCDToNDS, LoginUpdateToNDS, LeaveCDInNDS, and LockCDMediaIn) that were used in the previous commands.

Cddvd.nss supports the following disk formats:

- Universal Disc Format (UDF) for DVDs
- ISO 9660 for CDs
- Hierarchical File System (HFS) for Macintosh CDs

By default, cddvd.nss loads the formats in sequential order, with the UDF format for DVDs first, ISO9660 for CDs next, and CDHFS for Macintosh CDs last.

If a CD or DVD is in a drive when cddvd.nss loads, the disk is immediately activated as an NSS volume. Whenever the cddvd.nss module recognizes a newly inserted CD or DVD, it immediately activates the disk as a read-only NSS volume.

The volume name is the CD or DVD volume label, if one exists, and is acceptable to NetWare. Otherwise, cddvd.nss generates a volume name in this form: CD_xxxx (where x is a number). This volume functions the same as any other NetWare volume, except that it is read-only.

Although the NSS volume is activated, it is not automatically added to Novell eDirectory. You can add it to eDirectory later by enabling a cddvd.nss switch, such as

```
nss /UpdateCDtoNDS=cdname
```

Loading and Unloading the Cddvd.nss Module

The cddvd.nss module loads automatically when NSS starts. To load cddvd.nss manually, enter the following at the server console:

```
load cddvd.nss
```

To unload cddvd.nss, enter the following at the server console

```
unload cddvd.nss
```

Load Order of Formats for Dual-Formatted Drives

Disks in dual-formatted CD/DVD drives are activated as one volume and the format is decided by cddvd.nss. If you have an ISO/UDF bridge disk, which supports both ISO 9660 and UDF formats, you can instruct NSS to load ISO 9660 first by entering the following command at the server console.

```
nss /LoadISOVolumeFirst
```

Activating and Deactivating CD and DVD Image Files as NSS Volumes

In NetWare 6.5 Support Pack 2 and later, the cddvd.nss module allows you to activate a CD or DVD image file as a read-only NSS volume, if the source file resides on an existing NSS volume. You add the image file as a volume with the MountImageVolume switch. This volume functions the same as any other NSS volume, except that it is read-only. You remove it as a volume with the RemoveImageVolume switch.

While the CD or DVD image file exists on the server as an NSS volume, the following actions cause the image file to be removed as an NSS volume:

- Any file operations on the image source file, such as open, read, or write
- Deactivation of the NSS volume where the image source file resides

To activate a CD or DVD image file as an NSS volume, at the system prompt, enter

```
nss /MountImageVolume=path_imagefilename
```

Replace *path_imagefilename* with the path on the NSS volume where the image file resides, including its filename. For example:

```
nss /MountImageVolume=nssvol:\nw65_3.iso
```

You can mount and dismount the volume as with normal volumes, until you remove it by entering the following:

```
nss /RemoveImageVolume
```

Commands	Description
<pre>nss /MountImageVolume=path_imagefilename</pre>	<p>Add and mount the specified CD or DVD image file as a read-only NSS volume.</p> <p>Replace <i>path_imagefilename</i> with the path on the NSS volume where the image file resides, including its filename. For example:</p> <pre>nss /MountImageVolume=nssvol:\nw65_3.iso</pre>
<pre>nss /RemoveImageVolume=path_imagefilename</pre>	<p>Dismount and remove the specified CD or DVD image file as a read-only NSS volume.</p> <p>Replace <i>path_imagefilename</i> with the path on the NSS volume where the image file resides, including its filename. For example:</p> <pre>nss /RemoveImageVolume=nssvol:\lsuse9_1.iso</pre>

Activating and Deactivating DOS Partitions as NSS Volumes

After you load the dosfat.nss module, any DOS FAT partitions are dynamically made available as NSS volumes. The volume name displayed by the NetWare Volumes command is dosfat_x, where x is the drive letter, for example dosfat_c.

The following are some benefits of the dosfat.nss module:

- **Long Filenames:** DOS filenames for file systems such as OS/2*. This uses the Windows 95/98/ME method for placing long names onto a DOS FAT partition.
- **NetWare Trustee Rights:** Only users with supervisor rights can access the volume.
- **NetWare Utilities:** Any client or server utility that accesses or manages NetWare volumes can do the same with DOS FAT partitions.
- **MAP command.** NetWare clients can map to the volume and use it as any other NetWare mapping.
- **Local partition.** Allows access to the local partition.

Mounting and Dismounting an NSS Volume

After you set up and configure NSS volumes, you can mount and dismount volumes to make them available to users and APIs. After you mount a volume, it is only available to APIs until you activate it. Dismounting a volume makes it unavailable to users and to APIs.

1 In iManager, Storage > Volumes.

For instructions, see [“Accessing NSS Storage Management Role and Tasks” on page 34](#).

2 Select a server to manage.

For instructions, see [“Selecting a Server to Manage” on page 35](#).

A list of volumes appears in the Volumes list.

3 In the Volumes list, select one or more volumes that you want to mount or dismount.

4 Depending on the state of the volume, click Mount or Dismount.

After the page refreshes, you can see that the volume’s state changed. The details of dismounted volumes are not available on the iManager Volume Management page.

Mounting a USB Floppy Disk as a Local FAT Volume

If your server uses a USB floppy drive, NetWare 6.5 does not mount floppies automatically during the server installation. You might need to manually mount a floppy disk to install the NetWare 6.5 license.

Local File Allocation Table (FAT) volumes are available to the server but are not seen by users. By default, NetWare 6.5 does not automatically mount local FAT volumes such as the floppy disk in a USB floppy drive. Use the Local Fat Volume Mount (LFVMount) command to detect and mount any local FAT volumes not recognized by DOS and assign them a local drive letter.

To mount local FAT volumes, enter the following at the system console prompt:

```
lfvmount
```

The LFVMount command affects only the current local FAT volumes. For example, you must re-enter this command each time you change a floppy disk in the USB floppy drive.

Use the associated SET parameter (set auto lfvmount=<on | off (default)>) to configure automatic detection. If set to On, NetWare automatically detects and mounts local FAT volumes as you insert the media into the drive and then assigns drive letters to them. If set to Off (default), NetWare does not automatically detect and mount local FAT volumes; you must use the LFVMount command to manually mount them as needed.

To automatically mount local FAT volumes for a server, enter the following at the system console prompt:

```
set auto lfvmount=on
```

To prevent the automatic mounting of local FAT volumes for a server, enter the following at the system console prompt:

```
set auto lfvmount=off
```

If entered at the system console, the associated SET parameter remains in effect until you change it or until you reboot the server.

To make the SET parameter persistent through a server reboot, add one of the following commands in the startup.ncf file:

- ♦ set auto lfvmount=on
- ♦ set auto lfvmount=off

If no value is set in the startup.ncf file, NetWare does not automatically mount the local FAT volumes. You must use the LFVMount command to manually mount local FAT volumes as needed.

The Local Fat Volumes (lfvolumes) command displays a list of local FAT volumes that are currently mounted and provides detailed information about them.

To list information about local FAT volumes mounted on the server, enter the following at the system console prompt:

```
lfvolumes
```

The LFVMount command appears in the console-based help for console commands.

For help with the LFVMount command, enter one of the following at the system console prompt:

- ♦ **help mount**
- ♦ **help lfvmount**

Deleting an NSS Volume

Deleting a volume removes the data in the volume and frees the space to be used by other volumes in the same pool. When you delete a volume, it remains for salvageable until one of the following events occurs:

- ♦ Volume Purge Delay times out. The deleted volume is purged automatically. For information, see [“Setting the Purge Delay for the Salvage Area” on page 158](#).
- ♦ The available space on the server falls below the Low Watermark. Deleted volumes are purged until enough space is cleared so that the available space increases above the High

Watermark. For information, see “[Setting the Low and High Watermarks for Purging the Salvage Area](#)” on page 158.

- ◆ You manually purge the deleted volume. For information, see “[Viewing, Salvaging, or Purging Deleted NSS Volumes](#)” on page 158.

During that time, the space belonging to the deleted volume is not available to other volumes and the volume is salvagable. Once the purging process begins, the volume is no longer salvagable.

If it is necessary, you can restore a deleted volume before it is purged. See “[Viewing, Salvaging, or Purging Deleted NSS Volumes](#)” on page 158.

You cannot delete a sys: volume using iManager. Deleting a sys: volume removes the operating system. You need to reinstall NetWare to delete a sys: volume. However, if the sys: volume you want to delete does not contain the active operating system (for example, a remnant on a previously used disk), you can rename the volume, then delete it.

- 1 In iManager, click Storage > Volumes.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of volumes appears in the Volumes list.

- 3 Select one or more volumes that you want to delete.

Wait for the page to refresh and make the Delete option available for the selected volume.

- 4 Click Delete.

- 5 Click Yes to confirm the deletion, or click No to cancel the deletion.

WARNING: If you click Yes, the volumes and data on them are immediately destroyed.

Verifying and Rebuilding NSS Pools and Volumes

NSS allows you to temporarily deactivate individual storage pools to fix volume problems instead of bringing down the server. However, when you deactivate a storage pool, users do not have access to any of the volumes in that pool. You cannot rebuild or verify an NSS volume independently of other volumes in the same pool.

- ◆ “[Mounting the Volume to Repair Journalized Errors](#)” on page 142
- ◆ “[Verifying the Pool to Repair Inconsistent Data Blocks](#)” on page 143
- ◆ “[Restoring the Data from Backup](#)” on page 143
- ◆ “[Rebuilding the Pool](#)” on page 143
- ◆ “[Error and Log Files](#)” on page 143

Mounting the Volume to Repair Journalized Errors

Volume errors are typically transactions left unfinished during a system crash of some kind. This type of error is fixed automatically during volume mount by the journaling feature. If the errors persist, NSS requires you to use the Verify and Rebuild utilities to resolve any problems.

Verifying the Pool to Repair Inconsistent Data Blocks

The Verify option fixes NSS pools and volumes by searching for inconsistent data blocks or other errors. This utility indicates if there are problems with the file system. If there are no problems with the pool, it is safe to activate the pool.

The PoolVerify command is a read-only assessment of the pool. At the server console, enter

```
nss /poolverify
```

Select the pool name from the displayed list.

Restoring the Data from Backup

If you still have problems with the pool, consider whether there is a satisfactory backup available to restore your system. If restoring from backup is not an option, use the Rebuild utility.

Rebuilding the Pool

Rebuild verifies and uses the existing leaves of an object tree to rebuild all the other trees in the system.

IMPORTANT: The Verify and Rebuild utilities are not the same as the Vrepair command (used to rebuild Traditional volumes). You should use Rebuild only as a last resort to recover the file system after data corruption.

- 1 Deactivate the pool before you run Rebuild so users cannot access its volumes while you are rebuilding.

When you deactivate a storage pool, all the volumes in the pool automatically deactivate.

- 2 Run Pool Rebuild by entering the following commands at the server console:

```
nss /poolrebuild=poolname
```

This verifies and accounts for all blocks in the system. If the volume has errors, the errors appear on the screen. The NSS volume remains in maintenance mode; otherwise, it reverts to the active state.

- 3 When the rebuild is done, mount the volume.

Error and Log Files

When you use Rebuild and Verify a log file is generated at the root of the DOS drive. The error log, *sys:pool_name.vlf*, contains information about data that has been lost or recovered. Data loss, unfortunately, is a possibility during a rebuild.

Rebuild also copies errors and transactions into an error file called *volume_name.rlf* at the root of the DOS drive on your server. Every time you rebuild a particular NSS volume, the previous error file is overwritten. If you want to keep old error files, move them to another location. You can monitor the error file whenever an NSS volume does not come up in active mode after a rebuild.

Controlling Access to the Admin Volume and Files.cmd File

On your NetWare server, the *_admin:\manage_nss\files.cmd* file enables applications, such as NetStorage and other end-user browser-based tools, to communicate with the file server. The *files.cmd* file is a virtual file; it generates dynamic information that lets users see and modify their files through a browser.

Every user on the file server has access to the _admin:\manage_nss\files.cmd and thus inherits the following default file system trustee rights: Read, Write, and Scan. These rights make the Admin volume (_admin:) visible to end users. This behavior differs from NetWare 6.0 and earlier servers, where the files.cmd file is not visible to end users. Although end users can see the files.cmd file, they cannot delete this file or modify its properties.

To restrict access to the _admin:\manage_nss\files.cmd file or the Admin volume, you must modify a configuration file called sys:\etc\trustees.xml. For information, see the following:

- ◆ “[Assigning Volume Rights with Trustees.xml \(NetWare\)](#)” on page 144
- ◆ “[Restricting Access to Files.cmd \(NetWare\)](#)” on page 146

For information about virtual files, see the [Virtual File Services for NetWare](http://developer.novell.com/ndk/doc/vfs/index.html?page=/ndk/doc/vfs_vfs_enu/data/h5ubo7tt.html) (http://developer.novell.com/ndk/doc/vfs/index.html?page=/ndk/doc/vfs_vfs_enu/data/h5ubo7tt.html) in the Novell Developer Kit Documentation Web site (<http://developer.novell.com/ndk/doc.htm>).

Assigning Volume Rights with Trustees.xml (NetWare)

Use the sys:\etc\trustees.xml file to assign file system trustee rights to the root of an NSS volume on NetWare. Trustees.xml is executed every time the server boots.

The sys:\etc\trustees.xml file is useful for assigning rights to non-persistent files or directories, such as the Admin volume or a CD that you have activated as an NSS volume.

Refer to the following table for information about sys:\etc\trustees.xml tags:

XML Tags	Explanation
<code><name></code>	<p>Enter the full context and username of the user. You can enter the information in slash-separated format or Novell dot format.</p> <p>NOTE: This tag cannot contain multiple usernames.</p> <p>For example, if John Smith existed in the novell context in the aurora_tree, you would enter one of the following:</p> <p><code>\aurora_tree\novell\jsmith</code> or <code>jsmith.novell.aurora_tree</code></p>
<code><filename></code>	<p>Enter the name of volume, directory, and file that you are assigning rights to.</p> <p>For example, if you are assigning rights to the hosts file in the etc directory located on the sys: volume, you would enter the following into the brackets</p> <p><code><filename>sys:\etc\hosts</filename></code></p>

XML Tags	Explanation
<rights>	<p>The child elements to the Rights tag include the following tags for file system rights:</p> <ul style="list-style-type: none"> ◆ <accesscontrol/> for the Access Control right ◆ <create/> for the Create right ◆ <edit/> for the Edit right ◆ <filescan/> for the File Scan right ◆ <modify/> for the Modify Metadata right ◆ <read/> for the Read right ◆ <supervisor/> for the Supervisor right ◆ <write/> for the Write right

The follow is a sample of the trustees.xml code:

```

<specialTrustees>

  <addTrustee>

    <name>admin.novell.kona_tree</name>
    <fileName>sys:\etc\group</fileName>
    <rights>

      <read/>
      <write/>
      <filescan/>
      <edit/>

    </rights>
  </addTrustee>

  <addTrustee>

    <name>xxxx.novell.kona_tree</name>
    <fileName>sys:\etc\group</fileName>
    <rights>

      <read/>
      <write/>
      <filescan/>

    </rights>
  </addTrustee>

  <addTrustee>

    <name>fred.novell.kona_tree</name>
    <fileName>sys:\etc\group</fileName>

```

```

<rights>
  <read/>
  <write/>
  <filescan/>
</rights>
</addTrustee>
<addTrustee>
  <name>[public]</name>
  <fileName>_admin:manage_nss\files.cmd</fileName>
  <rights>
    <read/>
    <write/>
    <filescan/>
  </rights>
  <background/>
</addTrustee>
<addTrustee>
  <name>fred.novell.kona_tree</name>
  <fileName>sys:\etc\hosts</fileName>
  <rights>
    <read/>
    <write/>
    <filescan/>
  </rights>
</addTrustee>
</specialTrustees>

```

Restricting Access to Files.cmd (NetWare)

If you want to restrict access to the _admin:\manage_nss\files.cmd, you must do so by modifying the <addTrustee> tag in the sys:\etc\trustees.xml file.

Look for this code sample in the .xml file and modify [public] to reflect the user that needs restricted access to the _admin:\manage_nss\files.cmd file:

```

<addTrustee>
  <name>[public]</name>
  <fileName>_admin:manage_nss\files.cmd</fileName>
  <read/>

```

```

<write/>
<filescan/>
<background/>
</addTrustee>

```

For example, if you want John Smith, a contract employee, to have only file scan rights to this file, you would enter the following:

```

<addTrustee>
  <name>jsmith.novell.kona_tree</name>
  <fileName>_admin:manage_nss\files.cmd</fileName>
  <rights>
    <filescan/>
  </rights>
  <background/>
</addTrustee>

```

For further explanation of the XML tags, see [“Assigning Volume Rights with Trustees.xml \(NetWare\)” on page 144](#).

Using Data Shredding to Prevent Access to Deleted Files

Data shredding hides deleted and purged files by overwriting them with random patterns of hexadecimal characters. This prevents unauthorized users from using a disk editor to access purged files.

If the Data Shredding attribute for an NSS volume is disabled, unauthorized access to data is possible. An individual can extend a file, LSEEK to the end of the existing file data, and then read the data. This returns the decrypted leftover data that is in the block.

You can place up to seven data shred patterns over deleted data. Data shredding truly erases files. Only files that have been purged are shredded, so there remains a grace period between when the file is deleted and then purged for users who might delete the wrong file.

Data shredding consumes a great deal of disk connection bandwidth, resulting in a performance penalty for using the disk and system resources needed to overwrite the shredded file. Unless you must use data shredding for security reasons, the Data Shredding attribute for your NSS volume can be disabled or set to a lower number of shredding passes.

This section discusses the following:

- ◆ [“Setting the Data Shredding Attribute When You Create a Volume” on page 147](#)
- ◆ [“Setting the Data Shredding Attribute for an Existing Volume” on page 148](#)
- ◆ [“Disabling Data Shredding for an Existing Volume” on page 148](#)

Setting the Data Shredding Attribute When You Create a Volume

When you create a volume, simply select the Data Shredding check box and specify the number of shredding cycles (or specify 0 to indicate no shredding capability) when you set the volume’s

attributes. For more information, see “Configuring Nonencrypted NSS Volumes with iManager” on page 131.

Setting the Data Shredding Attribute for an Existing Volume

1 In iManager, click Storage > Volumes to open the Volume Management page.

For instructions, see “Accessing NSS Storage Management Role and Tasks” on page 34.

2 Select a server to manage.

For instructions, see “Selecting a Server to Manage” on page 35.

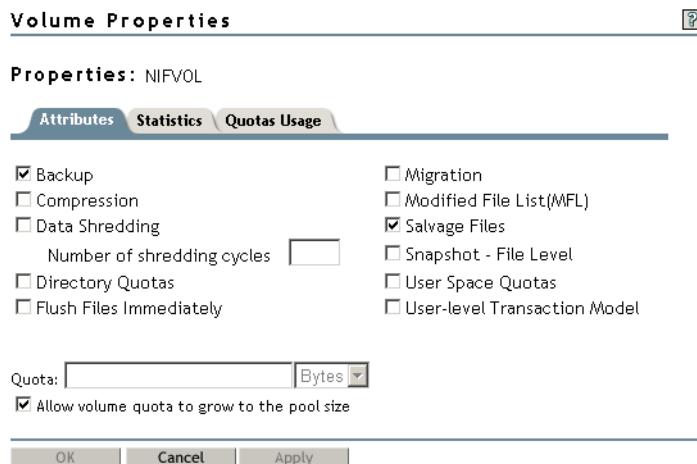
A list of devices appears in the Devices list.

3 From the Volumes list, select the volume that you want to manage.

4 Click Properties > Attributes.

This opens the Volume Properties page to the Attributes tab.

Storage Management > Volumes > Volume Properties



5 Select the Data Shredding check box.

6 Specify the number of shredding cycles, where 0 is no shredding and 1 to 7 are the valid number of cycles to shred data.

7 Click Apply or OK to save the change, or click Cancel to back out of the process.

If you click Apply, iManager saves the change and remains on the device page. If you click OK, iManager saves the change and takes you to the main Storage page. If you do not click Apply or OK, the setting is not implemented.

Disabling Data Shredding for an Existing Volume

WARNING: If you disable data shredding, an individual can recover leftover data on the drive and secure data might be exposed.

At the server console, enter

```
nss /nodataredding=volumename
```

where *volumename* is the name of the volume where you want to prevent the shredding capability.

Configuring Read Ahead Blocks Parameters

The Read Ahead Blocks attribute specifies the number of data blocks that NSS reads ahead for any open file on which read operations are ongoing in the specified server. The Read Ahead Blocks in Volumes attribute is not yet available in the Storage plug-in for iManager. It is enabled by default and set at 2 blocks. To modify the value, you must set it from the command line using the ReadAheadBlocks option.

The default block count of 2 blocks (8 kilobytes) satisfies the performance requirements for a typical volume. The valid range for block count is 0 blocks to 1024 blocks, where a block count of zero (0) implies no read ahead. However, the practical maximum is 128 blocks.

The most efficient value for block count depends on your hardware. In general, we recommend a block count of 8 to 16 blocks for large data reads; 2 blocks for CDs, 8 blocks for DVDs, and 2 blocks for ZLSS.

The block count should not exceed 128 blocks for most implementations. Aggressive read ahead is optimal for sequential access but it degrades random access. Block counts greater than 128 can starve other system components for memory or buffers, which can result in poor performance or can cause system hangs. As the number of concurrent connections to unique files increases, you should reduce the read-ahead block count..

To modify this parameter: At the server console, enter

```
nss /ReadAheadBlks=VolName:Count
```

Replace *VolName* with the volume name, such as *data*. Replace *Count* with the number of blocks to read ahead. The valid range is 0 (no read ahead) to 1024 blocks. Your setting is persistent; the value you set for a volume persists after reboot.

Using the Flush Files Immediately Attribute to Protect Against Possible Data Corruption on System Failure

The Flush Files Immediately attribute for volumes helps protect against data corruption by saving your file data from memory to a disk immediately after you close the file, instead of waiting for the next flush cycle. It also protects you against the risk of data being lost between flush cycles.

Normally, when data is written to disk by a user or process, the data is not actually written immediately to disk. Server operating systems juggle hundreds or thousands of demands that use memory to speed hardware-dependent functions, like disk writes, whenever possible. A file that gets written to disk might stay in the server memory for a short time (a matter of seconds or less) before actually changing bit patterns on a hard drive.

Optionally, with Flush Files Immediately, this server-juggling process can be overridden, forcing file changes out to the disk controller hardware immediately after the file is closed. The performance penalty comes on the rest of the server operations as they wait for a disk write, or dozens of disk writes, every few seconds on a busy server.

Setting the Flush Files Immediately Attribute When You Create a Volume

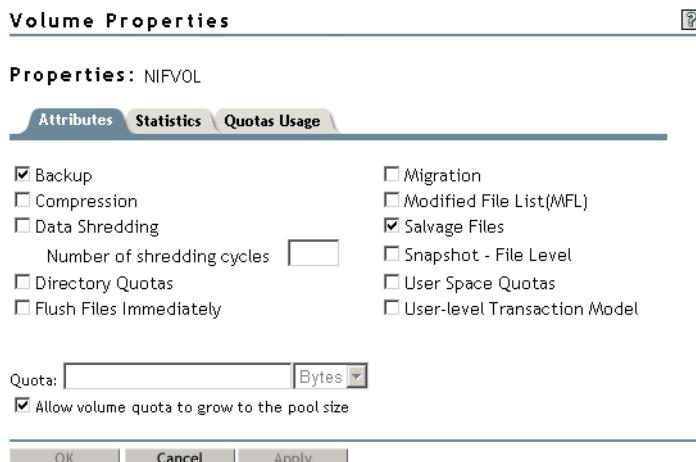
When you create the volume, simply select the Flush Files Immediately check box when you set the volume's attributes. For information, see “[Configuring Nonencrypted NSS Volumes with iManager](#)” on page 131.

Setting the Flush Files Immediately Attribute for an Existing Volume

- 1 In iManager, click Storage > Volumes to open the Volume Management page.
For information, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.
- 2 Select a server to manage.
For instructions, see “[Selecting a Server to Manage](#)” on page 35.
A list of devices appears in the Devices list.
- 3 From the Volumes list, select the volume that you want to manage.
- 4 Click Properties > Attributes.

This opens the Volume Properties page to the Attributes tab.

[Storage Management](#) ▶ [Volumes](#) ▶ [Volume Properties](#)



- 5 Select the Flush Files Immediately check box.
- 6 Click Apply or OK to save the change, or click Cancel to back out of the process.
If you click Apply, iManager saves the change and remains on the device page. If you click OK, iManager saves the change and takes you to the main Storage page. If you do not click Apply or OK, the setting is not implemented.

Enabling the Flush Files Immediately Attribute for All Volumes on a Server

At the server console, enter

```
nss /FlushFilesImmediately
```

To disable the Flush Files Immediately attribute for all volumes on the server: At the server console, enter

```
nss /NoFlushFilesImmediately
```

Using the Transaction Tracking System for Application-Based Transaction Rollback

The Novell Transaction Tracking System™ (TTS™) protects simple database applications by backing out application-based transactions that are incomplete because of a system failure. For example, a banking application might require that all steps in a user's session be complete before updating the database and ending the transaction. If a system failover occurred and the transaction did not complete all steps successfully, all of the steps would be rolled back to their condition before the transaction began. If all steps of the transaction are complete, the TTS replays the steps and completes the transaction successfully.

By default, TTS works with the Traditional file system. TTS cannot run on NSS and Traditional volumes at the same time on the same server. If you have both Traditional and NSS volumes on your system and you want to run TTS on NSS volumes instead of Traditional volumes, you must first disable TTS on all Traditional volumes, and then enable TTS on your NSS volumes.

Enabling TTS

To enable TTS on *each* NSS volume where you want it, enter `nss /transaction=volname` at the server console.

Disabling TTS

To disable TTS on all Traditional volumes, add `disable tts` to the autoexec.ncf file.

TTS Log File and Transaction Recovery

If a system failure occurs, TTS replays the TTS log file to recover lost application-based transactions as part of the failover recovery.

Before replaying the TTS log to recover lost transactions, TTS checks the integrity of the transaction file blocks in the log. If TTS detects no problems, the replay continues.

If TTS detects a bad block, it does not use the log file. TTS creates a new TTS log file to use as the system continues to operate.

IMPORTANT: Although the system continues to run, data might have been lost.

TTS renames the corrupted TTS log file to indicate the date and time that it detected the problem. For example, it renames

volume:\UXaction.log

to

volume:\XLogyyyymmddhhmmss.log

Corrupt TTS log files are relatively large, about 10 MB. TTS stores the corrupt TTS log file in the root directory of its transactioned volumes. If users report finding TTS log files in the root directory of their volumes, it indicates that a problem occurred and that TTS detected it.

NOTE: If a system failure causes corruption in the transaction log file, please report to Novell Support the network circumstances that lead to the corruption of the TTS log file. We want to examine the event to see if we can establish why the corruption might have occurred.

Using the File-Level Snapshot Attribute to Enable the Backup of Open Files

This section discusses the following key concepts and tasks:

- ◆ “Understanding File-Level Snapshots” on page 152
- ◆ “How the File Snapshot Attribute Works” on page 152
- ◆ “Sizing the Volume to Accommodate File Snapshots” on page 153
- ◆ “Assessing I/O Overhead for File Snapshots” on page 154
- ◆ “Configuring Volumes with the File Snapshot Attribute” on page 154
- ◆ “Configuring Backup Software to Use File Snapshots” on page 157
- ◆ “Restoring Volumes from Backup Media” on page 157

The file snapshot attribute is not the same as the pool snapshot feature. Pool snapshot is an NSS feature that makes block-level snapshots of a pool that persist until intentionally deleted. For information, see “[Managing NSS Pool Snapshots](#)” on page 115.

Understanding File-Level Snapshots

File-level snapshot is an attribute of an NSS volume that allows a temporary copy of an open file to be made at the time of a volume backup so that the last-known-good copy of the file is available for backup while the file is in use.

Normally, if a file is open when backup services begin, that open file cannot be backed up. With the file snapshot attribute set for a volume, NSS creates and maintains a virtual volume where it writes a partial or full copy of a file’s original data whenever a file on the source volume is open for write. This temporary copy of the file’s original data is made available to the backup software instead of the current contents of the open file. Consequently, open files can be copied to the backup media, even though changes in progress for the files are not backed up.

All file snapshot activity happens transparently to the user and to non-backup applications. The user and applications always read the current content of the file.

Not all backup software can take advantage of the file snapshot attribute, even if you set it.

The copy of the file is temporary. When the user or API closes the file, NSS deletes the file-snapshot copy.

How the File Snapshot Attribute Works

The file snapshot attribute uses block-level copy-on-write technology, a technique of capturing before images of data as it is modified by applications. The primary purpose of these images is to enable point-in-time backups of file systems while they are in use.

Before the file is open, the physical volume contains a file with data that fills multiple storage blocks on the device. The virtual volume contains only metadata about the file. Metadata includes owner, created date/time, and other information about the file and an empty Blocks Changed list.

Whenever the file opens, the NSS file snapshot attribute updates the metadata for the file, then monitors for writes to the file. NSS identifies writes at the block level. When it intercepts a write command, NSS does not immediately write to the physical location. Instead, NSS reads the data in the target block and copies the existing data in that block to the virtual volume. It adds the

addresses of the changed blocks to the Blocks Changed list. At this point in the process, the old data exists in two places: the target block and a block in the virtual volume.

Next, NSS allows the new data to overwrite the old data in the target block. Now, the target block contains new data. The file on the physical volume has some blocks that contain old data, and some blocks that contain new data, just as it would after any normal write process. All that is stored in the virtual volume is the metadata about the file and the blocks of data that represent what the file looked like at the moment it was opened (the blocks of data that NSS copied to the virtual volume).

With the file snapshot attribute disabled, your backup software normally cannot capture a file to backup media, if the file is open and changes are in progress. The backup passes over the file and does not copy it to the backup media. The state of the file is not captured to the backup media.

When the file snapshot attribute is enabled and your backup software takes advantage of the feature, the backup knows to read blocks from the virtual volume and from the physical volume for the open file. From the physical volume, the backup software reads the blocks that are as yet unchanged by any block writes. From the virtual volume, the backup software reads the blocks that contain the file's data as it was when the file opened. The total information saved to the backup media represents the state of the file when the file was opened.

The virtual volume and its contents are not directly accessible to users or non-backup APIs. It is only accessible to Novell Storage Management Services or third-party backup software that takes advantage of the file-snapshot flag. All other applications ignore the virtual volume. If accessing an open file, the backup software reads original data from the virtual volume, but any other application reads the file's current contents.

When the open file closes, NSS updates the file's metadata and erases the blocks of original data stored in the virtual volume.

This is how the last-known-good version of the file gets saved to the backup media when it would have been passed over previously. The backup media contains real data; it does not back up the virtual volume per se. It only copies data from the virtual volume to re-create the complete last-known-good copy of the open file.

Sizing the Volume to Accommodate File Snapshots

Initially, the virtual volume occupies very little storage space. It contains only an empty changed-block list. As an application opens a file to update its data, NSS dynamically allocates space in the virtual volume where it can copy blocks of the original data. As blocks of data change, NSS copies the original data to the virtual volume and updates the changed-block list to indicate which blocks have changed.

The size of the virtual volume depends on several factors:

- The size of the original file when it is opened
- How the files are used (such as how often they change, when they change, and who changes them)
- How many blocks of data that a single change affects (up to the number of blocks in the original file)
- How the application saves changes (such as by blocks or by the entire file)

It is a good idea to set the physical volume's size to grow dynamically to the size of the pool. Otherwise, you must periodically monitor the volume size to make sure it can accommodate the peak size of the virtual volume as the volume contents fluctuate at peak productivity times. Make sure your volume's size can also accommodate any seasonal productivity peaks.

Assessing I/O Overhead for File Snapshots

The amount of I/O overhead related to the dynamic file snapshots depends on the usage of the volume. Every time a file opens for write (not read), NSS makes a copy of the metadata about the file, but not the data itself. NSS makes a copy of only that part of the data in the file that a write changes. The algorithm is optimized in such a way that NSS does not make copies of data too often, given the behavior of most applications such as word processors.

Applications write data in different ways. Some close the file after each write, while others close the file intermittently and on demand. As soon as the application closes the file, even if the file is still open for read or for another write, NSS erases any related blocks for that file that are saved in the virtual volume. On executing the next open for write, the process begins again for the file, working with the last closed copy of the file.

Other applications write only differential data at the (logical) end of the file, leaving the existing data blocks intact. In this case, no existing data blocks are overwritten by the application, and there is no writing of data (only metadata) to the virtual volume.

However, in all cases, the backup software can still back up the last closed version of the file.

The thing to remember in assessing overhead is that every time a file is closed, NSS erases its metadata and the original data blocks that were copied to the virtual volume. The data in the virtual volume is not a perpetual copy that is constantly updated.

To assess overhead related to the File Snapshot attribute of an NSS volume:

- What types of applications are in use? How do those applications write to files? How are closes executed?
- How many files are there in the volume, categorized by application?
- How frequently are files changed? Does the frequency change by user or user group? Time of year? Type of application?
- How much data in the file changes typically with each use? How often are files opened for Read versus for Write?

Configuring Volumes with the File Snapshot Attribute

File snapshots apply only to volumes. You must configure a volume with this attribute in order to take advantage of the feature. After the attribute is set, the file-snapshot process is automatic.

You can set the file snapshot attribute for a volume as you create the volume, or you can opt to set the attribute later.

Setting the File Snapshot Attribute for a New Volume

To enable the file snapshot attribute when you first create the volume:

- 1 Open the New Volume wizard in iManager, following the normal setup. See [“Configuring Nonencrypted NSS Volumes with iManager” on page 131](#).
- 2 On the Attributes page in the New Volumes wizard, also select the Snapshot - File Level check box.
- 3 Complete the New Volume wizard.

Whenever the volume is first activated, NSS creates the virtual volume and the file snapshot process occurs automatically.

Setting the File Snapshot Attribute for an Existing Volume

To set up the file snapshot attribute after a volume is in use requires some pre-planning. Because you must deactivate and activate the volume to allow NSS to set up the virtual volume, you should initiate the file snapshot attribute at a time when no I/O operations are in progress and all cached data is also reflected in the storage media. For example, to make sure no transactions are lost:

- ◆ Allow in-progress transactions to complete gracefully.
- ◆ Temporarily block any new transactions.
- ◆ Flush any file changes that are cached in memory to the volume.

To enable the file snapshot attribute on a given volume:

- 1 Launch a Web browser.
- 2 Click File > Open, then enter

`http://svrname.your-company-name.com/iManager.html`

Replace *svrname* with the actual server host name. Replace *your-company-name.com* with your company's actual domain name. You can use the server's IP address (such as 192.168.1.1) instead.

- 3 In iManager, log in to the server context that the server belongs to.
- 4 In Roles and Tasks, select Storage > Volumes.
- 5 Use one of these methods to select a server in the tree you are logged in to:
 - ◆ Type the Novell eDirectory server object name for the server you want to manage, then click Apply. For example: svr1.novell.
 - ◆ Click the Search icon to open the eDirectory Object Selector. Browse or search the list to locate the server object of the server you want to manage, then click the server name.
 - ◆ Click the Object History icon to select a server you have recently managed.

After iManager connects to the server, the Volumes field lists all of the volumes for the selected server. Let the page load completely before proceeding to the next step.

- 6 Select a volume in the Volumes list.
- 7 (Conditional) Review the Details area to make sure the volume is active and mounted. If it is not, click Mount.

The Mount command activates and mounts the volume in one step. The volume should still be selected when the page reloads. If it is not, select the volume again.

- 8 Click Properties > Attributes.
- 9 Select the Snapshot - File Level check box.
- 10 Click Apply.
- 11 Click OK.

This should return you to Volumes page. If not, select Storage > Volumes.

- 12 Make sure the volume is selected, then click Deactivate.

You must deactivate and activate the volume to enable NSS to set up the virtual volume area where file snapshots are stored.

When the page reloads, the volume is in a deactive state.

- 13 If not already selected, select the volume, then click Activate.

NSS creates the metadata about files in the virtual volume during the activation process. When the page reloads, the volume is in the activated state and the virtual volume is ready for file-snapshot process.

Using Console Commands to Configure the File Snapshot Attribute

To enable the File Snapshot Attribute for one or multiple volumes, enter at the server console:

`nss/FileSyncOnWrite=VolName`

or

nss/FileSyncOnWrite=all

To disable File Snapshot, enter at the server console:

nss/NoFileSyncOnWrite

After you set up File Snapshot on your volume, deactivate the volume, then activate the volumes again. This ensures that there are no open files without a snapshot.

Configuring Backup Software to Use File Snapshots

NSS sets a flag that Novell Storage Management Services™ (SMS) and some third-party backup software can read to determine if there are copies of open files available to be backed up.

IMPORTANT: Even if you set this flag, not all third-party backup software takes advantage of the service.

Novell SMS automatically checks for the File Snapshot attribute when it backs up a volume. If the attribute is set, it takes advantage of the feature.

To open a snapshot file for backup, set a bit in the requested rights parameter and set the READ_ACCESS_BIT. This bit is 0x04000000. It is defined in the NSS header files as zPR_READ_ACCESS_TO_SNAPSHOT.

The default setting for File Snapshot is whenever your file system receives an open for write request, it will wait for the backup open to close the file. To return an error, the backup open should also set the deny-the-write bit.

To get information on a snapshot file, use the getInfo command. NSS supports any getInfo call that returns packed information with the RNewStyle bit set in the info mask. You need to set an additional bit 0x20000000 in the information mask. This bit is defined at RNSSInfoOnSnapshot in NSS header files. Both open and getInfo calls require the bit for requested rights and the bit for additional info mask.

The following calls also return information about File Snapshot:

- ◆ GetFileSize
- ◆ GetFileHoles

Restoring Volumes from Backup Media

Whenever backup software tries to read an open file, it reads data from the virtual volume and the volume. The virtual volume contains a list of changed blocks for the file. It reads the original data for those blocks from the virtual volume. Then, it reads the other blocks of data from the volume itself. The data saved to backup media is the file's original content before it was open.

When you restore the volume from its backup media, it restores just as it does normally. It requires no special action.

Configuring the NSS Volume Salvage Area

You can configure the purge delay, low watermark, and high watermark parameters for the salvage area on an NSS volume.

Setting the Purge Delay for the Salvage Area

The default for the Purge Delay setting is four days. This is the amount of time that you can still access the volume before it is removed from the system. To change the Purge Delay time, enter at the server console:

```
nss /logicalVolumePurgeDelay=value
```

In this command, replace *value* with the actual number of seconds to delay the auto purge. The default is 345600 (4 days). For example, if you want to change the Purge Delay time for one day, you would enter 86400.

The Purge Delay change command is not permanent. You must enter the command each time you restart the server. If you want to make the new setting permanent, add the command to the autoexec.ncf file.

Setting the Low and High Watermarks for Purging the Salvage Area

Purging begins in the salvage area when the volume's low watermark is reached and continues until its high watermark is reached. The default low watermark is when free space is 10% or less of the total disk space. The default high watermark is when free space is at least 20% of the total disk space.

When free disk space falls below a low watermark, NSS begins autopurging the salvage area. When enough files are purged such that the free disk space increases to a percentage equal to or greater than the high watermark, the autopurge stops. Autopurging does not start again until free space again drops below the low watermark.

The high and low watermarks can be configured at a pool level. The low watermark's percentage can range from a minimum of 0% to a maximum of 98%. The high watermark's percentage can range from a minimum 2% to a maximum of 100%. The high and low watermarks must be at least 2% apart from each other.

To configure the high and low watermarks, enter the following at the server console:

```
nss /PoolHighWaterMark=<poolname>:Percent  
nss /PoolLowWaterMark=<poolname>:Percent
```

For example, to set the low watermark to 5% and the high watermark to 10% for pool p_users, enter

```
nss /PoolHighWaterMark=p_users:10  
nss /PoolLowWaterMark=p_users:5
```

Viewing, Salvaging, or Purging Deleted NSS Volumes

If you delete a volume, NSS removes it from the pool. However, during a specified amount of time, called the Volume Purge Delay time, you can review and restore the volumes you have deleted. After the purge delay time elapses, NSS automatically removes volumes from the system and you can no longer access them. You can also manually purge any volumes you have deleted.

During the Purge Delay time (by default, four days after a volume is deleted), you can manually purge deleted volumes, view the volume contents, transfer files from the deleted volume to other volumes, or salvage the entire volume, if desired.

You can also change the Purge Delay time to extend or reduce the time for the automatic purging cycle. The Purge Delay time command can be changed by adding a line in the autoexec.ncf file. The default value for the Purge Delay is 345600 seconds, which is four days. Specify the time in seconds. See “[Configuring the NSS Volume Salvage Area](#)” on page 157.

The Deleted Volumes option on the Pools page opens a separate Deleted Volumes page where you can purge or salvage the deleted volumes for the pool. This option is only available if the selected pool has deleted volumes on it.

WARNING: If you delete an entire pool, all the volumes are deleted with it. You cannot restore a deleted pool or any deleted volumes in it.

To manage the deleted volumes in a pool:

1 In iManager, click Storage > Pools.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of pools appears in the Pools list.

3 Select the pool that you want to manage.

Wait for the page to refresh and display the details. The Deleted Volumes button is active only when there are deleted volumes in that list.

4 If the button is available, click Deleted Volumes.

This opens the Deleted Volumes page.

[Storage Management](#) ▶ [Pools](#) ▶ [Deleted Volumes](#)

Deleted Volumes:	Details:
Purge	PROJ46
Pause Purge	PROJ135
Restart Purge	SHVOL
Salvage...	TEMP30
Close	TEMP60
	TEMP90

Pool: PROJ46

Volume was deleted: Jun 9, 2003 4:19:07 PM

Scheduled Purge Time: Jun 13, 2003 4:19:07 PM

Current deletion state: Salvageable

5 Select a volume from the Deleted Volumes list.

The browser refreshes to display details in the Details area.

- ◆ **Pool:** The pool name.
- ◆ **Volume Was Deleted:** The time stamp when the volume was deleted.
- ◆ **Scheduled Purge Time:** The time that the Purge Delay expires for this deleted volume and the purging process is scheduled to begin.
- ◆ **Current Deletion State:** The deleted volume can be salvageable, purging, or paused.

