AUTHORIZED DOCUMENTATION

AFP, CIFS, and NFS (Native File Access Protocols) Administration Guide

Novell®
NetWare®

6.5 SP8

November 9, 2009

www.novell.com

Legal Notices

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

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

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

Copyright © 2005–2009 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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

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

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

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide 11

1 Overview 13

1.1 Native File Access Protocols and the Universal Password . . . 14
1.2 What's Next . . . 14

2 What's New 15

3 Installing Novell Native File Access Protocols on a NetWare 6.5 Server 17

3.1 Preparing for CIFS and AFP . . . 17
3.2 Administrator Workstation Prerequisites . . . 18
3.3 Client Computer Prerequisites . . . 19
3.4 Starting and Stopping AFP and CIFS Protocols . . . 19
3.5 What's Next . . . 20

4 Working with Macintosh Computers 21

4.1 Administrator Tasks for Native File Access for Macintosh Services . . . 21
4.1.1 Creating Simple Passwords for Several Macintosh Users . . . 21
4.1.2 Enabling and Disabling AFP . . . 22
4.1.3 Enabling and Disabling Delete Inhibit Emulation . . . 22
4.1.4 Editing the Context Search File . . . 22
4.1.5 Creating a Guest User Account . . . 23
4.1.6 Renaming Volumes . . . 23
4.1.7 AFP Console Commands . . . 24
4.2 Macintosh End User Tasks . . . 26
4.2.1 Accessing Network Files . . . 26
4.2.2 Logging In to the Network As Guest . . . 26
4.2.3 Changing Passwords from a Macintosh Computer . . . 27
4.2.4 Assigning Rights and Sharing Files from a Macintosh Computer . . . 27
4.3 Troubleshooting Native File Access for Macintosh . . . 29
4.3.1 Three Grace Logins Required on Universal Password Expiration . . . 29
4.3.2 AppleTalk Not Supported As a Transport Protocol . . . 30
4.3.3 Mac OS 8.x Will Not Mount Volumes Checked to Mount at Startup . . . 30
4.3.4 Unloading Afptcp.nlm and Wspdsi.nlm Programs . . . 30
4.3.5 Traditional Volume Access Not Supported . . . 30

5 Working with Windows Computers 31

5.1 Administrator Tasks for Native File Access for Windows Services . . . 31
5.1.1 Creating Simple Passwords for Windows Users . . . 31
5.1.2 Two Methods for Creating Simple Passwords for Windows Users . . . 33
5.1.3 Enabling Users to Change Their Simple Passwords with iManager . . . 34
5.1.4 Understanding Synchronization of NetWare Passwords and Simple Passwords . . . 35
5.1.5 Specifying Contexts in the Context Search File . . . 35
5.1.6 Managing Network Access with ConsoleOne . . . 36
5.1.7 Providing Network Access to Domain Users . . . 36
5.1.8 Enabling and Disabling CIFS . . . 36

5.1.9 Enabling and Disabling SMB Signing . . . 37
5.1.10 Changing CIFS Configuration . . . 38
5.1.11 Viewing Configuration Details . . . 40
5.2 Windows End User Tasks . . . 40
5.2.1 Accessing Files from a Windows Computer . . . 40
5.2.2 Mapping Drives from a Windows Computer . . . 41
5.3 Troubleshooting Native File Access for Windows . . . 41
5.3.1 Workstations Unable to Access a Windows 2000 Primary Domain Controller . . . 42
5.3.2 PDC and CIFS on Different Subnets . . . 42
5.3.3 Password Changes . . . 42
5.3.4 CIFS Server Not Visible in Network Neighborhood . . . 42
5.3.5 Traditional Volume Access Not Supported . . . 42
5.3.6 Virtual Server Restart Required after Stopping and Restarting CIFS . . . 43
5.3.7 Trustee Rights Required to CIFS Virtual Server . . . 43

6 Setting Up Novell Native File Access Protocols in a NetWare 6.5 Cluster 45

6.1 Prerequisites . . . 45
6.2 Setting Up for Macintosh . . . 46
6.3 Setting Up for Windows . . . 46
6.4 What's Next . . . 47

7 Working with UNIX Machines 49

7.1 Features of Native File Access for UNIX . . . 49
7.2 Overview of Native File Access for UNIX . . . 51
7.3 Prerequisites . . . 51
7.4 NFS Server . . . 52
7.4.1 Making NetWare File System Available to NFS Clients . . . 52
7.4.2 Accessing the NetWare File System from UNIX NFS Clients . . . 53
7.4.3 File Access Modes . . . 53
7.4.4 NFS Server File Lock Manager . . . 59
7.5 Network Information Service . . . 60
7.5.1 NIS Information in eDirectory . . . 61
7.5.2 Various NIS Configurations . . . 63
7.5.3 UNIX User Management with eDirectory . . . 64
7.6 User and Group Information . . . 64
7.6.1 UNIX Users and Groups . . . 64
7.6.2 UNIX Usernames, Group Names, and ID Numbers . . . 65
7.6.3 User Home Directories . . . 65
7.6.4 User Preferred Shells . . . 65
7.6.5 Handling UNIX User Passwords . . . 65
7.7 ConsoleOne Administration . . . 65
7.8 Administration Utilities . . . 66
7.8.1 SCHINST . . . 66
7.8.2 NISINST . . . 66
7.8.3 Manually Executing Administrative Utilities . . . 67
7.9 Upgrade Utility . . . 67
7.9.1 Upgrading Export Files from NetWare 5.1 / NetWare 6 . . . 67
7.10 Refreshing the Cache to update UNIX Profile . . . 68
7.11 Configuring and Managing Native File Access for UNIX . . . 68
7.11.1 Configuration Methods . . . 68
7.12 Configuring Server General Parameters . . . 69
7.12.1 File-Based Configuration of Server General Parameters . . . 70
7.12.2 ConsoleOne Configuration of Server General Parameters . . . 70
7.13 Migrating NIS Maps . . . 72

