

NCP Server for Linux Administration Guide

Open Enterprise Server 2 SP3

May 30, 2013

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.

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

Copyright © 2005–2010 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.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

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

Contents

About This Guide	11
1 NCP Server for Linux Overview	13
1.1 How NCP Server Works	13
1.2 Benefits of NCP Server	13
1.3 What's Next	14
2 What's New for NCP Server for Linux	15
2.1 What's New in the May 2013 Patch Release	15
2.2 What's New in the April 2013 Patch Release	15
2.3 What's New in the January 2013 Patch Release	16
2.4 What's New in the January 2012 Patch Release	17
2.5 What's New in the October 2011 Patch Release	17
2.6 What's New in the August 2011 Patch Release	17
2.7 What's New (OES 2 SP3 January Patch)	17
2.8 What's New (OES 2 SP3)	17
2.9 What's New (OES 2 SP2)	18
2.10 What's New (OES 2 SP1)	18
2.10.1 64-bit Support	18
2.10.2 eDirectory 8.8.4	18
2.10.3 Change in Syntax for Setting Inherit POSIX Permission	18
2.10.4 Novell AFP Supports Cross-Protocol File Locking with NCP for NSS Volumes	18
2.11 What's New (OES 2)	19
2.11.1 Novell Dynamic Storage Technology	19
2.11.2 NCP Server	19
3 Installing and Configuring NCP Server for Linux	21
3.1 Installation Requirements for NCP Server for Linux	21
3.1.1 Supported Platforms	22
3.1.2 NCP Server and Dynamic Storage Technology	22
3.1.3 Static Hostname and the NCP File Server Name	22
3.1.4 64-Bit Support	22
3.1.5 Novell eDirectory 8.8.4	22
3.1.6 eDirectory Rights Needed by a Container Administrator	23
3.1.7 Novell Storage Services	23
3.1.8 Novell Samba	23
3.1.9 Linux User Management	24
3.1.10 Novell AFP	24
3.1.11 Novell Cluster Services for Linux	24
3.1.12 SLP	24
3.1.13 Novell iManager 2.7 for Linux	26
3.1.14 Novell Remote Manager for Linux	26
3.1.15 OpenWBEM	26
3.1.16 Other OES 2 Linux Services	26
3.2 Installing NCP Server	26
3.2.1 Preparing for the OES 2 Install	26
3.2.2 Installing NCP Server at Install Time	27
3.2.3 Installing NCP Server on an Existing OES 2 Linux Server	28

3.3	Updating NCP Server	28
3.4	Configuring Global NCP Server Parameters	29
3.4.1	Directory Cache Management for NCP Server	30
3.4.2	Dynamic Storage Technology for NCP Server	30
3.4.3	Locks Management for File Access on NCP Server	32
3.4.4	Logs for NCP Server Events	32
3.4.5	NCP Communications	33
3.4.6	NCP Server Environment	33
3.4.7	NCP Volumes	34
3.4.8	NCP Volumes Low-Space Warning.	34
3.5	Restarting the Novell NCP/NSS IPC (ncp2nss) Daemon.	35
3.6	Restarting the Novell eDirectory (ndsd) Daemon.	35
3.7	Configuring the NCP Server Local Code Page	35
3.7.1	Using Novell Remote Manager for Linux to Configure the Local Code Page	36
3.7.2	Editing the /etc/opt/novell/ncpserv.conf File to Configure the Local Code Page	36
3.8	Configuring the Execute Only File Attribute for NCP Server	37
3.8.1	Using Novell Remote Manager for Linux to Configure the Execute Attribute Support.	37
3.8.2	Editing the /etc/opt/novell/ncpserv.conf File to Configure the Execute Attribute Support	37
3.9	Configuring Sendfile Support for NCP Server	38
3.9.1	Using Novell Remote Manager for Linux to Configure Sendfile Support.	38
3.9.2	Editing the /etc/opt/novell/ncpserv.conf File to Configure Sendfile Support	38
3.10	Configuring Opportunistic Locking for NCP Server	39
3.10.1	Using Novell Remote Manager for Linux to Configure OpLocks	39
3.10.2	Editing the /etc/opt/novell/ncpserv.conf File to Configure OpLocks.	39
3.11	Configuring Cross-Protocol File Locks for NCP Server	40
3.11.1	Using Novell Remote Manager for Linux to Configure Cross-Protocol Locks	41
3.11.2	Editing the /etc/opt/novell/ncpserv.conf File to Configure Cross-Protocol Locks.	41
3.12	Modifying the NCP File Server Name	42
3.12.1	Understanding the NCP File Server Name	42
3.12.2	Modifying the NCP File Server Name Parameter	43
3.13	Modifying the sys: Volume Mount Point	43
4	Migrating Data from NSS Volumes to NCP Volumes on Linux File Systems	45
4.1	Guidelines for Migrating Data from an NSS Volume on NetWare to an NCP Volume on Linux	45
4.1.1	Trustees and Trustee Rights	45
4.1.2	User Quotas.	45
4.1.3	Deleted Files	46
4.1.4	Encryption	46
4.1.5	Distributed File Services	46
4.2	Planning Your Migration.	47
4.2.1	System Requirements for the OES 2 Linux Server	47
4.2.2	Supported Platforms for the Source NSS Volume.	47
5	Using NCP Server and NCP Volumes in a Virtualization Environment	49
6	Planning for NCP Server and NCP Volumes	51
6.1	NCP Volumes on Linux	51
6.2	Security Issues.	51
6.2.1	POSIX Permissions on the NSS File System	51
6.2.2	POSIX Permissions on Linux File Systems.	52
6.3	Novell Dynamic Storage Technology.	52
6.4	User Quotas on Linux POSIX File Systems.	52

7	Management Tools for NCP Server	53
7.1	Novell Remote Manager for Linux	53
7.1.1	Installing Novell Remote Manager for Linux	53
7.1.2	Accessing Novell Remote Manager	53
7.1.3	Starting, Stopping, or Restarting Novell Remote Manager on Linux	54
7.1.4	Quick Reference for the NCP Server Plug-In for Novell Remote Manager for Linux	54
7.2	NCP Server Console (NCPCON) Utility	59
7.3	NCPTOP Quick Reference	60
8	Managing NCP Server	63
8.1	Monitoring NCP Server by Using Novell Remote Manager	63
8.2	Monitoring NCP Server by Using NCPCON	63
8.3	Monitoring NCP Server by Using NCPTOP	65
9	Managing Connections for NCP Volumes and NSS Volumes	67
9.1	Understanding Connections	67
9.1.1	Connection Information	67
9.1.2	Connection Listing	69
9.1.3	Detailed Connection Information	69
9.2	Managing User Login for NCP Server	70
9.2.1	Enabling Login	70
9.2.2	Disabling Login	70
9.3	Sending Messages to Logged-In Users	71
9.3.1	Enabling or Disabling Broadcast Message Support	71
9.3.2	Broadcasting a Message to All Users	71
9.3.3	Sending a Message to a Specific User	72
9.3.4	Configuring the Novell Client for Sending and Receiving Messages	72
9.4	Viewing Connections for NCP Server	73
9.4.1	Using Novell Remote Manager	73
9.4.2	Using NCPCON	75
9.5	Sorting Entries in the Connection Listing	75
9.6	Clearing Not-Logged-In Connections to NCP Server	76
9.7	Clearing Connections to NCP Server	76
9.7.1	Using Novell Remote Manager to Clear NCP Connections	76
9.7.2	Using NCPCON to Clear NCP Connections	77
9.8	Finding the Connection that Has a File Open	77
9.9	Viewing Open Files for an NCP Server Connection, and Closing All Open Files	77
9.10	Viewing Open Files for an NCP Server Connection, and Closing a Specific Open File	78
9.11	Generating and Viewing NCP Trustee Reports for NSS Volumes	79
9.11.1	Generating an NCP Trustee Report	80
9.11.2	Viewing a Saved NCP Trustee Report	80
9.11.3	Emailing a Saved NCP Trustee Report	80
10	Managing NCP Volumes	81
10.1	Understanding NCP Volumes	81
10.1.1	NCP Shares as NCP Volumes	81
10.1.2	NSS Volumes as NCP Volumes	82
10.1.3	Understanding Time Stamps on Linux	82
10.2	Creating NCP Volumes on Linux File Systems	83
10.2.1	Using Novell Remote Manager to Create an NCP Volume on a Linux File System	83
10.2.2	Creating an NCP Volume with NCPCON	84
10.3	Mounting NCP Volumes	85
10.3.1	Mounting an NCP Volume with Novell Remote Manager	85

10.3.2	Mounting an NCP Volume with NCPCON	85
10.3.3	Using the ncpmount(8) Command from a Client	86
10.4	Dismounting NCP Volumes	86
10.4.1	Dismounting an NCP Volume with NCPCON	86
10.4.2	Dismounting an NCP Volume with Novell Remote Manager	87
10.5	Viewing the Size of an NCP Volume	87
10.6	Purging Deleted Files from an NSS Volume	87
10.6.1	Purging Deleted Files with NCPCON	87
10.6.2	Purging Deleted Files with Management Tools	88
10.7	Removing an NCP Volume	88
10.7.1	Removing an NCP Volume with Novell Remote Manager	88
10.7.2	Removing an NCP Volume with NCPCON	89
10.8	Configuring Inherit POSIX Permissions for an NCP Volume	89
10.8.1	Configuring the Inherit POSIX Permissions for a New NCP Volume	90
10.8.2	Configuring the Inherit POSIX Permissions Setting for an Existing NCP Volume	90
10.9	Configuring the NCP/NSS Bindings for an NSS Volume	92
10.9.1	Understanding the NCP/NSS Bindings Parameter	92
10.9.2	Enabling the NCP/NSS Bindings for an NSS Volume	94
10.9.3	Disabling the NCP/NSS Bindings for an NSS Volume	95

11 Configuring NCP Volumes with Novell Cluster Services 97

11.1	Planning for NCP Volumes in a Cluster Environment	97
11.1.1	Novell Open Enterprise Server (OES) 2 Linux	97
11.1.2	Novell Cluster Services for Linux	97
11.1.3	NCP Server and Dynamic Storage Technology	98
11.1.4	Shareable Devices	98
11.1.5	EVMS Cluster Segment Manager	98
11.1.6	File Systems	98
11.1.7	Novell iManager 2.7	98
11.1.8	Novell Remote Manager for Linux	98
11.2	Clustering an NCP Volume on a Linux POSIX File System	99
11.2.1	Gathering Information for Clustering the NCP Volume	99
11.2.2	Creating and Cluster-Enabling a Linux POSIX Volume	101
11.2.3	Creating a Shared NCP Volume on the Linux POSIX Cluster Resource	101
11.2.4	Creating a Virtual NCP Server Object for Shared NCP Volumes	104
11.2.5	Modifying the Load Script for the Linux POSIX Cluster Resource	106
11.2.6	Modifying the Unload Script for the Linux POSIX Cluster Resource	107
11.2.7	Activating the Script Changes	107
11.3	Sample Load, Unload, and Monitor Scripts for a Cluster-Enabled NCP Volume	108
11.3.1	Sample Load Script for an NCP Volume Cluster Resource	108
11.3.2	Sample Unload Script for an NCP Volume Cluster Resource	109
11.3.3	Sample Monitor Script for an NCP Volume Cluster Resource	110

12 Managing File System Trustees, Trustee Rights, and Attributes on NCP Volumes 111

12.1	NCP on Linux Security	111
12.2	Understanding File System Trustees, Trustee Rights, and Attributes	114
12.2.1	Directory and File Trustee Rights	114
12.2.2	Directory and File Attributes	114
12.3	Managing File System Rights with NCPCON	115
12.3.1	Viewing File and Directory Rights	115
12.3.2	Adding File and Directory Rights	115
12.3.3	Removing File and Directory Rights	115
12.4	Managing File or Directory Trustees and Rights with iManager	116
12.5	Managing File or Directory Attributes with iManager	116

13 Using Opportunistic Locking for NCP File Handling	117
13.1 Understanding Opportunistic Locking for NCP Connections	117
13.1.1 Level 2 OpLocks	117
13.1.2 Level 1 OpLocks	118
13.1.3 Guidelines for Using OpLocks	118
13.2 Configuring OpLocks for NCP Server	119
13.3 Configuring File Caching in the Novell Client	120
13.4 Configuring OpLocks for NSS Volumes	120
13.5 Additional Information	120
14 Using the Inventory to Monitor NCP Volumes	121
14.1 Understanding the Volume Inventory	121
14.1.1 Inventory Summary	121
14.1.2 Available Space Trends	122
14.1.3 Graphical Profiles	122
14.1.4 Tabular Profiles	123
14.1.5 Inventory Detail Reports	123
14.1.6 Custom Scans	124
14.2 Accessing the Volume Inventory	125
14.3 Viewing Statistics for the Volume	125
14.4 Using Inventory Detail Reports to Move, Copy, or Delete Files on the Volume	126
14.5 Generating a Custom Inventory Report for DST Shadow Volumes	127
15 Troubleshooting for the NCP Server and NCP Volumes	129
15.1 NCP Clients Cannot Connect to the Server	129
15.2 Error -601 When Deleting an NCP Volume	129
15.3 Cross-Protocol Locking Stops Working	129
15.4 Error on Copying or Deleting Files When Extended Attributes Are Not Enabled	130
16 Security Considerations for NCP Server	131
16.1 UDP Port 524	131
16.2 Soft Links	131
16.3 Hard Links	132
16.4 Log Files	132
16.5 Audit Logs	133
A Commands and Utilities for NCP Server and NCP Volumes	135
A.1 NCPCON	135
A.1.1 Syntax	136
A.1.2 Getting Help	136
A.1.3 Starting and Stopping NCPCON Interactive Mode	137
A.1.4 Monitoring NCP Server	137
A.1.5 Managing NCP Server in a Cluster	138
A.1.6 Managing NCP Threads	138
A.1.7 Managing NCP Volumes	140
A.1.8 Managing File System Trustees and Trustee Rights for NCP Volumes	142
A.1.9 Managing NSS Volumes in a Cluster	144
A.1.10 Purging Deleted Files on NSS Volumes on Linux	144
A.1.11 Managing User Login	144
A.1.12 Sending Messages to Logged-In Users	144
A.1.13 Managing NCP Server Connections	145
A.1.14 Viewing or Closing Open Files	147

A.1.15	Managing Dynamic Storage Technology	148
A.1.16	Managing Dynamic Storage Technology on Novell Cluster Services for Linux Clusters	152
A.2	NCPCON SET Parameters	153
A.2.1	Directory Cache Management for NCP Server	154
A.2.2	Dynamic Storage Technology for NCP Server	155
A.2.3	Locks Management for File Access on NCP Server	156
A.2.4	Logs of NCP Server Events	157
A.2.5	NCP Communications	158
A.2.6	NCP Server Environment	158
A.2.7	NCP Volumes	159
A.2.8	NCP Volumes Low-Space Warning	160
A.3	NCP2NSS Command	161
A.4	ShadowFS Command	161
A.5	Virtual NCP Server Object Script	161
 B Additional NCP Server Commands and Options		 163
B.1	Configuration File Options	163
B.2	NCP2NSS Command Options	163
B.3	NCPCON Commands and Options	164
B.3.1	Hidden Options	164
B.3.2	Hidden Commands	164
B.4	NCPTOP Command Line Options	165
 C RPM Files for NCP Server		 167
 D Documentation Updates		 169
D.1	May 2013	169
D.2	April 2013	170
D.3	January 2013	170
D.4	September 2011	170
D.5	January, 2011	170
D.6	December, 2010	170
D.7	January 27, 2009	170
D.8	December 15, 2009	170
D.9	October 27, 2009	171
D.10	July 16, 2009	171
D.10.1	Configuring NCP Volumes with Novell Cluster Services	171
D.10.2	Managing NCP Volumes	171
D.10.3	Managing NSS Volumes in a Cluster	171
D.11	June 11, 2009	172
D.11.1	NCP Communications	172
D.12	February 13, 2009	172
D.12.1	Commands and Utilities for NCP Server and NCP Volumes	172
D.12.2	Using Opportunistic Locking for NCP File Handling	172
D.13	January 5, 2009	173
D.13.1	Commands and Utilities for NCP Server and NCP Volumes	173
D.13.2	Configuring NCP Volumes with Novell Cluster Services	173
D.13.3	Managing NCP Volumes	173
D.14	December 2008 (OES 2 SP1 Linux)	173
D.14.1	Commands and Utilities for NCP Server and NCP Volumes	174
D.14.2	Installing and Configuring NCP Server	174
D.14.3	Managing Connections for NCP Volumes and NSS Volumes	175
D.14.4	Managing NCP Volumes	175

D.14.5	Planning for NCP Server and NCP Volumes	175
D.14.6	Troubleshooting for NCP Server and NCP Volumes	175
D.14.7	Using NCP Server and NCP Volumes in a Virtualization Environment	176
D.14.8	What's New for NCP Server for Linux	176
D.15	May 5, 2008	176
D.15.1	Commands and Utilities for NCP Server and NCP Volumes	176
D.15.2	Configuring NCP Volumes for Novell Cluster Services Clusters	176
D.15.3	Managing NCP Volumes	177
D.15.4 Using Opportunistic Locking for NCP File Handling	177
D.16	February 12, 2008	178
D.16.1	Configuring NCP Volumes for Novell Cluster Services Clusters	178

About This Guide

Novell NCP Server services for Novell Open Enterprise Server (OES) 2 Linux enables users to access data on Linux file systems with the Novell Client by using the Novell trustee model for access control.

The following topics are included in this documentation:

- ♦ Chapter 1, “NCP Server for Linux Overview,” on page 13
- ♦ Chapter 2, “What’s New for NCP Server for Linux,” on page 15
- ♦ Chapter 3, “Installing and Configuring NCP Server for Linux,” on page 21
- ♦ Chapter 4, “Migrating Data from NSS Volumes to NCP Volumes on Linux File Systems,” on page 45
- ♦ Chapter 5, “Using NCP Server and NCP Volumes in a Virtualization Environment,” on page 49
- ♦ Chapter 6, “Planning for NCP Server and NCP Volumes,” on page 51
- ♦ Chapter 7, “Management Tools for NCP Server,” on page 53
- ♦ Chapter 8, “Managing NCP Server,” on page 63
- ♦ Chapter 9, “Managing Connections for NCP Volumes and NSS Volumes,” on page 67
- ♦ Chapter 10, “Managing NCP Volumes,” on page 81
- ♦ Chapter 11, “Configuring NCP Volumes with Novell Cluster Services,” on page 97
- ♦ Chapter 12, “Managing File System Trustees, Trustee Rights, and Attributes on NCP Volumes,” on page 111
- ♦ Chapter 13, “Using Opportunistic Locking for NCP File Handling,” on page 117
- ♦ Chapter 14, “Using the Inventory to Monitor NCP Volumes,” on page 121
- ♦ Chapter 15, “Troubleshooting for the NCP Server and NCP Volumes,” on page 129
- ♦ Chapter 16, “Security Considerations for NCP Server,” on page 131
- ♦ Appendix A, “Commands and Utilities for NCP Server and NCP Volumes,” on page 135
- ♦ Appendix B, “Additional NCP Server Commands and Options,” on page 163
- ♦ Appendix C, “RPM Files for NCP Server,” on page 167
- ♦ Appendix D, “Documentation Updates,” on page 169

Audience

This guide is intended for administrators who install, configure, and manage NCP Server and NCP volumes.

Feedback

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

Documentation Updates

The latest version of the *OES 2: NCP Server for Linux Administration Guide* is available on the [OES documentation Web site \(http://www.novell.com/documentation/oes2\)](http://www.novell.com/documentation/oes2).

Additional Information

For information on NCP features supported by NCP Server for Linux, see the *Novell Client 4.91 SP5 for Windows XP/2003 Installation and Administration Guide*, the *Novell Client 2 SP1 for Windows Administration Guide*, and the *Novell Client 2.0 SP3 for Linux Administration Guide*.

1 NCP Server for Linux Overview

On Novell Open Enterprise Server (OES) 2 for Linux servers, the NetWare Core Protocol (NCP) Server provides the same services that are available with NCP Server on NetWare. With NCP Server, you can define NCP volumes (NCP shares on Linux POSIX file systems) and use Novell Storage Services (NSS) volumes on Linux. Access to both types of volumes is controlled by using the Novell trustee model. Windows and Linux workstations running Novell Client software can access data and manage file sharing on OES 2 Linux servers just as they do on NetWare servers.

- ♦ [Section 1.1, “How NCP Server Works,” on page 13](#)
- ♦ [Section 1.2, “Benefits of NCP Server,” on page 13](#)
- ♦ [Section 1.3, “What’s Next,” on page 14](#)

1.1 How NCP Server Works

NCP has been used for years to manage access to the primary NetWare server resources. NCP makes procedure calls to the NetWare File Sharing Protocol (NFSP) that services requests for NetWare file and print resources. NCP is the principal protocol for transmitting information between a NetWare server and its clients.

NCP handles login requests and many other types of requests to the file system and the printing system. NCP is a client/server LAN protocol. Workstations create NCP requests and use TCP/IP to send them over the network. At the server, NCP requests are received, unpacked, and interpreted.

Services included with NCP are file access, file locking, security, tracking of resource allocation, event notification, synchronization with other servers, connection and communication, print services and queue management, and network management.

Novell Client software must be used to initiate a connection between a Windows or Linux workstation running Novell Client software and a Linux server running NCP Server services. Security and authentication issues require that linking clients to servers be a client/server application. Intelligence at both ends of the connection work together to verify that clients are who they claim to be, and that file controls are followed when using shared server files.

1.2 Benefits of NCP Server

NCP and Novell Client software together exceed the level of security and utility found in Windows, Macintosh, UNIX, or Linux networking. NCP and Novell Client software offer great benefits in ways that appeal to users and to managers.

If you look at the list of file attributes provided by NCP and NSS and then compare those to the file attributes in Windows, Macintosh, UNIX, or Linux networks, you will find that NCP and NSS provide much more control over files.

Some of the benefits provided by NCP Server on Linux include:

- ◆ Users can log in to the Linux network from the Novell Client workstation just like they do with NetWare. This means that for users familiar with a NetWare environment, there is no need to re-educate or retrain. There is also no need to reconfigure Novell Client workstations to access your Linux network.
- ◆ Users and administrators can map drives to volumes and directories on Linux servers just like they do on NetWare.
- ◆ NetWare-style login scripts can be created for users to automate drive mappings and other network functions.
- ◆ The file and directory attributes and rights that exist on NetWare are now available and configurable on Linux.
- ◆ Directory limits for individual users can be set and administered on Linux.
- ◆ The Novell Client provides the same functions to users of OES 2 Linux servers as are available for NetWare servers.

1.3 What's Next

For information about enhancements to NCP Server in this release, see [Chapter 2, “What’s New for NCP Server for Linux,”](#) on page 15.

For information on installing and configuring NCP Server on Linux, see [Chapter 3, “Installing and Configuring NCP Server for Linux,”](#) on page 21.

2 What's New for NCP Server for Linux

This section describes enhancements to the Novell NCP Server for Novell Open Enterprise Server (OES) 2 Linux.

- ♦ [Section 2.1, “What’s New in the May 2013 Patch Release,” on page 15](#)
- ♦ [Section 2.2, “What’s New in the April 2013 Patch Release,” on page 15](#)
- ♦ [Section 2.3, “What’s New in the January 2013 Patch Release,” on page 16](#)
- ♦ [Section 2.4, “What’s New in the January 2012 Patch Release,” on page 17](#)
- ♦ [Section 2.5, “What’s New in the October 2011 Patch Release,” on page 17](#)
- ♦ [Section 2.6, “What’s New in the August 2011 Patch Release,” on page 17](#)
- ♦ [Section 2.7, “What’s New \(OES 2 SP3 January Patch\),” on page 17](#)
- ♦ [Section 2.8, “What’s New \(OES 2 SP3\),” on page 17](#)
- ♦ [Section 2.9, “What’s New \(OES 2 SP2\),” on page 18](#)
- ♦ [Section 2.10, “What’s New \(OES 2 SP1\),” on page 18](#)
- ♦ [Section 2.11, “What’s New \(OES 2\),” on page 19](#)

2.1 What’s New in the May 2013 Patch Release

SLP Refresh Interval for Cluster Resource Virtual NCP Servers

NCP Server was modified to refresh its OpenSLP registration of cluster resource virtual NCP servers based on the setting for the eDirectory `advertise-life-time` (`n4u.nds.advertise-life-time`) parameter. The `n4u.nds.advertise-life-time` parameter is set by default to 3600 seconds (1 hour) and has a valid range of 1 to 65535 seconds. Previously, NCP Server re-registered the virtual NCP servers with SLP every 30 minutes regardless of the eDirectory `advertise-life-time` setting. For information about setting the eDirectory `advertise-life-time` parameter in a cluster, see “SLP” in the [OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux](#).

2.2 What’s New in the April 2013 Patch Release

Upgrade to eDirectory 8.8.7

An upgrade to Novell eDirectory 8.8 SP7 is available in the April 2013 Scheduled Maintenance for OES 2 SP3. For information about the eDirectory upgrade, see [TID 7011599](#) in the Novell Knowledgebase.

There will be no further eDirectory 8.8 SP6 patches for the OES platform. Previous patches for Novell eDirectory 8.8 SP6 are available on [Novell Patch Finder](#).

2.3 What's New in the January 2013 Patch Release

In addition to bug fixes, NCP Server has been modified to automatically log dismounts of NSS volumes and NCP volumes.

Upgrade to Novell iManager 2.7.6

The January 2013 Scheduled Maintenance for OES 2 SP3 includes a channel upgrade from Novell iManager 2.7.5 to Novell iManager 2.7.6.

Novell iManager 2.7.6 provides the following enhancements:

- ◆ Microsoft Internet Explorer 10 certification in the desktop user interface view on Windows 8 (excluding Windows 8 RT) and Windows Server 2012.
- ◆ Apple Safari 6.0 certification on Mac OSX Mountain Lion (version 10.8).
- ◆ iManager Workstation certification on Windows 8 Enterprise Edition (32-bit and 64-bit).
- ◆ iManager 2.7.6 support for Tomcat 7.0.32. and Java 1.7.0_04 versions.

iManager documentation links in this guide have been updated to reflect this change.

iManager 2.7.6 documentation is available on the [Web](#). For earlier iManager versions, see [Previous Releases](#).

Novell Client Support for Windows 8 and Server 2012

The January 2013 Scheduled Maintenance for OES 2 SP3 announces the availability of Novell Client 2 SP3 for Windows with support for:

- ◆ Windows 8 (32-bit and 64-bit) excluding Windows 8 RT
- ◆ Windows Server 2012 (64-bit)

Novell Client 2 documentation links in this guide have been updated to reflect the release of SP3.

Novell Client 2 SP3 for Windows documentation is available on the [Web](#). Documentation for earlier versions is available under [Previous Releases](#).

New Novell Cluster Services Plug-in for iManager 2.7.5 and Later

The Clusters plug-in for Novell iManager 2.7.5 or later supports the management of OES and NetWare clusters and resources. The availability of different cluster management features depends on the version of Novell Cluster Services and the server platform that are installed on the cluster being managed. A comparison of the old and new interface is available in “[What's New \(January 2013 Patches\)](#)” in the [OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux](#).

OES Client Services Support for Windows 8 and IE 10

In the January 2013 Scheduled Maintenance for OES 2 SP3, OES client services added support for user access from Windows 8 clients (excluding Windows 8 RT), with the exception of Domain Services for Windows (DSfW). DSfW was not tested with Windows 8 clients and does not support them.

Client applications are supported to run on Windows 8 clients in the desktop user interface view. Web-based client access is supported for the Internet Explorer 10 Web browser in the desktop user interface view for Windows 7 clients and Windows 8 clients.

OES Client Services Do Not Support Windows Server 2012

In the January 2013 Scheduled Maintenance for OES 2 SP3, OES client services were not tested with Windows Server 2012 servers. Client access support for Windows Server 2012 is not planned for OES 2 SP3.

2.4 What's New in the January 2012 Patch Release

- ♦ Modified Monitor Script to monitor the availability of NCP file services and it's related services.

2.5 What's New in the October 2011 Patch Release

- ♦ The maximum value of `CONCURRENT_ASYNC_REQUESTS` parameter has been increased to 256 from the earlier value of 128.

2.6 What's New in the August 2011 Patch Release

With the release of the August 2011 patches for OES 2 SP3, the base platform has been upgraded to SLES 10 SP4.

SLES 10 SP4 support is enabled by updating OES 2 SP3 servers with the `move-to-sles10-sp4` patch. Novell encourages customers to update to this latest set of patches. For more information, see ["Updating \(Patching\) an OES 2 SP3 Server"](#) in the *OES 2 SP3: Installation Guide*

SLES 10 SP4 is considered a lower-risk update that contains a set of consolidated bug fixes and support for newer hardware. It does not impact the kernel ABI or third-party certifications.

With the release of the August 2011 patches, OES 2 SP2 customers who upgrade to OES 2 SP3 via the `move-to` patch will receive the SLES 10 SP4 updates. New installations of OES 2 SP3, migrations to OES 2 SP3, and down-server upgrades to OES 2 SP3, should all be performed using SLES 10 SP4 media.

2.7 What's New (OES 2 SP3 January Patch)

New options added to manage NCP threads. For more information, see [Section A.1.6, "Managing NCP Threads,"](#) on page 138.

2.8 What's New (OES 2 SP3)

- ♦ Support to enable and disable write permissions on volumes using [NCPCON](#) utility.
- ♦ Addition of file path to close events
- ♦ Ability to disable login per volume
- ♦ NCP integration with CIFS for Shadow Volume (DST)
- ♦ **Auditing:** Support for IP Address Auditing and Close Written Flag and NSS File Handle

- ♦ **Directory Cache Management for NCP Server:** The default values for `MAXIMUM_CACHED_FILES_PER_SUBDIRECTORY`, `MAXIMUM_CACHED_FILES_PER_VOLUME`, and `MAXIMUM_CACHED_SUBDIRECTORIES_PER_VOLUME` is modified.

For more information, see [Section 3.4.1, “Directory Cache Management for NCP Server,”](#) on [page 30](#).

2.9 What’s New (OES 2 SP2)

- ♦ Cross-protocol locking is now enabled by default.

2.10 What’s New (OES 2 SP1)

The following enhancements for NCP Server are available in the OES 2 SP1 Linux release:

- ♦ [Section 2.10.1, “64-bit Support,”](#) on [page 18](#)
- ♦ [Section 2.10.2, “eDirectory 8.8.4,”](#) on [page 18](#)
- ♦ [Section 2.10.3, “Change in Syntax for Setting Inherit POSIX Permission,”](#) on [page 18](#)
- ♦ [Section 2.10.4, “Novell AFP Supports Cross-Protocol File Locking with NCP for NSS Volumes,”](#) on [page 18](#)

2.10.1 64-bit Support

NCP Server for OES 2 SP1 Linux is 64-bit enabled. Selecting NCP as part of a 64-bit installation installs 64-bit NCP. It requires Novell eDirectory 8.8 SP4.

2.10.2 eDirectory 8.8.4

This release supports eDirectory 8.8.4

2.10.3 Change in Syntax for Setting Inherit POSIX Permission

An equal sign (=) is no longer used in the `ncpcon change volume` command to set the Inherit POSIX Permissions parameter to on or off for an NCP volume.

2.10.4 Novell AFP Supports Cross-Protocol File Locking with NCP for NSS Volumes

Cross-protocol file locking is supported for the Novell Apple Filing Protocol (AFP) service that provides AFP access for Macintosh users to Novell Storage Services (NSS) volumes. This allows NCP users and AFP users to access files on an NSS volume and prevents them from concurrently modifying files by locking the file across protocols. It requires the following setup:

- ♦ NCP Server for Linux is installed and running.
- ♦ NSS for Linux is installed and running.
- ♦ Novell AFP is installed and running.

- ♦ Linux Samba is installed. It can be running or not running.
- ♦ The NCP cross-protocol file locking attribute is enabled by default. For information, see [Section 3.11, “Configuring Cross-Protocol File Locks for NCP Server,”](#) on page 40.

NOTE: For better performance, disable CPL if you do not use any other access protocol.

For information about installing and using Novell AFP for Linux, see the [OES 2 SP3: Novell AFP For Linux Administration Guide](#).

2.11 What’s New (OES 2)

The following enhancements for NCP Server are available in the initial release of Novell Open Enterprise Server 2 Linux:

- ♦ [Section 2.11.1, “Novell Dynamic Storage Technology,”](#) on page 19
- ♦ [Section 2.11.2, “NCP Server,”](#) on page 19

2.11.1 Novell Dynamic Storage Technology

Novell Dynamic Storage Technology allows rarely accessed files to be automatically moved, according to policies set by the administrator, from faster-access storage to lower-cost storage media where the files can be managed and backed up at a lower cost. You can set policies for when files are moved to secondary storage. The primary and secondary storage areas appear to users as a single unified file system.

For information about managing storage with Dynamic Storage Technology, see the [OES 2 SP3: Dynamic Storage Technology Administration Guide](#)

2.11.2 NCP Server

- ♦ You can modify the Inherit POSIX Permissions setting for files on NCP volumes, using Novell Remote Manager for Linux. See [Section 10.8, “Configuring Inherit POSIX Permissions for an NCP Volume,”](#) on page 89.
- ♦ File share modes have been added to lock files being accessed across protocols, such as between CIFS/Samba and NCP. See [Section 3.11, “Configuring Cross-Protocol File Locks for NCP Server,”](#) on page 40.
- ♦ The configurable DOS Archive Bit parameter is no longer available. Backups of NCP volumes should be done from the server, not an NCP client.

The NCP “execute only” bit is now used to provide the EXECUTE_ATTRIBUTE_SUPPORT parameter. The Novell Client for Linux uses this bit to represent the user mode execute bit on a file or subdirectory. For information, see [Section 3.8, “Configuring the Execute Only File Attribute for NCP Server,”](#) on page 37.

3 Installing and Configuring NCP Server for Linux

This section describes how to install and configure NCP Server for Linux on a Novell Open Enterprise Server (OES) 2 Linux server.

- ◆ [Section 3.1, “Installation Requirements for NCP Server for Linux,” on page 21](#)
- ◆ [Section 3.2, “Installing NCP Server,” on page 26](#)
- ◆ [Section 3.3, “Updating NCP Server,” on page 28](#)
- ◆ [Section 3.4, “Configuring Global NCP Server Parameters,” on page 29](#)
- ◆ [Section 3.5, “Restarting the Novell NCP/NSS IPC \(ncp2nss\) Daemon,” on page 35](#)
- ◆ [Section 3.6, “Restarting the Novell eDirectory \(ndsd\) Daemon,” on page 35](#)
- ◆ [Section 3.7, “Configuring the NCP Server Local Code Page,” on page 35](#)
- ◆ [Section 3.8, “Configuring the Execute Only File Attribute for NCP Server,” on page 37](#)
- ◆ [Section 3.9, “Configuring Sendfile Support for NCP Server,” on page 38](#)
- ◆ [Section 3.10, “Configuring Opportunistic Locking for NCP Server,” on page 39](#)
- ◆ [Section 3.11, “Configuring Cross-Protocol File Locks for NCP Server,” on page 40](#)
- ◆ [Section 3.12, “Modifying the NCP File Server Name,” on page 42](#)
- ◆ [Section 3.13, “Modifying the sys: Volume Mount Point,” on page 43](#)

3.1 Installation Requirements for NCP Server for Linux

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

- ◆ [Section 3.1.1, “Supported Platforms,” on page 22](#)
- ◆ [Section 3.1.2, “NCP Server and Dynamic Storage Technology,” on page 22](#)
- ◆ [Section 3.1.3, “Static Hostname and the NCP File Server Name,” on page 22](#)
- ◆ [Section 3.1.4, “64-Bit Support,” on page 22](#)
- ◆ [Section 3.1.5, “Novell eDirectory 8.8.4,” on page 22](#)
- ◆ [Section 3.1.6, “eDirectory Rights Needed by a Container Administrator,” on page 23](#)
- ◆ [Section 3.1.7, “Novell Storage Services,” on page 23](#)
- ◆ [Section 3.1.8, “Novell Samba,” on page 23](#)
- ◆ [Section 3.1.9, “Linux User Management,” on page 24](#)
- ◆ [Section 3.1.10, “Novell AFP,” on page 24](#)
- ◆ [Section 3.1.11, “Novell Cluster Services for Linux,” on page 24](#)
- ◆ [Section 3.1.12, “SLP,” on page 24](#)

- [Section 3.1.13, “Novell iManager 2.7 for Linux,” on page 26](#)
- [Section 3.1.14, “Novell Remote Manager for Linux,” on page 26](#)
- [Section 3.1.15, “OpenWBEM,” on page 26](#)
- [Section 3.1.16, “Other OES 2 Linux Services,” on page 26](#)

3.1.1 Supported Platforms

NCP Server for Linux supports OES 2 Linux and later.

3.1.2 NCP Server and Dynamic Storage Technology

The NetWare Core Protocol (NCP) Server for Linux provides the NCP services for NSS volumes on Linux and for NCP volumes on Linux POSIX file systems. Dynamic Storage Technology (DST) is a component of NCP Server. Using DST is optional, but NCP Server must be installed and running in order for DST to work.

For information about managing Dynamic Storage Technology, see the [OES 2 SP3: Dynamic Storage Technology Administration Guide](#).

3.1.3 Static Hostname and the NCP File Server Name

During the OES 2 Linux install, you assign a static IP address (IPv4 or IPv6), a hostname, and domain name to the server. NCP Server uses the server hostname (such as `server1`) as the NCP File Server Name, and generally considers that the hostname never changes. If you modify the hostname after the install, you must also modify the NCP File Server Name parameter. For information, see [Section 3.12, “Modifying the NCP File Server Name,” on page 42](#).

IMPORTANT: Modifying the IP address or hostname for an existing server impacts most services, not just NCP Server.

3.1.4 64-Bit Support

Selecting NCP Server as part of a 64-bit installation automatically installs 64-bit NCP server.

3.1.5 Novell eDirectory 8.8.4

NCP Server manages data access for NCP volumes, Dynamic Storage Technology (DST) shadow volumes, and Novell Storage Services (NSS) volumes. NCP Server restricts data access to users who have User objects defined in Novell eDirectory. For information about configuring eDirectory and users, see the [Novell eDirectory 8.8 Administration Guide](#).

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

3.1.6 eDirectory Rights Needed by a Container Administrator

A container administrator (or non-administrator user) needs the following eDirectory rights to install and manage the NCP and Dynamic Storage Technology service on an OES 2 SP3 Linux server:

- ♦ Object Create right on the container where the NCP Server objects are.
- ♦ Object Create right where the cluster container will be.

A container administrator (or non-administrator user) needs the following eDirectory rights to manage an NCP volume on an OES 2 SP3 Linux server:

- ♦ Object Write and Modify rights on the Volume object.

For example, to create an NCP volume NCPVOL1 in the container `sales.mycompany.com`, the administrator must have Create right on the Container object `sales` and the Write and Modify rights on the Volume object NCPVOL1.

The container administrator must be Linux-enabled with Linux User Management (LUM) and be added to the LUM `admingroup` for the server.

NOTE: If the eDirectory administrator username or password contains special characters (such as \$, #, and so on), make sure to escape each special character by preceding it with a backslash (\) when you enter credentials.