6 Select one or more volumes, then perform one or more of these actions:

- ◆ **Purge:** Immediately begins the process of purging the selected volumes and their contents.
- ◆ **Pause Purge/Restart Purge:** Pause Purge stops the volume purging process for selected volumes. Restart Purge purges the selected volumes.
- ◆ **Salvage:** Begins the restore process for deleted volumes you selected.
If you salvage a volume, you need to assign a new name to that volume. A wizard opens to allow you to name the salvaged volume.
The volume salvage process can slow the server response time, so you might want to do this when there is less server activity.
- ◆ **Close:** Closes the Deleted Volumes page.

Salvaging or Purging Deleted Files

Whenever users delete files from the server, the files are retained and can be recovered (salvaged) until they have been purged.

IMPORTANT: Files that have been purged can no longer be restored from salvage.

Deleted files are purged from the volume when one of the following events occurs:

- ◆ The Purge Delay setting times out. Deleted files are purged automatically.
- ◆ The server starts purging files if a volume starts to fill up; the oldest files that have been deleted are automatically purged.
- ◆ If you do not want a file to be restored after deletion, you can enable the Immediate Purge of Deleted Files parameter. The file is deleted and purged immediately.
- ◆ You manually purge the deleted files.

Use any of the following methods to salvage or purge deleted files.

- ◆ “[Salvaging or Purging Deleted Files with NetStorage](#)” on page 160
- ◆ “[Salvaging or Purging Deleted Files with the Novell Client](#)” on page 161
- ◆ “[Salvaging or Purging Deleted Files with Novell Remote Manager](#)” on page 161

Salvaging or Purging Deleted Files with NetStorage

Using NetStorage, admins and users can purge and possibly undelete NSS files that were previously deleted on your NetWare server.

- 1 Access NetStorage.
For information, see “[Novell NetStorage](#)” on page 43.
- 2 In the left column, select the directory where the deleted files were.
- 3 Click View, then click Show Deleted Files.
- 4 Select the check box next to one or more files you want to undelete or purge.
- 5 Click File, then click Undelete or click Purge.

Salvaging or Purging Deleted Files with the Novell Client

Using the Novell Client™ for Windows 2000/XP, admins and users can purge and possibly undelete NSS files that were previously deleted on your NetWare server.

- 1 Right-click the Novell Client icon (the red N) in the notification area to display the menu.
- 2 If you want to salvage a deleted file, click NetWare Utilities > Salvage, browse to locate the directory where the deleted file resided, then do one of the following:
 - ◆ To restore one or multiple deleted files, select the deleted files, then click Salvage File.
 - ◆ To restore all deleted files in the directory, click Salvage All.
- When you are done, click OK.
- 3 If you want to purge a deleted file, click NetWare Utilities > Purge, browse to locate the directory where the deleted file resided, then do one of the following:
 - ◆ To purge one or multiple deleted files, select the deleted files, then click Purge File.
 - ◆ To purge all deleted files in the directory, click Purge All.
 - ◆ To purge the directory's subdirectories and all deleted files in them, click Purge Subdirectories.
- 4 When you are done, click OK.

Salvaging or Purging Deleted Files with Novell Remote Manager

Using Novell Remote Manager, admins can purge and possibly undelete NSS files that were previously deleted on your NetWare server.

- 1 In a Web browser, connect to Novell Remote Manager on the NetWare server where the deleted file resides.

For information, see [“Accessing NSS Storage Management Role and Tasks” on page 34](#).
- 2 On the Volume Management page, click the volume name link where the file was deleted
- 3 From the directory list, click the Information icon to left of the directory name where the file was deleted.
- 4 On the Directory Information page, find the Salvageable Files field, then click the Select for List link.
- 5 Do one of the following:
 - ◆ **Salvage:** Locate the deleted file you want to restore, then click the Salvage button next to the filename.
 - ◆ **Purge:** Locate the deleted file you want to purge, then click the Purge button next to the filename.
 - ◆ **Purge All:** Click the Purge All Files button to purge all the files in the directory.

Understanding Space Quotas

You can conserve space in an NSS volume by restricting the amount of space available to a particular volume, directory, or user. These space restrictions, or quotas, work independently, with

the lower value being the most restrictive if all constraints apply. NSS allocates the space as it is needed.

If you set a quota to a value equal to or less than the current size of space in use for the specified volume, directory, or user, users cannot add files until enough files are deleted to free up space in the volume, directory, or user files. Users can continue to access existing files for which they are authorized users.

Volume Quotas

When you create an NSS volume, you have the option of setting a space quota for the volume or letting it grow to the size of the pool. At any time thereafter, you can view and configure the volume quota from the Volume Properties > Attributes tab in iManager. For information, see “[Managing NSS Volume Quotas](#)” on page 162.

If you set a volume quota to grow to the pool size, you can also add segments to the volume’s pool to expand its size, and therefore expand the volume quota.

As a volume nears its quota, automatic controls can be configured to manage space. For information, see “[Setting the Low and High Watermarks for Purging the Salvage Area](#)” on page 158.

Directory Quotas

Directory quotas limit the space available in an individual NSS directory. To use directory quotas on an NSS volume, you must first enable the Directory Quotas attribute.

For information about configuring attributes when you create a volume, see “[Managing NSS Volumes](#)” on page 127.

For information about setting directory quotas, see “[Managing Directory Quotas](#)” on page 164

User Space Quotas

User space restrictions limit the space available to a user of the NSS volumes across all directories and files owned by the user. To apply user space restrictions, you must first enable the User Space Quotas attribute.

For information, see “[Configuring User Space Quotas](#)” on page 169.

Example of Directory and User Space Quotas

Quotas are beneficial for systems where you want to control how your storage resources are used. In environments such as a university, where you set up a common work area for a large number of students and you want to limit the space that directory can consume, set a Directory Quota. You might also limit the amount of space an individual user’s work can consume by setting the User Quota.

For example, if a directory’s quota is 500 MB and the user’s quota is 1 GB, the user is limited to up to 500 MB in the specific directory. If the user can access multiple directories, each with a 500 MB quota, the maximum space the user’s work can consume for all directories combined is limited to the user’s 1 GB administrative limit.

Managing NSS Volume Quotas

- 1 In iManager, click Storage > Volumes.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

2 Select a server to manage.

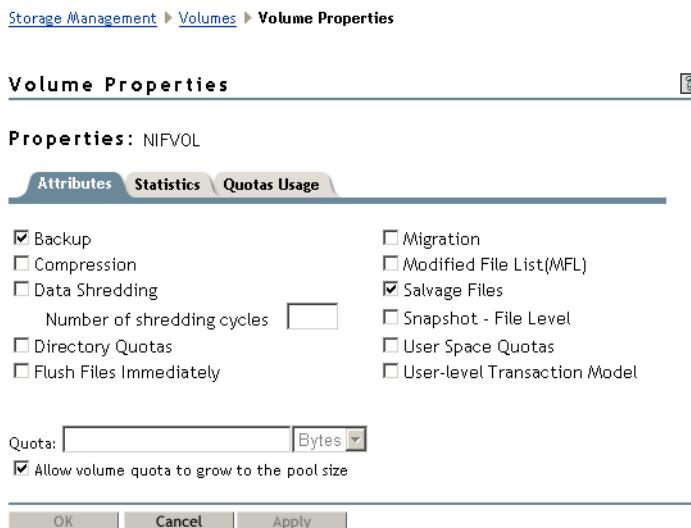
For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of volumes appears in the Volumes list.

3 In the Volumes list, select a volume that you want manage.

4 Click Properties.

The Properties page has three tabs: Attributes, Statistics, and Volume Quota. It opens to the Attributes tab.

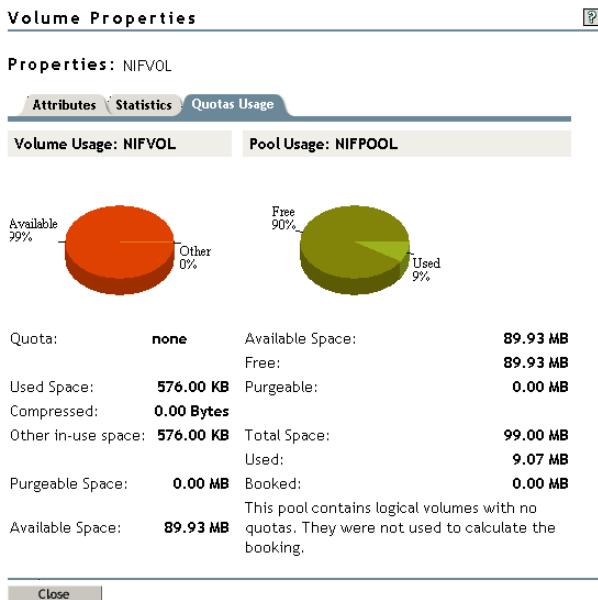


5 In the Quota field, do one of the following:

- ♦ **No Quota:** Select Allow Volume Quota to Grow to the Pool Size. NSS pools allow overbooking so the administrative sum of all volumes’ quotas in a pool can exceed the physical pool quota.
- ♦ **Quota:** Deselect Allow Volume Quota to Grow to the Pool Size, then specify the maximum size you want to allow volume to grow. The quota cannot exceed the pool size.

6 Click Apply.

7 Click the Quotas Usage tab to view the volume and pool space usage for the selected volume and to verify the new setting.



Managing Directory Quotas

Before you can set directory quotas, you must enable the volume's Directory Quotas attribute. As the Admin user, you can view and configure directory quotas with NetStorage and the Novell Client™. For NSS on NetWare, you can also use Novell Remote Manager for NetWare.

This section discusses the following:

- ◆ “Setting the Directory Quotas Attribute for an NSS Volume” on page 164
- ◆ “Novell NetStorage” on page 165
- ◆ “Novell Client” on page 165
- ◆ “Novell Remote Manager for NetWare” on page 166

Setting the Directory Quotas Attribute for an NSS Volume

After you set up and configure NSS volumes, you can view and modify attribute settings such as the Directory Quotas attribute.

- 1 In iManager, click Storage > Volumes.

For instructions, see “Accessing NSS Storage Management Role and Tasks” on page 34.

- 2 Select a server to manage.

For instructions, see “Selecting a Server to Manage” on page 35.

A list of volumes appears in the Volumes list.

- 3 In the Volumes list, select a volume that you want manage.

- 4 Click Properties.

The Properties page has three tabs: Attributes, Statistics, and Volume Quota. It opens to the Attributes tab.

- 5 On the Attributes tab, select or deselect the Directory Quotas check box, then click Apply.

Novell NetStorage

Using Novell NetStorage, you can manage directory quotas for directories in an NSS volume from any computer with a supported Web browser. This requires you to first configure a NetStorage server in the same context. For information, see the *NetWare 6.5 NetStorage Administration Guide*.

To create or change NSS directory quotas with NetStorage:

- 1 In a Web browser, connect to NetStorage.

For information, see “Novell NetStorage” on page 43.

- 2 Log in to NetStorage with the admin username and password.

You can also log in as any user with equivalent rights to the admin user.

- 3 Navigate to the directory you want to manage.

- 4 Right-click the directory, then select Properties.

- 5 Click the NetWare Info tab.

- 6 Do one of the following to configure the directory quota:

- ◆ **Space Restriction:** Select Restrict Size, then specify the directory quota in KB. The value must be a multiple of 4.
- ◆ **No Space Restriction:** Deselect Restrict Size to set the directory quota to Unlimited.
- ◆ **Complete Space Restriction:** Select Restrict Size, then specify the directory quota as 0 KB. If the directory already contains files and subdirectories, the directory cannot grow beyond the current space consumed.

- 7 Click Apply to accept the directory quota configuration.

Novell Client

The Novell Client for Windows 2000/XP allows the admin user to manage directory quotas for directories in an NSS volume from a Windows computer.

- 1 In the Novell Client, map a drive to the NSS directory you want to manage, or map to its parent directory.

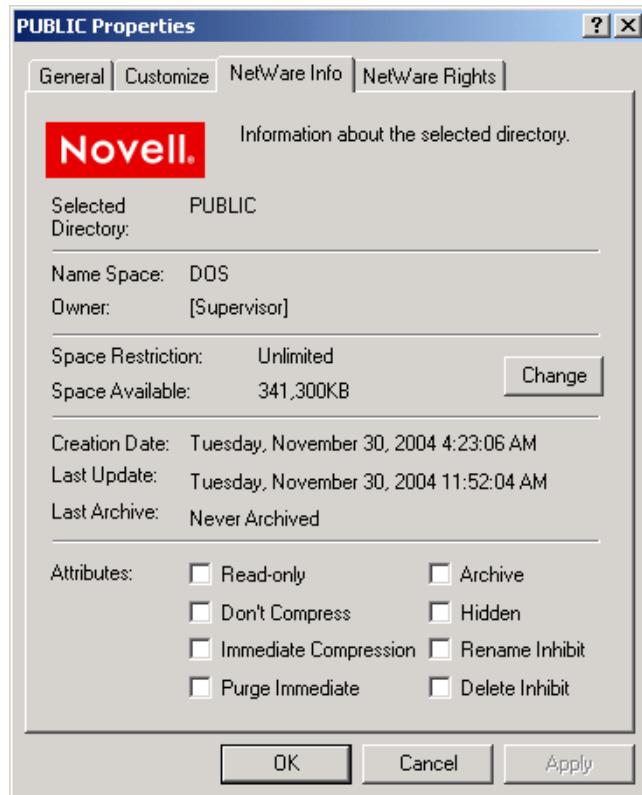
1a Right-click the Novell Client icon (the N icon on the status bar), then select Novell Map Network Drive.

1b Specify the network path to the directory. For example: 192.168.1.1/users.

1c Specify admin as the username, then click Map.

1d When prompted, enter the admin user password.

- 2 In a file browser, locate and right-click the directory you want to manage, then click Properties > NetWare Info.



3 In the Space Restriction field, click Change to open the Space Restriction dialog box.



4 Do one of the following to configure the directory quota:

- **Space Restriction:** Specify the directory quota in KB. The value must be a multiple of 4.
- **No Space Restriction:** Select No Space Restriction to set the directory quota to Unlimited.
- **Complete Space Restriction:** Select Complete Space Restriction to set the directory quota to 0 KB. If the directory already contains files and subdirectories, the directory cannot grow beyond the current space consumed.

5 Click OK to accept the directory quota.

Novell Remote Manager for NetWare

1 Access Novell Remote Manager for your NetWare server.

For information, see “Novell Remote Manager” on page 44.

- 2 Click Volumes to open the Volume Management page.
- 3 Locate the volume where the directory resides, then click the volume name link to view a directory listing for the volume.
- 4 Locate the directory you want to manage, then click the  Directory Information icon to the left of the directory to open the Directory management page.
- 5 In the Directory Entry Information field, click the File Space Limit link.

Directory entry information	
Owner	ADMIN
Creation date and time	Feb 1, 2005 5:11 pm
Effective rights	SRWCEMFA
Inherited rights filter	SRWCEMFA
File space limit	None
File space in use	0 KB

This link is not available if you did not enable the Directory Quotas attribute when you created the parent volume.

- 6 Do one of the following:
 - ◆ **Space Restriction:** Specify the maximum size (in kilobytes) for the selected directory, then click Set Space Restriction to apply the setting.
 - ◆ **No Space Restriction:** Click No Quota to remove space restrictions for the selected directory.
 - ◆ **Complete Space Restriction:** Specify the maximum size as 0 KB. If the directory already contains files and subdirectories, the directory cannot grow beyond its current space consumed.

Managing User Space Quotas

Before you can set user space quotas, you must enable the volume's User Space Quotas attribute. As the Admin user, you can view and configure user space quotas in Storage plug-in for iManager.

This section discusses the following:

- ◆ [“Setting the User Space Quotas Attribute for an NSS Volume” on page 168](#)
- ◆ [“Viewing User Space Quotas” on page 168](#)
- ◆ [“Configuring User Space Quotas” on page 169](#)
- ◆ [“Modifying a User Quota” on page 170](#)
- ◆ [“Deleting a User Quota” on page 170](#)

Setting the User Space Quotas Attribute for an NSS Volume

After you set up and configure NSS volumes, you can view and modify attribute settings such as the User Space Quotas attribute.

- 1 In iManager, click Storage > Volumes.

For instructions, see “Accessing NSS Storage Management Role and Tasks” on page 34.

2 Select a server to manage.

For instructions, see “Selecting a Server to Manage” on page 35.

A list of volumes appears in the Volumes list.

3 In the Volumes list, select a volume that you want manage.

4 Click Properties.

The Properties page has three tabs: Attributes, Statistics, and Volume Quota. It opens to the Attributes tab.

5 On the Attributes tab, select (enable) or deselect (disable) the User Space Quotas check box, then click Apply.

Viewing User Space Quotas

1 In iManager, click Storage > Volumes to open the Volume Management page.

For instructions, see “Accessing NSS Storage Management Role and Tasks” on page 34.

2 Select a server to view and manage.

For instructions, see “Selecting a Server to Manage” on page 35.

A list of devices appears in the Devices list.

3 In the Volumes list, select the volume that you want to manage.

Wait for the page to refresh to see details and options available for that volume.

4 View users and their quotas:

- ◆ To view only users with quotas, click User Quotas > Users with Quotas.

This opens the User Quotas page to the Users with Quotas tab.

[Storage Management](#) ▶ [Volumes](#) ▶ [User Restriction](#)

User Quotas

[Users with Quotas](#) [All Users](#)

A storage quota restricts the amount of space on the volume available to a user. Because NSS allocates space as needed, each quota can be as big as you want to make it. View all users or only the users with quotas. Then, add, modify, and delete quotas for users.

User Name	Quota	Space in Use	Space Available
<input type="checkbox"/> acatt.novell	1000.00 MB	0.00 Bytes	1000.00 MB
<input type="checkbox"/> bpeep.novell	1000.00 MB	0.00 Bytes	1000.00 MB
<input type="checkbox"/> pcharming.novell	1000.00 MB	0.00 Bytes	1000.00 MB

[Add...](#)

[Modify...](#)

[Delete](#)

- ◆ To view all users (with or without quotas) for that volume, click User Quotas > All Users.

This opens the User Quotas page to the All Users tab.

User Quotas

Users with Quotas **All Users** 

A storage quota restricts the amount of space on the volume available to a user. Because NSS allocates space as needed, each quota can be as big as you want to make it. View all users or only the users with quotas. Then, add, modify, and delete quotas for users.

	User Name	Quota	Space in Use	Space Available
<input type="checkbox"/>	.[Supervisor].	No User Quotas	943.51 MB	
<input type="checkbox"/>	admin.novell	1000.00 MB	6.98 MB	
<input type="checkbox"/>	bpeep.novell	1000.00 MB	0.00 Bytes	1000.00 MB
<input type="checkbox"/>	pcharming.novell	1000.00 MB	0.00 Bytes	1000.00 MB
<input type="checkbox"/>	NFAIUUser.novell	1000.00 MB	0.00 Bytes	

Add... **Modify...** **Delete**

Configuring User Space Quotas

- 1 In iManager, click Storage > Volumes, select a server, then select the volume you want to manage.
- 2 Click Quotas > All Users.
- 3 Click Add to open the User Space Quota wizard.

User Space Quota

 **Add User Quota** 

Enter the distinguished user name (userid.context), or browse to select one or more users from the User Name drop-down list. Set a storage quota to be applied to each of the selected users by entering the upper limit of storage (such as 750 MB).

User Name: 

User Quota: Bytes 

[<< Back](#) [Finish](#) [Cancel](#)

- 4 Click the Browse icon to open the User object list, then browse to select one or more users who you want to share the same quota.
- 5 In User Quotas, specify the maximum quota you want to assign to each of the selected users.
- 6 Use the Units drop-down list to select the units to use for the quota you specified. Options are bytes, kilobytes, megabytes, and gigabytes.
- 7 Click Finish.

Each of the usernames you selected now has user quotas assigned to it.

Modifying a User Quota

- 1 In iManager, click Storage > Volumes, select a server, then select the volume you want to manage.
- 2 Click Quotas > Users with Quotas.
- 3 Select the check box next to one or more user names whose user space quota you want to delete, then click Modify to open the Modify User Quota wizard.
The Modify User Quota wizard is similar to the Add User Quota wizard.
- 4 Specify the user space quota you want to apply individually to each of the selected users.
- 5 Use the Units drop-down list to select the units to use for the quota you specified in **Step 4**. Options are bytes, kilobytes, megabytes, and gigabytes.
- 6 Click Finish.

Each of the users you selected now has the new user quota assigned to his or her individual account on this volume.

Deleting a User Quota

- 1 In iManager, click Storage > Volumes, select a server, then select the volume you want to manage.
- 2 Click Quotas > Users with Quotas.
- 3 Select the check box next to one or more user names whose user space quota you want to delete, and then click Delete.
- 4 Do one of following:
 - ◆ To confirm, click Yes to remove the quotas. The user accounts no longer have quotas assigned to them for the selected volume.
 - ◆ To back out of the process, click No.

What's Next

For information about advanced volume features, see the following:

- ◆ [Managing Encrypted NSS Volumes \(page 171\)](#)
- ◆ [Using Compression to Conserve Storage Space on NSS Volumes \(page 177\)](#)
- ◆ [Using Distributed File Services for Moving and Splitting NetWare 6.x NSS Volumes \(page 191\)](#)

12

Managing Encrypted NSS Volumes

In NetWare® 6.5 Support Pack 2 and later, Novell® Storage Services™ provides optional Encrypted Volume Support (EVS) to meet the legal standard of making data inaccessible to software that circumvents normal access control, such as if the media were stolen. EVS is available only for newly created NSS data volumes. You cannot encrypt the sys: volume. EVS stores user data in encrypted format on the NSS volume, yet works transparently with most applications, NLM™ programs, and backup utilities that currently work with NSS.

This section discusses the following:

- ◆ “Understanding Encrypted Volume Support” on page 171
- ◆ “Creating an Encrypted Volume” on page 172
- ◆ “Using Encrypted Volumes in a Server Cluster” on page 173
- ◆ “Archiving Files from an Encrypted Volume” on page 174
- ◆ “Using Direct I/O on an Encrypted Volume” on page 174
- ◆ “Managing Encrypted Volumes with NSS Commands” on page 174
- ◆ “Removing Encrypted Volumes” on page 175
- ◆ “What’s Next” on page 176

Understanding Encrypted Volume Support

Any NSS volume, except the sys: volume, can be designated at volume creation time to be an encrypted volume. The Encrypted attribute stays with the volume throughout its life. An encrypted volume cannot later be converted to nonencrypted, nor can an nonencrypted volume later be converted to encrypted. This is a creation-time-only decision.

With EVS, encryption is transparent above the physical read/write layer of an NSS volume. It requires no changes for applications. All the rules of rights, trustees, ownership, sharing, visibility, locking, transactions, and restrictions remain the same. Performance for an encrypted volume is slightly degraded as compared to a nonencrypted volume under the same conditions.

Encryption Method

EVS uses the NICI libraries for all cryptographic support. NICI generates a 128-bit AES key for encryption that persists for the life of the volume. You cannot change the password because it is the key used to encrypt data. NICI uses the password to wrap the key and other volume-specific cryptographic information into a 128-bit package that is persistently stored in two locations on the NSS media: the Volume Data Block and the Volume Locator Beast. After the cryptographic data is wrapped for the activated volume, EVS eliminates the password from memory.

How EVS Works

On the first activation after a system reboot, you must enter a valid password. When the volume is activated, NSS loads the volume's persistent data from the Volume Data Block. If the Encrypted attribute is enabled for a volume, NSS searches in memory for a known key in the list of volume names and keys. If the key is present, it is used. If no key is present, NSS consults the list of volumes and passwords. If a password is available, it is used to unwrap the key from the persistent data and the new key is placed in the list of volumes and keys. The password is eliminated from memory. After the encrypted volume is activated, all encryption operations on user data are transparent to file system applications that use normal file I/O functions. Data written to files is held in cache until such time as it would be normally written. At physical write time, the data is encrypted to a temporary write buffer and written to the volume in encrypted format.

During reads, the cache is consulted, as it would normally be, to determine if a requested block is already in memory. If the requested data block is in cache, the clear-text data is transferred. If it is not, a physical read request is made, with the read directed to a temporary buffer. After read completion, but before control is returned to the calling program, the encrypted data in the temporary buffer is decrypted into a cache buffer. The read proceeds normally, with clear-text data being made available to all future requestors.

Guidelines for Using Encrypted Volumes

- The sys: volume cannot be encrypted. If your IT environment requires volume encryption, make sure to store user data on a separate volume.
- We recommend that you avoid mixing encryption and compression features in a volume. Use one or the other, but not both.
- You can enable the Encryption attribute only at volume creation time.
- If it is enabled, the Encrypted volume attribute persists for the life of the volume.
- To encrypt an existing volume, you must create a new encrypted volume, then migrate existing data from the nonencrypted volume to the encrypted volume.
- The encryption password is 6 to 16 standard ASCII characters.
- Backups of an encrypted volumes are not encrypted, unless it is a feature of the backup software you use.
- Make sure that you exclude the NSS cache memory from core dumps; otherwise, encrypted NSS volume data might be displayed in the clear.
- If you use Novell Archive and Version Services to create file versions of files on an encrypted NSS volume, make sure to encrypt the archive volume when you create it on the archive server. Otherwise, the file versions are not secure.

Creating an Encrypted Volume

In NetWare 6.5 Support Pack 2 and later, NSS Encrypted Volume Support (EVS) allows you to create encrypted NSS volumes using NSSMU version 3.20 build 940 or later. You cannot encrypt the sys: volume. You can create encrypted user data volumes only after the installation or upgrade process.

WARNING: We strongly recommend that you verify that your system is working as desired under NetWare 6.5 Support Pack 2 before using EVS to create encrypted volumes on the system. EVS is not supported by earlier versions of NSS. If you choose to encrypt a volume, you cannot roll back the system to an earlier version of NetWare without taking steps before the rollback to preserve data. For information, see ["Removing Encrypted Volumes" on page 175](#).

- 1 In NSSMU, select Volume Management, then press Enter.
- 2 To create a new volume, press the Insert key.
A query asks if you want to encrypt the volume.
- 3 To encrypt the new volume, select Yes, then press Enter.
EVS marks the volume with an attribute of Encrypted, then prompts you to enter a password for the volume.
- 4 Enter an encryption password, then enter it again to verify it.
The encryption password can be up to 16 standard ASCII characters, with a suggested minimum of 6. The password persists for the life of the volume; it cannot be changed later.
- 5 Set the volume size and other attributes, as desired.
When you are done, the encrypted volume is active and mounted.

You must supply the encryption password for the volume on the first volume activation after a system boot or reboot. For information about entering the password for a volume in a cluster, see “[Using Encrypted Volumes in a Server Cluster](#)” on page 173.

Using Encrypted Volumes in a Server Cluster

If you use an encrypted NSS volume in a Novell Cluster Services™ cluster, you must manually enter the password for the volume on one of the servers only when you first start or restart the cluster. You activate the NSS pool and volume on one of the servers, enter the volume password, then deactivate the pool and volume before you can bring the cluster resource online for the first time. NSS uses the password to create a key, which it stores in the server memory. The NCS software passes the key to other nodes. After all servers hold the key, the volume is available while any one of the servers is still participating actively in the cluster. If all servers in the cluster fail, you must repeat this procedure when you recover the cluster and restart services.

- 1 Boot or restart the servers in the cluster.
If you automated the loading of cluster resources, the cluster reports each resource is comatose because it cannot bring the corresponding encrypted volume online.
If you opt to manually start cluster resources, the cluster resources are not yet active.
- 2 From one of the nodes in the cluster, activate the encrypted volumes.

2a Activate the cluster pool and its encrypted volumes by entering the following commands at the server console:

```
nss /poolactivate=poolname  
nss /volumeactivate=volumename
```

At the prompt, enter the password for the encrypted volume. NSS creates the 128-bit encryption key and stores it in the server’s memory.

If the server already knows the key for the volume, you are not prompted for the password.

2b To deactivate the cluster pool, enter

```
nss /pooldeactivate=poolname
```

3 Follow the normal procedures to activate the cluster resources.

For information, see the *Novell Cluster Services 1.7 Administration Guide*. The node passes the key information to the other nodes. While at least one of the servers is actively participating in the cluster, you do not have to reenter the encryption password again.

Archiving Files from an Encrypted Volume

If you use Novell Archive and Version Services to archive files from an encrypted volume, the destination path for Archive Manager must be on an encrypted volume. If the destination path is a nonencrypted volume, the versioned data is stored in a nonencrypted state.

Using Direct I/O on an Encrypted Volume

Direct I/O to an encrypted volume bypasses the EVS encryption engine and allows data to be stored in nonencrypted format on the encrypted volume. This capability is useful for diagnostic, repair, or special-purpose applications, but should be avoided otherwise.

You should avoid using direct-I/O applications on encrypted volumes, especially for user data that you intend to be stored in encrypted format.

Managing Encrypted Volumes with NSS Commands

You can use NSS console commands to display volume status and to activate, mount, deactivate, or dismount encrypted volumes. You must enter a password only on the first activation following a system reboot. Thereafter, other environmental security and authentication measures control access to user data.

The following table provides the syntax for NSS commands to use with encrypted volumes. You can use this syntax to activate an encrypted volume from the console command line prompt or in a script file. In each case, replace *volname* with the name of the encrypted NSS volume. In general, you cannot use the wildcard option of “all” as the *volname*. Until an encrypted volume is activated with its password following each system reboot, the All option does not find the volume and does not execute the command. The system returns an error message, requesting more information.

Replace *volpassword* with the password you used when you created the encrypted volume. If the password is not supplied and a corresponding key is not found in memory, NSS prompts for the password at the command line.

Command	Use To
<code>nss /activate=volname:volpassword</code>	Activate the encrypted NSS volume the first time after a system reboot.
<code>nss /activate=volname</code> If prompted, enter <i>volpassword</i> for the encrypted volume.	Activate the encrypted NSS volume in two steps. The password is required only on the first activation following a system reboot.
<code>nss /volumeactivate=volname:volpassword</code>	Activate the encrypted NSS volume the first time after a system reboot.
<code>nss /activate=all</code>	Activate all encrypted NSS volumes that have been previously activated with their passwords.

Command	Use To
<code>nss /forceactivate=volname</code>	Forces activation for an encrypted NSS volume that has been previously activated with its password. Encrypted NSS volumes that were not previously activated return an error message, requesting more information.
<code>nss /volumes</code>	Display the status of encrypted and nonencrypted NSS volumes. The encrypted volume returns a status of Encrypted.
<code>mount volname</code>	Mount an encrypted or nonencrypted NSS volume. The mount command is usable for encrypted volumes only after a previous activate with password. Otherwise, it returns an error message, requesting more information.
<code>mount all</code>	Activate and mount all encrypted NSS volumes that have been previously activated with their passwords. Encrypted NSS volumes that were not previously activated return an error message, requesting more information.

You cannot use wildcard options and commands to activate encrypted volumes, such as `nss /VolumeAutoActivate`.

Removing Encrypted Volumes

Encrypted volumes require NetWare 6.5 Support Pack 2 and later. Because earlier releases of NSS cannot activate an encrypted volume, you cannot roll back the system from Support Pack 2 to Support Pack 1. If you do, the encrypted volume fails to activate and its pool cannot be repaired.

To prevent this potential data loss, make sure that the system upgrade to Support Pack 2 is active and performing as desired before creating encrypted volumes.

If a rollback becomes necessary, you must remove the encrypted volume from the server before you perform the rollback.

1 Create a nonencrypted volume.

For information, see “[Creating an Encrypted Volume](#)” on page 172.

2 Use one of these methods to save the encrypted volume’s data on the nonencrypted volume:

- ◆ Back up the volume’s data in nonencrypted format on backup media, then restore the data to the nonencrypted volume.
- ◆ Make a volume-to-volume copy of the data from the encrypted volume to the nonencrypted volume.

3 Delete the encrypted volume.

4 Perform the system rollback.

What's Next

Manage other NSS features of your encrypted volume as you would for a nonencrypted volume. For information, see “[Managing NSS Volumes](#)” on page 127.

13

Using Compression to Conserve Storage Space on NSS Volumes

Novell® Storage Services™ file compression uses algorithms to reduce the amount of space a file consumes in your storage system. Compression helps conserve disk space and increase the amount of data a volume can store. No data in the file is permanently eliminated to compress the file; all original data is recovered when the file is decompressed.

Compression is a common file service available for both NSS and Traditional volumes. For information on Traditional volumes and compression, see *NetWare 6.5 Traditional File System Administration Guide*.

This section discusses the following:

- ◆ “Understanding File Compression” on page 177
- ◆ “Planning for File Compression” on page 180
- ◆ “Configuring Compression Parameters for a Server” on page 182
- ◆ “Configuring a Volume for Compression” on page 184
- ◆ “Suspending Compression for Volumes or Files” on page 186
- ◆ “Disabling Compression for a Volume” on page 186
- ◆ “Restoring Data to a Uncompressed Volume” on page 186
- ◆ “Configuring Compression Attributes for Directories and Files” on page 186
- ◆ “Using NSS Commands to Configure and Monitor Compression” on page 188
- ◆ “Copying Compressed Files between Volumes with the Ncopy Command” on page 189
- ◆ “Viewing the File Attributes with the Ndir Command” on page 189
- ◆ “Repairing Compressed Volumes with the Compfix Utility” on page 189

Understanding File Compression

Although the cost of storage media is decreasing, you might consider compression to store more information on media where available space is limited. This section discusses the following:

- ◆ “Compression Settings” on page 178
- ◆ “Compression and Decompression Processes” on page 178
- ◆ “Compression Criteria” on page 178
- ◆ “Decompression Criteria” on page 179
- ◆ “Compression and Storage Backup” on page 179

Compression Settings

File compression requires configuration at three levels: server, volume, and individual directories and files. The server's compression parameters govern when and how compression works for all compressed volumes on the server. The volume's Compression attribute determines if its files can be compressed. You can enable the attribute when you create a new volume or add it at any time for an existing volume. After it is set, the Compression attribute persists for the life of the volume. For individual directories and files, you can set compression preferences that allow file compression to occur immediately for specified files, regardless of the server's compression parameters. You can also specify restrictions for individual files that make them ineligible for compression.

Compression and Decompression Processes

File compression and decompression processes occur in the background, as needed for each compressed volume, to support normal file access and immediate file compression settings. Scheduled compression occurs during a specified time each day. Typically, the scheduled period is set to nonpeak hours, but it can occur at any time you prefer.

During scheduled compression, NSS evaluates file time stamps and all compression settings to determine which files qualify for compression. When it queues eligible files for compression, the compression process begins and handles as many compression tasks as it can in the available time. Any remaining queued files wait for the next compression opportunity.

To minimize the impact of compression and decompression on system performance, you can limit the maximum number of concurrent process threads the system devotes to it. The system queues compression and decompression requests, then processes them as process threads become available.

NSS retains the uncompressed file during the compression process. Before NSS compresses a file, it verifies that the file system has enough space available for both the uncompressed file and the compressed file to temporarily coexist. If there is not enough space available, the file is not compressed. If compression completes successfully, NSS replaces the uncompressed file with the compressed file. If errors occur during compression, NSS discards the compressed file and marks the uncompressed file with a Cannot Compress (Cc) attribute.

NSS does not attempt to compress a file while its Cc attribute is set to On. If the file is opened and saved, its Cc attribute is reset to Off. You can also run the Compxfix utility to clear the Cc attribute. For information, see ["Repairing Compressed Volumes with the Compxfix Utility" on page 189](#).

Compression Criteria

Typically, files that have been inactive for a specified period of time are eligible for compression. Other criteria can be used to identify files for compression:

- Files reside in a directory marked for immediate compression
- Files reside in subdirectories of a directory marked recursively for immediate compression
- Individual files are marked for immediate compression

Several factors prevent an uncompressed file from being compressed, even if it meets inactivity criteria:

- The file is flagged with a Do Not Compress (Dc) attribute.
- The file is an NSS sparse file, so its physical storage size is already minimized. A sparse file contains numerous contiguous zeros that NSS stores in a special way to conserve space.

- The amount of space freed by compressing a file does not meet the specified minimum reduction criteria. For example, if the Minimum Compression Percentage Gained parameter is set to 20%, a file would not be compressed if compression reduced its file size by only 10%.
- The file compression service is suspended.
- The queue of files marked for compression is long and cannot be completed during the specified hours set aside for compression activities.
- The volume does not contain enough space to hold both the original version and the compressed version of the file while compression occurs.
- The file has been deleted and the Deleted File Compression Option parameter does not allow compression of deleted files.

Decompression Criteria

Decompression occurs as needed to support file access, but other factors affect whether the uncompressed version or compressed version of the file remains in the volume after the access. The files remain compressed in the following cases:

- The percentage of free disk space available on the volume is insufficient to allow a decompressed file to remain in its uncompressed state.
- The Convert Compressed to Uncompressed Option parameter requires that compressed files always remain compressed.
- The file was opened for the first time for viewing only and the Convert Compressed to Uncompressed Option parameter requires that the file must be opened at least twice for a viewing only or opened once for modification before the file remains uncompressed after access.

Whenever you open a compressed file, NSS decompresses the file, but it keeps the compressed copy of the file while the file is open. The first time you open a compressed file for viewing only, when you close the file, NSS discards the decompressed copy of the file. The compressed file remains on the system. If you open the file a second time for viewing only, the file is considered active. When you close the file, NSS keeps the uncompressed file and discards the compressed copy of the file. If you modify the file and save it, NSS saves the uncompressed file, then discards the compressed file.

Compression and Storage Backup

When you back up a compressed volume, files are written to the backup media in compressed or uncompressed format, according to how they are currently stored. To back up compressed files in uncompressed format, you must decompress the files first, then back up the files.

When you recover a volume, the files are restored in their saved format to the destination volume. If you try to restore a compressed file to a volume without compression, the file is not readable. For information, see “[Guidelines to Back Up Compressed Files](http://www.novell.com/documentation/nw65/smsadmin/data/hwcql1x9.html)” (<http://www.novell.com/documentation/nw65/smsadmin/data/hwcql1x9.html>) in the *NetWare 6.5 Storage Management Services Administration Guide* (<http://www.novell.com/documentation/nw65/smsadmin/data/hjc2z4tu.html>), or see your third-party backup application’s documentation.

Planning for File Compression

To effectively use compression for your NSS volumes, you must understand the following key concepts:

- ◆ “Inactivity Determines Which Files Are Eligible for Background Compression” on page 180
- ◆ “Some Files Do Not Compress Well” on page 180
- ◆ “Some Volumes Are Not Good Candidates for Compression” on page 181
- ◆ “Decompression Activity Depends on Available Space” on page 181
- ◆ “Immediate Compression Impacts CPU Performance” on page 181
- ◆ “Files Remain Compressed during Backup and Restore” on page 181
- ◆ “If Set, the Compression Attribute Persists for the Life of the Volume” on page 181
- ◆ “How to Monitor Compression Activity” on page 181

Inactivity Determines Which Files Are Eligible for Background Compression

NSS compresses files based on the interval of time that a file remains inactive. With background compression, files automatically pass in and out of their compressed state as they are unused, then used. It is not necessary to separate application files from data files for file compression. Most application files are used regularly and are not inactive long enough to qualify for compression.

Use the compression parameter named **Days Untouched before Compression** to set the length of the interval of inactivity. The parameter uses the date the file was last accessed for reading or writing to determine if a file is inactive, and therefore, eligible for compression.

To determine the optimal period of inactivity to use, consider the frequency of use of different types of files and your compression goals. Application files tend to be used more frequently, while user data is used less frequently. For example, the shorter the period of inactivity is, the higher the frequency of compression. The longer the period of inactivity is, the lower the frequency of compression, and the less likely it is that files are ever compressed.

Use the **Flag** command to enable immediate compression for a file or directory. For information, see “[Configuring Compression Attributes for Directories and Files](#)” on page 186.

Some Files Do Not Compress Well

To avoid the overhead of decompressing files that do not compress well, the system calculates the compressed size of a file before actually compressing it. If no disk space is saved by compression, or if the size difference does not meet the value specified by the **set** command’s **Minimum Percentage Compression Gain** parameter, the file is not compressed.

NSS does not compress NSS sparse files. A sparse file contains numerous contiguous zeros that NSS stores in a special way to conserve space. A sparse file’s logical size is larger than its physical disk usage. If a sparse file were compressed, it would actually consume more storage space than it normally does.

A file must be larger than 8 KB and smaller than 256 MB to be eligible for compression. The compression algorithm determines these limits.

Some Volumes Are Not Good Candidates for Compression

Compression is not recommended for the sys: volume. Reserve compression for user data volumes. You cannot use compression on an NSS volume on a CD or DVD drive.

Decompression Activity Depends on Available Space

Compressed files are uncompressed as they are needed, then remain uncompressed until they are inactive for a designated period. For a file to be uncompressed, there must be enough free space on the volume to accommodate the decompression process and the uncompressed file size.

Immediate Compression Impacts CPU Performance

Compression requires processor resources, memory resources, and hard disk space during the compression and decompression processes. Compression is usually a low priority process thread because of compression's impact on performance. If you flag many large files for immediate compression during peak system usage, CPU performance might deteriorate.

You can configure the server's compression parameters to control how compression services use resources. For example, you can schedule compression to occur only during non-peak hours to free CPU resources during peak and normal hours. For information, see [“Configuring Compression Parameters for a Server” on page 182](#).

Files Remain Compressed during Backup and Restore

Backup applications that use Novell Storage Management Services™ (SMS) back up and restore files in their compressed state.

If Set, the Compression Attribute Persists for the Life of the Volume

The Compression attribute for a volume can be set when you create the NSS volume, or at any time thereafter. After you set the Compression attribute for a volume, you cannot turn it off; the parameter is in effect for the life of the volume.

You can suspend the compression activity, as needed, using the [Enable File Compression](#) parameter. This parameter suspends compression for all volumes on the server. For information, see [“Suspending Compression for Volumes or Files” on page 186](#) and [“Disabling Compression for a Volume” on page 186](#).

If you want to turn off file compression permanently, you must back up the volume in its uncompressed state, then restore the data to a new volume on which the Compression attribute is not set.

How to Monitor Compression Activity

Monitor compression activity using the Compress Screen parameter. For instructions, see [“Using NSS Commands to Configure and Monitor Compression” on page 188](#).

Configuring Compression Parameters for a Server

Compression parameters govern compression behavior for all volumes on your server. The server-level settings apply to all files and directories in compression-enabled volumes on the server.