7.13.1 File-Based Migration . . . 73
7.13.2 ConsoleOne Migration . . . 74
7.13.3 Managing Users and Groups . . . 77
7.14 Managing NFS Server . . . 79
7.14.1 Starting and Stopping NFS Server . . . 80
7.14.2 NFS Server Load Time Options . . . 80
7.14.3 NFS Server Console Commands . . . 80
7.14.4 Export Options . . . 81
7.14.5 Managing NFS Server Using iManager . . . 84
7.14.6 Administering NFS Server . . . 85
7.14.7 Managing the Exported Paths . . . 86
7.14.8 Exporting a New Path . . . 87
7.14.9 Editing Exported Path Properties . . . 89
7.15 Managing NIS Server . . . 89
7.15.1 iManager-Based Management for NIS Server . . . 89
7.15.2 File-Based Management for NIS Server . . . 95
7.15.3 ConsoleOne Management for NIS Server . . . 98
7.16 Cluster-Enabling Native File Access for UNIX . . . 113
7.16.1 Prerequisite . . . 114
7.16.2 Cluster-Enabling Native File Access for UNIX . . . 114
7.16.3 Upgrading Cluster-Enabled Native File Access for UNIX . . . 117
7.16.4 Component-Specific Configuration . . . 118
7.17 Interoperability . . . 118
7.18 Performance Tuning . . . 119
7.18.1 Performance Testing . . . 119

8 Primary Domain Controllers on NetWare 121

8.1 Requirements . . . 121
8.2 Installing PDC on NetWare Software . . . 122
8.3 Configuring PDCs on NetWare Servers . . . 122
8.3.1 Creating a PDC on a NetWare CIFS Server . . . 122
8.3.2 Adding Servers to the Domain . . . 124
8.3.3 Adding a Network Attached Storage Filer to the Domain . . . 124
8.3.4 Adding an Access Control List for the Domain . . . 125
8.4 Managing PDCs on NetWare Servers . . . 125
8.4.1 Removing Servers from the Domain . . . 125
8.4.2 Deleting Domains . . . 126
8.4.3 Promoting BDCs to PDCs . . . 126
8.4.4 Getting Domain Information . . . 127
8.5 Creating Login Scripts for Domain Users . . . 127

A System Messages 129

A.1 NFS Server . . . 129
A.2 MakeNIS . . . 130
A.3 NIS Installation . . . 131
A.4 NIS Services . . . 131
A.5 Yppasswd . . . 132

B NFAU Known Issues 135

B.1 UNIX/NFS Issues . . . 135

C Native File Access for UNIX FAQs 137

C.1 General FAQs . . . 137
C.1.1 When upgrading to NetWare 6.5 from NetWare 5.1 / NetWare 6.0, I am receiving a file overwrite warning for nfsstart.ncf. What should I do? . . . 137
C.1.2 NFS Server is not loading on a server in tree with NetWare 5.1 NDS 7 replica ring. How can I resolve this? . . . 138
C.1.3 When I try to load NFS Services using Ndsilib.nlm, -669 error displays on the logger screen. How can I resolve this? . . . 138
C.1.4 When the administrator changes the UNIX profile of the user, the updated profiles are not cached immediately. How can the profile be updated immediately? . . . 138
C.1.5 What is the significance of the SEARCH_ROOT parameter in SYS:ETC\NFS.CFG file? . . . 138
C.1.6 How do I manually set the UNIX profile of a user? . . . 138
C.1.7 How do I set a User's UNIX profile to the Root's profile? . . . 139
C.1.8 Could not authenticate ContextHandle. Load schinst and try again. Exiting...9601 139
C.1.9 When I execute nfsstart after reinstalling the directory services in the server or joining the server to an existing tree or deleting the NFAUUser object, messages such as "Error unloading, killed loaded module (ndsilib.nlm)", or "Unable to Login.: error -669 Could not authenticate ContextHandle. Load schinst and try again. Exiting...-669" display. What should I do? . . . 139
C.1.10 While executing the SCHINST -n, what does the message "Error: Unable to login. Error Code: 35076" imply? This is displaying even when the Schema is fine and nfauuser object has been recreated. . . . 140
C.1.11 During nfsstop, ndsilib.nlm does not get unloaded and it displays a message showing dependency on nwftpd. . . . 140
C.2 NFS Server FAQs . . . 140
C.2.1 Where can I view / modify the NFS attributes of a file apart from a UNIX client? . . . 141
C.2.2 When using NetWare mode, why does the NetWare owner change for directories not reflect right away on UNIX client? . . . 141
C.2.3 What can I do when the mount point of a previously exported path is active even after the path is removed from exports file? . . . 142
C.2.4 What is the difference in the export options /pathname -ro -root and /pathname -ro -anon? . . . 142
C.2.5 What is the result of specifying only -ro as the export option? . . . 142
C.2.6 I'm trying to export a traditional volume using NFS Server, but it fails to mount on an NFS Client even though showmount shows the export. Why? . . . 142
C.2.7 I am using IBM AIX 4.3 NFS client and am facing issues in simultaneous acquiring and releasing of locks over the same region of a file from two different processes. Can I avoid them? . . . 142
C.2.8 While upgrading the iManager snap-ins from iManager configuration, the message "This package has an earlier version than the module that is currently installed. Installation has been cancelled." displays. How can I resolve this? . . . 142
C.2.9 I unable to export a non-English path if I use Notepad on Windows to modify the exports file. How can I resolve this? . . . 143
C.2.10 Does NFS Server support exports for directories with spaces in the name? . . . 143
C.2.11 The non-root user is unable to create files in mounted directory that is exported as rw without root access. Can this be resolved? . . . 143
C.2.12 File operations are failing when NDS_ACCESS is set to 0 in etc\nfs.cfg. Can this be resolved? . . . 143
C.2.13 Is there a tool or a utility using which I can view the user and group attributes? . . . 143
C.2.14 Why are the mount points inaccessible after upgrading from NetWare 6.5 (FCS, Support Pack 1, or 2) to OES NetWare? . . . 143
C.2.15 Why do the file permissions change when it is updated from a mapped drive from Windows client? . . . 144
C.2.16 How do i enable hard link support after applying OES NetWare SP2(NetWare 6.5 SP4) . . . 144
C.2.17 Issues with initializing XNFS after upgrading NetWare from SP7 to SP8 . . . 144
C.3 NIS Services FAQs . . . 144