3.1.7 Novell Storage Services

Novell Storage Services (NSS) requires NCP Server; however, NSS is not required for using NCP Server with NCP volumes on Linux file systems.

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

For information about installing NSS, see [“Installing and Configuring Novell Storage Services”](#) in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

3.1.8 Novell Samba

You can install and configure Novell Samba to provide file access for CIFS/Samba users to NCP volumes. For information about configuring Samba services, see the *OES2 SP3: Samba Administration Guide*.

If both NCP users and Samba/CIFS users access the same NCP volume or NSS volume, you should enable cross-protocol file locking for NCP. For information, see [Section 3.11, “Configuring Cross-Protocol File Locks for NCP Server,”](#) on page 40.

NCP uses the `sambasharemodes.so` library file to support the cross-protocol file locking capability that coordinates access to files by NCP users and CIFS/Samba users. NCP updates that are released through the OES 2 Linux and later update channels and in support packs include the `sambasharemodes.so` library file that you need for NCP. Patches for Linux Samba are also released separately through the SUSE Linux Enterprise Server 10 SP1 and later update channels. For 32-bit OES 2 Linux and later, it is okay to accept Samba updates separately. However, for 64-bit OES 2 Linux and later, there is a risk of breaking the cross-protocol locks functionality if the `sambasharemodes.so` library file is modified from the version released with NCP.

3.1.9 Linux User Management

Users must be Linux-enabled with Linux User Management in order to access data via CIFS/Samba protocols. Linux User Management is selected and installed automatically when you install NCP Server and Dynamic Storage Technology. For information about Linux-enabling users with Linux User Management, see the [OES 2 SP3: Novell Linux User Management Administration Guide](#).

3.1.10 Novell AFP

Cross-protocol file locking is supported for the Novell Apple Filing Protocol (AFP) service that provides AFP access for Macintosh users to NSS volumes. This allows NCP users and AFP users to access files on an NSS volume and prevents them from concurrently modifying files by locking the file across protocols. It requires the following setup:

- ♦ NCP Server for Linux is installed and running.
- ♦ NSS for Linux is installed and running.
- ♦ Novell AFP is installed and running.
- ♦ Linux Samba is installed. It can be running or not running.
- ♦ The NCP cross-protocol file locking attribute is enabled. For information, see [Section 3.11, “Configuring Cross-Protocol File Locks for NCP Server,”](#) on page 40.

For information about installing and using Novell AFP for Linux, see the [OES 2 SP3: Novell AFP For Linux Administration Guide](#).

3.1.11 Novell Cluster Services for Linux

NCP Server supports the sharing of NSS volumes on Linux, NCP volumes on Linux POSIX file systems, and DST shadow volumes in clusters with Novell Cluster Services for Linux. NCP Server itself is not clustered, and must be installed and configured on each OES 2 Linux node in the cluster where you plan to fail over these volumes.

For information about configuring NCP volumes in cluster resources, see [Chapter 11, “Configuring NCP Volumes with Novell Cluster Services,”](#) on page 97.

For information about configuring DST shadow volumes in cluster resources, see [“Configuring DST Shadow Volumes with Novell Cluster Services for Linux”](#) in the [OES 2 SP3: Dynamic Storage Technology Administration Guide](#).

For information about configuring NSS volumes in cluster resources, see [“Configuring Cluster Resources for Shared NSS Pools and Volumes”](#) in the [OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux](#).

For information about installing and managing Novell Cluster Services for Linux, see [OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux](#).

3.1.12 SLP

SLP (Service Location Protocol) is a required component for Novell Cluster Services on Linux when you are using NCP to access file systems on cluster resources. NCP requires SLP for the `ncpcon bind` and `ncpcon unbind` commands in the cluster load and unload scripts. For example, NCP is needed for NSS volumes and for NCP volumes on Linux POSIX file systems.

SLP is not automatically installed when you select Novell Cluster Services. SLP is installed as part of the Novell eDirectory configuration during the OES 2 Linux install. You can enable and configure SLP on the eDirectory Configuration - NTP & SLP page. For information, see “[Specifying SLP Configuration Options](#)” in the *OES 2 SP3: Installation Guide*.

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

The SLP daemon (`slpd`) must also be installed and running on all nodes in the cluster when you manage the cluster or cluster resources.

NCP Server re-registers cluster resource virtual NCP servers with SLP based on the setting for the eDirectory `advertise-life-time` (`n4u.nds.advertise-life-time`) parameter. The parameter is set by default to 3600 seconds (1 hour) and has a valid range of 1 to 65535 seconds.

You can use the `ndsconfig set` command to set the `n44.nds.advertise-life-time` parameter. To reset the parameter in a cluster, perform the following tasks on each node of the cluster:

- 1 Log in to the node as the `root` user, then open a terminal console.
- 2 Take offline all of the cluster resources on the node, or cluster migrate them to a different server. At a command prompt, enter

```
cluster offline <resource_name>
```

or

```
cluster migrate <resource_name> <target_node_name>
```

- 3 Modify the eDirectory SLP advertising timer parameter (`n4u.nds.advertise-life-time`), then restart `nds` and `slpd`. At a command prompt, enter

```
ndsconfig set n4u.nds.advertise-life-time=<value_in_seconds>
```

```
rcnds restart
```

```
rcslpd restart
```

- 4 Bring online all of the cluster resources on the node, or cluster migrate the previously migrated resources back to this node.

```
cluster online <resource_name>
```

or

```
cluster migrate <resource_name> <node_name>
```

- 5 Repeat the previous steps on the other nodes in the cluster.

OpenSLP stores the registration information in cache. You can configure the SLP Directory Agents to preserve a copy of the database when the SLP daemon (`slpd`) is stopped or restarted. This allows SLP to know about registrations immediately when it starts.

For more information about configuring and managing SLP, see “[Configuring OpenSLP for eDirectory](#)” in the *Novell eDirectory 8.8 SP7 Administration Guide*.

3.1.13 Novell iManager 2.7 for Linux

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

3.1.14 Novell Remote Manager for Linux

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

For information about using Novell Remote Manager for Linux, see the [OES 2 SP3: Novell Remote Manager for Linux Administration Guide](#). For information about management options for NCP Server, see [Section 7.1.4, “Quick Reference for the NCP Server Plug-In for Novell Remote Manager for Linux,”](#) on page 54.

3.1.15 OpenWBEM

In OES 2 Linux, OpenWBEM is a PAM-enabled Linux utility that must be enabled and running on the OES 2 Linux server when managing services with Novell Remote Manager for Linux and Novell iManager. During the install, make sure you enable OpenWBEM (the default) when configuring Linux services. For information, see [“Services in OES 2 That Require LUM-Enabled Access”](#) in the [.OES 2 SP3: Planning and Implementation Guide](#)

3.1.16 Other OES 2 Linux Services

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

3.2 Installing NCP Server

- ♦ [Section 3.2.1, “Preparing for the OES 2 Install,”](#) on page 26
- ♦ [Section 3.2.2, “Installing NCP Server at Install Time,”](#) on page 27
- ♦ [Section 3.2.3, “Installing NCP Server on an Existing OES 2 Linux Server,”](#) on page 28

3.2.1 Preparing for the OES 2 Install

[Table 3-1](#) identifies settings for the OES 2 Linux server that are used as the default settings for NCP Server at install time, and are written to the `/etc/opt/novell/ncpserv.conf` file. This file specifies parameters that enable file systems on Linux to be available to workstations that connect to it via the Novell Client or the Microsoft NCP Client. It helps enforce the Novell trustee model of file access for NCP users and CIFS/Samba users.

You can change the settings for these parameters as needed to ensure that workstations on the network can access the server. If you later modify the settings for the server, you must re-configure them for NCP Server, too.

Table 3-1 Server Settings Used by NCP Server

Linux Server Setting	NCP Server Parameter Entry in <code>npserv.conf</code>	Reference
Server Hostname	<code>NCP_FILE_SERVER_NAME hostname</code>	Section 3.12, "Modifying the NCP File Server Name," on page 42
Server local code page	<code>LOCAL_CODE_PAGE code</code>	Section 3.7, "Configuring the NCP Server Local Code Page," on page 35
<code>SYS</code> : volume mount point	<code>VOLUME sys /usr/novell/sys</code>	Section 3.13, "Modifying the <code>sys</code> : Volume Mount Point," on page 43

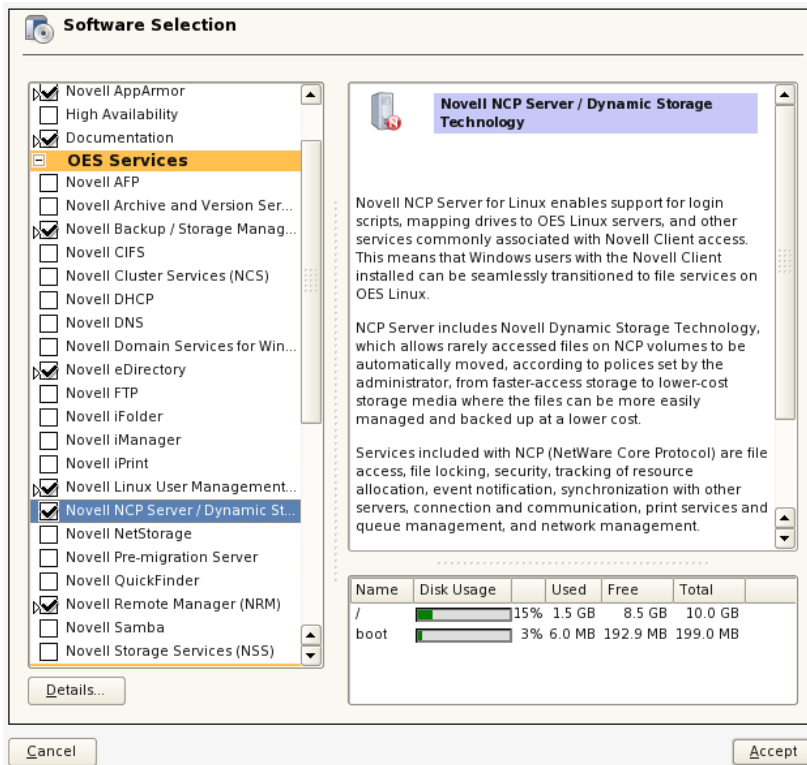
3.2.2 Installing NCP Server at Install Time

NCP Server for Linux can be installed during the OES 2 Linux installation. For general install instructions, see the [OES 2 SP3: Installation Guide](#).

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

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

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



- 3 If you plan to use NSS volumes, select *Novell Storage Services* from the *OES Services* options.

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

- 4 If you plan to provide access for CIFS/Samba users to NSS volumes on Linux, NCP volumes on Linux POSIX file systems, or DST shadow volumes, select *Novell Samba* from the *OES Services* options.
- 5 Optionally select *Novell iManager* from the *OES Services* options.
You must install Novell iManager somewhere in your network, but it is not necessary to install it on every server.
- 6 If you plan to configure NSS volumes on Linux, NCP volumes on Linux POSIX file systems, or DST shadow volumes on a cluster node, select *Novell Cluster Services (NCS)* from the *OES Services* options.
- 7 Click *Finish* to continue with the installation.

3.2.3 Installing NCP Server on an Existing OES 2 Linux Server

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

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

For general instructions for installing and configuring OES 2 components on an existing OES 2 Linux server, see [“Installing or Configuring OES 2 SP3 on an Existing Server”](#) in the *OES 2 SP3: Installation Guide*.

3.3 Updating NCP Server

NCP uses the `sambasharemodes.so` library file to support the cross-protocol file locking capability that coordinates access to files by NCP users and CIFS/Samba users. NCP updates that are released through the OES 2 Linux and later update channels and in support packs include the `sambasharemodes.so` library file that you need for NCP. Patches for Linux Samba are also released separately through the SUSE Linux Enterprise Server 10 SP1 and later update channels. For 32-bit OES 2 Linux and later, it is okay to accept Samba updates separately. However, for 64-bit OES 2 Linux and later, there is a risk of breaking the cross-protocol locks functionality if the `sambasharemodes.so` library file is modified from the version released with NCP.

3.4 Configuring Global NCP Server Parameters

- ◆ [Section 3.4.1, “Directory Cache Management for NCP Server,” on page 30](#)
- ◆ [Section 3.4.2, “Dynamic Storage Technology for NCP Server,” on page 30](#)
- ◆ [Section 3.4.3, “Locks Management for File Access on NCP Server,” on page 32](#)
- ◆ [Section 3.4.4, “Logs for NCP Server Events,” on page 32](#)
- ◆ [Section 3.4.5, “NCP Communications,” on page 33](#)
- ◆ [Section 3.4.6, “NCP Server Environment,” on page 33](#)
- ◆ [Section 3.4.7, “NCP Volumes,” on page 34](#)
- ◆ [Section 3.4.8, “NCP Volumes Low-Space Warning,” on page 34](#)

NCP Server provides several global parameters for the SET utility that can be used to customize NCP Server for a given server. Initially, the parameters and default settings are in force, but the parameters are not explicitly added to the `/etc/opt/novell/ncpserv.conf` file. After you modify its default setting, an entry for the parameter and its new setting are added to the file. The parameter entry remains in the file even if you modify the setting back to the default.

IMPORTANT: If you use NCP Server in a cluster, make sure to set the same global policies on each OES 2 Linux node in the cluster where you plan to fail over the shared volumes.

There are three methods available for modifying parameter settings:

- ◆ **Novell Remote Manager:** You can view or modify server-level parameters by using Novell Remote Manager for Linux. Select *Manage NCP Services > Manage Server*, then select the *Parameter Value* link for the parameter in order to modify the setting. When you modify settings from Novell Remote Manager, NCP Server automatically restarts the Novell eDirectory daemon and the Novell NCP/NSS IPC daemon (if NSS is installed).
- ◆ **Command Line:** You can also modify the setting from its default value by adding the parameter using the `ncpcon set` command.

```
ncpcon set parameter_name=value
```

Replace *parameter_name* and *value* with the settings you want to change. NCP Server automatically restarts the Novell eDirectory daemon and the Novell NCP/NSS IPC daemon (if NSS is installed). These commands are dynamic.

- ◆ **Edit the Configuration File:** You can also modify the setting from its default value by adding the parameter to the `/etc/opt/novell/ncpserv.conf` file, then specifying the new value.

If you modify the `/etc/opt/novell/ncpserv.conf` file, you must restart the Novell eDirectory daemon to make the changes go into effect. For information, see [Section 3.6, “Restarting the Novell eDirectory \(ndsd\) Daemon,” on page 35](#).

When NSS is installed and running, and you modify values for any of the NCP Server parameters by directly editing the `/etc/opt/novell/ncpserv.conf` file, you must manually restart `ncp2nss`. For information, see [Section 3.5, “Restarting the Novell NCP/NSS IPC \(ncp2nss\) Daemon,” on page 35](#).

The following sections identify the global NCP Server parameters with their default values and valid options. For additional information about each parameter, see [Section A.2, “NCPCON SET Parameters,” on page 153](#).

- ◆ [Section 3.4.1, “Directory Cache Management for NCP Server,” on page 30](#)
- ◆ [Section 3.4.2, “Dynamic Storage Technology for NCP Server,” on page 30](#)
- ◆ [Section 3.4.3, “Locks Management for File Access on NCP Server,” on page 32](#)

- ♦ [Section 3.4.4, “Logs for NCP Server Events,” on page 32](#)
- ♦ [Section 3.4.5, “NCP Communications,” on page 33](#)
- ♦ [Section 3.4.6, “NCP Server Environment,” on page 33](#)
- ♦ [Section 3.4.7, “NCP Volumes,” on page 34](#)
- ♦ [Section 3.4.8, “NCP Volumes Low-Space Warning,” on page 34](#)

3.4.1 Directory Cache Management for NCP Server

Table 3-2 Server Parameter Information for Directory Cache Management

Parameter Name and Description	Default Value	Value Options
MAXIMUM_CACHED_FILES_PER_SUBDIRECTORY Controls the maximum number of file entries that can be cached by the system for a given folder in the directory cache.	10240	Minimum is 512 files.
MAXIMUM_CACHED_FILES_PER_VOLUME Controls the maximum number of file entries that can be cached by the system for a given volume in the directory cache.	256000	Minimum is 2048 files.
MAXIMUM_LAZY_CLOSE_FILES Controls the maximum number of files' handles that can be lazy closed in the directory cache.	4096	16 to 64000
MAXIMUM_CACHED_SUBDIRECTORIES_PER_VOLUME Controls the maximum number of folder entries that can be cached by the system for a volume in the directory cache.	102400	4096
LOG_CACHE_STATISTICS Controls whether cache statistics are logged in the <code>ncpserv.log</code> file.	0	0 - Disable 1 - Enable

3.4.2 Dynamic Storage Technology for NCP Server

For information about configuring global policies for DST, see the [OES 2 SP3: Dynamic Storage Technology Administration Guide](#).

Table 3-3 Server Parameter Information for Dynamic Storage Technology

Parameter Name and Description	Default Value	Value Options
<p>DUPLICATE_SHADOW_FILE_ACTION</p> <p>Controls how duplicate files conflicts are handled.</p>	0	<p>0 - Show duplicate shadow files (default)</p> <p>1 - Hide duplicate shadow files</p> <p>2 - Rename duplicate shadow files</p> <p>3 - Delete duplicate files from shadow area</p> <p>4 - Move duplicate shadow files to / ._DUPLICATE_FILES</p>
<p>DUPLICATE_SHADOW_FILE_BROADCAST</p> <p>Controls whether broadcast messages are sent to NCP users whenever duplicate files conflicts occur.</p>	1	<p>0 - Disable</p> <p>1 - Enable</p>
<p>REPLICATE_PRIMARY_TREE_TO_SHADOW</p> <p>Controls how the primary tree is replicated from the primary tree to the shadow tree. By default, it is disabled, and paths are replicated to the secondary storage area when data is actually moved from the primary location to the secondary location. If it is enabled, the entire tree is replicated even if no files in a path have been moved to the secondary storage location.</p>	0	<p>0 - Disable</p> <p>1 - Enable</p>
<p>SHIFT_ACCESSED_SHADOW_FILES</p> <p>Controls whether files are moved from the secondary volume to the primary volume if the volume is accessed twice during a specified elapsed time. Use SHIFT_DAYS_SINCE_LAST_ACCESS to specify the time period. The file is moved after it is closed.</p>	0	<p>0 - Disable</p> <p>1 - Enable</p>
<p>SHIFT_MODIFIED_SHADOW_FILES</p> <p>Controls whether files are moved from the secondary volume to the primary volume if the file is modified. The file is moved after it is closed.</p>	1	<p>0 - Disable</p> <p>1 - Enable</p>
<p>SHIFT_DAYS_SINCE_LAST_ACCESS</p> <p>Specifies the number of elapsed days during which a file must be accessed twice before it is moved. This applies only if SHIFT_ACCESSED_SHADOW_FILES is enabled.</p>	1	<p>0 - Disable</p> <p>1 to 365 (in days)</p>

3.4.3 Locks Management for File Access on NCP Server

Table 3-4 Server Parameter Information for Locks Management

Parameter Name and Description	Default Value	Value Options
<p>CROSS_PROTOCOL_LOCKS</p> <p>Controls cross-protocol file locking support with Samba.</p> <p>Cross-protocol locks help prevent the same file from being concurrently accessed for modifications from both a Samba and NCP client.</p>	1	<p>1 - Enable</p> <p>0 - Disable</p>
<p>OPLOCK_SUPPORT_LEVEL</p> <p>Controls NCP opportunistic locking.</p>	2	<p>0 - Disable</p> <p>1 - Exclusive locks</p> <p>2 - Shared and exclusive locks</p>
<p>MAXIMUM_FILE_LOCKS_PER_CONNECTION</p>	1000	<p>This value is hard coded. Modifying the value has no effect.</p>

3.4.4 Logs for NCP Server Events

Table 3-5 Server Parameter Information for Logging NCP Server Events

Parameter Name and Description	Default Value	Value Options
<p>LOG_LEVEL</p> <p>Controls the nature and types of messages that are logged to the /var/opt/novell/log/ncpserv.log file.</p>	WARN	<p>Each level logs entries for its level and the levels above it.</p> <p>NOTHING</p> <p>ERROR</p> <p>WARNING</p> <p>INFO</p> <p>DEBUG</p> <p>ALL</p>
<p>LOG_CACHE_STATISTICS</p> <p>Controls whether cache statistics are logged in the ncpserv.log file.</p>	0	<p>0 - Disable</p> <p>1 - Enable</p>
<p>LOG_IDBROKER_ERRORS</p> <p>Controls whether ID broker errors are logged in the ncpserv.log file.</p>	0	<p>0 - Disable</p> <p>1 - Enable</p>
<p>LOG_MAXIMUM_FILE_SIZE</p> <p>This parameter is used to control the maximum size of the ncpserv.log file in bytes. The default is 4 MB.</p>	4000000	<p>Maximum file size in bytes.</p>

Parameter Name and Description	Default Value	Value Options
LOG_MEMORY_STATISTICS	0	0 - Disable
Controls whether memory statistics are logged in the <code>ncpserver.log</code> file.		1 - Enable
LOG_TIMESTAMPS	1	0 - Disable
Enables or disables timestamps for each message. With this parameter turned on, a timestamp is appended to each message.		1 - Enable

3.4.5 NCP Communications

Table 3-6 Server Parameter Information for Communications

Parameter Name and Description	Default Value	Value Options
FIRST_WATCHDOG_PACKET	0	0 - Disable
Controls how long to wait in minutes of inactivity before checking to see if an NCP connection is still alive.		1-120(minutes) - Enable
DISABLE_BROADCAST	0	0 - Disable
Controls the ability to broadcast messages from the NCP Server.		1 - Enable

3.4.6 NCP Server Environment

Table 3-7 Server Parameter Information for the NCP Server Environment

Parameter Name and Description	Default Value	Value Options
ALLOW_UTF8	1	0 - Disable
Controls UTF-8 support for file names. When ALLOW_UTF8 is enabled, you must also enable UTF8 support in the Novell Client. If you want the server to support clients from different locales (code pages) and allow them to share files, you must use the UTF-8 NCPs.		1 - Enable
LOCAL_CODE_PAGE	CP437	Valid language codes
Controls which base code page is used by the NCP Server.		
NCP_FILE_SERVER_NAME	Server hostname	This setting must match the server hostname, such as <code>server1</code> .
This parameter is set by eDirectory when the NCP Server is installed, and must not be modified arbitrarily.		
For information, see Section 3.12, "Modifying the NCP File Server Name," on page 42.		

3.4.7 NCP Volumes

Table 3-8 Server Parameter Information for Volume and File Management

Parameter Name and Description	Default Value	Value Options
COMMIT_FILE	0	0 - Disable 1 - Enable
EXECUTE_ATTRIBUTE_SUPPORT	1	0 - Disable 1 - Enable
KEEP_NSS_FILE_DELETOR_IDS	1	0 - Disable 1 - Enable
SENDFILE_SUPPORT	0	0 - Disable 1 - Enable
SYNC_TRUSTEES_TO_NSS_AT_VOLUME_MOUNT	0	0 - Disable 1 - Enable
Controls trustee resynchronization for an NSS volume when it is mounted for NCP.		
VOLUME_GONE_WARN_USERS	1	0 - Disable 1 - Enable
Controls whether a message is broadcast to warn users when the volume path is no longer present.		

3.4.8 NCP Volumes Low-Space Warning

Table 3-9 Server Parameter Information for Volume Low-Space Warning

Parameter Name and Description	Default Value	Value Options
VOLUME_EMPTY_WARN_USERS	1	0 - Disable 1 - Enable
Controls whether a message is broadcast to warn users when no volume space is available.		
VOLUME_LOW_WARN_USERS	1	0 - Disable 1 - Enable
Controls whether a message is broadcast to warn users when volume space is low.		
VOLUME_LOW_WARNING_RESET_THRESHOLD	128	0 to 100000
Sets the high watermark threshold (in MB), which is the level where the low watermark threshold is reset, and users no longer receive the low-space message.		
VOLUME_LOW_WARNING_THRESHOLD	64	0 to 100000
Sets the low watermark threshold (in MB) that indicates space is low.		

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

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

- 1 On the OES 2 Linux server, open a terminal console, then log in as the root user.
- 2 At the terminal console prompt, enter

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

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

```
Shutting down Novell NCP/NSS IPC daemon...
Exited
Starting the Novell NCP/NSS IPC daemon.
```

3.6 Restarting the Novell eDirectory (ndsd) Daemon

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

Use the following steps to stop and start `ndsd` when a single instance is running.

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

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

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

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

3.7 Configuring the NCP Server Local Code Page

NCP Server supports most commonly used code pages. NCP Server by default uses the code page corresponding to the code page used by the Linux server operating system that is specified at install time.

For example, if the Linux server is installed as a Japanese server, NCP Server uses the shift-JIS as its local code page. If the Linux server is installed as a French server, NCP Server uses the CP850 as its local code page.

Some examples of code page are CP437, CP850, CP737, CP866, CP874, CP949, SJIS, BIG5, and GBK. For a complete list of available code pages, open a terminal console, then enter

```
iconv --list | more
```

If you want NCP Server to use a code page that might be different than the one that is set for the server, you must specify that code page in the `/etc/opt/novell/ncpserv.conf` configuration file. After you modify it from its initial setting, the code page for the NCP Server does not change if you change the code page used for the server. You must modify the settings separately as needed.

- ♦ [Section 3.7.1, “Using Novell Remote Manager for Linux to Configure the Local Code Page,” on page 36](#)
- ♦ [Section 3.7.2, “Editing the `/etc/opt/novell/ncpserv.conf` File to Configure the Local Code Page,” on page 36](#)

3.7.1 Using Novell Remote Manager for Linux to Configure the Local Code Page

To set the parameter by using Novell Remote Manager for Linux:

- 1 In a Web browser, access Novell Remote Manager for Linux on the server, then log in as the root user.
The URL is the IP address of the server (such as 192.168.1.1) and port 8009.

```
https://192.168.1.1:8009
```
- 2 Select *Manage NCP Services > Manage Server* to view the *Server Parameter Information*.
- 3 Click the link for the `LOCAL_CODE_PAGE` setting.
- 4 In *New Value*, type the new code value you want to use for NCP Server, then click *Change*.
- 5 On the *Server Parameter Information* page, verify that the new setting is displayed for the `LOCAL_CODE_PAGE` parameter.

3.7.2 Editing the `/etc/opt/novell/ncpserv.conf` File to Configure the Local Code Page

To manually edit the value in the `/etc/opt/novell/ncpserv.conf` file:

- 1 Open the `/etc/opt/novell/ncpserv.conf` configuration file in a text editor.
- 2 Add the following command line:

```
LOCAL_CODE_PAGE Code_Page
```

Replace *Code_Page* with the code page you want to use for the NCP Server. It can be the same or different than the code page currently assigned.

- 3 Save the file.
- 4 Restart the Novell eDirectory (`nds`) Daemon by entering the following commands:

```
/etc/init.d/nds stop  
  
/etc/init.d/nds start
```

3.8 Configuring the Execute Only File Attribute for NCP Server

The NCP “execute only” attribute can be associated with the user mode execute bit on a file or subdirectory. With this setting turned on, NCP clients can set or clear this bit. The Novell Client for Linux uses this bit to represent the user mode execute bit on a file or subdirectory.

The Execute Only file attribute for NCP Server is enabled by default. You can enable or disable support for the attribute with the *Execute_Attribute_Support* option in the `/etc/opt/novell/ncpserv.conf` configuration file.

- ♦ [Section 3.8.1, “Using Novell Remote Manager for Linux to Configure the Execute Attribute Support,” on page 37](#)
- ♦ [Section 3.8.2, “Editing the `/etc/opt/novell/ncpserv.conf` File to Configure the Execute Attribute Support,” on page 37](#)

3.8.1 Using Novell Remote Manager for Linux to Configure the Execute Attribute Support

- 1 In a Web browser, access Novell Remote Manager for Linux on the server, then log in as the root user.

The URL is the IP address of the server (such as 192.168.1.1) and port 8009.

```
https://192.168.1.1:8009
```

- 2 Select *Manage NCP Services > Manage Server* to view the *Server Parameter Information*.
- 3 Click the link for the *EXECUTE_ATTRIBUTE_SUPPORT* setting.
- 4 In *New Value*, type a 0 (disable) or 1 (enable), then click *Change*.
- 5 On the *Server Parameter Information* page, verify that the new setting is displayed for the *EXECUTE_ATTRIBUTE_SUPPORT* parameter.

3.8.2 Editing the `/etc/opt/novell/ncpserv.conf` File to Configure the Execute Attribute Support

You can enable or disable support for the Execute Only attribute by manually editing the value for the *EXECUTE_ATTRIBUTE_SUPPORT* parameter in the `/etc/opt/novell/ncpserv.conf` file.

- 1 Open the `/etc/opt/novell/ncpserv.conf` configuration file in a text editor.
- 2 If the *EXECUTE_ATTRIBUTE_SUPPORT* parameter is not present, add the following line as the default setting of enabled:

```
EXECUTE_ATTRIBUTE_SUPPORT 1
```

- 3 You can optionally disable support, by changing the value from 1 to 0.

```
EXECUTE_ATTRIBUTE_SUPPORT 0
```

- 4 Save the file.
- 5 Restart the Novell eDirectory (ndsd) Daemon by entering the following commands:

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

3.9 Configuring Sendfile Support for NCP Server

The Linux `sendfile()` API improves the performance for file reads. `sendfile()` support is disabled by default.

Samba has had problems in the past with `sendfile()`. If you enable `sendfile()` and experience problems with Samba, you can disable `sendfile()` support in the `/etc/opt/novell/ncpserv.conf` configuration file.

- ♦ [Section 3.9.1, “Using Novell Remote Manager for Linux to Configure Sendfile Support,” on page 38](#)
- ♦ [Section 3.9.2, “Editing the `/etc/opt/novell/ncpserv.conf` File to Configure Sendfile Support,” on page 38](#)

3.9.1 Using Novell Remote Manager for Linux to Configure Sendfile Support

- 1 In a Web browser, access Novell Remote Manager for Linux on the server, then log in as the root user.

The URL is the IP address of the server (such as 192.168.1.1) and port 8009.

```
https://192.168.1.1:8009
```

- 2 Select *Manage NCP Services > Manage Server* to view the *Server Parameter Information*.
- 3 Click the link for the `SENDFILE_SUPPORT` setting.
- 4 In *New Value*, type a 0 (disable) or 1 (enable), then click *Change*.
- 5 On the *Server Parameter Information* page, verify that the new setting is displayed for the `SENDFILE_SUPPORT` parameter.

3.9.2 Editing the `/etc/opt/novell/ncpserv.conf` File to Configure Sendfile Support

You can enable or disable `sendfile()` API support by manually adding or editing the value for the `SENDFILE_SUPPORT` parameter in the `/etc/opt/novell/ncpserv.conf` file.

- 1 On the OES 2 Linux server, log in as the root user.
- 2 Open the `/etc/opt/novell/ncpserv.conf` configuration file in a text editor.
For example, to use `gedit`, open a terminal console, then enter

```
gedit /etc/opt/novell/ncpserv.conf
```

- 3 If the `SENDFILE_SUPPORT` parameter is not present, add the following line as the default setting of disabled:

```
SENDFILE_SUPPORT 0
```

- 4 You can optionally enable `sendfile` support by changing the value from 0 to 1.

```
SENDFILE_SUPPORT 1
```

- 5 Save the file.
- 6 Restart the Novell eDirectory (`nds`) Daemon by entering the following commands:

```
/etc/init.d/nds stop  
  
/etc/init.d/nds start
```

- 7 Synchronize the change with NSS by restarting `/etc/init.d/ncp2nss`. At a terminal console prompt, enter the following as the root user:

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

3.10 Configuring Opportunistic Locking for NCP Server

Opportunistic locking (oplocks) provides a way to cache file data at the client. It improves file access performance because it allows the client to read and write data using its local cache, and interact with the file server only when necessary, which reduces the amount of traffic on the network. Oplocks is enabled by default in NCP Server.

IMPORTANT: To use oplocks effectively, make sure users are running Novell Client 4.2 SP2 and later.

There are two levels of oplocks available with NCP Server. You can set oplocks to either of these levels or disable oplocks completely. By default, oplocks is set to level 2, which includes both level 1 and level 2 functionality.

For more information on oplocks with NCP Server, see [Section 13.1, “Understanding Opportunistic Locking for NCP Connections,”](#) on page 117.

- ♦ [Section 3.10.1, “Using Novell Remote Manager for Linux to Configure OpLocks,”](#) on page 39
- ♦ [Section 3.10.2, “Editing the `/etc/opt/novell/ncpserv.conf` File to Configure OpLocks,”](#) on page 39

3.10.1 Using Novell Remote Manager for Linux to Configure OpLocks

- 1 In a Web browser, access Novell Remote Manager for Linux on the server, then log in as the root user.

The URL is the IP address of the server (such as 192.168.1.1) and port 8009.

```
https://192.168.1.1:8009
```

- 2 Select *Manage NCP Services > Manage Server* to view the *Server Parameter Information*.
- 3 Click the link for the `OPLOCK_SUPPORT_LEVEL` setting.
- 4 In *New Value*, type a 0 (disable) or 1 (exclusive lock), or 2 (shared lock), then click *Change*.
- 5 On the *Server Parameter Information* page, verify that the new setting is displayed for the `OPLOCK_SUPPORT_LEVEL` parameter.

3.10.2 Editing the `/etc/opt/novell/ncpserv.conf` File to Configure OpLocks

You configure oplocks support in the `/etc/opt/novell/ncpserv.conf` configuration file. There is no need to add a line to the `ncpserv.conf` file to set oplocks to level 2, because it is by default set to that level. You need the line in order to change it back to the default of 2, of course.

To disable oplocks support:

- 1 Open the `/etc/opt/novell/ncpserv.conf` configuration file in a text editor.
- 2 Add the `OPLOCK_SUPPORT_LEVEL` option with the value of 0 as follows:

```
OPLOCK_SUPPORT_LEVEL 0
```

- 3 Save the file.

- 4 Restart the Novell eDirectory (nfsd) Daemon by entering the following commands:

```
/etc/init.d/nfsd stop  
/etc/init.d/nfsd start
```

To set oplocks support to level 1 or 2:

- 1 Open the `/etc/opt/novell/ncpserv.conf` configuration file in a text editor.
- 2 Add the `OPLOCK_SUPPORT_LEVEL` option, and specify a level 1 (exclusive lock) or 2 (shared lock, default):

```
OPLOCK_SUPPORT_LEVEL 1  
  
or  
  
OPLOCK_SUPPORT_LEVEL 2
```

- 3 Save the file.
- 4 Restart the Novell eDirectory (nfsd) Daemon by entering the following commands:

```
/etc/init.d/nfsd stop  
/etc/init.d/nfsd start
```

3.11 Configuring Cross-Protocol File Locks for NCP Server

Cross-protocol locks are enabled by default. Enabling cross-protocol locks turns on the cross-protocol checking for physical record locks. This lets you concurrently run applications from Samba clients, Novell AFP clients, Novell CIFS clients, and NCP clients; and each recognizes when the other has the file in use. Enabling cross-protocol locks enables file share modes. File share modes allow an application to specify whether or not it allows other clients to read and/or write the file while it is using it. Commonly, this is used to allow other clients to read the same file but not write to it while the primary client is using it. Without share modes, applications incorrectly assume that they have exclusive access to a file.

NCP Server has an internal byte-ranging mechanism to prevent potential data corruption when files on NSS and NCP volumes are accessed by NCP clients. Cross-protocol file locking (CPFL) uses the Linux Advisory byte-range lock to prevent potential data corruption when files are accessed by non-NCP file access protocols and by other applications that directly access the files with POSIX APIs. By default, CPFL is enabled (`CROSS_PROTOCOL_LOCKS = 1`) on OES 2 Linux servers. CPFL is enforced globally for all NCP and NSS volumes on the server.

WARNING: Disabling cross-protocol file locking can cause data corruption if any application or non-NCP file access protocol accesses the same data that is accessed via NCP. We recommend that you do not disable CPFL, even if NCP is the only active file access protocol.

Non-NCP file access protocols include Novell Samba, Novell CIFS, and Novell AFP. Applications include any application or service that accesses data on an NCP volume or NSS volume, such as SSH, FTP, restore, scripts, antivirus, database, management tools, and so on.

For example, when ConsoleOne is used to administer the GroupWise database, GroupWise agents directly access the files. You must enable `CROSS_PROTOCOL_LOCKS` in order for the Linux Advisory byte-range locks to work and prevent any potential data corruption.

NOTE: For better performance, you can disable CPFL if you are not using non-NCP file access protocols and the files are not directly accessed by other applications. However, this is not recommended; see the Warning above.

- ♦ [Section 3.11.1, “Using Novell Remote Manager for Linux to Configure Cross-Protocol Locks,” on page 41](#)
- ♦ [Section 3.11.2, “Editing the /etc/opt/novell/ncpserv.conf File to Configure Cross-Protocol Locks,” on page 41](#)

3.11.1 Using Novell Remote Manager for Linux to Configure Cross-Protocol Locks

- 1 In a Web browser, access Novell Remote Manager for Linux on the server, then log in as the root user.

The URL is the IP address of the server (such as 192.168.1.1) and port 8009.

```
https://192.168.1.1:8009
```

- 2 Select *Manage NCP Services > Manage Server* to view the *Server Parameter Information*.
- 3 Click the link for the `CROSS_PROTOCOL_LOCKS` setting.
- 4 In *New Value*, type a 0 (disable) or 1 (enable), then click *Change*.
- 5 On the *Server Parameter Information* page, verify that the new setting is displayed for the `CROSS_PROTOCOL_LOCKS` parameter.

3.11.2 Editing the /etc/opt/novell/ncpserv.conf File to Configure Cross-Protocol Locks

You can enable or disable cross-protocol locks support in the `/etc/opt/novell/ncpserv.conf` configuration file. Support is disabled by default.

To enable cross-protocol locks:

- 1 Open the `/etc/opt/novell/ncpserv.conf` configuration file in a text editor.
- 2 Add the `CROSS_PROTOCOL_LOCKS` option with the value of 1 as follows:

```
CROSS_PROTOCOL_LOCKS 1
```

- 3 Save the file.
- 4 Restart the Novell eDirectory (`nds`) Daemon by entering the following commands:

```
/etc/init.d/nds stop  
/etc/init.d/nds start
```

To disable cross-protocol locks:

- 1 Open the `/etc/opt/novell/ncpserv.conf` configuration file in a text editor.
- 2 Modify the setting from 1 to 0 for the `CROSS_PROTOCOL_LOCKS` option as follows:

```
CROSS_PROTOCOL_LOCKS 0
```

- 3 Save the file.
- 4 Restart the Novell eDirectory (`nds`) Daemon by entering the following commands:

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

3.12 Modifying the NCP File Server Name

The NCP File Server Name parameter is set by default to the hostname of the server at install time. Typically, the hostname does not change because it affects so many installed services. It might be easier to reinstall the server than to discover and modify the hostname setting for all services that include the hostname in their configuration files.

If you modify the server hostname, use the information in this section to modify the NCP File Server Name parameter.