To configure the server's compression parameters, use one of the following management utilities:

- ♦ Monitor
- ♦ Novell Remote Manager
- ♦ Set Command

This section discusses the following:

- ♦ [“Understanding Compression Parameters” on page 182](#)
- ♦ [“Setting Compression Parameters with Monitor” on page 184](#)
- ♦ [“Setting Compression Parameters with Novell Remote Manager” on page 184](#)
- ♦ [“Setting Compression Parameters with the Set Command” on page 184](#)

Understanding Compression Parameters

The following table describes each compression parameter, its purpose, supported values, and default value.

Parameter	Use to
Compression Daily Check Stop Hour	<p>Specify the hour when you want the file compressor to stop scanning enabled volumes for files that need to be compressed and to stop compressing them.</p> <p>Supported Values: 0 to 23</p> <p>Hours are specified by a 24-hour clock: (0 = midnight; 23 = 11 p.m.).</p> <p>Default Value: 6</p>
Compression Daily Check Starting Hour	<p>Specify the hour when you want the file compressor to start scanning enabled volumes for files that need to be compressed and to compress them.</p> <p>If the Compression Daily Check Stop Hour parameter is the same as the Compression Daily Check Starting Hour, then the file compressor starts checking every day at the Compression Daily Starting Hour time and runs as long as necessary to finish all files that meet the compressible criteria.</p> <p>Supported Values: 0 to 23</p> <p>Hours are specified by a 24-hour clock: (0 = midnight; 23 = 11 p.m.).</p> <p>Default Value: 0</p>
Minimum Compression Percentage Gain	<p>Set the minimum percentage a file must compress to remain in a compressed state.</p> <p>Supported Values: 0 to 50</p> <p>Default Value: 20</p>

Parameter	Use to
Enable File Compression	<p>Specify whether file compression for the volume is suspended. While file compression is suspended, files that would have been compressed are queued, then compressed when compression is re-enabled.</p> <p>Supported Values: On or Off</p> <p>On allows file compression on compression-enabled volumes.</p> <p>Off suspends compression; immediate compression requests are queued until the value is reset to On, when the files meeting criteria are compressed.</p> <p>Default Value: On</p>
Maximum Concurrent Compressions	<p>Specify the maximum concurrent or simultaneous compressions allowed.</p> <p>Supported Values: 1 to 8</p> <p>Default Value: 2</p>
Convert Compressed to Uncompressed Option	<p>Specify what the file system does with an uncompressed version of a file after the server has decompressed it.</p> <p>Supported Values: 0, 1, or 2</p> <p>0 = Always leave the file compressed</p> <p>1 = Leave the file compressed until second access if it is read only once during the time specified by the Days Untouched Before Compression parameter</p> <p>2 = Always leave the file decompressed</p> <p>Default Value: 1</p>
Decompress Percent Disk Space Free to Allow Commit	<p>Specify the percentage of free disk space required on a volume for file decompression to permanently change compressed files to decompressed. This parameter prevents newly decompressed files from filling up the volume.</p> <p>Supported Values: 0 to 75</p> <p>Default Value: 10</p>
Decompress Free Space Warning Interval	<p>Specify the time between alerts when the file system is not changing compressed files to decompressed because of insufficient disk space.</p> <p>Supported Values: 0 seconds to 29 days 15 hours 50 minutes 3.8 seconds</p> <p>Setting the interval to 0 turns off the alert.</p> <p>Default Value: 31 minutes 18.5 seconds</p>
Deleted Files Compression Option	<p>Specify whether and when deleted files are compressed.</p> <p>Supported Values: 0, 1, or 2</p> <p>0 = Do not compress deleted files</p> <p>1 = Compress deleted files the next day</p> <p>2 = Compress deleted files immediately</p> <p>Default Value: 1</p>

Parameter	Use to
Days Untouched Before Compression	<p>Specify the number of days the system waits after a file was last accessed before it is compressed. To effectively stop compression for a volume, set the elapsed time very high. Eventually, files are decompressed and remain uncompressed because they never cross the inactivity threshold.</p> <p>Supported Values: 0 to 100000</p> <p>Default Value: 14</p>

Setting Compression Parameters with Monitor

Monitor is a console-based management tool that allows you to configure and monitor server parameters, such as compression. In Monitor, select Common File Systems from the Available Options menu. The menu options include the ten compression parameters, as defined in the preceding section.

For information about using Monitor, see “[Monitor](#)” in the *NetWare 6.5 Utilities Reference*.

Setting Compression Parameters with Novell Remote Manager

You can modify compression parameter values using the Set Parameters option in Novell Remote Manager. For information on using Set Parameters, see “[Viewing or Changing Set Parameters](#)” in the *NetWare 6.5 Novell Remote Manager Administration Guide for NetWare*.

Setting Compression Parameters with the Set Command

You can use the Set command at the server console to configure and view Common File System parameters for compression. Compression parameters apply to both the NSS file system and the Traditional file system.

Enter the following at the server console

```
set parameter = value
```

Replace *parameter* with the compression parameter’s name. Replace *value* with its setting.

The system is immediately configured to the specified setting. Commands issued at the command prompt override any setting in the autoexec.ncf file. Parameter settings are persistent in NSS. If the server goes down, your setting modifications are not lost.

You can place Set commands that you execute at the console prompt in the autoexec.ncf or the startup.ncf file. Whenever a parameter value is set in the autoexec.ncf file, the server configures itself to that setting each time the server is booted, unless the value is modified. Use the NWCONFIG utility to edit both the autoexec.ncf and the startup.ncf file. For information, see “[NWCONFIG](#)” in the *NetWare 6.5 Utilities Reference*.

Configuring a Volume for Compression

To use compression on a volume, set the volume’s Compression attribute to On. You can set the Compression attribute when you create a new volume or enable the attribute for an existing non-compressed volume. After you enable compression for a volume, you can suspend compression, but you cannot turn the Compression attribute off.

IMPORTANT: You cannot use file compression on a volume on a CD or DVD drive.

For information, see “[Suspending Compression for Volumes or Files](#)” on page 186.

Enabling Compression for a New Volume

When you create a new volume, simply select the Compression check box when you set the volume’s attributes. For information, see “[Configuring Nonencrypted NSS Volumes with iManager](#)” on page 131.

Enabling Compression for an Existing Volume

- 1 In iManager, click Storage > Volumes to open the Volume Management page.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

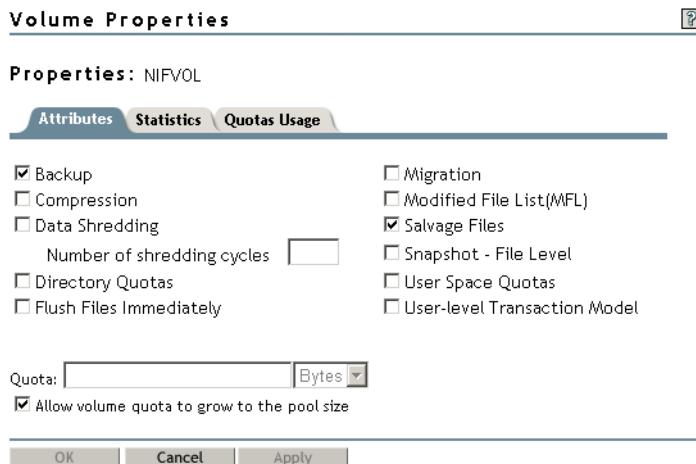
A list of volumes appears in the Volumes list.

- 3 From the Volumes list, select the volume that you want to manage.

- 4 Click Properties > Attributes.

This opens the Volume Properties to the Attributes page.

[Storage Management](#) ▶ [Volumes](#) ▶ [Volume Properties](#)



- 5 Select the Compression check box to enable file compression for the selected volume.

IMPORTANT: After compression is enabled for a volume, you cannot deselect the Compression check box to turn off compression. You can suspend compression or restore uncompressed data to an uncompressed volume. For information, see “[Suspending Compression for Volumes or Files](#)” on page 186 or “[Restoring Data to a Uncompressed Volume](#)” on page 186.

- 6 Click Apply or OK to save the change, or click Cancel to back out of the process.

If you click Apply, iManager saves the change and remains on the Volumes page. If you click OK, iManager saves the change and takes you to the main Storage page. If you do not click Apply or OK, the setting is not implemented; the volume remains uncompressed.

Suspending Compression for Volumes or Files

You can temporarily suspend file compression for all volumes, using the set command's [Enable File Compression](#) parameter. While file compression is suspended, files that would have been compressed are queued for compression, then compressed when compression is re-enabled. For information, see [“Configuring Compression Attributes for Directories and Files” on page 186](#).

You can suspend compression for a file by setting its [Do Not Compress](#) flag. For information, see [“Configuring Compression Attributes for Directories and Files” on page 186](#).

Disabling Compression for a Volume

After compression is enabled for a volume, you cannot deselect the Compression attribute check box to turn off compression. Use one of the following methods to disable compression for a volume.

- ♦ To effectively stop compression for a volume, set the [Days Untouched Before Compression](#) parameter's elapsed time to the maximum value. Eventually, files will be decompressed as they are used and remain uncompressed because they never cross the threshold for inactivity.
- ♦ Restore the data to an uncompressed volume. For information, see [“Restoring Data to a Uncompressed Volume” on page 186](#).
- ♦ Set [Enable File Compression](#) to Off. Eventually, files will be decompressed as they are used and remain uncompressed.

Restoring Data to a Uncompressed Volume

- 1 Decompress the volume data.
- 2 Back up an uncompressed data.
- 3 Create a new volume with the Compression attribute disabled.
- 4 Restore the old volume contents as uncompressed data from your backup media.

Configuring Compression Attributes for Directories and Files

You can use the Flag command at a server console to view or modify file and directory attributes for compression. File and directory compression attributes override the compression attribute setting for the volume itself.

- ♦ [“Using the Flag Command” on page 187](#)
- ♦ [“Setting Compression Attributes for a Directory” on page 187](#)
- ♦ [“Setting Compression Attributes for a File” on page 188](#)
- ♦ [“Viewing Compression Status for Files and Directories” on page 188](#)

For general Flag command options, see [“FLAG” in the *NetWare 6.5 Utilities Reference*](#).

Using the Flag Command

The Flag command is typically in the sys:\public directory. The general syntax for the Flag command is

```
sys:public\flag.exe path [+ | -] attribute... [/option...] [/? | /VER]
```

Parameter	Use to
(no parameter)	If you type FLAG with no parameters, the attribute status of all the files in the current directory appears.
<i>path</i>	Specify the path to the file or directory whose attributes or search modes you want to modify.
+ -	<p>Add attributes to a specified file or directory with the + (plus), or specify neither + nor - (minus).</p> <p>Remove attributes from a specified file or directory with the - (minus).</p> <p>If you add and remove attributes in the same command, group all + (plus) attributes together and all - (minus) attributes together.</p>
<i>attribute</i>	<p>Specify one or more file or directory attributes.</p> <p>See “Setting Compression Attributes for a Directory” on page 187 and “Setting Compression Attributes for a File” on page 188.</p>
<i>/option</i>	<p>Replace option with any available option.</p> <p>Use the /S option to search the subdirectories in the specified directory recursively to apply the command to files in the directory and to its subdirectories and the files beneath them.</p> <p>For other options, see “General FLAG Options” in the <i>NetWare 6.5 Utilities Reference</i>.</p>
/?	View online help. The Flag command ignores other parameters when the /? switch is used.
/VER	View the version number of the utility and the list of files it uses to execute. The Flag command ignores other parameters, except /?, when /VER is used.

Setting Compression Attributes for a Directory

Use the Flag command to add or delete compression attributes for a specified directory.

Option	Use to
Ic (Immediate compress)	<p>Compress the files in the specified directory as soon as the operating system can.</p> <p>This does not apply to the directory's subdirectories and the files in them. Use Ic in combination with the /S option to apply immediate compression to the directory's subdirectories and their files recursively.</p>

For example, to add the Immediate Compress attribute to the sys:\course\winter directory, enter

```
flag sys:\course\winter +Ic
```

For example, to remove the Immediate Compress attribute from the sys:\course\winter directory, enter

```
flag sys:\course\winter -Ic
```

Setting Compression Attributes for a File

Use the Flag command to add or delete compression attributes for a specified file.

Option	Use to
Dc (Do not compress)	Prevent a specified file from being compressed.
Ic (Immediate compress)	Compress a file as soon as the OS can.

For example, to add the Do Not Compress attribute to all files in the current directory, enter

```
flag *.* +Dc
```

For example, to remove the Immediate Compress attribute from the students.sxi file in the sys:\course\winter directory, enter

```
flag sys:\course\winter\students.sxi -Ic
```

Viewing Compression Status for Files and Directories

Status flags show the compression attribute information for a file or directory. You cannot modify Status flags.

Status	Indicates
Cc (Cannot compress)	The file cannot be compressed because of limited space savings.
Co (Compressed)	The file is currently stored in compressed format.

To view the compression status of a file, enter the following at the server console:

```
flag path
```

Replace *path* with the path to the directory or file. For example, to view the attributes of the students.sxi file in sys:\course\winter directory, enter

```
flag sys:\course\winter\students.sxi
```

To view the attributes of all files in the current directory, enter

```
flag
```

Using NSS Commands to Configure and Monitor Compression

NSS offers the following commands for configuring and monitoring compression. Enter the commands at the server console.

Command	Use to
<code>nss /Compression=volume_name</code>	Enable the Compression attribute for the specified volume.
<code>nss /Compression=all</code>	Enable the Compression attribute for all volumes on the server.
<code>nss /StopNormalCompression</code>	Stop all queued compression for files, based on the compression triggered by a file open or close.
<code>nss /BGCompression</code>	Allow compression to occur in the background at any time, instead of only within specified hours.
<code>nss /NoBGCompression</code>	Stop background compression. Allow compression to occur only within the specified hours.
<code>nss /CompScreen</code>	Display the NSS volume compression statistics on the compression screen.

Copying Compressed Files between Volumes with the Ncopy Command

The Ncopy command provides two attributes to specify your intention for copying a compressed file to a compressed volume or a non-compressed volume. Enter the commands at the server console.

Command	Use to
<code>ncopy /R</code>	Retain compression on supported media.
<code>ncopy /R/</code>	Retain compression on unsupported media.

Viewing the File Attributes with the Ndir Command

The Ndir command allows you to view file attributes and compression information for all files in a directory. Enter the commands at the server console.

Command	Use to
<code>ndir /R</code>	View the file attributes for all files in a directory.
<code>ndir /COMP</code>	View the compression information for all files in a directory. It shows the amount of disk space saved by compressing data.
<code>ndir /COMP /VOL</code>	View the compression information for the volume. It also shows the disk space saved on the volume.

Repairing Compressed Volumes with the Compfix Utility

Use the Compfix utility to repair compression information for compressed volumes or to clear the Cannot Compress attribute for files in the compressed volume. Load compfix.nlm on your server, then enter the Compfix command at the server console. Compfix.nlm runs on processor 0 only.

`compfix -[attribute] [-noheader] path [log_volume]`

Parameter	Use to
path	Specify the compressed volume or the individual file on a volume that has compression errors you want to repair. For example, <i>volume</i> or <i>volume</i> : <i>path</i> , where <i>path</i> includes the file name and is in the Long name space.
<i>log_volume</i>	If <i>log_volume</i> is specified, log data is written to <i>log_volume</i> :\\compfix.txt.
	If <i>log_volume</i> is not specified, log data is written to <i>volume</i> :\\compfix.txt.
-noheader	If -noheader is specified, no compression header will be validated. Use this on scanned volumes.
-fs	Fix compression statistics. Make sure the volume is in maintenance mode before you begin for statistics to be properly computed.
-lc	List all corrupted compressed files on the volume.
-df	Diagnose an individual compressed file.
-ff	Fix an individual compressed file.
-fc	Fix all fixable corrupted compressed files on the volume.
-bg	Diagnose the background compression effect for an individual file.
-cc	Clears the Cannot Compress (Cc) attribute for files in the specified volume or for a specified file.

The following table illustrates typical uses of the Compfix utility.

Command	Use to
compfix -fs <i>volume</i>	Fix compression statistics for the specified volume. The specified volume should be in maintenance mode in order for statistics to be computed correctly.
compfix -lc [-noheader] <i>volume</i> [<i>log_volume</i>]	List all corrupted compressed files on the specified volume.
compfix -df [-noheader] <i>volume</i> :\\ <i>path</i> [<i>log_volume</i>]	Diagnose an individual compressed file.
compfix -ff <i>volume</i> :\\ <i>path</i>	Fix an individual compressed file.
compfix -fc [-noheader] <i>volume</i> [<i>log_volume</i>]	Fix all fixable corrupted compressed files on the specified volume.
compfix -bg <i>volume</i> :\\ <i>path</i> [<i>log_volume</i>]	Diagnose the background compression effect for an individual file.
compfix -cc <i>volume</i> [<i>log_volume</i>]	Clears the Cannot Compress (Cc) attribute for files in the specified volume.

14

Using Distributed File Services for Moving and Splitting NetWare 6.x NSS Volumes

In NetWare® 6 and later, Novell® Distributed File Services (DFS) allows you to develop a logical view of your storage solution and provides tools to help you modify the underlying physical organization to maximize the use and performance of available storage resources.

This section discusses the following topics:

- ◆ “Understanding DFS” on page 191
- ◆ “Prerequisites and Guidelines for DFS” on page 193
- ◆ “Creating a DFS Management Context for NCP” on page 195
- ◆ “Enabling DFS Junction Support for CIFS Clients” on page 196
- ◆ “Creating a DFS Junction Manually with ConsoleOne” on page 197
- ◆ “Viewing a DFS Junction” on page 197
- ◆ “Deleting a DFS Junction Manually with ConsoleOne” on page 198
- ◆ “Managing the Volume Location Database Service” on page 198
- ◆ “Moving Volumes with iManager” on page 199
- ◆ “Splitting Volumes with iManager” on page 201
- ◆ “Managing Move or Split Jobs” on page 203

Understanding DFS

Novell Distributed File Services provides tools to help you modify the underlying physical organization to maximize the use and performance of available storage resources. With DFS, you can split a volume at any directory and move its contents to a new volume. It places a junction file in the directory’s location and uses a Volume Location Database (VLDB) to redirect queries automatically to the data’s new location, which preserves the logical file organization from the user perspective. DFS tools include the VLDB, DFS Junctions, and the Move Volume and Split Volume functions.

In NetWare 6.x, Novell Distributed File Services comprise the following key components.

- ◆ “Volume Location Database” on page 192
- ◆ “DFS Junctions” on page 192
- ◆ “Move Volume Jobs” on page 192
- ◆ “Split Volume Jobs” on page 192
- ◆ “Original and New Volumes” on page 193

Volume Location Database

With DFS, you can create a Volume Location Database (VLDB) for NetWare 6.x NSS volumes in the same Novell eDirectory™ tree. The VLDB maps the physical location of NetWare 6.x NSS volumes on all servers in the tree. It is the VLDB service and database that allows you to create junctions. DFS junctions retrieve the current location of a volume from the VLDB in order to dynamically redirect queries to the physical location of the volume it represents.

DFS Junctions

A DFS junction is a logical placeholder for data stored on a NetWare 6.x NSS volume. It is a virtual directory that points to the root of a destination volume. The junction itself can be located anywhere in the source volume. A junction functions like an alias in Novell eDirectory that appears to be a normal eDirectory object. To the user, a DFS junction appears to be any normal directory in your NetWare file system. For DFS junctions created manually with ConsoleOne®, the destination volume can be any NetWare 6.x NSS volume in the same eDirectory tree. For junctions created automatically by a Split Volume process, the destination volume can be any NetWare 6.x NSS volume in the same eDirectory management context.

Whenever you create a junction, the VLDB service assigns the junction a unique ID, which is automatically stored in its database. Whenever a user views the contents of a junction, the client looks at the unique ID, queries the database to find the path to the physical volume associated with the unique ID, and then displays the contents of that physical volume.

Junctions eliminate the user's need to know the path to the physical location of the data. For example, if John's data is located on servers X, Y, and Z, you can create junctions on server X that point to all of his data on servers Y and Z. That way, John only needs to remember the path to server X, because with junctions, it appears as if the data is all located in one place.

The benefit of this feature is twofold: Not only does it decrease administration costs by allowing you to move a volume to a different server without making any announcements or needing to reeducate users, but it also simplifies the number of paths a user needs to remember if the data is spread among different volumes or servers.

Move Volume Jobs

With DFS, you can move a NetWare 6.x NSS volume and its contents to a new NSS volume faster than with a normal copy. You can move a crowded volume to a different pool that has space available or is expandable. You can move volumes to different servers in the same context to balance associated traffic and workload across multiple servers. After the move, you must modify scripts and mappings for the original volume to point to the new volume. Any DFS junctions that pointed to, or are in, the original volume are automatically updated in the VLDB with the new volume information.

Split Volume Jobs

With DFS, you can split a NetWare 6.x NSS volume at a specified directory and relocate the directory contents to a new volume on the same or different server anywhere in the same eDirectory management context. The new volume typically resides in a different pool. After a successful relocation of directory contents, DFS automatically creates a DFS junction at the split point, which replaces the directory. The DFS junction redirects queries to the new location. Users can continue to access their data on the new volume, without modifying the familiar logical paths.

For example, suppose you have a server that holds all of your users' home directories. You know that you have enough free space for the data; however, the files are accessed so frequently that it increases the server load and decreases performance. Using DFS, you can split the volume, moving the home directories of the users with last names starting with L-Z to another volume in the same server or a different server. After the volume is split, NSS uses the junction to redirect traffic from the L-Z users. Users can log in to the original server even though their data is now physically located on a different volume.

Original and New Volumes

When you move or split a volume, the data is relocated from the original location to a new location and new volume. The new volume typically has a different name than the original volume; the names must be different if the new volume resides on the same server as the original volume.

Element	Description
Original location	The NetWare 6.0 or later server where the original NSS volume resides when the Move Volume or Split Volume job is initiated
Original volume	The source of the content for the new volume. For moves, it is the NetWare 6.0 or later NSS or Traditional volume that you want to relocate. For splits, it is the NetWare 6.0 or later NSS volume that you want to split.
New location	The destination NetWare 6.0 or later server where the new NSS volume resides
New volume	The NetWare 6.0 or later NSS volume that is created to contain the data from the original volume

Prerequisites and Guidelines for DFS

This section discusses the following prerequisites and guidelines for using DFS:

- ◆ [“Prerequisites for Creating and Using DFS Junctions” on page 193](#)
- ◆ [“Guidelines for Creating DFS Junctions Manually” on page 194](#)
- ◆ [“Guidelines for Original Volumes and New Volumes” on page 194](#)
- ◆ [“Guidelines for Managing Move Volume or Split Volume Jobs” on page 195](#)
- ◆ [“Guidelines for Files in Nearline Storage” on page 195](#)

Prerequisites for Creating and Using DFS Junctions

- ◆ DFS is available only on NSS volumes on NetWare 6.0 and later.
- ◆ You can create DFS junctions only in NSS volumes that reside on your NetWare 6.0 or later server.
- ◆ You can point a DFS junction in an NSS volume on NetWare to an NSS volume or a NetWare Traditional volume.
- ◆ Volumes must have an eDirectory Volume object to be usable with DFS. For example, if you create a DFS junction manually in ConsoleOne, you specify the destination volume for the data by selecting its eDirectory Volume object. Typically, whenever you create an NSS

volume, NSS creates a corresponding eDirectory object. It would be unusual not to have an eDirectory Volume Object for your volume.

To update the eDirectory Volume object, see “[Updating eDirectory Volume Objects](#)” on [page 133](#).

- ◆ You must create a DFS Management context before you can use DFS.

For information, see “[Creating a DFS Management Context for NCP](#)” on [page 195](#).

- ◆ If you are using CIFS, you must enable DFS support for CIFS clients.

For information, see “[Enabling DFS Junction Support for CIFS Clients](#)” on [page 196](#).

Guidelines for Creating DFS Junctions Manually

For DFS junctions you create manually, the following additional criteria must be met:

- ◆ The original and destination locations must be in the same Novell eDirectory tree.
- ◆ The destination volume must have an object defined in eDirectory.
- ◆ The destination volume’s server and the DFS junction’s server must share a networking protocol common to both, such as NCP™ or CIFS.

Guidelines for Original Volumes and New Volumes

Consider the following guidelines for original volumes and new volumes:

- ◆ You can split only NetWare 6.0 or later NSS volumes.
- ◆ You can move NetWare 6.0 or later NSS volumes or Traditional volumes.
- ◆ For both moves and splits, the destination volume must be an NSS volume on a NetWare 6.0 or later server.
- ◆ The destination volume can reside in the same or different pool than the original NSS volume.
- ◆ The destination volume can reside on the same or different server than the original NSS volume.
- ◆ The original NSS volume and the destination NSS volume must be in the same Novell eDirectory DFS Management Context.
- ◆ The access rights for the original and destination locations must be the same. The access rights for the original location are transferred automatically to the new volume. Make sure you have the appropriate rights on the destination server.
- ◆ The destination volume should be configured with the same attributes as the original volume. Review the attribute settings for the original volume before you begin a move or split job to be sure you know which attributes to set.
- ◆ The original volume and new volume must reside on servers configured to share the same networking protocol, such as NCP or CIFS.

Guidelines for Managing Move Volume or Split Volume Jobs

Consider the following guidelines for managing your move or split jobs:

- ♦ If the server crashes during a volume move or split operation, the operation resumes where it left off when the server comes back up.
- ♦ You can set up as many move or split jobs as you want; however, DFS can run only four active move or split operations at one time. After four requests, any additional requests must wait for one of the running operations to complete, or you must pause a job and start the operation you want to run.
- ♦ After you move a volume, you must modify mappings and scripts to point to the new physical location of the moved volume. If the volume contained DFS junctions, the junctions continue to work normally.
- ♦ When you split a volume, DFS automatically creates a DFS junction at the directory point where you split the volume. If the directory or its subdirectories contained DFS junctions, the junctions continue to work normally.

Guidelines for Files in Nearline Storage

If the Data Migration attribute is set for the NSS volume you want to move or split, some of its data might reside on tertiary storage media as nearline storage. The Move and Split processes demigrates the files from the tertiary storage and copies them to the new location. Make sure the original volume and new volume have enough space to incorporate both inline and nearline files during the demigration.

Creating a DFS Management Context for NCP

Before you create a DFS junction, you must create at least one DFS Management Context at an O or OU level in the Novell eDirectory tree where you want to create the junction. You can create more than one Management Context if you have a geographically diverse company. In that way, each geographic area can manage and control the junctions and the VLDB service within its own domain.

When you create a DFS Management Context, you specify which servers run the VLDB service and hold the actual database. It is the VLDB service, which includes its database, that allows you to create DFS junctions.

- 1 On the server that you want to make a VLDB server, open ConsoleOne and log in with the administrator username.
- 2 Navigate to the eDirectory container where you want to enable DFS support.
- 3 Right-click an O-level or an OU-level context in the eDirectory tree, then click New > DFS Management Context.
- 4 Select the server from the Available list, click the Right-arrow to move it into the Selected list, then click Next.

The server you select runs the VLDB service and houses the database.

- 5 Specify where you want to store the database on the server, and then click Finish.

The default location is the sys:\etc directory.

After you create the DFS Management Context, DFS creates attributes for volume objects in the eDirectory container object for the specified server, and it starts DFS on the server you selected.

- 6 (Conditional) For a larger eDirectory tree, with servers located in multiple eDirectory containers, manually run VLDB Repair from the server console.

IMPORTANT: You must start the VLDB Repair command from the server console immediately after creating the DFS Management Context; do not start it from ConsoleOne.

The VLDB Repair adds a GUID to every volume object in the eDirectory containers for other servers in the tree and enables the DFS Junction function for all the NetWare 6.x servers in the tree.

- 7 (Optional) You can specify a second server in the same LAN as a VLDB server, which allows you to maintain a copy of the database on another server to prevent data loss or corruption.
 - 7a On the second server, open ConsoleOne.
 - 7b Open the server's Property page.
 - 7c Click Add Replica.

Enabling DFS Junction Support for CIFS Clients

If you have clients that use CIFS networking protocol instead of a NetWare client, you must enable DFS Junction support for CIFS clients on all servers where you created DFS junctions. You must enable CIFS protocols for the destination servers, too. DFS Junction support for clients is available on NetWare 6.5 or later servers.

If new volumes are added within the DFS Management Context container after you enable DFS Junction support for CIFS clients, you might need to run VLDB Repair to update the VLDB database, depending on the utility that was used to create the new volume.

To enable DFS Junction support for CIFS clients on NetWare 6.5 servers:

- 1 On your NetWare 6.5 server, edit the sys:etc\cifsctxs.cfg file.

Add all CIFS/DFS users contexts to the file. CIFS uses a flat tree structure.

- 2 Enable DFS Junction support for CIFS for each server:

- 2a In iManager, click File Protocols.

For instructions, see [“Accessing Novell iManager” on page 34](#).

- 2b Select a server to manage.

For instructions, see [“Selecting a Server to Manage” on page 35](#).

- 2c Select the Enable DFS check box, then click Apply.

- 2d Repeat [Step 2b](#) and [Step 2c](#) for each of the NetWare 6.5 servers.

- 3 If you have not created a DFS Management Context, do it now.

For information, see [“Creating a DFS Management Context for NCP” on page 195](#).

- 4 In ConsoleOne, set the user Simple Password.

If Universal Password is enabled for the user container, it automatically synchronizes eDirectory and Simple Password.

IMPORTANT: Make sure the Windows logon user and password match the Simple Password's username and password. DFS only passes the default Windows logon username and password.

- 5 In ConsoleOne, create junctions, if desired.

For information, see [“Creating a DFS Junction Manually with ConsoleOne” on page 197](#).

Creating a DFS Junction Manually with ConsoleOne

You can create a DFS junction manually to impose a logical overlay for your storage structure. When you use Novell iManager to split volumes, the process creates DFS junctions automatically to replace the directory where you split the volume.

- 1 (Conditional) If it does not already exist, you must create a DFS Management context and make sure the VLDB service is up and running. For information, see “[Creating a DFS Management Context for NCP](#)” on page 195.
- 2 In ConsoleOne, create a subdirectory or use an existing subdirectory of any NetWare 6.x NSS volume.
- 3 Right-click the subdirectory, then click New > Shortcut > Junction.

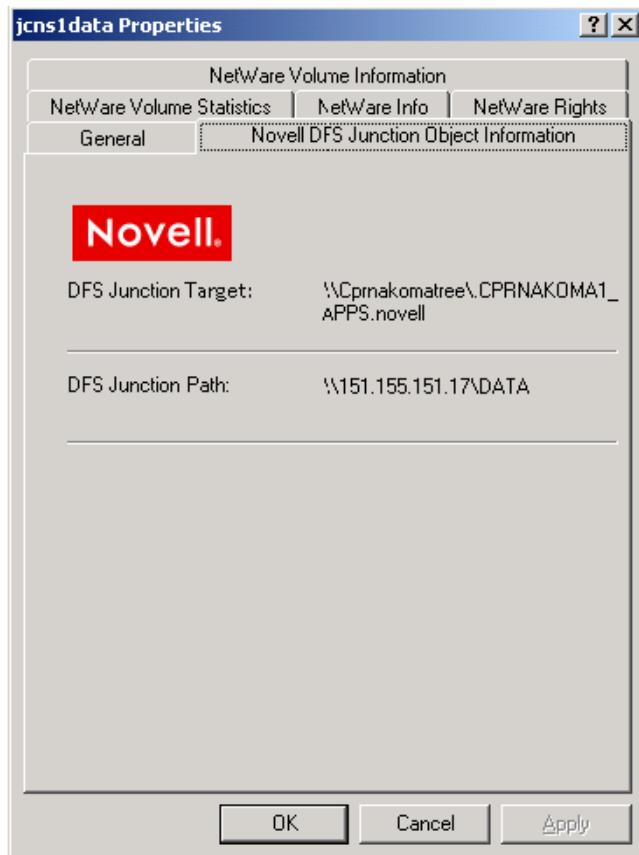
You can also create a junction at the root of a volume. However, to do this, instead of right-clicking the subdirectory, select the volume, then click the up-arrow in the ConsoleOne toolbar.

- 4 Verify that the eDirectory tree name is correct, browse to the volume that you are pointing to from the junction, then click Next.
- 5 Name the junction, then click Finish.
- 6 To view the newly created junction, from the Console One toolbar, click View > Refresh.

Viewing a DFS Junction

You can access DFS junctions with the latest Novell Client™ via the NCP protocol, Web-based services via Novell NetStorage, and the Microsoft* Client via the CIFS protocol. Right-click on the junction to view its property page.

If you are using an unsupported protocol to access a DFS junction, you see something that looks like a small file, but you are unable to read or open it.



Deleting a DFS Junction Manually with ConsoleOne

To delete a junction:

- 1 In ConsoleOne, locate and right-click the junction.
- 2 Select Delete Shortcut > Junction.

Managing the Volume Location Database Service

VLDB services run only on NetWare servers. You can manage the VLDB service from the server console or using the VLDB management service.

VLDB Commands

To view a listing of the available commands, enter at the server console:

```
vlldb help
```

To repair the VLDB, enter the following at the server console of the primary VLDB server:

```
vlldb repair
```

The VLDB Repair adds a GUID entry for all volumes in the eDirectory tree to the VLDB, such as the GUID for NSS volumes.

VLDB Management Service in ConsoleOne

To access the VLDB management service:

- 1 In ConsoleOne, right-click any server that has the VLDB service running.
- 2 Click Properties > Supported Services > NSS VLDB.

The management service shows you basic information, such as the version of the service, whether the service is running, and the database location.

The management service also allows you to perform the following tasks:

- ◆ Adjust processing threads
- ◆ Start and stop the VLDB service
- ◆ Add and remove replicas

To add or remove replicas, you must access the VLDB service from the server that you want to remove or add a replica to. In ConsoleOne, right-click the server, then click Properties > Supported Services > NSS VLDB. After you are in the management service, click either Add Replica or Remove Replica.

- ◆ Repair a database in one or more of the following ways:
 - ◆ **Low-Level Repair:** The repair option restores the last saved copy of your backup files to the database.
 - ◆ **Get Database from Another Replica:** You can use this feature only if you have the VLDB service running on more than one server. The VLDB service gets a copy of the database from another server that is currently running the service.
 - ◆ **Rebuild:** When you rebuild a database, the VLDB service walks the eDirectory tree, looks at volume and server objects, and then completely rebuilds the database from scratch.

Moving Volumes with iManager

When you move a volume, DFS moves the volume's file structure, data, and user rights information from the original location to a new volume in the network.

IMPORTANT: You cannot move the sys: volume.

- 1 Make sure you meet the [“Prerequisites and Guidelines for DFS” on page 193](#).
- 2 You must create at least one DFS Management Context at an O or OU class level in the Novell eDirectory tree. Both the original volume location and the new volume location must be in the same DFS Management Context. You must create at least one Volume Location Database (VLDB) server in this management context.

For information, see [“Creating a DFS Management Context for NCP” on page 195](#).

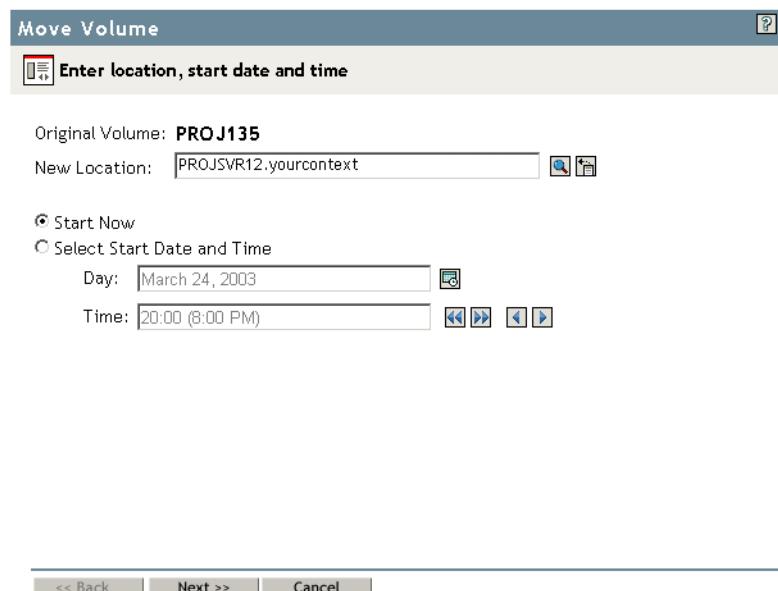
- 3 (Optional) If you plan to temporarily retain the deleted original volume in the salvage area after a successful volume move, verify that your server's Purge Delay setting meets your needs. The default Purge Delay setting is 4 days (345600 seconds), but the actual setting might differ. If desired, modify the Purge Delay setting.

At the server console, enter

```
nss /logicalVolumePurgeDelay=value
```

where *value* is the number of seconds until a deleted volume is purged from the salvage area. For information, see “[Configuring the NSS Volume Salvage Area](#)” on page 156.

- 4 Make sure users and applications are not accessing files on the volume throughout the move or split process.
- 5 In iManager, click Storage > Volumes.
For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.
- 6 Select a server to manage.
For instructions, see “[Selecting a Server to Manage](#)” on page 35.
- 7 From the Volumes list, select the volume that you want to move.
- 8 Click Properties > Attributes to view the current attribute settings for the volume.
Remember this information for [Step 13](#), where you specify the attributes for the destination volume.
- 9 From the Volumes list, select the volume, then click Move to open the Move Volume wizard.



- 10 Specify the following parameters, then click Next.
 - **New Location:** Specify the eDirectory common name of the server where you want to move the selected volume.
 - **Schedule:** Select Start Now to begin the move immediately, or specify the date and time you want to schedule the move.
Make sure that the volume is active at the time that the move is to begin.
 - **Purge Immediately:** Select Purge Immediately to purge the original volume’s deleted data from the server’s salvage area immediately following the successful completion of a volume move job.
If Purge Immediately is disabled (deselected), DFS delays the purge of the volume’s deleted data according to the server’s Purge Delay setting and the normal purge process.

You can manually purge or restore the original volume's deleted data at any time during the purge delay period, using the normal method of purging deleted volumes. For information, see ["Viewing, Salvaging, or Purging Deleted NSS Volumes" on page 157](#).

11 Specify a unique name for the new volume.

Typically, the new volume's name is different from the original volume's name. The new volume's name must meet the uniqueness requirements in the new location and conform to volume naming conventions. For guidelines about naming volumes, see ["Naming NSS Storage Objects" on page 52](#). It is possible, though not necessarily advisable, to use the same name under some conditions, such as when the original location and the new location are different servers.

IMPORTANT: If the name you provide is not unique, you receive an error message. You must click Cancel to back out of the wizard, then begin the move process again.

12 Specify the pool on the new location where you want the new volume to reside, specify the volume quota, then click Next.

Only pools that have free space appear in the list. You can select an existing pool from the list or create a new pool. If you create a new pool, the wizard guides you through steps similar to the process for creating a new pool. For instructions, see ["Creating Pools with iManager" on page 101](#).

If no pools are listed, there is no space available to create a volume in the new location. Cancel the wizard, add more devices to the server and expand the desired pool, or free up space by deleting existing pools, then return to the Volume Management page to begin the move process from the beginning.

13 Specify the attributes for the new volume you are creating, based on the volume attributes of the original volume that you viewed in [Step 8](#).

The wizard displays only the default settings for volume attributes. The attribute settings might not be the same as those set for the volume you are moving. Settings, such as Compression, that cannot be changed after they are set for a volume must be the same on the original volume and the new volume.

14 Click Finish.

The move can take a few minutes to several hours, depending on how much data needs to be moved.

15 To view the job's status or to pause and resume the job, click Volume Job Control.

For information, see ["Managing Move or Split Jobs" on page 203](#).

16 (Optional) After the job completes successfully, if you disabled the Purge Volume Immediately option, you can manually purge or restore the original volume's deleted data at any time during the purge delay period, using the normal method of purging deleted volumes.

For information, see ["Viewing, Salvaging, or Purging Deleted NSS Volumes" on page 157](#).

17 Manually update script files, configuration files, or mappings by modifying the location of the original volume to the location of the new volume.

Splitting Volumes with iManager

When you split a volume, NSS creates a DFS junction to serve as a placeholder for that volume and its contents. This might involve any directory level of the file system structure, from the volume's root directory to its most distant subdirectory. Everything below the specified directory,

including its subdirectories and the data therein, moves from the original location to a new volume in the network.

- 1 Make sure you meet the “[Prerequisites and Guidelines for DFS](#)” on page 193.
- 2 You must create at least one DFS Management Context at an O or OU class level in the Novell eDirectory tree. Both the original volume location and the new volume location must be in the same DFS Management Context. You must create at least one Volume Location Database (VLDB) server in this management context.

For information, see “[Creating a DFS Management Context for NCP](#)” on page 195.

- 3 Make sure users and applications are not accessing files on the volume throughout the move or split process.

- 4 In iManager, Storage > Volumes.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 5 Select a server to manage.

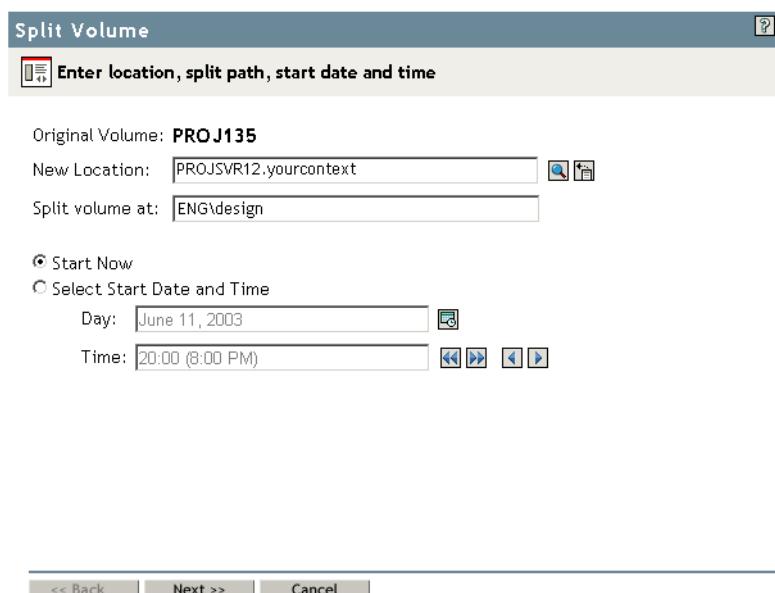
For instructions, see “[Selecting a Server to Manage](#)” on page 35.