C.3.1 Why does the Solaris NIS Clients to NetWare NIS Server have problems? How can it be resolved? . . . 145
C.3.2 When is the NISSERV_ *ServerName* object created and what is its role in NIS functionality? . . . 145
C.3.3 When I select the properties of the NISSERVER object, an error message displays. What should I do? . . . 145
C.3.4 I am unable to migrate or create a domain using makenis? What do I need to do? 145
C.3.5 I am unable to change the password from a UNIX machine for a migrated user. What do I need to do? . . . 146
C.3.6 What is the 0_ *2* user object that is automatically and randomly created when installing two servers in to the same NDS tree? . . . 146
C.3.7 I am viewing a series of messages such as "Nullpointer passed to routine Kmutex" when running makenis? How can this be resolved? . . . 146
C.3.8 What are the ways to view the list of domains served by the nisServer object? . . . 146

D Documentation Updates 147

D.1 November 9, 2009 . . . 147
D.2 June, 2009 . . . 147
D.3 December, 2008 . . . 147
D.4 October, 2006 (NetWare 6.5 Support Pack 6) . . . 147

About This Guide

This guide contains information on installing, configuring, and managing Novell® Native File Access Protocols software specific to the Windows* and Macintosh* native protocols—CIFS and AFP, respectively.

This guide is divided into the following sections:

- Chapter 1, “Overview,” on page 13.
- Chapter 2, “What's New,” on page 15.
- Chapter 3, “Installing Novell Native File Access Protocols on a NetWare 6.5 Server,” on page 17.
- Chapter 4, “Working with Macintosh Computers,” on page 21.
- Chapter 5, “Working with Windows Computers,” on page 31.
- Chapter 6, “Setting Up Novell Native File Access Protocols in a NetWare 6.5 Cluster,” on page 45.
- Chapter 7, “Working with UNIX Machines,” on page 49.
- Chapter 8, “Primary Domain Controllers on NetWare,” on page 121
- Appendix A, “System Messages,” on page 129.
- Appendix B, “NFAU Known Issues,” on page 135.
- Appendix C, “Native File Access for UNIX FAQs,” on page 137.

Audience

This Guide is intended for NetWare administrators who want to use Native File Access Protocols software specific to Windows*, Macintosh*, and UNIX.

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 Novell Documentation Web site (http://www.novell.com/documentation/feedback.html) and enter your comments there.

Documentation Updates

The most recent version of the *NW6.5 SP8: AFP, CIFS, and NFS (Native File Access Protocols) Administration Guide* is available on the NetWare 6.5 SP8 Documentation Web site (http://www.novell.com/documentation/nw65).

Additional Documentation

For documentation on CIFS on Linux, see *OES 2 SP2: Novell CIFS for Linux Administration Guide*.

Documentation Conventions

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

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

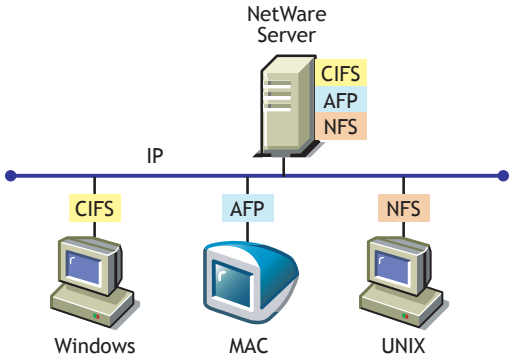
When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as UNIX *, should use forward slashes as required by your software.

Overview

1

Novell® Native File Access Protocols lets Macintosh, Windows, and UNIX workstations access and store files on NetWare® servers without having to install any additional software, such as the Novell Client™. The software is installed only on the NetWare server and provides "out of the box" network access. Just connect the network cable, start the computer, and you have access to servers on your network. No client software installation or configuration is required.

Novell Native File Access Protocols software enables the NetWare server to use the same protocol (referred to as *native*) as the client workstation to copy, delete, move, save, and open files. Windows workstations perform these tasks using the native Common Internet File System (CIFS) protocol, Macintosh workstations use the native Apple* Filing Protocol (AFP), and UNIX computers use the Network File System (NFS) protocol.



Enabling native protocols on a NetWare server means that users can access files on the network, map network drives, and create shortcuts to NetWare servers using the native methods available in their specific operating system. Windows users can use their familiar Network Neighborhood (or My Network Places). Macintosh users can use Chooser or the Go menu to access network files and even create aliases. Because the NetWare server is running native protocols, users can copy, delete, move, save, and open network files—just like they would if they were working locally.

By consolidating user management through Novell ® eDirectory®, Native File Access Protocols simplifies overall network administration. All users who need access to the network are represented in eDirectory through User objects, which enables you to easily and effectively assign trustee rights, control access, and manage all User objects from a single location on the network.

NOTE: Windows users can also be managed through a Windows Domain Controller and UNIX users can be managed through Network Information Service (NIS).

- Section 1.1, “Native File Access Protocols and the Universal Password,” on page 14
- Section 1.2, “What's Next,” on page 14

1.1 Native File Access Protocols and the Universal Password

Universal password is included in NetWare 6.5 which eliminates the need for simple passwords and removes problems that previously existed with password synchronization. The universal password is not enabled by default. If you enable the universal password, the simple password that was required for Native File Access Protocols in previous releases is no longer necessary. With the universal password feature disabled, simple passwords are still required. To learn more about universal password, including how to enable it, see Deploying Universal Password in the *Novell Password Administration Guide*.

1.2 What's Next

Novell Native File Access Protocols are installed by default with NetWare 6.5. To get started, continue with Chapter 3, “Installing Novell Native File Access Protocols on a NetWare 6.5 Server,” on page 17.

What's New

2

There are no feature changes in this release of Novell Native File Access Protocols.

Installing Novell Native File Access Protocols on a NetWare 6.5 Server

3

The Novell® Native File Access Protocols (NFAP) are currently installed and configured to default settings automatically when you install your NetWare 6.5 server.