- ♦ [Section 3.12.1, “Understanding the NCP File Server Name,” on page 42](#)
- ♦ [Section 3.12.2, “Modifying the NCP File Server Name Parameter,” on page 43](#)

3.12.1 Understanding the NCP File Server Name

- ♦ [“NCP File Server Name” on page 42](#)
- ♦ [“Using Underscore Characters in the NCP File Server Name” on page 42](#)
- ♦ [“Linux Server Hostname” on page 42](#)

NCP File Server Name

NCP Server uses the server hostname (such as *server1*) as the NCP File Server Name. The setting is initially based on the value you use for the OES 2 Linux server hostname at install time. When installing OES 2 Linux on a virtual machine, this is the hostname you give to the guest server, not the hostname of the physical host server.

IMPORTANT: The NCP File Server Name parameter is included in the `ncpserv.conf` file for informational purposes only.

If you modify the server hostname, you must also modify `NCP_FILE_SERVER_NAME` parameter by editing the `/etc/opt/novell/ncpserv.conf` file.

Using Underscore Characters in the NCP File Server Name

NCP Server allows the use of the underscore (`_`) character for the NCP File Server Name parameter.

Linux Server Hostname

The Linux server hostname is tied to a specified machine (physical or virtual) and is typically unique within a given network. The hostname information is stored in the `/etc/hosts` file and the `/etc/HOSTNAME` file. The following simple rules are used for server hostnames to conform to accepted Internet standards:

- ♦ Hostnames can use alphabetic (a to z) characters, numeric (0 to 9) characters, and hyphens (-).
- ♦ Hostnames can begin and end with a letter or a digit, but cannot be only digits.
- ♦ Hostnames are case insensitive.

In the OES 2 Linux install and in YaST, underscores are treated as invalid characters for server hostnames and domain names, and cannot be set there. Any service, utility, or command that checks the hostname for invalid characters might not work if you use underscores in the hostname. However, many services, including BIND for the DNS Server, allow their check-names functions to be disabled or to ignore invalid characters in the hostname.

3.12.2 Modifying the NCP File Server Name Parameter

- 1 On the OES 2 Linux server, open a terminal console, then log in as the root user.
- 2 Open the `/etc/opt/novell/ncpserv.conf` file in a text editor.

For example, to use gedit, enter

```
gedit /etc/opt/novell/ncpserv.conf
```

- 3 Locate the `NCP_FILE_SERVER_NAME` parameter.

For example, the entry for a server with a fully qualified hostname of `server1.example.com` is set to a value of `server1` as follows:

```
NCP_FILE_SERVER_NAME server1
```

- 4 Type the new hostname. For example:

```
NCP_FILE_SERVER_NAME server-abc
```

- 5 Save the file.
- 6 Restart the Novell eDirectory (ndsd) Daemon by entering the following commands:

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

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

- 7 Restart the Novell NCP/NSS IPC daemon by entering

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

For information about why this is necessary, see [Section 3.5, “Restarting the Novell NCP/NSS IPC \(ncp2nss\) Daemon,”](#) on page 35.

3.13 Modifying the sys: Volume Mount Point

At install time, OES 2 Linux sets up the `sys:` volume with the Linux path of `/usr/novell/sys`, and creates an NCP volume for it in the `/etc/opt/novell/ncpserv.conf` file. The `sys:` volume contains the same `login` and `public` directories that exist on NetWare. These directories let Novell clients run commands for logging in, mapping drives, and so on, as well as providing the means for client commands to be run from login scripts.

Typically, mount path never changes. If you need to modify the path, use the following procedure:

- 1 On the OES 2 Linux server, open a terminal console, then log in as the root user.
- 2 Open the `/etc/opt/novell/ncpserv.conf` file in a text editor.

For example, to use gedit, enter

```
gedit /etc/opt/novell/ncpserv.conf
```

- 3 Locate the volume definition entry for the `sys:` volume.

The default path of the `sys:` volume is `/usr/novell/sys`, so its initial setting is:

```
VOLUME sys /usr/novell/sys
```

- 4 Type the new path. For example:

```
VOLUME sys /newpath/sys
```

- 5 Save the file.
- 6 Restart the Novell eDirectory (ndsd) Daemon by entering the following commands:

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

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

- 7 If NSS is installed on the server, restart the Novell NCP/NSS IPC daemon by entering

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

For information about why this is necessary, see [Section 3.5, “Restarting the Novell NCP/NSS IPC \(ncp2nss\) Daemon,”](#) on page 35.

4 Migrating Data from NSS Volumes to NCP Volumes on Linux File Systems

This section describes migration and compatibility issues for migrating data from Novell Storage Services (NSS) volumes on NetWare 6.5 SP8 servers or OES 1 Linux servers to NCP volumes on Novell Open Enterprise Server (OES) 2 Linux servers.

- ♦ [Section 4.1, “Guidelines for Migrating Data from an NSS Volume on NetWare to an NCP Volume on Linux,” on page 45](#)
- ♦ [Section 4.2, “Planning Your Migration,” on page 47](#)

4.1 Guidelines for Migrating Data from an NSS Volume on NetWare to an NCP Volume on Linux

Consider the guidelines in this section when planning your data migration from NSS volumes to NCP volumes by using the File System Migration Tool, or by using migration commands.

- ♦ [Section 4.1.1, “Trustees and Trustee Rights,” on page 45](#)
- ♦ [Section 4.1.2, “User Quotas,” on page 45](#)
- ♦ [Section 4.1.3, “Deleted Files,” on page 46](#)
- ♦ [Section 4.1.4, “Encryption,” on page 46](#)
- ♦ [Section 4.1.5, “Distributed File Services,” on page 46](#)

4.1.1 Trustees and Trustee Rights

Both NSS volumes and NCP volumes use the Novell trustee model for controlling access to data. If you migrate data from an NSS volume on NetWare to an NCP volume, the trustees and trustee rights are enforced.

IMPORTANT: Make sure that the trustees are also authorized Novell eDirectory users of the destination server.

4.1.2 User Quotas

NCP Server does not provide a user quotas feature, so NCP volumes cannot support user quotas that are set on the NSS volume you are migrating. After the data is migrated, the quotas are not enforced in the NCP volume.

After the migration, you can use Linux tools to set user quotas on the Linux POSIX file system underneath the NCP share if the Linux file system being used under the NCP share supports user quotas and the Linux file system resides on a local, iSCSI, or Fibre Channel drive. All users of the NCP volume must be LUM enabled.

4.1.3 Deleted Files

NCP volumes do not support the deleted file salvage and purge that is available for NSS volumes. If you have deleted files on the NSS volume, they are not migrated. If you want to salvage deleted files, do it before you migrate the data. In addition, the Salvage (Undelete) and Purge options in the Novell Client, NetStorage, and the Files and Folders plug-in to iManager are disabled for NCP volumes on Linux file systems.

4.1.4 Encryption

NCP volumes do not support volume encryption. If you migrate data from an encrypted NSS volume, the data is not encrypted on the NCP volume. This would be a major security violation.

WARNING: We strongly recommend that you do not migrate data from an encrypted NSS volume to an NCP volume.

Consider migrating the device that contains the encrypted NSS volume from the NetWare server to the Linux server. For information on this scenario, see [“Moving Non-Clustered Devices From NetWare 6.5 SP8 Servers to OES 2 Linux Servers”](#) in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

4.1.5 Distributed File Services

Novell Distributed File Services is a feature of Novell Storage Services. If an NSS volume contains junctions or is a junction target, it affects how you migrate the data.

- ♦ [“NSS Volumes That Contain Junctions”](#) on page 46
- ♦ [“NSS Volumes That Are Junction Targets”](#) on page 46

NSS Volumes That Contain Junctions

DFS does not support junctions on NCP volumes on Linux file systems. If the original NSS volume contains junctions, its junctions are broken after migrating its data to an NCP volume. Instead of migrating data to an NCP volume, consider one of the following methods to move the data to an NSS volume on OES 2 Linux:

- ♦ Use the File System Migration Tool to migrate the data from the NSS volume on NetWare to an NSS volume on OES 2 Linux.
- ♦ Use the Novell Distributed File Services Move Volume task to move the NSS volume from NetWare to Linux. For information, see [“Using DFS to Move NSS Volumes”](#) in the *OES 2 SP3: Novell Distributed File Services Administration Guide for Linux*.
- ♦ Move the devices that contain the pool from NetWare to Linux. For information, see [“Migrating NSS Devices from NetWare 6.5 SP8 to OES 2 Linux”](#) in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

NSS Volumes That Are Junction Targets

NCP volumes can be the target of junctions on NSS volumes. If the original NSS volume is a junction target, it resides in a DFS management context. The Data Migration Tool uses the same Volume object for a volume when it is migrated within the same tree. This allows the volume to keep the same DFS GUID, so junctions that point to the volume are broken only until the VLDBs that are involved are repaired, as described in [Table 4-1](#):

Table 4-1 *Post-Migration DFS Tasks*

Destination Server's DFS Management Context	Post-Migration DFS Tasks
Same	Run VLDB repair in the DFS management context.
Different	Run a VLDB repair in both the original and destination DFS management contexts.
None, but in the same tree	Create a DFS management context that contains the destination server. This creates a new VLDB that contains the destination volume information.

For information about running a VLDB repair, see [“Repairing the VLDB”](#) in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

4.2 Planning Your Migration

You can optionally use the File System Migration Tool to migrate data and trustee information from an NSS volume on NetWare to an NCP volume on an OES 2 Linux server. For information, see [“Migrating File System from NetWare, OES 1 or OES 2 to OES 2 SP3 Linux”](#) in the *OES 2 SP3: Migration Tool Administration Guide*.

- ◆ [Section 4.2.1, “System Requirements for the OES 2 Linux Server,”](#) on page 47
- ◆ [Section 4.2.2, “Supported Platforms for the Source NSS Volume,”](#) on page 47

4.2.1 System Requirements for the OES 2 Linux Server

The destination server is an OES 2 Linux server. The destination volume is an existing NCP volume on a Linux POSIX file system.

- ◆ NCP Server must be installed and running.
- ◆ Users of the data must be Novell eDirectory users. They will have the same trustee rights to the NCP volume on the destination server as to the original NSS volume.
- ◆ Linux User Management must be installed and enabled on the OES 2 Linux server if you plan to give access to CIFS/Samba users of the NCP volume.
- ◆ Use the NCP Server Console utility (ncpcon) to create the target NCP volume.
- ◆ Ensure that the user who performs the migration has Read/Write access rights to the POSIX path that corresponds to the NCP volume.

4.2.2 Supported Platforms for the Source NSS Volume

The File System Migration Tool supports migrating data from NSS volumes on the following platforms or later versions:

- ◆ OES 2 NetWare
- ◆ NetWare 6.5 SP8
- ◆ OES 1 Netware SP3
- ◆ OES 1 SP2 Linux

5 Using NCP Server and NCP Volumes in a Virtualization Environment

NCP Server works regardless of whether it is installed on a Novell Open Enterprise Server (OES) 2 Linux server running on a physical server or on a virtual machine (VM) guest server (DomU). NCP Server is not supported on the Xen VM host environment (that is, not supported to run in Dom0).

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

For information on setting up NetWare on a Xen VM guest server, see “[Installing and Managing NetWare on a Xen-based VM](#)” in the *OES 2 SP3: Installation Guide*.

For information on setting up OES 2 Linux on a Xen VM guest server, see “[Installing, Upgrading, or Updating OES on a Xen-based VM](#)” in the *OES 2 SP3: Installation Guide*.

6 Planning for NCP Server and NCP Volumes

This section describes requirements and guidelines for using NCP Server and NCP volumes for Novell Open Enterprise Server (OES) 2 Linux servers.

- ♦ [Section 6.1, “NCP Volumes on Linux,” on page 51](#)
- ♦ [Section 6.2, “Security Issues,” on page 51](#)
- ♦ [Section 6.3, “Novell Dynamic Storage Technology,” on page 52](#)
- ♦ [Section 6.4, “User Quotas on Linux POSIX File Systems,” on page 52](#)

6.1 NCP Volumes on Linux

NCP volumes can be created on Linux POSIX file systems (such as Ext3, XFS, and Reiser) on an OES 2 Linux server.

By default, Novell Storage Services (NSS) volumes on Linux are NCP volumes. However, NSS volumes are managed using NSS management tools and commands.

IMPORTANT: Except where otherwise noted, NCP volumes refers only to NCP shares on Linux POSIX file systems.

NSS volumes are mounted by default in NSS and NCP Server on server restart. You can prevent an NSS volume from mounting automatically in NCP Server by modifying its NCP/NSS Bindings so that the volume is not automatically mounted at server restart. For information, see [Section 10.9, “Configuring the NCP/NSS Bindings for an NSS Volume,” on page 92](#).

6.2 Security Issues

- ♦ [Section 6.2.1, “POSIX Permissions on the NSS File System,” on page 51](#)
- ♦ [Section 6.2.2, “POSIX Permissions on Linux File Systems,” on page 52](#)

6.2.1 POSIX Permissions on the NSS File System

NSS users access the volumes with their eDirectory usernames, not a local Linux identity. Access is granted by using the Novell trustee model of trustees, trustee rights, and inherited rights filters. The server’s root user is the only local user who has local access to the NSS file system.

NSS maps the file system settings for trustee rights to the POSIX file system, but it is not a one-to-one mapping. Many security features available in the Novell trustee model are not available in POSIX, so POSIX settings cannot be viewed in the same way that they might be for a non-NSS Linux file system.

For information about how NSS maps file system rights and attributes, see [“Viewing Key NSS Directory and File Attributes as Linux POSIX Permissions”](#) in the *OES 2 SP3: File Systems Management Guide*.

6.2.2 POSIX Permissions on Linux File Systems

For NCP volumes on Linux POSIX file systems, make sure that the Inherit POSIX Permissions option is disabled (the default setting). When this setting is disabled, the local Linux environment access is restricted to the `root` user and the file owner or creator, which is the most secure configuration. For information, see [Section 10.8, “Configuring Inherit POSIX Permissions for an NCP Volume,”](#) on [page 89](#).

Inherit POSIX Permissions is not allowed to be set on an NSS volume. There is an explicit check for this, and if it is an NSS volume, an Error 22 is returned. NSS has its own handling of POSIX permissions. For information, see [Section 6.2.1, “POSIX Permissions on the NSS File System,”](#) on [page 51](#).

6.3 Novell Dynamic Storage Technology

Dynamic Storage Technology is a component of NCP Server on OES 2 Linux and later. It is supported for use with NSS volumes on Linux. For information, see the *OES 2 SP3: Dynamic Storage Technology Administration Guide*.

6.4 User Quotas on Linux POSIX File Systems

NCP Server does not provide a user quotas feature for Linux POSIX file systems. User quotas are possible if the Linux file system being used under the NCP share supports user quotas and the Linux file system resides on a local, iSCSI, or Fibre Channel drive. All users of the NCP volume must be LUM enabled. Manage the user quotas using the Linux file system tools.

7 Management Tools for NCP Server

This section describes the tools for managing NCP Server and NCP volumes on a Novell Open Enterprise Server (OES) 2 Linux server.

- ♦ [Section 7.1, “Novell Remote Manager for Linux,” on page 53](#)
- ♦ [Section 7.2, “NCP Server Console \(NCPCON\) Utility,” on page 59](#)
- ♦ [Section 7.3, “NCPTOP Quick Reference,” on page 60](#)

7.1 Novell Remote Manager for Linux

Use the NCP Server plug-in for Novell Remote Manager for Linux to manage NCP Server and NCP volumes on an OES 2 Linux server.

- ♦ [Section 7.1.1, “Installing Novell Remote Manager for Linux,” on page 53](#)
- ♦ [Section 7.1.2, “Accessing Novell Remote Manager,” on page 53](#)
- ♦ [Section 7.1.3, “Starting, Stopping, or Restarting Novell Remote Manager on Linux,” on page 54](#)
- ♦ [Section 7.1.4, “Quick Reference for the NCP Server Plug-In for Novell Remote Manager for Linux,” on page 54](#)

7.1.1 Installing Novell Remote Manager for Linux

Novell Remote Manager for Linux is installed by default as part of your OES 2 Server installation whenever any OES 2 pattern is selected. For information about managing Novell Remote Manager for Linux, see the *OES 2 SP3: Novell Remote Manager for Linux Administration Guide*.

7.1.2 Accessing Novell Remote Manager

- 1 Access Novell Remote Manager by pointing your browser to the URL of the server you want to manage.

Do this by entering the following in the address (URL) field:

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

For example:

```
http://192.168.123.11:8008
```

```
https://192.168.123.11:8009
```

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

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

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

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

Novell Remote Manager on Linux is installed and runs by default. If it hangs, you can use the `/etc/init.d/novell-httpstkd` script to get status or to stop, start, or restart `httpstkd`. For the latest information about `httpstkd`, see [“Starting or Stopping HTTPSTKD”](#) in the *OES 2 SP3: Novell Remote Manager for Linux Administration Guide*.

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

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

7.1.4 Quick Reference for the NCP Server Plug-In for Novell Remote Manager for Linux

- ♦ [“NCP Volumes \(NCP Shares\)”](#) on page 54
- ♦ [“NCP Server Parameters”](#) on page 55
- ♦ [“NCP Server Connections”](#) on page 56
- ♦ [“NCP Trustee Reports”](#) on page 56
- ♦ [“NCP Logs and Audit Logs”](#) on page 57
- ♦ [“NCP Server Statistics”](#) on page 57
- ♦ [“NCP Server Diagnostics”](#) on page 58
- ♦ [“Dynamic Storage Technology”](#) on page 58

NCP Volumes (NCP Shares)

[Table 7-1](#) describes the management tasks available for *Manage NCP Services > Manage Shares* task in Novell Remote Manager for Linux.

Table 7-1 *Manage NCP Services > Manage Shares*

Subtasks	Management Tasks
Share Name link	<p>Browse files and directories.</p> <p>View and set file system attributes for files and directories on NSS volumes.</p> <p>View file information.</p> <p>View directory information.</p>
Mount/Unmount	<p>Mount NCP volumes and NSS volumes to make them available to NCP clients.</p> <p>Unmount NCP volumes and NSS volumes to make them unavailable to NCP clients.</p>
Info icon	<p>NCP share information, such as the Linux file system path for the volume, file system type, NCP volume ID, status, capacity, and cache statistics.</p> <p>Open files listed for each NCP connection.</p> <p>Add a shadow volume for the NCP volume.</p> <p>For unmounted DST shadow volumes, click the <i>Info</i> icon to remove the shadow volume relationship. Removing a shadow volume removes the entry in the <code>ncpserv.conf</code> file, but does not delete the volumes that make up the shadow volume.</p>
Create new share	<p>Creates an NCP volume name (share) on a Linux POSIX file system (Ext3, XFS, or Reiser), and associates it to a path on your server. You are prompted for a volume (share) name and a path to the volume. This creates a mount point to the volume you specify and makes it accessible to NCP clients.</p> <p>IMPORTANT: Using this method to create an NCP volume cannot be used to create an NSS volume. You must use NSS tools to create and manage NSS volumes on Linux.</p>
Delete existing share	<p>Removes the NCP volume and path association for NCP volumes on Linux POSIX file systems (Ext3, XFS, or Reiser). This does not remove or delete data from the directory; it removes only the volume mount point that was created for the NCP share.</p>
NCP/NSS Bindings	<p>View or modify whether NSS volumes are NCP accessible. If they are not accessible, the <code>EXCLUDE_VOLUME volumename</code> command is added to the <code>/etc/opt/novell/ncp2nss.conf</code> file.</p> <p>Use this option for NSS volumes on clusters where the load script handles NCP mount of NSS volumes.</p> <p>Use this option for NSS volumes that you want to use as the secondary storage area in a Dynamic Storage Technology shadow volume.</p>

NCP Server Parameters

[Table 7-2](#) describes the management task available for *Manage NCP Services > Manager Server* task in Novell Remote Manager for Linux.

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

Subtasks	Management Tasks
Server Parameter Information	<p>View NCP Server parameters for the SET command and their current values.</p> <p>Click the <i>Parameter Value</i> link to modify the value. For a list of parameters and their default values, see Section 3.4, "Configuring Global NCP Server Parameters," on page 29.</p>

NCP Server Connections

[Table 7-3](#) describes the management tasks available for *Manage NCP Services > Manage Connections* task in Novell Remote Manager for Linux.

Table 7-3 *Manage NCP Services > Manage Connections*

Subtasks	Management Tasks
Connection Information	<p>View connection statistics.</p> <p>Clear all <i>Not Logged In</i> connections.</p>
Connection Listing	<p>View a list of connections.</p> <p>Click the name link for the connection to view statistics for the connection and a list of its open files.</p> <p>Clear selected connections.</p>
Name link for the connection	<p>View statistics for the connection.</p> <p>View the network address, status, privileges, and security equivalence for a logged-in-user.</p> <p>Send a message to the selected connection.</p>
Broadcast messages to everyone	<p>Broadcast messages to all logged in NCP users. The <code>DISABLE_BROADCAST</code> parameter must be disabled (value of 0) in order for broadcast messages to be sent. Users must be using a Novell Client version that supports receiving broadcast messages, and the client must be configured to receiving messages.</p>

NCP Trustee Reports

[Table 7-4](#) describes the management tasks available for *Manage NCP Services > NCP Trustee Report* task in Novell Remote Manager for Linux.

Table 7-4 *Manage NCP Services > NCP Trustee Report*

Subtasks	Management Tasks
Generating an NCP Trustee Report for NSS volumes	View the NCP Trustee Report. A volume's trustee report shows the rights settings by folder for each user or group that is a trustee on the NSS volume.
Viewing a Saved NCP Trustee Report	View the last saved trustee report for an NSS volume. The saved report provides the same trustee rights information that was available when the report was created.
Emailing a Saved NCP Trustee Report	Email an NCP volume's trustee report to addresses that are configured in the <code>httpstkd.conf</code> file.

NCP Logs and Audit Logs

[Table 7-5](#) describes the management tasks available for *Manage NCP Services > View Logs* task in Novell Remote Manager for Linux.

Table 7-5 *Manage NCP Services > View Logs*

Subtasks	Management Tasks
Logs	Download and view the <code>ncpserv.log</code> and <code>ncp2nss.log</code> .
Audit Logs	Download and view the following audit logs: <ul style="list-style-type: none">◆ <code>ncpserv.audit.log</code><p>All the operations performed by NCP Engine are logged into this file in XML format. For example, add trustee, remove trustee, volume mount and dismount, NSS event handler startup/shutdown, add/remove volume, create shadow volume, security sync, kill NCP connections, etc.No file operations are logged in this file.</p>◆ <code>ncp2nss.audit.log</code><p>The following <code>ncp2nss</code> events are logged into this file: Open command file, write command file, <code>ncp2nss</code> daemon halted, <code>ncp2nss</code> daemon running, NSS not detected, domain socket not created, domain socket not accessible, <code>uneb</code> not started, failed to import <code>uneb</code> symbols, failed to create <code>uneb</code> processing thread, <code>ndp</code> library not started, failed to import <code>ndp</code> library symbols and failed to initialize <code>ndp</code> library.</p>◆ <code>SYS.audit.log</code>◆ <code>volumename.audit.log</code> (an audit log is listed for each NSS volume)

NCP Server Statistics

[Table 7-6](#) describes the management tasks available for *Manage NCP Services > View Statistics* task in Novell Remote Manager for Linux.

Table 7-6 *Manage NCP Services > View Statistics*

Subtasks	Management Tasks
Server Information	View server name, server version, and product version. View the number of connections.
Server Statistics	View server statistics such as up time, traffic, and caching memory use.

NCP Server Diagnostics

[Table 7-7](#) describes the management tasks available for *Manage NCP Services > Diagnostic Information* task in Novell Remote Manager for Linux.

Table 7-7 *Manage NCP Services > Diagnostic Information*

Subtasks	Management Tasks
NCP Engine	View statistics for NCP events. Click the <i>Process ID (PID)</i> link to view information about the currently running process.
NSS Interface Daemon	View statistics for NSS events. Click the <i>Process ID (PID)</i> link to view information about the currently running process.

Dynamic Storage Technology

[Table 7-8](#) describes the management tasks available for *View File Systems > Dynamic Storage Technology Options* task in Novell Remote Manager for Linux.

Table 7-8 *View File Systems > Dynamic Storage Technology Options*

Subtasks	Management Tasks
Volume Information	View a list of NCP volumes and NSS volumes on the server. Click the <i>Add Shadow</i> link next to an NSS volume to view share information, where you can create a shadow volume. (NCP volumes are not supported as shadow volumes in the initial release.) Click the <i>Inventory</i> link next to a shadow volume to view an inventory report for both the primary and secondary volumes. Click the <i>View Log</i> link next to an NSS volume to download a copy of the audit log for the selected volume.

Subtasks	Management Tasks
Add Shadow link	<p>This option takes you to the Share Information page. Scroll down to the <i>Volume Tasks</i> area to find the <i>Add Shadow Volume</i> task.</p> <p>The Share Information page and Add Shadow Volume page do not distinguish or validate whether the volumes you choose are actually supported file systems and available combinations.</p> <p>WARNING: NSS volumes must already exist when you create the shadow volume. The <i>Create if not present</i> option is available for future support of NCP volumes on Linux file systems. Do not use this option for NSS volumes.</p>
Inventory link	<p>View statistics and graphical trend displays for the volume's files and directories. For a DST shadow volume, the report includes information for both the primary storage area (primary area) and the secondary storage area (shadow area).</p>
Volume Information (<i>Info</i> icon)	<p>NCP share information, such as the Linux file system path for the volume, file system type, NCP volume ID, status, capacity, and cache statistics.</p> <p>Open files listed for each NCP connection.</p> <p>Add a shadow volume for the NCP volume.</p> <p>For unmounted DST shadow volumes, click the Info icon to access the dialog to remove the shadow volume relationship. This removes the entry in the <code>ncpserv.conf</code> file, but does not delete the volume itself.</p> <p>To unmount a shadow volume, click <i>Manage NCP Services > Manage Shares</i>, then click <i>Unmount</i> option next to the shadow volume.</p>
Dynamic Storage Technology Policies	<p>Create a new policy.</p> <p>View a list of existing policies.</p> <p>Click the <i>Policy Name</i> link to modify or delete the policy.</p>
Duplicate File Resolution Options	<p>Set a global policy for how to handle duplicate files.</p>
ShadowFS Configuration	<p>Set a global policy for whether to automatically start FUSE and Shadow File System at boot time.</p>

7.2 NCP Server Console (NCPCON) Utility

The NCP Server Console (`ncpcon(8)`) utility is a Linux server console program for executing NetWare-related server console commands. You can use it to configure and manage NCP-specific functions on your OES 2 Linux server.

NCPCON is a management utility for NCP Server on Novell Open Enterprise Server (OES) 2 Linux. You must issue NCPCON commands as the `root` user. NCPCON commands can be issued using either of the following methods:

- ♦ Use `ncpcon` in interactive mode by starting `ncpcon`, then entering the command at the NCPCON prompt.
- ♦ Use `ncpcon` in a scripting or command line mode by prepending the server console command with `ncpcon`. For scripting, double-quote the desired NCP Server console command. For example:

```
ncpcon mount sys
```

For a list of commands and usage information, see [Section A.1, “NCPCON,” on page 135](#).

When NCPCON fails, the errors are logged in `ncpcon.err` file located at `/var/opt/novell/log`. The file stores the error number of the failed NCPCON command. The `ncpcon.err` file is overwritten if it already exists.

7.3 NCPTOP Quick Reference

You can monitor NCP Server connections, communications, volumes, and diagnostics by using NCPTOP. NCPTOP is a monitoring utility that looks like the NetWare Monitor utility, and is an interactive, real-time reporting utility. It is part of the `novell-ncpserv` RPM.

After NCP Server has been installed, you can start NCPTOP by entering `ncptop` at a terminal console prompt on the Linux server. Different statistic monitoring functions of NCPTOP can be accessed by using the function keys, or you can tab through the reports. The purpose of each function key and its options are displayed within the NCPTOP utility. [Table 7-9](#) provides an overview of tasks available.

Table 7-9 NCPTOP Reports

Function Key	Report	Description
F2	General	Displays a general communications report for NCP Server. See Figure 7-1 for an example report.
F3	Volume	Lists NCP volumes, and allows you to get the following details for a volume: <ul style="list-style-type: none">◆ Status◆ Mount Point◆ Shadow Mount Point◆ Capacity◆ Cached Files◆ Cached Folders◆ Trustee Count
F4	Connection	Lists the current connections, and allows you to get details for each connection.
F5	Diagnostics	Lists further diagnostic options. See Figure 7-2 for an example report.
F6	Parameters	Displays the current settings for the NCPCON set parameters. See Figure 7-3 for an example report. For information about the parameters, see the Section A.2, “NCPCON SET Parameters,” on page 153 .
F7	Version	Reports the versions of the NCP Server software components.

Figure 7-1 General Communications Report in NCPTOP

```
[F12] Exit [F2] General [F3] Volume [F4] Connection [F5] Diagnostics
[F6] Parameters [F7] Version [+/-] sec. [tab] Next Scr

Server Up Time: 2 Hours 39 Minutes 45 Seconds

LOG_LEVEL = WARN
MAXIMUM_CACHED_FILES_PER_SUBDIRECTORY = 10240
MAXIMUM_CACHED_FILES_PER_VOLUME = 256000
MAXIMUM_CACHED_SUBDIRECTORIES_PER_VOLUME = 102400
MAXIMUM_LAZY_CLOSE_FILES = 4096
LOG_CACHE_STATISTICS = 0
LOG_MEMORY_STATISTICS = 0
LOG_IDBROKER_ERRORS = 0
OPLOCK_SUPPORT_LEVEL = 2
CROSS_PROTOCOL_LOCKS = 0
MAXIMUM_FILE_LOCKS_PER_CONNECTION = 1000
EXECUTE_ATTRIBUTE_SUPPORT = 1
SENDFILE_SUPPORT = 0
LOCAL_CODE_PAGE = CP437
SHIFT_MODIFIED_SHADOW_FILES = 1
SHIFT_ACCESSED_SHADOW_FILES = 0
SHIFT_DAYS_SINCE_LAST_ACCESS = 1
FIRST_WATCHDOG_PACKET = 0
```

Figure 7-2 Diagnostic Reports List in NCPTOP

```
[F12] Exit [F2] General [F3] Volume [F4] Connection [F5] Diagnostics
[F6] Parameters [F7] Version [+/-] sec. [tab] Next Scr

Server Up Time: 2 Hours 27 Minutes 59 Seconds

View Diagnostics
 1 - Directory Cache           11 ncp2nss Manage I/F
 2 - Communications           12 ncp2nss Requests
 3 - IPC                       13 ncp2nss IPC
 4 - Error counters           14 ncp2nss NEB events
 5 - Trustees                  15 ncp2nss Volumes
 6 - NSS Events                16 ncp2nss User/Directory quotas
 7 - Deleted files             17 ncp2nss Deleted files
 8 - User/Directory quotas     18 ncp2nss Trustees

Enter selection ?
```

Figure 7-3 NCP Server Parameters Report in NCPTOP

```
[F12] Exit [F2] General [F3] Volume [F4] Connection [F5] Diagnostics
[F6] Parameters [F7] Version [+/-] sec. [tab] Next Scr

Server Up Time: 2 Hours 39 Minutes 45 Seconds

LOG_LEVEL = WARN
MAXIMUM_CACHED_FILES_PER_SUBDIRECTORY = 10240
MAXIMUM_CACHED_FILES_PER_VOLUME = 256000
MAXIMUM_CACHED_SUBDIRECTORIES_PER_VOLUME = 102400
MAXIMUM_LAZY_CLOSE_FILES = 4096
LOG_CACHE_STATISTICS = 0
LOG_MEMORY_STATISTICS = 0
LOG_IDBROKER_ERRORS = 0
OPLOCK_SUPPORT_LEVEL = 2
CROSS_PROTOCOL_LOCKS = 0
MAXIMUM_FILE_LOCKS_PER_CONNECTION = 1000
EXECUTE_ATTRIBUTE_SUPPORT = 1
SENDFILE_SUPPORT = 0
LOCAL_CODE_PAGE = CP437
SHIFT_MODIFIED_SHADOW_FILES = 1
SHIFT_ACCESSED_SHADOW_FILES = 0
SHIFT_DAYS_SINCE_LAST_ACCESS = 1
FIRST_WATCHDOG_PACKET = 0
```

8 Managing NCP Server

This section describes how to manage NCP Server on a Novell Open Enterprise Server (OES) 2 Linux server.

- ♦ [Section 8.1, “Monitoring NCP Server by Using Novell Remote Manager,” on page 63](#)
- ♦ [Section 8.2, “Monitoring NCP Server by Using NCPCON,” on page 63](#)
- ♦ [Section 8.3, “Monitoring NCP Server by Using NCPTOP,” on page 65](#)

8.1 Monitoring NCP Server by Using Novell Remote Manager

Viewing server information can help you troubleshoot server problems. It reports process information and allows you to change file attributes for specific NCP-related program files.

- 1 In Novell Remote Manager, click *Manage NCP Services > View Diagnostic Information*.
- 2 Click the PID value to access additional pages for process information and to change file attributes for specific NCP-related program files.

8.2 Monitoring NCP Server by Using NCPCON

- 1 Open a terminal console on the Linux server you want to manage, then log in as the root user.
- 2 At a terminal console prompt, enter

```
ncpcon
```

- 3 In NCPCON, use any of the following NCPCON commands to view server information:

Command	Description
<code>config</code>	Displays the NCP Server configuration information such as the server name, server version, product version, NCP version, mixed-mode paths status (yes/no), and commit files status (yes/no).

Command	Description
stats	<p>Displays NCP statistics such as the following.</p> <ul style="list-style-type: none"> ◆ Server up time ◆ Packets in ◆ Packets dumped ◆ Packet receive buffer memory ◆ Packet reply buffer memory ◆ NCP requests ◆ NCP connections in use ◆ Connection table memory ◆ Mounted volumes ◆ Number of open files ◆ Local ID tracking ◆ File handle memory ◆ Volume sys: file and subdirectory caching memory ◆ Volume sys: trustee and inherited rights mask tracking memory
version	<p>Displays version information for all currently running Novell NCP Server components, the OES build, and the hardware platform.</p>
volume	<p>Displays a list of currently mounted NCP volumes.</p>
volume <i>ncp_volume_name</i>	<p>Displays information about the specified volume. The volume must be mounted before you issue the command.</p>
log [filename] [level]	<p>Adjusts the logging level of either the NCP Server log (<code>/var/opt/novell/log/ncpserv.log</code>) or the ncp2nss daemon log (<code>/var/opt/novell/log/ncp2nss.log</code>).</p> <p>This command can be added to a cluster load script.</p> <p>Options:</p> <ul style="list-style-type: none"> ◆ filename <ul style="list-style-type: none"> [ncpserv.log ncp2nss.log] ◆ level <ul style="list-style-type: none"> [debug dump error everything info nothing warning] <p>Examples:</p> <pre>log ncpserv.log debug log ncp2nss.log error</pre> <p>By default, the logging level is set to warning for both the NCP Server and ncp2nss daemon logs.</p>

8.3 Monitoring NCP Server by Using NCPTOP

You can monitor NCP Server connections, communications, volumes, and diagnostics using NCPTOP (`ncptop(8)`), an interactive, real-time reporting utility.

- 1 Open a terminal console, then log in as the root user.
- 2 At the terminal console prompt, enter

```
ncptop
```

- 3 Press the function keys to view reports:

Function Key	Reports	Description
F2	General	Displays a general communications report for NCP Server.
F3	Volume	Lists NCP volumes, and allows you to get the following details for a volume: <ul style="list-style-type: none">◆ Status◆ Mount Point◆ Shadow Mount Point◆ Capacity◆ Cached Files◆ Cached Folders◆ Trustee Count
F4	Connection	Lists the current connections, and allows you to get details for each connection.
F5	Diagnostics	Lists further diagnostic options.
F6	Parameters	Displays the current settings for the NCPCON set parameters. For more information about the parameters, see the Section A.2, "NCPCON SET Parameters," on page 153.
F7	Version	Reports the versions of the NCP Server software components.

9 Managing Connections for NCP Volumes and NSS Volumes

The Connection Manager allows you to view information about and manage NetWare Core Protocol (NCP) client connections on a Novell Open Enterprise Server (OES) 11 server. Connections include those for NCP volumes (NCP shares on Linux POSIX file systems) and Novell Storage Services volumes.

- ♦ [Section 9.1, “Understanding Connections,” on page 67](#)
- ♦ [Section 9.2, “Managing User Login for NCP Server,” on page 70](#)
- ♦ [Section 9.3, “Sending Messages to Logged-In Users,” on page 71](#)
- ♦ [Section 9.4, “Viewing Connections for NCP Server,” on page 73](#)
- ♦ [Section 9.5, “Sorting Entries in the Connection Listing,” on page 75](#)
- ♦ [Section 9.6, “Clearing Not-Logged-In Connections to NCP Server,” on page 76](#)
- ♦ [Section 9.7, “Clearing Connections to NCP Server,” on page 76](#)
- ♦ [Section 9.8, “Finding the Connection that Has a File Open,” on page 77](#)
- ♦ [Section 9.9, “Viewing Open Files for an NCP Server Connection, and Closing All Open Files,” on page 77](#)
- ♦ [Section 9.10, “Viewing Open Files for an NCP Server Connection, and Closing a Specific Open File,” on page 78](#)
- ♦ [Section 9.11, “Generating and Viewing NCP Trustee Reports for NSS Volumes,” on page 79](#)

9.1 Understanding Connections

The *Connection Manager* reports the status of current connections for NCP Server and lists the connections. You can access the reports using the *Connection Manager* page in Novell Remote Manager or the `connection` command in the NCP Server Console (`ncpcon(8)`) utility. In Novell Remote Manager, you can also view open files for a connection, clear specific NCP connections, and send a broadcast message out to current NCP connections.