- 6 From the Volumes list, select a volume that you want to split.

- 7 Click Properties > Attributes to view the current attribute settings for the volume.

Remember this information for [Step 12](#), where you specify the attributes for the destination volume.

- 8 Click Split to open the Split Volume wizard.



- 9 Specify the following parameters, then click Next.

- **New Location:** Specify the eDirectory common name of the server where you want to move the selected volume.
- **Split Volume At:** Specify the directory in the selected volume where you want the DFS junction to occur. All data below that point moves to the new volume created at the new location.

IMPORTANT: Do not include a leading slash in the path.

- ◆ **Schedule:** Select Start Now to begin the move immediately, or specify the date and time you want to schedule the move.

WARNING: Make sure that the volume is active but not in use by users or APIs at the time that the move is to begin.

10 Create and name the new volume.

Typically, the new volume's name is different from the original volume's name. The new volume's name must meet the uniqueness requirements in the new location and conform to volume naming conventions. For guidelines about naming volumes, see [“Naming NSS Storage Objects” on page 52](#). It is possible, though not necessarily advisable, to use the same name under some conditions, such as when the Original Location and the New Location are different servers.

IMPORTANT: If the name you provide is not unique, you receive an error message. You must click Cancel to back out of the wizard, then begin the split process again.

11 Specify the pool on the new location where you want the new volume to reside, specify the volume quota, then click Next.

Only pools that have free space appear in the list. You can select an existing pool from the list or create a new pool. If you create a new pool, the wizard guides you through steps similar to the process for creating a new pool. For instructions, see [“Creating Pools with iManager” on page 101](#).

If no pools are listed, there is no space available to create a volume in the New Location. Cancel the wizard, add more devices to the server and expand the desired pool, or free up space by deleting existing pools, then return to the Volume Management page to begin the move process from the beginning.

12 Specify the attributes for the new volume, based on the volume attributes of the original volume that you viewed in [Step 7](#).

The wizard displays only the default settings for volume attributes. The attribute settings might not be the same as those set for the volume you are moving. Settings, such as Compression, that cannot be changed after they are set for a volume must be the same on the original volume and the new volume.

13 Click Finish.

The split can take a few minutes to several hours, depending on how much data needs to be relocated.

14 To view the job’s status or to pause and resume the job, click Volume Job Control.

For information, see [“Managing Move or Split Jobs” on page 203](#).

Managing Move or Split Jobs

After you initiate a Move job or a Split job using the Volume Management page in iManager, use the Move/Split Job Control page to view its status. The report displays the status of all the active jobs and recently completed jobs that were initiated from the selected server. You can pause, resume, reschedule, finish, or delete a process, depending on the state it is in.

From the Move/Split Job Control Management page, you can perform the following tasks:

- ◆ [“Viewing the Status of Move or Split Jobs” on page 204](#)
- ◆ [“Pausing a Move or Split Job” on page 205](#)

- ◆ “Resuming a Move or Split Job” on page 205
- ◆ “Rescheduling a Move or Split Job” on page 206
- ◆ “Viewing Files Skipped by a Move or Split Job” on page 206
- ◆ “Deleting a Move or Split Job” on page 207
- ◆ “Finishing a Move or Split Job” on page 207

Viewing the Status of Move or Split Jobs

The Move/Split Job Control Status Report shows the following information:

- ◆ **Type:** Distinguishes the job as a Move or Split job.
- ◆ **Name:** If it is a Move, this is the name of the original volume. If it is a Split, it is the name of the original volume plus the path to the original directory location where you are splitting the volume.
- ◆ **Percent Complete:** The estimated percentage of data to be copied from the original volume that has been copied to the new volume as of the instant the status report was created.

To update the status, click Move/Split Job Control in Roles and Tasks.

- ◆ **State:** States are defined in logical tasks so that the Move or Split job can start and stop at several points in the process and go back to repeat any subprocesses, as needed.

Possible states include the following:

- ◆ Scheduled
- ◆ Running
- ◆ Files Skipped (administrator action required)
- ◆ Failed
- ◆ Deleted
- ◆ Completed
- ◆ **Comment:** A comment you typed when you issued a Pause command.

To access a report of move and split jobs:

- 1 In iManager, click Storage > Move/Split Job Control.

For instructions, see “[Accessing NSS Storage Management Role and Tasks](#)” on page 34.

- 2 Select a server to manage.

For instructions, see “[Selecting a Server to Manage](#)” on page 35.

A list of move and split jobs appears.

Move / Split Job Control Management

To move and split volumes, use the Move and Split functions on the Volume Management page. The Move/Split Job Control page reports the status of all the active move and split jobs initiated from this server. You can pause/resume, reschedule, finish, or delete a job, depending on the state it is in.

Server:

<input type="checkbox"/>	Type	Name	Percent Complete	State	Time	Comment
<input checked="" type="checkbox"/>	Move	MOVE_FROM:	0	Scheduled	7/30/03 8:00 PM	
<input type="checkbox"/>	Split	SPLIT_FROM:install\javabin	0	Paused	7/30/03 6:30 PM	pause it again

3 (Optional) Click the Sort arrow next to the column heading that you want to sort jobs by.

4 When you are done, click OK.

Pausing a Move or Split Job

Pause suspends one or more Move/Split jobs until you manually resume or delete them. Only four combined Move or Split jobs can be running on a given server at a time. The Volume Manager performs the jobs in the order they are scheduled. If four operations are in progress and you want to activate others that you decide are a higher priority, you can pause one or more of the active jobs, thus allowing the new job to run immediately.

You might want to pause a Move or Split job during times that users need access to the content in the original volume during times when Move/Split jobs are normally running.

- 1 In iManager, open the Move/Split Job Control Management page to view a job status report. For instructions, see [“Viewing the Status of Move or Split Jobs” on page 204](#).
- 2 Select the Job check box next to one or more active jobs that you want to pause.
- 3 Click Pause.
- 4 Type a Comment to be displayed in the status report, such as the reason you are pausing the job.
- 5 Click OK.

After the page refreshes, the jobs report their status as Pausing or Paused. If you inadvertently selected some jobs that are not eligible to be rescheduled, iManager ignores the Pause command for those jobs. It applies only to those jobs that the command is valid for.

Resuming a Move or Split Job

Resume continues one or more paused Move/Split jobs so that they can continue from wherever they were in the Move or Split process when you paused them.

- 1 In iManager, open the Move/Split Job Control Management page to view a job status report. For instructions, see [“Viewing the Status of Move or Split Jobs” on page 204](#).

- 2 Select the Job check box next to one or more paused jobs that you want to resume.
- 3 Click Resume.
- 4 Click OK.

After the page refreshes, the jobs report their status as Scheduled or Running, depending on when the job was originally scheduled to run. If you inadvertently selected some jobs that are not eligible to be rescheduled, iManager ignores the Resume command for those jobs. It applies only to those jobs that the command is valid for.

You cannot resume a completed, failed, or deleted job.

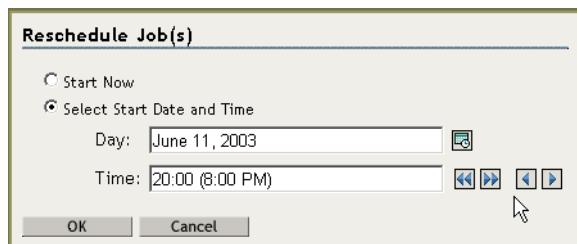
Rescheduling a Move or Split Job

Reschedule changes the date and time that the selected jobs should run. Applies the same date and time to all of the selected jobs.

IMPORTANT: You cannot reschedule a completed, failed, or deleted job.

- 1 In iManager, open the Move/Split Job Control Management page to view a job status report. For instructions, see [“Viewing the Status of Move or Split Jobs” on page 204](#).
- 2 Select the Job check box next to one or more uncompleted jobs that you want to reschedule.
- 3 Click Reschedule.

This opens a Reschedule Jobs dialog box.



- 4 To set the new schedule:
 - ♦ To start the job immediately, Select Start Now.
 - ♦ To start the job at a future date or time, specify the start date and time when you next want the move or split job to begin.
- 5 Click OK.

After the page refreshes, the jobs report their status with the new schedule. If you inadvertently selected some jobs that are not eligible to be rescheduled, iManager ignores the Reschedule option for those jobs. It applies only to those jobs that the command is valid for.

Viewing Files Skipped by a Move or Split Job

If a Move or Split Volume job reports a Files Skipped status, some files could not be moved because they were open at the time that DFS attempted to copy them.

- 1 To retrieve the Operation ID number of the Move or Split Volume job, enter the following command at the server command prompt:

```
volmn status
```

NSS displays a list of the Move and Split jobs that are in progress or were initiated or run in the past seven days.

- 2 Find the Move or Split job of interest and make a note of its Operation ID (OpID) number.

For example, Move(Vol1) might have an Operation ID number of 104211375.

- 3 To display a list of the files skipped, enter the following at the server command prompt:

```
volmn list OpID
```

For example, enter

```
volmn list 104211375
```

Deleting a Move or Split Job

Delete cancels a selected job before it begins or up to a certain point in the Move or Split process. If the process is beyond a certain state, it returns an error message to prevent you from deleting the process.

If the deletion continues, it stops the job at the next convenient step in the process, but performs no cleanup. The target volume exists and contains all files copied to it before the you deleted the job. Deleted jobs appear in the status report for a week by default.

IMPORTANT: If deletion continues, the original data is still intact. There is no loss of service or need to copy data from the destination volume back to the original volume.

- 1 In iManager, open the Move/Split Job Control Management page to view a job status report. For instructions, see [“Viewing the Status of Move or Split Jobs” on page 204](#).
- 2 Select the Job check box next to one or more scheduled or paused jobs that you want to cancel.
- 3 Click Delete.

After the page refreshes, the selected jobs report their status as Deleted. Some jobs might not allow themselves to be deleted, depending on how far into the move or split process they are when you click delete.

If you inadvertently selected some jobs that are not eligible to be deleted, iManager ignores the Delete command for those jobs. It applies only to those jobs that the command is valid for. You cannot delete a completed, failed, or previously deleted job.

Finishing a Move or Split Job

Finish continues a Move or Split job that has reached a state that requires manual intervention so that it can finish even though some files might remain behind.

- 1 In iManager, open the Move/Split Job Control Management page to view a job status report. For instructions, see [“Viewing the Status of Move or Split Jobs” on page 204](#).
- 2 Select the Job check box next to one or more jobs waiting for administrator intervention that you want to complete, acknowledging and understanding the exceptions noted.
- 3 Click Finish.

After the page refreshes, the selected jobs report their status as Scheduled, Running, or Complete, depending on how much work was left to do in the job.

If you inadvertently selected some jobs that are not eligible to be finished, iManager ignores the Finish command for those jobs. It applies only to those jobs for which the command is valid.

15

Monitoring the NSS File System Status

This section discusses the following methods for monitoring the status of the Novell® Storage Services™ file system:

- ◆ “Monitoring Status of NSS Devices, Pools, and Volumes with iManager” on page 209
- ◆ “Monitoring Compression and Salvage Statistics” on page 209
- ◆ “Monitoring Quotas and Space Usage for NSS Pools and Volumes” on page 212
- ◆ “Monitoring File System Parameters” on page 214
- ◆ “Monitoring Server Status with the Monitor Utility” on page 214
- ◆ “Monitoring Server Status with Novell Remote Manager” on page 215

Monitoring Status of NSS Devices, Pools, and Volumes with iManager

Use the following table to determine where to go to view the status of your NSS storage devices, pools, and volumes.

To monitor the status of:	Refer to:
Devices	Viewing Details for a Device
Partitioned free space	Viewing Partitions on a Device
NSS pools	Viewing Pool Details
NSS volume details	Viewing the Details of a Volume
NSS volume quota and space usage	Viewing Properties of a Volume
NSS volume attributes	Viewing Properties of a Volume

Monitoring Compression and Salvage Statistics

For each volume, the Volume Properties Statistics page in iManager reports statistics about the compressed and salvageable files in the volume, the GUID of the volume, and the block size being used.

Figure 6 Sample Statistics Page from the Volume Properties

Storage Management ▶ Volumes ▶ Volume Properties

Volume Properties ?

Properties: NIFVOL

Attributes **Statistics** **Quotas Usage**

Compression		Salvage	
Compressed Space:	0.00 Bytes	Minimum Keep Seconds:	
		Maximum Keep Seconds:	0
Files:		Low Water Mark:	10
Not Deleted:	0	High Water Mark:	20
Deleted:	0		
Uncompressed:	0	Next Scheduled Purge	
		Purgeable Space:	0.00 MB
		Unpurgeable Space:	0.00 MB
		Deleted Files:	0
		Oldest Deleted Time:	0

GUID: **A7942770-9C3E-01D7-80-00-1A1A3BF816F4**

Block Size: **4.00 KB**

Close

If the compression attribute is set, the Compression report shows statistics of all the compressed files for the selected volume.

Statistic	Description
Compressed Space	The amount of space in the volume in use by compressed files
Files	The total number of files in the volume and information by the following categories: <ul style="list-style-type: none">◆ Not Deleted: The total number of files in the volume that are currently available to users◆ Deleted: The total number of files in the volume that are deleted but not yet purged from the system◆ Uncompressed: The total number of files in the volume that are not stored in compressed form

If the Salvage Files attribute is enabled, the Salvage report shows statistics about deleted files that have not yet been purged.

Statistic	Description
Minimum Keep Seconds	Minimum time (in seconds) to keep deleted files
Maximum Keep Seconds	Maximum time (in seconds) to keep deleted files
Low Water Mark	If the amount of free space drops below this percentage, the file system begins purging deleted files.
High Water Mark	If there are files to delete, the autopurging process stops when the amount of free space reaches this percentage.
Next Scheduled Purge	Date and time of the next purge
Purgeable Space	Amount of space in the volume that is occupied by deleted files that are queued for purging
Unpurgeable Space	Amount of space in the volume that is occupied by files
Deleted Files	The number of deleted files in salvage.
Oldest Deleted Time	Timeline for deleted files. The file system purges the files in the same order they were deleted.
GUID	The Global Unique Identifier (GUID) number that NSS assigns to the volume. This number is necessary so your file system can locate the specific volume.
Block Size	The maximum amount of data committed to a single write process. Possible sizes include 4, 8, 16, 32, or 64 KB.

Other information reported includes the volume's GUID and block size.

Statistic	Description
GUID	The Global Unique Identifier (GUID) number that NSS assigns to the volume. This number is necessary so your file system can locate the specific volume.
Block Size	The maximum amount of data committed to a single write process. Possible sizes include 4, 8, 16, 32, or 64 KB.

1 In iManager, click Storage > Volumes.

For instructions, see [“Accessing NSS Storage Management Role and Tasks” on page 34](#).

2 Select a server to manage.

For instructions, see [“Selecting a Server to Manage” on page 35](#).

3 In the Volumes list, select a volume that you want manage.

4 Click Properties.

The Properties page has three tabs: Attributes, Statistics, and Quotas Usage. It opens by default to the Attributes tab.

5 Click the Statistics tab to view the compression and salvage statistics for the selected volume.

Monitoring Quotas and Space Usage for NSS Pools and Volumes

For each volume, the Volume Properties Quotas Usage page in iManager reports the space usage for the selected volume and the pool that contains the volume.

Figure 7 Sample Quota Usage Page from the Volume Properties



Volume Usage reports the amount of space on the volume, categorized by usage: Compressed, Other In-use, Purgeable, and Available.

Statistic	Description
Quota	Indicates whether the volume has a quota. If there is a quota, the volume can grow only to the size of the quota. If there is no quota, the volume can grow to the amount of available physical space in the pool.

Statistic	Description
Used Space	<p>The amount of space currently in use and information by the following categories:</p> <ul style="list-style-type: none"> ♦ Compressed: If the Compressed attribute is enabled, reports the amount of space in the volume containing data that is compressed. ♦ Other In-Use Space: The amount of space in the volume containing data that is not compressed. ♦ Purgeable Space: The amount of space in the Salvage system that you can use as free space. You can manually purge deleted files to free space. ♦ Available: Available free space that is not in the Salvage system.

Pool Usage reports the amount of space on the pool, categorized by usage: Free, Purgeable, Used, and Booked.

Statistic	Description
Available Space	<p>The amount of space in the pool that is not currently in use and information by the following categories:</p> <ul style="list-style-type: none"> ♦ Free: The total amount of free space that is available on the pool. ♦ Purgeable: The amount of space in the Salvage system that you can use as free space. You can manually purge deleted files to free space.
Total Space	<p>The total amount of space allocated to the pool and information by the following categories:</p> <ul style="list-style-type: none"> ♦ Used: The total amount of space currently in use by all volumes on the pool. ♦ Overbooked/Booked: If the amount of space assigned to the pool's volumes exceeds the amount of physical space available in the pool, the Overbooked field shows the amount of exceeded space. Otherwise, the Booked field shows the total amount of space in all volumes in the pool. If any of the volumes do not have a quota, these volumes are not calculated in the total combined quota.

1 In iManager, click Storage > Volumes.

For instructions, see [“Accessing NSS Storage Management Role and Tasks” on page 34](#).

2 Select a server to manage.

For instructions, see [“Selecting a Server to Manage” on page 35](#).

3 In the Volumes list, select a volume that you want manage.

4 Click Properties.

The Properties page has three tabs: Attributes, Statistics, and Quotas Usage. It opens by default to the Attributes tab.

5 Click the Quotas Usage tab to view the current space usage statistics for the selected volume.

Monitoring File System Parameters

- ♦ “Monitoring NSS File System Parameters with Novell Remote Manager” on page 214
- ♦ “Monitoring NSS File System Parameters with Novell NetStorage” on page 214

Monitoring NSS File System Parameters with Novell Remote Manager

Use Novell Remote Manager for NetWare to monitor the status of the NSS file system parameters listed in the following table. For information about using Novell Remote Manager, see the *NetWare 6.5 Novell Remote Manager Administration Guide for NetWare*.

Use this link	To do these tasks
Volumes	<ul style="list-style-type: none">♦ Monitor disk space usage by directory♦ Purge or salvage deleted volumes or files♦ Configure file system trustee rights and attributes for directories and files♦ View or change a list of Set parameters

Monitoring NSS File System Parameters with Novell NetStorage

Use the Novell NetStorage to monitor the status of the NSS file system parameters listed in the following table.

Use this link	To do these tasks
Volumes	<ul style="list-style-type: none">♦ Monitor disk space usage by directory♦ Purge or salvage deleted volumes or files♦ Configure file system trustee rights and attributes for directories and files

Monitoring Server Status with the Monitor Utility

Use the Monitor utility to view operational status of server memory and disks.

At the server console, enter

monitor

The Monitor utility opens to the General Information window. You can view operational status such as the number of Current Disk Requests and the number of Open Files.

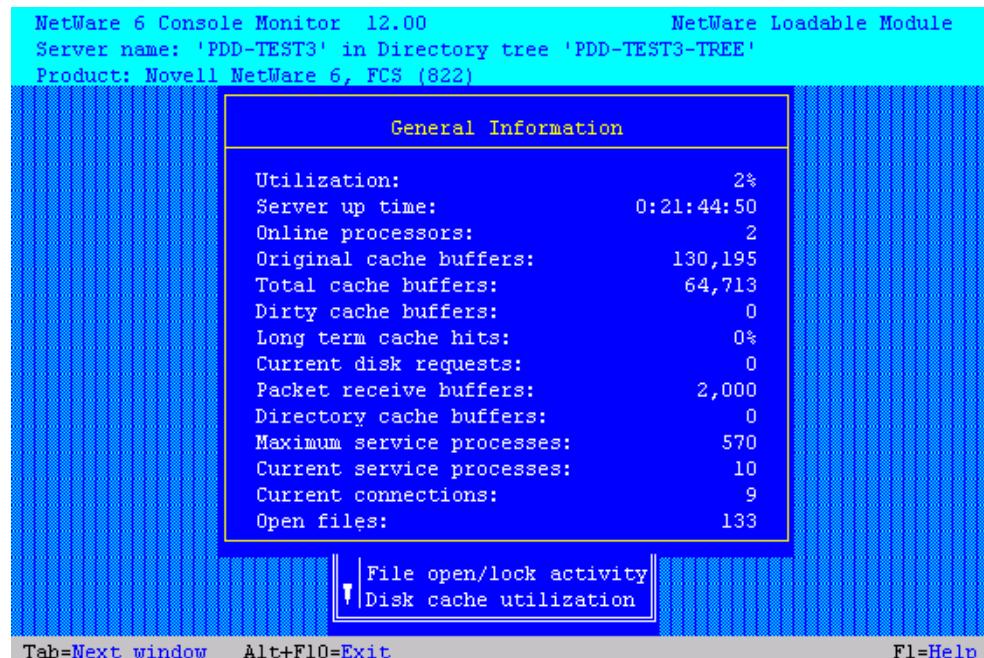
Other options available from the Monitor utility include the following:

- ♦ Connections
- ♦ Storage devices
- ♦ Volumes
- ♦ LAN/WAN drivers
- ♦ Load modules

- ◆ File open/lock activity
- ◆ Disk cache utilization

For more information about available options, see “Monitor” in the *NetWare 6.5 Utilities Reference*.

Figure 8 Monitor Status of Server Memory and Disk



Monitoring Server Status with Novell Remote Manager

Use Novell Remote Manager to monitor the status of the NSS file system parameters listed in the following table. For information about using Novell Remote Manager, see the *NetWare 6.5 Novell Remote Manager Administration Guide for NetWare*.

Use this link	To do these tasks
Volumes	<ul style="list-style-type: none"> ◆ Monitor disk space usage by user ◆ Monitor disk space usage by directory ◆ Purge deleted files ◆ View or change file and directory Trustee rights and Inherited Rights filters ◆ View or manage files in use by connections ◆ View or change a list of Set parameters
Partition Disks	<ul style="list-style-type: none"> ◆ Manage disk partitions ◆ Mirror partitions
Console Screens	Access, view, and run the server console screens
View Statistics	Access and view statistics for Media Manager and other systems

16 Using NSS Server Console Commands

This section discusses the Novell® Storage Services™ console commands.

NOTE: You can abbreviate NSS command options by providing just enough of the command to be unique. For example, `nss /ca` would be unique enough to be an abbreviation for the `nss /CacheStats` command.

- ◆ “[Online Help Commands](#)” on page 217
- ◆ “[Status Commands](#)” on page 218
- ◆ “[NSS Startup Commands](#)” on page 219
- ◆ “[Maintenance Commands](#)” on page 220
- ◆ “[System Volume Recovery Commands](#)” on page 221
- ◆ “[Volume Compression Commands](#)” on page 222
- ◆ “[Volume Purge Delay Commands](#)” on page 222
- ◆ “[Performance Tuning Commands](#)” on page 223
- ◆ “[Cache Balancing Commands](#)” on page 223
- ◆ “[Other NSS Commands](#)” on page 224
- ◆ “[Commands for Mounting CDs and DVDs as NSS Volumes](#)” on page 226
- ◆ “[Commands for CD and DVD Image Files as NSS Volumes](#)” on page 227
- ◆ “[DOS FAT Commands](#)” on page 227
- ◆ “[Multiple Server Activation Prevention Commands](#)” on page 227
- ◆ “[Multipath Connection Failover Commands](#)” on page 228
- ◆ “[Pool Snapshot Commands](#)” on page 229
- ◆ “[NSS File System Rights Utility](#)” on page 230

This section does not include a complete list of NSS commands. To see a complete list, enter `nss /help` at the server console.

Online Help Commands

To access online Help for NSS console commands: At the server console, enter one of the following commands:

```
nss /help
```

```
nss /?
```

The interface returns a list of NSS commands, each with a brief definition and any constraints such as the default value, a range of valid values, and persistence information.

Default Value

The default value is the setting used for a given server configuration parameter unless you modify it for your particular implementation. Default values are the best choice for a majority of server configurations, but you should review the settings as you fine-tune the server.

Range of Valid Values

The range of valid values establishes the constraints for any particular variable setting.

Persistence

If a command's setting is persistent, the values you set remain in effect for the server through any subsequent server reboots until you next modify the settings. If a command is not persistent, the setting remains in effect only until the next server reboot.

Status Commands

NSS provides the following commands to show the status of various NSS parameters. To view a complete list, use the nss /help command.

Commands	Description
Status	Lists the current NSS status information.
Pools	Lists all of the NSS pools that are currently available on the server.
PoolAutoDisplay	Displays load-time policies for pools on the server.
Volumes	Lists all of the NSS volumes that are currently mounted and active, including the Admin volume.
SpaceInformation	Lists the amount of space on active pools and their associated volumes.
ListFreeSpace	Lists the amount of available space that has not been assigned to a pool.
nss /StorageAlertMessages	Enables NSS to send Low Storage messages to all users. [Default=On]
nss /NoStorageAlertMessages	Disables NSS from sending Low Storage messages to all users.
CompScreen	Display the NSS Compression Statistics GUI. For more information, see "Volume Compression Commands" on page 222 .
CacheStats	Shows the caching statistics for buffers.
FileCacheStats	Shows the caching statistics for file system objects.
NameCacheStats	Shows the caching statistics for names.
ResetStats	Resets caching and file statistics.
nss /ErrorCode=code	Translates and describes the specified error code.
nss /GetMFLStatus=volume	Shows the modified file list status for the specified volume.
Modules	Lists the providers, loadable storage subsystems, and semantic agents.
Version	Displays the version information for NSS.

NSS Startup Commands

NSS provides the following startup commands. Startup commands are only valid when NSS is loading.

Issuing NSS Startup Commands while NetWare Boots

NSS Startup commands can run as part of the NetWare c:\nwserver\server.exe command by using the -z option. However, these commands are not persistent through a server reboot; you must enter them each time you boot your server.

At the server command line, enter

server -z"/parameter=value"

In the above example, the -z tells the server to look for specific NSS startup commands. The information in quotes is the actual command with command values, if any. For example:

server -z"CDDVD"

Making NSS Startup Commands Persist through a Server Reboot

NSS Startup commands issued at the command line during a server boot do not persist through a server reboot. To make non-persistent command settings persist automatically through a server reboot, place the commands in the nssstart.cfg file, which NSS reads on startup.

- 1 In a text editor, create a file called nssstart.cfg in the c:\nwserver directory.
- 2 Enter any NSS startup commands that you want to persist through server reboots.

Each NSS command should be preceded by a forward slash (/) and followed with a space. For example:

/numworktodos=40 /cddvd /dosfat

- 3 Save and close your c:\nwserver\nssstart.cfg file.

Startup Commands

Commands	Description
CDDVD	If it is specified in the nssstart.cfg file, loads the cddvd.nss module that is essential for CD, DVD, and Macintosh support. For more information, see "Activating and Deactivating CDs and DVDs as NSS Volumes" on page 137 .
defaultNLMs	If it is specified in the nssstart.cfg file, loads only default NSS NLM™ programs and any additional LSS modules specified on the command line.
DOSFAT	If it is specified in the nssstart.cfg file, loads only those modules that are essential for accessing FAT 16 and FAT 12 drives. NetWare does not support FAT 32 drives.
/allLSS	If it is specified in the nssstart.cfg file, it loads all LSS modules.
/noLSS	If it is specified in the nssstart.cfg file, it does not load the LSS modules.

Commands	Description
/NumAsyncIOs= <i>value</i>	Sets the number of asynchronous I/O entries to allocate. [Default=2048; Range=4 to 65536]
/NumBonds= <i>value</i>	Sets the number of bond entries to allocate. [Default=5000; Range=512 to 2097152]
/NumWorkToDoS= <i>value</i>	If used in the nssstart.cfg file, sets the number of WorkToDo entries. Entries can execute concurrently. NSS uses WorkToDo entries for tasks such as flushing file metadata to disk in the background. Increasing the number of WorkToDo entries might be useful on a system that is heavily used. NSS always reserves 20 WorkToDo entries. [Default=50; Range=5 to 100]
/zLSS	If it is specified in the nssstart.cfg file, loads only those modules that are essential for zLSS support.

Maintenance Commands

NSS provides the following maintenance for pools and volumes. To view a complete list, use the `nss /help` command.

Commands	Description
<code>nss /BackgroundChecking</code>	Enables the background file system checker. [Default=On]
<code>nss /NoBackgroundChecking</code>	Disables the background file system checker.
<code>ForceBackgroundCheck</code>	Force background file system checking to start.
<code>nss /FixDirectoryQuotas=<i>volume</i></code>	Recomputes used space for directory quotas for the specified volume.
<code>nss /FixMFL</code>	Repairs the modified file list to be consistent with the file system.
<code>nss /MFL=<i>volume</i></code>	Enables modified file list maintenance for the specified volume.
<code>nss /NoMFL=<i>volume</i></code>	Disables modified file list maintenance for the specified volume.
<code>nss /MFLVerify=<i>volume</i></code>	Compares the modified file list with the specified volume and reports any inconsistencies.
<code>nss /IncludeType=<i>type</i></code>	Include pools of the specified type for the given command. Possible types are SHARED, CORRUPT, and QUESTIONS.
<code>nss /OverrideType=<i>type</i></code>	Override pools of the specified type for the given command. Possible types are SHARED, CORRUPT, and QUESTIONS.
<code>Pools</code>	Shows all of the currently available NSS pools.
<code>nss /PoolAutoDisplay</code>	Displays current pool load time policies.
<code>nss /PoolAutoActivate=<i>pool</i></code>	Activates specified pools at load time.

Commands	Description
<code>nss /PoolAutoDeactivate=pool</code>	Leaves specified pools deactivated at pool load time.
<code>nss /PoolAutoMaintenance=pool</code>	Places specified pools in maintenance mode at pool load time.
<code>nss /PoolAutoVerify</code>	Verifies the specified pool's physical integrity at startup time.
<code>nss /PoolRebuild=pool</code>	Rebuilds the specified pools.
<code>PoolRebuild</code>	Select the pools to rebuild from a menu, then it rebuilds them.
<code>nss /PoolVerify=pool</code>	Verifies the physical integrity of the specified pool.
<code>PoolVerify</code>	Allows you to select pools from a menu and verifies their physical integrity.
<code>nss /VolumeActivate=volume</code>	Activates the specified NSS volume.
<code>nss /VolumeDeactivate=volume</code>	Deactivates the specified NSS volume.
<code>nss /VolumeAutoActivate=volume</code>	Activates the specified volume at load time.
<code>nss /VolumeAutoDeactivate=volume</code>	Deactivates the specified volume at load time.
<code>nss /ForceActivate=volume</code>	Forces an NSS volume to become active.
<code>VolumeAutoDisplay</code>	Displays the current volume's load time policies.
<code>nss /VolumeMaintenance=volume</code>	Places a specified volume into maintenance mode. Volumes can be put in maintenance mode, but maintenance occurs only at the storage pool level.
<code>nss /UpgradeObjectsOnVolume</code>	Upgrades objects on volumes to the current version.

System Volume Recovery Commands

NSS provides the following commands for recovering the system volume. To view a complete list, use the `nss /help` command.

Commands	Description
<code>nss /ChangeSysQuota</code>	Lets you change the quota (in MB) for the sys: volume. Setting this value to zero sets the Quota to none and allows the sys: volume to grow to the size of the pool.
<code>nss /ExpandSys</code>	Lets you expand the pool that contains your sys: volume. When prompted, enter the partition ID of the free space you plan to use to expand the pool. You can obtain the partition ID of all free partitions by using the <code>/ListFreeSpace</code> command.
<code>nss /ListFreeSpace</code>	Lists all free partitions and NSS partitions that have not been assigned to a pool. Use this command to obtain the partition ID required when using the <code>/ExpandSYS</code> command.
<code>nss /RenameToSys</code>	Lets you rename the sys: volume back to sys: if you have previously renamed it. At the prompt, enter the name of the volume you want to rename to sys:.
<code>nss /SalvageSys</code>	Lets you restore the sys: volume if you have deleted it (only if it has not yet been purged).

Volume Compression Commands

NSS offers the following commands for configuring and monitoring compression. To view a complete list, use the `nss /help` command.

Command	Use to
<code>CompScreen</code>	Display the NSS volume compression statistics on the compression screen.
<code>nss /Compression=volume_name</code>	Enables the Compression attribute for the specified volume. After you enable the Compression attribute, the setting persists for the life of the volume. You cannot disable compression, but you can set parameters to effectively turn it off.
<code>nss /Compression=all</code>	Enable the Compression attribute for all volumes on the server.
<code>nss /StopNormalCompression</code>	Stop all queued compression for files, based on the compression triggered by a file open or close.
<code>nss /BGCompression</code>	Allow compression to occur in the background at any time, instead of only within specified hours.
<code>nss /NoBGCompression</code>	Stop background compression and clears any queued background compression requests. Allow compression to occur only within the specified hours.

Volume Purge Delay Commands

NSS offers the following commands for tuning the purging processes for a volume. To view a complete list, use the `nss /help` command.

Commands	Description
<code>nss /LogicalVolumePurgeDelay=value</code>	The number of seconds before deleted logical volumes are purged. This allows time to reverse the deletion. [Default=345600]
<code>nss /LogicalVolumePurgeDelayAfterLoad</code>	The number of seconds after NSS loads before deleted logical volumes are purged. This allows time to reverse the deletion. [Default=7200]
<code>nss /LogicalVolumePurgeDelayAfterContinue=value</code>	The number of seconds to delay purging a logical volume after clicking Continue. After a volume starts to purge, it cannot be salvaged. [Default=900]
<code>nss /PoolHighWaterMark=<poolname>:Percent</code>	Purging begins in the salvage area when the volume's low watermark is reached and continues until its high watermark is reached. When enough files are purged such that the free disk space increases to a percentage equal to or greater than the high watermark, the autopurge stops. Autopurging does not start again until free space again drops below the low watermark. The high and low watermarks must be at least 2% apart from each other. [Default=20; Range=2 to 100]

Commands	Description
<code>nss /PoolLowWaterMark=<poolname>:Percent</code>	<p>Purging begins in the salvage area when the volume's low watermark is reached and continues until its high watermark is reached. When free disk space falls below a low watermark, NSS begins autopurging the salvage area.</p> <p>The high and low watermarks must be at least 2% apart from each other.</p> <p>[Default=10; Range=0 to 98]</p>

Performance Tuning Commands

NSS offers the following commands for tuning your storage solution. To view a complete list, use the `nss /help` command.

Commands	Description
<code>nss /AllocAheadBlks=value</code>	<p>Sets the number of blocks to allocate ahead on writes.</p> <p>[Default=15; Range=0 to 63]</p>
<code>nss /ReadAheadBlks=VolName:Count</code>	<p>Specify VolName as the name of the volume that you are setting the attribute for. Specify the Count to be the number of 4 KB blocks that you want to NSS to read ahead. The default block count is 2 blocks, which satisfies the performance requirements for a typical volume. The valid range for a block count is 0 blocks to 1024 blocks, where a block count of zero (0) implies no read ahead. However, 128 blocks is the practical maximum.</p> <p>Read-ahead block counts higher than 128 can starve other system components for memory or buffers, which can impair performance or cause the system to hang. As the number of concurrent connections to unique files increase, you should reduce the number of read-ahead blocks.</p> <p>[Default=2; Maximum=1024; Practical maximum=128]</p>
<code>nss /LogicalVolumePurgeDelay=value</code>	<p>The number of seconds before deleted logical volumes are purged. This allows time to reverse the deletion.</p> <p>[Default=345600]</p>
<code>nss /LogicalVolumePurgeDelayAfterLoad</code>	<p>The number of seconds after NSS loads before deleted logical volumes are purged. This allows time to reverse the deletion.</p> <p>[Default=7200]</p>
<code>nss /LogicalVolumePurgeDelayAfterContinue=value</code>	<p>The number of seconds to delay purging a logical volume after clicking Continue. After a volume starts to purge, it cannot be salvaged.</p> <p>[Default=900]</p>

Cache Balancing Commands

NSS provides commands to balance the cache for NSS on NetWare.

WARNING: If you give NSS more memory than you allow for the server, NSS fails to load. Your NSS-based sys: volume becomes inoperable until you load the c:\nwserver\server.exe with an NSS override to correct the situation. For information, see ["NSS Startup Commands" on page 219](#).

Commands	Description
nss /CacheBalance= <i>value</i>	Enables the dynamic balancing of free memory for the NSS buffer cache. Sets the specified percentage of free kernel memory that NSS uses for its buffer cache. [Default=85; Range=1 to 99]
nss /NoCacheBalance	Disables the dynamic balancing of free memory for the NSS buffer cache.
nss /MinBufferCacheSize= <i>value</i>	Sets the specified minimum number of NSS buffer cache entries. [Default=512; Range=384 to 1048576]
nss /MinOSBufferCacheSize= <i>value</i>	Sets the specified minimum number of NetWare buffer cache entries. [Default=256; Range=256 to 1048576]
nss /NameCacheSize= <i>value</i>	Sets the specified maximum number of Name cache entries. [Default=100000; Range=17 to 1000000]
nss /CacheUserMaxPercent= <i>value</i>	Sets the specified maximum percentage of buffer cache that can be used for user data. [Default=80; Range=10 to 100]
nss /ClosedFileCacheSize= <i>value</i>	Sets the number of closed files that can have their beast objects cached in memory. On average, each Closed File Cache entry consumes 0.4 - 1KB of RAM. [Default=50000; Range=16 to 1000000; Recommended=100000]
CacheStats	Shows the caching statistics for buffers.
FileCacheStats	Shows the caching statistics for file system objects.
NameCacheStats	Shows the caching statistics for names.
ResetStats	Resets caching and file statistics.
nss /FlushFilesImmediately= <i>volume</i>	Synchronously flush data to the specified volume when its files are closed instead of waiting for the next scheduled write of data to the volume.
nss /NoFlushFilesImmediately= <i>volume</i>	Disables synchronously flushing files to the specified volume when its files are closed. Instead, data is written to the volume on the next scheduled write of data to the volume.
nss /FileFlushTimer= <i>value</i>	Sets the flush time in seconds for writing data to modified open files. Increasing this number might reduce the number of writes to disk; however, it increases the amount of data that is lost if the system crashes.
	[Default=10 seconds; Range=1 to 3600 seconds]
nss /IDCacheResetInterval	Set the number of seconds between invalidation of the ID cache. [Default=90000 Range=0-200000000]

Other NSS Commands

NSS provides these additional commands for managing pools and volumes. To view a complete list, use the `nss /help` command.

Commands	Description
nss /NoClassicDirectoryQuotas	Turns emulation of Traditional NetWare volumes on or off. [Default=Off]
nss /DataShredding	Enables data shredding for the volume. This is the number of times you want to shred data. [Default=1; Range=0 to 7, where 0 indicates no shredding]
nss /NoDataShredding	Disables data shredding on the volume.
nss /DirectoryQuotas	Enables directory quotas on the volume.
nss /NoDirectoryQuotas	Disables directory quotas on the volume.
nss /FileCopyOnWrite	Creates a copy of files in the volume when they are open for write.
nss /NoFileCopyOnWrite	Does not create a copy of files on the volume when they are open for write.
nss /FlushFilesImmediately	Synchronously flush files in the volume when they are closed.
nss /NoFlushFilesImmediately	Disables synchronously flushing files in the volume.
nss /LVDeleteStatusBasic	Displays information about deleted logical volumes.
nss /LVDeleteStatusSalvagable	Displays information about salvagable logical volumes.
nss /Migration= <i>volume_name/all</i>	Enables migration of files on the volumes.
nss /NoMigration= <i>volume_name/all</i>	Disables migration of files on the volumes.
nss /Salvage= <i>volume_name/all</i>	Enables salvage of deleted files on volumes. <i>Volume_name</i> enables the Salvage command on the specified NSS volume on the specified server. All enables the Salvage command on all NSS volumes on the specified server.
nss /NoSalvage= <i>volume_name/all</i>	Disables salvage of deleted files on volumes. <i>Volume_name</i> disables the Salvage command on the specified NSS volume on the specified server. All disables the Salvage command on all NSS volumes on the specified server.
nss /StorageAlarmThreshold= <i>value</i>	Lets you set the threshold for a low storage space warning. [Default=10; Range=0 to 1000000]
nss /(No)StorageAlertMessages	Turns On or Off the low storage message to users. [Default=On]
nss /StorageResetThreshold= <i>value</i>	Lets you reset the threshold for a low storage space warning. [Default=10; Range=1 to 1000000]
nss /NoTransaction= <i>volume_name/all</i>	Disables transactional writes in files on the volumes.
nss /UserSpaceRestrictions	Enables user space restrictions on the volume.
nss /NoUserSpaceRestrictions	Disables user space restrictions on the volume.
nss /Transaction= <i>volume name/all</i>	Enables transactional writes in files on the volumes.
nss /ZLSSIOStatus	Displays current NSS IO status information.

Commands	Description
nss /ZLSSPendingWriteIOs	Number of write inputs dropped to the storage subsystem. (0 = all available) [Default=1000; Range=0 to 3000]
nss /ZLSSPoolScan	Scans for and loads all ZLSS pools.
nss /ZLSSVolumeUpgrade	Allows the 5.x/ZLSS VolumeUpgrade to the NetWare 6 format to occur during the installation process.

Commands for Mounting CDs and DVDs as NSS Volumes

Cddvd.nss is loaded automatically on startup by default. Use the following commands to manage CDs, DVDs, and Macintosh CDs as NSS volumes.

NOTE: The cddvd.nss module replaces cdrom.nlm and cd9660.nss for CD support, udf.nss for DVD support, and cdhfs.nss for Macintosh* CD support. The following commands for cddvd.nss are the same ones used for previous CD and DVD management modules.

Commands	Description
CDDVD	If CDDVD is specified in the nssstart.cfg file, loads only those modules essential for CD and DVD support.
nss /(No)LeaveCDinNDS	If the switches UpdateCDToNDS or LoginUpdateCDToNDS is enabled, enable this switch to retain the CD or DVD volume objects when the actual disks are removed. [Default=Off]
nss /(No)LoadISOVolumeFirst	If this switch is enabled, try to load UDF-bridge CD as and ISO9660 volume first. By default, a UDF-bridge CD is loaded as DVD format first and CD format second. [Default=Off]
nss /(No)LockCDMediaIn	If this switch is enabled, whenever CDs or DVDs are activated or deactivated as NSS volumes, lock/unlock the media in the device. [Default=Off]
nss /(No)UpdateCDToNDS	If this switch is enabled, whenever CDs or DVDs are activated or deactivated as NSS volumes, update their Novell eDirectory objects. [Default=Off]
nss /(No)LoginUpdateCDToNDS	If this switch is enabled, whenever CDs or DVDs are activated or deactivated as NSS volumes, update their Novell eDirectory objects. You must login as admin. [Default=Off]
nss /(No)MountISODiscSetInOneVolume	If this switch is enabled, cddvd.nss attempts to load an ISO9660 multiple-disk set as a single NSS volume. This volume is not mounted until all discs among the set are available to cddvd.nss. If this switch is disabled, cddvd.nss mounts each disk in the set as one individual NSS volume. [Default=Off]

Commands for CD and DVD Image Files as NSS Volumes

Cddvd.nss is loaded automatically on startup by default. Cddvd.nss provides the following commands for adding and removing CD and DVD image files as NSS Volumes.