NOTE: The NetWare 6.5 Customized Installation option includes a Refresh Native File Access Login Methods check box. The purpose of the check box is to provide support for the migration tool that backs up an eDirectory tree, moves an existing server to new hardware, installs a new OS, then restores the previous tree. It is only necessary to select this, if you want to reinstall NFAP login methods during a NetWare server migration.

Additional information and requirements for managing and accessing NetWare 6.5 servers running the Novell Native File Access Protocols include:

- Section 3.1, “Preparing for CIFS and AFP,” on page 17
- Section 3.2, “Administrator Workstation Prerequisites,” on page 18
- Section 3.3, “Client Computer Prerequisites,” on page 19
- Section 3.4, “Starting and Stopping AFP and CIFS Protocols,” on page 19
- Section 3.5, “What's Next,” on page 20

3.1 Preparing for CIFS and AFP

Three key products have interdependencies that must be considered when properly preparing your network to implement Native File Access Protocols for both CIFS and AFP users. The three products are CIFS/AFP, NMAS™, and NICI. CIFS and AFP depend on Novell Modular Authentication Services™ (NMAS) for name resolution and authentication of NFAP users. NMAS is dependent on NICI for encryption/decryption services. A problem with any of these three products will cause CIFS/AFP users to be denied access to a Novell Netware server.

To properly configure CIFS and AFP, you should

1. Read Deploying Universal Password (http://www.novell.com/documentation/password_management32/pwm_administration/data/allq21t.html) in the *Novell Password Management Administration Guide*.

   Novell Netware 6.5 introduces the option to implement a new Universal Password, which replaces the use of the simple password previously required for NMAS authentication. The Universal Password includes the ability to create password policies and removes the need to maintain two separate passwords for NFAP users.

2. Ensure that the `sys:\system\nici\nicisdi.key` file (Tree Key) on every NMAS server in the tree is synchronized with the key domain server.

We recommend that not only servers running NMAS, but also all network servers have matching (synchronized) tree keys. See Deploying Universal Password (http://www.novell.com/documentation/password_management32/pwm_administration/data/allq21t.html) in the *Novell Password Management Administration Guide* for instructions on how to prepare your NICI environment.

3. Ensure that NMAS is installed on or added to a NetWare 6.5 server that has a read/write eDirectory replica of the eDirectory partition where the user objects reside.

   NMAS is included with NetWare 6.5 and is automatically installed with NFAP. It can be added to NetWare 5.1 with eDirectory 8.7.3 or later. For more information on NMAS, see the *NMAS 3.2 Administration Guide* (http://www.novell.com/documentation/nmas32/admin/index.html?page=/documentation/nmas32/admin/data/a20gkue.html).

3.2 Administrator Workstation Prerequisites

Changing the default configuration settings and managing Novell Native File Access services can be done using either iManager or ConsoleOne. iManager requires that you use a supported browser. See "Browsers" in the *Novell iManager 2.7 Installation Guide*.

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

The following table provides compatibility information between the source and target protocols needed to use iManager in a heterogeneous environment. A protocol annotated with an asterisk is the default and is configured automatically. Where available, CIFS must be configured before you can use it; additional CIFS setup requirements are noted, if required.

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

ConsoleOne administration must be done from a Windows-based Administrator workstation. Make sure that the workstation meets the following system requirements.

- ❑ Windows workstation running one of the following:
  - Windows 95/98 running Novell Client™ for Windows 95/98 version 3.21.0 or later
  - Windows NT/2000/XP running Novell Client for Windows NT/2000/XP version 4.80 or later

  Download Novell Client software (http://download.novell.com).
- ❑ Client NICI 2.6.5 (or later) for Windows (Strong Encryption) installed

  Download the NICI Encryption Module software (http://download.novell.com).

  The NICI client software must be installed on the Administrator Workstation in order to manage passwords using ConsoleOne®. NICI software must be installed only on the Administrator Workstation, not on any other client computers.

  NOTE: NICI (Weak Encryption) works for user authentication but does not support changing passwords from a Windows workstation.

3.3 Client Computer Prerequisites

To access NetWare servers running Novell Native File Access Protocols, client computers must be connected to the network, properly configured to run TCP/IP, and be running one of the following operating systems:

- Mac OS version 8.1 or later or Mac OS X
- Windows 95/98/ME, Windows 2000, Windows NT* version 4, or Windows XP

  Windows computers must be running Client for Microsoft* Networks, which is a standard Windows component. The Client for Microsoft Networks can be manually installed by clicking *Start* > *Settings* > *Control Panel* > *Network* > *Add* > *Client* > *Microsoft*.
- Any NFS* platform capable of NFS v2 or NFS v3 such as UNIX, Linux*, or FreeBSD*

3.4 Starting and Stopping AFP and CIFS Protocols

Each time the server starts, the Novell Native File Access Protocols are loaded from commands that were automatically added to the autoexec.ncf configuration file by the installation program.

You can also load and unload the Native File Access Protocols service manually at the server console.

Macintosh (AFP) Protocols

1. At the server console, type `AFPSTRT` to load the Macintosh (AFP) protocols on the server.

   Any changes made in the AFP configuration files since the last time you started the service are applied when the AFP protocols are reloaded.
2. At the server console, type `AFPSTOP` to unload the Macintosh (AFP) protocols on the server.

Windows (CIFS) Protocols

1. At the server console, type `CIFSSTRT` to load the Windows (CIFS) protocols on the server.

   Any changes made in the CIFS configuration files since the last time you started the service are applied when the CIFS protocols are reloaded.
2. At the server console, type `CIFSSTOP` to unload the Windows (CIFS) protocols on the server.

3.5 What's Next

After installing NetWare 6.5, if you do not enable the universal password feature, you must create simple passwords for Macintosh and Windows users before they can access files on the server using their native protocols.

To set up and manage Macintosh users, see Chapter 4, “Working with Macintosh Computers,” on page 21.

To set up and manage Windows users, see Chapter 5, “Working with Windows Computers,” on page 31.

To set up and manage UNIX users, see Chapter 7, “Working with UNIX Machines,” on page 49.