- ♦ [Section 9.1.1, “Connection Information,” on page 67](#)
- ♦ [Section 9.1.2, “Connection Listing,” on page 69](#)
- ♦ [Section 9.1.3, “Detailed Connection Information,” on page 69](#)

9.1.1 Connection Information

The *Connection Information* report displays the current status of the following parameters:

Table 9-1 Connection Information Report

Parameter	Description
Connection Slots Allocated	<p>Displays the number of slots currently allocated for use. As connection slots required on this server exceed the current number of slots displayed here, new slots are allocated.</p> <p>Depending on the server's memory, connection slots are usually allocated in blocks of 16. Connection slots are allocated as needed by users, NetWare Loadable Module (NLM) programs, and other services.</p>
Connection Slots Being Used	<p>Displays the number of connection slots currently in use. As this number matches or exceeds the Connection Slots Allocated entry, more connection slots are allocated to the connection table.</p>
Signing Level	<p>Displays the level at which NCP packet signature signing is set on the server. NCP packet signatures prevent packet forgery by requiring the server and the workstation to sign each NCP packet. A higher packet signature number impacts the performance of your server. At some point, the need for security might outweigh certain performance issues.</p> <ul style="list-style-type: none">◆ 0: The server does not sign packets (regardless of the client level).◆ 1: The server signs packets only if the client requests it (client level is 2 or higher). This is the default value.◆ 2: The server signs packets if the client is capable of signing (client level is 1 or higher).◆ 3: The server signs packets and requires all clients to sign packets or logging in will fail. <p>To set this value for NCP Server on Linux, issue the following command at a terminal console prompt:</p> <pre>ncpcon SET NCP Packet Signature Option = number</pre> <p>For more information about configuring and managing the NCP Packet Signature, see Using NCP Packet Signature (http://www.novell.com/documentation/nw65/os_svr_adm_nw/?page=/documentation/nw65/os_svr_adm_nw/data/h1hge52k.html#h1hge52k). On Linux, make sure to issue the NCP server commands in the NCP Console (ncpcon(8)).</p>
Login State	<p>Displays whether users are allowed to log in to the server.</p> <p>To disable users from being able to log in to the server (for server maintenance or other reasons), enter <code>disable login</code> at the NCPCON prompt, or enter <code>ncpcon disable login</code> at a terminal console prompt.</p> <p>To allow users to log in to the server, enter <code>enable login</code> at the NCPCON prompt, or enter <code>ncpcon enable login</code> at a terminal console prompt.</p>
Licensed Connections	<p>Displays the number of connections that are currently licensed. Licensed connections are authenticated, logged in, and consume a license. An unlicensed connection does not consume a license and can be authenticated or not. An unlicensed, authenticated connection can access the eDirectory database but cannot access any other resources.</p>

Parameter	Description
Not Logged In Connections	<p>Clears all user connections that are open but not currently authenticated to the server. The connections can be cleared whether they are based on an NLM or based on a user.</p> <p>Use this parameter to clear all user or NLM connections that are not logged in.</p> <p>IMPORTANT: Some connections based on an NLM, such as backup NLM programs, maintain a Not Logged In connection until it is time to log in and perform the specified service. If the connection is cleared, the NLM might not be able to reestablish a connection to the server unless it is unloaded and reloaded. This might prevent the NLM from performing the required task.</p>

9.1.2 Connection Listing

The Connection Listing page displays the following information about each current connection:

Table 9-2 Connection Listing Report

Parameter	Description
Station	Shows the connection number for each connection. Connection 0 is the connection used by the server. The server's operating system uses connection numbers to control each station's communication with other stations. Remote Manager does not distinguish connections that don't count against the server's connection limit.
Name	<p>Shows the name of the user, server, service, login status, and links to specific information about that user connection such as the login time, connection number, network address, login status, number of NCP requests, files in use, and security equivalence.</p> <p>Connections with an asterisk (*) displayed next to the name indicate an unlicensed connection (it does not consume a license). These licenses can be either authenticated or not authenticated. An unlicensed, authenticated connection can access the Novell eDirectory database but not other server resources.</p> <p>From this detailed Connection Information page, you can also clear the connection or send a message to the user.</p>
Reads & Writes	Shows the number of reads and writes (in bytes) made by each connection.
NCP Request	Shows the number of NCP requests made by each connection.
Login Time	Shows the login day, date, and time for the connection.

9.1.3 Detailed Connection Information

For each connection, the Connection Manager reports additional details, which are available by clicking the *Name* link for the connection. Some parameters are not present if they do not apply.

Table 9-3 Detailed Connection Information Report for a Specific Connection

Parameter	Description
Connection	The station number for the connection.
Login Status	Shows whether the connection is Authenticated or Not Logged In.
Authentication Method	Shows the authentication method used if the connection is logged in.
Login Time	Shows the login day, date, and time for the connection.
Privileges	Shows whether the connection has privileges, such as Supervisor or Console Operator.
Connection Type	Shows whether the connection is internal or external.
Bytes Read	Shows the total number of reads made by the connection.
Bytes Written	Shows the total number of writes made by the connection.
NCP Requests	Shows the total number of NCP requests made by the connection.
IP Address	Shows the IP address where the connection originates.
Open Files	Shows the files open for the connection.
Security Equivalence	Shows the name of the user, server, or service if it is logged in.

9.2 Managing User Login for NCP Server

- ◆ [Section 9.2.1, “Enabling Login,” on page 70](#)
- ◆ [Section 9.2.2, “Disabling Login,” on page 70](#)

9.2.1 Enabling Login

- 1 Open a terminal console, then log in as the root user.
- 2 At the terminal console prompt, enter

```
ncpcon enable login
```

9.2.2 Disabling Login

- 1 Open a terminal console, then log in as the root user.
- 2 At the terminal console prompt, enter

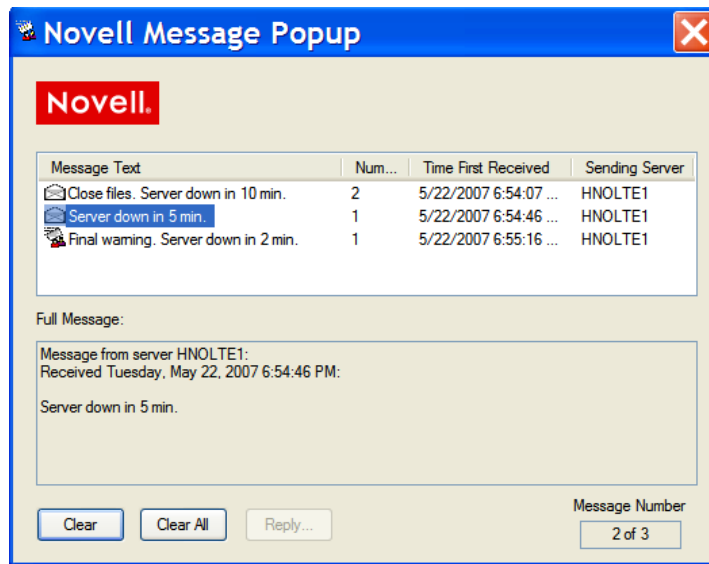
```
ncpcon disable login
```

9.3 Sending Messages to Logged-In Users

You can use the Connection Manager to send a message to NCP clients that are connected to the NCP Server via the Novell Client. Broken connections and users that are not logged in through Novell Client software do not receive the message. You typically send messages before you shut down, reset, or restart your server for any reason. You might also want to send a message to a specific user before you close an open file or clear a connection.

For example, the message appears in a *Novell Message Popup* dialog box at the users' workstations.

Figure 9-1 Example Message Delivery



- ◆ [Section 9.3.1, “Enabling or Disabling Broadcast Message Support,” on page 71](#)
- ◆ [Section 9.3.2, “Broadcasting a Message to All Users,” on page 71](#)
- ◆ [Section 9.3.3, “Sending a Message to a Specific User,” on page 72](#)
- ◆ [Section 9.3.4, “Configuring the Novell Client for Sending and Receiving Messages,” on page 72](#)

9.3.1 Enabling or Disabling Broadcast Message Support

The ability to send broadcast messages is enabled by default. You can disable this feature by enabling the `DISABLE_BROADCAST` parameter. The parameter's default setting is 0, which allows messages.

- 1 In Novell Remote Manager for Linux, select *Manage NCP Services > Manage Server*.
- 2 In the Server Parameter Information list, click the Parameter Value link for the `DISABLE_BROADCAST` parameter.
- 3 Specify the new value as 0 (default, enables broadcasting) or 1 (disables broadcasting), then click *Change*.

9.3.2 Broadcasting a Message to All Users

- 1 In Novell Remote Manager, click *Manage NCP Services > Manage Connections* to open the *Connections Manager* page.
- 2 Type the message in the *Broadcast Message to Everyone* field.

You can enter up to 252 characters and spaces in the message.

- 3 Click *Send*.

9.3.3 Sending a Message to a Specific User

- 1 In Novell Remote Manager, click *Manage NCP Services > Manage Connections* to open the *Connections Manager* page.
- 2 Scroll down to view the connections in the *Connection Listing* report.
- 3 Optionally sort the list by clicking the *Sort* icon ▼ in the column heading of interest.
- 4 Click the *Name* link for a specific connection to view details about it.
- 5 Type the message for the user in the *Send Message* field.

You can enter up to 252 characters and spaces in the message.

- 6 Click *Send*.

9.3.4 Configuring the Novell Client for Sending and Receiving Messages

For OES 2 SP1 and later, the Send Message capability is available in the Novell Client 4.9x for Windows XP/2003, the Novell Client 1.0 SP1 for Vista, and the Novell Client 2.0 for Linux.

The ability for a user to send and receive broadcast messages on the user's workstation is controlled by four NCP client property settings in the Novell Client Properties (right-click Red N, then select Novell Client Properties).

Table 9-4 Novell Client Properties for Broadcast Messages

Property	Description	Settings
Receive Broadcast Messages (under the Advanced Settings tab)	Specifies which broadcast messages, if any, to be received by this client.	All - Receive all broadcast messages. Server Only - Receive broadcast messages sent by NCP server only. None - Do not receive any broadcast messages.
Enable Send Message (under the Advanced Menu Settings tab)	Enables or disables the Send Message function for this client.	On (default) or Off
Enable Send Message to Server Dialog (under the Advanced Menu Settings tab)	Enables or disables the ability of this client to send broadcast messages to the NCP server where the user is logged in.	On or Off (default)
Enable Send Message to User Dialog (under the Advanced Menu Settings tab)	Enables or disables the ability of this client to send broadcast messages to specific NCP users.	On (default) or Off

A user can send a broadcast message by doing the following:

- 1 Right-click the Red N to open the menu, then select *Novell Utilities > Send Message > To Users* to open the Send Message dialog box.

- 2 From the list of available servers, double-click the server to see a list of users and groups connected to that server.

- 3 Type the message.

You can enter up to 252 characters and spaces in the message.

- 4 Select the users and groups to send the message to. Press and hold down the Control key to select multiple users or groups.

Only users who are logged in are eligible to receive the messages. Broken connections, users who are not logged in through Novell Client software, and users who are logged in with a Novell Client that does not support the Send Message feature cannot receive the message.

- 5 Click *Send*.

The Send Message Results dialog box appears, showing the users and groups to whom the message was sent.

9.4 Viewing Connections for NCP Server

For an explanation of the connection parameters, see [Section 9.1, “Understanding Connections,”](#) on page 67.

- ♦ [Section 9.4.1, “Using Novell Remote Manager,”](#) on page 73
- ♦ [Section 9.4.2, “Using NCPCON,”](#) on page 75

9.4.1 Using Novell Remote Manager

- 1 In Novell Remote Manager, click *Manage NCP Services > Manage Connections* to open the Connection Manager page.

The Connection Manager page reports the *Connection Information* and *Connection Listing*.

Connections



Connection Manager

Connection Information

Connection Slots Allocated 64

Connection Slots Being Used 18

Signing Level 1

Login State Allow Logins

Licensed Connections 1

Not Logged In Connections [Clear all "Not Logged In" Connections](#)

Broadcast Message to Everyone

Connections

Connection Listing					
Clear	Station	Name	Reads & Writes	NCP Requests	Login Time
	0	.CN=avalon.O=novell.T=AVALON_TREE.	0	0	Mon, May 21 2007 10:56:00 am
<input type="checkbox"/>	1	*.CN=avalon.O=novell.T=AVALON_TREE.	0	0	Mon, May 21 2007 10:56:17 am

- Optionally sort the *Connection Listing* by clicking the *Sort* icon ▼ in the column heading of the information of interest.

The default sort order is by stations. The current sort order is indicated by the *Sorted By* icon ▾ in the column heading. The *Login Time* heading sorts from the least recent to the most recent.

- (Optional) Click the *Name* link for a specific connection to view more details about it.

Connection Information



avalon.novell

[\[Back to Connections\]](#)

[Clear Connection](#)

Connection Information

Connection 1

Login Status Authenticated

Authentication Method NDS

Login time Tue, May 22 2007 10:53:42 am

Privileges Supervisor

Connection Type Internal

NCP Requests 0

Bytes Read 0

Bytes Written 0

Network Address IP 137.65.67.37

Send Message

Open Files

Security Equivalence .CN=avalon.O=novell.T=AVALON_TREE.
.O=novell.T=AVALON_TREE.
.T=AVALON_TREE.
.[Public].

9.4.2 Using NCPCON

- 1 Open a terminal console, then log in as the root user.
- 2 At the terminal console prompt, enter the following to open the NCP Server Console (`ncpcon(8)`) utility:

```
ncpcon
```

- 3 At the NCPCON prompt, do any of the following:
 - ♦ Get the *Connection Information* report by entering

```
connection
```
 - ♦ Get the *Connection Listing* report by entering

```
connection list
```
 - ♦ Get the *Detailed Connection Information* report for a specific connection by entering

```
connection connection_number
```


Replace *connection_number* with the station number of the connection of interest. You can find the connection number by viewing the connection listing.


9.5 Sorting Entries in the Connection Listing

In the *Connection Listing* report on the Connection Manager page, you can sort the connection information by any of the column headings:

- ♦ *Station* (default; ascending order, with Connection 0 first)
- ♦ *Name* (alphabetical order)
- ♦ *Reads and Writes* (descending order, largest volume of traffic first)
- ♦ *NCP Requests* (descending order, highest number of requests first)
- ♦ *Login Time* (reverse chronological order, longest duration first)

The current sort order is indicated by the Sorted By icon  in the column heading.

- 1 In Novell Remote Manager, click *Manage NCP Services > Manage Connections* to open the *Connection Manager* page.
- 2 Scroll down to view the *Connection Listing* report.
- 3 Sort the entries in the *Connection Listing* by clicking the *Sort* icon  in the column heading of interest.

When the page refreshes, the list is sorted in order by that connection information, and the *Sorted By* icon  appears in its column heading.

9.6 Clearing Not-Logged-In Connections to NCP Server

If users cannot connect to the server, all the licensed user connections might be in use. You can view and clear the connections of users with active connections that are not logged in to the server.

For example, if a user reboots a workstation without properly logging out, the server sends a watchdog packet to that workstation to see if it is still communicating with the server. The server continues to send watchdog packets until the workstation logs in again and re-establishes its connection with the server, or until the watchdog drops the connection because of the lack of response from the workstation.

IMPORTANT: You should be careful in clearing connections based on NLM programs because some backup NLM programs establish a connection during the server initialization process and maintain a Not Logged In connection to the server until it is time to log in and run the backup process. These types of NLM connections cannot re-establish a connection to the server unless the NLM is manually unloaded and reloaded at the server console, which might prevent it from functioning properly at the designated time of execution.

To clear connections to the NCP Server for users or NLM programs that are not logged in:

- 1 In Novell Remote Manager, click *Manage NCP Services > Manage Connections* to open the *Connection Manager* page.
- 2 In the *Connection Listing*, click the *Sort* icon ▼ for the *Name* column so that all *Not Logged In* connections are grouped together.
- 3 Review the *Not Logged In* connections to determine which ones you want to clear.
- 4 Optionally click the *Name* link for a specific connection to view more details about it.
- 5 Do one of the following:
 - ♦ **Clear All Not Logged in Connections:** Under *Connection Information*, click the *Clear All "Not Logged In" Connections* link.
 - ♦ **Clear One or Multiple Not Logged In Connections:** Under *Connection Listing*, select the check box next to the specific *Not Logged In* connections you want to clear, then click *Clear ALL Marked Connections*.

9.7 Clearing Connections to NCP Server

You might need to clear connections for one or multiple users. For example, if a user's workstation quits working, it usually leaves its connection to the server open and might also leave files open. You can clear the user's connection to allow the open files to close.

- ♦ [Section 9.7.1, "Using Novell Remote Manager to Clear NCP Connections,"](#) on page 76
- ♦ [Section 9.7.2, "Using NCPCON to Clear NCP Connections,"](#) on page 77

9.7.1 Using Novell Remote Manager to Clear NCP Connections

- 1 In Novell Remote Manager, click *Manage NCP Services > Manage Connections* to open the *Connections Manager* page.
- 2 Scroll down to view the connections in the *Connection Listing* report.
- 3 Optionally sort the list by clicking the *Sort* icon ▼ in the column heading of interest.
- 4 Review the connections to determine which ones you want to clear.

- 5 Optionally click the *Name* link for a specific connection to view more details about it. From this page, you can click the *Clear Connection* link, or click *Back to Connections* to return to the *Connection Manager* page.
- 6 Select the check box next to each specific connection that you want to clear.
- 7 Click *Clear ALL Marked Connections*.

9.7.2 Using NCPCON to Clear NCP Connections

- 1 Open a terminal console, then log in as the root user.
- 2 At the terminal console prompt, enter the following to open the NCP Server Console (`ncpcon(8)`) utility:

```
ncpcon
```

- 3 Get the *Connection Listing* report by entering
- 4 Review the list to locate the connection number of the connection you want to clear.
- 5 Optionally get the *Detailed Connection Information* for a specific connection by entering

```
connection connection_number
```

- 6 Clear the connection by entering

```
connection clear connection_number
```

9.8 Finding the Connection that Has a File Open

Sometimes you know the filename of the file you want to close, and you need to find the connection associated with the file.

- 1 Open a terminal console, then log in as the root user.
- 2 At the console prompt, enter the following command to get a list of NCP connections for a given file:

```
ncpcon files list f=filename
```

Replace *filename* with the Linux path for the file, including the filename, such as `/usr/novell/sys/text.txt`.

```
ncpcon files list f=/usr/novell/sys/test.txt
```

9.9 Viewing Open Files for an NCP Server Connection, and Closing All Open Files

Before clearing a connection and closing all of its open files, you might want to get an idea of the types of files that the user or operation might be accessing. For example, you might want more information about the connection if the connection has been open a long time, or it has a large volume of traffic associated with it.

- 1 In Novell Remote Manager, click *Manage NCP Services > Manage Connections* to open the *Connections Manager* page.
- 2 Scroll down to view the connections in the *Connection Listing* report.

- 3 Optionally sort the list by clicking the Sort icon ▼ in the column heading of interest.
- 4 Click the *Name* link for a specific connection to view its details.
- 5 Scroll down to view the *Open Files* section for a list of files currently opened by the selected connection.

The application that is used to open a file determines whether the file is held open and locked for access to other users. Some applications open the file and copy the information to a working file, and overwrite the original when you save changes. These open files do not appear in the Open Files list. Other applications create a temporary file for changes and lock the original file for write access to other users. These open files appear in the Open Files list. The temporary file is listed in a file system view, but does not appear as an open file. When you clear the connection, the open files in the list are closed, and the application should automatically close and delete the temporary files.

For example, Microsoft Word creates a system file that begins with ~\$, such as ~\$myfile8.doc. OpenOffice and LibreOffice create a hidden file that begins with .~lock, such as .~lock.myfile10.odt. You can view the temporary files by selecting *Manage Shares*, then navigating the NCP volume or NSS volume to the folder where the open file is stored.

- 6 (Optional) If the connection is opened by a user, you can send a brief message before clearing the connection. Type the message in the *Send Message* field, then click *Send*.
Broadcast messages work only for users that are using a Novell Client that supports broadcast messages, and the broadcast message option is enabled.
- 7 (Optional) Clear the connection and close all open files by clicking *Clear Connection* link at the top of the report.

9.10 Viewing Open Files for an NCP Server Connection, and Closing a Specific Open File

You might want to close a specific open file for a connection for the following scenario:

- ♦ A file in a shared storage area has been held open for a very long time. The application that is being used (such as Microsoft Word or OpenOffice) has locked the file for write access to other users.
- ♦ You know which user has the file open, and the user is not available to close the file, or cannot close the file.
- ♦ The user has multiple files open.
- ♦ You want to close only one of the files.

Use `NCPCON` to view the list of open files for a connection, then close a specific open file:

- 1 Open a terminal console, then log in as the `root` user.
- 2 At the console prompt, enter the following command to get a list of NCP connections for a given file:

```
ncpcon files list f=filename
```

Replace *filename* with the Linux path for the file, including the filename, such as `/media/nss/VOL1/Document.rtf`.

For example, the following response shows that the `admin` user in connection 15 has a lock held open on the file:

```
# ncpcon files list f=/media/nss/VOL1/Document.rtf
... Executing " files list f=/media/nss/VOL1/Document.rtf"

Connection  User Name          Rights
15          .CN=admin.O=novell.T=SUMMER. 0x9

Count of locks found on the file /media/nss/VOL1/Document.rtf: 1.
... completed OK [elapsed time = 1 Second 4294051 msecs 640 usecs]
```

- 3 Visually confirm that you have the correct file and connection.
- 4 Enter the following command to close the open file by filename:

```
ncpcon files close f=filename
```

For example, enter

```
ncpcon files close f=/media/nss/VOL1/Document.rtf
```

You can alternatively specify the connection number to close all open files for that connection, including the filename of interest.

```
ncpcon files close c=connection_number
```

For example, enter

```
ncpcon files close c=15
```

- 5 Verify that any temporary file that the application opened for the file has been removed from the folder by the application. Otherwise, the user might not be able to save changes to the file of interest.

For more information about temporary files created by an application, see [Step 5 in Section 9.9, "Viewing Open Files for an NCP Server Connection, and Closing All Open Files,"](#) on page 77.

- 5a In Novell Remote Manager, select *Managing NCP Services > Manage Shares*.
- 5b Click the volume's name link, then navigate the directory structure to the folder where the open file was located.
- 5c Use the Search feature to find a temporary file for the open file, such as `~$myfile.doc` or `~lock.myfile.odt`.
- 5d Click the *File Information* icon next to the file name.
- 5e On the File Information page, click *Delete File*.

9.11 Generating and Viewing NCP Trustee Reports for NSS Volumes

Under *Manage NCP Services*, the new *NCP Trustee Report* option allows you to generate a trustee report for a specified NSS volume. This includes Dynamic Storage Technology shadow volumes that are comprised of two NSS volumes. You can display the last trustee report in the Web browser, or send the report to the e-mail addresses that you have pre-configured for Novell Remote Manager. A trustee report shows the rights settings by folder for each user or group that is a trustee on the NSS volume.

- ♦ [Section 9.11.1, "Generating an NCP Trustee Report,"](#) on page 80
- ♦ [Section 9.11.2, "Viewing a Saved NCP Trustee Report,"](#) on page 80
- ♦ [Section 9.11.3, "Emailing a Saved NCP Trustee Report,"](#) on page 80

9.11.1 Generating an NCP Trustee Report

- 1 Log in to Novell Remote Manager as the `root` user.
- 2 In the left navigation panel, select *Manage NCP Services > NCP Trustee Report*.



- 3 On the NCP Trustee Reports page, locate the NSS volume in the list, then click its *Create* link in the *Generate Report* column.
- 4 View the NCP Trustee Report.

A volume's trustee report shows the rights settings by folder for each user or group that is a trustee on the NSS volume. For example, the following trustee report shows the rights for a folder in a Dynamic Storage Technology shadow volume.



9.11.2 Viewing a Saved NCP Trustee Report

You can view the last saved trustee report for an NSS volume. The saved report provides the same trustee rights information that was available when the report was created.

- 1 Log in to Novell Remote Manager as the `root` user.
- 2 In the left navigation panel, select *Manage NCP Services > NCP Trustee Report*.
- 3 Locate the NSS volume of interest in the list, then click its *Display* link in the *View Last Report* column.

9.11.3 Emailing a Saved NCP Trustee Report

You can email an NCP volume's trustee report to addresses that are configured in the `httpstkd.conf` file. For information about setting up email addresses for Novell Remote Manager, see "[Email Notification Commands](#)" in the *OES 2 SP3: Novell Remote Manager for Linux Administration Guide*.

- 1 Log in to Novell Remote Manager as the `root` user.
- 2 In the left navigation panel, select *Manage NCP Services > NCP Trustee Report*.
- 3 Locate the NSS volume of interest in the list, then click its *Send* link in the *Email Report* column.

10 Managing NCP Volumes

This section describes how to create and manager NCP volumes on a Novell Open Enterprise Server (OES) 2 Linux server.

- ♦ [Section 10.1, “Understanding NCP Volumes,” on page 81](#)
- ♦ [Section 10.2, “Creating NCP Volumes on Linux File Systems,” on page 83](#)
- ♦ [Section 10.3, “Mounting NCP Volumes,” on page 85](#)
- ♦ [Section 10.4, “Dismounting NCP Volumes,” on page 86](#)
- ♦ [Section 10.5, “Viewing the Size of an NCP Volume,” on page 87](#)
- ♦ [Section 10.6, “Purging Deleted Files from an NSS Volume,” on page 87](#)
- ♦ [Section 10.7, “Removing an NCP Volume,” on page 88](#)
- ♦ [Section 10.8, “Configuring Inherit POSIX Permissions for an NCP Volume,” on page 89](#)
- ♦ [Section 10.9, “Configuring the NCP/NSS Bindings for an NSS Volume,” on page 92](#)

10.1 Understanding NCP Volumes

NCP volumes are NCP shares on Linux POSIX file systems such as Ext3, XFS, and Reiser. Novell Storage Services (NSS) volumes are a special type of NCP volume.

The directory and file access is controlled with the NetWare trustee model for file system trustees and trustee rights. Users access data on NCP volumes by using the Novell Client software on their Windows, Vista, or Linux workstations. This document refers collectively to those workstations as “Novell clients”.

To give eDirectory users access to the files via Samba, you can Linux-enable users with Linux User Management. NCP authenticates users and enforces the trustee settings. For information about Linux-enabling users with Linux User Management, see the [OES 2 SP3: Novell Linux User Management Administration Guide](#).

- ♦ [Section 10.1.1, “NCP Shares as NCP Volumes,” on page 81](#)
- ♦ [Section 10.1.2, “NSS Volumes as NCP Volumes,” on page 82](#)
- ♦ [Section 10.1.3, “Understanding Time Stamps on Linux,” on page 82](#)

10.1.1 NCP Shares as NCP Volumes

Create NCP shares by specifying mount points on any Linux POSIX file system by using NCP Server Console (NCPCON, `ncpcon(8)`) utility or Novell Remote Manager (NRM) for Linux.

When NCP Server is installed, an NCP volume named SYS is automatically created and mounted. Its NCP share mount point is `/usr/novell/sys`. This NCP volume contains the same `login` and `public` directories that exist on NetWare. These directories let Novell clients run commands for logging in, mapping drives, and so on, as well as the means for client commands to be run from login scripts.

Creating an NCP volume for Linux POSIX file systems adds the NCP volume mount information to `/etc/opt/novell/ncpserv.conf` and creates a Volume object in Novell eDirectory. Volume names can be up to 14 alphanumeric characters. Underscores are allowed.

If the server is in a Novell Distributed File Services management context, you must run VLDB repair to create a DFS GUID (globally unique ID) to add as an attribute of the Volume object, and to add the volume information to the VLDB database. For information about using DFS junctions for NSS volumes, see the *OES 2 SP3: Novell Distributed File Services Administration Guide for Linux*.

10.1.2 NSS Volumes as NCP Volumes

By default, NSS volumes created with NSS management tools are NCP volumes. You create and manage NSS volumes by using the NSS Management Utility (NSSMU) or the Storage plug-in for Novell iManager, just as you do on NetWare.

In order to create an NSS volume on your OES 2 Linux server, you must install the Novell Storage Services component of OES 2 Services.

IMPORTANT: For information about creating and managing NSS volumes on Linux, see “[Managing NSS Volumes](#)” in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

Novell clients can access NSS files on a Linux server if the following requirements are met:

- ◆ NCP Server is installed and running on the server.
- ◆ The administrator user has created NSS pools and volumes with NSSMU or the Storage plug-in to iManager.
- ◆ The administrator, or a user with sufficient file system rights, has made the appropriate volume, directory, and file trustee assignments for users of the data (that is, for non-administrator users).

If the server is in a Novell Distributed File Services management context, a DFS GUID is automatically created when you create an NSS volume with NSSMU or iManager. Its DFS GUID is added as an attribute of the volume’s Volume object in eDirectory, and an entry is added to the VLDB. For information about using DFS junctions for NSS volumes, see the *OES 2 SP3: Novell Distributed File Services Administration Guide for Linux*.

10.1.3 Understanding Time Stamps on Linux

In NCPCON and in the Novell Remote Manager for Linux, you can make your selection based on three time stamps:

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

These time stamps are defined by POSIX and supported by Linux. Many operations change more than one time stamp. The change time is controlled automatically.

NCP can modify the access time and the modify time, but cannot control whether the change time is reset. For example, if you copy a file from one location to another, NCP can preserve the access and modify times, but the change time is reset because the file’s path changed. That is, it had a status change but the file was not opened for access and its data was not modified.

10.2 Creating NCP Volumes on Linux File Systems

Creating an NCP share on a Linux POSIX file system creates an NCP volume name and associates it to a path for its mount point. You must create one or multiple NCP volumes in order to make Linux POSIX file system files and directories on an OES 2 Linux server accessible to workstations running Novell Client software. Novell clients can then access files and folders on that NCP volume just like they do on NetWare.

IMPORTANT: The procedures in this section apply only to NCP shares on Linux POSIX file systems, not NSS volumes. For information about creating and managing NSS volumes on Linux, see [“Managing NSS Volumes”](#) in the *OES 2 SP3: NSS File System Administration Guide for Linux*.

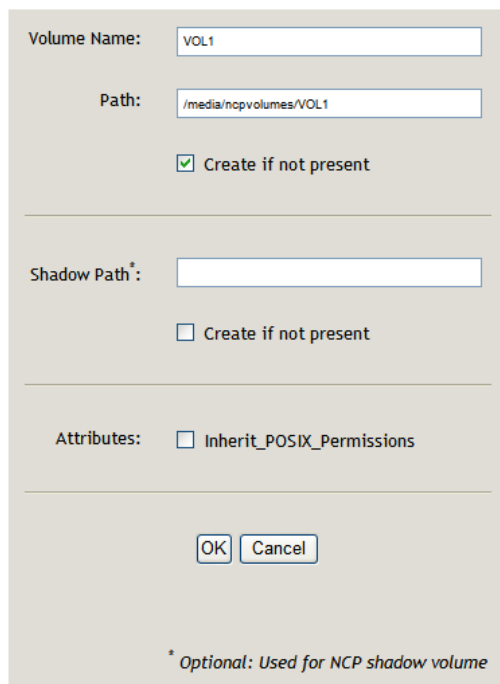
- ♦ [Section 10.2.1, “Using Novell Remote Manager to Create an NCP Volume on a Linux File System,”](#) on page 83
- ♦ [Section 10.2.2, “Creating an NCP Volume with NCPCON,”](#) on page 84

10.2.1 Using Novell Remote Manager to Create an NCP Volume on a Linux File System

- 1 In Novell Remote Manager, click *Manage NCP Services > Manage Shares*, then click *Create New Share*.
- 2 In *Volume Name*, type the name of the NCP volume you want to create, such as *VOL1*.

The share name you specify is the volume name NCP clients will see. It is associated to a path on your Linux server. Names can be up to 14 alphanumeric characters. Underscores are allowed.

Step 1: Enter NCP Volume (share) to create



Volume Name:

Path:

Create if not present

Shadow Path* :

Create if not present

Attributes: Inherit_POSIX_Permissions

* Optional: Used for NCP shadow volume

- 3 In *Path*, specify the path on a Linux POSIX file system (Ext3, XFS, or Reiser) to the NCP share name, then select *Create If Not Present* check box beneath it if the directory in the path does not already exist.

For example, type `/media/ncpvolumes/VOL1` as the share path.

IMPORTANT: You should not create an NCP share on NSS file systems. NSS volumes are by default NCP shares.

- 4 In *Shadow Path*, leave the field blank and do not select the *Create If Not Present* check box beneath it.

IMPORTANT: In the initial release of Dynamic Storage Technology (DST), the *Shadow Path* field is a placeholder for a future capability that will allow you to create a DST shadow volume when you create the NCP volume's share. When this DST capability is supported, the NCP share is the primary storage location, and the shadow path is the secondary storage location that is also a share on Linux file systems. This capability is not supported in the initial release of OES 2 Linux and DST.

- 5 (Optional) Enable or disable the *Inherit POSIX Permissions* option by selecting or deselecting the check box.

The *Inherit POSIX Permissions* option is disabled (deselected) by default. This setting applies only for the specified NCP volume on Linux POSIX file systems (that is, for Ext3, XFS, or Reiser file systems, and not for NSS).

IMPORTANT: We recommend that the *Inherit POSIX Permissions* option be disabled (deselected). For information about the security implications of enabling this option, see [Section 10.8, "Configuring Inherit POSIX Permissions for an NCP Volume,"](#) on page 89.

- 6 Click *OK* to confirm the creation of the NCP volume (share).

This creates a mount point to the volume (share) name you specified, and mounts it to make it accessible to NCP clients.

- 7 Verify that the share was created successfully by clicking *Manage NCP Services > Manage Shares* to see a list of NCP shares.

The NCP volume should appear in the list, and be mounted. Mounted volumes appear with the name hyperlinked, and an *Unmount* button next to it.



10.2.2 Creating an NCP Volume with NCPCON

- 1 Open a terminal console on the Linux server that you want to manage, then log in as the `root` user.
- 2 Use one of the following methods to create an NCP share on a Linux POSIX volume:

- ♦ At the terminal console prompt, enter `ncpcon` to open the NCPCON utility, then enter

```
create volume ncp_volume_name path
```

- ♦ At the terminal console prompt, enter

```
ncpcon create volume ncp_volume_name path
```

For example, if the volume name is `vol1` and the path is `/home/novell`, enter

```
ncpcon create volume vol1 /home/novell
```

Replace *ncp_volume_name* with the name you want to assign to the new volume. Volume names are not case sensitive. Replace *path* with the path to the directory on your Linux server where you want the mount point to be created.

10.3 Mounting NCP Volumes

After creating an NCP volume, you must mount it to make it accessible to users via the Novell Client. Any NCP volume that has been dismounted must also be mounted before it can be accessed.

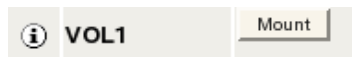
- ♦ [Section 10.3.1, “Mounting an NCP Volume with Novell Remote Manager,” on page 85](#)
- ♦ [Section 10.3.2, “Mounting an NCP Volume with NCPCON,” on page 85](#)
- ♦ [Section 10.3.3, “Using the ncpmount\(8\) Command from a Client,” on page 86](#)

10.3.1 Mounting an NCP Volume with Novell Remote Manager

If you create an NCP volume with Novell Remote Manager, the volume is automatically mounted when it is created.

To mount an NCP volume:

- 1 In Novell Remote Manager, click *Manage NCP Services > Manage Shares*, then click the *Mount* button next to the NCP volume you want to mount.



10.3.2 Mounting an NCP Volume with NCPCON

- 1 Open a terminal console on the Linux server that you want to manage, then log in as the `root` user.
- 2 Use one of the following methods to mount an NCP volume:

- ♦ At the terminal console prompt, enter `ncpcon` to open the NCPCON utility, then enter

```
mount ncp_volume_name
```

- ♦ At the terminal console prompt, enter

```
ncpcon mount ncp_volume_name
```

For example, if volume `sys` is dismounted, mount it by entering

```
ncpcon mount sys
```

Replace *ncp_volume_name* with the name of the NCP volume you want to mount. Volume names are not case sensitive. You can also replace *ncp_volume_name* with *all* to mount all NCP volumes on the server.

10.3.3 Using the `ncpmount(8)` Command from a Client

You might use the Linux `ncpmount(8)` command to mount an NCP volume from a client in the following scenarios:

- ♦ If the Novell Client is not installed on the client
- ♦ If you want to automatically mount the NCP volume on system start

The connection must be established using native NCP over a TCP/IP network. The `ncpmount` command is part of the `ncpfs` package. For NCP volumes on OES Linux, only the DOS and LONG namespaces are supported for the `ncpmount` command. For NetWare servers, the DOS, AFP, NFS, and LONG namespaces are supported for the `ncpmount` command.

When you invoke the `ncpmount` command from a client to mount an NCP volume on the client, it sends a "Name Spaces Loaded List from Volume Number" request to NCP Server.

For NCP server on Linux, the response to the request is:

- ♦ 0x00 (DOS)
- ♦ 0x04 (LONG/OS/2)

For NCP Server on NetWare, the response to the request is:

- ♦ 0x00 (DOS)
- ♦ 0x01 (AFP)
- ♦ 0x02 (NFS)
- ♦ 0x04 (LONG/OS/2)

10.4 Dismounting NCP Volumes

Dismounting an NCP volume removes accessibility for Novell clients to the mount point represented by the volume name.

- ♦ [Section 10.4.1, "Dismounting an NCP Volume with NCPCON," on page 86](#)
- ♦ [Section 10.4.2, "Dismounting an NCP Volume with Novell Remote Manager," on page 87](#)

10.4.1 Dismounting an NCP Volume with NCPCON

- 1 Open a terminal console on the Linux server that you want to manage, then log in as the root user.
- 2 Use one of the following methods to dismount an NCP volume:

- ♦ At the terminal console prompt, enter `ncpcon` to open the NCPCON utility, then enter

```
dismount ncp_volume_name
```

- ♦ At a terminal console prompt, enter

```
ncpcon dismount ncp_volume_name
```

For example, if volume `vol1` is mounted, dismount it by entering

```
ncpcon dismount vol1
```

Replace `ncp_volume_name` with the name of the NCP volume you want to dismount. Volume names are not case sensitive.

10.4.2 Dismounting an NCP Volume with Novell Remote Manager

- 1 In Novell Remote Manager, click *Manage NCP Services > Manage Shares*, then click the *Unmount* button next to the NCP volume you want to dismount.

10.5 Viewing the Size of an NCP Volume

The amount of space available to an NCP volume depends on the size of the partition where the underlying Linux POSIX file system was created and any additional devices that might be mapped to paths that are under the NCP volume's share path. Space on the Linux file system is overbooked from the point of view of the NCP shares on it. If you create multiple NCP volumes on the same Linux volume, each NCP volume reports the space available to it as the unused space on the Linux volume.

You can use the Volume Inventory report in Novell Remote Manager for Linux to view the size of the NCP volume and the space available to it. Do not use Linux utilities (such as `df -h`) to determine the size of an NCP volume.

- 1 Open Novell Remote Manager for Linux for the server you want to manage.
- 2 Select *View File System*, then select *Volume Inventory*.
- 3 Click the link of the NCP volume to create a Volume Inventory report for the volume.
- 4 Under *Key Statistics*, view the *Space in Use* and *Space Available*.

10.6 Purging Deleted Files from an NSS Volume

Deleted files might be available for salvage on NSS volumes where the Salvage attribute is enabled. Purging deleted files permanently removes them from the volume. Purged files cannot be salvaged.

- ♦ [Section 10.6.1, "Purging Deleted Files with NCPCON," on page 87](#)
- ♦ [Section 10.6.2, "Purging Deleted Files with Management Tools," on page 88](#)

10.6.1 Purging Deleted Files with NCPCON

The `purge volume` command in NCPCON purges deleted files from an NSS volume on Linux. This command works only with NSS volumes.

- 1 Open a terminal console on the Linux server you want to manage, then log in as the `root` user.
- 2 Use one of the following methods to dismount an NCP volume:

- ♦ At the terminal console prompt, enter `ncpcon` to open the NCPCON utility, then enter

```
purge volume ncp_volume_name
```

- ♦ At a terminal console prompt, enter

```
ncpcon purge volume ncp_volume_name
```

For example, to purge all deleted files on an NSS volume `vol1`, enter

```
ncpcon purge volume vol1
```

Replace `ncp_volume_name` with the name of the NSS volume where you want to purge all deleted files. Volume names are not case sensitive.

10.6.2 Purging Deleted Files with Management Tools

Purging deleted NSS files by using Novell Remote Manager for Linux is currently not possible.