While the CD or DVD image source file is loaded as an NSS volume, the following actions cause the image file to be removed as an NSS volume:

- Any file operations on the image source file, such as open, read, or write
- Deactivation of the NSS volume where the image source file resides

Commands	Description
<code>nss /MountImageVolume=<i>path_imagefilename</i></code>	Add and mount the specified CD or DVD image file as a read-only NSS volume. Replace <i>path_imagefilename</i> with the path on the NSS volume where the image file resides, including its filename. For example: <code>nss /MountImageVolume=nssvol:\lsuse9_1.iso</code>
<code>nss /RemoveImageVolume=<i>path_imagefilename</i></code>	Dismount and remove the specified CD or DVD image file as a read-only NSS volume. Replace <i>path_imagefilename</i> with the path on the NSS volume where the image file resides, including its filename. For example: <code>nss /RemoveImageVolume=nssvol:\lsuse9_1.iso</code>

DOS FAT Commands

NSS provides the following commands for managing DOS FAT partitions.

Commands	Description
<code>DOSFAT</code>	If DOSFAT is specified in the nssstart.cfg file, loads only those modules essential for accessing FAT 16 and FAT 12 drives. NetWare does not support FAT 32 drives.
<code>nss /FATPartition=<i>partition_type_number</i></code>	Supports up to three additional partition types containing 16-bit FATs, such as /FATPartition=12,13.
<code>nss /{No}FATLongNames</code>	Enables long filenames on FAT volumes. [Default=On]

Multiple Server Activation Prevention Commands

The management file for pool MSAP is _admin\manage_nss\pool\poolname\zIss\msap.xml. One file exists for each pool. This file contains MSAP statistics for the pool. The MSAP attribute is displayed in the enabledAttributes field of the poolinfo.xml management file.

For manage.cmd, the pool operation getPoolInfo returns the MSAP tag (<msap>) in the supportedAttributes tag (<supportedAttributes>) and the enabledAttributes tag (<enabledAttributes>).

For APIs, the pool feature `zpool_feature_msap` can be viewed and controlled using the `zGetInfo` and `zModifyInfo` commands.

MSAP Console Command	Description
<code>nss /msapserver</code>	Enables MSAP for all the pools on the server. By default, MSAP is enabled for every pool on the server. We recommend that you never disable MSAP.
<code>nss /nomsapserver</code>	Disables MSAP for all the pools on the server. This command remains in effect only until the server is next rebooted. We recommend that you never disable MSAP.
<code>nss /msaprebuild</code>	Rebuilds a corrupt MSAP block. Before issuing the command to rebuild, you must deactivate the pool because a corrupt MSAP prevents a pool from going into Maintenance state. Rebuilding an MSAP block does not give the rebuilders ownership of the pool.
<code>nss /poolmsap=poolname</code>	Enables MSAP for a given pool on the server. MSAP is enabled the next time the pool is activated. (Enter the command, deactivate the pool, then activate the pool. MSAP is now enabled.)
<code>nss /nopoolmsap=poolname</code>	Disables MSAP for a given pool. Use the command when the pool is activated. MSAP is disabled the next time the pool is activated. (Enter the command, deactivate the pool, then activate the pool. MSAP is now disabled.)
<code>nss /pools</code>	Displays the message "Multi-use detect" for pools that have MSAP enabled.

Multipath Connection Failover Commands

NSS provides the following Media Manager commands for managing multipath I/O failover.

Media Manager Multipath I/O Console Command	Description
<code>list failover devices device_id</code>	<p>This command lists all of the failover devices. It also lists all the paths associated with each device, their assigned priorities, and the path that is selected.</p> <p>To list the paths associated with all the devices on the server, enter the command without specifying the <code>device_id</code>.</p> <p>To list the paths associated with a given device, enter the command followed by the <code>device_id</code>.</p>
<code>mm set failover priority pathid=number</code>	This command sets the priority level for the selected path. The <code>pathid</code> must be a valid path ID. The <code>number</code> is the priority to set for the selected path. The number must be a decimal integer value between 1 and 4 million, with 1 being the highest priority and 4 million being the lowest priority.
<code>mm set failover priority pathid=number /insert</code>	The <code>/insert</code> option inserts the specified path with its specified priority. For example, if you have four existing paths that are assigned the priorities of 1, 2, 3, and 4, and you enter a new path followed by a number 2 and the <code>/insert</code> option, then the paths that were previously assigned to 2, 3, and 4 priority are bumped to priority 3, 4, and 5 in order to accommodate the new path that has been assigned priority 2.

Media Manager Multipath I/O Console Command	Description
mm set failover state <i>pathid</i> =up /setpath	This command sets the state of the specified path to Up. The <i>pathid</i> must be a valid path ID.
	If the Up option is followed by the /setpath option, NSS automatically selects the highest priority path from among all the paths that are in the Up state, including the new path.
mm set failover state <i>pathid</i> =down /setpath	This command enables you to designate a path to be in the Down state so you can perform preventative maintenance or reroute cables on a good, functional path. If the path is bad, NSS automatically moves the path to a Down state.
	If the Down option is followed by the /setpath option, NSS automatically selects the highest priority path from among the other paths that are currently in the Up state.
mm set failover path <i>pathid</i>	This command activates the selected path as <i>selected</i> , which means it serves as the primary path. The <i>pathid</i> must be a valid path that is currently in the Up state. The priority of a path remains static regardless of whether a path is considered up or down or whether a path is selected or not selected as the primary path.
mm restore failover path <i>device_id</i>	This command forces the device to reselect the highest priority path that is online. The <i>deviceid</i> must be a valid device ID.
mm reset failover registry	This command resets the multipath settings in the operating system registry.

Pool Snapshot Commands

The following table shows the server console commands you can use to manage pool snapshots.

Snapshot Management Commands	Description
mm snap create <i>snappool</i> <i>datapool</i> <i>snapname</i>	Creates a pool snapshot.
mm snap activate <i>snapname</i>	Activates a pool snapshot.
mm snap deactivate <i>snapname</i>	Deactivates a pool snapshot.
mm snap delete <i>snapname</i>	Deletes a pool snapshot.
mm snap rename <i>snapname</i> <i>newsnapname</i>	Renames the pool as specified
mm snap list	Lists the snapshots on the server.
mm snap shred <i>snapname</i> = on	Turns on shredding for the internal volume of the pool where you are storing the specified snapshot.
	If this option is enabled:
	<ul style="list-style-type: none"> ♦ You can have only one snapshot at a time of its original pool. ♦ After you delete the snapshot, allow enough time for the shredding process before you create a new one.

Snapshot Management Commands	Description
mm snap shred <i>snapname</i> = off	<p>Turns off shredding for the internal volume of the pool where you are storing the specified snapshot.</p> <p>If any pool snapshot was created on this pool prior to the NetWare 6.5 SP3 release, shredding is already turned on. Use this command to turn off shredding.</p>

The following table shows the attribute descriptions for pool snapshot commands.

Attributes for Pool Snapshot Commands	Description
snappool	The unique name of the original data pool that you are snapping; must be 2 to 16 characters.
datapool	The unique name of the stored-on pool for the pool snapshot; must be 2 to 16 characters.
snapname	The unique snapshot name of the pool snapshot, which is used as its pool name when the pool snapshot is activated; must be 2 to 16 characters.

NSS File System Rights Utility

The NSS Rights Utility allows you to specify file system Trustee rights for directories and files in the NSS File System. For information, see “RIGHTS Utility for NetWare” in the *NetWare 6.5 Utilities Reference*.

Configuring the System Cache to Fine-Tune NSS Performance

Under certain conditions, the NSS performance can be tuned to great benefit without sacrificing NetWare's performance. NSS tuning can be *proactive*, to get the highest possible speed from your storage system, or *reactive*, because there is a problem.

This section focuses on different proactive strategies that can improve NSS performance. In addition to this document, more in-depth information on NSS tuning can be found in the July 2002 Appnote, *Novell Storage Services (NSS) Performance Monitoring and Tuning* (<http://developer.novell.com/research/appnotes/2002/july/01/a020701.htm>).

This section discusses the following:

- ♦ “Do I Need to Tune NSS?” on page 231
- ♦ “Adjusting NSS Parameters” on page 231
- ♦ “Setting the Cache Balance” on page 232
- ♦ “Setting the Cache Buffers” on page 235
- ♦ “Setting the Closed File Cache Size” on page 237
- ♦ “Setting the File/Buffer Flush Timer” on page 237
- ♦ “Setting the Name Cache” on page 238

Do I Need to Tune NSS?

There are many factors that contribute to decreasing server performance; however, if you are noticing that your server is performing poorly and you suspect the storage subsystem (NSS), you can monitor the storage subsystem by using specific NSS command line options. These options help you determine if any tuning is required.

For further details and explanation, see the Command Line Options for Monitoring NSS in the July 2002 Appnote, *Novell Storage Services (NSS) Performance Monitoring and Tuning* (<http://developer.novell.com/research/appnotes/2002/july/01/a020701.htm>).

Adjusting NSS Parameters

After you have determined that your storage subsystem needs tuning, your next step is to determine what NSS parameters can be adjusted to improve your current NSS performance.

Before beginning, review the following section, [Important NSS Tuning Guidelines](#).

Important NSS Tuning Guidelines

- ◆ Make sure that you are running the latest version of NSS before adjusting parameters.
- ◆ Do not split your resources between two file systems. Use NSS volumes only on your server, not a combination of NSS volumes and NetWare Traditional volumes.

When the file system module (filesys.nlm) loads on NetWare, RAM that is not allocated elsewhere is given to the legacy cache. When NSS loads, it also takes about 60% of the RAM that is not allocated elsewhere for NSS. Because the two file systems are disparate, this will halve the performance of both caches. When applications load the amount of cache for both file systems, performance is reduced even further.

If you *must* run multiple file systems, try to get to know the usage patterns of each system. This might enable you to balance RAM between them more effectively.

- ◆ Purchase more RAM, if needed to improve performance.

Start with These Parameters

Tuning NSS is a matter of modifying a parameter or two, resetting the cache performance statistics, and then waiting and watching for performance gains or degradation.

IMPORTANT: Before you begin to adjust settings, you need to be aware that if you give NSS more memory than the server has, NSS fails to load. If your sys: volume is NSS-based, your server will be inoperable until you load the server with an NSS override to correct the situation.

If you need to restore a setting after a failed tuning attempt: At the server console, enter

server -z parameter

Adjusting the following parameters can improve your NSS performance:

- ◆ “Setting the Cache Balance” on page 232
- ◆ “Setting the Cache Buffers” on page 235
- ◆ “Setting the Closed File Cache Size” on page 237
- ◆ “Setting the File/Buffer Flush Timer” on page 237
- ◆ “Setting the Name Cache” on page 238

Setting the Cache Balance

The cache performance statistics are divided into SYS (system) and USER cache. System data is everything that isn’t user data. It includes the roll-back ZLOG (journal) and the roll-forward Purge Log, and the various databases and structures where NSS keeps information about files—for example, the name tree, the beast tree, and the visibility list.

If user data from cached files leaves no space for the system data, the file system performance might suffer. Under normal circumstances, you should see a 98% hit rate for both user data cache and system data cache. In some cases a lower cache rate is normal—for example, in situations where backups have run, or when large file copies have just occurred, or in a business that deals with large files that consistently flush the cache. If you want to raise the cache statistics in these situations, you will need to dedicate more RAM to NSS.

The following table lists a few NSS parameters that can be used to adjust the cache balance between user and system data:

Task	Purpose	Command
Control the division of the file system cache between user and system data	<p>If you have a server with a few files and volume attributes and a generous amount of cache RAM, you can increase this parameter.</p> <p>The default percentage for user data cache is 70%. Remember that whatever is not system cache is user cache.</p> <p>[Default=70]</p>	nss /CacheUserMaxPercent= <i>value</i>
Set the amount of cache that NSS takes from the file system	<p>Every 30 seconds (by default) or whenever the server loads an NLM™, NSS rebalances the NSS file system cache to the percentage specified by the CacheBalance parameter.</p> <p>NOTE: You can change the default time interval with the CacheBalanceTimer command.</p> <p>A low cache balance impedes the performance of NSS.</p> <p>We recommend that you set the cache balance parameter to equal the percentage of the total disk space you allocate for NSS. However, do not exceed 80 percent. You might want to initially set the parameter at 50 percent and adjust this number as necessary.</p> <p>[Default=60; Range=1 to 99]</p>	nss /CacheBalance= <i>value</i>
Set the number of cache buffers allocated for NSS	<p>This sets the minimum number of 4 KB cache buffers allocated for NSS file system access.</p> <p>[Default=512; Range=256 to 1048576]</p> <p>On a server with only NSS volumes, you can adjust the CacheBalance parameter to 85% without any problem. However, you should monitor the Least Recently Used (LRU) Sitting Time on the NetWare server to ensure that you are not running the server too low on memory.</p> <p>To safeguard against this, use the MinOSBufferCacheSize command to set a hard limit for the amount of RAM that can be used exclusively by the operating system.</p> <p>TIP: LRU Sitting Time is found in the Monitor utility under Disk Cache Utilization. Under normal circumstances, the server should be up for over 24 hours, so this statistic should never drop below 24 hours. It is important to understand that LRU Sitting Time is a measure of non-cache memory, not file system cache memory.</p>	nss /MinBufferCacheSize= <i>value</i>

Task	Purpose	Command
Set a minimum amount of RAM exclusively for the operating system	<p>If you allocate too much memory to your NSS cache, the server can run out of memory. To prevent this, set aside a minimum number of 4 KB cache buffers for the exclusive use of the server operating system.</p> <p>[Default=256; Range=256 to 1048576]</p>	nss /MinOSBufferSize= <i>value</i>
Set a maximum amount of memory to transfer to NSS during a cache balancing session	<p>Usually when the CacheBalance is recalculated, a small amount of RAM is either given or taken away from the NSS Cache. This parameter controls the maximum cache balance transfer (in the number of 4 KB cache buffers) given to the NSS file system cache per cache balance.</p> <p>If your server has applications running on it that can consume significant amounts of RAM for a short period of time, you might want to increase this parameter. Otherwise your server may take several minutes to get back to the correct amount of cache dictated by the CacheBalance parameter.</p> <p>This parameter does not affect memory requests made of NSS by the OS. For example, if NSS is asked to give back 5 MB of RAM, it will comply at the time of the request in one transfer.</p> <p>[Default=1024; Range=16 to 1048576]</p>	nss /CacheBalanceMaxBuffersPerSession= <i>value</i>
Show the cache hit ratio at the server console	<p>This is the number of cache hits divided by the number of attempts to get a file cache buffer from the cache. Any amount above 90% is good. This means the system is spending less time going to the disk to retrieve data.</p> <p>Cache hit is the number of times that NSS finds the desired file block in the cache buffers. Lower numbers indicate that NSS needs more memory.</p> <p>If you allocate more memory to NSS, the cache hit percentage increases. You can add more memory by adding more physical memory, increasing the cache balance, or increasing the minimum number of cache buffers for NSS. We do not recommend lowering the minimum number of OS cache buffers.</p>	nss /CacheHit

Task	Purpose	Command
Determine how often NSS rebalances the amount of cache it uses	<p>This lets you determine how often (in seconds) NSS rebalances the amount of cache it uses according to the total amount of memory on the server.</p> <p>If you have difficulty loading NLM programs because of low memory, you might want to lower this timer setting. A lower setting forces NSS to rebalance more often. If your server is stable, you might want to increase this timer so NSS does not work as hard; this ensures that the cache remains balanced. NSS monitors the total number of cache buffers to determine if the CacheBalance percentage is met. It then adjusts the timer to provide the appropriate number of cache buffers.</p> <p>[Default=30; Range=1 to 3600]</p>	<code>nss /CacheBalanceTimer=value</code>
Reset cache statistics	<p>This lets you clear the current statistics and start over.</p> <p>This is useful for checking the results of changes to the system.</p>	<code>nss /reset</code>

Setting the Cache Buffers

A cache buffer is a block (4 KB) of RAM that temporarily stores data. When you install NSS, it consumes 60% of the cache buffers by default.

The following are guidelines for changing the cache buffers:

- ◆ You can set a maximum of 1048576 cache buffers.
- ◆ You can set the buffers in percentages rather than integers.

Use the following commands at the server console to set your cache buffers or tune your cache parameters. You can set or tune cache buffers at anytime.

Task	Purpose	Command
Set the number of cache buffers allocated for NSS	<p>This sets the minimum number of cache buffers allocated for NSS file system access. The default and minimum number of cache buffers is 512. The range is 256 to 1048576.</p> <p>On a server with only NSS volumes, you can adjust the /CacheBalance parameter to 85% without any problem. However, you should monitor the Least Recently Used (LRU) Sitting Time on the NetWare server to ensure that you are not running the server too low on memory.</p> <p>To safeguard against this, use the nss /MinOSBufferCacheSize command to set a hard limit for the amount of RAM that can be used exclusively by the operating system.</p> <p>TIP: LRU Sitting Time is found in the Monitor utility under Disk Cache Utilization. Under normal circumstances, the server should be up for over 24 hours, so this statistic should never drop below 24 hours. It is important to understand that LRU Sitting Time is a measure of non-cache memory, not file system cache memory.</p>	nss /MinBufferCacheSize= value
Limit the number of cache buffers	<p>When the cache balance is recalculated, a small amount of RAM is either given or taken away from the NSS Cache.</p> <p>This parameter controls the maximum cache balance transfer (in 4 KB blocks) that is given to the NSS file system cache per cache balance. The default is 1024 (4 MB) per session. The range is 16 - 1048576.</p> <p>If your server has applications running on it that can consume significant amounts of RAM for a short period of time, you might want to increase this parameter.</p>	nss/CacheBalanceMaxBufferPerSession=value
Look up cache buffers	To quickly look up cache buffers, the cache uses a hashing algorithm that maps names to buckets. Sometimes multiple names map to the same bucket. When this occurs, all names must be searched to determine if the entry is in the cache. The number of entries in the hash table is proportional to the amount of free memory available when you load NSS.	nss/NumHashBuckets
Set the cache for file and directory entries	<p>This sets the number of name cache entries. Because NSS keeps a cache of the file and directory names it has recently accessed, setting the number of name cache entries speeds up opening files and path searches. The default is 2111. The range is 3 to 65521.</p>	nss/NameCacheSize
Use percentages instead of integers for cache balancing	This sets the buffers to percentages rather than integers for dynamic balancing of free memory for the buffer cache. The default is On. Use this command in combination with the /MinBufferCacheSize switch.	nss/(No)CacheBalance

Task	Purpose	Command
Set the number of authorization cache entries	This specifies the number of cache buffers to be used to speed up authorization requests.	nss /AuthCacheSize
	If many trustees are set on different files and directories, we recommend that you increase this number to at least 20000. [Default=1024; Range=16 to 50000]	
Show cache buffer statistics	This shows the cache buffer statistics.	nss /CacheStats
Reset cache statistics	This lets you clear the current statistics and start over. This is useful for checking the results of changes to the system.	nss /reset

Setting the Closed File Cache Size

The ClosedFileCacheSize parameter keeps the beast objects in cache so that NSS does not need to go to disk and unpack beast information again when it wants the same files. At the server console, enter

nss /ClosedFileCacheSize=xx

The default is 50,000. The range is 16 - 1,000,000. On average, each Closed File Cache entry consumes 0.4 - 1 KB of RAM.

Set this parameter to 100,000 or more if you have applications on your server that consistently cycle through the same set of files and you suspect that this cache is being flushed when combined with normal server operations.

TIP: The Closed File Cache grows up to the specified amount. Unlike file system cache, Closed File Cache does not take the maximum amount of memory it needs from the start. It also adapts; as memory is consumed by other processes, it dynamically reduces the number of entries so the system does not become starved for memory.

Setting the File/Buffer Flush Timer

Increasing the flush time settings can improve performance, but does it at the risk of data loss during a system failure. The timers directly relate to the amount of uncommitted data in NSS Cache.

Task	Purpose	Command
Set the amount of time before files are flushed.	This sets the maximum amount of time that modified files are kept in a cache buffer before flushing the files to disk.	nss /FileFlushTimer
	Increasing the /FileFlushTimer setting beyond a minute or two can lead to overflowing the ZLOG file and throttling system operations. [Default=10; Range=1 to 3600]	

Task	Purpose	Command
Set the amount of time before buffers are written.	This sets the maximum amount of time that modified NSS file system cache buffers are kept in memory before they are written to disk. [Default=1; Range=1 to 3600]	nss /BufferFlushTimer

Setting the Name Cache

The NameCache parameter specifies the amount of recently used Name Tree entries that NSS caches. At the server console, enter

nss /NameCache=xx

The default is 2111. The range is 3 - 65,521. Each entry uses about 150 bytes of memory.

In medium to large servers with enough RAM, you might consider increasing this value to 40,000.

NOTE: Name cache grows up to the specified limit. Unlike the file system cache, it does not take the maximum amount of memory it needs from the start.

18

Troubleshooting NSS

This section describes some problems you might experience with Novell® Storage Services™ (NSS) and provides suggestions for resolving or avoiding them.

- ◆ “[Tuning NSS Volumes for GroupWise Servers](#)” on page 239
- ◆ “[Cannot See Volumes and Devices](#)” on page 239
- ◆ “[NSS Does Not Recognize a Device](#)” on page 240
- ◆ “[Cannot Create an NSS Pool or Volume](#)” on page 240
- ◆ “[Cannot Create an NSS Volume](#)” on page 240
- ◆ “[File Compression Is Not Working](#)” on page 240
- ◆ “[Software RAID 1 Fails to Recognize a Replacement Device](#)” on page 240
- ◆ “[Problems Moving NetWare 6.5 NSS Pools to NetWare 6.0 Servers](#)” on page 241
- ◆ “[Problems Following DFS Junctions in Windows 2000/XP Releases](#)” on page 241

For additional troubleshooting information, see the [Novell Knowledgebase](http://support.novell.com) (<http://support.novell.com>).

Tuning NSS Volumes for GroupWise Servers

NSS performance has been dramatically improved in NetWare® 6.5. As a result, the only tuning that you need to do to enhance the performance of GroupWise® on NSS is to disable the salvage feature by entering the following at the server command line:

```
nss /NoSalvage
```

Cannot See Volumes and Devices

If you cannot see your volumes or the devices associated with those volumes, you might have a connection failure. Connection failures can occur if an adapter, cable, or switch in the path between the server and the storage device fails for any reason. If there is a connection failure, repair or reconfigure the equipment.

If you have multiple interconnect paths in your server-to-storage configuration, turn on Multiple Connection Path Support. For instructions, see “[Managing Multiple Connection Paths to Devices](#)” on page 95. Then repair the equipment.

If you cannot see your volumes or the devices associated with those volumes, you might not have the appropriate multipath drivers that support the multipath functionality. Turn off the multipath support. For instructions, see “[Managing Multiple Connection Paths to Devices](#)” on page 95. Load the proper drivers, then turn on Multiple Connection Path Support.

NSS Does Not Recognize a Device

If your server does not recognize a device, it might be because NSS recognizes only what the Media Manager recognizes. For this release, NSS recognizes hard drives, CD drives, DVD drives, USB drives, and Zip* drives. Device size must be 2 TB or less.

Cannot Create an NSS Pool or Volume

If you cannot create an NSS pool or volume, there are a few possible causes.

Your server might not have enough free space to create more storage pools or NSS volumes. Ensure you have enough free space to create another NSS storage pool or NSS volume. See [“Viewing Partitions on a Device” on page 61](#).

Each NSS volume must be part of a storage pool. Before you create an NSS volume, create a storage pool.

Cannot Create an NSS Volume

If you cannot create an NSS volume, consider these possible solutions:

- NSS might not own enough free space for another NSS volume. Add another storage device.
- If you mix Traditional and NSS volumes, there is a maximum of 255 volumes together plus the system volume. Dismount an NSS volume from a pool or dismount a Traditional volume to free up space.

File Compression Is Not Working

If you cannot compress a file, you might not have set the Compression attribute when you created your NSS volume. To apply the file compression option to an existing NSS volume: From iManager, click Storage > Volumes > Properties > Attributes, then select Compression.

For information, see [“Using Compression to Conserve Storage Space on NSS Volumes” on page 177](#).

Software RAID 1 Fails to Recognize a Replacement Device

If a drive fails that is part of a software RAID 1 device, your system might not recognize the replacement drive and does not begin remirroring automatically.

To recover:

- 1 Reboot the system to rescan devices and recognize the replacement drive.
- 2 Dismount the NSS volumes on the software RAID device to stop the I/O.
- 3 Expand the software RAID 1 device and specify space from the replacement drive as a new RAID segment. Remirroring begins automatically.
- 4 Allow the remirror to complete before mounting the NSS volumes.

Problems Moving NetWare 6.5 NSS Pools to NetWare 6.0 Servers

NetWare 6.5 data pools are normally compatible for clustering purposes with NetWare 6.0, both backwards and forwards. The Media Manager changed between NetWare 6.0 and 6.5, but the media format is the same.

If you move a device from the NetWare 6.5 server to a NetWare 6.0 server, and if you can see the NetWare 6.5 pool on the disk, but cannot activate it on your NetWare 6.0 server, the most likely causes might be a name conflict or that the pool was mirrored.

Pool and volume names must be unique on the server. Renaming the NetWare 6.5 pool should allow it to be activated on the NetWare 6 server.

If the pool was mirrored, the old media manager on NetWare 6.0 probably would have problems with it because the information is different. You should remove the mirror before trying to move the disk to NetWare 6.0.

Problems Following DFS Junctions in Windows 2000/XP Releases

Windows 2000 Service Pack 4 and Windows XP Service Pack 2 might have problems following DFS junctions over CIFS because of a defect in Windows. (This problem exhibits itself in a pure Windows environment.)

To avoid this problem for your users with these releases of Windows, install the Novell Client on their desktops.

Another option is to modify the lmhosts file for all client computers with appropriate entries for any volumes on NetWare servers that use DFS junctions.

1 In a text editor, open the lmhosts file.

- ◆ **Windows 2000:** c:\WINNT\system32\drivers\etc\lmhosts
- ◆ **Windows XP:** c:\windows\system32\drivers\etc\lmhosts

If you do not have an lmhosts file, use the lmhosts.sam file as an example.

2 For each volume the user connects to that has a DFS junction, add a line at the end of the file that identifies the IP address and NetBIOS name of the data server where the volume resides.

```
192.168.1.1      servername-W
```

Replace *192.168.1.1* with the actual IP address and *servername* with the host name of your server.

For example, suppose you have the following server with VOL1 that contains one or more DFS junctions:

- ◆ Server IP address: 10.10.1.1
- ◆ Server name: USERSVR
- ◆ NetBIOS server name: USERSVR-W
- ◆ Volume name: VOL1

The line you add to the lmhosts file would be:

```
10.10.1.1      USERSVR-W
```

3 Save and close the lmhosts file.

- 4 If necessary, repeat **Step 1** to **Step 3** on each client computer, or create an lmhosts file and distribute it to the client machines.
- 5 On each client, map a network drive to the user's data volume.
 - 5a In the Windows Explorer file manager, click Tools > Map Network Drive.
 - 5b In Folder, type one of the following:

```
\192.168.1.1\volume  
\servername-W\volume
```

Replace *192.168.1.1* with the actual IP address or *servername* with the host name of your server.
 - 5c Select Reconnect at Logon.
 - 5d Click Finish.

Continuing the example above, the user could map to \\10.10.1.1\VOL1 or to \\USERSVR-W\VOL1.

19

Managing File System Access to Directories and Files

After you create Novell® Storage Services™ volumes, you are ready to organize and manage your applications and data in the file system.

This section presents a simple example of a network directory structure to help you plan your file system. Based on the example and the accompanying information, you can begin to design a directory hierarchy suitable to your own needs.

IMPORTANT: We recommend that you create separate volumes for applications and user data, reserving the sys: volume for the operating system and its extensions.

This section discusses the following:

- ◆ “Understanding File Systems” on page 243
- ◆ “Planning Your Directory Structure” on page 248
- ◆ “Configuring and Managing Directories” on page 252
- ◆ “Understanding Access and Usage Control for Directories and Files” on page 259
- ◆ “Configuring File System Trustees, Trustee Rights, Inherited Rights Filters, and Attributes for Directories and Files” on page 267

Understanding File Systems

The NSS and Traditional file systems provide a uniform method of referring to directories and files and locating them on a variety of storage media. As with your office filing system, you must impose organization on data you store in a volume. Within each volume, you can group information in logical containers called folders or directories.

This section describes the following key components of your NetWare file system:

- ◆ “Directory Structures” on page 244
- ◆ “Directory Path” on page 245
- ◆ “Root Directory” on page 245
- ◆ “Fake Root Directory” on page 245
- ◆ “Directory Map Objects” on page 246
- ◆ “Drive Map” on page 247

Directory Structures

The NSS and Traditional file systems provide a uniform method of referring to directories and files and locating them on a variety of storage media. As with your office filing system, you must impose organization on data you store in a volume. Within each volume, you can group information in logical containers called folders or directories.

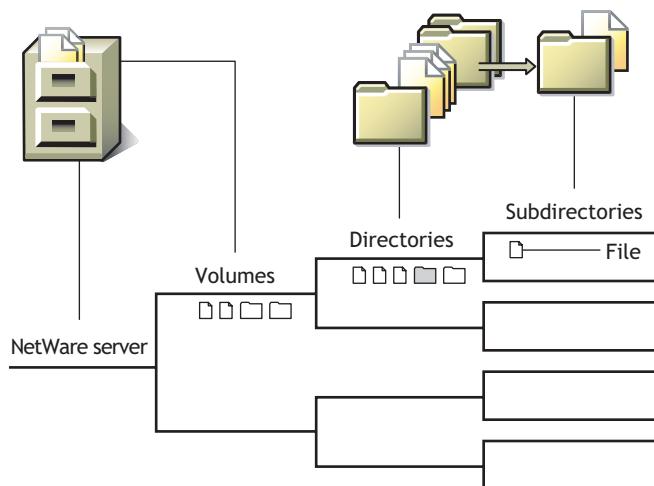
A directory is a logical separation within a volume where you store files and subordinate directories, called subdirectories. The directory is a special type of file that contains a list of its files and subdirectories. It can also contain metadata about the directory, such as who can access it and its attributes. For NetWare Traditional, the directory's metadata is stored in a Directory Entry Table (DET), separate from the directory itself.

A file is the basic logical container for storing information, such as an image, a document, a program, text, or a database.

Within each volume, the directory structure is hierarchical. It is an inverted tree structure with a single root. The topmost directory in the hierarchy is called the root directory. A directory is called the parent directory of the subdirectories and files in it. A volume can contain any number of directories. A directory can contain any number of files and subdirectories.

The following figure illustrates how volumes are similar to drawers in an office filing cabinet that contain related information. For example, the sys: volume on NetWare contains the operating system and its extensions. Other volumes might contain applications, corporate data, or user home directories and files.

Figure 9 Sample Directory Structure for NSS and Traditional File Systems on a NetWare Server



There is no one best solution for organizing files with directories. You can use a combination of approaches, such as by geographic location, applications, business units, projects, or owners. For information, see [“Planning Your Directory Structure” on page 248](#).

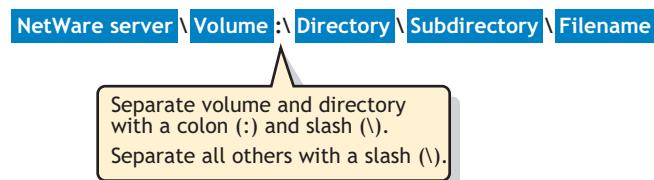
To control who can access directories and files on your NSS and Traditional NetWare file systems, you must assign file system trustees, trustee rights, and inherited rights filters. For information, see [“File System Trustee Rights” on page 260](#).

To control how authenticated users can use directories and files, you must set directory and file attributes. For information, see [“Understanding Directory and File Attributes for NSS Volumes or NetWare Traditional Volumes” on page 265](#)

Directory Path

A directory or file is located by its *path*, which states where the directory or file is logically located in a volume. A path includes the volume, directory, and any subdirectories leading to the file. The following figure shows how to specify a full path. Listing the server is optional. It is usually excluded when specifying a path relative to the server where you are logged in. The slash after the colon is required in some interfaces and optional in others. Refer to the interface's documentation to determine if a colon and slash combination (:\) is required to separate a volume and directory.

Figure 10 Directory Path Conventions



If your network uses multiple server or client operating systems or multiple file systems, keep in mind the conventions of the different file systems, such as delimiters, path length, and case sensitivity. For example, the NSS and Traditional file systems on NetWare use backslashes as delimiters and are case insensitive, while file systems native to Linux and UNIX use forward slashes and are case sensitive. As another example, NetWare allows 255 characters in a directory path (counting the drive letter and delimiters), but DOS allows only 127 characters. For more information, check the application's documentation.

Root Directory

The root directory is the base directory in the volume. The root directory of a volume typically contains only directories.

Storing files at this level is possible, but it can be a security risk. Granting file system Trustee rights to files at the root of the volume necessitates granting rights to the entire volume. For information about Trustee rights, see [“File System Trustee Rights” on page 260](#).

To avoid this security risk, create Fake Roots for applications that want to write files to the root directory. For information, see [“Fake Root Directory” on page 245](#).

Fake Root Directory

A fake root is a directory in a volume that functions as a root directory for a specific software application.

Some applications require their executable files to be located in a root directory. However, for security, you should not grant users rights to files at the root of the volume.

NetWare allows you to map a directory as drive that serves as a fake root directory, using the Map Root command. This allows you to install an application in a directory and assign rights for it at that directory level. For information, see [“Creating a Fake Root Directory with the Map Root Command” on page 254](#).

Fake roots work with the NetWare DOS Requester, with NetWare shells, and with clients, including Windows* 98/ME and Windows 2000/XP/2003. Fake roots do not work for IBM* OS/2* clients. (Under OS/2, all mapped drives are roots, and search drives do not exist.)

For Windows NT*/2000/XP workstations that use Novell Client™ login scripts, a Map command in the login script automatically enables a mapped NetWare subdirectory as a fake root directory. For information about disabling this behavior, see “[Disabling the Default Use of Map as Map Root in Login Scripts](#)” on page 254.

Directory Map Objects

In Novell eDirectory™, the Directory Map object is a pointer to a path in the NetWare server file system that represents a particular directory in the file system. It allows you to make simpler references to directories by using a Directory Map object in your login scripts instead of the fixed path. Directory Map objects are available only for NetWare NSS and Traditional volumes.

For instructions, see “[Creating and Configuring a Directory Map Object](#)” on page 255.

Using a Directory Map Object

Directory Map objects can be especially useful in Novell Client login scripts to point to directories that contain applications or other frequently used files. In Novell Client login scripts, you can map a drive to a Directory Map object instead of to the directory. If the application’s location in the directory structure changes, you can update the path in the Directory Map object instead of changing the related drive maps in numerous login scripts. For information about Map commands, see “[Login Script Commands and Variables](#)” in the *Novell Login Scripts Guide*.

For example, suppose a word processing application resides in a directory called `appsvol:wpapps\oo10`. You map a network-search drive to that directory in login scripts you create for users.

Later, you upgrade the word processing application and rename its directory from `appsvol:wpapps\oo10` to `appsvol:wpapps\oo11`. You must modify the path in the network drive map in every login script where that network-search map appears.

If you map the directory path to a Directory Map object instead of a network-search drive, you can avoid tedious modifications of the login scripts. Use the eDirectory plug-in for Novell iManager to create a Directory Map object. For example, create a Directory Map object called `default_wpapp`, for `appsvol:wpapps\oo11`. Place a Map command in your login scripts that map a search drive to the Directory Map object, rather than to the specific directory. For example:

```
map ins s2:=.default_wpapp.dept.domain_us
```

When users log in, their network-search drive is mapped to the `default_wpapp` Directory Map object, which, in turn, points to `appsvol:wpapps\oo11`.

Later, if you install a yet another default word processor and change the directory’s name to `appsvol:wpapps\superwp`, you need to change only the directory path in the `default_wpapp` Directory Map object. You do not need to change the Map command in the login script because the Map command still indicates the correct Directory Map object.

Additional Information

For information, see “[Object Classes and Properties](#)” in the *Novell eDirectory 8.7.3 Administration Guide*.

Drive Map

A drive map is a pointer to a location in your local or network file system. The map assigns a local drive letter to a directory path on a volume where you have access rights. The directory path includes the volume, directory, and any subdirectories leading to the file. The local drive letter can be used instead of the complete path name.

Drive maps can be permanent or temporary:

- ♦ **Permanent Map:** To map a drive so you can use it every time you log in, place a Map command in your Novell Client login script, or use the mapping functionality of your client operating system and enable it to reconnect at login. The network drive is remapped every time you log in.
- ♦ **Temporary Map:** To map a drive so you can use it only during your current session, use the Novell Map Network Drive command in the Novell Client, use the NetWare Map command from a system prompt, or use the mapping functionality of your client operating system. The network drive map is valid only until you log out.

NetWare recognizes three types of drive mappings:

- ♦ “Local Drive Maps” on page 247
- ♦ “Network Drive Maps” on page 247
- ♦ “Network-Search Drive Maps” on page 247

For information about how to use the NetWare Map command, see [Map](http://www.novell.com/documentation/nw65/utlrfenu/data/h7onc376.html) (<http://www.novell.com/documentation/nw65/utlrfenu/data/h7onc376.html>) in the *NetWare 6.5 Utilities Reference* or see “Login Script Commands and Variables” in the *Novell Login Scripts Guide*.

Local Drive Maps

You create local drive maps to establish directory paths to local storage media such as your workstation disk drives, CD drives, Zip* drives, USB drives, and floppy disk drives.

Typically, the Lastdrive command in your DOS configuration settings is set to end with drive E: (lastdrive=e), or with the last drive specification in use on your system. Typically, drives C: through E: are used for local drives, but you can assign more drive letters, if needed, by modifying the Lastdrive command.

To change this default, use a text editor to add or modify the DOS Lastdrive command in your workstation config.sys file. For example:

```
lastdrive=z
```

Network Drive Maps

Network drive maps point to volumes and directories on the network where you have access rights. Typically, drives F: through Z: are used for network drive maps. Each user can map drive letters to different directories.

Network-Search Drive Maps

Network-search drive maps point to directories that contain frequently used files such as applications files. This map enables the system to locate an application file even if it is not located in the directory where you are working.

Network-search drive maps are numbered, although they also have drive letters. For example, a network-search drive 1 (or s1) can also be known as network drive Z:.

You can map up to 16 network-search drives, beginning with drive letter Z: (s1) and moving backwards through the alphabet to K: (s16). You cannot map a network-search drive and a regular network drive to the same drive letter.

If you request a file that the system cannot find in your current directory, the system looks in every directory that a network-search drive is mapped to. The system searches, following the numerical order of the search drives, until the program file is found or cannot be located.

Network-search drive maps are not supported on IBM OS/2 workstations. The search functionality is provided with the OS/2 Path, Libpath, and Dpath commands in the config.sys file.

Planning Your Directory Structure

This section presents a simple example of a network directory structure to help you plan your file system. Based on the example and the accompanying information, you can begin to design a directory hierarchy suitable to your own needs.

IMPORTANT: We recommend that you create separate volumes for applications and user data, reserving the sys: volume for the operating system and its extensions.

This section discusses the following:

- ◆ “Organizing Directory Structures Based on Access Requirements” on page 248
- ◆ “Managing Directory Structures for Network Applications” on page 249
- ◆ “Designing Application Directory Structures” on page 249
- ◆ “Designing Data Directory Structures” on page 251
- ◆ “Designing Home or User Directory Structures” on page 251

Organizing Directory Structures Based on Access Requirements

Security is one of the most important aspects of file system organization. File system trustees and trustee rights specify who can access different directories and files. File system directory and file attributes specify what authenticated users can do with the file, such as being able to merely read a file or to modify it.

Organizing the Directory Structure

Organize directories and files according to who needs access to them. In other words, use the directory structure to reflect access requirements.

For example, you can structure the hierarchy of directories in such a way as to take advantage of the inheritance aspect of rights. Associate file system trustees and trustee rights with volumes, directories, and files as a safeguard against deletion or modification by users. Specify directory and file attributes to control what users can do.

Grouping the User Community

Group the user community based on each user’s access requirements.

Users grouped by role (relative to file access) can be assigned ownership of directories and files, and users whose roles vary can be assigned rights on the basis of equivalence.

Users needing a particular kind of access to certain directories and files can be grouped so that appropriate access belongs to the group (and consequently, to each member).

Managing Directory Structures for Network Applications

You can install various types of network applications, such as word processing or spreadsheet programs, to make them available to users. When installing applications, keep the following in mind:

- ◆ To install applications on your NSS or Traditional file system, you must be a Trustee with the Create right for the directory where you will be installing the application. The Supervisor user of the server automatically has this file system Trustee right.
- ◆ Follow the instructions in the application's documentation for installing the application onto a network. Make sure the application is designed for network (multiuser) use.
- ◆ When creating application directories, consider issues related to ease of distribution, installation, and operational control for network applications.
- ◆ If the application requires that it be installed at the root of a volume, but you would rather install it in a subdirectory for security reasons, you can map the directory to a fake root.

For information, see [“Fake Root Directory” on page 245](#).

- ◆ After you install the application:

- ◆ Designate Novell eDirectory organization, role, and user objects as file system Trustees for the application directory and its contents.
- ◆ Assign access rights for each trustee.
- ◆ Configure attributes for the directory and its files.

For information, see [“Understanding Access and Usage Control for Directories and Files” on page 259](#).

- ◆ To allow users to access network-based applications, map search drives to the directories that contain these applications. For information, see [“Network-Search Drive Maps” on page 247](#).