Working with Macintosh Computers

4

This section contains the following information:

- Section 4.1, “Administrator Tasks for Native File Access for Macintosh Services,” on page 21
- Section 4.2, “Macintosh End User Tasks,” on page 26
- Section 4.3, “Troubleshooting Native File Access for Macintosh,” on page 29

4.1 Administrator Tasks for Native File Access for Macintosh Services

Native File Access for Macintosh provides several ways to simplify your administration tasks and customize how Macintosh workstations interact with the network. Tasks and issues to:

- Section 4.1.1, “Creating Simple Passwords for Several Macintosh Users,” on page 21
- Section 4.1.2, “Enabling and Disabling AFP,” on page 22
- Section 4.1.3, “Enabling and Disabling Delete Inhibit Emulation,” on page 22
- Section 4.1.4, “Editing the Context Search File,” on page 22
- Section 4.1.5, “Creating a Guest User Account,” on page 23
- Section 4.1.6, “Renaming Volumes,” on page 23
- Section 4.1.7, “AFP Console Commands,” on page 24

4.1.1 Creating Simple Passwords for Several Macintosh Users

You can create simple passwords for users one at a time using iManager or ConsoleOne®. The process for creating simple passwords is the same for Macintosh and Windows users. See “Two Methods for Creating Simple Passwords for Windows Users” on page 33 for instructions on creating simple passwords.

If you want to create passwords for several Macintosh users at once, you can add the CLEARTEXT option to the LOAD AFPTCP command at the server console. For example:

```
LOAD AFPTCP CLEARTEXT
```

When the CLEARTEXT option is added to the AFPTCP command, users logging in to the server from a Macintosh workstation are prompted to provide their eDirectory® username and eDirectory password. After the eDirectory password is verified, a simple password is automatically created and stored in eDirectory. The simple password is the same as the eDirectory password.

The CLEARTEXT option is meant to be a temporary way to create simple passwords for many Macintosh users. After Macintosh users have created simple passwords, the AFPTCP NLM™ should be loaded without the CLEARTEXT option.

WARNING: The CLEARTEXT option allows unencrypted passwords to be sent over the network. If you are concerned about someone capturing your password over the network, you should not use this option. Instead, you should manage passwords using ConsoleOne on the Administrator workstation.

4.1.2 Enabling and Disabling AFP

Administrators can enable or disable AFP on NetWare servers using iManager. AFP is enabled by default when NetWare 6.5 is installed.

1. In a Web browser, specify the following in the address (URL) field:

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

   For example:

   `http://192.168.0.1/nps/iManager.html`
2. At the login prompt, specify the server administrator username and password.
3. In the left frame, click *File Protocols,* then click *Enable / Disable AFP*.
4. Type the NetWare server name where you want to enable or disable AFP, or browse and select it.
5. Select or Deselect the *AFP* check box to enable or disable AFP.
6. Click *Apply* to save your changes.

4.1.3 Enabling and Disabling Delete Inhibit Emulation

Prior to NetWare 6.5 Support Pack 6, if the delete inhibit attribute was set on a directory such as a home directory, `AFPTCP.NLM` would by default send that information to MAC clients. The MAC OS 10.4.6 client would then enforce that attribute on the files contained within that directory. This resulted in users not being able to delete or rename files in their own home directory.

A new command line switch was added for AFPTCP called DeleteInhibitEmulation. The default if you do not specify this switch when loading `AFPTCP.NLM` is that AFPTCP does not send delete inhibit or rename inhibit information back to MAC clients. The Delete Inhibit and Rename Inhibit attributes are not enforced on MAC clients without this switch.

To have the Delete Inhibit and Rename Inhibit attributes enforced on MAC clients, load `AFPTCP.NLM` on the server using the following command:

```
load afttcp deleteinhibitemulation
```

You can also unload and reload `AFPTCP.NLM` without the switch to disable this functionality after enabling it.

4.1.4 Editing the Context Search File

A context search file allows Macintosh users to log in to the network without specifying their full context. The context search file contains a list of contexts that are searched when no context is provided or the object cannot be found in the provided context. When the Macintosh user species a username, the server searches through each context in the list until it finds the correct User object.

Macintosh allows only 31 characters for the username. If the full eDirectory context and username are longer than 31 characters, you must use a search list to provide access.

TIP: Macintosh users do not need to specify a context or have an entry in the context search file if their User objects are placed in the same container as the Server object.

If User objects with the same name exist in different contexts, the first one in the context search list will be used.

To edit the context search file, do the following:

1. Using any text editor, edit the ctxs.cfg file stored in the `sys:\etc` directory of the server running Novell Native File Access Protocols.
2. On separate lines, specify the contexts to search.

   For example, if you had users with full eDirectory distinguished names such as Robert.sales.acme, Maria.graphics.marketing.acme, Sophia.graphics.marketing, and Ivan.marketing.acme, then you would specify the following contexts to the ctxs.cfg file:

   ```
   sales.acme
   graphics.marketing.acme
   marketing.acme
   ```

3. Save the file in the `sys:\etc` directory.

   The file is read the next time a Macintosh user logs in.

When Macintosh users log in, they specify only a username and a password. The system finds the User object in the context specified in the ctxs.cfg file.

4.1.5 Creating a Guest User Account

Novell Native File Access Protocols let you create a Guest User object. Macintosh users are accustomed to being able to log in as Guest with no password required.

1. From the Administrator Workstation, use ConsoleOne to create a User object named Guest.
2. Determine and assign the appropriate rights to the Guest object by double-clicking Guest object and clicking *Rights to Files and Folders*.
3. Remove the ability for the user to change the password by clicking *Restrictions* and deselecting *Allow User to Change Password*.
4. Enable the Guest account by adding the full eDirectory context of the Guest object to the context search file as described in “Editing the Context Search File” on page 22.
5. Unload and reload the afptcp.nlm program with the GUESToption to make the *Guest* button available on the login screen.

Any Macintosh user can now log in as Guest with no password and receive the access rights assigned to the Guest object.

4.1.6 Renaming Volumes

Volumes can be renamed so that they appear in Chooser under a different name.

1. Using any text editor, create a file named `afpvol.cfg`.

2 On separate lines, specify the current name of the volume and, in quotes, the new name of the volume. For example:

```
server1.sys "System Volume"
server1.img "Graphics"
#The above volume contains image files.
```

NOTE: The pound sign (#) marks a line as a comment.