You can purge and salvage (or undelete) NSS files on your Linux server by using the following tools:

- ♦ **The Files and Folders role in iManager 2.7:** For instructions, see “[Salvaging and Purging Deleted Volumes, Directories, and Files](#)” in the *OES 2 SP3: NSS File System Administration Guide for Linux*.
- ♦ **NetStorage:** For instructions, see “[Purging and Salvaging Deleted NSS Files](#)” in the *OES 2 SP3: NetStorage Administration Guide*.
- ♦ **Novell Client:** For information, see “[Using the Novell Client](#)” in the *OES 2 SP3: File Systems Management Guide*.

10.7 Removing an NCP Volume

Removing an NCP volume deletes the NCP share mount point information (path and volume name association) from the `/etc/opt/novell/ncpserv.conf` file. It also removes the NCP volume’s Volume object from Novell eDirectory. It does not remove or delete data from the directory represented by the share path. NCP clients cannot see or access the data after it is no longer defined as an NCP volume.

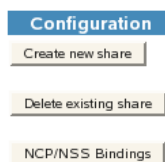
IMPORTANT: If the NCP volume is in a Novell Distributed File Services management context, removing the NCP volume’s Volume object breaks junctions that point to that NCP volume. If you create an NCP volume by the same name for the same share, the junctions are still broken because the DFS GUID is different. You must delete and re-create the junctions that point to the new NCP volume.

After an NCP volume has been removed, if you need to restore the mount point, you must create a new NCP volume for the share as you did when you first created it.


- ♦ [Section 10.7.1, “Removing an NCP Volume with Novell Remote Manager,”](#) on page 88
- ♦ [Section 10.7.2, “Removing an NCP Volume with NCPCON,”](#) on page 89

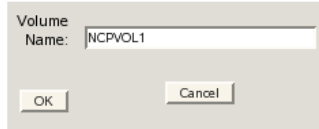
10.7.1 Removing an NCP Volume with Novell Remote Manager

- 1 In Novell Remote Manager, click *Manage NCP Services > Manage Shares*.
- 2 In the *Configuration* area, click *Delete Existing Share*.



- 3 Enter the name of the NCP volume you want to remove, click *OK*.

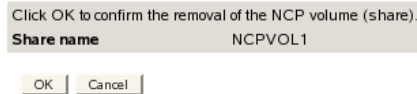
Step 1: Enter NCP Volume (share) name to remove 



Volume Name: NCPVOL1
OK Cancel

- 4 Verify the information, then *OK* to confirm the volume removal.

Step 2: Confirmation of NCP Volume (share) removal.



Click OK to confirm the removal of the NCP volume (share).
Share name NCPVOL1
OK Cancel

- 5 When the NCP share has been removed successfully, click *Done* to return to the Manage Shares page.

10.7.2 Removing an NCP Volume with NCPCON

- 1 Open a terminal console on the Linux server you want to manage, then log in as the root user.
- 2 Use one of the following methods to remove an NCP volume:

- ♦ At the terminal console prompt, enter `ncpcon` to open the NCPCON utility, then enter

```
remove volume ncp_volume_name
```

- ♦ At a terminal console prompt, enter

```
ncpcon remove volume ncp_volume_name
```

For example, to remove volume `vol1`, enter

```
ncpcon remove volume vol1
```

Replace `ncp_volume_name` with the name of the NCP volume that you want to remove. Volume names are not case sensitive.

10.8 Configuring Inherit POSIX Permissions for an NCP Volume

For NCP volumes on Linux, the ability to inherit POSIX permissions (Group ID and mode bits) from a parent directory is disabled by default. This ensures that local access to data (that is, local access in the Linux environment, not via Novell eDirectory) is available only to the `root` user. Only authorized eDirectory users can access the data. As with NetWare volumes, NCP Server controls access to data by using the Novell trustee model of file system trustees and trustee rights.

If the *Inherit POSIX Permissions option* is enabled, it allows the POSIX permissions (GID and mode bits) to be inherited from the parent directory. This lets shared areas be more easily created and managed for local Linux users. However, it makes the volume less secure.

IMPORTANT: The disabled setting for the *Inherit POSIX Permissions option* is a more secure management method for NCP volumes.

Inherit POSIX Permissions is disabled by default and is not allowed to be set on an NSS volume. There is an explicit check for this, and if the volume is an NSS volume, an error 22 is returned. NSS has its own handling of POSIX permissions. For information, see [Section 6.2.1, "POSIX Permissions](#)

on the NSS File System,” on page 51.

Inherit POSIX Permissions is disabled by default on clustered NCP volumes in the OES 2 SP1 Linux and earlier releases. You cannot use the methods described in this section to set the Inherit POSIX Permissions option for a clustered NCP volume because it does not have an entry in the `ncpserv.conf` file. The clustered NCP volume is defined in the mount command line in its cluster resource load script and removed in its unload script.

IMPORTANT: For clustered NCP volumes, an option to set Inherit POSIX Permissions in the cluster load script is planned for OES 2 SP2 Linux. Contact Novell Support if you need to enable the Inherit POSIX Permissions option for a clustered NCP volume on OES 2 SP1 Linux.

Use any of the following methods to configure the Inherit POSIX Permissions setting for unclustered NCP volumes:

- ♦ [Section 10.8.1, “Configuring the Inherit POSIX Permissions for a New NCP Volume,” on page 90](#)
- ♦ [Section 10.8.2, “Configuring the Inherit POSIX Permissions Setting for an Existing NCP Volume,” on page 90](#)

10.8.1 Configuring the Inherit POSIX Permissions for a New NCP Volume

You can enable or disable the *Inherit POSIX Permissions* option when you create an NCP volume on a Linux POSIX file system in Novell Remote Manager. The option is disabled by default. For information about creating an NCP volume, see [Section 10.2.1, “Using Novell Remote Manager to Create an NCP Volume on a Linux File System,” on page 83](#).

10.8.2 Configuring the Inherit POSIX Permissions Setting for an Existing NCP Volume

- ♦ [“Using Novell Remote Manager” on page 90](#)
- ♦ [“Using NCPCON” on page 91](#)
- ♦ [“Using ncpconf” on page 91](#)

Using Novell Remote Manager

- 1 In a Web browser, open Novell Remote Manager for Linux for the server you want to manage, then log in as the `root` user.
- 2 Select *Manage NCP Services > Manage Shares*.
- 3 On the NCP Shares page, locate the volume’s share name in the *Active Shares* area.
- 4 If the volume is mounted, click *Unmount* next to its share name.
- 5 Click the *Information* icon next to the volume’s share name.
- 6 On the Share Information page, click *Attributes*.
- 7 On the Modify Volume Properties page, enable or disable the *Inherit_POSIX_Permissions* parameter by selecting or deselecting its check box, then click *Update*.
- 8 On the NCP Shares page, mount the volume by clicking *Mount* next to its share name.

Novell Remote Manager for Linux automatically restarts the Novell eDirectory daemon to make the changed setting take effect.

Using NCPCON

1 Open a terminal console, then log in as the `root` user.

2 Start NCPCON by entering the following at the terminal console prompt:

```
ncpcon
```

3 Display the current volume settings by entering the following at the NCPCON prompt:

```
change volume ncp_volumename
```

Replace `ncp_volumename` with the name of the NCP volume you want to manage.

4 Dismount the volume by entering the following at the NCPCON prompt:

```
dismount ncp_volumename
```

Replace `ncp_volumename` with the name of the volume you want to manage.

5 Enable or disable the `Inherit_POSIX_Permissions` setting the parameter to `On` or `Off`, by entering one the following commands:

```
change volume ncp_volumename Inherit_POSIX_Permissions on
```

```
change volume ncp_volumename Inherit_POSIX_Permissions off
```

6 Mount the volume by entering the following at the NCPCON prompt:

```
mount ncp_volumename
```

7 Display the volume settings again to verify the change you made to the `Inherit_POSIX_Permissions` setting. At the NCPCON prompt, enter

```
change volume ncp_volumename
```

8 Exit NCPCON by entering

```
exit
```

Using ncpconf

You can enable or disable the *Inherit POSIX Permissions* parameter for an existing NCP volume by adding the `Inherit_POSIX_Permissions` flag to the `VOLUME` definition for that volume in the NCP Server configuration file (`/etc/opt/novell/ncpserv.conf`). Remove the flag from a volume definition to disable it.

1 Dismount the NCP volume where you want to change the setting.

1a Open a terminal console, then log in as the `root` user.

1b At the terminal console prompt, enter

```
ncpcon dismount ncp_volumename
```

Replace `ncp_volumename` with the name of the volume you want to manage.

2 Modify the setting for the volume in the `/etc/opt/novell/ncpserv.conf` file.

2a Open the `/etc/opt/novell/ncpserv.conf` file in text editor.

2b Do one of the following:

- ♦ **Enable:** Add the `Inherit_POSIX_Permissions` flag to the end of the `VOLUME` definition line for the NCP volume where you want to enable it:

For example:

```
VOLUME TEST1 /usr/Novell/TEST1 Inherit_POSIX_Permissions
```

- ♦ **Disable:** Remove the `Inherit_POSIX_Permissions` flag from the VOLUME definition line for the NCP volume where you want to disable it. This is the default setting.

For example:

```
VOLUME TEST1 /usr/Novell/TEST1
```

2c Save the file.

The changes do not go into effect until you restart `ndsd`.

3 Restart the Novell eDirectory (`ndsd`) daemon to make the changes to `ncpserv.conf` go into effect.

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

3a Use one of the following commands to stop `ndsd`:

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

3b Use one of the following commands to start `ndsd`:

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

4 Mount the NCP volume.

4a Open a terminal console, then log in as the `root` user.

4b At the terminal console prompt, enter

```
ncpcon mount ncp_volumename
```

Replace *ncp_volumename* with the name of the volume that you modified.

10.9 Configuring the NCP/NSS Bindings for an NSS Volume

- ♦ [Section 10.9.1, “Understanding the NCP/NSS Bindings Parameter,”](#) on page 92
- ♦ [Section 10.9.2, “Enabling the NCP/NSS Bindings for an NSS Volume,”](#) on page 94
- ♦ [Section 10.9.3, “Disabling the NCP/NSS Bindings for an NSS Volume,”](#) on page 95

10.9.1 Understanding the NCP/NSS Bindings Parameter

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

be mounted in NSS, but not in NCP Server. This allows DST to control access to the secondary storage area via the primary storage area. Files in the secondary storage area cannot be directly accessed by users.

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

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

NCP / NSS Bindings ?

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

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

Share Management Home

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

NCP / NSS Bindings ?

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

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

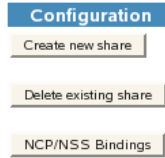
Share Management Home

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

10.9.2 Enabling the NCP/NSS Bindings for an NSS Volume

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

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



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

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

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

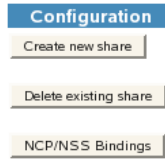
Available NSS volumes		
NCP Accessible	Volume Name	Mount point
Yes: <input checked="" type="radio"/> No: <input type="radio"/> Save Selection	VOL1	/media/nss/VOL1
Yes: <input type="radio"/> No: <input checked="" type="radio"/> Save Selection	ARCVOL	/media/nss/ARCVOL

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

10.9.3 Disabling the NCP/NSS Bindings for an NSS Volume

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

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



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

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

- 5 Beneath the volume's setting for *NCP Accessible*, click *Save Selection* to save and apply the new setting.
- 6 Verify that the NSS volume is not available for NCP by selecting *Manage NCP Services > Manage Shares* to view a list of active volumes.

If the NCP/NSS bindings were successfully disabled, the NSS volume should not appear in the *Volume Information* list.

11 Configuring NCP Volumes with Novell Cluster Services

This section describes how to share NetWare Core Protocol (NCP) volumes in Novell Open Enterprise Server (OES) 2 Linux clusters running Novell Cluster Services for Linux.

- ♦ [Section 11.1, “Planning for NCP Volumes in a Cluster Environment,” on page 97](#)
- ♦ [Section 11.2, “Clustering an NCP Volume on a Linux POSIX File System,” on page 99](#)
- ♦ [Section 11.3, “Sample Load, Unload, and Monitor Scripts for a Cluster-Enabled NCP Volume,” on page 108](#)

11.1 Planning for NCP Volumes in a Cluster Environment

Creating NCP volumes on clustered Linux POSIX file systems allows your NCP users to access the data using NCP clients. NCP volumes can be used in a cluster environment with some modifications to the load and unload scripts for the Linux POSIX cluster resource.

Make sure your system satisfies the [“Requirements for Creating Linux POSIX Volume Cluster Resources”](#) in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*. The additional prerequisites in this section apply for NCP volumes:

- ♦ [Section 11.1.1, “Novell Open Enterprise Server \(OES\) 2 Linux,” on page 97](#)
- ♦ [Section 11.1.2, “Novell Cluster Services for Linux,” on page 97](#)
- ♦ [Section 11.1.3, “NCP Server and Dynamic Storage Technology,” on page 98](#)
- ♦ [Section 11.1.4, “Shareable Devices,” on page 98](#)
- ♦ [Section 11.1.5, “EVMS Cluster Segment Manager,” on page 98](#)
- ♦ [Section 11.1.6, “File Systems,” on page 98](#)
- ♦ [Section 11.1.7, “Novell iManager 2.7,” on page 98](#)
- ♦ [Section 11.1.8, “Novell Remote Manager for Linux,” on page 98](#)

11.1.1 Novell Open Enterprise Server (OES) 2 Linux

NCP Server for Linux runs only on OES 2 Linux servers. For information about installing and configuring OES 2 Linux, see the [“OES 2 SP3: Installation Guide”](#).

11.1.2 Novell Cluster Services for Linux

NCP Server for Linux supports Novell Cluster Services for OES 2 Linux or later servers. For information, see [“Installing and Configuring Novell Cluster Services on OES 2 Linux”](#) in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

11.1.3 NCP Server and Dynamic Storage Technology

The NCP Server and Dynamic Storage Technology (DST) software are not cluster aware. This OES install option must be selected and installed on every OES 2 Linux node in the cluster where you want to fail over shared NCP volumes. You do not cluster NCP Server services or DST services.

For install information, see [Chapter 3, “Installing and Configuring NCP Server for Linux,”](#) on page 21.

11.1.4 Shareable Devices

The NCP volume must reside on a shareable device. For more information, see [“Shared Disk Configuration Requirements”](#) and [“SAN Rules for LUN Masking”](#) in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

- You need an unpartitioned disk or LUN that is connected via Fibre Channel or iSCSI protocols to the OES 2 Linux server.
- The disk or LUN must be able to be managed by EVMS.

11.1.5 EVMS Cluster Segment Manager

Novell Cluster Services for Linux requires that shared devices be managed by EVMS (Enterprise Volume Management System) and have a Cluster Segment Manager on the device. For information, see [“Requirements for Creating Linux POSIX Volume Cluster Resources”](#) in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

11.1.6 File Systems

In a cluster environment, NCP Server supports NCP volumes on Linux POSIX file systems, including Ext3, XFS, and ReiserFS. For information about requirements and caveats, see [“Requirements for Creating Linux POSIX Volume Cluster Resources”](#) in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.

To create or modify home directories on clustered NCP volumes or to manage any other elements that are managed using eDirectory objects, you must cluster migrate the cluster resource back to the node where the NCP volume was created before you perform those management tasks.

11.1.7 Novell iManager 2.7

The Clustering plug-in to iManager 2.7 is used to configure cluster resources, load scripts, and unload scripts for the Linux POSIX volume’s clustered resource. The Directory Administration plug-in is used to create the virtual cluster server object for the NCP volume.

11.1.8 Novell Remote Manager for Linux

The NCP Server plug-in to Novell Remote Manager for Linux is used to configure the NCP volume (or share) on a clustered Linux POSIX file system.

11.2 Clustering an NCP Volume on a Linux POSIX File System

This section describes how to configure a Linux POSIX file system for clustering with Novell Cluster Services for Linux, then how to set up a clustered NCP volume on the cluster resource. You can set up NCP volumes at the root of the cluster resource, or for subdirectories on it. You can create multiple NCP volumes on a Linux POSIX cluster resource. To provide NCP access to the share, you must create an NCS:NCP Server object and associate it with one or multiple NCP volumes, and bind the object to the IP address of the Linux POSIX cluster resource.

IMPORTANT: NCP Server does not support cross-protocol locks across a cluster migration or failover of the resource. If a file is opened with multiple protocols when the migration or failover begins, the file should be closed and reopened after the migration or failover to acquire cross-protocol locks on the new node.

For prerequisites, see [Section 11.1, “Planning for NCP Volumes in a Cluster Environment,”](#) on page 97.

- ♦ [Section 11.2.1, “Gathering Information for Clustering the NCP Volume,”](#) on page 99
- ♦ [Section 11.2.2, “Creating and Cluster-Enabling a Linux POSIX Volume,”](#) on page 101
- ♦ [Section 11.2.3, “Creating a Shared NCP Volume on the Linux POSIX Cluster Resource,”](#) on page 101
- ♦ [Section 11.2.4, “Creating a Virtual NCP Server Object for Shared NCP Volumes,”](#) on page 104
- ♦ [Section 11.2.5, “Modifying the Load Script for the Linux POSIX Cluster Resource,”](#) on page 106
- ♦ [Section 11.2.6, “Modifying the Unload Script for the Linux POSIX Cluster Resource,”](#) on page 107
- ♦ [Section 11.2.7, “Activating the Script Changes,”](#) on page 107

11.2.1 Gathering Information for Clustering the NCP Volume

Gather the information that you will use as you follow the steps to cluster an NCP volume.

IMPORTANT: On Linux, all names are case sensitive in the tools and cluster scripts.

Cluster Information	Example	Caveats
cluster name	cluster1	Name of the cluster.
cluster context	ou=cluster1,ou=boston,o=mycompany	Context where you created the cluster.
RESOURCE_IP	10.10.10.44	IP address of the Linux POSIX cluster resource. The cluster resource must have a unique static IP address that is in the same subnet as the IP addresses that are used for the cluster and cluster nodes.

Cluster Information	Example	Caveats
container_name	csM44	<p>Name of the EVMS Cluster Segment Manager (CSM) container.</p> <p>The container name must be one word, must consist of standard alphanumeric characters, and must not be any of the following reserved words:</p> <p>Container Disk EVMS Plugin Region Segment Volume</p>
evms_volumename	lxvol44	Name of the EVMS volume that you create on the CSM.
MOUNT_DEV	<i>/dev/evms/ container_name/ evms_volumename</i>	<p>The Linux path for the EVMS volume. For example:</p> <p><i>/dev/evms/csm44/lxvol44</i></p>
MOUNT_FS	ext3, XFS, or reiserfs	<p>The file system type you specify when you mount the volume.</p> <p>IMPORTANT: NCP Server for Linux supports NCP volumes on Ext3, XFS, or Reiser file systems.</p>
MOUNT_POINT	<i>/path_to_mount_point</i>	<p>The mount location for the EVMS volume. You can mount the EVMS volume anywhere. It can have the same or different name than the underlying EVMS volume. For example:</p> <p><i>/mnt/lxvol44 /mnt/users /home</i></p>
NCP_VOLUME	USERS	This is the name you give to the NCP volume. This is the share name seen by the users.
NCP_mount_point	<i>/path_to_mount_point</i>	The NCP share mount point must be the same as that for the EVMS volume (that is, at the root of the EVMS volume), or it can be a subdirectory below that location.
NCP_SERVER	cluster1_lxvol44_server	<p>The virtual server object (NCS:NCP Server) name for the NCP volume.</p> <p>This example uses a naming convention based on the one used by NSS pool resources (<i>clustername_poolname_server</i>), but the Linux POSIX cluster resource name is used instead.</p> <p><i>clustername_resourcename_server</i></p>

11.2.2 Creating and Cluster-Enabling a Linux POSIX Volume

The following procedure assumes that you are using a disk (or LUN) that does not contain data that you want to keep. You will initialize the disk and remove all segment managers.

WARNING: Initializing a disk destroys all data on it.

- 1 On the first OES 2 Linux node in the cluster, log in as the `root` user, then open a terminal console.
- 2 In NSSMU, initialize the disk that you want to use, mark the device as shareable for clustering, then exit NSSMU.
- 3 In EVMSGUI, create a Linux POSIX volume on a shared disk that is managed by EVMS.
For instructions, see [“Creating Linux POSIX Volumes on Shared Devices”](#) in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.
- 4 In iManager, cluster-enable the shared Linux POSIX volume with Novell Cluster Services.
For instructions, see [“Cluster-Enabling a Linux POSIX Volume on a Shared Device”](#) in the *OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux*.
- 5 After you have configured the Linux POSIX cluster resource, continue with [Section 11.2.3, “Creating a Shared NCP Volume on the Linux POSIX Cluster Resource,”](#) on page 101.

11.2.3 Creating a Shared NCP Volume on the Linux POSIX Cluster Resource

- ♦ [“Before You Begin”](#) on page 101
- ♦ [“Creating a Shared NCP Volume”](#) on page 102

Before You Begin

After you create the NCP volume by using the procedure in this section, you must restart `ndsd` on this node. Stopping `ndsd` sends a notification that the server is down to NCP users of the local volumes and existing cluster volumes that are mounted on the server.

Two cluster best practices should be observed:

- ♦ Perform maintenance tasks during non-peak hours so that users are minimally affected.
- ♦ When performing maintenance on a node, cluster migrate existing cluster resources to another node if you want the related users to be undisturbed.

If NCP users are connected to local or exiting cluster volumes on the node when you stop `ndsd`, they receive a `"Server is down"` notification from the NCP client.

When you start `ndsd`, NCP users of local volumes on the node are automatically reconnected and their sessions continue.

If you do not cluster migrate the existing cluster resources to another node, when you start `ndsd`, NCP users of existing cluster volumes on the node are not automatically reconnected because their cluster resources are no longer bound to NCP. You can offline the resources and then online the resources, or issue the `ncpcon bind` command for each resource at a terminal console (same as the command used in each of their respective load scripts). After a cluster resource is bound to NCP, its NCP users are automatically reconnected and their sessions continue.

To prevent NCP users from receiving any broadcast messages while you are performing these tasks, you can disable the NCP broadcast message support for the server. For instructions, see [Section 9.3.1, “Enabling or Disabling Broadcast Message Support,”](#) on page 71.

Creating a Shared NCP Volume

Use the following procedure to create one or more shared NCP volumes on the Linux POSIX cluster resource.

- 1 On one node in the cluster, you must create the NCP volume once in order to create its Volume object in Novell eDirectory. You do not create the NCP volume on every server.

For detailed instructions, see [Section 10.2, “Creating NCP Volumes on Linux File Systems,”](#) on page 83.

- 1a In Novell Remote Manager, click *Manage NCP Services > Manage Shares*, then click *Create New Share*.
- 1b In *Volume Name*, type the name of the NCP volume you want to create, such as `USERS`.
- 1c In *Path*, specify the Linux path of the cluster-enabled Linux POSIX file system or one of its subdirectories, then select the *Create If Not Present* check box if the subdirectory in the path does not already exist.

For example, if the mount point for the cluster-enabled Linux POSIX file system is `/mnt/lxvol144`, you can create the NCP volume at its root by specifying `/mnt/lxvol144` as the share path, or you can create the NCP volume for a subdirectory on it, such as `/mnt/lxvol144/USERS`.

For our ongoing example, we create the NCP volume at the root of the Linux POSIX cluster resource. The mount point of the EVMS volume and the NCP volume is the same, such as `/mnt/lxvol144`.

- 1d In *Shadow Path*, leave the field blank and do not select the *Create If Not Present* check box beneath it.

IMPORTANT: Dynamic Storage Technology does not support using NCP volumes in shadow volume pairs for OES 2 Linux. This field is a placeholder for future capabilities.

- 1e Make sure the *Inherit POSIX Permissions* option is disabled by deselecting the check box. In OES 2 SP1 Linux and earlier versions, the Inherit POSIX Permissions setting is disabled by default. Enabling the setting here has no effect when you mount the clustered NCP volume in the cluster load script. The setting also cannot be enabled later for clustered NCP volumes as you can for unclustered volumes.

IMPORTANT: For clustered NCP volumes, an option to set Inherit POSIX Permissions in the cluster load script is planned for OES 2 SP2 Linux. Contact Novell Support if you need to enable the Inherit POSIX Permissions option for a clustered NCP volume on OES 2 SP1 Linux.

- 1f Click *OK* to confirm the creation of the NCP volume (share).

This creates the Volume object for the NCP volume on the server, such as `cn=servername_USERS,ou=context,o=mycompany`. This object will be renamed later when you create the virtual NCP server (`NCS:NCP Server`) object.

This also creates a mount point to the volume (share) name you specified, and mounts the NCP volume to make it accessible to NCP clients.

- 2 Verify that the share was created successfully by clicking *Manage NCP Services > Manage Shares* to see a list of NCP shares.

The NCP volume should appear in the list, and be mounted. Mounted volumes appear with the name hyperlinked, and an *Unmount* button next to it.

- 3 Dismount the share from the node by clicking *Manage NCP Services > Manage Shares*, then clicking the *Unmount* button next to it.
- 4 Repeat [Step 1](#) through [Step 3](#) for each NCP volume that you want to create on the Linux POSIX cluster resource.
- 5 Remove the NCP volume names that you created in the previous steps from the `/etc/opt/novell/ncpserv.conf` file, or comment out the lines.

You want the load and unload scripts for the cluster to control the mounts and dismounts for the NCP volumes. You will modify the cluster scripts later.

If an NCP volume line is present and active in the `ncpserv.conf` file, the node tries to mount the volume on system startup, even if the cluster resources are not loaded on the node. Mounting and dismounting volumes that are on clustered resources should be done in the cluster load and unload scripts, or at the command line after the resource is loaded. Thus, the names of the NCP volumes on the cluster resource should not appear in the `ncpserv.conf` file on any of the nodes.

5a On the cluster node where you created the NCP volumes, open a terminal console then log in as the root user.

5b Open the `/etc/opt/novell/ncpserv.conf` file in a text editor.

```
gedit /etc/opt/novell/ncpserv.conf
```

5c Remove or comment out the line. Volume entries look like this:

```
VOLUME volumename /path_to_mount_point
```

For example, change

```
VOLUME USERS /mnt/lxvol44
```

to this:

```
;VOLUME USERS /mnt/lxvol44
```

5d Save your changes and close the file.

- 6 Restart the Novell eDirectory (`ndsd`) daemon by entering the following commands:

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

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

- 7 If NSS is installed on the server, restart the Novell NCP/NSS IPC daemon by entering

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

For information about why this is necessary, see [Section 3.5, "Restarting the Novell NCP/NSS IPC \(`ncp2nss`\) Daemon,"](#) on page 35.

- 8 For each of the other nodes in the cluster where you want to mount the shared cluster resource, create the path for the mount points of each of the NCP volumes that you created in [Step 1](#) through [Step 4](#).

8a On a cluster node, open a terminal console as the root user.

8b At the terminal console prompt, enter

```
mkdir /path_to_mount_point
```

For example, if the mount point is /mnt/lxvol144, enter

```
mkdir /mnt/lxvol144
```

- 9 Continue with [Section 11.2.4, “Creating a Virtual NCP Server Object for Shared NCP Volumes,”](#) on page 104.

11.2.4 Creating a Virtual NCP Server Object for Shared NCP Volumes

After you create a shared NCP volume, you must create a virtual NCP Server object (NCS:NCP Server) in Novell eDirectory in order to make it possible for NCP clients to access the data on the NCP volume. The NCS: NCP Server object is not created automatically as it is with clustered NSS pools. When you are done, you must add a line to the script that identifies the name of this virtual server and binds it to the IP address of the Linux POSIX cluster resource.

Do not use periods in cluster resource names. Novell clients interpret periods as delimiters. If you use a space in a cluster resource name, that space is converted to an underscore.

The /opt/novell/ncs/bin/ncs_ncpserv.py script creates a virtual NCP Server object (NCS:NCP Server) in eDirectory, and associates it with none, one, or multiple NCP volumes that you specify. It automatically renames the NCP Volume objects to use the cluster name instead of the server name where the NCP volume was created. NCP clients access files on the Linux POSIX volume via the virtual server name.

The bind command are automatically added to the load script and the unload script to bind the NCP volumes to the IP address of the cluster resource.

- ♦ [“Syntax” on page 104](#)
- ♦ [“Examples” on page 104](#)
- ♦ [“Procedure” on page 105](#)

Syntax

At the terminal console prompt on the master node of the cluster, enter the following command as the root user:

```
./ncs_ncpserv.py -c lx_volumename -i resource_ip_address [-v <ncp_volumename |  
"ncp_volumename1:ncp_volumename2:..."> ]
```

Replace the *lx_volumename*, *resource_ip_address*, and *ncp_volumename* with the information for your particular solution.

If the -v option is not specified, all of the NCP volumes that currently exist on the Linux POSIX cluster resource are bound to the IP address.

If you enter multiple volume names, use colons to delimit the names and put quotation marks around the list of names. Volume names can be listed by the volume name (MY_NNCP_VOL06) or by the volume distinguished name (cn=CLUS_02_MY_NNCP_VOL06,o=novell), or any combination of the two methods.

Examples

In the following examples, the resource IP address is 10.10.10.44, the cluster name is cluster1 and the cluster context is ou=cluster1,o=mycompany.

Example 1

To specify a single NCP volume named USERS on the lxvol44 cluster resource, enter

```
./ncs_ncpserv.py -c lxvol44 -i 10.10.10.44 -v USERS
```

The following confirmation message is displayed:

```
NCP Server 'cn=cluster1_lxvol44_server,ou=cluster1,o=mycompany' created.

Object 'cn=servername_USERS,ou=cluster1,o=mycompany' renamed to
'cn=cluster1_USERS,ou=cluster1,o=mycompany'.
The volume name you need to use in the scripts is: USERS
NCP server 'cn=cluster1_lxvol44_server,ou=cluster1,o=mycompany' and volume
'cn=cluster1_USERS,ou=cluster1,o=mycompany' are linked with each other.
```

Example 2

To specify multiple NCP volumes on the lxvol44 cluster resource, enter

```
./ncs_ncpserv.py -c lxvol44 -i 10.10.10.44 -v
"USERS:MY_NCP_VOL06:cn=servername_MY_NCP_VOL07,ou=cluster1,o=novell"
```

The following confirmation message is displayed:

```
NCP Server 'cn=cluster1_lxvol44_server,ou=cluster1,o=mycompany' created.

Object 'cn=servername_USERS,ou=cluster1,o=mycompany' renamed to
'cn=cluster1_USERS,ou=cluster1,o=mycompany'.
The volume name you need to use in the scripts is: USERS
NCP server 'cn=cluster1_lxvol44_server,ou=cluster1,o=mycompany' and volume
'cn=cluster1_USERS,ou=cluster1,o=mycompany' are linked with each other.

Object 'cn=servername_MY_NCP_VOL06,ou=cluster1,o=mycompany' renamed to
'cn=cluster1_MY_NCP_VOL06,ou=cluster1,o=mycompany'.
The volume name you need to use in the scripts is: MY_NCP_VOL06
NCP server 'cn=cluster1_lxvol44_server,ou=cluster1,o=mycompany' and volume
'cn=cluster1_MY_NCP_VOL06,ou=cluster1,o=mycompany' are linked with each other.

Object 'cn=servername_MY_NCP_VOL07,ou=cluster1,o=mycompany' renamed to
'cn=cluster1_MY_NCP_VOL07,ou=cluster1,o=mycompany'.
The volume name you need to use in the scripts is: MY_NCP_VOL07
NCP server 'cn=cluster1_lxvol44_server,ou=cluster1,o=mycompany' and volume
'cn=cluster1_MY_NCP_VOL07,ou=cluster1,o=mycompany' are linked with each other.
```

Procedure

- 1 On the master cluster node, open a terminal console, then log in as the root user.
- 2 In the console, use the `cd` command to go to the `/opt/novell/ncs/bin` directory.
- 3 At the terminal console prompt, enter

```
./ncs_ncpserv.py -c lx_volumename -i resource_ip_address -v ncp_volumename
```

Replace the *lx_volumename*, *resource_ip_address*, and *ncp_volume* with the information for your particular solution.

For example, to include the NCP volume USERS on the lxvol44 cluster resource where the IP address is 10.10.10.44 and the cluster context is `ou=cluster1,ou=boston,o=mycompany`, enter

```
./ncs_ncpserv.py -c lxvol44 -i 10.10.10.44 -v USERS
```

The confirmation message is displayed:

NCP Server 'cn=cluster1_lxvol44_server,ou=cluster1,ou=boston,o=mycompany' created.
 Object 'cn=servername_USERS,ou=cluster1,ou=boston,o=mycompany' renamed to 'cn=cluster1_USERS,ou=cluster1,ou=boston,o=mycompany'.
 The volume name you need to use in the scripts is: USERS
 NCP server 'cn=cluster1_lxvol44_server,ou=cluster1,ou=boston,o=mycompany' and volume 'cn=cluster_USERS,ou=cluster1,ou=boston,o=mycompany' are linked with each other.

- 4 Continue with [Section 11.2.5, “Modifying the Load Script for the Linux POSIX Cluster Resource,”](#) on page 106.

11.2.5 Modifying the Load Script for the Linux POSIX Cluster Resource

After you have created the NCP volume and an NCS:NCP Server object, you must modify the load script so that it mounts the NCP volume path as the Linux POSIX cluster resource is brought online. You must also bind the NCS:NCP Server object to the resource. For an example load script, see [Section 11.3.1, “Sample Load Script for an NCP Volume Cluster Resource,”](#) on page 108.

- 1 In iManager, select *Clusters > Cluster Options*, then select the cluster.
- 2 Click the name link of the Linux POSIX cluster resource to open its Cluster Resource Properties page.
- 3 Click the *Scripts* tab to open the *Load* script.
- 4 In the definition area, add the following lines to define the NCP volume and the virtual NCP server name:

```
# define NCP volume
NCP_VOLUME=USERS
# define NCP server name
NCP_SERVER=cluster1_lxvol44_server
```

Replace `USERS` with the name of the NCP volume you created. Replace the NCP server name with the name for your virtual NCP server.

- 5 Above the exit line, add a line to mount the NCP volume:

```
# mount the NCP volume
exit_on_error ncpcon mount $NCP_VOLUME=VOL_ID,PATH=$MOUNT_POINT
```

The volume ID is a value between 0 and 254 (up to 255 volumes per server) that you specify so that the same volume ID is used by the NCP volume on all nodes in the server. Cluster volumes are typically numbered from 254 and downward to avoid conflicts with the automatic volume ID assignments that begin with 0.

- 6 Under the mount line, add a line to bind the NCP server name to the resource IP address:

```
# bind the NCP volume
exit_on_error ncpcon bind --ncpservname=$NCP_SERVER --ipaddress=$RESOURCE_IP
```

- 7 Click *Apply* to save your changes.

The script changes are not active until the next time the cluster resource is taken offline, and then brought online. Do not active the script changes at this time.

- 8 Continue with [Section 11.2.6, “Modifying the Unload Script for the Linux POSIX Cluster Resource,”](#) on page 107.

11.2.6 Modifying the Unload Script for the Linux POSIX Cluster Resource

After you have created the NCP volume and an NCS:NCP Server object, you must modify the unload script so that it dismounts the NCP volume path as the Linux POSIX cluster resource is brought offline. You must also unbind the NCS:NCP Server object from the resource. For an example unload script, see [Section 11.3.2, “Sample Unload Script for an NCP Volume Cluster Resource,”](#) on page 109.

- 1 In iManager, select *Clusters > Cluster Options*, then select the cluster.
- 2 Click the name link of the Linux POSIX cluster resource to open its Cluster Resource Properties page.
- 3 Click the *Scripts* tab, then click *Unload* to open the *Unload* script.
- 4 In the definition area, add the following lines to define the NCP volume and the virtual NCP server name:

```
# define NCP volume
NCP_VOLUME=USERS
# define NCP server name
NCP_SERVER=cluster1_lxvol44_server
```

Replace `USERS` with the name of the NCP volume you created. Replace the NCP server name with the name for your virtual NCP server. Use the same values for variables that you did in the load script.

- 5 Under the definition, add a line to unbind the NCP server name from the resource IP address:

```
# unbind the NCP volume
ignore_error ncpcon unbind --ncpservname=$NCP_SERVER --
ipaddress=$RESOURCE_IP
```

- 6 Under the unbind line, add a line to dismount the NCP volume:

```
# dismount the NCP volume
ignore_error ncpcon dismount $NCP_VOLUME
```

- 7 Click *Apply* to save your changes.

The script changes are not active until the next time the cluster resource is taken offline, and then brought online.

- 8 Continue with [Section 11.2.7, “Activating the Script Changes,”](#) on page 107.

11.2.7 Activating the Script Changes

The script changes are not active until the next time the cluster resource is taken offline, and then brought online.

- 1 In iManager, select *Clusters > Cluster Manager*, then select the cluster.
- 2 Select the check box next to the Linux POSIX cluster resource, then click *Offline*.
Wait until the resource is reports an Offline status before continuing.
- 3 Select the check box next to the Linux POSIX cluster resource, then click *Online*.
Wait until the resource is reports an Online status before continuing.
- 4 Verify that an NCP user can access the volume. On a workstation, use the Novell Client to map a drive to the NCP volume.

11.3 Sample Load, Unload, and Monitor Scripts for a Cluster-Enabled NCP Volume

The settings in the sample scripts in this section are based on the values in [Table 11-1](#). Make sure to replace the values with the settings from your own configuration.

Table 11-1 Sample Script Variables and Values

Variable	Template Value	Your Value
RESOURCE_IP	a.b.c.d	10.10.10.44
MOUNT_FS	reiserfs	ext3
container_name	name	csn44
MOUNT_DEV	/dev/evms/\$container_name/ volume_name	/dev/evms/\$container_name/ lxvol44
MOUNT_POINT	/mnt/mount_point	/mnt/lxvol44
NCP_VOLUME	volume_name	USERS
NCP_SERVER	ncp_server_name	cluster1_lxvol44_server
volume ID	VOL_ID	252

- ♦ [Section 11.3.1, “Sample Load Script for an NCP Volume Cluster Resource,”](#) on page 108
- ♦ [Section 11.3.2, “Sample Unload Script for an NCP Volume Cluster Resource,”](#) on page 109
- ♦ [Section 11.3.3, “Sample Monitor Script for an NCP Volume Cluster Resource,”](#) on page 110

11.3.1 Sample Load Script for an NCP Volume Cluster Resource

You modify the load script for the cluster resource of the Linux POSIX file system by adding the extra lines needed for the NCP volume on it. The settings in the sample script are based on the values in [Table 11-1 on page 108](#). Make sure to replace the values with the settings from your own configuration.

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfncs

# define the IP address
RESOURCE_IP=10.10.10.44
# define the file system type
MOUNT_FS=ext3
# define the container name
container_name=csn44
# define the device
MOUNT_DEV=/dev/evms/$container_name/lxvol44
# define the mount point
MOUNT_POINT=/mnt/lxvol44
# define NCP volume
NCP_VOLUME=USERS
# define NCP server name
NCP_SERVER=cluster1_lxvol44_server

# activate the container
exit_on_error activate_evms_container $container_name $MOUNT_DEV $NCS_TIMEOUT
```

```

# create the EVMS volume mount point if it does not exist
ignore_error mkdir -p $MOUNT_POINT

# mount the file system
exit_on_error mount_fs $MOUNT_DEV $MOUNT_POINT $MOUNT_FS

# add the IP address
exit_on_error add_secondary_ipaddress $RESOURCE_IP

# mount the NCP volume
exit_on_error ncpcon mount $NCP_VOLUME=252,PATH=$MOUNT_POINT

# bind the NCP volume
exit_on_error ncpcon bind --ncpsservername=$NCP_SERVER --ipaddress=$RESOURCE_IP

exit 0

```

11.3.2 Sample Unload Script for an NCP Volume Cluster Resource

You modify the unload script for the cluster resource of the Linux POSIX file system by adding the extra lines needed for the NCP volume on it. The settings in the sample script are based on the values in [Table 11-1 on page 108](#). Make sure to replace the values with the settings from your own configuration.