To make the mapped search drives permanent, place them in login scripts, which are executed when users log in. For information, see the [Novell Login Scripts Guide](#).

- ◆ You can create a Directory Map object that points to an application directory.

Directory Map objects are useful in login scripts. Instead of mapping a drive to a specific directory path, you map a drive to a Directory Map object that points to a directory.

If you change the directory path, you need to change only the Directory Map object's definition.

- ◆ If you install the application in the sys:\public directory, it is not necessary to make file system Trustee assignments or map a search drive. Because users generally have Read and File Scan rights in sys:public, users can see and use all applications installed there. Use this directory structure only if you want all users to have access to all applications.

Designing Application Directory Structures

Application directories are storage areas where you install applications for convenient network access by groups, users, and other applications. You can install a variety of network applications, such as word processing or spreadsheet programs, and make them available to users.

For ease of management, create a separate volume for your applications and store applications in different directories. Mixing NetWare utilities with application program files complicates the file structure when you upgrade a network. An application file might have the same filename as a NetWare utility file or another application's program file. If filenames are the same, one file overwrites the other because two files with the same filename cannot coexist in a directory.

Keep program files separate from data files to simplify application management. For example, program files seldom change, but user data changes frequently. By creating a separate application volume and data volume, you can back up program files separately from data files. Frequent network backup can then focus only on data directories, with application volumes being backed up as needed. Creating data directories for shared data files allows single-point backup and management of shared files.

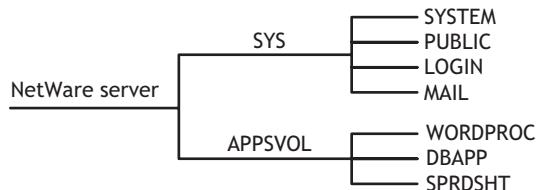
This section describes the following examples of application directory structures:

- ◆ “[Application Volume with Separate Application Directories Off Its Root](#)” on page 250
- ◆ “[Sys: Volume with a Parent Application Directory Off Its Root](#)” on page 250
- ◆ “[Sys: Volume with Separate Application Directories Off Its Root](#)” on page 250
- ◆ “[Sys:public Directory with a Parent Application Directory](#)” on page 251

Application Volume with Separate Application Directories Off Its Root

Create a separate volume for applications. Create a separate directory for each application off the root of the application volume, as shown in the following example.

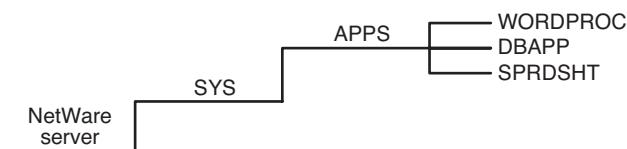
Figure 11 Application Volume with Separate Application Directories Off Its Root



Sys: Volume with a Parent Application Directory Off Its Root

In the sys: volume, create a parent application directory at the root. Create a separate directory for each application in the parent application directory, as shown in the following example.

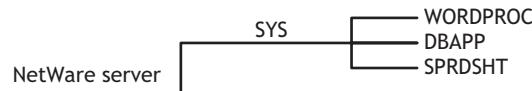
Figure 12 Sys: Volume with a Parent Application Directory Off Its Root



Sys: Volume with Separate Application Directories Off Its Root

In the sys: volume, create a separate directory for each application at the root of the volume, as shown in the following example.

Figure 13 Sys: Volume with Separate Application Directories Off Its Root

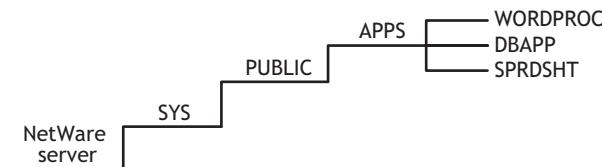


Sys:public Directory with a Parent Application Directory

Because users generally have Read and File Scan rights in sys:public, users can see and use all applications installed in it. Use this directory structure only if you want all users to have access to all applications.

We do not recommend installing applications in the sys:public directory. If you decide to use the sys:public directory, create a parent directory for applications in sys:public, as shown in the following example.

Figure 14 Sys:public Directory with a Parent Application Directory



Designing Data Directory Structures

Data directories are storage areas where groups and users store work files and databases. Data directories allow users to share data, create work directories, and make Trustee assignments for groups or users who need access to these directories. You can also create a directory to transfer files between directories on the network.

For ease of management, create a separate volume for your data and store different types of data in different directories.

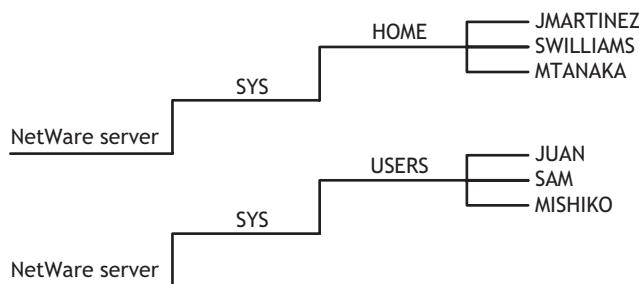
Designing Home or User Directory Structures

To provide personal workspace for users, create a separate home or user volume and create a subdirectory in it for each user. You can also create parent directories for groups of user directories. The data files a home or user directory contains are not available to other users, except network administrators or managers who have the necessary access rights.

For ease of management, create a separate volume for your home or user directories.

If you decide to use the sys: volume, create a parent directory in volume sys:, such as home or users. Within the parent directory, the name of each subdirectory should be the username. Usernames can be up to 47 characters, but DOS displays only 8 characters in a one-level directory name.

Figure 15 Home or User Directory Structure



Configuring and Managing Directories

This section discusses the following system administration tasks:

- ♦ “[Creating a Directory](#)” on page 252
- ♦ “[Viewing Directory and File Information](#)” on page 253
- ♦ “[Copying or Moving Directories and Files](#)” on page 254
- ♦ “[Creating a Fake Root Directory with the Map Root Command](#)” on page 254
- ♦ “[Disabling the Default Use of Map as Map Root in Login Scripts](#)” on page 254
- ♦ “[Creating and Configuring a Directory Map Object](#)” on page 255
- ♦ “[Mapping Network Drives](#)” on page 258

Creating a Directory

You can create directories locally using the NetWare GUI console, and remotely using the following management tools:

Management Tool	NSS on Linux	NSS on NetWare	NetWare Traditional File System
Novell NetStorage	Yes	Yes	No NetStorage does not support Traditional volumes.
Novell Client™ for Windows 2000/XP	Yes	Yes	Yes
Novell Remote Manager for Linux	No	No	No
Novell Remote Manager for NetWare	No	Yes	Yes

To create a directory, you must have the Create right for the directory that you want to add the new directory to. When creating a root directory, select the Volume object instead of selecting a parent directory.

- 1 In your Web browser, log in to Novell Remote Manager on the NetWare or Linux server where you want to create a directory in an NSS volume. The general form of the URL is <http://192.168.1.1:8008>
Replace *192.168.1.1* with the actual IP address or DNS name of your server.
- 2 Click Manage Server > Volumes.
- 3 Click the Properties icon next to the Volume you want to manage.

The screenshot shows the 'Properties' page for the directory `/TEST/acatt_home`. The 'Directory entry information' section displays the following details:

Owner	ACATT
Creation date and time	Jun 30, 2004 12:51 pm
Effective rights	SRWCEMF
Inherited rights filter	SRWCE_F
File space limit	None
File space in use	Not available

The 'Trustee information' section lists three entries:

Object name	Trustee rights	Actions
.CN=acatt,O=novell,T=TODDSBUILDTREE.	SRWCEMF	Delete
.CN=ddogg,O=novell,T=TODDSBUILDTREE.	R_F	Delete
.CN=animals,O=novell,T=TODDSBUILDTREE.	RWCEMF	Delete

Below the trustee table are buttons for 'Add Trustee', 'User Name:' (with a 'Browse' button), and 'Delete Directory and Contents'.

The 'Salvagable files' section indicates 'None'.

At the bottom are buttons for 'Rename Directory' (with 'New name:' set to `acatt_home`) and 'Create Subdirectory' (with 'New name:' empty).

- 4 Type the name of the subdirectory, then click Create Subdirectory.

Viewing Directory and File Information

You can see extended information about a directory or file with Novell NetStorage, Novell Remote Manager, and the Novell Client.

You can view directory information such as

- ◆ Owner and trustees
- ◆ Creation date and time
- ◆ Attributes, effective rights, and the IRF
- ◆ Disk space limitations

You can view file information such as

- ◆ Owner and trustees
- ◆ Attributes, effective rights, and the Inherited Rights and Filters (IRF)

- ◆ Name space
- ◆ File size
- ◆ Creation, access, archive, and modify dates

For information, see “[Understanding Access and Usage Control for Directories and Files](#)” on [page 259](#).

Copying or Moving Directories and Files

You can copy or move a directory’s subdirectories and files, if you have the necessary rights to do so. You cannot move the location of the directory itself, unless you also have the necessary rights for the parent directory of the target directory and for the destination directory.

To copy or move a directory’s subdirectories and files, you must have File Scan rights to the source directory, and you must have the Create right to the destination directory.

To move a directory’s subdirectories and files, you must also have the Erase right to the source directory, because moving files includes deleting them from the source directory. For instructions, see “[Viewing Details of Directories or Files and Performing Specific Actions on Them](#)” in the *NetWare 6.5 Novell Remote Manager Administration Guide for NetWare*.

Creating a Fake Root Directory with the Map Root Command

If your application must be installed at the root, load the files in a directory, then use the Map Root command in the login script to designate the directory as a fake root directory. For information about using the Map command in a login script, see “[Login Script Commands and Variables](#)” in the *Novell Login Scripts Guide*.

For example, suppose you want to install a word processing application, named *mywpapp*, on the apps: volume, and it requires a root directory installation. You do not want to put the application in the apps: volume’s root directory for security reasons. Instead, you install the application in the *apps:wpapps\mywpapp* subdirectory. In the Novell Client login script for users of the application, you use the Map Root command to map the subdirectory to the K: drive as a fake root:

```
map root s16:=k:=apps:wpapps\mywpapp
```

To change the fake root back to the original root, remap the drive.

NOTE: You cannot use the DOS Change Directory (cd) command at the fake root to return to the original root.

Disabling the Default Use of Map as Map Root in Login Scripts

For Windows NT/2000/XP workstations that use Novell Client login scripts, a Map command in the login script has the same effect as using an explicit Map Root command. It automatically enables a mapped NetWare subdirectory as a fake root directory. Applications installed in the subdirectory serving as the fake root cannot access directories above that subdirectory.

If necessary, you can disable the Map command’s automatic Map Root behavior on Windows by adding SET MAPROOTOFF="1" as the first line in the login script. To create a fake root when the MapRootOff parameter is enabled, the login script must explicitly use the Map Root command.

For more information, see the *Novell Login Scripts Guide*.

Creating and Configuring a Directory Map Object

- 1 In your Web browser, log in to Novell iManager on the NetWare 6.5 server where you want to create the Directory Map object. The general form of the URL is

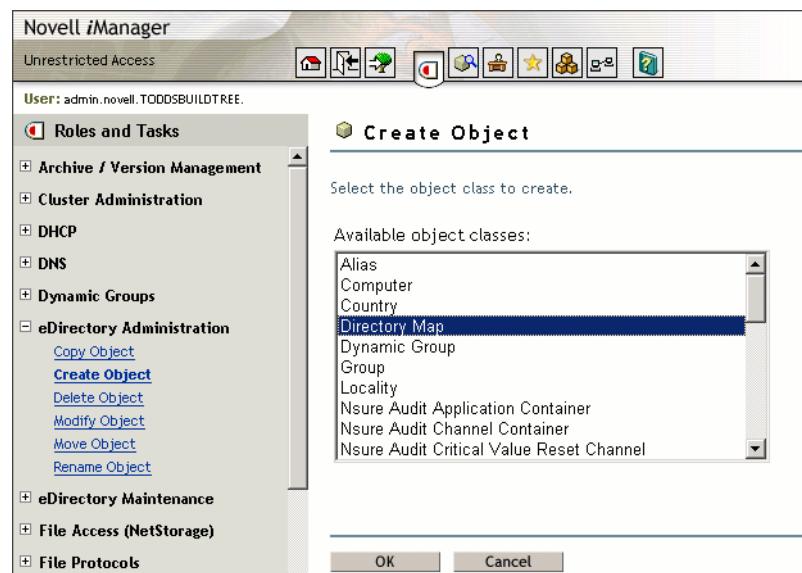
`http://192.168.1.1/nps/iManager`

Replace `192.168.1.1` with the actual IP address or DNS name of your server.

The NetWare server must contain a NetWare NSS or Traditional volume.

To provide access from your tree to NetWare file systems in other trees, you can create NetWare Server and Volume objects in your tree that point to the NetWare servers and volumes in the other trees. The NetWare Server objects must be created before the Volume or Directory Map objects.

- 2 In Roles and Tasks, click eDirectory Administration > Create Object to open the Create Object page.



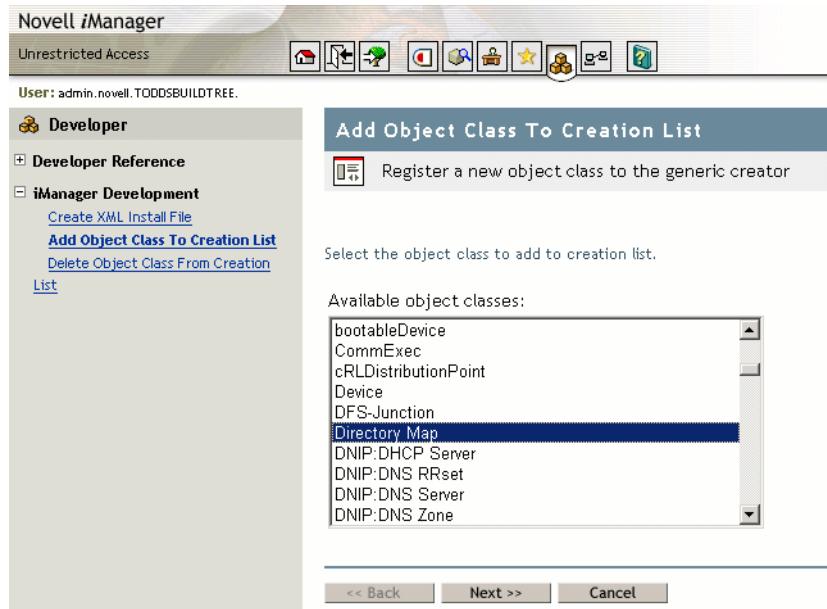
- 3 (Conditional) If Directory Map is not one of the Available Object Classes, you must add the Directory Map object class to the list.

When you select the Create Object task, it presents a list of available object classes. By default, the Create Object task lists only the most commonly-used object classes in the list. You can add additional object classes to the list, which enables you to create corresponding objects using the Create Object option.

IMPORTANT: Role-Based Services must be configured before you can use the iManager Development role. For information, see “[Setting Up Role-Based Services](http://www.novell.com/documentation/imanager20/imanager20/data/bob1yft.html#bob1yft)” (<http://www.novell.com/documentation/imanager20/imanager20/data/bob1yft.html#bob1yft>) in the *Novell iManager 2.5 Administration Guide*.

- 3a In iManager, click the Developer icon 

- 3b Click iManager Development > Add Object Class To Creation List.



3c Select Directory Map from the Available Object Classes list, then click Next.

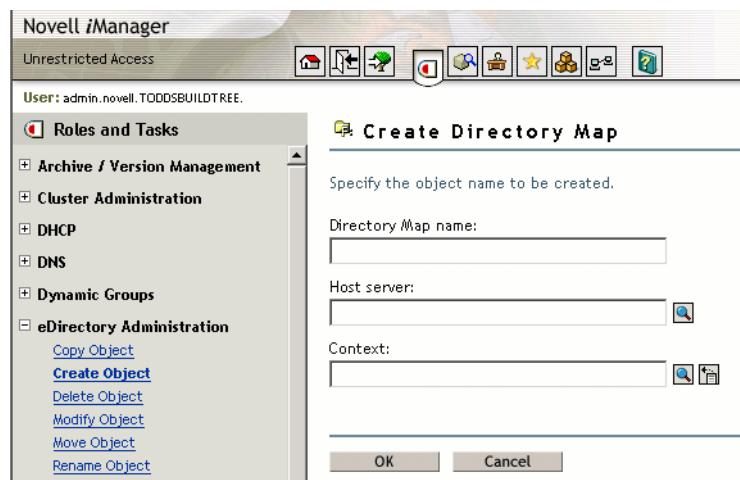
3d At the summary page, verify that the value of the <class-name> entry is com.novell.emframe/fw.GenericCreator, click Finish, then click OK.

3e Return to the Create Object task by clicking the Roles and Tasks icon , then clicking eDirectory Administration > Create Object.

3f Verify that the object classes you added are in the list of available object classes.

In case of errors during this process, the Web server might need to be restarted in order for the newly added object type to be available in the Create Object task.

4 In the Available Object Classes list, select Directory Map, then click OK.

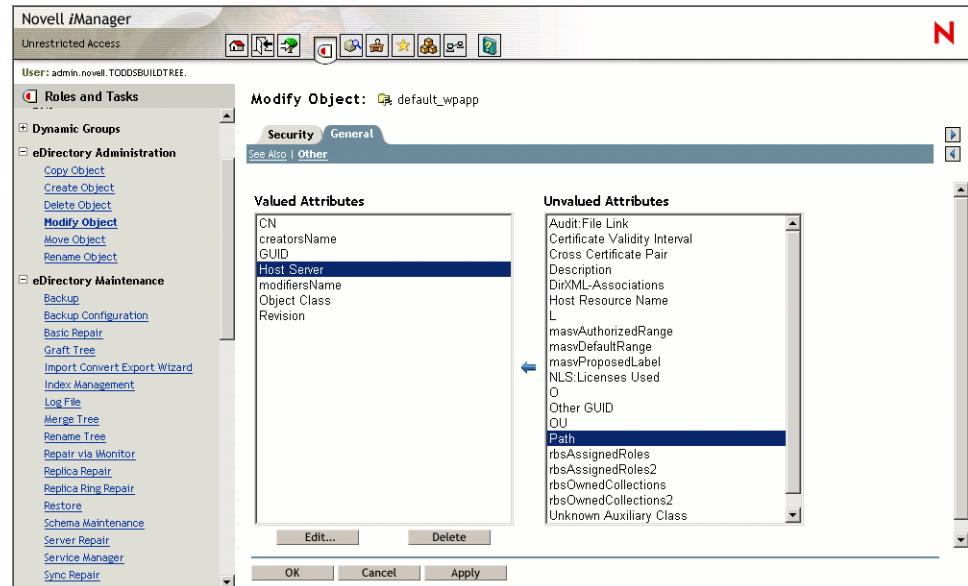


5 Specify the following information for the Directory Map object, then click OK.

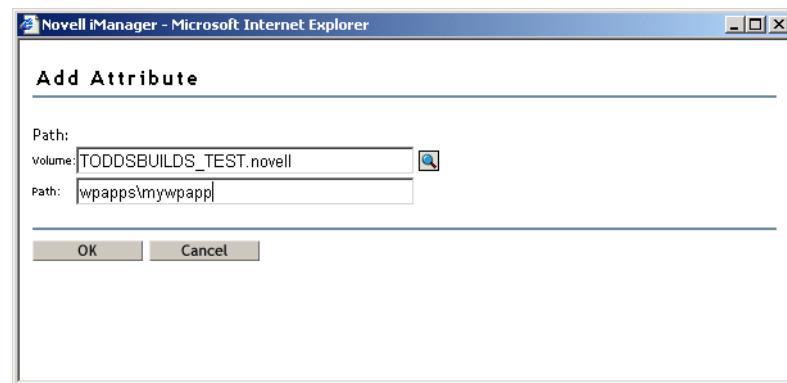
- ◆ **Directory Map Name:** Type the common name that represents this Directory Map object for use in Map and Map Root commands.
- ◆ **Host Server:** Select the NetWare 6.5 server where the directory resides.

- ◆ **Context:** Select the context of the directory you plan to specify as the path this object represents.

6 Click Modify > General > Other to open the Modify Object Page to the Directory Map's Attributes information.



7 In the Unvalued Attributes list, select Path, then click the left-arrow to add the attribute.



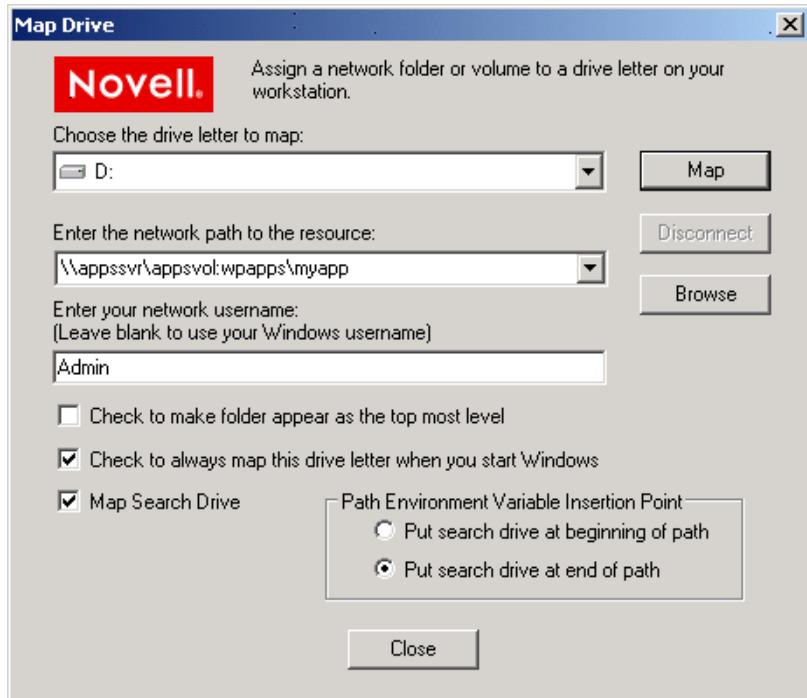
8 Specify the volume and path for the Directory Map object that the object represents, then click OK.

Novell iManager creates the Directory Map object with the specified volume and path, whether or not the specified path actually exists.

9 (Conditional) If the path you specified for the Directory Map object does not exist on the NetWare 6.5 server, create the specified path.

Mapping Network Drives

1 In the taskbar of your workstation, right-click the Novell Client icon, then select Novell Map Network Drive.



2 Specify a drive letter to map.

3 Type or browse to the path to the network resource where you want to map a drive.

4 Specify the login name to use for the map.

If none is provided, the client uses your Windows logon username. If necessary, the client later prompts you for the password that matches the server login username you provide.

5 (Optional) Enable the Check to Make Folder Appear as the Top-Most Level option.

6 (Optional) Enable the Check to Always Map This Drive Letter When You Start Windows option.

7 (Optional) Enable the Map Search Drive option. Specify whether to put the search drive at the beginning or end of the path.

8 Click Map.

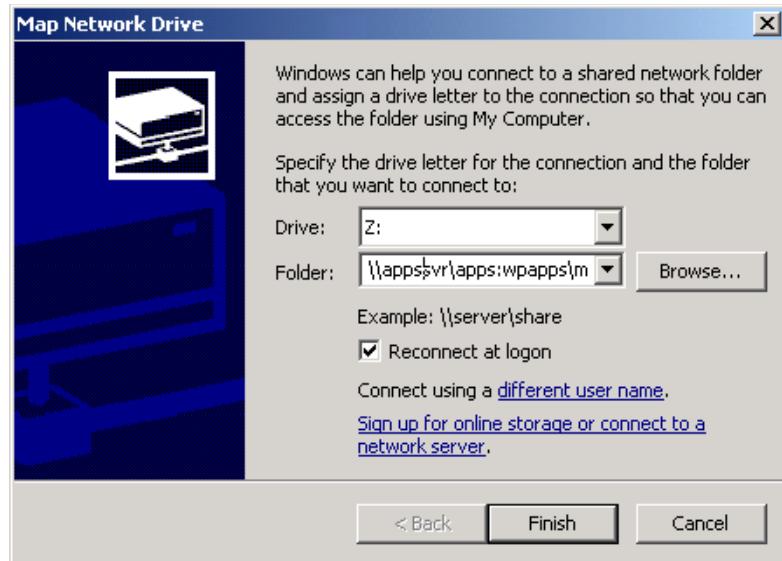
For more information, see “[Common Networking Tasks](#)” in the *Novell Client for Windows Installation and Administration Guide*.

You can also map network drives by placing commands in the Novell Client login scripts. For information, see the *Novell Login Scripts Guide*.

Mapping Network Drives with Windows Explorer

You can also use native methods for mapping drives on your Windows client.

1 In Windows Explorer, click Tools > Map Network Drive.



- 2 Specify a drive letter to map.
- 3 Type or browse to specify the folder you want to map.
- 4 (Optional) To make the map recur for subsequent logins to the network, enable Reconnect at Logon.
- 5 Click Finish.

Mapping Network Drives on DOS Clients with the Map Command

You can also use native methods for mapping drives on your DOS client. Use the Map command to map drives and search drives to network directories. For a general description of the Map command, see “[MAP](#)” in the *NetWare 6.5 Utilities Reference*.

Understanding Access and Usage Control for Directories and Files

Security is one of the most important aspects of file system organization. The NSS File System and the NetWare® Traditional File System use the Novell trustee model to secure access to directories and files. Novell eDirectory objects, file system Trustee rights, and file system attributes for directories and files work together to allow you to determine who can access a directory or file and which actions are possible.

This section discusses the following measures for controlling access to directories and files:

- ◆ “[eDirectory Objects and Security Equivalence](#)” on page 260
- ◆ “[File System Trustee Rights](#)” on page 260
- ◆ “[The Connection Manager for NetWare](#)” on page 264
- ◆ “[Novell Client](#)” on page 265
- ◆ “[Understanding Directory and File Attributes for NSS Volumes or NetWare Traditional Volumes](#)” on page 265

eDirectory Objects and Security Equivalence

Administrators, users, and network resources are represented as objects in an eDirectory database. Use the eDirectory plug-ins to Novell iManager to create eDirectory objects, such as Admin objects, User objects, Group objects, Organizational Role objects, and container objects. For information, see the *Novell eDirectory 8.7.3 Administration Guide*.

Security equivalences help to simplify the task of assigning objects as file system Trustees for your directories and files. You can establish security equivalences explicitly, automatically, or implicitly. A user who is security equivalent to another eDirectory object effectively has all the rights of that object, both in eDirectory and in the NetWare file system. A user is automatically security equivalent to the groups and roles that he or she belongs to. All users are implicitly security equivalent to the [Public] trustee and to each container above their User objects in the eDirectory tree, including the Tree object. You can also explicitly grant a user security equivalence to any eDirectory object.

Security equivalence is recorded in eDirectory as the value for the Security Equal To property of a User object. You can modify an object's Security Equal To property to explicitly assign it the same rights as those assigned to another object. Whenever you assign an object to be a member in a Group object or Organizational Role object, the security equivalence is automatically added to the object's Security Equal To property. Security equivalence for an object is implied by its parent container and by the Public container, which applies to all users.

When you specify that an eDirectory object has security equal to a second object, the rights of the second object are added to the rights of the first object when the system calculates the first object's effective rights. For example, suppose you make a User object named Joe security equivalent to the Admin object. After you create the security equivalence, Joe has the same rights to the tree and file system as Admin.

Security equivalence is effective only for one step; it is not transferred by a subsequent security equivalence. For example, if you make a third user security equivalent to Joe in the example above, that user receives only Joe's original security settings. The third user does not receive Admin rights or any other Security Equal To properties Joe might have.

Whenever a user attempts to access a network resource, eDirectory calculates the user's security equivalence and makes that information available to NetWare. NetWare compares the user's security equivalence information to the Trustee assignments for the path and target directory or file to determine if the user can access the target resource and what action on it is permitted.

For more information about eDirectory objects and rights, see “[eDirectory Rights](#)” in the *Novell eDirectory 8.7.3 Administration Guide*.

File System Trustee Rights

File system Trustee rights determine access and usage for directories and files on NSS volumes and Traditional volumes. A trustee is any eDirectory object, such as a User object, Group object, Organizational Role objects, or container object, that you grant one or more rights for a directory or file. Trustee assignments allow you to assign ownership, set permissions, and monitor user access.

The file system stores each file system Trustee's ID and rights assignment as metadata with its directory or file in the NSS file system. In the NetWare Traditional file system, the file's security and attributes metadata is stored in the Directory Entry Table (DET) of its parent directory. For NSS, the files and directory properties contain this information.

File system Trustee rights granted at the directory level apply to all the files and subdirectories in that directory, unless the rights redefined at the file or subdirectory level override them.

File system Trustee rights assigned to files and subdirectories redefine the rights that users inherit from directory rights.

Eight file system Trustee rights can be granted at either the directory or file level, as described in the table below:

File System Trustee Right	Description
Supervisor	<p>Grants the trustee all rights to the directory or file and any subordinate items.</p> <p>The Supervisor right cannot be blocked with an IRF (Inherited Rights Filter) and cannot be revoked. Users who have this right can also grant other users any rights to the directory or file and can change its Inherited Rights Filter.</p> <p>Default=Off</p>
Create	<p>Grants the trustee the ability to create directories and files and salvage deleted files.</p> <p>Default=Off</p>
Erase	<p>Grants the trustee the ability to delete directories and files.</p> <p>Default=Off</p>
File Scan	<p>Grants the trustee the ability to view directory and file names in the file system structure, including the directory structure from that file to the root directory.</p> <p>Default=On</p>
Modify	<p>Grants the trustee the ability to rename directories and files, and change file attributes. Does not allow the user to modify the contents of the file.</p> <p>Default=Off</p>
Read	<p>Grants the trustee the ability to open and read files, and open, read, and execute applications.</p> <p>Default=On</p>
Write	<p>Grants the trustee the ability to open and modify (write to) an existing file.</p> <p>Default=Off</p>
Access Control	<p>Grants the trustee the ability to add and remove trustees for directories and files and modify their trustee assignments and IRFs.</p> <p>Default=Off</p>

Inherited Rights Masks

In NetWare, trustee rights assignments made at a given directory level flow down to lower levels until they are either changed or masked out. This is referred to as *inheritance*. The mechanism provided for preventing inheritance is called the Inherited Rights Mask (IRM).

IRMs are taken into account when NSS builds what is referred to as the effective Access Control List (ACL) for a file or directory. The effective ACL is a list of all users who have rights to the

directory and includes the rights they have. It is calculated by starting at the root of the volume and working down to the file.

At each level, the IRM is applied to all rights inherited from the parent directory. Only those rights allowed by the mask are inherited by the child object. Rights for the various trustees explicitly assigned to the child are then collected. When a trustee inherits rights from above, the new rights replace the old ones (except the Supervisor right, which cannot be masked or removed by a new assignment to the same trustee).

By the time NSS reaches the target file or directory, it has a list of all trustees and the rights assigned and inherited for the requested file or directory. This list is then compared against the entries in the connection table structure. Every time there is a match in the connection table with an entry in the effective ACL, the rights are added to those that the owner of the connection has to the requested file or directory.

In reality, the rights are not calculated at every directory level. The actual algorithm NSS uses to calculate the rights for a particular file or directory is somewhat complicated because it ties in closely with the way the rights cache is implemented. The algorithm almost never needs to start at the root and work down.

In effect, when the effective rights of a user to an object are finally resolved, you have a list of all users who have rights to the file or directory (the effective ACL) and a list of all users in the connection table. These lists are seldom very large.

The one exception to this is a connection that has Admin-equivalent rights (not to be confused with having the Supervisor right from a trustee assignment). Admin-equivalent users have all rights to files, and they cannot be masked out by an IRM or explicit trustee assignment. The only way to keep an Admin-equivalent user from accessing files is to make a special trustee assignment that bars access to all but system connections. This assignment cannot be set through normal tools.

All rights other than Supervisor can be stripped away with an IRM at any level for nearly any user, except a user that has Supervisor right to the Server object itself (such as Admin and equivalents, which usually have rights resulting from an eDirectory rights inheritance). In this situation, the Admin user can see all files and folders regardless of IRMs because the access is not granted in the file system. Instead, a bit is set in the connection table to indicate that the user is an admin and as such has full access to the server and all volumes thereon.

Visibility Lists

The Visibility list is only used for making parent directories visible for navigation purposes. If a user has rights to a file, the NCP™ (via NCP Server for NetWare or NCP Server for Linux) makes all directories above the file visible to the user. This saves the administrator the task of assigning explicit rights to each directory above where the actual rights are assigned.

Visibility entries are stored in a manner similar to explicitly-assigned trustees. The first four entries are in the actual beast object; the rest are stored in overflow beast objects linked from the directory beast object.

Visibility lists only appear on directories. There is one entry for every trustee assigned anywhere in the subtree below the directory. Therefore, the further toward the root you go, the more GUIDs you see against that directory. At the root, the list has GUIDs for every trustee on the volume.

Each visibility entry has an eDirectory GUID and a count of the number of references to that GUID in the entries for the directory (not the subtree) where the Visibility list is assigned. This includes trustees that are explicitly assigned, as well as trustees in Visibility lists.

A Visibility list entry can be created in one of two ways:

- An immediate subordinate directory or file has a trustee that the parent does not.
- A visibility entry for a subordinate subdirectory is present.

Visibility counts do not consider trustees from directories or contents of directories that are not immediately subordinate to the considered directory.

The Visibility list is not affected by adding, deleting, or modifying IRMs. These operate in a transverse flow to the Visibility list. In other words, IRMs flow down the directory structure, while the Visibility list works up the structure.

For each request, GUID entries in the connection table are compared for the connection requesting against all GUIDs on the directory in question. If a match is found, the directory is made visible to the user in the Visibility list.

Supervisor Trustee Rights

A trustee of a Server object in eDirectory is automatically granted the Supervisor right [S] to the root directory of every NSS or NetWare Traditional volume attached to that server. You cannot override Supervisor rights with Trustee rights applied at the subdirectory or file level, nor with Inherited Rights Filters. The Admin User object is automatically a trustee of the Server object.

The Supervisor user of the NSS or NetWare Traditional volume is automatically a trustee for all directories and files on the system and has all file system Trustee rights for them. The Supervisor right allows its trustee to assign other eDirectory objects as trustees and to specify any of the file system Trustee rights to them.

A trustee must have the Access Control right [A] to make trustee assignments in a directory or file.

Also, a trustee with the Write right to the File Server object is granted the Supervisor right to the file system.

Trustee Assignments for a Volume

If you grant a user privileges at the root directory of a volume, the user gains privileges to the entire volume unless those rights are specifically revoked at a lower level. You should be especially cautious about granting the Access Control right in a root directory. Users with the Access Control right can grant themselves all other rights in any subdirectory on the volume. You can improve network security by granting each user privileges only to the specific directories he or she uses.

Default Trustee Rights

In a trustee assignment for a directory, the default rights are File Scan and Read. Any trustee assignment, whether for a directory or a file, also includes the right to see the path leading from the root to that directory or file.

A new assignment of trustee rights at the file level can revoke rights assigned at the directory level, or it can allow additional rights.

Inherited Trustee Rights

Subdirectories and files can inherit rights from their parent directory. The directory's rights flow down through its structure to subdirectories and files, except for specific subdirectories or files with their own trustee assignments that supersede inherited rights. The trustee can exercise rights on subordinate directories and files without having explicit Trustee assignments on each item.

When granting a trustee assignment to a subdirectory or file, the trustee assignment takes precedence over the inherited rights of its parent directory.

Public Trustee Rights

[Public] is a specialized trustee; it is not an eDirectory object. [Public] represents any network user, logged in or not, for rights assignment purposes. [Public] has Browse rights to the top of the tree, giving all users the right to view any object in the tree.

You can always specify [Public] as the trustee of a file, directory, or object. An unspecified authorized user who tries to access a file, directory, or object without any other rights is allowed the rights granted to the [Public] trustee.

Example of Rights Needed for Typical Access Tasks

The following table lists some common tasks and the rights required to do them.

Task	Trustee Assignment Needed
Read from a closed file	Read
See a filename	File Scan
Search a directory	File Scan
Write to a closed file	Write, Create, Erase, Modify
Create and write to a file	Create
Copy files into a directory	Create
Remove an empty subdirectory	Erase
Delete a file	Erase
Change directory or file attributes	Modify
Rename a file	Modify
Change the Inherited Rights Filter	Access Control
Change trustee assignments	Access Control
Modify a directory's disk space assignment for users	Access Control

The Connection Manager for NetWare

For NetWare, the Connection Manager module (connmgr.nlm) builds a connection table when a user connects to the file system. When a file is requested from either the NSS file system or the NetWare Traditional file system, the Connection Manager gathers information for the connection table from the eDirectory Services module (ds.nlm) in the form of a connection table comprised of the eDirectory EIDs for the object, for group memberships, and for security equivalences.

When the connection is established, the information in the connection table is relatively static unless the connected user is added to a new group or is given an explicit trustee assignment or security equivalence. In those situations, the connection manager updates the connection table and sends out an event that the table has changed. NSS uses this event to update its own connection table.

Connections to the NetWare Traditional File System

For the NetWare Traditional file system, the table of EIDs is all that is needed to proceed with authentication. After eDirectory provides the list of EIDs, the Connection Manager compares the list to the Directory Entry Table (DET) for the Traditional volume. It determines valid trustees by looking at the assigned trustees in the directory structure above (for trustee inheritance) and at the target file system object (for explicit trustee assignments). Inherited Rights Masks (IRMs) are also taken into consideration.

Connections to the NSS File System

For the NSS file system, the NSS connection table establishes an entry for a user when the regular connection table entry is created, rather than at the file system access time. Logically, the NSS connection table is part of the connection table with NSS-specific information, including the eDirectory object's GUID.

NSS uses GUIDs as the key for trustees. It keeps its own connection table with these GUIDs and compares it with the beast object entry to look for valid trustees. It finds valid trustees by looking at assigned trustees in the directory structure above (for trustee inheritance) and at the target file system object (for explicit trustee assignments), also taking IRMs into consideration.

If this fails to provide a method of access, NSS then checks the Visibility list to see if the requested object is a parent directory that requires visibility due to a rights assignment for a child directory. For information about the Visibility list, see [“Visibility Lists” on page 262](#).

When GUIDs are used instead of EIDs, it does not matter which server you are on, provided it is in the same tree, which is why Novell Cluster Services uses NSS pools and volumes.

NSS does not directly access the connection table. However, it does make calls to read information from it to form its own connection table with GUIDs and file system Trustee rights. For information about Trustee rights, see [“File System Trustee Rights” on page 260](#).

Novell Client

The Novell Client™ establishes an authenticated connection to the server through eDirectory. It does not perform periodic authentication checks, nor does it track rights. NCP Server and NSS work together to ensure that the Security Equivalence Vector is up-to-date, and that the entries in it are used to give correct access to the file system. The client does not control the rights process. To do so would introduce a security flaw into the client/server relationship in NetWare.

Understanding Directory and File Attributes for NSS Volumes or NetWare Traditional Volumes

Directory and file attributes assign properties to individual directories or files. Some attributes are meaningful only when applied at the file level, but some apply to both the directory and the file levels.

File attributes apply universally to all users. For example, a file that has a read-only attribute is read-only for all users. The file attribute settings are like an on/off switch. Attributes can be set by any trustee with the Modify right to the directory or file, and attributes stay set until they are changed. Attributes do not change when you log out or when you down a file server.

IMPORTANT: Be careful when assigning a directory and file attribute. The attribute applies to all users.

For example, if a trustee with the Modify right enables the Delete Inhibit attribute for a file, no one, including the owner of the file or the network administrator, can delete the file. However, any trustee with the Modify right can disable the Delete Inhibit attribute to allow the file's deletion.

The table below describes directory and file attributes and whether they are apply to directories, files, or both.

Attribute Code	Description	Applies to
A	Archive Needed identifies files that have been modified since the last backup. This attribute is assigned automatically.	Files only
Ci	Copy Inhibit prevents users from copying a file. This attribute overrides the trustee Read right and File Scan right.	Files only
Dc	Do Not Compress keeps data from being compressed. This attribute overrides settings for automatic compression of files not accessed within a specified number of days.	Directories and files
Di	Delete Inhibit prevents users from deleting a directory or file. This attribute overrides the trustee Erase right. When it is enabled, no one, including the owner and network administrator, can delete the directory or file. A trustee with the Modify right must disable this right to allow the directory or file to be deleted.	Directories and files
Dm	Do Not Migrate prevents directories and files from being migrated from the server's server disk to another storage medium.	Directories and files
Ds	Do Not Suballocate prevents data from being suballocated.	Files only
H	The Hidden attribute hides directories and files so they do not appear in a file manager or directory listing.	Directories and files
I	Index allows large files to be accessed quickly by indexing files with more than 64 File Allocation Table (FAT) entries. This attribute is set automatically.	Files only
Ic	Immediate Compress sets data to be compressed as soon as a file is closed. If applied to a directory, every file in the directory is compressed as each file is closed.	Directories and files
N	Normal indicates the Read/Write attribute is assigned and the Shareable attribute is not. This is the default attribute assignment for all new files.	Directories and files
P	Purge flags a directory or file to be erased from the system as soon as it is deleted. Purged directories and files cannot be recovered.	Directories and files
Ri	Rename Inhibit prevents the directory or file name from being modified.	Directories and files
Ro	Read Only prevents a file from being modified. This attribute automatically sets Delete Inhibit and Rename Inhibit.	Files only
Rw	Read/Write allows you to write to a file. All files are created with this attribute.	Files only
Sh	Shareable allows more than one user to access the file at the same time. This attribute is usually used with Read Only.	Files only
Sy	The System attribute hides the directory or file so it does not appear in a file manager or directory listing. System is normally used with operating system files, such as DOS system files.	Directories and files
T	Transactional allows a file to be tracked and protected by the Transaction Tracking System™ (TTS™).	Files only

Attribute Code	Description	Applies to
X	The Execute attribute indicates program files such as .exe or .com.	Files only

Configuring File System Trustees, Trustee Rights, Inherited Rights Filters, and Attributes for Directories and Files

This section discusses how to configure trustee rights, inherited rights filters, and access attributes. For an explanation of rights and attributes and considerations about controlling access to your file system, see “[Understanding Access and Usage Control for Directories and Files](#)” on page 259.