3 Save the file in the `sys:\etc` directory of the server running Novell Native File Access Protocols.

After the volume has been renamed, it keeps the name even if you delete the file and restart the server. To return to the previous name, repeat these steps and rename the volume to its original name.

For example:

```
System volume "server1.sys" .
```

4 Unload and reload the `afptcp.nlm` program.

Volumes will appear to Macintosh users with the new volume names.

4.1.7 AFP Console Commands

Several server console commands are provided with AFP to help you perform certain AFP-related tasks. The following table lists the AFP-related server console commands and gives a brief description of each command. To execute an AFP console command, specify the command followed by any desired command line switches or parameters.

Table 4-1 *AFP Console Commands*

Command	Description
AFPLog {ON | OFF}{log text}	Turns the logging feature on or off, and adds a log message to the log. When logging is on, AFP log and error messages are written to the `SYS:\ETC\AFPTCP.LOG` file. Specifying this command followed by a string of text appends that string of text into the log file. This allows you to insert your own comment into the log.

Command	Description
AFPCount {ON | OFF | EnumOff}	If AFPCount is set to ON, AFP enumerates the contents of every directory that it opens and returns accurate counts of the number of offspring (files and directories) in a directory. This option makes AFP slower, but returns accurate counts to Macintosh clients. If AFPCount is set to OFF, empty directories return a count of 0 offspring and non-empty directories return an estimate count. This option improves performance, but does not provide accurate counts. If this option is set to EnumOff, a standard estimate is provided for all enumerate requests, including those for empty directories.This command lets you choose to have accurate counts, or to have estimates that speed up performance.
AFPVolInfo {volume name}{all}	Displays AFP information about a specific volume, or all volumes mounted on the server.
AFPNames {case-sensitive | case-insensitive}{all}{volume}	Lets you specify whether a volume should operate in case-sensitive mode or in case-insensitive mode. The default for new volumes is case-sensitive mode. You can also specify whether you want case sensitivity to apply to a specific volume or all volumes on the server.
AFPClearText {ON | OFF}	AFPClearText controls whether logging in with a clear-text password is allowed. Clear-text passwords are not encrypted. This mode should normally be set to OFF to require encrypted safe passwords. Turning this option on should only be done for debugging or in situations where password security is not important.
AFPRightsMode {defaultRights | noSharing ||all}	Setting this option to defaultRights causes AFPTCP to return default rights for users, groups, and everyone. Setting this option to noSharing causes AFPTCP to return actual rights for the current user only. This disables file sharing from the Macintosh. Setting this option to all causes AFPTCP to return actual rights for users, groups and everyone.
AFPSetWorldRights {ON | OFF}	Setting this option to ON lets users set rights and give access to network directories and their contents for everyone (world). Setting this option to OFF causes AFPTCP to ignore the Set rights requests coming from Macintosh clients so users cannot set rights to give access to others.
AFPGuest {ON | OFF}	Setting this option to ON or OFF lets the user enable or disable guest logins through AFP.

Command	Description
AFPvolume {ON | OFF}{netware volume name}	Setting this option to ON or OFF lets you choose whether or not a volume appears as an advertised AFP volume to Macintosh clients. You must specify the NetWare volume you want this switch to apply to. Turning this switch off causes volume to not appear to Macintosh clients as a volume that is available to be mapped to.

4.2 Macintosh End User Tasks

When Novell Native File Access Protocols is properly configured, the Macintosh end users on your network will be able to perform the following tasks:

- Section 4.2.1, "Accessing Network Files," on page 26
- Section 4.2.2, "Logging In to the Network As Guest," on page 26
- Section 4.2.3, "Changing Passwords from a Macintosh Computer," on page 27
- Section 4.2.4, "Assigning Rights and Sharing Files from a Macintosh Computer," on page 27

4.2.1 Accessing Network Files

Macintosh users can use Chooser to access files and directories each time they are required or they can create an alias on the desktop that is retained after rebooting.

1. In Mac OS 8 or 9, click the *Apple* menu > *Chooser* > *AppleTalk* > *Server IP Address*.

   In Mac OS X, click *Go* > *Connect to Server*.
2. Specify the IP address or DNS name of the NetWare® server, then click *Connect*.
3. Specify the username and password, and then click *Connect*.
4. Select a volume to be mounted on the desktop.

   Although you now have access to the files, mounting the volume to the desktop does not make it available after rebooting.
5. (Optional) Create an alias to the desired volume or directory.

   Aliases are retained after rebooting.

   5a Click the NetWare server icon.

   5b Click *File* > *Make Alias*.

   The alias icon appears on the desktop.

4.2.2 Logging In to the Network As Guest

If the network administrator has set up the Guest User object account as described in "Creating a Guest User Account" on page 23, Macintosh users can log in to the network as Guest with no password required.

1. In Mac OS 8 or 9, click the *Apple* menu > *Chooser* > *AppleTalk* > *Server IP Address*.

   In Mac OS X, click *Go* > *Connect to Server*.

2 Type the IP address or DNS name of the NetWare server, then click *Connect*.

3 Click *Guest Login* > *Connect*.

The Guest user has rights to access network resources as configured by the network administrator.

4.2.3 Changing Passwords from a Macintosh Computer

Macintosh users can change their passwords. When they change their simple password, their eDirectory password is automatically synchronized.

1 In Mac OS 8 or 9, click the *Apple* menu > *Chooser* > *AppleTalk* > *Server IP Address*.

In Mac OS X, click *Go* > *Connect to Server*.

2 Type the IP address or DNS name of the NetWare server, then click *Connect*.

3 Specify the username.

4 Click *Change Password*.

5 Type the old password and the new password, then click *OK*.

A maximum of eight characters is allowed for passwords. Passwords longer than eight characters are truncated to eight characters.

NOTE: Native File Access for Macintosh (AFP) software keeps the simple password and the NetWare passwords synchronized. In other words, when a Mac user changes either password using the native client software, password synchronization is automatic and transparent.