```

#!/bin/bash
. /opt/novell/ncs/lib/ncsfncs

# define the IP address
RESOURCE_IP=10.10.10.44
# define the file system type
MOUNT_FS=ext3
# define the container name
container_name=csm44
# define the device
MOUNT_DEV=/dev/evms/$container_name/lxvol44
# define the mount point
MOUNT_POINT=/mnt/lxvol44
# define NCP volume
NCP_VOLUME=USERS
# define NCP server name
NCP_SERVER=cluster1_lxvol44_server

# unbind the NCP volume
ignore_error ncpcon unbind --ncpsservername=$NCP_SERVER --ipaddress=$RESOURCE_IP

# dismount the NCP volume
ignore_error ncpcon dismount $NCP_VOLUME

# if not using SMS for backup, comment out this sleep delay
sleep 10

# unmount the volume
ignore_error umount_fs $MOUNT_DEV $MOUNT_POINT $MOUNT_FS

# del the IP address
ignore_error del_secondary_ipaddress $RESOURCE_IP

# deactivate the container
ignore_error deactivate_evms_container $container_name $NCS_TIMEOUT

# return status
exit 0

```

11.3.3 Sample Monitor Script for an NCP Volume Cluster Resource

You modify the monitor script for the cluster resource of the Linux POSIX file system by first enabling monitoring for the cluster resource, then modifying the variable values. The settings in the sample script are based on the values in [Table 11-1 on page 108](#). Make sure to replace the values with the settings from your own configuration.

```
#!/bin/bash
. /opt/novell/ncs/lib/ncsfncs

# define the IP address
RESOURCE_IP=10.10.10.44
# define the file system type
MOUNT_FS=ext3
# define the container name
container_name=csm44
# define the device
MOUNT_DEV=/dev/evms/$container_name/lxvol44
# define the mount point
MOUNT_POINT=/mnt/lxvol44
# define NCP volume
NCP_VOLUME=lxvol44
# define NCP server name
NCP_SERVER=cluster1_lxvol44_server

# test the file system
exit_on_error status_fs $MOUNT_DEV $MOUNT_POINT $MOUNT_FS

# status the IP address
exit_on_error status_secondary_ipaddress $RESOURCE_IP

exit 0
```

To monitor the cluster resource, use the following in the monitor script:

```
exit_on_error ncpcon volume <volume_name>
```

To monitor the availability of NCP file services and it's related services, use the following in the monitor script:

```
rcnstd status
if test $? != 0; then
    exit_on_error rcnstd restart
fi
sleep 5

exit_on_error rcnstd status
/etc/init.d/ncp2nss status
if test $? != 0; then
    exit_on_error /etc/init.d/ncp2nss restart
fi
sleep 5
exit_on_error /etc/init.d/ncp2nss status
```

12 Managing File System Trustees, Trustee Rights, and Attributes on NCP Volumes

This section describes the NetWare trustee model and how to manage trustees and trustee rights for NCP volumes on a Novell Open Enterprise Server (OES) 2 Linux server.

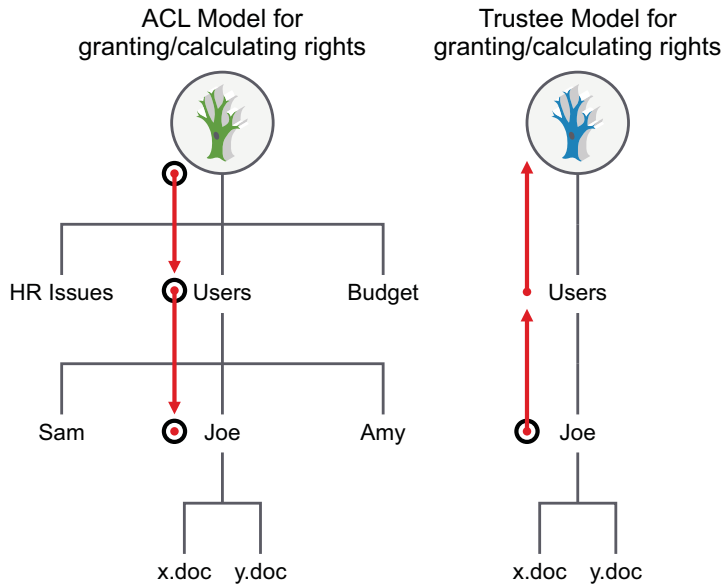
- ♦ [Section 12.1, “NCP on Linux Security,” on page 111](#)
- ♦ [Section 12.2, “Understanding File System Trustees, Trustee Rights, and Attributes,” on page 114](#)
- ♦ [Section 12.3, “Managing File System Rights with NCPCON,” on page 115](#)
- ♦ [Section 12.4, “Managing File or Directory Trustees and Rights with iManager,” on page 116](#)
- ♦ [Section 12.5, “Managing File or Directory Attributes with iManager,” on page 116](#)

12.1 NCP on Linux Security

The NetWare and Linux security models are quite different. The basic NetWare security model assumes that users have no rights until they are granted specific rights. Those rights are inherited by the users in all child subdirectories. This means that a single trustee assignment can give a user rights to a large number of subdirectories and files. A user’s home directory is set up so that only the user and the system administrator have rights there. A user’s files are secure.

The POSIX/Linux security model takes a different approach. The POSIX permissions are specified for each file and subdirectory, and nothing is inherited. If a user is to have access to all the files in a subdirectory, the permissions (UID, GID, and mode bits) must be set for each file in a manner that gives the user the appropriate access. This can’t be done with a simple trustee assignment to the parent subdirectory. In order for a user to use the `dir` or `ls` command, the user must have the read and execute rights in that directory and all its parent directories up to the root. Because of this, users usually have read rights by default across most of the system, and then the rights for everyone are masked for areas that need to be private. This means that the default for POSIX is open and shared rather than private. In POSIX, files are private when you make them private rather than private by default.

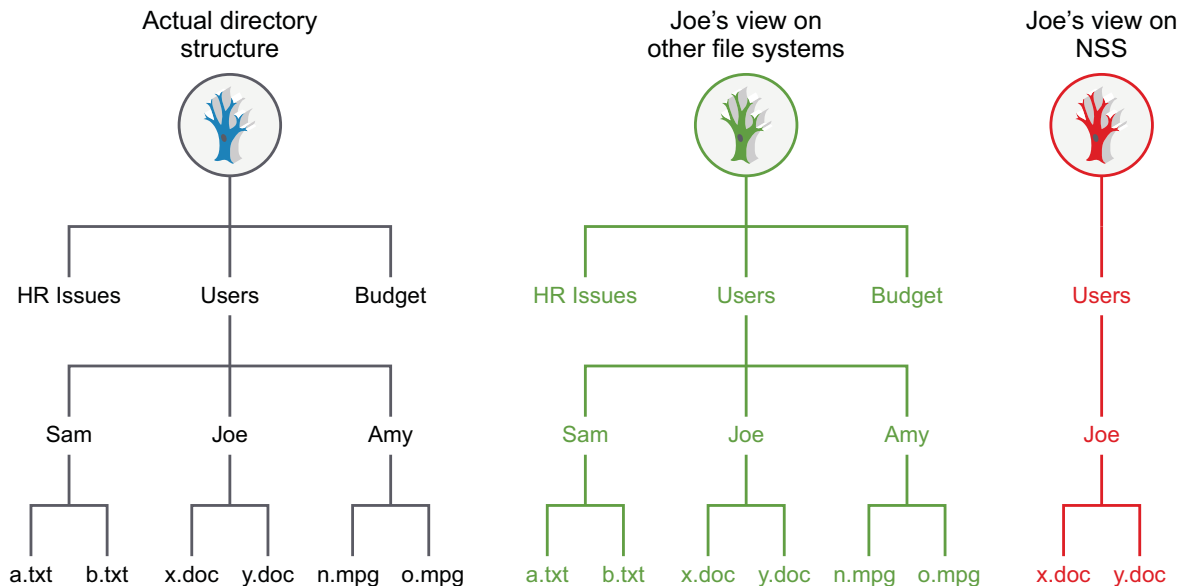
Figure 12-1 Comparison of the Linux ACL Model and the Novell Trustee Model



Novell Storage Services (NSS) volume on Linux and NCP volumes on Linux use the Novell trustee model to control user access to files. Users can see only those directory paths that they need to see in order to access their files. On a Linux POSIX file system using Access Control Lists, visibility of the entire directory structure is not restricted.

For example, [Figure 12-2](#) shows how the user Joe has restricted visibility into the file system to view only those paths needed to access the files in his home directory on an NSS volume on Linux. On Linux POSIX file systems without NCP Server, Joe is able to view the entire directory structure.

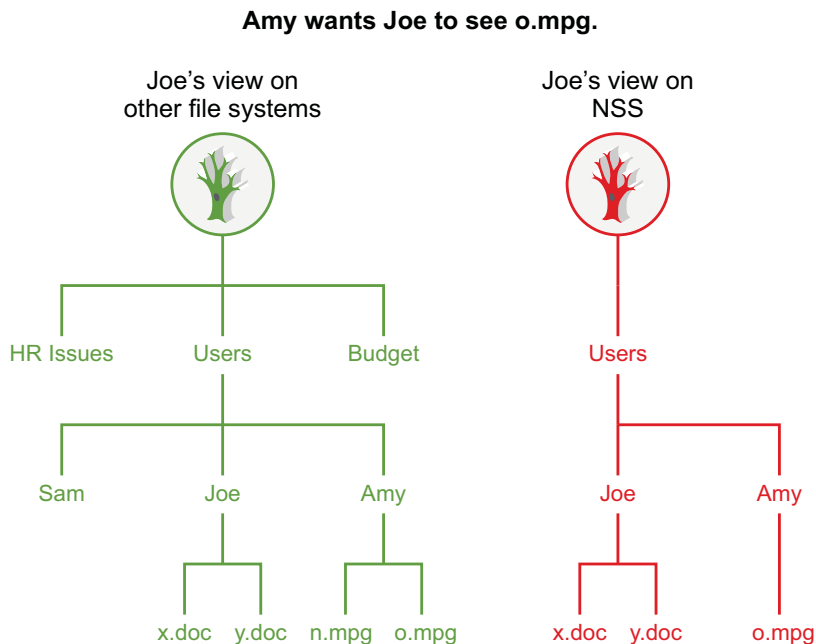
Figure 12-2 Comparison of File Visibility for Users of Linux POSIX Volumes and NSS Volumes on Linux



If users want to share files with others, they can grant rights through trustee assignments on the individual files, or by creating a shared subdirectory and assigning trustees to it. When a user is given a trustee assignment to a file or directory, he or she can automatically see each parent directory along the path up to the root. However, the user cannot see the contents of those directories, just the path to where he or she has rights.

For example, if the user Amy wants user Joe to see a particular file in her home directory, she can add Joe as a trustee of the file, then grant Joe limited rights to see the file. Joe can see the path to the file, but cannot see other files in Amy's home directory, as shown in Figure 12-3. On Linux file systems without NCP Server, Joe would be able to see all files in Amy's home directory.

Figure 12-3 File Visibility Granted to Trustees



These differences in access control approaches can become problems when you try to share files between NCP users and Linux users that rely on the POSIX rights for their access (Local, SSH, and Samba users). In order for the Linux/POSIX users to access files, they need to be granted read and execute (r and x) rights through the group and other mode bits for subdirectories along the path up to the root of the volume. This gives them the right to see and read all files in those directories up to the root. This is unlike NCP rights on NetWare, where users see only the subdirectory path to the locations where they have been granted trustee rights. For shared volumes, NetWare users should be aware that Linux/POSIX users might have more rights to files and subdirectories than NCP users do.

Because the NetWare model is secure/private until granted specific rights, all files and subdirectories created by NCP clients have the following POSIX security permissions:

- ◆ The UID is that of the user (or `root` if the user is not Linux-enabled with Linux User Management).
- ◆ The GID is `root`.
- ◆ The mode bits are:

`rwx --- ---`

This way, by default, the only people who can access a file or subdirectory from a LINUX environment are `root` and the creator of the file or subdirectory. An option is included with OES that lets a volume be configured such that the permissions (GID and mode bits) are inherited from the

parent directory. This lets shared areas be more easily created and managed. This option is not enabled by default. The more secure model of the OES release is still the default. See [Section 10.8, “Configuring Inherit POSIX Permissions for an NCP Volume,”](#) on page 89 for information on how to enable or disable this option.

Because NSS is not a POSIX file system, NSS rights don't behave like standard POSIX rights. NSS volumes keep track of trustee assignments; all trustee assignments are synchronized between NCP and NSS. For NSS volumes, access is based on trustee rights for the user (UID) rather than the permissions (UID, GID, and mode bits). This makes things simpler because Linux/POSIX-based users (Local, SSH, and Samba) do not have more rights than the same user would have if he were accessing files through NCP. This makes NSS easier to manage.

12.2 Understanding File System Trustees, Trustee Rights, and Attributes

- ♦ [Section 12.2.1, “Directory and File Trustee Rights,”](#) on page 114
- ♦ [Section 12.2.2, “Directory and File Attributes,”](#) on page 114

12.2.1 Directory and File Trustee Rights

A trustee is any Novell eDirectory object, such as a User object, Group object, Organizational Role object, 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.

NCP Server for Linux provides the same file and directory trustee rights for both NSS and Linux POSIX file systems. These are the same rights that exist for the NSS file system on NetWare. They include:

- ♦ Read (Default=On)
- ♦ Write (Default=Off)
- ♦ Create (Default=Off)
- ♦ Erase (Default=Off)
- ♦ Modify (Default=Off)
- ♦ File Scan (Default=On)
- ♦ Access Control (Default=Off)
- ♦ Supervisor (Default=Off)

12.2.2 Directory and File Attributes

NCP Server for Linux supports the directory and file attributes for NSS volumes. For a complete list of file attributes, see [“Understanding File System Access Control Using Trustees”](#) in the *OES 2 SP3: File Systems Management Guide*.

The following file and directory attributes are supported for NCP volumes on Linux POSIX file systems.

- ♦ Read Only
- ♦ Hidden
- ♦ Shareable

Other file and directory attributes that are listed for NCP Server's support of the NSS file system are not supported for Linux POSIX file systems.

The other NSS file and directory attributes might appear to be supported on Linux POSIX file systems, and might also appear to be configurable, but the other file and directory attributes are not supported, and are ignored if files are accessed through NCP. For example, it might appear that you have set the Copy Inhibit attribute for a specific file, but that file can still be copied if it is on a non-NSS file system.

NOTE: File attributes and NCP support tend to get mixed together in the minds of NetWare administrators. It is important to remember that file and directory attributes are supported and enforced by the file system that underlies an NCP volume, not by the NCP Server.

12.3 Managing File System Rights with NCPCON

Use the NCPCON utility to view, add, or remove file and directory rights for NSS volumes and NCP volumes on Linux.

- [Section 12.3.1, "Viewing File and Directory Rights," on page 115](#)
- [Section 12.3.2, "Adding File and Directory Rights," on page 115](#)
- [Section 12.3.3, "Removing File and Directory Rights," on page 115](#)

12.3.1 Viewing File and Directory Rights

To view file or directory rights, enter `ncpcon` at the Linux server console and then enter the following:

```
rights view path
```

Replace *path* with the directory path to the file or directory that you want to view trustee rights for. This lets you view the trustee assignments that have been specifically made for that file or directory. Effective rights are not displayed by using this command.

12.3.2 Adding File and Directory Rights

To add file or directory rights, enter `ncpcon` at the Linux server console and then enter the following:

```
rights add path fdn mask
```

Replace *path* with the directory path to the file or directory that you want to add trustee rights to.

Replace *fdn* with the fully distinguished name of the user or object that you want to grant rights to.

Replace *mask* with the rights that you want to grant to the user or object.

For example, if you wanted to grant Read and File Scan rights to the `users:bob` directory for user Bob, and Bob's context is `bob.acme`, you would enter the following after starting the NCPCON utility:

```
rights add users:bob bob.acme RF
```

12.3.3 Removing File and Directory Rights

To remove file or directory rights, enter `ncpcon` at the Linux server console and then enter the following:

```
rights rem path fdn
```

Replace *path* with the directory path to the file or directory that you want to remove trustee rights from.

Replace *fdn* with the fully distinguished name of the user or object that you want to remove rights from.

For example, if you wanted to remove trustee rights to the `users:bob` directory from user Bob, and Bob's context is `bob.acme`, you would enter the following after starting the NCPCON utility:

```
rights rem users:bob bob.acme
```

12.4 Managing File or Directory Trustees and Rights with iManager

You can optionally manage trustees and trustee rights for files and directories by using the *Files and Folders* role in Novell iManager.

- 1 In iManager, click *Files and Folders > Properties*.
- 2 Click the *Search* icon to select the directory or file that you want to manage.
- 3 Click *NetWare Info*, then view, add, or remove trustees and set trustee rights for the selected file or directory.
Changes are not saved until you click *Apply* or *OK*.
- 4 Click *Inherited Rights*, then view or modify inherited trustees and rights for the parent directories for the selected file or directory.
Changes are not saved until you click *Apply* or *OK*.
- 5 Click *Apply* or *OK* to save your changes.

12.5 Managing File or Directory Attributes with iManager

You can optionally manage the file or directory attributes by using the *Files and Folders* role in Novell iManager.

- 1 In iManager, click *Files and Folders > Properties*.
- 2 Click the *Search* icon to locate and select the directory or file that you want to manage.
- 3 On the Properties page, select *NetWare Info*.
- 4 Enable or disable the file attribute by selecting or deselecting the check box next to the attribute.
For NCP volumes, you can modify the following attributes:
 - ♦ Read Only
 - ♦ Hidden
 - ♦ ShareableChanges are not saved until you click *Apply* or *OK*.
- 5 Click *Apply* or *OK* to save your changes.

13 Using Opportunistic Locking for NCP File Handling

This section contains information to help you understand opportunistic locking (OpLocks) for NCP Server for Novell Open Enterprise Server (OES) 2 Linux.

- ♦ [Section 13.1, “Understanding Opportunistic Locking for NCP Connections,” on page 117](#)
- ♦ [Section 13.2, “Configuring OpLocks for NCP Server,” on page 119](#)
- ♦ [Section 13.3, “Configuring File Caching in the Novell Client,” on page 120](#)
- ♦ [Section 13.4, “Configuring OpLocks for NSS Volumes,” on page 120](#)
- ♦ [Section 13.5, “Additional Information,” on page 120](#)

13.1 Understanding Opportunistic Locking for NCP Connections

OpLocks, or opportunistic locks, are a way to cache file data at the client. This allows the client to read and write data using its local cache and interact with the file server only when necessary. OpLocks are acquired after a normal NCP file handle has been obtained. OpLocks should help both client and network performance by reducing the amount of traffic on the network.

When a server requires a client to release its oplock, it sends it a tickle packet. Tickle packets are very similar to broadcast packets. The main difference is that they include a dollar sign (\$) character instead of an exclamation point (!) character for the control information. Tickle packets also contain the file handle, so the client knows which oplock to release.

There are two types of OpLocks: L1 (level 1) and L2 (level 2). You can set OpLocks to either of these levels or disable OpLocks completely. By default, OpLocks is set to level 2, which includes both level 1 and level 2 functionality.

WARNING: Level 2 OpLocks are inappropriate for server-side database applications: Do not use OpLock Level 2 with databases. Level 1 OpLocks can remain switched on.

- ♦ [Section 13.1.1, “Level 2 OpLocks,” on page 117](#)
- ♦ [Section 13.1.2, “Level 1 OpLocks,” on page 118](#)
- ♦ [Section 13.1.3, “Guidelines for Using OpLocks,” on page 118](#)

13.1.1 Level 2 OpLocks

L2 OpLocks give the client shared read access to the file. Multiple clients can have L2 OpLocks for the same file. Not all clients accessing the same shared file require L2 OpLocks; some might not have an oplock at all. The L2 oplock entitles the client to cache file data locally for reads, but not for writes.

This is useful when the client reads the same data over and over. L2 OpLocks should be released when the client application closes a file, because the server won't notify the client when another connection wants exclusive access to that file (delete, rename, exclusive open, etc.).

When a client writes to a file that has L2 OpLocks for other clients, all the other clients are sent a tickle packet to notify them that their local cache for that file is no longer valid. When the client receives this tickle packet, it does the following:

1. Acknowledges the tickle packet.
2. Invalidates its local cache for the file.
3. Clears its oplock for the file.

The server does not grant an L2 oplock for a file that has been written to recently by a client other than the one requesting the lock.

13.1.2 Level 1 OpLocks

L1 OpLocks give the client exclusive access to the file. The client can cache reads and writes locally. The client can even close the file without notifying the server; this is useful for when the client application opens and closes the same file over and over.

L1 OpLocks can be acquired by using NCP to open the file and then setting the corresponding oplock request bits. If another connection has the file open, the L1 oplock is denied—you cannot get an oplock on a file that is currently shared with another client.

If another connection tries to access (open, rename, or delete) an L1 oplocked file, the owner of the oplock is notified with a tickle packet that the lock needs to be broken. The client then does the following:

1. Acknowledges the tickle packet. For protocols like IPX and UDP, this lets the server know that the client received the tickle packet.
2. Flushes any dirty cache buffers to the server.
3. Acquires any cached physical record locks if it plans on keeping the file open.
4. Performs one of the following four operations:
 - ♦ Clears the oplock.
 - ♦ Refuses to clear the oplock.
The Novell Client never does this.
 - ♦ Downgrades the oplock to an L2 shared lock.
 - ♦ Closes the file.

With all L1 OpLocks, the server waits for the client holding the L1 oplock to respond before allowing the new access request to continue. Because NCP allows only one outstanding request for a client connection, the server must be careful never to send a tickle packet to the client making the initial access request. This avoids a deadlock situation.

13.1.3 Guidelines for Using OpLocks

Oplock support can be turned off or on at the client or at the server. The server lets the user enable only L1 OpLocks or both L1 and L2 OpLocks.

OpLocks are automatically released when a file is closed.

A client can't open, rename, or delete a file while another client has an L1 oplock on it. The request causes a tickle packet to be sent to the client holding the oplock; the server then waits for a reply from that client and then continues based on the client's response.

When a client has an L1 oplock for a file, it doesn't need to send physical record lock requests to the server for that file. It can track the locks locally. If the client later needs to release the oplock, it needs to acquire any outstanding physical record locks from the server before continuing. For L2 OpLocks, physical record locks should be managed at the server instead of the client to avoid deadlocks.

If a client tries to open, rename, or delete a file that it already has L1 oplocked, the open fails because the server cannot delay the request and wait for notification from the client that it has cleared the oplock.

13.2 Configuring OpLocks for NCP Server

Opportunistic locking (OpLocks) improves file access performance and is enabled by default in NCP Server. OpLocks provides a way to cache file data at the client. It allows the client to read and write data using its local cache, and interact with the file server only when necessary. OpLocks improves both client and network performance by reducing the amount of traffic on the network.

IMPORTANT: Ensure that users are running Novell Client 4.9 SP2 and later.

There are two levels of OpLocks available with NCP Server. You can set OpLocks to either of these levels or disable OpLocks completely. By default, OpLocks is set to level 2, which includes both level 1 and level 2 functionality.

You can modify the `OPLOCK_SUPPORT_LEVEL` parameter setting by using Novell Remote Manager for Linux as follows:

- 1 In Novell Remote Manager for Linux, select *Manage NCP Services > Manage Server*.
- 2 Click the *Parameter Value* link for `OPLOCK_SUPPORT_LEVEL`.
- 3 Set the value to 0, 1, or 2.
 - ◆ **0:** Disables OpLocks support.
 - ◆ **1:** Enables OpLocks support at L1.
 - ◆ **2:** Enables OpLocks support at L2 (the default).
- 4 Click *OK* to apply the change.

You can also change or disable the setting by adding an `OPLOCK_SUPPORT_LEVEL` command to the `/etc/opt/novell/ncpserv.conf` configuration file. If you have never modified the `OPLOCK_SUPPORT_LEVEL` from the default setting of 2, then there will not be a line for that parameter in the file. You must add the parameter line. If you have previously modified the setting, the parameter appears as a line in the file, and you can simply change its value. After you manually modify the file, you must restart `ndsd`.

- 1 Log in as the root user, then open the `/etc/opt/novell/ncpserv.conf` configuration file in a text editor.
- 2 Do one of the following:
 - ◆ If the `OPLOCK_SUPPORT_LEVEL` parameter is not listed, add a line for the `OPLOCK_SUPPORT_LEVEL` option with the value of 0, 1, or 2.

For example, to disable OpLocks support, set the value to 0 by adding this line:

```
OPLOCK_SUPPORT_LEVEL 0
```

For example, to set OpLocks support to L1, set the value to 1 by adding this line:

```
OPLOCK_SUPPORT_LEVEL 1
```

- ♦ If the `OPLOCK_SUPPORT_LEVEL` parameter is already listed in the file, change its value to the desired setting of 0, 1, or 2.

3 Save the file.

4 After changing the `oplock` level in `/etc/opt/novell/ncpserv.conf`, you must restart `ndsd` to apply the changes. Open a terminal console as the `root` user, then enter

```
rcndsd restart
```

13.3 Configuring File Caching in the Novell Client

Opportunistic locking is supported for Novell Client 4.9 SP2 and later. In order to take advantage of opportunistic locking, the client must be enabled for file caching.

To enable file caching for a Novell Client:

- 1 On the desktop, right-click the *Novell Client* icon in the status area, then select *Novell Client Properties*.
- 2 In the *Novell Client Configuration* dialog box, select *Advanced Settings*.
- 3 In the *Parameter Groups* drop-down list, select *Performance, Cache*.
- 4 In the list of options, select *File Caching*, then set its value to *On*.
- 5 In the list of options, select *File Caching on exclusively opened files*, then set its value to *Off*.
- 6 Select *OK* to save and apply the settings.

13.4 Configuring OpLocks for NSS Volumes

On Linux, opportunistic locking for NSS volumes is controlled by the NCP Server `OPLOCK_SUPPORT_LEVEL` parameter setting. This NCP setting applies to all NSS volumes on the server.

```
ncpcon OPLOCK_SUPPORT_LEVEL=<level>
```

13.5 Additional Information

For issues and troubleshooting tips, see [Information on Opportunistic Locking \(Technical Information Document 7001112 \(formerly known as TID 10095627\)\)](http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=7001112&sliceId=1&docTypeID=DT_TID_1_1) (http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=7001112&sliceId=1&docTypeID=DT_TID_1_1).

14 Using the Inventory to Monitor NCP Volumes

In Novell Remote Manager for Linux, you can view reports for the NCP (NetWare Core Protocol) volume, with statistics and information about its files.

- ◆ [Section 14.1, “Understanding the Volume Inventory,” on page 121](#)
- ◆ [Section 14.2, “Accessing the Volume Inventory,” on page 125](#)
- ◆ [Section 14.3, “Viewing Statistics for the Volume,” on page 125](#)
- ◆ [Section 14.4, “Using Inventory Detail Reports to Move, Copy, or Delete Files on the Volume,” on page 126](#)
- ◆ [Section 14.5, “Generating a Custom Inventory Report for DST Shadow Volumes,” on page 127](#)

14.1 Understanding the Volume Inventory

The inventory reports key statistics about the files in the selected volume, such as files scanned and the available space trends. It reports information for NCP volumes on Linux POSIX file systems, Novell Storage Services (NSS) volumes, and Dynamic Storage Technology (DST) shadow volumes.

- ◆ [Section 14.1.1, “Inventory Summary,” on page 121](#)
- ◆ [Section 14.1.2, “Available Space Trends,” on page 122](#)
- ◆ [Section 14.1.3, “Graphical Profiles,” on page 122](#)
- ◆ [Section 14.1.4, “Tabular Profiles,” on page 123](#)
- ◆ [Section 14.1.5, “Inventory Detail Reports,” on page 123](#)
- ◆ [Section 14.1.6, “Custom Scans,” on page 124](#)

14.1.1 Inventory Summary

The inventory summary reports the number of files scanned on the volume and key statistics.

For a DST shadow volume, it shows information for the primary storage area and the secondary storage area. It also reports key statistics for the primary storage area, the secondary storage area, and both areas combined as the shadow volume.

Key Statistics	Description
Total Subdirectories	The total number of subdirectories in the volume.
Total Files	The total number of files in the volume.

Key Statistics	Description
Space in Use	The amount of space currently in use in the volume for data and metadata. On NSS volumes where salvage is enabled, the space in use includes space used by deleted files and directories.
Space Available	The amount of free space in the volume.
File Types	The number of different file types in use throughout the entire volume.
Soft Link Files	The NSS file system and NCP Server do not support soft links to files. In the initial release of DST, this is a placeholder for future non-NCP support.
Soft Link Subdirectories	The NSS file system and NCP Server do not support soft links to subdirectories. In the initial release of DST, this is a placeholder for future non-NCP support.

14.1.2 Available Space Trends

The *Available Space Trends* report shows the trends for space usage on the volume. For a DST shadow volume, it shows information for the primary storage area and the secondary storage area.

14.1.3 Graphical Profiles

The *Profiles* portion of the inventory report graphically displays information about the volume. Graphical profiles are displayed by size in bytes and file count for the following categories:

- ◆ [“File Type Profiles” on page 122](#)
- ◆ [“File Owner Profiles” on page 122](#)
- ◆ [“Time Stamp Profiles” on page 122](#)
- ◆ [“File Size Profiles” on page 123](#)

File Type Profiles

File Type Profiles indicates storage space usage by file types that are actually in use on your system, such as LOG, TDF, DAT, XML, EXE, and so on.

File Owner Profiles

File Owner Profiles indicates storage space usage by the designated owner of the file. It is not unusual in NCP to see the `root` user as the owner of files. For NCP volumes and NSS, file access is governed by the file system trustees assigned to the file, not the file owner. Trustees are users who have User objects defined in Novell eDirectory, and who have been granted file system rights for the file. NCP tracks ownership via the user’s eDirectory GUID.

Time Stamp Profiles

Three time stamp profiles are generated:

- ◆ **Files Modified Profiles:** Modified dates indicate the last time someone changed the contents of a file.
- ◆ **Files Accessed Profiles:** Access dates indicate the last time someone accessed a file, but did not change the contents if this differs from the modified date.

- ♦ **Files Changed Profiles:** Change dates indicate the last time someone changed the metadata of a file, but did not change the contents if this differs from the modified date.

Time stamps are grouped by the following time periods:

More than 2 years
1 year to 2 years
6 months to 1 year
4 months to 6 months
2 months to 4 months
1 month to 2 months
2 weeks to 1 month
1 week to 2 weeks
1 day to 1 week
Within last day

File Size Profiles

File Size Profiles reports the size of files, grouped by the following size ranges:

More than 256 MB
64 MB to 256 MB
16 MB to 64 MB
4 MB to 16 MB
1 MB to 4 MB
256 KB to 1 MB
64 KB to 256 KB
16 KB to 64 KB
4 KB to 16 KB
1 KB to 4 KB
Less than 1 KB

14.1.4 Tabular Profiles

Statistical data used to create the graphs is also available in tables that report statistics for the volume.

For a DST shadow volume, data is categorized for the primary area, the secondary area, and both areas combined as the shadow volume. The count for file entries for the primary area and shadow (secondary) area are linked to detail reports that list the files matching that particular category and group. From the file lists, you have the option to copy, move, or delete one or multiple files.

14.1.5 Inventory Detail Reports

An *Inventory Detail Report* lists all of the files that match a particular category and group for a file count entry in the tabular reports in the volume inventory. You can select one or multiple files in the list, then select one of the following operations to be performed:

- ♦ Move the selected volumes to the other file tree. (This option is available only for DST shadow volumes.)
- ♦ Move the selected files to a specified path on the server.

- ♦ Copy the selected files to a specified path on the server.
- ♦ Delete the selected files.

14.1.6 Custom Scans

At the bottom of the inventory report, you can create custom scans: *Customer Directory Tree Scans* for NCP volumes, or *Custom Shadow Volume Options* for DST shadow volumes. These scans allow you to generate reports based on key statistics of interest, and perform actions on them.

- ♦ [“Volume Operations for DST Shadow Volumes” on page 124](#)
- ♦ [“Search Patterns” on page 124](#)
- ♦ [“File Owner Restrictions” on page 124](#)
- ♦ [“Time Stamp Restrictions” on page 124](#)
- ♦ [“File Size Restrictions” on page 125](#)

Volume Operations for DST Shadow Volumes

In the *Custom Shadow Volume Options* scan, you can perform one of the following operations for DST shadow volumes on the files that match the search criteria you specify:

- ♦ List primary area selected files
- ♦ Move selected files from primary area to shadow area.
- ♦ List shadow area selected files.
- ♦ Move selected files from shadow area to primary area.

Search Patterns

In *Search Patterns*, you can specify wildcards and characters to select files by filenames or extensions.

File Owner Restrictions

In *File Owner Restrictions*, select *None* or a user name. The search applies only to files where the file owner matches the specified owner.

Time Stamp Restrictions

You can specify one or multiple time stamps to consider for the search:

- ♦ Last Modified Time
- ♦ Last Accessed Time
- ♦ Last Changed Time

If no time stamp is selected, time stamps are not considered in the search criteria.

If a time stamp is selected, you can specify one or multiple time ranges to consider for the search:

Within last day
1 day to 1 week
1 week to 2 weeks
2 weeks to 1 month

- 1 month to 2 months
- 2 months to 4 months
- 4 months to 6 months
- 6 months to 1 year
- 1 year to 2 years
- More than 2 years

File Size Restrictions

You can specify one or multiple ranges of file sizes to consider for the search:

- Less than 1 KB
- 1 KB to 4 KB
- 4 KB to 16 KB
- 16 KB to 64 KB
- 64 KB to 256 KB
- 256 KB to 1 MB
- 1 MB to 4 MB
- 4 MB to 16 MB
- 16 MB to 64 MB
- 64 MB to 256 MB
- More than 256 MB

14.2 Accessing the Volume Inventory

- 1 Open Novell Remote Manager for Linux in a Web browser, then log in as the root user.
- 2 Use one of the following methods to view the volume inventory:
 - ♦ Select *View File System > Volume Inventory*, locate the volume in the *NCP Volumes Available for Inventory* list, then click the *Volume* link for the volume.

Volume Inventory ?

NCP Volumes available for Inventory	
Volume	Mount Point
SYS	(/usr/novell/sys)
ADMIN	(/_admin)
VOL1	(/media/nss/VOL1)

- ♦ Select *View File System > Dynamic Storage Technology Options*, locate the volume in the list, then click the *Inventory* link next to it.

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

14.3 Viewing Statistics for the Volume

- 1 In Novell Remote Manager, access the volume inventory for the NCP volume or shadow volume.

For information, see [Section 14.2, “Accessing the Volume Inventory,”](#) on page 125.

- 2 In the inventory summary area, click a link to go directly to one of the following reports, or scroll to view the reports. For information about each statistical report, see [Section 14.1, “Understanding the Volume Inventory,”](#) on page 121.
 - ◆ Available space trend graph
 - ◆ File type profiles
 - ◆ File owner profiles
 - ◆ Last modified profiles
 - ◆ Last accessed profiles
 - ◆ Change time profiles
 - ◆ File size profiles
 - ◆ Links to specific reports
 - ◆ Custom directory tree scan (NCP volume or NSS volume), or Custom shadow volume options (DST shadow volume)
- 3 Click the *Data Tables* link for a profile to jump directly to the tabular display of the information that was used to generate the graph.

14.4 Using Inventory Detail Reports to Move, Copy, or Delete Files on the Volume

- 1 In Novell Remote Manager, access the volume inventory for the shadow volume.
For information, see [Section 14.2, “Accessing the Volume Inventory,”](#) on page 125.
- 2 In the summary area, click *Links to Specific Reports*, or scroll down to the *Links to Specific Reports* section to view the tabular reports of information used to generate the profiles.
- 3 Review the following categories to locate the files of interest:
 - ◆ Last modified range
 - ◆ Last accessed range
 - ◆ Change time range
 - ◆ File size range
 - ◆ File owner
 - ◆ File extension
- 4 Click the link of the data entry for the files that you want to manage. Files are grouped by Primary area and by shadow (secondary) area.
- 5 In the *Inventory Detail Report*, select one or multiple files in the list, then do one of the following:
 - ◆ Move the selected volumes to the other file tree (primary or shadow (secondary) file tree). (This option is available only for DST shadow volumes.)
 - ◆ Move the selected files to a specified path on the server.
 - ◆ Copy the selected files to a specified path on the server.
 - ◆ Delete the selected files.

14.5 Generating a Custom Inventory Report for DST Shadow Volumes

You can customize the inventory report to limit the search sizes and times reported. The reporting criteria can be combinations of the specific categories described in [Section 14.1.6, "Custom Scans,"](#) on page 124.

- 1 In Novell Remote Manager, access the volume inventory for the shadow volume.
For information, see [Section 14.2, "Accessing the Volume Inventory,"](#) on page 125.
- 2 Scroll down to the *Custom Shadow Volume Options* area at the end of the shadow volume inventory.
- 3 In *Volume Operations*, select one of the following actions to perform on the files that meet the search criteria you specify for the scan in later steps.
 - ◆ List primary area selected files
 - ◆ Move selected files from primary area to shadow area.
 - ◆ List shadow area selected files.
 - ◆ Move selected files from shadow area to primary area.
- 4 In *Search Patterns*, specify wildcards and characters to select files by filename or extension. The default is **.**, which does not restrict the search to specific filenames or extensions; all files are considered.
- 5 (Optional) In *File Owner Restrictions*, select *None*, or select a username from the drop-down list.
If *None* is selected, file ownership is not considered for the search. If a username is specified, the search applies only to files where the file owner matches the specified owner.
- 6 (Optional) In *Time Stamp*, specify one or multiple time stamps to be searched. If none are selected, the time stamps are not considered when searching.
 - ◆ Last Modified Time
 - ◆ Last Accessed Time
 - ◆ Last Changed Time
- 7 In *Range*, if you specified a time stamp restriction, specify one or multiple ranges to be searched.
 - Within last day
 - 1 day to 1 week
 - 1 week to 2 weeks
 - 2 weeks to 1 month
 - 1 month to 2 months
 - 2 months to 4 months
 - 4 months to 6 months
 - 6 months to 1 year
 - 1 year to 2 years
 - More than 2 years
- 8 (Optional) In *File Size Restrictions*, specify one or multiple file sizes to be searched.
 - Less than 1 KB
 - 1 KB to 4 KB
 - 4 KB to 16 KB
 - 16 KB to 64 KB
 - 64 KB to 256 KB

256 KB to 1 MB
1 MB to 4 MB
4 MB to 16 MB
16 MB to 64 MB
64 MB to 256 MB
More than 256 MB

- 9** After you specify the volume operation and search criteria, click *Start Scan*.
- 10** If you chose to list the files, an Inventory Detail Report is generated where you can move, copy, or delete files.
 - 10a** Select one or multiple files in the list, then select one of the following actions:
 - ♦ *Move the selected volumes to the other file tree.* (This option is available only for DST shadow volumes.)
 - ♦ *Move the selected files to a specified path on the server.*
 - ♦ *Copy the selected files to a specified path on the server.*
 - ♦ *Delete the selected files.*
 - 10b** Click *OK* to confirm the action.

The action is performed on the selected files, then a confirmation list of the files and the number of files moved is displayed.

If you chose to move selected files from one volume to another, the files that meet the search criteria are automatically moved, then a confirmation list of the files and the number of entries moved is displayed.
- 11** If you view the inventory chart again after the move, you can see that the files that matched the specified criteria before the move are now reported on the other volume.

15 Troubleshooting for the NCP Server and NCP Volumes

This chapter describes issues and possible workarounds for NCP Server and NCP volumes on Novell Open Enterprise Server (OES) 2 Linux servers.

- ♦ [Section 15.1, “NCP Clients Cannot Connect to the Server,” on page 129](#)
- ♦ [Section 15.2, “Error -601 When Deleting an NCP Volume,” on page 129](#)
- ♦ [Section 15.3, “Cross-Protocol Locking Stops Working,” on page 129](#)
- ♦ [Section 15.4, “Error on Copying or Deleting Files When Extended Attributes Are Not Enabled,” on page 130](#)

15.1 NCP Clients Cannot Connect to the Server

If users are not able to connect to the server, all the licensed user connections might be in use.

To resolve this problem, you can view and clear connections of users with active connections that are not logged in to the server. For information about clearing connections, see the following sections:

- ♦ [Section 9.6, “Clearing Not-Logged-In Connections to NCP Server,” on page 76.](#)
- ♦ [Section 9.7, “Clearing Connections to NCP Server,” on page 76](#)

15.2 Error -601 When Deleting an NCP Volume

If you attempt to create a volume at the command line by using the command syntax for creating an NCP volume inside a cluster load script (`ncpcon mount MYVOL=98@"/usr/novell/myvol"`), when you remove the NCP volume, you get a -601 error. This error indicates that the Volume object cannot be removed. The volume is removed successfully. This is a cosmetic error that occurs because the wrong command was used to create the volume.

When the command is used inside of a load script, the Volume object is intentionally not re-created each time the load script runs, regardless of the node where the cluster resource is being loaded. The Volume object is associated with the virtual cluster server, not the server where it is currently loaded.

To avoid getting the -601 error, use the `ncpcon create volume` command to create NCP volumes at the command line, which automatically creates a Volume object in eDirectory.

15.3 Cross-Protocol Locking Stops Working

Cross-protocol locking allows Samba/CIFS users and NCP users to concurrently access files by allowing only one user at any time to open the file for write. Multiple users who are accessing via NCP and Samba/CIFS can open a file for read only.

WARNING: Allowing users who access files via different protocols to concurrently open a file for write can lead to data corruption.

NCP Server for Linux provides cross-protocol locking for NCP and Linux Samba/CIFS users.

If cross-protocol locking is enabled for NCP Server for Linux but stops working for DST shadow volume pairs--that is, multiple users can open a file for read and write--it is probably because ShadowFS needs to be restarted. To resolve this problem, stop the shadowfs process, then start shadowfs. For information, see [“Starting and Stopping ShadowFS Manually”](#) in the *OES 2 SP3: Dynamic Storage Technology Administration Guide*.

15.4 Error on Copying or Deleting Files When Extended Attributes Are Not Enabled

When copying or deleting files that have Extended Attributes (EA), Novell Client displays the error, “Not enough free disk space” or “Path cannot be found.” To resolve this issue, you must enable EA on the file system:

- 1 Run the following command to verify if EA is enabled on the file system:

```
tune2fs -l Device |grep Default mount options
```

If the value of Default mount options is none, enable EA on the file system.

- 2 To enable EA on the file system, run the following commands:

```
tune2fs -o user_xattr Device
```

```
mount -o remount Device
```

On enabling EA, the value of Default mount options is user_xattr.

The value of Device is the device or path where the file system is mounted. It can be found at /etc/fstab.

16 Security Considerations for NCP Server

This section describes security issues and recommendations for NCP Server on a Novell Open Enterprise Server (OES) 2 Linux server. It is intended for security administrators or anyone who is responsible for the security of the NCP Server for Linux system. It requires a basic understanding of NCP Server. It also requires the organizational authorization and the administrative rights to effect the configuration recommendations.

- ♦ [Section 16.1, “UDP Port 524,” on page 131](#)
- ♦ [Section 16.2, “Soft Links,” on page 131](#)
- ♦ [Section 16.3, “Hard Links,” on page 132](#)
- ♦ [Section 16.4, “Log Files,” on page 132](#)
- ♦ [Section 16.5, “Audit Logs,” on page 133](#)

16.1 UDP Port 524

NCP Server uses UDP port 524 when mounting volumes with the `ncpmount (8)` command. NCP Server opens this port in the server firewall when it is installed.

16.2 Soft Links

Although NCP Server for Linux provides limited support for hardlinks, soft links are intentionally not supported. The following soft link features can be exploited to create security problems where users can give themselves access to subdirectories where they have no rights:

- ♦ The Linux POSIX permissions set on the soft link do not need to match the permissions set on the source file or directory.
- ♦ The soft link and source file are not restricted to paths on the same volume and file system.
- ♦ Soft links can link to files or directories.
- ♦ The name of the soft link does not need to match the name of the source file.

For example, directories on an NCP volume on Linux file systems can have different inherited rights, so the link can have different effective rights than the source. Security breaches can occur if someone accidentally creates a soft link to a sensitive area of the system, such as the `/etc` directory. A hacker can exploit the system by creating a soft link to a password file, then overwriting its contents. Soft links can cause security problems for programs that fail to consider the possibility that the file being opened may actually be a link to a different file. This is especially dangerous when the vulnerable program is running with elevated privileges.

16.3 Hard Links

NCP Server supports hardlinks for a file on an NCP volume (NCP share on a non-NSS file system) if the destination location for the hardlink is on the same NCP volume as the source file, and any of the following conditions is met:

- ◆ If the user is supervisor equivalent of the NCP volume, or
- ◆ If the user is the owner of the file, or
- ◆ If the "Other" Read/Write mode bits are set on the file on the non-NSS file system.

Other users are unable to open hard-linked files. This is because of a hard-link security problem where users can give themselves write access to files where they should only have read access.

For example, a user has world-readable access to `/etc/fileA`. The user creates a hardlink to `/etc/fileA` and specifies a destination for the link to be a directory on the same file system where the user has read/write access, such as the user's home directory. The user now has granted himself read/write access to `fileA`.

NCP Server supports hardlinks for a file on an NSS volume if the destination location for the hardlink is on the same NSS volume as the source file, and any of the following conditions is met:

- ◆ If the user is supervisor equivalent of the NSS volume, or
- ◆ If the user is the owner of the file.

In addition, the `Hardlinks` attribute must be enabled for the NSS volume to allow hardlinks support. The hardlinks can be in the same directory or in multiple directories in the same NSS volume. When hardlinks are used, the volume's users must be enabled with Linux User Management. The NSS file system is designed to provide secure support for hardlinks on NSS volumes. For information about how the hardlinks on an NSS volume work with file ownership, trustees, trustee rights, and inherited rights, see "[Understanding Hard Links](#)" in the OES 11 SP1: NSS File System Administration Guide for Linux.

16.4 Log Files

The following log files are located in the `/var/opt/novell/log` directory:

- ◆ `ncpserv.log`
- ◆ `ncp2nss.log`
- ◆ `ncptop.log`

Log files are managed by `logrotate`. For information on usage, see its man page (`man logrotate`).

The control files for `logrotate` are:

- ◆ `/etc/logrotate.d/novell-ncpserv-log`
- ◆ `/etc/logrotate.d/novell-ncpserv-audit`
- ◆ `/etc/logrotate.d/novell-ncp2nss-log`
- ◆ `/etc/logrotate.d/novell-ncp2nss-audit`

By default, the rollover size is 16 MB and 5 compressed copies are kept.

16.5 Audit Logs

The following audit log files are available:

- ♦ `/var/opt/novell/log/ncpserv.audit.log`
- ♦ `/var/opt/novell/log/ncp2nss.audit.log`
- ♦ `/usr/novell/sys/._NETWARE/SYS.audit.log`

A Commands and Utilities for NCP Server and NCP Volumes

This section describes commands and utilities for NCP Server services and NCP volumes on Novell Open Enterprise Server (OES) 2 Linux.

- ♦ [Section A.1, “NCPCON,” on page 135](#)
- ♦ [Section A.2, “NCPCON SET Parameters,” on page 153](#)
- ♦ [Section A.3, “NCP2NSS Command,” on page 161](#)
- ♦ [Section A.4, “ShadowFS Command,” on page 161](#)
- ♦ [Section A.5, “Virtual NCP Server Object Script,” on page 161](#)

A.1 NCPCON

The NCP Server Console (`ncpcon(8)`) is a management utility for NCP Server on Novell Open Enterprise Server 2 Linux. The man page for NCPCON is located in the `/usr/share/man/man8` directory. To view the man page when you are at the server console, enter `man ncpcon` at the terminal console prompt.

- ♦ [Section A.1.1, “Syntax,” on page 136](#)
- ♦ [Section A.1.2, “Getting Help,” on page 136](#)
- ♦ [Section A.1.3, “Starting and Stopping NCPCON Interactive Mode,” on page 137](#)
- ♦ [Section A.1.4, “Monitoring NCP Server,” on page 137](#)
- ♦ [Section A.1.5, “Managing NCP Server in a Cluster,” on page 138](#)
- ♦ [Section A.1.6, “Managing NCP Threads,” on page 138](#)
- ♦ [Section A.1.7, “Managing NCP Volumes,” on page 140](#)
- ♦ [Section A.1.8, “Managing File System Trustees and Trustee Rights for NCP Volumes,” on page 142](#)
- ♦ [Section A.1.9, “Managing NSS Volumes in a Cluster,” on page 144](#)
- ♦ [Section A.1.10, “Purging Deleted Files on NSS Volumes on Linux,” on page 144](#)
- ♦ [Section A.1.11, “Managing User Login,” on page 144](#)
- ♦ [Section A.1.12, “Sending Messages to Logged-In Users,” on page 144](#)
- ♦ [Section A.1.13, “Managing NCP Server Connections,” on page 145](#)
- ♦ [Section A.1.14, “Viewing or Closing Open Files,” on page 147](#)
- ♦ [Section A.1.15, “Managing Dynamic Storage Technology,” on page 148](#)
- ♦ [Section A.1.16, “Managing Dynamic Storage Technology on Novell Cluster Services for Linux Clusters,” on page 152](#)

A.1.1 Syntax

The NCPCON utility can be used in three modes:

- ♦ [“Interactive Mode” on page 136](#)
- ♦ [“Command Line Mode” on page 136](#)
- ♦ [“Scripting Mode” on page 136](#)

Interactive Mode

Open a terminal console, log in as the `root` user, then enter

```
ncpcon
```

This opens the NCPCON interactive console in the terminal console where you can enter the NCP Server console commands. Enter `exit` to stop the interactive mode.

Command Line Mode

For command line mode, issue an NCP Server command at a terminal console prompt by prefacing the command with `ncpcon`:

```
ncpcon [command]
```

For example:

```
ncpcon mount sys
```

When using `ncpcon` to issue commands directly from the console command prompt, you must escape the quote character (`"`) by preceding the character with a backslash (`\`). For example, a `send` command is entered as follows from the console command line prompt:

```
ncpcon send \"hello world\" to all
```

Escaping the quote character is not required when entering the command from the `ncpcon` prompt. For example, the `send` command is entered as followed from the `ncpcon` prompt:

```
send "hello world" to all
```

Scripting Mode

For scripting mode, issue the NCP Server command in the script by prefacing the command with `ncpcon`, then placing double-quotation marks around the NCP Server command:

```
ncpcon "[command]"
```

For example:

```
ncpcon "mount sys"
```

A.1.2 Getting Help

```
help [command]
```

Use this command to list the `ncpcon` console commands. To get specific help for a command, type `help` and the command.

EXAMPLES


```
help
help mount
help remove volume
```

A.1.3 Starting and Stopping NCP CON Interactive Mode

ncpcon

Use this command to start the ncpcon interactive mode.

EXAMPLE

```
ncpcon
```

exit

Use this command to exit out of the NCP CON application when you are using it in the interactive mode. The command is not used in the command line/scripting mode.

EXAMPLE

```
exit
```

A.1.4 Monitoring NCP Server

Use the commands in this section to manage the NCP Server service on your OES server.

config

Displays the NCP Server configuration information such as the server name, server version, product version, NCP version, mixed-mode paths status (yes/no), and commit files status (yes/no).

EXAMPLE

```
config
```

stats

Use this command to display NCP statistics, including the following:

- ◆ Server up time
- ◆ Packets in
- ◆ Packets dumped
- ◆ Packet receive buffer memory
- ◆ Packet reply buffer memory
- ◆ NCP requests
- ◆ NCP connections in use
- ◆ Connection table memory
- ◆ Mounted volumes
- ◆ Number of open files
- ◆ Local ID tracking
- ◆ File handle memory
- ◆ Volume SYS: file and subdirectory caching memory
- ◆ Volume SYS: trustee and inherited rights mask tracking memory

EXAMPLE

```
stats
```

version

This command displays version information for all currently running Novell NCP Server components, the OES build, and the hardware platform.

EXAMPLE

```
version
```

A.1.5 Managing NCP Server in a Cluster

NCPCON supports the `bind` and `unbind` commands for use with Novell Cluster Services for Linux on an OES 2 Linux server.

Use these commands in load or unload scripts when you want to configure the NCP access for files in a cluster resource that can be moved or failed over to another node in the cluster. NCP is required for NSS volumes, NCP volumes on Linux POSIX file systems, and Dynamic Storage Technology shadow volumes.

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

For information about configuring and managing Novell Cluster Services for Linux, see the [OES 2 SP3: Novell Cluster Services 1.8.8 Administration Guide for Linux](#).

bind *cluster_resource_name ip_address*

Binds the specified cluster resource name. Use this command to assign an IP address to the NCP Server cluster resource name.

EXAMPLE

```
bind oes_2_cluster 192.168.1.1
```

In a cluster load script, use the following syntax:

```
exit_on_error ncpcon bind --ncpservname=oes_2_cluster --  
ipaddress=192.168.1.1
```

unbind *cluster_resource_name ip_address*

Unbinds the specified cluster resource name. Use this command to remove the assignment of an IP address from the NCP Server cluster resource name.

EXAMPLE

```
unbind oes_2_cluster 192.168.1.1
```

In a cluster unload script, use the following syntax:

```
ignore_error ncpcon unbind --ncpservname=oes_2_cluster --  
ipaddress=192.168.1.1
```

A.1.6 Managing NCP Threads

Use the commands in this section to configure the larger number of concurrent NCP threads and to verify the current NCP utilization.

ncpcon set ADDITIONAL_SSG_THREADS=<value>

Sets the number of additional SSG Threads (over and above the fixed 25 NCP threads) that can be used to serve incoming NCP file service requests. These threads are used when the fixed 25 NCP threads are busy and taking more than expected time to finish.

Default: 7, Valid Range: 7 to 103.

ncpcon set CONCURRENT_ASYNC_REQUESTS=<value>

Sets the maximum number of the Async eDirectory NCP request threads that can be created.

Default: 15, Valid Range: 15 to 128.

ncpcon threads

Allows you to verify the current number of concurrent NCP threads running on the server. Use this command to verify the settings that you make for the ADDITIONAL_SSG_THREADS and CONCURRENT_ASYNC_REQUESTS settings.

Example - NCP SSG Thread Statistics

Total Number of Active SSG Threads: 13

Max Number of Additional SSG Threads (over and above fixed 25 NCP Threads): 12

Total Number of NCP Streams: 20

Current Average Load per Thread: 1.54

Peak Number of Active SSG Threads: 25

Peak Number of NCP Streams: 2148

Peak Average Load per Thread: 85.92

Total Number of Active SSG Threads: The currently active SSG threads.

Max Number of Additional SSG Threads (over and above fixed 25 NCP Threads): When all 25 fixed SSG threads are exhausted, then this number defines the additional number of threads that can be created to serve other incoming NCP file service requests. This value can be modified using the `ncpcon set ADDITIONAL_SSG_THREADS=value` command. Default=7, Valid Range: 1 to 103.

Total Number of NCP Streams: The current number of NCP connections that have been handled by the Active SSG threads.

Current Average Load per Thread: The current average load of NCP connections on the Active SSG threads.

Peak Number of Active SSG Threads: The highest number (peak) of the Active SSG threads.

Peak Number of NCP Streams: The highest number (peak) of NCP streams.

Peak Average Load per Thread: The highest number (peak) of streams per thread.

Example - Async (eDir) Threads and Requests Statistics

Number of Running Threads: 0

Max Thread Size: 25

Thread Peak Size: 25

Number of Queued Requests: 0

Queued Requests Peak Size: 174

Number of Running Threads: The currently running number of Async threads that can handle eDir Requests.

Max Thread Size: The maximum number of the Async threads that can be created. This value can be modified using the `ncpcon set CONCURRENT_ASYNC_REQUESTS=value` command. Default: 15, Valid Range: 15 to 256.

Thread Peak Size: The highest number (peak) of Async threads the server required so far. This number is reset when the service is restarted.

Number of Queued Requests: The number of queued eDir requests (after the Async threads got exhausted).

Queued Requests Peak Size: The highest number (peak) of eDir requests that have been queued so far (after the Async threads got exhausted).

A.1.7 Managing NCP Volumes

Use the commands in this section to create, manage, or remove NCP volumes on Linux POSIX file systems on your OES 2 Linux server. NCP volumes use the Novell Trustee Model for controlling user access to files. Users access the volume through the Novell Client.

change volume *ncp_volumename* [*option*]

Display the current volume options setting for the specified volume, or change the setting for a specified option on the specified volume. You must dismount the NCP volume before you can change its options settings with this command.

This command cannot be added to a cluster load script.

OPTION

Inherit_POSIX_Permissions <on|off>

This is disabled by default. When this setting is disabled, only the root user and the owner of the file can access the volume as local users in a Linux environment. Disabling the POSIX inheritance is the most secure setting because NCP volumes use the Novell Trustee Model for file system access control.

If this option is enabled on a volume, the POSIX permissions are permitted to be inherited from parent directories. If POSIX inheritance is enabled, local access in the Linux environment by users who are not authenticated via Novell eDirectory can create security problems.

EXAMPLES

To view the current setting, enter the following at the console command prompt:

```
ncpcon change volume sys
```

To enable Inherit POSIX Permissions on the sys volume, start NCPCON by entering ncpcon at the console command prompt, then enter the following at the ncpcon prompt:

```
dismount sys
change volume sys Inherit_POSIX_Permissions on
mount sys
exit
```

create volume *ncp_volumename* *path*

Use this command to create an NCP volume by defining an NCP share on an existing POSIX file system on your Linux server. This command creates a Volume object in Novell eDirectory, and associates the volume name to a path on your server when using file system types other than the Novell Storage Services (NSS) file system.

This command does not remove or delete data in the mount point location. It adds the NCP volume's volume name and mount information to the NCP Server configuration file (`/etc/opt/novell/ncpserv.conf`).

Replace *ncp_volumename* with the name for the volume.

Replace *path* with the path to an existing folder on the Linux server that is used as the mount point for the NCP volume. The folder must be on a Linux POSIX file system volume.

After creating the NCP volume, you must mount it to make it accessible to NCP clients.

EXAMPLE

```
create volume vol1 /media/ncpvolumes/vol1
```

dismount <ncp_volumename | all>

Use this command to dismount a specified NCP volume on your Linux server, or to dismount all NCP volumes on your Linux server.

EXAMPLES

To dismount the NCP volume named VOL1, enter

```
dismount VOL1
```

To dismount all NCP volumes, enter

```
dismount all
```

mount < all | volumename | volumename=volume_id,path=/volume_mntpoint >

Use this command to mount an NCP volume on your Linux server. This command makes the NCP volume accessible to NCP clients. Replace *volumename* with the name of the volume, such as VOL1. To mount all volumes, replace the volume name with `all`.

Replace *volume_id* with a value from 0 to 254 as the server volume ID when you want to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource. Replace */volume_mntpoint* with the Linux mount point for the NCP volume, such as `/media/ncpvolumes/VOL1`.

In a cluster load script, use the following syntax:

```
exit_on_error ncpcon mount volumename=volume_ID,path=/volume_mntpoint
```

For example:

```
exit_on_error ncpcon mount USERS=254,path=/media/ncpvolumes/USERS
```

EXAMPLES

```
mount sys
```

```
mount all
```

```
mount VOL1=254,path=/media/ncpvolumes/VOL1
```

remove volume ncp_volumename

Use this command to remove the NCP volume and path association. This command does not remove or delete data from the mount location. This command removes the NCP volume mount information from `/etc/opt/novell/ncpserv.conf` configuration file.

EXAMPLE

```
remove volume VOL1
```

volumes, volume volumename

Displays a list of currently mounted NCP volumes. You can also specify a specific volume name with the command to get information about that volume.

EXAMPLES

```
volumes
volume VOL1
```

volume data

Displays a list of currently mounted NCP volumes and information about them. For example, if the volume is a Dynamic Storage Technology shadow volume pair, it identifies the Linux paths of its primary and secondary volumes.

EXAMPLE

```
volume data
```

disable write <volume name> [Broadcast message]

This command disables write permission on files in the specified volume. The broadcast message is optional but if specified the message is sent to all the clients accessing the specified volume.

NOTE: This command when executed closes any files that are opened for writing.

Example

```
disable write VOL1 Closing all open files on this volume.
```

enable write <volume name> [Broadcast message]

Use this command to enable write permissions on a volume that has been previously disabled for writing using the `disable write` command.

The broadcast message is optional but if specified the message is sent to all the clients accessing the specified volume.

Example

```
enable write VOL1 Files on this volume can now be edited.
```

A.1.8 Managing File System Trustees and Trustee Rights for NCP Volumes

Use the commands in this section to manage file system trustees and trustee rights for NCP volumes for Linux POSIX file systems on your OES 2 Linux server. NCP volumes use the Novell Trustee Model for controlling user access to files.

```
rights <view path | add path fdn options | remove path fdn>
```

Allows you to view, add, or remove trustees and trustee rights for a specified path. Replace *fdn* with the typeless fully distinguished name (username.context) of the trustee, such as bob.example. Replace *options* with all, none, or the combination of rights to assign for the specified trustee. List the rights together without spaces or commas, such as RF. For visibility, users need the Read and File Scan rights.

OPTIONS

all

All rights

none

No rights

S

Supervisor

R

Read

W

Write

C

Create

E

Erase

M

Modify

F

File scan

A

Access control

EXAMPLES

```
rights view sys:login
```

```
rights add users:bob bob.example RF
```

```
rights remove users:bob bob.example
```

```
irm <view path | set path mask>
```

Displays or sets the inherited rights mask on the specified path. Specify both the NCP volume and directory in the NetWare path format, such as `volname:dir1/dir2`. Replace *mask* with the mask options `all`, `none`, or the combination of rights to block from being inherited. List the rights together without spaces or commas, such as `SAE`.

MASK OPTIONS**all**

All rights

none

No rights

S

Supervisor

R

Read

W

Write

C

Create

E

Erase

M

Modify

F

File scan

A

Access control

EXAMPLES

```
irm view sys:login
irm set users: SA
irm set users:bob RF
```

A.1.9 Managing NSS Volumes in a Cluster

Use the following load script to mount NSS volumes in a cluster resource.

```
ncpcon mount <VOLUMENAME>=<VOLUMEID>
ncpcon mount /opt=ns=LONG <VOLUMENAME>=<VOLUMEID>
ncpcon mount /opt=ns=UNIX <VOLUMENAME>=<VOLUMEID>
```

A.1.10 Purging Deleted Files on NSS Volumes on Linux

```
purge volume nss_volumename
```

Use this command to purge, or permanently remove, deleted files from an NSS volume on Linux. This command works only with NSS volumes where the Salvage attribute has been previously enabled.

EXAMPLE

```
purge volume vol1
```

A.1.11 Managing User Login

Use the commands in this section to enable or disable login for NCP clients to the Linux server.

```
disable login
```

Use this command to prevent NCP clients from logging in to the Linux server.

EXAMPLE

```
disable login
```

```
enable login
```

Use this command to allow NCP clients to log in to the Linux server.

EXAMPLE

```
enable login
```

A.1.12 Sending Messages to Logged-In Users

```
send "text_message" to <station | station1,station2... | all>
```

Use this command to send a message to logged-in NCP clients. Replace *text_message* with a message of up to 252 characters and spaces. Specify multiple logged-in stations by separating the connection numbers with commas and no spaces. Specify *all* to send the message to all logged-in users.

To find the connection number assigned to a user's connection, use the `connection` commands in [Section A.1.13, "Managing NCP Server Connections,"](#) on page 145.

EXAMPLE

To issue the command at the `ncpcon` prompt:

```
send "Hello, world" to 1
send "Hello, world" to 1,2,4
send "Hello, world" to all
```

To issue the command at the terminal console prompt:

```
ncpcon send \"Hello, world\" to 1
ncpcon send \"Hello, world\" to 1,2,4
ncpcon send \"Hello, world\" to all
```

A.1.13 Managing NCP Server Connections

Use the `connection` commands in this section to display the NCP Server connection information for all current connections, or for a given connection. You can also display a list of the connections and clear the connections. The general syntax is:

```
connection [list | connection_number | clear connection_number]
```

connection

Displays an overview of current NCP Server connection information.

Parameter	Description
Connection Slots Allocated	<p>Displays the number of slots currently allocated for use. As connection slots are required on this server that exceed the current number of slots displayed here, new slots are allocated.</p> <p>Depending on the server's memory, connection slots are usually allocated in blocks of 16. Connection slots are allocated as needed by users, NetWare Loadable Module (NLM) programs, and other services.</p>
Connection Slots Being Used	<p>Displays the number of connection slots currently in use. As this number matches or exceeds the Connection Slots Allocated entry, more connection slots are allocated to the connection table.</p>
Signing Level	<p>Displays the level at which NCP packet signature signing is set on the server. NCP packet signatures prevent packet forgery by requiring the server and the workstation to sign each NCP packet. A higher packet signature number impacts the performance of your server. At some point, the need for security might outweigh certain performance issues.</p>
Login State	<p>Displays whether users are allowed to log in to the server.</p> <p>To disable users from being able to log in to the server (for server maintenance or other reasons), enter <code>disable login</code> at the NCPCON prompt, or enter <code>ncpcon disable login</code> at a terminal console prompt.</p> <p>To allow users to log in to the server, enter <code>enable login</code> at the NCPCON prompt, or enter <code>ncpcon enable login</code> at a terminal console prompt.</p>

Parameter	Description
Licensed Connections	Displays the number of connections that are currently licensed. Licensed connections are authenticated, logged in, and consume a license. An unlicensed connection does not consume a license and can be authenticated or not. An unlicensed, authenticated connection can access the Novell eDirectory database but cannot access any other resources.
Not Logged In Connections	<p>Clears all user connections that are open but not currently authenticated to the server. The connections can be cleared whether they are based on an NLM or based on a user.</p> <p>Use this parameter to clear all user or NLM connections that are not logged in.</p> <p>IMPORTANT: Some connections based on an NLM, such as backup NLM programs, maintain a Not Logged In connection until it is time to log in and perform the specified service. If the connection is cleared, the NLM might not be able to re-establish a connection to the server unless it is unloaded and reloaded. This might prevent the NLM from performing the required task.</p>

EXAMPLE

`connection`

`connection list`

Displays a list of all current NCP Server connections.

Parameter	Description
<i>Station</i>	Shows the connection number for each connection. Connection 0 is the connection used by the server. The server's operating system uses connection numbers to control each station's communication with other stations. Remote Manager does not distinguish connections that don't count against the server's connection limit.
<i>Name</i>	<p>Shows the name of the user, server, service, or login status and links to specific information about that user connection such as the login time, connection number, network address, login status, number of NCP requests, files in use, and security equivalence.</p> <p>Connections with an asterisk (*) displayed next to the name indicate an unlicensed connection (it does not consume a license). These licenses can be either authenticated or not authenticated. An unlicensed, authenticated connection can access the Novell eDirectory database but not other server resources.</p> <p>From this detailed Connection Information page, you can also clear the connection or send a message to the user.</p>
<i>Reads & Writes</i>	Shows the number of reads and writes (in bytes) made by the connection.
<i>NCP Request</i>	Shows the number of NCP requests made by the connection.
<i>Login Time</i>	Shows the login day, date, and time for the connection.

EXAMPLE

```
connection list
```

```
connection connection_number
```

Displays detailed information about a specified NCP Server connection. Replace *connection_number* with the station of interest. You can find the station's connection number from the report displayed by issuing the `connection list` command.

Parameter	Description
Connection	The station number for the connection.
Login Status	Shows whether the connection is Authenticated or Not Logged In.
Authentication Method	Shows the authentication method used if the connection is logged in.
Login Time	Shows the login day, date, and time for the connection.
Privileges	Shows whether the connection has privileges, such as Supervisor or Console Operator.
Connection Type	Shows whether the connection is internal or external.
Bytes Read	Shows the total number of reads made by the connection.
Bytes Written	Shows the total number of writes made by the connection.
NCP Requests	Shows the total number of NCP requests made by the connection.
IP Address	Shows the IP address where the connection originates.
Open Files	Shows the files open for the connection.
Security Equivalence	Shows the name of the user, server, or service if it is logged in.

EXAMPLE

```
connection 1
```

```
connection clear connection_number
```

Clears the NCP Server connection for a specified station. Replace *connection_number* with the station of interest. You can find the station's connection number from the report displayed by issuing the `connection list` command.

EXAMPLE

```
connection clear 1
```

A.1.14 Viewing or Closing Open Files

```
files operation <v=volumename | f=filename | c=connection_number>
```

Use this command to list or close open files on an NCP volume by volume, filename, or connection number.

To find the connection number assigned to a user's connection, use the `connection` commands in [Section A.1.13, "Managing NCP Server Connections,"](#) on page 145.

OPERATION OPTIONS

list

Lists the open files for a specified NCP volume by volume, filename, or connection number.

close

Closes the open files for a specified NCP volume by volume, filename, or connection number.

OPTIONS**v=*volumename***

Replaces *volumename* with the name of the NCP volume.

f=*filename*

Replaces *filename* with path on the Linux file system of the file you want to close, such as /usr/novell/sys/*filename.ext*.

c=*connection_number*

Replaces *connection_number* with the station number of the connection whose open files you want to close.

EXAMPLES

```
files list v=sys
files list f=/usr/novell/sys/test.txt
files list c=9
files close v=sys
files close f=/usr/novell/sys/test.txt
files close c=9
```

A.1.15 Managing Dynamic Storage Technology

NCPCON supports the commands in this section for use with Novell Dynamic Storage Technology. For information about configuring and managing shadow volumes and file systems, see the [OES 2 SP3: Dynamic Storage Technology Administration Guide](#).

create shadow_volume [options] *primary_volumename shadow_path*

Creates a shadow association between an NCP volume and an NCP shadow volume. Specify the volume name for the primary volume and the path of mount location for the NCP shadow volume. Adds the SHADOW_VOLUME mount information to the `/etc/opt/novell/ncpserv.conf` file.

By using `ncpcon` to issue the command, you do not need to restart `ndsd` in order for the changes to take effect.

OPTIONS**/Cluster_Resource**

Causes the shadow volume to be created in NCP, but does not add a shadow volume entry to the `/etc/opt/novell/ncpserv.conf` file. The absence of the entry is desired in order to allow the NCP volume to fail over to other nodes in a Novell Cluster Services for Linux cluster.

Use this option in the cluster load script to create a shadow volume for a cluster resource. Because the volume is not defined in `ncpserv.conf`, you do not need the `ncpcon remove shadow_volume` command in the cluster unload script.

Use this option in combination with the `/ID=volume_id` option.

/ID=*volume_id*

Specifies the server volume ID (0 to 254) to use when mounting the shadow volume. Use this option to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource on any node in the cluster.

Use this option in combination with the `/Cluster_Resource` option.

EXAMPLES

```
create shadow_volume vol1 /home/shadows/vol1
```

Creates a shadow volume where `vol1` is the primary storage area and `/home/shadows/vol1` is its mount point as a shadow volume.

```
create shadow_volume /cluster_resource /id=254 vol1 /home/shadows/vol1
```

Creates a shadow volume where `vol1` is the primary storage area and `/home/shadows/vol1` is its mount point as a shadow volume. The shadow volume is created in NCP, but no entry is added to the `ncpserv.conf` file. The server volume ID is 254 on any node in the cluster where it is mounted.

```
remove shadow_volume [/l] volumename
```

Removes the shadow association between the primary storage area and secondary storage area. The shadow volume must be dismounted before this operation can be done.

This command removes the `SHADOW_VOLUME` command from the `/etc/opt/novell/ncpserv.conf` file. If the `/l` option is specified, it then leaves files where they are on either on the primary and secondary volumes. If the `/l` option is not specified, it then moves all files from the secondary storage area back to the primary storage area. Make sure that the primary volume has sufficient space to accommodate all the files before you remove the shadow relationship.

Because it is moving files back to the primary, the removal process can take some time, depending on how much data must be moved. After completion, a summary report is created and displayed.

This command can be added to a cluster load script.

EXAMPLES

Issue the following commands from the NCP Console, or prepend the command with `ncpcon` when issuing from a script or at a terminal console prompt.

```
remove shadow_volume vol1
```

Removes the shadow relationship for shadow volume `vol1`, and moves all files from the secondary storage area to the primary storage area. You must dismount `vol1` before you issue this command.

```
remove shadow_volume /l vol1
```

Removes the shadow relationship for shadow volume `vol1`, and leaves files where they currently are on the secondary storage area and the primary storage area. You must dismount `vol1` before you issue this command.

```
shadow volumename operation=<lp | ls | mp | ms> [options]
```

Allows you to list files on the shadow volume, or to move files between the primary storage area and the secondary storage area based on specified criteria. All files on the selected shadow volume that match the criteria are moved. Use the command from within `cron` jobs to automate data partitioning.

OPERATION OPTIONS

lp

Lists primary files. Lists all files currently residing on the primary storage area.

ls

Lists shadow files. Lists all files currently residing on the secondary storage area.

mp

Moves files to primary. Moves files that match the specified criteria to the primary storage area from the secondary storage area.

ms

Moves files to shadow. Moves files that match the specified criteria to the secondary storage area from the primary storage area.

OPERATIONS

pattern="searchPattern"

Specifies the file pattern to match against.

owner="username.context"

Specifies the Novell eDirectory username and context of the owner of the files to match against.

uid=uidValue

Specifies the Linux user ID to match against.

time=[time_field]

Specifies which time field to match against, where the *time_field* is:

[m] [a] [c]

- ♦ **m**: Last time modified (content)
- ♦ **a**: Last time accessed
- ♦ **c**: Last time changed (metadata)

range=[time_period]

Specifies which time period to match against, where the *time_period* is:

[a] [b] [c] [d] [e] [f] [g] [h] [i] [j]

- ♦ **a**: Within last day
- ♦ **b**: 1 day to 1 week
- ♦ **c**: 1 week to 2 weeks
- ♦ **d**: 2 weeks to 1 month
- ♦ **e**: 1 month to 2 months
- ♦ **f**: 2 months to 4 months
- ♦ **g**: 4 months to 6 months
- ♦ **h**: 6 months to 1 year
- ♦ **i**: 1 year to 2 years
- ♦ **j**: More than 2 years

size=[size_differential]

Specifies the size differential to match against, where the *size_differential* is:

[a] [b] [c] [d] [e] [f] [g] [h] [i] [j] [k]

- ♦ **a:** Less than 1 KB
- ♦ **b:** 1 KB to 4 KB
- ♦ **c:** 4 KB to 16 KB
- ♦ **d:** 16 KB to 64 KB
- ♦ **e:** 64 KB to 256 KB
- ♦ **f:** 256 KB to 1 MB
- ♦ **g:** 1 MB to 4 MB
- ♦ **h:** 4 MB to 16 MB
- ♦ **i:** 16 MB to 64 MB
- ♦ **j:** 64 MB to 256 MB
- ♦ **k:** More than 256 MB

output="filename"

Output the search results to the specified file.

EXAMPLES

```
shadow vol1 operation=ls pattern="*.exe"
```

Lists all files of type EXE that currently reside on the secondary storage area for the shadow volume vol1.

```
shadow vol1 operation=lp size=g
```

Lists all files of sizes between 1 MB to 4 MB that currently reside on the primary storage area for the shadow volume vol1.

```
shadow vol1 operation=ms range=j
```

Moves all files on the primary storage area that have not been modified, accessed, or changed in more than 2 years from the primary storage area to the secondary storage area for the shadow volume vol1.

```
shift "volumename:\path\filename" [primary | shadow]
```

Returns the specified file's location as being on the primary storage area or secondary storage area. Specify the primary or secondary options to move the specified file from its current location to the specified storage area.

OPTIONS

primary

Moves the specified file from the secondary storage area to the primary storage area. The file must be closed when you issue the command; otherwise, the command fails.

shadow

Moves the specified file from the primary storage area to the secondary storage area. The file must be closed when you issue the command; otherwise, the command fails.

EXAMPLES

```
shift "sys:\textfile.txt"
```

Show the specified file's storage area location in the shadow volume as primary (the primary storage area) or shadow (the secondary storage area) for the shadow volume sys.

```
shift "sys:\textfile.txt" primary
```

Move the specified file's storage area location from the secondary storage area to the primary storage area for the shadow volume sys.

```
shift "sys:\textfile.txt" shadow
```

Move the specified file's storage area location from the primary storage area to the secondary storage area for the shadow volume `sys`.

A.1.16 Managing Dynamic Storage Technology on Novell Cluster Services for Linux Clusters

NCPCON supports the commands in this section for use with Novell Dynamic Storage Technology in combination with Novell Cluster Services for Linux clusters. For information about configuring and managing shadow volumes and file systems in a cluster, see the [OES 2 SP3: Dynamic Storage Technology Administration Guide](#).

Use the following syntax in cluster load scripts to mount the volume in a cluster. With clustering, no changes are needed to the `ncpserv.conf` file for shadowing. The primary volume information is also not added to the `ncpserv.conf` file.

Scenario 1: Primary NSS and Shadow NSS

```
ncpcon mount volumename=volID,SHADOWVOLUME=shadow_volumename
```

Use this command in a cluster load script when the primary volume is an NSS volume and the secondary volume is an NSS volume. Both NSS volumes must already exist and be mounted in NSS.

Replace `volID` with a value from 0 to 254 as the server volume ID to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource.

EXAMPLE

```
ncpcon mount VOL1=254,SHADOWVOLUME=ARCHIVE1
```

Mounts the NSS volume named `VOL1` with a volume ID of 254. The primary volume is an existing NSS volume named `VOL1` (`/media/nss/VOL1`). The secondary volume is an existing NSS volume named `ARCHIVE1` (`/media/nss/ARCHIVE1`).

Scenario 2: Primary Non-NSS and Shadow Non-NSS (Not supported in the initial release.)