- ◆ “[Tools for Managing File System Trustees and Attributes](#)” on page 267
- ◆ “[Generating a Server Security Report](#)” on page 268
- ◆ “[Viewing a File System Trustee Report for a Volume](#)” on page 269
- ◆ “[Managing File System Trustees, Trustee Rights, and Inherited Rights Filters](#)” on page 269
- ◆ “[Managing Attributes for Directories and Files](#)” on page 274
- ◆ “[Trustee Rights Utility for Linux](#)” on page 277
- ◆ “[Trustee Rights Utility for NetWare](#)” on page 280
- ◆ “[Attributes Utility for Linux](#)” on page 282
- ◆ “[FLAG](#)” on page 284

Tools for Managing File System Trustees and Attributes

- ◆ “[Accessing Novell NetStorage](#)” on page 267
- ◆ “[Accessing the Novell Client for Windows 2000/XP](#)” on page 268
- ◆ “[Accessing Novell Remote Manager for NetWare](#)” on page 268

Accessing Novell NetStorage

To access NetStorage, launch your Web browser and open it to the following location:

`http://192.168.1.1/oneNet/NetStorage`

Replace `192.168.1.1` with the actual DNS name or IP address of your NetStorage server or the IP address for Apache-based services. If Apache-based services use a port other than 80, you must also specify that port number with the URL. For example, if the port number is 51080, the URL would be in the form

`http://192.168.1.1:51080/oneNet/NetStorage`

The date and time on the workstation being used to access NetStorage should be reasonably close (within a few hours) to the date and time on the server running NetStorage to avoid conflicts.

NetStorage uses Novell eDirectory™ for authentication. Log in with your administrator username and password to manage file system access for directories and files on NSS volumes. You can also log in as any username with equivalent rights to the administrator. This limitation does not apply if you have created a Storage Location object using SSH (Secure Shell).

NOTE: Viewing or changing directory and file attributes and rights using NetStorage is only possible using a browser. This functionality is not available using Microsoft Web Folders.

Accessing the Novell Client for Windows 2000/XP

In combination with NCP Server on your OES Linux or NetWare server, the Novell Client™ for Windows 2000/XP supports the following:

- ◆ Management of file system trustees, trustee rights, and inherited rights filters for directories and files on NSS volumes
- ◆ Purge and salvage of deleted files on NSS volumes, if the volume is configured to support it
- ◆ Drive mapping for NSS volumes
- ◆ Login scripts for automatic drive mapping on login

For information, see the *Novell Client for Windows Installation and Administration Guide*.

Accessing Novell Remote Manager for NetWare

- 1 In your Web browser, log in as administrator to Novell Remote Manager on the NetWare server where you want to create a directory. The general form of the URL is

`http://192.168.1.1:8008`

Replace `192.168.1.1` with the actual IP address or DNS name of your server.

- 2 Click Manage Server > Volumes.

- 3 Click the Properties icon  next to the Volume you want to manage.

Generating a Server Security Report

You can generate the server Security report in Novell Remote Manager to help track potential security risks. This report shows only the information that the logged-in user is allowed to view. To receive a report with the most helpful information, log in as the Admin user or as a user with eDirectory rights equivalent to Admin.

To generate the Security report for your NetWare server:

- 1 Open a Web browser to the Novell Remote Manager, then log in as administrator or equivalent.
- 2 In the left navigator, click Reports/Log Files to open the Reports/Log Files page.
- 3 Click View Security Report.

From this report, you can track the following file system security information:

- ◆ Trustee assignments for each volume

Granting a user privileges at the root directory of a volume gives that user privileges to the entire volume unless those rights are specifically revoked at a lower level. You should be especially cautious about granting the Access Control right in a root directory. Users with the Access Control right can grant themselves all other rights in any subdirectory on the volume. You can improve network security by granting each user privileges only to the specific directories he or she uses.

- ◆ Trustee assignments for each common folder on the sys: volume

User, organization, role, or other eDirectory objects should have only limited access, such as Read and File Scan rights, to common directories on volume sys: such as sys:public and sys:\login.

- ◆ A list of users that have security equivalence to user Admin

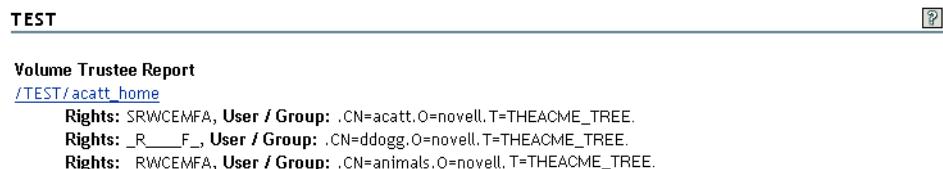
As the number of users with rights equivalent to user Admin increases, your security risks multiply. Any time a user with rights equivalent to user Admin leaves a server unattended, anyone can gain access to the server.

For information, see “[Security Report](#)” in the *NetWare 6.5 Novell Remote Manager Administration Guide for NetWare*.

Viewing a File System Trustee Report for a Volume

For NetWare, administrators can view a Volume Trustee Report to see which users are trustees of which files and directories on a volume.

- 1 In Novell Remote Manager for NetWare, click Manage Server > Volumes to open the Volume Management page.
- 2 Click the Info icon next to volume you are monitoring.
- 3 Scroll down the page, then click the Volume Trustee Report link.



TEST

Volume Trustee Report
[/TEST/acatt_home](#)

Rights: SRWCEMFA, User / Group: .CN=acatt.O=novell.T=THEACME_TREE.
Rights: _R____F_, User / Group: .CN=ddogg.O=novell.T=THEACME_TREE.
Rights: _RWCEMFA, User / Group: .CN=animals.O=novell.T=THEACME_TREE.

Managing File System Trustees, Trustee Rights, and Inherited Rights Filters

Use the following methods to modify file system trustees for directories and files on NSS or NetWare Traditional file systems.

- ◆ “[Using Novell NetStorage](#)” on page 269
- ◆ “[Using the Novell Client to Manage Trustees and Trustee Rights](#)” on page 270
- ◆ “[Using the Novell Client to Manage Inherited Rights and Filters](#)” on page 271
- ◆ “[Using Novell Remote Manager for NetWare](#)” on page 273

Using Novell NetStorage

- 1 Open your Web browser to NetStorage and log in.

For information, see “[Accessing Novell NetStorage](#)” on page 267.

- 2 Right-click the directory or file you want to manage, then select Properties.
- 3 Click the NetWare Info tab to view or modify attributes or the NetWare Rights tab to view or modify rights.

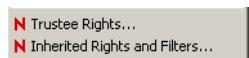
Although the option label refers to NetWare, use the option for your NSS volumes on Linux or NetWare.

For information, see “[File System Trustee Rights](#)” on page 260.

Using the Novell Client to Manage Trustees and Trustee Rights

Administrators and users can manage file system Trustee rights for network directories and files, using the Novell Client on their workstations.

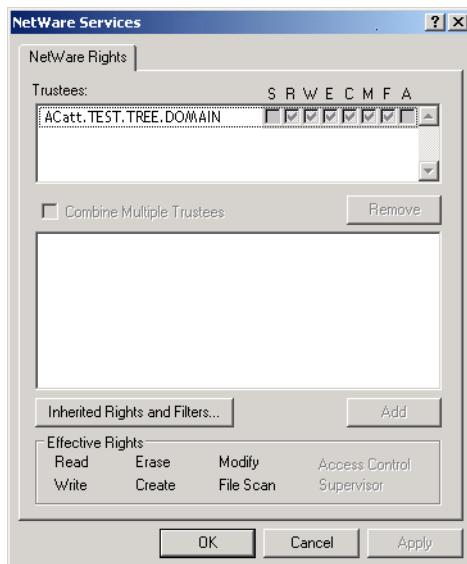
- 1 In a file manager, right-click the network directory or file, then select Trustee Rights.



- 2 In the Trustees area, click the username to display the user's trustee rights.

Each trustee's rights are shown by a check mark under the letters of the associated rights. If there are no trustees listed, access for the selected directory or file is currently governed only by its Inherited Rights and Filters.

If you are viewing the properties of multiple directories or files, the trustees and rights shown are the combined trustees and rights for all the files.



- 3 In the Effective Rights area, view the actual rights of the selected user.

Explicit file system Trustee rights override inherited rights. If there are no trustees listed, the effective rights are the same as the inherited rights.

- 4 (Conditional) If you have the Supervisor right or the Access Control right for the selected network directory or file, you can configure trustee rights.

Do one or more of the following:

- ◆ **Add a Trustee:** Click Add, type the fully distinguished name (*username.context.tree.domain*) of the user you want to add, then click OK.
- ◆ **Modify Trustee Rights:** Select one or more trustees, select or deselect the check box for each trustee right you want to modify, then click Apply.
- ◆ **Delete a Trustee:** Select one or more trustees, then click Remove.
- ◆ **Combine Multiple Trustees:** This option is available only when viewing the file system Trustee Rights for multiple directories or files. Additionally, at least one of the selected directories or files must have at least one trustee assignment.

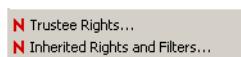
Select one or more trustees from the Trustees list, select Combine Multiple Trustees, then click Apply. The trustees' rights are combined and applied to all selected directories and files. All selected trustees become trustees of all selected directories and files.

5 Click OK.

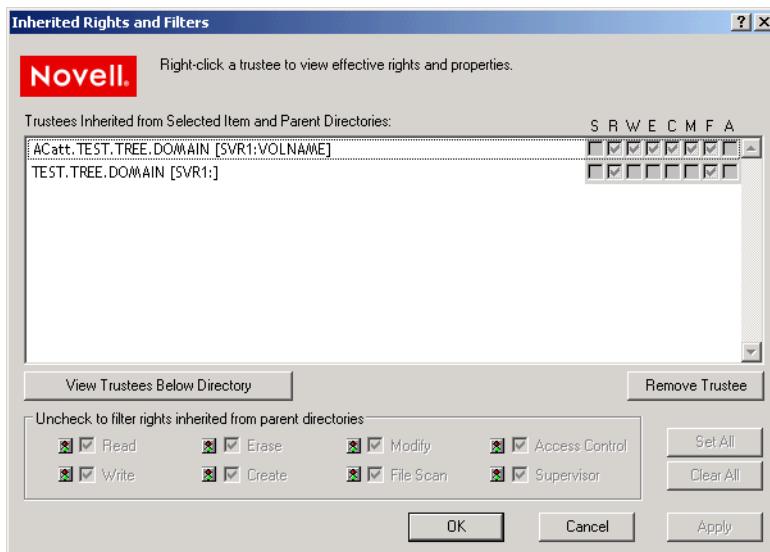
Using the Novell Client to Manage Inherited Rights and Filters

Administrators and users can manage file system inherited rights and filters for network directories and files, using the Novell Client on their workstations. For information about filtering inherited rights, see “[Inherited Trustee Rights](#)” on page 263.

- 1 Use one of the following methods to access the Inherited Rights and Filters dialog box:
 - ♦ In a file manager, right-click the network directory or file, then select Inherited Rights and Filters.



- ♦ In the file system Trustee Rights window, click Inherited Rights and Filters.



- 2 (Conditional) If you have the Supervisor right or the Access Control right for the selected network directory or file, you can configure its inherited rights. Do one or more of the following:

- ♦ **Modify Trustee Rights:** Select the trustee you want to manage from the Trustees Inherited from Selected Item and Parent Directories. Select or deselect the check box of the file system Trustee right you want to modify, then click Apply.

Changing the Inherited Rights and Filters does not grant rights; it removes rights previously assigned at a higher level in the path. Deselect the right to filter the right for a specific trustee or for all trustees of the selected directory or file.

- ♦ **Delete a Trustee:** Select the trustee you want to manage from the Trustees Inherited from Selected Item and Parent Directories, then click Remove Trustee.

- 3 (Conditional) If you selected a directory, click View Trustees Below Directory to view a list of trustees for files or directories in the selected directory.
- 4 When you are done, click OK.

Using Novell Remote Manager for NetWare

Administrators can also use Novell Remote Manager for NetWare to perform these tasks on NetWare.

- 1 In Novell Remote Manager, click Manage Server > Volumes to open the Volume Management page.
- 2 Click the Volume link of the volume you want to manage.
- 3 Browse to the directory or file you want to manage.
- 4 Click the Properties icon to the left of the directory or file you want to manage.

The screenshot shows the Novell Remote Manager interface for managing a directory. The URL in the address bar is `/TEST/acatt_home`. The main content area displays 'Directory entry information' with the following details:

Owner	ACATT
Creation date and time	Jun 30, 2004 12:51 pm
Effective rights	SRWCEMFA
Inherited rights filter	SRWCE_F
File space limit	None
File space in use	Not available

Below this, the 'Trustee information:' section lists three users with their rights and delete options:

Object name	Trustee rights	Delete
.CN=acatt.O=novell.T=TODDSBUILDTREE.	SRWCEMFA	Delete
.CN=ddogg.O=novell.T=TODDSBUILDTREE.	R_F	Delete
.CN=animals.O=novell.T=TODDSBUILDTREE.	RWCEMFA	Delete

At the bottom, there are buttons for 'Add Trustee' (disabled), 'User Name:' (input field), 'Browse' (button), and 'Delete Directory and Contents' (button). Below these are buttons for 'Rename Directory' (disabled), 'New name: /acatt_home' (input field), 'Create Subdirectory' (disabled), and 'New name:' (input field).

- 5 Do one or more of the following:
 - ◆ **Add a Trustee:** Type the full distinguished name or bindery name of the User object you want to add in the User Name field of the Trustee Information, or browse to the User object and select it, then click Add Trustee.
 - ◆ **Modify Trustee Rights:** Locate the User object name in the list of User objects under the Trustee Information, then click the Trustee Rights link next to the username. Select or deselect the check box for the trustee right you want to change, then click OK.
 - ◆ **Delete a Trustee:** Locate the User object name in the list of User objects under the Trustee Information, then click the Delete link next to the username.

- ◆ **Modify the Inherited Rights Filter:** Click the Inherited Rights Filter link in the directory or file information table. Select or deselect the check box for the rights you want to modify, then click OK.

Changing the Inherited Rights Filter does not grant rights; it only removes rights previously assigned at a higher level in the tree.

Managing Attributes for Directories and Files

Administrators can configure NetWare directory and file attributes using the following methods:

- ◆ “Using Novell NetStorage” on page 274
- ◆ “Using the Novell Client” on page 274
- ◆ “Using Novell Remote Manager” on page 275
- ◆ “Using the NetWare GUI” on page 276

For information about NetWare directory and file attributes and how to apply them, see “[Understanding Directory and File Attributes for NSS Volumes or NetWare Traditional Volumes](#)” on page 265.

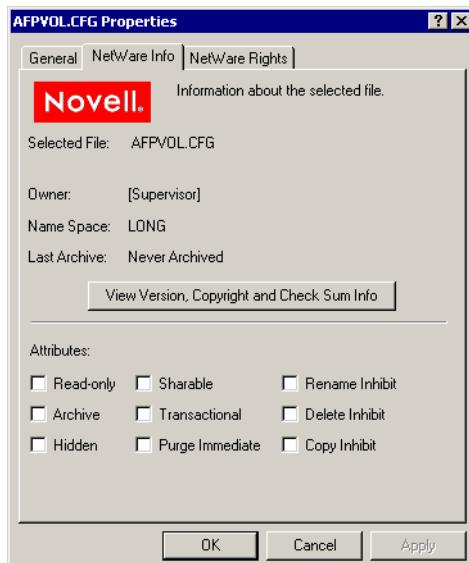
Using Novell NetStorage

- 1 Open your Web browser to NetStorage and log in.
For information, see “[Accessing Novell NetStorage](#)” on page 267.
- 2 Right-click the directory or file you want to manage, then select Properties.
- 3 Click the NetWare Info tab to view or modify attributes for the selected directory or file.
Although the option label refers to NetWare, use the option for your Linux and NetWare NSS volumes.
For information, see “[Understanding Directory and File Attributes for NSS Volumes or NetWare Traditional Volumes](#)” on page 265

Using the Novell Client

Administrators and users with trustee rights can specify some file system attributes for directories and files, using the Novell® Client™ on their workstations.

- 1 In a file manager, right-click the network directory or file, select Properties, then click NetWare Info.



2 In the Attributes area, select the attribute to enable it, then click Apply.

The attribute change is applied only if all the following conditions are met:

- ◆ The user has the correct trustee rights necessary to modify the selected attribute.
- ◆ The attribute must be a viable attribute for the underlying file system where the file resides. For example, some attributes apply only to NetWare Traditional volumes.
- ◆ The attribute must be enforceable by NCP or NSS in the current network configuration.

3 Click OK.

Using Novell Remote Manager

- 1 In Novell Remote Manager for NetWare, click Manage Server > Volumes to open the Volume Management page.
- 2 Click the Volume link of the volume you want to manage.
- 3 Browse to the directory or file you want to manage.
- 4 View the resource's attributes in the Attributes column.

NetWare File Listing					
Info	Name	Type	Size	Date and time	Attributes
•	acatt_home		N/A	Jun 30, 2004 12:05 pm	---A-----
Icon	Icon		0	Jun 30, 2004 12:03 pm	---A-Rw-----
VOLDATA.TDF	VOLDATA.TDF		1,784	Jul 9, 2004 3:00 pm	---A-Rw-----
Volume_Inventory.xml	Volume_Inventory.xml		4,756	Jun 30, 2004 1:10 pm	---A-Rw-----
Volume_Trustees.xml	Volume_Trustees.xml		374	Jun 30, 2004 1:10 pm	---A-Rw-----

4 Files.
6 KBytes in use.
180 MBytes available.

5 To modify the attributes, click the Attributes link.

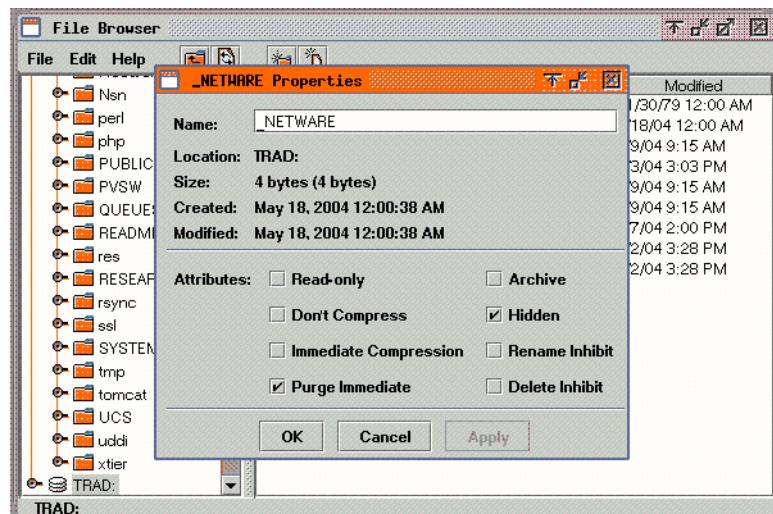
/TEST/acatt_home

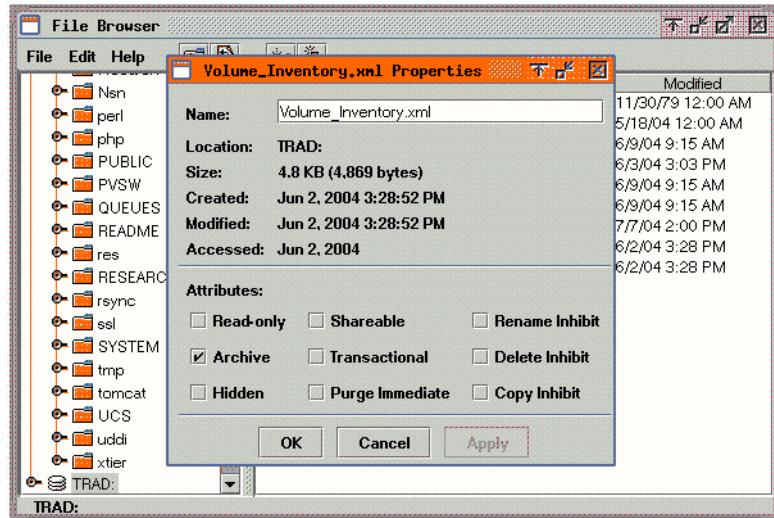
Folder Attributes	Description
<input type="checkbox"/> System	If checked, this indicates a system file or folder.
<input type="checkbox"/> Hidden	If checked, this indicates that this file or folder is excluded from normal directory searches.
<input checked="" type="checkbox"/> Archive	If checked, this indicates that the file or folder needs to be archived.
<input type="checkbox"/> Immediate Purge	If checked, this indicates that when this file or folder or the folder contents are deleted and are unrecoverable.
<input type="checkbox"/> Don't Compress	If checked, this indicates that this file or the contents of the folder cannot be compressed..
<input type="checkbox"/> Don't Migrate	If checked, this indicates that this file or folder cannot be migrated to near line storage..
<input type="checkbox"/> Delete Inhibit	If checked, this indicates that this file or folder cannot be deleted.
<input type="checkbox"/> Rename Inhibit	If checked, this indicates that this file or folder name cannot be renamed.
<input type="checkbox"/> Immediate Compress	If checked, this indicates that this file or the folder contents will be scheduled for compression..
<input type="button" value="OK"/> <input type="button" value="Reset"/>	

6 Select or deselect the check box for the attribute you want to set.
 7 Click OK.

Using the NetWare GUI

- 1 In your NetWare GUI console, browse to the directory or file you want to view or change the attributes of.
- 2 Right-click the directory or file to open its Properties page.





- 3 View the attributes in the Attribute area.
- 4 Select or deselect the check box for the attribute you want to set.
- 5 Click OK.

Trustee Rights Utility for Linux

The Trustee Rights Utility for Linux allows you to specify Trustee rights for directories and files in NSS volumes on OES Linux. This utility does not provide support for Trustees on Linux file systems. It is also not meant to be used to set trustees for NSS volumes on OES NetWare. The trustee information is saved in the file and directory metadata in the NSS volume and works seamlessly with OES NetWare if the volume is moved to OES NetWare.

Purpose

Use this utility at a workstation to

- ◆ View or modify user or group rights for files
- ◆ View or modify user or group rights for directories and volumes

Syntax

```
rights [OPTIONS]
rights [TOPTIONS] trustee USERNAME
rights [DOPTIONS] delete USERNAME
rights [IOPTIONS] irf
rights [EROPTIONS] effective USERNAME
rights [SOPTIONS] show
```

Actions

The first argument indicates the action to be taken.

trustee	Add or modify a trustee on a file or directory.
delete	Remove a trustee from a file or directory.

irf	Set the inherited rights filter on a directory.
effective	Display a user's effective rights.
show	Display the trustees and inherited rights filter.

Options

OPTIONS

-v, --version	Display the program version information.
-h, --help	Display the help screen.

OPTIONS

-r, --rights=MASK	Specify the rights to be given to this trustee. For information, see MASK. If the No Rights (n) option is assigned, the trustee is removed. If rights are not specified, the default assignment is Read and File Scan rights.
-f, --file=filename	Specify the name of file or directory to assign trustees to. Filename is the path for the file or directory. For example: -f /users/username/userfile.sxi --file=/designs/topsecret If a file or directory is not specified, the current directory is used.

OPTIONS

-f, --file=filename	The name of file or directory to delete trustees from. Filename is the path for the file or directory. If a file or directory is not specified, the current directory is used.
---------------------	---

OPTIONS

-r, --rights=MASK	Specify the rights to be passed through the filter. For information, see MASK. If rights are not specified, the default assignment is All Rights.
-f, --file=filename	Specify the name of the directory where the filter is to be applied. Filename is the path for the directory. If a directory is not specified, the current directory is used.

EROPTIONS

-f, --file=filename	The name of file or directory where effective right are to be calculated. Filename is the path for the file or directory. If a file or directory is not specified, the current directory is used.
---------------------	--

OPTIONS

-f, --file=filename Specify the name of the file or directory to display a list of its trustees.
 If a file or directory is not specified, the current directory is used.

USERNAME

The username is the fully distinguished name of an eDirectory object, including the tree name. For example: `username.context.treename` or `joe.engineer.acme_tree`.

MASK

The mask is a string of characters, with each character representing a type of rights. The following table lists the rights, the letter to use for each right, and what the right is used for.

Right	Use to
s (Supervisor)	Grant all rights to the file or directory.
r (Read)	Open and read files in the directory.
w (Write)	Open and write to files in the directory.
c (Create)	Create files and subdirectories.
e (Erase)	Erase files and directories.
m (Modify)	Rename files and directories, and change file attributes.
f (File Scan)	View and search on file and directory names in the file system structure.
a (Access Control)	Add and remove trustees and change trustee rights to files and directories.
n (No Rights)	Remove all rights.
a (All Rights)	Add All rights except Supervisor.

Example

```
rights -f /designs/topsecret -r rwfc trustee joe.engineer.acme_tree
```

This command assigns Read, Write, File Scan, and Create rights to the `/designs/topsecret` directory for user `joe` in the `engineer` context of the `acme_tree` eDirectory tree.

Trustee Rights Utility for NetWare

The Trustee Rights Utility for NetWare allows you to specify Trustee rights for directories and files in NSS volumes on OES NetWare.

Purpose

Use this utility icononat a workstation to

- ◆ View or modify user or group rights for files
- ◆ View or modify user or group rights for directories and volumes

Syntax

```
RIGHTS path [[ + | - ] rights] [/option...] [/? | /VER]
```

Parameter	Use to
<i>path</i>	Specify the path to the file, directory, or volume you want to modify or view rights to (you must always specify a path).
+ -	Add or delete the specified rights. See "Using RIGHTS" on page 281.
<i>rights</i>	Specify one or more file or directory rights. See "File and Directory Rights" on page 281.
/option	Replace <i>option</i> with any available option. See "RIGHTS Options" on page 280.
/?	View online help. All other parameters are ignored when /? is used.
/VER	View the version number of the utility and the list of files it uses to execute. All other parameters are ignored when /VER is used.

RIGHTS Options

Option	Use to
/C	Scroll continuously through output.
/F	View the Inherited Rights Filter (IRF).
/I	View the trustee and group rights that created the inherited rights, and view where the inherited rights came from.
/NAME= <i>username</i>	View or modify rights for the user or group listed. Replace <i>username</i> with the name of the user or group whose rights you want to view or modify.
/S	View or modify subdirectories below the current level.
/T	View trustee assignments in a directory.

File and Directory Rights

The following table lists the rights, the letter to use for each right, and what the right is used for.

Right	Use to
S (Supervisor)	Grant all rights to the file or directory.
R (Read)	Open and read files in the directory.
W (Write)	Open and write to files in the directory.
C (Create)	Create files and subdirectories.
E (Erase)	Erase files and directories.
M (Modify)	Rename files and directories, and change file attributes.

Right	Use to
F (File Scan)	View and search on file and directory names in the file system structure.
A (Access Control)	Add and remove trustees and change trustee rights to files and directories.
N (No Rights)	Remove all rights.
REM (Remove)	Remove the user or group as a trustee of the specified file or directory.
ALL	Add All rights except Supervisor.

Using RIGHTS

- ◆ If you use + (plus) to add rights, the rights you list are added to the existing rights.
- ◆ If you use - (minus) to remove rights, the rights you list are deleted from the existing rights.
- ◆ If you add and delete rights in the same command, group all added rights together and all deleted rights together.
- ◆ If you list rights without using + or -, the rights you list replace the existing rights.
- ◆ You must always specify a path. You can use a period (.) to represent your current directory.
- ◆ You can use wildcard characters.

Examples

- ◆ To set the trustee rights in the current directory for user JANICE to Read, Write, and File Scan, type

```
RIGHTS . R W F /NAME=JANICE
```

- ◆ To remove user ERNESTO from ALICE/SYS:USERS, type

```
RIGHTS ALICE/SYS:USERS REM /NAME=ERNESTO
```

- ◆ To see where user PATRICK's inherited rights came from for SYS:USERS/HOME, type

```
RIGHTS SYS:USERS/HOME /NAME=PATRICK /I
```

Attributes Utility for Linux

The Attributes (ATTRIB) Utility for Linux allows you to specify file system attributes for directories and files in NSS volumes on OES Linux.

IMPORTANT: This utility works only with directories and files in the NSS file system on Linux.

Purpose

Use at a workstation to

- ◆ View or modify file system attributes for files
- ◆ View or modify file system attributes for directories

Syntax

```
attrib [OPTIONS] [filename]
```

If both the set and clear options are selected, the clear option is done before the set option. If the filename is not specified, the operation is done on the current directory.

Options

OPTIONS

Option	Description
<code>-s, --set=ATTRIBUTES</code>	Sets the attributes on the file
<code>-c, --clear=[ATTRIBUTES all]</code>	Clears the attributes on the file
<code>-l, --long</code>	Displays a long version of the file's attributes
<code>-q, --quiet</code>	Does not display any normal output
<code>-v, --version</code>	Displays the program version information
<code>-h, --help</code>	Displays the ATTRIB help screen

ATTRIBUTES

Multiple attributes are comma separated.

Code	Description	Applies to Files	Applies to Directories
aa	Attribute Archive identifies that a file's metadata has been modified since the last backup. This attribute is assigned automatically.	Yes	No
all	All (used only for the Clear option) represents all attributes that can be modified.	Yes	Yes
ar	Archive identifies files that have modified content since the last backup. This attribute is assigned automatically.	Yes	No
cc	Cannot compress (status display only) displays if the file cannot be compressed because of limited space savings.	Yes	No
ci	Copy Inhibit prevents users from copying a file. This attribute overrides the trustee Read right and File Scan right.	Yes	No
cm	Compressed (status display only) displays whether the file is currently stored in compressed format.	Yes	No
dc	Do Not Compress keeps data from being compressed. This attribute overrides settings for automatic compression of files not accessed within a specified number of days.	Yes	No
di	Delete Inhibit prevents users from deleting a directory or file. This attribute overrides the trustee Erase right. When it is enabled, no one, including the owner and network administrator, can delete the directory or file. A trustee with the Modify right must disable this right to allow the directory or file to be deleted.	Yes	Yes
ex	Execute indicates program files such as .exe or .com.	Yes	No

Code	Description	Applies to Files	Applies to Directories
hi	Hidden hides directories and files so they do not appear in a file manager or directory listing.	Yes	Yes
ic	Immediate Compress sets data to be compressed as soon as a file is closed. If applied to a directory, every file in the directory is compressed as each file is closed.	Yes	Yes
	The files in the specified directory are compressed as soon as the operating system can perform the operation after the file is closed. This does not apply to the directory's subdirectories and the files in them.		
ip	Immediate Purge flags a directory or file to be erased from the system as soon as it is deleted. Purged directories and files cannot be recovered.	Yes	Yes
ln	Link (status display only) indicates a symbolic link (soft link).	Yes	No
mg	Migrated (status display only) displays if the file or directory is migrated to near-lin media.	Yes	Yes
mi	Migrate Inhibit prevents directories and files from being migrated from the server's disk to a near-line storage medium.	Yes	Yes
ri	Rename Inhibit prevents the directory or file name from being modified.	Yes	Yes
ro	Read Only prevents a file from being modified. This attribute automatically sets Delete Inhibit and Rename Inhibit.	Yes	No
sd	Subdirectory (status display only) indicates that the entry is a directory, not a file.	No	Yes
sh	Sharable allows more than one user to access the file at the same time. This attribute is usually used with Read Only.	Yes	No
sy	System hides the directory or file so it does not appear in a file manager or directory listing. System is normally used with operating system files, such as Linux or NetWare system files.	Yes	Yes
tr	Transactional allows a file to be tracked and protected by the Transaction Tracking System™ (TTS™).	Yes	No
vo	Volatile indicates that a file can change without being written to so that opportunistic locks cannot be set on it.	Yes	No

Example

```
attrib /designs/topsecret -c=all -s=ro,di
```

This command clears all attributes, then sets read-only and delete-inhibit on the /designs/topsecret file.

FLAG

For NetWare, you can use the FLAG utility to set directory and file attributes from the command line. For information, see “FLAG” in the *NetWare 6.5 Utilities Reference*.

20 Managing Hard Links

The Novell Storage Services™ File System supports zero or more hard links for files. This section discusses the following:

- ◆ “[Understanding Hard Links](#)” on page 283
- ◆ “[Creating a Hard Link](#)” on page 284
- ◆ “[Deleting a Hard Link](#)” on page 284

Understanding Hard Links

Hard links let NSS users create multiple names for a single file object in the same or multiple directories in an NSS volume. The names link to the original file inode in the file system. One file can have names in several different directories as long as all the directories reside on the same volume. It is not possible to create hard links to the same file in multiple file systems.

IMPORTANT: Hard links to directories, data streams, and extended attributes are not allowed.

Hard Links and Disk Quotas

The size of the file is charged to the original file owner’s disk quota. If other users create hard links to the file, they are not charged disk quota. The file’s owner can delete any links to the file in directories the owner can access. Hard links from directories the owner cannot access can cause the file to be retained, and the owner continues to be charged for its quota.

Limited Number of Hard Links

The number of hard links you can use for a file depends on the length of the names you choose for the file and the space required to store each name in all four namespaces (UNIX, Long, DOS, and Macintosh). The sum of the name information for all of the file’s names is limited to about 512 Unicode characters. If a file name is very long (greater than 200 Unicode characters), you can create very few, if any, hard links.

WARNING: When combined, all name information (names in each namespace) for a file cannot exceed 512 Unicode characters.

If you exceed the 512 Unicode character limit, you cannot create new hard links until you make room for them. Use any of the following methods:

- ◆ Delete one or more hard links for the file.
- ◆ Create hard links for the file with shorter names that can be stored optimally in each namespace.
- ◆ Rename the original file with a shorter name that can be stored optimally in each name space.

Creating a Hard Link

Creating a hard link to a file does not copy the contents of the file to the new location; it simply makes a new name by which the file can be known, in addition to the file's existing name or names. All of the names are equally real, and no one of them is preferred to the others. The actual content of the file is maintained in only one place: the original file. Users in different directories can use hard links to access and share the same file. A single user can use hard links to access a file from different directories.

To create a hard link, use the Link (ln) command from a Linux client. At a terminal console, enter

```
ln /path/filename /linkpath/linkfilename
```

Replace */path/filename* with the path name for the original file. Replace */linkpath/linkfilename* with the path name for the hard linked filename. To maximize the number of hard links you can use, choose short names that can be stored optimally in each namespace. For information, see [“Understanding Hard Links” on page 283](#).

For help with syntax and options, refer to the Link Manual Page from a Linux client. At a terminal console, enter

```
man 2 ln
```

For example, from a Linux client, you can use the Link command to link the file /tmp/timetest to /usr/tmp/t1, using the following command:

```
ln /tmp/timetest /usr/tmp/t1
```

The file can now be referred to by either name. You can delete the original name or any link name, but the contents of the file are not removed until the final name is deleted.

Deleting a Hard Link

Deleting a hard link to a file deletes the link and might also delete the contents of the file if it is the last remaining link to the file's contents. NSS keeps a count of how many links a file has and does not delete a file until all names for the file have been deleted (the link count goes to zero). Deleting the primary link to the file does not delete the file's contents as long as hard links exist; it deletes only the primary link. You delete a file when you delete the primary link between the original filename and the file, and you delete all hard links to that file.

To delete a hard link, use the Remove (rm) command from a Linux client. At a terminal console, enter

```
rm /linkpath/linkfilename
```

Replace */linkpath/linkfilename* with the path name for the hard linked filename.

For example, from a Linux client, you can use the Remove command to remove hard link /usr/tmp/t1 by entering the following command:

```
rm /usr/tmp/t1
```

A

Upgrading NetWare 5 Volumes to NetWare 6.x NSS Volumes Using Volume Copy Upgrade

This section discusses how to convert legacy NetWare® 5 NSS volumes and NetWare Traditional volumes to NSS volumes for use with NetWare 6.5.

- ◆ “[Copying and Upgrading Legacy Volumes with Volume Copy Upgrade](#)” on page 285
- ◆ “[Upgrading Legacy NSS Volumes](#)” on page 291
- ◆ “[Upgrading Legacy NSS Volumes in Clusters](#)” on page 292

Copying and Upgrading Legacy Volumes with Volume Copy Upgrade

Volume Copy Upgrade (VCU) is a volume conversion utility that lets you copy metadata and user data from legacy NetWare Traditional volumes and NSS volumes to NetWare 6.5 and later NSS volumes. You can also use VCU to copy NSS volumes. Volume copy upgrade moves the volume to the NSS pool and all of the volume’s file and directory attributes remain the same. Copying the data to the new location can take several hours, depending on the size of the volume. You can run VCU from the server command line or from a GUI application that runs on the server or on a workstation.

- ◆ “[Understanding Volume Copy Upgrade](#)” on page 285
- ◆ “[Using VCU from the Command Line](#)” on page 287
- ◆ “[Using VCU from a Java Application](#)” on page 288
- ◆ “[After the Volume Copy or Volume Upgrade](#)” on page 291

Understanding Volume Copy Upgrade

Volume Copy Upgrade (vcu.nlm) provides the following capabilities:

- ◆ VCU creates an inherited rights filter file, called irf.out. This file contains information about whether the Inherited Rights Filters were moved correctly during a volume copy or restore. Mismatches are preceded by three asterisks (***).

The irf.out file is stored in the same location as errors.out (at the root directory of the destination volume).

IMPORTANT: When you use VCU to upgrade a Traditional NetWare sys: volume to the NSS sys: volume, the implied trustee rights do not transfer with this method. After you upgrade volume sys: to NSS, you must manually add a public trustee with Read and File Scan rights to the sys:login directory.

- ◆ You can use VCU to copy and restore NSS volumes and to copy NetWare Traditional volumes to NSS volumes.
- ◆ You can run vcu.nlm from a Windows client.

Before you begin to upgrade NetWare Traditional volumes, make sure that the NSS pool that you are copying data to has enough space to accommodate the source volume's uncompressed data. Use the `ndir` command to determine how much space is saved by using compression on the volume. For information, see [“Viewing the File Attributes with the Ndir Command” on page 189](#). Add the space saved to the space used to find the total uncompressed volume size of the Traditional volume.

An NSS volume is about 110% of the size of NetWare Traditional volumes because files and directories stored on NSS have more metadata associated with them. For example, if you want to move 2 GB of viable data (disregard free blocks or salvage blocks), the destination NSS volume needs to have at least 2.2 GB of free space available.

IMPORTANT: Upgrade only one volume at a time.

The syntax for `vcu.nlm` is:

Copy Upgrade	<code>vcu [/p /l /d /m] origVolName nssPool</code>
Restore the Original Volume	<code>vcu [/r /m] origVolName renamedVolName</code>
Help	<code>vcu /h</code>

The VCU parameters are listed in the following table:

VCU Parameters and Help	Description
<code>origVolName</code>	The name of the original NetWare Traditional volume or NSS volume that you want to copy to a new NSS volume of the same name.
<code>nssPool</code>	The pool where the new NSS volume resides.
<code>renamedVol</code>	The name assigned to the original NetWare Traditional volume or NSS volume that you successfully copied to the NSS volume.
<code>/h</code>	Lists the syntax and options for the command.

The following table lists the possible VCU switches when copying or upgrading volumes. The switches are optional; you can include them in any order in your VCU command line.

VCU Option	Description
<code>/d</code>	Deletes the original volume if the copy process is successful. If you choose to delete the Traditional volume, the new NSS volume retains the name of the original volume.
<code>/l</code>	Does not write errors to log file (<code>Dst_Vol:error.out</code>).
<code>/m</code>	Renames the physical volume and its default Novell eDirectory™ objects.
<code>/p</code>	Does not display the entire copy status on the VCU screen. You get only a brief message after the volume copy is completed.

The following table lists the possible VCU options when restoring volumes:

VCU Option	Description
<code>/r</code>	Lets you restore the old volume to its original name. (Use this option if you want to delete the new NSS volume and rename the old one with its original name.)

VCU Option	Description
/m	Renames the physical volume and its default Novell eDirectory objects.

For example, to convert a NetWare Traditional volume named users to an NSS volume named users, enter:

```
vcu /m users p_users
```

To continue the example, suppose that you decide to undo the copy and return to the legacy volume. To remove the NSS volume users and restore the original name to the NetWare Traditional volume, enter:

```
vcu /r /m users users_old
```

Using VCU from the Command Line

Copying Volumes

- 1 Stop all applications on the server that access the volumes you are copying.

WARNING: Before using this utility to copy Traditional or NSS volumes, stop all applications that access the volume you are copying. This is especially important for the sys: volume. If any applications are open on the sys: volume when you begin the volume copy, your sys: volume might become corrupted and render your server unusable.

- 2 At the command line, specify the volume that you want to copy, then specify the existing NSS pool (on the same server) where you want to store the data from the volume (VCU can convert volumes with long names) by using this format:

```
vcu original_volume_name NSS_pool_name
```

For customization options, see “[Understanding Volume Copy Upgrade](#)” on page 285.

For example, if you wanted to copy the Apps volume and put the data on a volume in Pool2, you would enter the following at the server console:

```
vcu apps pool2
```

In this example, VCU copies the data in the volume apps and places it in a volume on Pool2, named apps_new.

When volumes are copied using VCU, a new NSS volume named *originalvolumename_new* is automatically created for you in the specified pool. If the original volume name is longer than 10 characters, or if the newly created NSS volume name conflicts with another existing volumes, the new NSS volume will be named vcuxxx_new, where the xxxx is a random number generated by NSS.

- 3 Select Yes to rename your volumes.

After the volume copy is finished, VCU asks you if you want to rename your volumes. If you select Yes, VCU renames your original volume to *originalvolumename_old* and the new NSS volume from *originalvolumename_new* back to the name of the original volume. If you select No, you must manually rename the new volume later.

NOTE: By using the /m switch, VCU also lets you rename the volume's default eDirectory object for both NSS and Traditional volumes (except for the sys: volume).

- 4 Review the information in “[After the Volume Copy or Volume Upgrade](#)” on page 291 and perform any required follow-up actions.

Restoring Volumes

At the server console, enter

```
vcu /r VCUTargetVolName VCUTargetVolName_old
```

For example, if you want to restore Vol2, you would enter the following:

```
vcu /r Vol2_new Vol2_old
```

VCU would delete Vol2_new, then rename Vol2_old back to its original name of Vol2.

TIP: To rename the volume's default eDirectory object, insert the /m switch into the command line.

Using VCU from a Java Application

You can also upgrade volumes using the VCU Java application called vcuApp.jar. You can access the VCU GUI application from a server or a workstation.