4.2.4 Assigning Rights and Sharing Files from a Macintosh Computer

Although using iManager or ConsoleOne from the Administrator workstation is the recommended method for managing rights, Macintosh users have some file sharing and management capability using Chooser/Finder.

For more information on how to use ConsoleOne to set up and manage rights, see the *ConsoleOne 1.3.x User Guide*, or view the ConsoleOne Online Help.

For more information on how to use iManager to set up and manage rights, see the *Novell iManager 2.7.3 Administration Guide*.

- "NetWare Rights versus Macintosh Rights" on page 27

NetWare Rights versus Macintosh Rights

Using Chooser/Finder to access network files and folders is fairly consistent with the Macintosh environment, but there are some differences between NetWare and Macintosh file sharing. Macintosh users can view the sharing information about specific folders by clicking Get Info/ Sharing.

Inherited Rights and Explicit Rights

The Macintosh file system uses either inherited rights (which use the enclosing folder's privileges) *or* explicit rights (which assign rights to a group or user). A folder in the Macintosh file system cannot have both inherited and explicit rights.

NSS uses both inherited *and* explicit rights to determine the actual rights that a user has. NSS allows a folder (or directory) to hold file rights for multiple groups and users. Because of these differences, Macintosh users will find that access rights to folders and files might function differently than expected.

NSS uses inherited rights, so the Macintosh Use Enclosing Folder’s Privileges option is automatically turned off. When a Macintosh user views the Get Info/Sharing dialog box for a NSS folder, only the User/Group assignments are visible if there is an explicit assignment on the folder. If the NSS folder inherits User/Group rights from a parent group or container, those rights are not displayed in the dialog box, nor will there be any indication that the folder is inheriting rights from a group or container.

Owner, User/Group, and Everyone Rights

Because NSS allows multiple groups and users to have rights to a single folder, users are not able to delete rights assignments using the Apple Macintosh interface. Users can *add* assignments to allow basic file sharing, but more complex rights administration must be done using the management utilities such as iManager or ConsoleOne.When specifying Owners, Users, and Groups, there is no way to select from current groups. You must specify the correct NetWare name and context (fully distinguished eDirectory name).

TIP: No context is required if the context is specified in the context search file.

Owner Rights

In the Apple File Sharing environment, an owner is a user who can change access rights. In the NSS environment, users can change access rights if they have been granted the Access Control right for the folder. In NSS, an owner means the one who created the file. A NSS owner has no rights by virtue of ownership. In the NSS environment, the owner is the current user if he has access control rights to the folder.

If the user does not have access control rights, the NetWare owner will be shown if the NSS owner is not the current user. If the current user does not have rights to change access and is also the NSS owner, a message to "Use NetWare Utility" is displayed in the Owner field.

In Apple File Sharing, there can be more than one owner. If you change the owner, access control rights are added to the new owner, but are not removed from the current owner. In NSS, there are two ways to have access control rights: 1) have the Access Control right and 2) have the Supervisor right. Adding a new owner only adds the Access Control right, not the Supervisor right. If the current owner already has the Supervisor right added through other management utilities, that right will remain. The Supervisor right also gives full file access rights. This means that if you are the current user and have the Supervisor right, you also have read/write access and you cannot change those rights.

Display only allows for one owner. If multiple users have file access rights, only the current user is shown in the Owner field. This means you could change the owner (which in NetWare simply means adding the Access Control right to the new user) and when you open the file sharing dialog box again, you will be listed as the owner, even though you have just given ownership or the Access Control right to someone else.

User / Group

Only one user/group can be displayed for a folder, although NSS allows multiple users and groups to be assigned file access rights. If both users and groups have access to a NSS folder, groups are displayed before users. The group with the most access rights is preferred over groups with lesser access rights. Only users or groups with explicit rights (not inherited rights) are shown in the User/Group field. Users and groups with inherited rights are not shown in the dialog box, nor is there any indication that there are users and groups with inherited rights.

Adding a group or user does not remove the current group or user; it simply adds the rights to the group or user specified. If the user specifies the wrong user or group name, the user gets no feedback. If multiple users or groups are assigned to the folder, it is possible that the user is unable to see the user or group that was just assigned. It could be very difficult to know if the rights assignment worked or not.

Rights set through this interface are inherited by the folder's subfolders. It is impossible to manage all inherited rights from the Macintosh interface. (Although not recommended, you could set the inherited rights filters from the management utilities to turn off inherited rights.)

Everyone

Assignment of rights to Everyone acts like the Macintosh user expects, with the exception that Everyone's rights are inherited. In NetWare, the object that represents the rights of any authenticated user is used to set Everyone's rights. Everyone's rights can change from folder to folder, but once they are set, they are inherited by subfolders.

4.3 Troubleshooting Native File Access for Macintosh

This section contains the following troubleshooting issues:

- Section 4.3.1, "Three Grace Logins Required on Universal Password Expiration," on page 29
- Section 4.3.2, "AppleTalk Not Supported As a Transport Protocol," on page 30
- Section 4.3.3, "Mac OS 8.x Will Not Mount Volumes Checked to Mount at Startup," on page 30
- Section 4.3.4, "Unloading Afptcp.nlm and Wspdsi.nlm Programs," on page 30
- Section 4.3.5, "Traditional Volume Access Not Supported," on page 30

4.3.1 Three Grace Logins Required on Universal Password Expiration

If you set a password expiration date using Universal Password, you should notify Macintosh * users that three grace logins are required to change a password. If users wait until the final grace login, they will be denied access to the network and the password will expire.

When Macintosh users are notified that they need to change their password, they will need three grace logins in order to log in and change the password. Two grace logins are required for the Macintosh interface (the user logs in once, then logs out, then logs in again to change the password). In addition, there is currently a counting problem. When there is one grace login left, the user is not able to log in. This issue will be resolved in NetWare 6.5 Support Pack 1.

4.3.2 AppleTalk Not Supported As a Transport Protocol

Older Macintosh applications that have unique dependencies upon AppleTalk* as a transport protocol must be updated to a version that is known to work over TCP/IP. The AppleTalk stack protocols (TLAP, ELAP, LLAP, DDP, RTMP, AEP, ATP, NBP, ADSP, ZIP, ASP, and PAP) are not supported over TCP/IP by Apple*.