```
ncpcon mount volumename=volID,SHADOWPATH=shadowpath,path=primarypath
```

Use this command when the primary volume is a non-NSS volume and the secondary volume is a non-NSS volume.

Replace `volID` with a value from 0 to 254 as the server volume ID to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource.

EXAMPLE

```
ncpcon mount VOL1=254,SHADOWPATH=/media/ncpvolumes/ARCHIVE1,path=/media/ncpvolumes/VOL1
```

Mounts the NCP volume named `VOL1` with a volume ID of 254. The primary volume's path is `/media/ncpvolumes/VOL1`. The secondary volume's path is `/media/ncpvolumes/ARCHIVE1`.

Scenario 3: Primary Non-NSS and Shadow NSS (Not supported in the initial release.)

```
ncpcon mount volumename=volID,SHADOWVOLUME=shadow_volumename,path=primarypath
```

Use this command when the primary volume is a non-NSS volume and the secondary volume is an NSS volume. The NSS volume must already exist on the system and be mounted in NSS.

Replace *volID* with a value from 0 to 254 as the server volume ID to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource.

EXAMPLE

```
ncpcon mount VOL1=254,SHADOWVOLUME=ARCHIVE1,path=/media/ncpvolumes/VOL1
```

Mounts the NCP volume named VOL1 with a volume ID of 254. The primary volume's path is /media/ncpvolumes/VOL1. The secondary volume is an existing NSS volume named ARCHIVE1 (mounted at /media/nss/ARCHIVE1).

Scenario 4: Primary NSS and Shadow Non-NSS (Not supported in the initial release.)

```
ncpcon mount volumename=volID,SHADOWPATH=shadowpath
```

Use this command when the primary volume is an NSS volume and the secondary volume is a non-NSS volume. The NSS volume must already exist on the system and be mounted in NSS.

Replace *volID* with a value from 0 to 254 as the server volume ID to ensure that the volume has the same ID on all servers when it is mounted in a cluster resource.

Example

```
ncpcon mount VOL1=254,SHADOWPATH=/media/ncpvolumes/ARCHIVE1
```

Mounts an NSS volume named VOL1 with a volume ID of 254. The primary volume is an existing NSS volume named VOL1 (/media/nss/VOL1). The secondary volume is an NCP volume named ARCHIVE1 that is mounted at /media/ncpvolumes/ARCHIVE1.

A.2 NCPCON SET Parameters

NCPCON provides several SET parameters that can be used to customize your NCP Server configuration. The parameters can be changed by entering `set parameter_name` while in the NCPCON utility. You can also enter `ncpcon set parameter_name` at the Linux command line.

The following sections identify the global NCP Server parameters with their default values and valid options:

- ♦ [Section A.2.1, "Directory Cache Management for NCP Server,"](#) on page 154
- ♦ [Section A.2.2, "Dynamic Storage Technology for NCP Server,"](#) on page 155
- ♦ [Section A.2.3, "Locks Management for File Access on NCP Server,"](#) on page 156
- ♦ [Section A.2.4, "Logs of NCP Server Events,"](#) on page 157
- ♦ [Section A.2.5, "NCP Communications,"](#) on page 158
- ♦ [Section A.2.6, "NCP Server Environment,"](#) on page 158
- ♦ [Section A.2.7, "NCP Volumes,"](#) on page 159
- ♦ [Section A.2.8, "NCP Volumes Low-Space Warning,"](#) on page 160

A.2.1 Directory Cache Management for NCP Server

Table A-1 Server Parameter Information for Directory Cache Management

Parameter Name and Description	Default Value	Value Options
<p>MAXIMUM_CACHED_FILES_PER_SUBDIRECTORY</p> <p>Controls the maximum number of file entries that can be cached by the system for a given folder in the directory cache.</p> <p>The NCP engine attempts to cache all files in a subdirectory for better performance, but sometimes memory is insufficient, so the NCP engine handles instances where only some of the file metadata is cached.</p> <p>Changing this parameter might improve or worsen performance, depending on your usage patterns.</p>	10240	Minimum is 512 files.
<p>MAXIMUM_CACHED_FILES_PER_VOLUME</p> <p>Controls the maximum number of file entries that can be cached by the system for a given volume in the directory cache.</p> <p>The NCP engine attempts to cache as many files as possible for better performance, but sometimes memory is insufficient, so the NCP engine handles instances where only some of the file metadata is cached.</p> <p>Changing this parameter might improve or worsen performance, depending on your usage patterns.</p>	256000	Minimum is 2048 files.
<p>MAXIMUM_LAZY_CLOSE_FILES</p> <p>Controls the maximum number of files' handles that can be lazy closed in the directory cache.</p> <p>When the NCP engine opens files for a client, it manages one Linux file handle for each file that is opened, regardless of how many clients open the same file. When a file is closed by the client, the NCP engine waits before closing the file just in case a client wants to reopen the file. This is called a "lazy close."</p> <p>This parameter controls how many files can be in a lazy close state at one time. If the configured maximum lazy close files number has been reached, the files that are closed by a client also have their Linux file handles immediately closed.</p> <p>Linux limits how many file handles can be in use at one time (64,000), so setting this number too high can have negative consequences.</p>	4096	16 to 64000
<p>MAXIMUM_CACHED_SUBDIRECTORIES_PER_VOLUME</p> <p>Controls the maximum number of folder entries that can be cached by the system for a volume in the directory cache.</p>	102400	4096
<p>LOG_CACHE_STATISTICS</p> <p>Controls whether cache statistics are logged in the ncpserv.log file.</p>	0	0 - Disable 1 - Enable

A.2.2 Dynamic Storage Technology for NCP Server

For information about configuring global policies for DST, see the [OES 2 SP3: Dynamic Storage Technology Administration Guide](#).

Table A-2 Server Parameter Information for Dynamic Storage Technology

Parameter Name and Description	Default Value	Value Options
DUPLICATE_SHADOW_FILE_ACTION Controls how duplicate files conflicts are handled.	0	0 - Show duplicate shadow files (default) 1 - Hide duplicate shadow files 2 - Rename duplicate shadow files 3 - Delete duplicate files from shadow area 4 - Move duplicate shadow files to / . _DUPLICATE_FILES
DUPLICATE_SHADOW_FILE_BROADCAST Controls whether broadcast messages are sent to NCP users whenever duplicate files conflicts occur.	1	0 - Disable 1 - Enable
REPLICATE_PRIMARY_TREE_TO_SHADOW Controls how the primary tree is replicated from the primary tree to the shadow tree. By default, it is disabled, and paths are replicated to the secondary storage area gradually as data is moved from the primary location to the secondary location. If it is enabled, the entire tree is replicated even if no files in a path have been moved to the secondary storage location.	0	0 - Disable 1 - Enable
SHIFT_ACCESSED_SHADOW_FILES Controls whether files are moved from the secondary volume to the primary volume if the volume is accessed twice during a specified elapsed time. Use <code>SHIFT_DAYS_SINCE_LAST_ACCESS</code> to specify the time period. The file is moved after it is closed.	0	0 - Disable 1 - Enable
SHIFT_MODIFIED_SHADOW_FILES Controls whether files are moved from the secondary volume to the primary volume if the file is modified. The file is moved after it is closed.	1	0 - Disable 1 - Enable
SHIFT_DAYS_SINCE_LAST_ACCESS Specifies the number of elapsed days during which a file must be accessed twice before it is moved. This applies only if <code>SHIFT_ACCESSED_SHADOW_FILES</code> is enabled.	1	0 - Disable 1 to 365 (in days)

A.2.3 Locks Management for File Access on NCP Server

Table A-3 Server Parameter Information for Locks Management

Parameter Name and Description	Default Value	Value Options
<p>CROSS_PROTOCOL_LOCKS</p> <p>Controls cross-protocol file locking support between NCP and other protocols, including Novell Samba, Novell CIFS, Novell AFP, and ConsoleOne. Novell CIFS and Novell AFP support cross-protocol file locking in OES 2 SP2 Linux and later. Cross-protocol locks help prevent the same file from being concurrently accessed for modifications with multiple protocols. Each recognizes when the other has the file in use.</p> <p>Turning this option on decreases performance, so do not turn it on unless you plan on sharing files across multiple protocol clients.</p>	1	1 - Enable 0 - Disable
<p>OPLOCK_SUPPORT_LEVEL</p> <p>Controls NCP opportunistic locking.</p> <p>Oplocks are locks that allow the client to cache file data for better performance.</p>	2	0 - Disable 1 - Exclusive locks 2 - Shared and exclusive locks
<p>MAXIMUM_FILE_LOCKS_PER_CONNECTION</p>	1000	This value is hard-coded. Modifying the value has no effect.

NCP Server has an internal byte-ranging mechanism to prevent potential data corruption when files on NSS and NCP volumes are accessed by NCP clients. Cross-protocol file locking (CPFL) uses the Linux Advisory byte-range lock to prevent potential data corruption when files are accessed by non-NCP file access protocols and by other applications that directly access the files with POSIX APIs. By default, CPFL is enabled (`CROSS_PROTOCOL_LOCKS = 1`) on OES 2 Linux servers. CPFL is enforced globally for all NCP and NSS volumes on the server.

WARNING: Disabling cross-protocol file locking can cause data corruption if any application or non-NCP file access protocol accesses the same data that is accessed via NCP. We recommend that you do not disable CPFL, even if NCP is the only active file access protocol.

Non-NCP file access protocols include Novell Samba, Novell CIFS, and Novell AFP. Applications include any application or service that accesses data on an NCP volume or NSS volume, such as SSH, FTP, restore, scripts, antivirus, database, management tools, and so on.

For example, when ConsoleOne is used to administer the GroupWise database, GroupWise agents directly access the files. You must enable `CROSS_PROTOCOL_LOCKS` in order for the Linux Advisory byte-range locks to work and prevent any potential data corruption.

NOTE: For better performance, you can disable CPFL if you are not using non-NCP file access protocols and the files are not directly accessed by other applications. However, this is not recommended; see the Warning above.

A.2.4 Logs of NCP Server Events

Table A-4 Server Parameter Information for Logging NCP Server Events

Parameter Name and Description	Default Value	Value Options
<p>LOG_LEVEL</p> <p>Controls the nature and types of messages that are logged to the /var/opt/novell/log/ncpserv.log file.</p>	WARN	<p>Each level logs entries for its level and the levels listed above it.</p> <p>NOTHING – Disable logging.</p> <p>ERROR – Log only error messages.</p> <p>WARNING – Log warning and error messages.</p> <p>INFO – Log informational, warning and error messages.</p> <p>DEBUG – Log informational, warning, debug and error messages.</p> <p>ALL – Log all messages.</p>
<p>LOG_CACHE_STATISTICS</p> <p>Controls whether cache statistics are logged in the ncpserv.log file.</p> <p>Turning this setting on causes the NCP engine's directory cache to output statistics to a log file. Information such as the number of cached files, number of cached directories, number of open files, etc. is logged.</p>	0	<p>0 - Disable</p> <p>1 - Enable</p>
<p>LOG_IDBROKER_ERRORS</p> <p>Controls whether ID broker errors are logged in the ncpserv.log file.</p>	0	<p>0 - Disable</p> <p>1 - Enable</p>
<p>LOG_MAXIMUM_FILE_SIZE</p> <p>This parameter is used to control the maximum size of the ncpserv.log file in bytes. The default is 4 MB.</p> <p>Syntax:</p> <p>LOG_MAXIMUM_FILE_SIZE <i>size</i></p>	4000000	Maximum file size in bytes.
<p>LOG_MEMORY_STATISTICS</p> <p>Controls whether memory statistics are logged in the ncpserv.log file.</p>	0	<p>0 - Disable</p> <p>1 - Enable</p>

Parameter Name and Description	Default Value	Value Options
LOG_TIMESTAMPS	1	0 - Disable 1 - Enable
Enables or disables time stamps for each message. With this parameter turned on, a time stamp is appended to each message.		
Syntax:		
LOG_TIMESTAMPS YES NO		

A.2.5 NCP Communications

Table A-5 Server Parameter Information for Communications

Parameter Name and Description	Default Value	Value Options
FIRST_WATCHDOG_PACKET	0	0 - Disable 1-120(minutes) - Enable
Controls how long to wait in minutes of inactivity before checking to see if an NCP connection is still alive.		
DISABLE_BROADCAST	0	0 - Disable 1 - Enable
Controls the ability to broadcast messages from the NCP Server.		

A.2.6 NCP Server Environment

Table A-6 Server Parameter Information for the NCP Server Environment

Parameter Name and Description	Default Value	Value Options
ALLOW_UTF8	1	0 - Disable 1 - Enable
Controls UTF-8 support for file names. When support for UTF-8 is set to 1, the server informs clients that it supports case 89 NCPs, which use UTF-8 file names. If the value is set to 0, the server informs clients that it does not support case 89 NCPs.		
When ALLOW_UTF8 is enabled, you must also enable UTF8 support in the Novell Client. If you want the server to support clients from different locales (code pages) and allow them to share files, you must use the UTF-8 NCPs.		

Parameter Name and Description	Default Value	Value Options
<p>LOCAL_CODE_PAGE</p> <p>Controls which base code page is used by the NCP Server.</p> <p>This setting defines the local code page used for file and subdirectory names, except for case 89 NCPs that use UTF-8. This value should be set to match the majority of your clients.</p> <p>Syntax:</p> <pre>LOCAL_CODE_PAGE code_page</pre> <p>For example:</p> <pre>LOCAL_CODE_PAGE CP437</pre> <p>You can get the complete list by typing the following command at the linux command line:</p> <pre>iconv - - list more</pre>	CP437	<p>Valid language codes</p> <p>Commonly used values are:</p> <p>CP437 for the standard English character set.</p> <p>CP850 for European character sets.</p> <p>CP932 for Japanese</p> <p>CP949 for Korean</p> <p>CP866 for Russian</p> <p>GBK for simplified Chinese</p> <p>BIG5 for traditional Chinese</p>
<p>NCP_FILE_SERVER_NAME</p> <p>This parameter is set by eDirectory when the NCP Server is installed, and must not be modified arbitrarily.</p> <p>For information, see Section 3.12, "Modifying the NCP File Server Name," on page 42.</p>	Server hostname	This setting must match the server hostname, such as <code>server1</code> .

A.2.7 NCP Volumes

Table A-7 Server Parameter Information for Volume and File Management

Parameter Name and Description	Default Value	Value Options
<p>COMMIT_FILE</p> <p>This parameter assures an NCP client that all data previously written to a file has been written to disk. Because files must be stored on the physical storage medium before certain actions are attempted, this call provides a checkpoint that guarantees that the file has been flushed from cache and written to disk.</p> <p>When this parameter is enabled, it calls the Linux <code>fsync</code> command to flush data from cache and write it to the disk, then it returns success to the calling function.</p> <p>When this parameter is disabled (the default setting), nothing is done, but it returns success to the calling function.</p>	0	<p>0 - Disable</p> <p>1 - Enable</p>

Parameter Name and Description	Default Value	Value Options
<p>EXECUTE_ATTRIBUTE_SUPPORT</p> <p>With this setting turned on, the NCP “execute only” attribute can be associated with the user mode execute bit on a file or subdirectory. With this setting turned on, NCP clients can set or clear this bit.</p> <p>The Novell Client for Linux uses this bit to represent the user mode execute bit on a file or subdirectory.</p>	1	0 - Disable 1 - Enable
<p>KEEP_NSS_FILE_DELETOR_IDS</p> <p>This option is for retaining the deleter ID when a file is deleted on NSS volumes.</p> <p>NCP notifies NSS to provide the identity of the user who initiated the delete. This information is then retained by NSS and available when the file is salvaged, assuming that the Salvage attribute is enabled for the NSS volume when the file is deleted and salvaged.</p>	1	0 - Disable 1 - Enable
<p>SENDFILE_SUPPORT</p> <p>This option allows the NCP Server to send file read data to the client directly from the Linux Kernel Ring 0 environment, rather than copying it to Ring 3 and then back to Ring 0. Turning this option on gives you a slight performance improvement.</p>	0	0 - Disable 1 - Enable
<p>SYNC_TRUSTEES_TO_NSS_AT_VOLUME_MOUNT</p> <p>Controls trustee resynchronization for an NSS volume when it is mounted for NCP.</p>	0	0 - Disable 1 - Enable
<p>VOLUME_GONE_WARN_USERS</p> <p>Controls whether a message is broadcast to warn users when the volume path is no longer present.</p>	1	0 - Disable 1 - Enable

A.2.8 NCP Volumes Low-Space Warning

Table A-8 Server Parameter Information for Volume Low-Space Warning

Parameter Name and Description	Default Value	Value Options
<p>VOLUME_EMPTY_WARN_USERS</p> <p>Controls whether a message is broadcast to warn users when no volume space is available.</p>	1	0 - Disable 1 - Enable
<p>VOLUME_LOW_WARN_USERS</p> <p>Controls whether a message is broadcast to warn users when volume space is low.</p>	1	0 - Disable 1 - Enable
<p>VOLUME_LOW_WARNING_RESET_THRESHOLD</p> <p>Sets the high watermark threshold (in blocks), which is the level where the low watermark threshold is reset, and users no longer receive the low-space message. An NSS block is 4 KB.</p>	128	0 to 100000

Parameter Name and Description	Default Value	Value Options
VOLUME_LOW_WARNING_THRESHOLD	64	0 to 100000
Sets the low watermark threshold (in blocks) that indicates space is low. An NSS block is 4 KB.		

A.3 NCP2NSS Command

```
/opt/novell/ncpserv/sbin/ncp2nss
/etc/init.d/ncp2nss { [re]start|stop|status }
```

A.4 ShadowFS Command

```
rcnovell-shadowfs
/etc/init.d/novell-shadowfs { [re]start|stop|status }
```

A.5 Virtual NCP Server Object Script

The script `/opt/novell/ncs/bin/ncs_ncpserv.py` creates a virtual NCP Server object in Novell eDirectory, and associates it with none, one, or multiple NCP volumes that you specify. Having an NCP Server object makes it easier for clients to access NCP volumes on clusters. You specify the IP address of the cluster resource that you want to use to manage all of the NCP volumes and the shared EVMS volumes and disks where the NCP shares reside. You must bind the NCP Server object to the IP address of that cluster resource.

Issue the command at a terminal console prompt as the `root` user. Novell cluster services must be installed and running.

```
./opt/novell/ncs/bin/ncs_ncpserv.py -c ncp_server_name -i ip_address [-v <volumename | "volumenames"]
```

Replace the `ncp_server_name` with the name you want to use for the virtual NCP server. It can be the same or different than the cluster resource you created when you cluster-enabled the Linux POSIX volume.

Replace `ip_address` with a static IP address for the virtual server. Replace `volumename` with the name of the NCP volumes that you want to assign to this virtual NCP Server object. The virtual NCP Server object is the "NCS:NCP Server" attribute."

If the `-v` option is not specified, all of the NCP volumes that currently exist on the EVMS volume are bound to the IP address. If you enter multiple volume names, use colons to delimit the names and put quotation marks around the list of names. The multiple volume names can be listed by the name (`MY_NNCP_VOL06`) or by the distinguished name

(`cn=CLUS_02_MY_NNCP_VOL06,o=novell`), or any combination of the two methods.

Examples

To include all of the NCP volumes on the cluster resource, enter

```
./ncs_ncpserv.py -c ncp_serv01 -i 10.10.10.45
```

To specify a single NCP volume on the cluster resource, enter

```
./ncs_ncpserv.py -c ncp_serv01 -i 10.10.10.45 -v MY_NNCP_VOL05
```

To specify multiple NCP volumes on the cluster resource, enter

```
./ncs_ncpserv.py -c ncp_server02 -i 10.10.10.46 -v  
"MY_NNCP_VOL06:cn=CG_02_MY_NNCP_VOL07,o=novell"
```

B Additional NCP Server Commands and Options

This section describes NCP Server commands, command line options, and configuration file options that should not be used except under direction from Novell Support.

- ♦ [Section B.1, “Configuration File Options,” on page 163](#)
- ♦ [Section B.2, “NCP2NSS Command Options,” on page 163](#)
- ♦ [Section B.3, “NCPCON Commands and Options,” on page 164](#)
- ♦ [Section B.4, “NCPTOP Command Line Options,” on page 165](#)

B.1 Configuration File Options

The following configuration file options apply to the `ncpcon.conf`, `ncpserv.conf`, and `ncp2nss.conf` configuration files. These files are located in the `/etc/opt/novell/` directory.

`LOG_TIMESTAMPS [Yes|No]`

The default setting is No.

`LOG_MAX_FILE_SIZE size`

Replace *size* with the value in bytes. The default size is 4194304 (4 MB).

B.2 NCP2NSS Command Options

`/opt/novell/ncpserv/sbin/ncp2nss`

The following hidden options apply to the `ncp2nss` command:

`--d`

Used to start the NCP2NSS daemon as a foreground process instead of as a background daemon.

`--h`

Help

B.3 NCPCON Commands and Options

The commands in this section are not included in the general management commands for NCP Server Console utility. You must be logged in as the `root` user to issue the commands.

- ♦ [Section B.3.1, “Hidden Options,” on page 164](#)
- ♦ [Section B.3.2, “Hidden Commands,” on page 164](#)

B.3.1 Hidden Options

The following options are available for `ncpcon` in command line mode. The syntax is

```
ncpcon [option]
```

--@filename

Uses the file for `ncpcon` input processing.

--help

Lists the syntax for command line mode and interactive mode.

--ncpservername

Used with `bind` and `unbind` commands.

--ipaddress

Used with `bind` and `unbind` commands.

--valid

Used with the `mount` command.

B.3.2 Hidden Commands

The commands in this section are used only for diagnostic purposes.

diag

Use this command to display NCP Server diagnostics or `ncp2nss` daemon diagnostics.

Examples:

```
diag
```

```
diag ncp2nss
```

flush volume volume_name

Flushes file system dirty data from the specified volume. You can add the `ncpcon flush volume volume_name` command to a cluster load script.

nss resync=volume_name

Resynchronizes NCP Server and NSS information for the specified volume.

nss verify=volume_name

Verifies NCP Server and NSS information for the specified volume.

B.4 NCPTOP Command Line Options

--d

Outputs logging information to the `/var/opt/novell/log/ncptop.log` file.

--h

Displays help information.

C RPM Files for NCP Server

The following RPM files are installed for NCP (NetWare Core Protocol) Server on Novell Open Enterprise Server (OES) 2 Linux.

novell-ncp.i386.rpm

Contains the NCP Server shared library (`libncpengine.so`) that runs as part of Novell eDirectory. This component handles all client NCP requests.

novell-ncpserv-nrm.i386.rpm

Contains the Novell Remote Manager for Linux plug-in (`libnrm2ncp.so`) provided by the NCP team.

novell-ncpserv.i386.rpm

Contains `ncpcon` and `ncptop` tools to help administrators manage the NCP Server. It also contains daemons that connect the `ncpserv` to other services on the server: `ncp2nss` and `lum2ncp`.

novell-nrm.i386

Contains `httpstkd` and the shared library (`libnrm.so`) that creates Novell Remote Manager for Linux as an `httpstk` plug-in. It also contains other files used by Novell Remote Manager.

D Documentation Updates

This section contains information about documentation content changes made to the *OES 2: NCP Server for Linux Administration Guide* since the initial release of Novell Open Enterprise Server 2. If you are an existing user, review the change entries to readily identify modified content. If you are a new user, simply read the guide in its current state.

Refer to the publication date, which appears on the title page, to determine the release date of this guide. For the most recent version of the *OES 2: NCP Server for Linux Administration Guide*, see the [OES 2 documentation Web site \(http://www.novell.com/documentation/oes2/novell-client-access.html#ncp-srvr\)](http://www.novell.com/documentation/oes2/novell-client-access.html#ncp-srvr).

In this section, content changes appear in reverse chronological order, according to the publication date. Within a dated entry, changes are grouped chapter and sequenced alphabetically. Each change entry provides a link to the related topic and a brief description of the change.

This document was updated on the following dates:

- ♦ [Section D.1, “May 2013,” on page 169](#)
- ♦ [Section D.2, “April 2013,” on page 170](#)
- ♦ [Section D.3, “January 2013,” on page 170](#)
- ♦ [Section D.4, “September 2011,” on page 170](#)
- ♦ [Section D.5, “January, 2011,” on page 170](#)
- ♦ [Section D.6, “December, 2010,” on page 170](#)
- ♦ [Section D.7, “January 27, 2009,” on page 170](#)
- ♦ [Section D.8, “December 15, 2009,” on page 170](#)
- ♦ [Section D.9, “October 27, 2009,” on page 171](#)
- ♦ [Section D.10, “July 16, 2009,” on page 171](#)
- ♦ [Section D.11, “June 11, 2009,” on page 172](#)
- ♦ [Section D.12, “February 13, 2009,” on page 172](#)
- ♦ [Section D.13, “January 5, 2009,” on page 173](#)
- ♦ [Section D.14, “December 2008 \(OES 2 SP1 Linux\),” on page 173](#)
- ♦ [Section D.15, “May 5, 2008,” on page 176](#)
- ♦ [Section D.16, “February 12, 2008,” on page 178](#)

D.1 May 2013

- ♦ Updated [Chapter 2, “What’s New for NCP Server for Linux,” on page 15](#).
- ♦ Update [Section 3.1.12, “SLP,” on page 24](#) with details.

D.2 April 2013

- ♦ Updated [Chapter 2, “What’s New for NCP Server for Linux,”](#) on page 15.

D.3 January 2013

- ♦ Updated [Section 16.2, “Soft Links,”](#) on page 131 with details.

D.4 September 2011

- ♦ Updated the [What’s New for NCP Server for Linux](#) chapter with details of August patch.

D.5 January, 2011

Added new options to manage NCP threads. For more information, see [Section A.1.6, “Managing NCP Threads,”](#) on page 138.

D.6 December, 2010

- ♦ Updated [Commands and Utilities for NCP Server and NCP Volumes](#) with information to enable and disable write permissions on volumes.
- ♦ Modified [Section 3.4.1, “Directory Cache Management for NCP Server,”](#) on page 30 for the default values of `MAXIMUM_CACHED_FILES_PER_SUBDIRECTORY`, `MAXIMUM_CACHED_FILES_PER_VOLUME`, and `MAXIMUM_CACHED_SUBDIRECTORIES_PER_VOLUME`.
- ♦ Added [Section 15.4, “Error on Copying or Deleting Files When Extended Attributes Are Not Enabled,”](#) on page 130.
- ♦ Modified [Section 3.11, “Configuring Cross-Protocol File Locks for NCP Server,”](#) on page 40 and [Section A.2.3, “Locks Management for File Access on NCP Server,”](#) on page 156.

D.7 January 27, 2009

- ♦ Removed link to information stopping and starting `ndsd` when you are running multiple instances of it on the same server. This statement is removed as multiple instances are not supported on OES2.

D.8 December 15, 2009

- ♦ Updated [Chapter 2, “What’s New for NCP Server for Linux,”](#) on page 15
- ♦ Removed instances of AFP requiring Samba to access CPL.
- ♦ Updated [Chapter 3, “Installing and Configuring NCP Server for Linux,”](#) on page 21 to indicate that now you can concurrently run applications from Samba clients, Novell AFP clients, Novell CIFS clients, and NCP clients.

D.9 October 27, 2009

- ♦ [Section 2.10.4, “Novell AFP Supports Cross-Protocol File Locking with NCP for NSS Volumes,” on page 18](#) is updated with CPL being enabled by default in OES2 SP2 and the following note:

NOTE: For better performance, disable CPL if you do not use any other access protocol.

- ♦ [Section 3.11, “Configuring Cross-Protocol File Locks for NCP Server,” on page 40](#) is updated with CPL being enabled by default and the following note:

NOTE: For better performance, disable CPL if you are not using any other access protocol.

- ♦ [Section A.2.3, “Locks Management for File Access on NCP Server,” on page 156](#) is updated with CPL default value as 1.

D.10 July 16, 2009

Updates were made to the following sections. The changes are explained below.

- ♦ [Section D.10.1, “Configuring NCP Volumes with Novell Cluster Services,” on page 171](#)
- ♦ [Section D.10.2, “Managing NCP Volumes,” on page 171](#)
- ♦ [Section D.10.3, “Managing NSS Volumes in a Cluster,” on page 171](#)

D.10.1 Configuring NCP Volumes with Novell Cluster Services

Location	Change
Chapter 11, “Configuring NCP Volumes with Novell Cluster Services,” on page 97	Modified the load script.

D.10.2 Managing NCP Volumes

Location	Change
Section A.1.7, “Managing NCP Volumes,” on page 140	Modified the syntax to use ",PATH=" instead of "@" in the syntax and example lines.

D.10.3 Managing NSS Volumes in a Cluster

Location	Change
Section A.1.9, “Managing NSS Volumes in a Cluster,” on page 144	Added a section on updating the load script to mount NSS volumes.

D.11 June 11, 2009

Updates were made to the following sections. The changes are explained below.

- ♦ [Section D.11.1, “NCP Communications,” on page 172](#)

D.11.1 NCP Communications

Location	Change
Section A.2.5, “NCP Communications,” on page 158 and Section 3.4.5, “NCP Communications,” on page 33	Modified the value options for FIRST_WATCHDOG_PACKET. Earlier the value option was specified as 1. You can specify a value between 1-120 minutes.

D.12 February 13, 2009

Updates were made to the following sections. The changes are explained below.

- ♦ [Section D.12.1, “Commands and Utilities for NCP Server and NCP Volumes,” on page 172](#)
- ♦ [Section D.12.2, “Using Opportunistic Locking for NCP File Handling,” on page 172](#)

D.12.1 Commands and Utilities for NCP Server and NCP Volumes

Location	Change
Section A.2.7, “NCP Volumes,” on page 159	Added a description for the KEEP_NSS_FILE_DELETOR_IDS parameter and the COMMIT_FILE parameter.

D.12.2 Using Opportunistic Locking for NCP File Handling

Location	Change
Section 13.1, “Understanding Opportunistic Locking for NCP Connections,” on page 117	WARNING: Level 2 OpLocks are inappropriate for server-side database applications: Do not use OpLock Level 2 with databases. Level 1 OpLocks can remain switched on.
Section 13.4, “Configuring OpLocks for NSS Volumes,” on page 120	This section is new.

D.13 January 5, 2009

Updates were made to the following sections. The changes are explained below.

- ♦ [Section D.13.1, “Commands and Utilities for NCP Server and NCP Volumes,”](#) on page 173
- ♦ [Section D.13.2, “Configuring NCP Volumes with Novell Cluster Services,”](#) on page 173
- ♦ [Section D.13.3, “Managing NCP Volumes,”](#) on page 173

D.13.1 Commands and Utilities for NCP Server and NCP Volumes

Location	Change
Section A.1.7, “Managing NCP Volumes,” on page 140	The <code>ncpcon change volume</code> command cannot be added to a cluster load script.

D.13.2 Configuring NCP Volumes with Novell Cluster Services

Location	Change
Step 1e in Section 11.2.3, “Creating a Shared NCP Volume on the Linux POSIX Cluster Resource,” on page 101	Added information about configuring Inherit POSIX Permissions for a clustered NCP volume.

D.13.3 Managing NCP Volumes

Location	Change
Section 10.8, “Configuring Inherit POSIX Permissions for an NCP Volume,” on page 89	Added information about configuring Inherit POSIX Permissions for a clustered NCP volume.

D.14 December 2008 (OES 2 SP1 Linux)

Updates were made to the following sections. The changes are explained below.

- ♦ [Section D.14.1, “Commands and Utilities for NCP Server and NCP Volumes,”](#) on page 174
- ♦ [Section D.14.2, “Installing and Configuring NCP Server,”](#) on page 174
- ♦ [Section D.14.3, “Managing Connections for NCP Volumes and NSS Volumes,”](#) on page 175
- ♦ [Section D.14.4, “Managing NCP Volumes,”](#) on page 175
- ♦ [Section D.14.5, “Planning for NCP Server and NCP Volumes,”](#) on page 175
- ♦ [Section D.14.6, “Troubleshooting for NCP Server and NCP Volumes,”](#) on page 175

- ♦ [Section D.14.7, “Using NCP Server and NCP Volumes in a Virtualization Environment,”](#) on page 176
- ♦ [Section D.14.8, “What’s New for NCP Server for Linux,”](#) on page 176

D.14.1 Commands and Utilities for NCP Server and NCP Volumes

Location	Change
Section A.1.5, “Managing NCP Server in a Cluster,” on page 138	SLP is required to be installed and running when using the <code>ncpcon bind</code> and <code>ncpcon unbind</code> commands.
Section A.1.7, “Managing NCP Volumes,” on page 140	An equal sign (=) is no longer used in the <code>ncpcon change volume</code> command to set the Inherit POSIX Permissions parameter for an NCP volume. Added information for the <code>volume data</code> command.
Section A.2.3, “Locks Management for File Access on NCP Server,” on page 156	Beginning OES 2 SP1 Linux, Novell Apple Filing Protocol (AFP) uses Linux Samba to take advantage of the NCP cross-protocol file locking protection for its Macintosh users for NSS volumes. Users can access data with NCP clients, Samba clients, and AFP clients.
Section A.5, “Virtual NCP Server Object Script,” on page 161	This feature is new for OES 2 SP1 Linux.

D.14.2 Installing and Configuring NCP Server

Location	Change
Section 3.1.4, “64-Bit Support,” on page 22	This section is new.
Section 3.1.10, “Novell AFP,” on page 24	This section is new.
Section 3.1.12, “SLP,” on page 24	This section is new.
Section 3.3, “Updating NCP Server,” on page 28	This section is new.
Section 3.11, “Configuring Cross-Protocol File Locks for NCP Server,” on page 40	NCP Server for Linux provides cross-protocol locking for NCP and Linux Samba. Beginning OES 2 SP1 Linux, Novell Apple Filing Protocol (AFP) uses Linux Samba to take advantage of the NCP cross-protocol file locking protection for its Macintosh users for NSS volumes. Users can access data on NSS volumes with NCP clients, Samba/CIFS clients, and AFP clients. In OES 2 SP2 Linux and later, Novell CIFS supports cross-protocol file locking with NCP and Novell AFP when the NCP Cross-Protocol File Locking parameter is enabled.

Location	Change
Section 3.4.3, "Locks Management for File Access on NCP Server," on page 32	Beginning OES 2 SP1 Linux, Novell Apple Filing Protocol (AFP) uses Linux Samba to take advantage of the NCP cross-protocol file locking protection for its Macintosh users for NSS volumes. Users can access data on NSS volumes with NCP clients, Samba/CIFS clients, and AFP clients.

D.14.3 Managing Connections for NCP Volumes and NSS Volumes

Location	Change
Section 9.3.1, "Enabling or Disabling Broadcast Message Support," on page 71	This section is new.
Section 9.3.4, "Configuring the Novell Client for Sending and Receiving Messages," on page 72	This section is new.

D.14.4 Managing NCP Volumes

Location	Change
Section 10.8, "Configuring Inherit POSIX Permissions for an NCP Volume," on page 89	An equal sign (=) is no longer used in the <code>ncpcon change volume</code> command to set the Inherit POSIX Permissions parameter for an NCP volume.

D.14.5 Planning for NCP Server and NCP Volumes

Location	Change
Section 6.4, "User Quotas on Linux POSIX File Systems," on page 52	This section is new.

D.14.6 Troubleshooting for NCP Server and NCP Volumes

Location	Change
Section 15.2, "Error -601 When Deleting an NCP Volume," on page 129	This section is new.
Section 15.3, "Cross-Protocol Locking Stops Working," on page 129	This section is new.

D.14.7 Using NCP Server and NCP Volumes in a Virtualization Environment

Links to external references were updated.

D.14.8 What's New for NCP Server for Linux

Location	Change
Section 2.10, "What's New (OES 2 SP1)," on page 18	This section is new.

D.15 May 5, 2008

Updates were made to the following sections. The changes are explained below.

- ♦ [Section D.15.1, "Commands and Utilities for NCP Server and NCP Volumes," on page 176](#)
- ♦ [Section D.15.2, "Configuring NCP Volumes for Novell Cluster Services Clusters," on page 176](#)
- ♦ [Section D.15.3, "Managing NCP Volumes," on page 177](#)
- ♦ [Section D.15.4, "Using Opportunistic Locking for NCP File Handling," on page 177](#)

D.15.1 Commands and Utilities for NCP Server and NCP Volumes

Location	Change
"Command Line Mode" on page 136	You must escape quote characters when using <code>ncpcon</code> to issue commands at the console command prompt.
Section A.1.7, "Managing NCP Volumes," on page 140	Corrected errors in the syntax for the <code>mount</code> command and the <code>change volume</code> command.

D.15.2 Configuring NCP Volumes for Novell Cluster Services Clusters

Location	Change
Section 11.2.4, "Creating a Virtual NCP Server Object for Shared NCP Volumes," on page 104	Corrected a misspelled option in Step 2: <code>--ncpservname</code>
Section 11.2.3, "Creating a Shared NCP Volume on the Linux POSIX Cluster Resource," on page 101	Updated the procedure.

Location	Change
Section 11.2.5, "Modifying the Load Script for the Linux POSIX Cluster Resource," on page 106	Corrected syntax errors in the examples as follows: <pre>exit_on_error ncpcon mount volumename=valid@/volumepath exit_on_error ncpcon mount USERS=254@/media/ncpvolumes/USERS</pre>
Section 11.3.1, "Sample Load Script for an NCP Volume Cluster Resource," on page 108	Updated the script.
Section 11.3.2, "Sample Unload Script for an NCP Volume Cluster Resource," on page 109	Updated the script.
Section 11.3.3, "Sample Monitor Script for an NCP Volume Cluster Resource," on page 110	This section is new.

D.15.3 Managing NCP Volumes

Location	Change
Section 10.8, "Configuring Inherit POSIX Permissions for an NCP Volume," on page 89	Corrected the syntax for using the <code>ncpcon change volume</code> command to set the Inherit POSIX Permissions parameter for an NCP volume.

D.15.4 Using Opportunistic Locking for NCP File Handling

Location	Change
Section 13.2, "Configuring OpLocks for NCP Server," on page 119	After changing the Opportunistic Lock (oplock) level in <code>/etc/opt/novell/ncpserv.conf</code> , you must restart <code>ndsd</code> to apply the changes. Open a terminal console as the <code>root</code> user, then enter <pre>rcndsd restart</pre>

D.16 February 12, 2008

Updates were made to the following section. The changes are explained below.

- ♦ [Section D.16.1, “Configuring NCP Volumes for Novell Cluster Services Clusters,”](#) on page 178

D.16.1 Configuring NCP Volumes for Novell Cluster Services Clusters

Location	Change
Section 11.2, “Clustering an NCP Volume on a Linux POSIX File System,” on page 99	<p>The syntax for the mount and dismount commands has been corrected. The general format for a load script is:</p> <pre>exit_on_error ncpcon mount <i>VOLUMENAME</i> volid=200@/mnt/ mountpoint</pre> <p>The general format for an unload script is:</p> <pre>exit_on_error ncpcon dismount <i>VOLUMENAME</i></pre>
Section 11.2.4, “Creating a Virtual NCP Server Object for Shared NCP Volumes,” on page 104	This section is new.