Accessing VCU from the Server

1 Use one of the following methods:

- ♦ At the server console, enter
vcux
- ♦ At the GUI console, click Novell > Utilities > Volume Copy Upgrade.

Accessing VCU from a Workstation

1 Make sure that Java 1.4 or later is installed on your workstation.

2 Map a drive to the _Admin volume.

3 To run the VCU application from a server:

3a Map a drive on the workstation to sys:java\lib\ on the server.

3b Open a directory browser to the mapped drive, then double-click the vcuApp.jar icon.

4 To run the VCU application locally on the workstation:

4a Browse to sys:\java\lib\vcuApp.jar on the server.

4b Copy vcuApp.jar to a directory on your workstation.

4c To run the application, use one of these methods:

- ♦ Open the local directory, then double-click the vcuApp.jar icon.
- ♦ At the DOS prompt, enter

```
java -jar your_directory\vcuApp.jar
```

Continue with the next section, “[Copying Volumes](#)” on page 288.

Copying Volumes

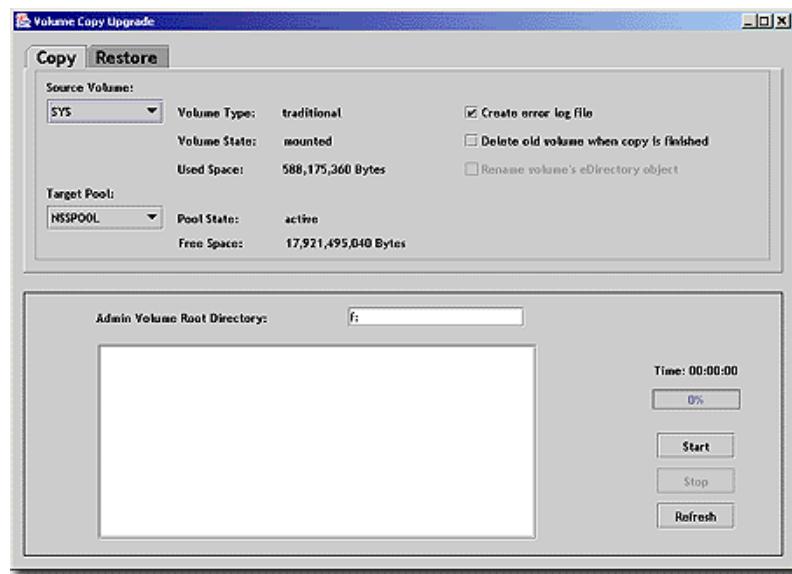
1 Stop all applications on the server that access the volumes you are copying.

WARNING: Before using this utility to copy Traditional or NSS volumes, stop all applications that access the volume you are copying. This is especially important for the sys: volume. If any applications are open on the sys: volume when you begin the volume copy, your sys: volume might become corrupted and render your server unusable.

2 Launch VCU.

For instructions, see [“Using VCU from a Java Application” on page 288](#).

The following graphic is an example of what the VCU Copy screen looks like.



3 Click the Copy tab.

4 (Conditional) If you are running VCU from a workstation, specify the drive letter of the drive that you mapped to the _Admin volume, followed by a colon (:), in the Admin Volume Root Directory text box, then click Refresh.

If you are running VCU from the server, the Admin Volume Root Directory text box is automatically filled in for you.

5 Select the source volume and the target pool from the drop-down lists.

If you have recently added a pool or volume via iManager, click the Refresh button to see the new pool or volume appear in the drop-down list.

Make sure the target pool has enough space to accommodate the data that will be copied from the source volume.

6 Refer to the following table to determine whether you want to create an error log, rename the copied volume’s default eDirectory object, or delete the old volume after the volume data is copied:

Options	Results
Create an Error Log	Creates an error log called ERROR.OUT and saves it at the root directory of the destination volume. For more information, see “Copying and Upgrading Legacy Volumes with Volume Copy Upgrade” on page 285 .
Delete Old Volume When Copy Is Finished	Deletes the old (original) physical volume; however, the volume’s eDirectory object remains.

Options	Results
Rename Volume's eDirectory Object	Renames the volume's default eDirectory object. For more information, see "Copying Volumes" on page 288 .

7 Click Start to begin the volume copy.

If you stop the volume copy for any reason, then click Start again, the volume copy does not resume where it left off, but starts again at the beginning.

8 (Optional) Rename your volumes.

After the volume copy is finished, VCU asks you if you want to rename your volumes. If you click Cancel, VCU is finished. If you click OK, VCU renames your original volume to *originalvolumename*_old and the new NSS volume from *originalvolumename*_new back to the name of the original volume.

9 Review the information in ["After the Volume Copy or Volume Upgrade" on page 291](#) and perform any required follow-up actions.

Restoring Volumes

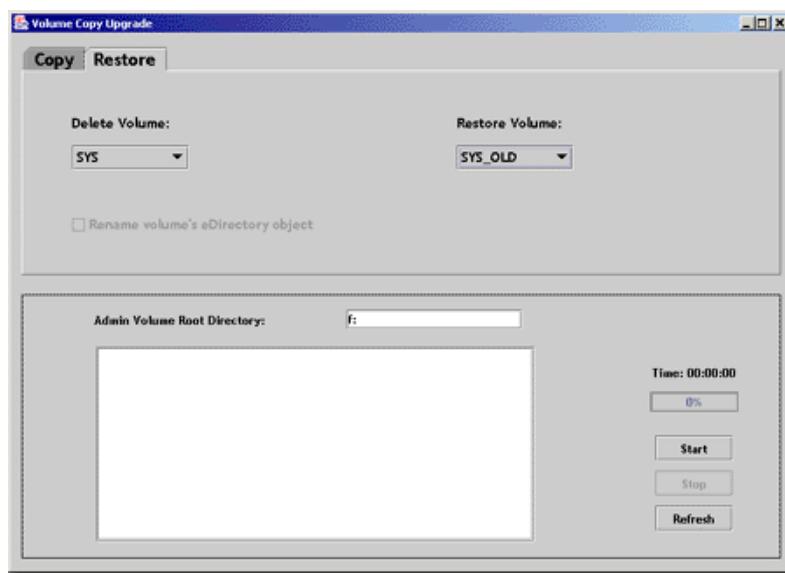
1 Stop all applications on the server that access the volumes you are copying.

WARNING: Before using this utility to copy Traditional volumes or NSS volumes, stop all applications that access the volume you are copying. This is especially important for the sys: volume. If any applications are open on the sys: volume when you begin the volume copy, your sys: volume might become corrupted and render your server unusable.

2 Launch VCU.

For instructions, see ["Using VCU from a Java Application" on page 288](#).

The following graphic is an example of the VCU Restore dialog box.



3 Click the Restore tab.

4 (Conditional) If you are running VCU from a workstation, specify the drive letter of the drive that you mapped to the _Admin volume, followed by a colon (:), in the Admin Volume Root Directory text box, then click Refresh.

If you are running VCU from the server, the Admin Volume Root Directory text box is automatically filled in for you.

5 From the drop-down list, select the volume that you want to delete and restore.

If you have recently added a pool or volume via iManager, click the Refresh button to see the new pool or volume appear in the drop-down list.

6 Determine if you want to rename the volume's default eDirectory object.

7 Click Start.

When you click Start, the volume that you are restoring is automatically renamed to the name of the volume that you are deleting.

After the Volume Copy or Volume Upgrade

- ♦ Restart the server if you are upgrading the sys: volume to ensure that the volume copied properly.

- ♦ Verify that the volume data was copied successfully.

IMPORTANT: After you copy Traditional volume data to an NSS volume, you cannot access the new NSS volume from NetWare 5.1. You need to either retain the data in the Traditional volume, or copy the data back to the Traditional volume.

Upgrading Legacy NSS Volumes

Follow this procedure to copy and upgrade your legacy NSS volumes to NetWare 6.5 NSS volumes after you have upgraded the operating system. When you upgrade the operating system of a NetWare 5.x server, the NSS volumes are not automatically upgraded and do not function until you upgrade them.

If you upgrade your server from NetWare 6.0 to NetWare 6.5, the NSS media format upgrade occurs automatically in the background as you use the volume. Typically, this can take up to 21 days, depending on the amount of data you have on the volume and whether you are using compression. There are no negative performance implications for this gradual conversion.

IMPORTANT: You do not need to manually upgrade legacy NSS volumes in clusters after an upgrade. The cluster automatically calls to perform the upgrade.

1 View and verify the time stamp.

Before you upgrade NSS volumes, you must ensure that Novell eDirectory™ is running properly; otherwise, the upgrade process might remove your trustee assignments. To ensure that eDirectory is running, you need to verify the time stamp for the backlink process.

1a Open iMonitor in a network browser by entering the IP address of the server followed by /nds.

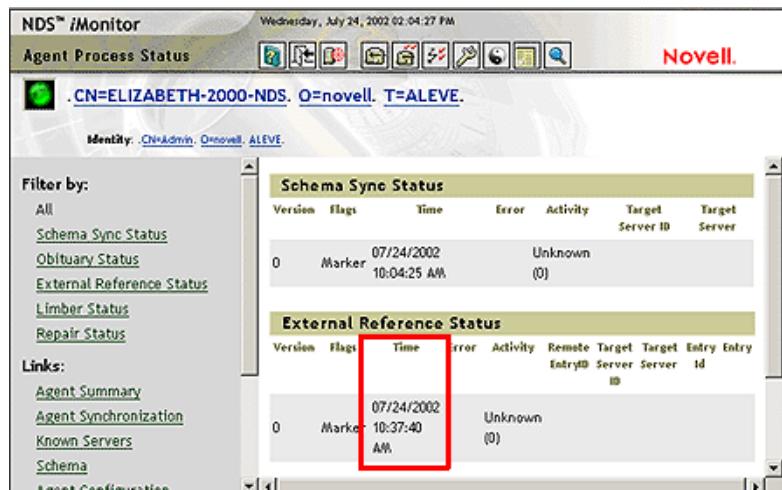
For example: <http://192.168.1.1/nds>

1b Click Agent Process Status > External Reference Status.

1c Make sure the time stamp (under the Time column) shows a time later than the time you began the upgrade. Specifically, look for the time stamp when eDirectory unloaded during the upgrade.

IMPORTANT: If the time stamp shows a time earlier than when you began the upgrade, the backlink process is not complete. Do not upgrade your existing Netware 5 NSS volumes until the backlink is complete.

The following graphic provides an example of the time stamp.



2 At the server console, enter one of the following:

- ◆ **`nss /zlssvolumeupgrade=all`**
Specify “all” to upgrade all the NetWare 5 volumes on the selected server.
- ◆ **`nss /zlssvolumeupgrade=volume`**
Specify the volume to upgrade one of the NetWare 5 volumes on the selected server.

After you upgrade the volumes, use the Mount All command to mount all of the volumes. You can also mount the volumes individually.

Upgrading Legacy NSS Volumes in Clusters

If your legacy NSS volumes are in clusters, the upgrade of your cluster services also automatically upgrades your legacy NSS volumes. Novell Cluster Services™ includes a pre-upgrade step that backs up the Trustees for your files and directories. The cluster automatically calls `nss /zlssvolumeupgrade` to perform the upgrade from the NetWare 5 NSS volume media format to NetWare 6.5 NSS volume media format. For information, see “[Upgrading Novell Cluster Services](#)” in the *Novell Cluster Services 1.7 Administration Guide*.

B

Comparison of NSS and NetWare Traditional File Systems

This section compares features and capabilities of the Novell® Storage Services™ (NSS) File System on NetWare® and the NetWare Traditional File System.

- ◆ “Comparison of Features for NSS and Traditional File Systems” on page 293
- ◆ “SET Parameters Shared by NSS and Traditional File Systems” on page 297
- ◆ “SET Parameters for the NSS File System” on page 298
- ◆ “SET Parameters for the Traditional File System” on page 299
- ◆ “Comparison of Directory and File Attributes” on page 300

Comparison of Features for NSS and Traditional File Systems

The following table describes key features of the NSS File System and the NetWare Traditional File System:

Feature Description	NSS File System	NetWare Traditional File System
Management interfaces	Novell iManager NSSMU Novell Remote Manager (limited feature set)	Novell Remote Manager
Device and partition management	Novell iManager NSSMU	Novell Remote Manager
File system management for directories and files	Novell Client™ Novell NetStorage (via Web browser only, not WebDAV) Novell Remote Manager Trustee Rights Utility	Novell Client Novell Remote Manager
Interface	64-bit	32-bit
File protocols	NCP™ NFAP (AFP, NFS, CIFS)	NCP
Character format	Unicode	ASCII double-byte

Feature Description	NSS File System	NetWare Traditional File System
Maximum device size recognized (physical or logical)	2 TB	2 TB
Minimum device size recognized (physical or logical)	10 MB	10 MB
Maximum partition size	2 TB	1 TB
Minimum partition size	10 MB	10 MB
Maximum number of partitions (logical or physical devices) per NSS pool or Traditional volume	<p>No practical limit, but the combined size cannot exceed the maximum NSS pool size of 8 TB.</p> <p>A single partition must have more than 10 MB and up to 2 TB of available space to be recognized by NSS.</p>	Up to 32 partitions, but the combined size cannot exceed the maximum Traditional volume size of 1 TB.
Maximum NSS pool or Traditional volume size	<p>8 TB</p> <p>An NSS pool of 8 TB requires at least 4 segments of up to 2 TB each. You can combine any number of partitions of 10 MB to 2 TB in size, but the combined size cannot exceed 8 TB.</p>	<p>1 TB</p> <p>A Traditional volume of 1 TB requires 1 to 32 partitions of 10 MB to 1 TB in size, but the combined size cannot exceed 1 TB.</p>
Minimum NSS pool or Traditional volume size	10 MB	10 MB
Maximum file size	Up to 8 TB per file, depending on the volume size and available space in the volume.	Up to 4 GB per file, depending on the volume size and available space in the volume.
Maximum number of files per volume	Up to 8 trillion, regardless of how many namespaces are loaded.	Up to 16 million files with 1 namespace. The practical limit is up to 4 million files with 3 namespaces.
Maximum number of files open concurrently	1 million	100 thousand
Maximum number of data volumes mounted concurrently per server	<p>255 plus the sys: volume.</p> <p>You can mount NSS volumes beyond 256, but they are not visible or accessible through the normal Netware APIs.</p>	255 plus the sys: volume.
Maximum size of a volume	<p>Up to 8 TB, depending on the pool size and available space in the pool.</p> <p>If a pool contains multiple volumes, the cumulative administrative maximum sizes of all volumes can exceed the pool size, using the overbooking feature, although real total size is bound by physical limitations. Because space is allocated to volumes as needed, a volume might not reach its quota.</p>	<p>Up to 1 TB.</p> <p>The total size allocated for all volumes on the server cannot exceed the physical size of all devices combined, so overbooking is not possible. Unused space goes to waste if volumes grow unevenly.</p>

Feature Description	NSS File System	NetWare Traditional File System
Time to mount a volume	<p>Only a few seconds.</p> <p>NSS uses a journaling file system and does not need to scan the entire file system to create a directory entry table (DET) and to load a File Allocation Table (FAT).</p>	<p>Up to several minutes, depending on volume size.</p> <p>The mount process scans the entire file system to create a DET before loading the volume. The time to mount increases based on the number of files, the number of namespaces used, and the size of the files.</p> <p>The mount process also loads the volume's FAT. Volumes with a smaller block size require more server memory to mount and manage, and it takes longer to mount the volume.</p>
Volume namespace	<p>Accommodates all namespaces and requires less memory to mount than Traditional volumes.</p>	<p>Each namespace you add to a Traditional volume requires additional server memory.</p> <p>If you add namespace support to a volume and do not have enough memory, that volume cannot be mounted.</p>
Minimum server memory required to activate a volume	<p>Requires only 1 MB of available RAM to activate a single volume of any size and any number of files. Loads a file's metadata into memory only as you access the file.</p>	<p>Loads the DET into memory at the time of the mount. The amount of memory required increases with volume size and number of files. For a maximum volume size and number of objects, the memory required can be up to 1 GB just to activate the volume.</p>
File access time	<p>Same for each file, regardless of its location on the volume.</p>	<p>Depends on the file's location on the volume.</p>
File save time	<p>Offers the Flush Files Immediately attribute for NSS volumes to write files to disk on save instead of waiting for the next disk write cycle. This helps prevent possible data loss between disk write cycles and helps ensure data integrity.</p>	<p>Caches file in memory until the next disk write cycle.</p>
File compression	Yes	Yes
Volume encryption	Yes	No
Error correction and data recovery time on system failure	<p>Journaling file system logs changes. On system failure, replays the most recent transactions to confirm validity, then repairs errors or rolls back to the original condition, typically in 15 to 60 seconds, unless the volume is corrupted.</p> <p>If the volume is corrupted, repair can take up to several hours, depending on the volume size.</p>	<p>Must verify the entire volume contents with vrepair.nlm, which can take several hours, depending on the volume size.</p>

Feature Description	NSS File System	NetWare Traditional File System
Software RAID support	RAID 0 (striping)	RAID 0 (striping)
	RAID 1 (mirroring)	RAID 1 (mirroring)
	RAID 5 (striping with parity)	RAID 10 (mirroring RAID 0 devices)
	RAID 10 (mirroring RAID 0 devices)	
	RAID 15 (mirroring RAID 5 devices)	
Data shredding	Yes, up to 7 times	No
Transaction Tracking System™ (TTS™)	Yes	Yes
	Requires exclusive use per server. To use TTS, first disable TTS for all Traditional volumes, and then enable TTS for your NSS volumes.	Requires exclusive use per server. Use for Traditional or for NSS, but not for both on the same server. TTS is enabled by default.
Directory quotas and User space quotas	Yes	Yes, enabled by default
File snapshot attribute (make a temporary snapshot copy of an open file for backup)	Yes; allows backup of open files without deactivating the volume.	No
Pool snapshot (retain point-in-time version of a pool using block-level copy on write)	Yes; allows backup of block-level changes, without deactivating the volume.	No
	Uses a brief freeze-release process to capture information for last remaining open files.	
Backup support	Reviews a journaled list of files modified since the previous backup.	Does not have a modified file list. It must scan the entire file system to identify files modified since the previous backup.
Backup systems support	TSA, TSA600 for files over 2 GB, SMS, and Enhanced SBackup	TSA, SMS, and Enhanced SBackup
Device maintenance support	Activate and deactivate devices by pool.	Activate and deactivate devices by Traditional volume.
CD and DVD device recognition	Default process with full support for ISO 9660 and Macintosh HFS formats.	CDs and DVDs cannot be Traditional volumes in NetWare 6.5.
	Use CDs and DVDs as read-only NSS volumes.	
Operating system version detection	Default process	Manual process
DOS FAT compatible	Yes	No
Ability to access DOS partitions on the NetWare server	Load dosfat.nss to treat as a standard NSS volume.	No
Block suballocation	Unnecessary; superseded by technology.	Yes

Feature Description	NSS File System	NetWare Traditional File System
Auditing	Unnecessary; superseded by technology.	Yes
File name locks	Unnecessary; superseded by technology.	Yes
Data migration	Yes	Yes

SET Parameters Shared by NSS and Traditional File Systems

The SET parameters for the Common File System are shared by NSS and Traditional file systems. The following are the default settings in NetWare 6.5 for the Common File System SET parameters.

IMPORTANT: When modifying Common File System SET parameters, ensure that your planned settings satisfy the requirements for both your NSS and Traditional volumes on NetWare.

Common File System SET Parameters	Default Value
Maximum Transactions	10000
Maximum Concurrent Directory Cache Writes	75
Minimum File Delete Wait Time	1 minute 5.9 seconds
Immediate Purge Of Deleted Files	Off
Compression Daily Check Stop Hour	6
Compression Daily Check Starting Hour	0
Minimum Compression Percentage Gain	20
Enable File Compression	On
Maximum Concurrent Compressions	2
Convert Compressed To Uncompressed Option	1
Decompress Percent Disk Space Free To Allow Commit	10
Decompress Free Space Warning Interval	31 minutes 18.5 seconds
Deleted Files Compression Option	1
Days Untouched Before Compression	14

SET Parameters for the NSS File System

The following are the default settings in NetWare 6.5 for the NSS file system SET parameters.

Common File System SET Parameters for NSS and Traditional File Systems		Default Value
NSS Auto Locks HFS CD-ROM Disc in device		Off
NSS Auto Update CDHFS Volume Objects To NDS		Off
Mount ISO 9660 multi disc set as one CD9660 volume		Off
NSS Auto Locks CD-ROM Disc in device		Off
NSS Auto Update CD9660 Volume Objects To NDS		Off
Emulate Classic NetWare Directory Quotas		Off
NSS Work To Do Count		50
NSS Maximum Cache Balance Buffers Per Session		1024
NSS Cache Balance Timer		30
NSS Cache Balance Percent		60
NSS Cache Balance Enable		On
NSS Buffer Flush Timer		1
NSS Minimum OS Cache Buffers		256
NSS Minimum Cache Buffers		256
NSS File Flush Timer		10
NSS Closed File Cache Size		50000
NSS Open File Hash Shift		16
NSS Auth Cache Size		1024
NSS ASCII Name Cache Enable		On
NSS Name Cache Enable		On
NSS Name Cache Size		2111
NSS Low Volume Space Alerts		On
NSS Low Volume Space Warning Reset Threshold		15
NSS Low Volume Space Warning Threshold		10

SET Parameters for the Traditional File System

The following are the default settings in NetWare 6.5 for the Traditional file system SET parameters.

SET Parameters for the Traditional File System	Default Value
Volume Log File State	1
Volume TTS Log File State	1
Volume Log File Overflow Size	4194304
Volume TTS Log File Overflow Size	4194304
Auto TTS Backout Flag	On
TTS Abort Dump Flag	Off
TTS Unwritten Cache Wait Time	1 minute 5.9 seconds
TTS Backout File Truncation Wait Time	59 minutes 19.2 sec
Dirty Directory Cache Delay Time	0.5 seconds
Directory Cache Allocation Wait Time	2.2 seconds
Directory Cache Buffer Nonreferenced Delay	5.5 seconds
Maximum Directory Cache Buffers	2000
Minimum Directory Cache Buffers	500
Maximum Number Of Internal Directory Handles	100
Maximum Number Of Directory Handles	20
Maximum Record Locks Per Connection	500
Maximum File Locks Per Connection	2500
Maximum Record Locks	20000
Maximum File Locks	200000
Read Ahead Enabled	On
Read Ahead LRU Sitting Time Threshold	10 seconds
Minimum File Cache Buffers	20
Maximum Concurrent Disk Cache Writes	750
Dirty Disk Cache Delay Time	3.3 seconds
Minimum File Cache Report Threshold	20
Automatically Repair Bad Volumes	On
File Delete Wait Time	5 minutes 29.6 seconds

SET Parameters for the Traditional File System	Default Value
Allow Deletion Of Active Directories	On
Maximum Percent of Volume Space allowed for Extended Attributes	10
Maximum Extended Attributes per File or Path	16
Purge Files On Dismount	Off
Fast Volume Mounts	On
Maximum Percent Of Volume Used By Directory	13
Maximum Subdirectory Tree Depth	25
Volume Low Warn All Users	On
Volume Low Warning Reset Threshold	256
Volume Low Warning Threshold	256
Turbo FAT Re-Use Wait Time	5 minutes 29.6 seconds
Allow Unowned Files To Be Extended	On
Auto Mount Mirrored Volume Containing Inactive Device	Off

Comparison of Directory and File Attributes

Attribute Code	Description	Applies to Files	Applies to Directories	NSS	Traditional
A	Archive Needed identifies files that have been modified since the last backup. This attribute is assigned automatically.	Yes	No	Yes	Yes
Ci	Copy Inhibit prevents Macintosh users from copying a file. This attribute overrides Read and File Scan trustee rights.	Yes	No	Yes	Yes
Dc	Do Not Compress keeps data from being compressed. This attribute overrides settings for automatic compression of files not accessed within a specified number of days.	Yes	No	Yes	Yes
Di	Delete Inhibit means that the directory or file cannot be deleted. This attribute overrides the Erase trustee right.	Yes	Yes	Yes	Yes
Dm	Do Not Migrate prevents directories and files from being migrated from the server's server disk to another storage medium.	Yes	Yes	Yes	No migration support
Ds	Do Not Suballocate prevents data from being suballocated.	Yes	No	Not needed	Yes
H	The Hidden attribute hides directories and files so they cannot be listed using the DIR command.	Yes	Yes	Yes	Yes

Attribute Code	Description	Applies to Files	Applies to Directories	NSS	Traditional
I	Index allows large files to be accessed quickly by indexing files with more than 64 File Allocation Table (FAT) entries. This attribute is set automatically.	Yes	No	Not needed	yes
Ic	Immediate Compress sets data to be compressed as soon as a file is closed. If applied to a directory, every file in the directory is compressed as each file is closed.	Yes	Yes	Yes	Yes
N	Normal indicates the Read/Write attribute is assigned and the Shareable attribute is not. This is the default attribute assignment for all new files.	Yes	Yes	Yes	Yes
P	Purge flags a directory or file to be erased from the system as soon as it is deleted. Purged directories and files cannot be recovered.	Yes	Yes	Yes	Yes
Ri	Rename Inhibit prevents the directory or file name from being modified.	Yes	Yes	Yes	Yes
Ro	Read Only prevents a file from being modified. This attribute automatically sets Delete Inhibit and Rename Inhibit.	Yes	No	Yes	Yes
Rw	Read/Write allows you to write to a file. All files are created with this attribute.	Yes	No	Yes	Yes
Sh	Shareable allows more than one user to access the file at the same time. This attribute is usually used with Read Only.	Yes	No	Yes	Yes
Sy	System hides the directory or file so it does not appear in a file manager or directory listing. System is normally used with operating system files, such as NetWare system files.	Yes	Yes	Yes	Yes
T	Transactional allows a file to be tracked and protected by the Transaction Tracking System (TTS).	Yes	No	Explicit	Implicit and explicit
X	The Execute attribute indicates program files such as .exe or .com.	Yes	No	Yes	Yes

C

NSS Nomenclature

This section discusses the nomenclature used for key Novell® Storage Services™ media objects in NetWare® 6.5. This information can help you better understand the nature of error messages you might receive when using NSS. The table table identifies the media object, defines it, and indicates the version of NetWare where the media object first appeared. All ZLSS (NSS Journaled Storage System) file blocks are 4 KB in size.

Media Object	Definition	NetWare Version Where First Used
Beast B-Tree	The Balanced Tree (B-Tree) that tracks all the file's metadata. This includes when the file was created, who created the file, the size of the file, and the location of the file's data.	5.0
Checkpoint	Four blocks (one in each Superblock) that track where to start playing the journal if the server crashes. The checkpoint contains the metadata of the Journal .	5.0
Directory B-Tree	Used to implement an NSS volume's Directory Quota feature.	5.0 Support Packs
Entry ID (EID)	An eDirectory™ entry within the FLAIM database (the underlying database for Directory Services 8.35 and later, including all eDirectory versions). EIDs are 32 bits and are unique for each server. EIDs are used within eDirectory to reference objects on a specific server. They are unique for each object for each server, meaning that object CN=Admin.O=EMA_CORP potentially has a different EID on server FS1 than on server FS2. This can be demonstrated with dsbrowse.nlm, a tool you can use to examine the local eDirectory database on the NetWare server. If you examine an object on one server and compare it with the same object on another server, the EID between the two instances of the object are probably dissimilar.	6.0
Epoch File Log (EFL) B-Tree	Tracks files that change during an administrator-specified interval of time called an epoch. This feature is used by Novell Archive and Version Services.	6.5
Globally Unique ID (GUID)	A globally unique identifier within eDirectory. The scope of this uniqueness is within one tree, although no actual checking is done to ensure this. GUIDs are 128 bits and are unique for each object. GUIDs allow an object to be referenced no matter which server you are accessing.	5.0
Journal	The file used to quickly make the file system consistent after a server crash. The journal is sometimes referred to as a zlog.	5.0
Logged Pool Data Block	The block that tracks information about the pool, including the number of used blocks and salvageable blocks. Holds some of the items found in the zPoolInfo_s portion of the zInfo_s structure.	6.0

Media Object	Definition	NetWare Version Where First Used
Logged Volume Data Block	The block that tracks the number of files, used blocks, and compressed files of a volume. Holds some of the items found in the <code>zVolumeInfo_s</code> portion of the <code>zInfo_s</code> structure.	5.0
Modified File List (MFL) B-Tree	Tracks files and folders that have the Archive attribute set by the user. The Archive flag indicates that the file or folder needs to be backed up. NSS uses this list to quickly find files that need to be backed up during scheduled backups. This Archive file-and-folder attribute is unrelated to Novell Archive and Version Services.	6.0
Multiple Server Access Protection (MSAP)	The block used to reduce accidental use of a pool by more than one server at a time. A single copy of this block is stored in the second Superblock .	6.0 Support Packs
Name Tree B-Tree	The B-Tree that tracks the directory structure of a volume.	5.0
Pool Data Block	The block that tracks persistent pool configurable items. For example, a pool's features are stored here. Holds some of the items found in <code>zPoolInfo_s</code> portion of the <code>zInfo_s</code> structure.	6.0
Purge Log	Tracks transactions over an extended period so they can be completed after a crash. For example, the log records file deletes and truncates that need to be completed after a crash.	5.0
Purge Tree B-Tree	Used to store information about all salvageable files. This tree is used when the file system needs to auto purge files to create free blocks.	5.0
Snapshot	Used by the Media Manager to track pool snapshots. The object tracks which snapshots exist on a pool and where all blocks of a snapshot are stored. The root of this object resides in the first Superblock . All other blocks are allocated from a file on the internal volume.	6.5
Superblock	There are four Superblocks of 16 blocks each. The four Superblocks are replicas that reside in four fixed locations within the pool. The Superblock is used by the Checkpoints , Superblock Header , Snapshot , and Multiple Server Access Prevention .	5.0
Superblock Header	Four blocks (copies of each other, one in each Superblock) used to locate all other ZLSS media objects. These are the first blocks that the file system reads when a volume is loaded. Starting with NetWare 6.0, these blocks are read when a pool is loaded.	5.0
User B-Tree	Used to implement an NSS volume's User Quota feature. Starting with NetWare 6.0, the B-Tree also stores Novell eDirectory information related to User Quota.	5.0 Support Packs
Volume Data Block	The block that tracks configurable items in NSS volumes such as the volume's attributes and the high and low watermarks for salvage. It holds some of the items found in <code>zVolumeInfo_s</code> portion of the <code>zInfo_s</code> structure.	5.0
ZID	A numeric ID within the NSS file system, used to reference an object with the object store (also known as the <i>beast tree</i>). ZIDs are 64 bits and are unique for each volume.	6.0

D

Documentation Updates

This section contains information about documentation content changes made to the *Novell Storage Services Administration Guide* since the initial release of NetWare® 6.5. 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 front cover and the Legal Notices page, to determine the release date of this guide. For the most recent version of the *Novell Storage Services Administration Guide*, see the [Novell documentation Web site](http://www.novell.com/documentation/lg/nw65/nss_enu/data/front.html) (http://www.novell.com/documentation/lg/nw65/nss_enu/data/front.html).

In this section, content changes appear in reverse chronological order, according to the publication date. Within a dated entry, changes are grouped and sequenced, according to where they appear in the document itself. 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:

- ◆ “May 14, 2005” on page 305
- ◆ “February 28, 2005” on page 306
- ◆ “August 8, 2004” on page 309
- ◆ “July 2, 2004” on page 310
- ◆ “May 17, 2004” on page 311

May 14, 2005

Updates were made to the following sections. The changes are explained below.

- ◆ “Management Tools for NSS” on page 305
- ◆ “Securing Access to NSS Volumes and Files” on page 306

Management Tools for NSS

The following change was made to this section:

Location	Change
“Prerequisites for Using the Storage, Archive Versioning, CIFS, and Clustering iManager Plug-Ins” on page 30	For information about installing WBEM, see “Setting Up OpenWBEM” (http://www.novell.com/documentation/oes/cimom/data/bv3wjre.html) in the <i>OpenWBEM Services Administration Guide for OES</i> (http://www.novell.com/documentation/oes/cimom/data/front.html).

Securing Access to NSS Volumes and Files

The following change was made to this section:

Location	Change
“Controlling Access to the Admin Volume and Files.cmd File” on page 142	<p>The child elements to the Rights tag (<rights>) should be the following tags for file system rights:</p> <ul style="list-style-type: none">◆ <accesscontrol/> for the Access Control right◆ <create/> for the Create right◆ <edit/> for the Edit right◆ <filescan/> for the File Scan right◆ <modify/> for the Modify Metadata right◆ <read/> for the Read right◆ <supervisor/> for the Supervisor right◆ <write/> for the Write right

February 28, 2005

Updates were made to the following sections. The changes are explained below.

- ◆ “What’s New” on page 306
- ◆ “Management Tools for NSS” on page 306
- ◆ “Planning for NSS Storage Solutions” on page 307
- ◆ “Managing Devices” on page 307
- ◆ “Managing Software RAID Devices” on page 307
- ◆ “Managing NSS Pool Snapshots” on page 308
- ◆ “Managing NSS Volumes” on page 308
- ◆ “Monitoring the NSS File System Status” on page 308
- ◆ “Troubleshooting NSS” on page 309
- ◆ “Managing Hard Links” on page 309
- ◆ “Managing File System Access to Directories and Files” on page 309
- ◆ “Comparison of NSS and NetWare Traditional File Systems” on page 309

What’s New

This section consists of information previously presented in the Overview of NSS and information about feature changes for NetWare 6.5 Support Pack 3.

Management Tools for NSS

The following changes were made to this section:

Location	Change
Downloading and Installing Plug-In Updates	This section is new.
Novell NetStorage	This section is new.
Novell Client for Windows 2000/XP	This section is new.
Trustee Rights Utility	This section is new.

Planning for NSS Storage Solutions

The following changes were made to this section:

Location	Change
Security Considerations	This section is new.
Coexistence and Migration Issues	This section is new.
Naming NSS Storage Objects	This section was updated to include maximum lengths for various storage objects and the encryption password.

Managing Devices

The following change was made to this section:

Location	Change
Understanding Devices	This section was updated for clarification.

Managing Software RAID Devices

The following changes were made to this section:

Location	Change
Understanding Software RAID Devices	This section was updated for clarification.
Creating a Software RAID 10 with NSSMU	This section is new.
Creating a Software RAID 15 with NSSMU	This section is new.
Creating a RAID 1 Mirror to Duplicate Data	This section is new.

Managing NSS Pool Snapshots

The following changes were made to this section:

Location	Change
Deleting Pool Snapshots	This section was updated for new processes and commands for deleting pool snapshots.
Modifying the Stored-On Pool	This section is new.
Managing Pool Snapshots Using Commands	This section was updated to include the shredding commands for deleting pool snapshots.

Managing NSS Volumes

The following changes were made to this section:

Location	Change
Understanding NSS Volumes	This section is new.
Controlling Access to the Admin Volume and Files.cmd File	This section combined information from two closely tied topics about the trustees.xml file.
Configuring the NSS Volume Salvage Area	This section is new. It combines information about setting purge delay times and high and low watermarks for your volume when the Salvage attribute is set.
Verifying and Rebuilding NSS Pools and Volumes	The Pool Verify command was corrected to nss /poolverify.

Monitoring the NSS File System Status

The following changes were made to this section:

Location	Change
Monitoring Compression and Salvage Statistics	This section is new.
Monitoring Quotas and Space Usage for NSS Pools and Volumes	This section is new.
Monitoring File System Parameters	This section is new.

Troubleshooting NSS

The following changes were made to this section:

Location	Change
Tuning NSS Volumes for GroupWise Servers	This section is new.
Software RAID 1 Fails to Recognize a Replacement Device	This section is new.
Problems Moving NetWare 6.5 NSS Pools to NetWare 6.0 Servers	This section is new.
Problems Following DFS Junctions in Windows 2000/XP Releases	This section is new.

Managing Hard Links

This section is new.

Managing File System Access to Directories and Files

This section was updated with content from the *File Systems Management Guide for OES* related to managing access for NetWare file systems.

Comparison of NSS and NetWare Traditional File Systems

This section is new.

August 8, 2004

Updates were made to the following sections. The changes are explained below.

- ♦ “Managing Partitions” on page 309
- ♦ “Configuring and Managing Directories and Files” on page 309

Managing Partitions

This section is new in this release.

Configuring and Managing Directories and Files

The following change was made to this section:

Location	Change
File System Trustee Rights	The file system stores each NetWare trustee's ID and rights assignment as metadata with its directory or file in the NSS file system. In the NetWare Traditional file system, the file's security and attributes metadata is stored in the Directory Entry Table (DET) of its parent directory.

July 2, 2004

Updates were made to the following sections. The changes are explained below.

- ◆ “Overview of NSS” on page 310
- ◆ “Management Utilities for NSS” on page 311
- ◆ “Configuring and Managing NSS Volumes” on page 311
- ◆ “Using NSS Server Console Commands” on page 311
- ◆ “Configuring and Managing Directories and Files” on page 311

Overview of NSS

The following change was made to this section:

Location	Change
CD and DVD Image Files as NSS Volumes	In NetWare 6.5 Support Pack 2, you can now activate a CD or DVD image file as an NSS volume, if the source image file resides on an existing NSS volume and the cddvd.nss module is running.

Management Utilities for NSS

The following change was made to this section:

Location	Change
Novell iManager Storage Plug-In	Expanded information about tasks and subtasks.

Configuring and Managing NSS Volumes

The following changes were made to this section:

Location	Change
Activating and Deactivating CDs and DVDs as NSS Volumes	This information was reorganized.
Activating and Deactivating CD and DVD Image Files as NSS Volumes	In NetWare 6.5 Support Pack 2, you can activate and deactivate a CD or DVD image file as an NSS volume, if the file resides on an existing NSS volume and the cddvd.nss module is running.
Activating and Deactivating DOS Partitions as NSS Volumes	This information was reorganized.

Using NSS Server Console Commands

The following changes were made to this section:

Location	Change
Commands for Mounting CDs and DVDs as NSS Volumes	The cddvd.nss module replaces cdrom.nlm and cd9660.nss for CD support, udf.nss for DVD support, and cdfhs.nss for Macintosh* CD support. The following commands for cddvd.nss are the same ones used for previous CD and DVD management modules.
Commands for CD and DVD Image Files as NSS Volumes	In NetWare 6.5 Support Pack 2, two commands were added to support activation of CD or DVD image files as NSS volumes, if they are on existing NSS volumes. These commands are part of the cddvd.nss module.

Configuring and Managing Directories and Files

This section is new in this release.

May 17, 2004

Updates were made to the following sections. The changes are explained below.

- ◆ “Overview of NSS” on page 312
- ◆ “Management Utilities for NSS” on page 312

- ◆ “Managing Devices” on page 312
- ◆ “Configuring and Managing NSS Pools” on page 312
- ◆ “Using NSS Pool Snapshots to Support Data Backup and Restore Services” on page 313
- ◆ “Configuring and Managing NSS Volumes” on page 313
- ◆ “Managing Encrypted NSS Volumes” on page 313
- ◆ “Using Compression to Conserve Storage Space on NSS Volumes” on page 313
- ◆ “Using Distributed File Services for Moving and Splitting NSS Volumes” on page 313
- ◆ “Monitoring the Status of the NSS File System” on page 313
- ◆ “Using NSS Console Commands” on page 314
- ◆ “Appendix A: Upgrading to NSS Volumes in Clusters” on page 314
- ◆ “Appendix C: Documentation Updates” on page 314

Overview of NSS

The following changes were made to this section:

Location	Change
Benefits of NSS	Added information about Encrypted Volume Support.
Encrypted Volume Support	Added information about Encrypted Volume Support.
Multiple Device Selection in NSSMU	Added information about new capability in NSSMU that allows you to select multiple devices for initialization or sharing.

Management Utilities for NSS

The following changes were made to this section:

Location	Change
Novell iManager Storage Plug-In	Reorganized information.
NSSMU	Added information about Encrypted Volume Support, multiple device selection, and the installation option to create volumes later.

Managing Devices

The former Configuring NSS section was reorganized into separate sections for devices, pools, volumes, and Distributed File Services.

Configuring and Managing NSS Pools

The former Configuring NSS and Managing NSS sections were reorganized into separate sections for devices, pools, volumes, and Distributed File Services. This section combines information for configuring and managing pools.

Using NSS Pool Snapshots to Support Data Backup and Restore Services

This section was reorganized.

Configuring and Managing NSS Volumes

The former Configuring NSS and Managing NSS sections were reorganized into separate sections for devices, pools, volumes, and Distributed File Services. This section combines information for configuring and managing volumes.

Managing Encrypted NSS Volumes

The [Managing Encrypted NSS Volumes](#) section is new in this release.

Using Compression to Conserve Storage Space on NSS Volumes

The following changes were made to this section:

Location	Change
Configuring Compression Parameters for a Server	This section is new in this release.
Configuring Compression Attributes for Directories and Files	This section is new in this release.
Using NSS Commands to Configure and Monitor Compression	This section was updated with more command information.
Copying Compressed Files between Volumes with the Ncopy Command	This section is new in this release.
Viewing the File Attributes with the Ndir Command	This section is new in this release.
Repairing Compressed Volumes with the Comfix Utility	This section is new in this release.

Using Distributed File Services for Moving and Splitting NSS Volumes

The former Configuring NSS and Managing NSS sections were reorganized into separate sections for devices, pools, volumes, and Distributed File Services. This section discusses Distributed File Services.

Monitoring the Status of the NSS File System

The following changes were made to this section:

Location	Change
Monitoring Status of NSS Devices, Pools, and Volumes with iManager	This section consolidates links to information found elsewhere in this guide.
Monitoring Server Status with the Monitor Utility	This section is new in this release. It adds information about preexisting capabilities.
Monitoring Server Status with Novell Remote Manager	This section is new in this release. It adds information about preexisting capabilities.

Using NSS Console Commands

The following changes were made to this section:

Location	Change
Other NSS Commands	<p>The following commands were omitted because they are not valid:</p> <ul style="list-style-type: none"> ◆ nss /AutoVerifyVolume=volume_name ◆ nss /RebuildVolume=volume_name ◆ nss /VerifyVolume=volume_name

Appendix A: Upgrading to NSS Volumes in Clusters

The following changes were made to this section:

Location	Change
Upgrading Legacy NSS Volumes in Clusters	This section is new in this release.

Appendix C: Documentation Updates

The Documentation Updates section is new in this release.