Therefore, we do not support those legacy protocols. Both Novell and Apple have embraced TCP/IP as the Internet standard transport protocol.

IMPORTANT: Older NetWare for Macintosh and Prosoft versions of afp.nlm and appletlk.nlm are not supported. Do not attempt to mix old Macintosh NLM™ programs with the new afptcp.nlm.

4.3.3 Mac OS 8.x Will Not Mount Volumes Checked to Mount at Startup

Mac OS 8.*x* will not mount volumes checked to mount at startup. To resolve this, add the server volume's alias to the StartUp Items folder inside the System Folder on the Macintosh's local startup disk.

4.3.4 Unloading Afptcp.nlm and Wspdsi.nlm Programs

The Winsock component used by the Macintosh Native File Access NLM program does not always clean up all open sockets. If you unload afptcp.nlm and then explicitly unload wspdsi.nlm, you might get the following warning in flashing red text:

```
WARNING!!!

1 active Winsock 2 DSI socket session(s)

Unloading WSPDSI.NLM with active session(s) will abend the server.

Unload all Winsock 2 apps with active SSL socket session(s).

Unload module anyway?
```

The warning is correct. WSPDSI assumes there are still active AFP sessions and it will abend the server if you unload it.

There is no need to unload WSPDSI manually. Afptcp.nlm loads it automatically on startup and afpstop.ncf does not unload it. It remains loaded. Under normal use, you should not see this warning.

4.3.5 Traditional Volume Access Not Supported

Native File Access for Macintosh is supported only on NSS volumes. Traditional volumes are not available to Macintosh users.

Working with Windows Computers

5

This section contains the following information:

- Section 5.1, “Administrator Tasks for Native File Access for Windows Services,” on page 31
- Section 5.2, “Windows End User Tasks,” on page 40
- Section 5.3, “Troubleshooting Native File Access for Windows,” on page 41

5.1 Administrator Tasks for Native File Access for Windows Services

Native File Access for Windows provides several ways to simplify your administration tasks and customize how Windows workstations interact with the network:

- Section 5.1.1, “Creating Simple Passwords for Windows Users,” on page 31
- Section 5.1.2, “Two Methods for Creating Simple Passwords for Windows Users,” on page 33
- Section 5.1.3, “Enabling Users to Change Their Simple Passwords with iManager,” on page 34
- Section 5.1.4, “Understanding Synchronization of NetWare Passwords and Simple Passwords,” on page 35
- Section 5.1.5, “Specifying Contexts in the Context Search File,” on page 35
- Section 5.1.6, “Managing Network Access with ConsoleOne,” on page 36
- Section 5.1.7, “Providing Network Access to Domain Users,” on page 36
- Section 5.1.8, “Enabling and Disabling CIFS,” on page 36
- Section 5.1.9, “Enabling and Disabling SMB Signing,” on page 37
- Section 5.1.10, “Changing CIFS Configuration,” on page 38
- Section 5.1.11, “Viewing Configuration Details,” on page 40

5.1.1 Creating Simple Passwords for Windows Users

In order to take advantage of Novell® Native File Access software, all users must have a NetWare® User object created in eDirectory™.

NOTE: A NetWare User object specifies attributes and information about which network resources the user can access. User objects are created using iManager or ConsoleOne®. For more information about iManager, see the “iManager Security Issues”. For more information about ConsoleOne, see the *ConsoleOne 1.3.x User Guide*.

Also, if the universal password feature in NetWare 6.5 is *not* enabled, most users must also have a *simple password* created for them before they can access network resources using Native protocols. The exception is when Native File Access for Windows software has been configured to use the Domain authentication method.

To avoid user lockout in windows pass through mode, change the following settings in windows PDC to `RequireSecuritySignature - Disable`

Execute command at PDC:

```
net config server /autodisconnect:-1
```

This section describes the two Windows authentication methods and password requirements and explains how to create simple passwords for Windows users.

- "Windows Authentication Methods and Simple Passwords" on page 32

Windows Authentication Methods and Simple Passwords

The method that Windows workstations (using their Native Common Internet File System, or CIFS, Protocol) use to authenticate to the CIFS-enabled NetWare server is determined by which authentication method is configured. The two Windows authentication methods are Local and Domain.

If Local authentication is being used, each Windows user must have a simple password associated with their NetWare/eDirectory User object in order to access network resources using Native protocols. However, if Domain authentication is being used, a simple password is not required. The reason is that Domain authentication uses passthrough authentication to the Windows Domain Contoller. As a result, when implementing Domain authentication, Novell Native File Access software does not support the Change Password feature from the client; the password must be changed using the Domain Controller User Manager tool.

In order to understand how the Novell Native File Access software incorporates the security of NetWare with the Native operating system's security (such as Microsoft Networking), it is useful to first know the functionality and interrelation of the following four distinct passwords used in a mixed networking environment.

- **Windows Local Password:** The Windows operating system requires a username and password to log in to the computer. This password, called the *local password*, is stored on the computer's local hard disk.
- **Windows Domain Controller Password:** Windows networking uses a domain controller, which is a computer running Windows Server software that manages user access to the Microsoft network. When Windows users log in to the network using a Domain Controller, they are required to specify a username and password for authentication. This password, called the *domain controller password*, is stored on the domain controller computer.
- **NetWare Password:** To access the NetWare network, each user must have a user account created specifically for him or her. This account is called a *User object* and is stored in the Novell eDirectory data store. It consists of a NetWare username and a corresponding *NetWare password*.

  When the workstation is running Novell Client™ software, users log in by specifying their NetWare username (including context) and password. NetWare usernames and passwords are stored securely in the eDirectory structure on NetWare servers.
- **Simple Password:** The *simple password* is also associated with a corresponding User object and is required to provide network access from workstations that do not have Novell Client software installed. As with the NetWare password, the simple password is stored securely in eDirectory on the network.

IMPORTANT: Remember that if Local authentication has been implemented, Windows users must have a simple password in order to access network resources using their Native protocol (CIFS). However, if Domain authentication has been implemented for your server, a simple password is not required.

5.1.2 Two Methods for Creating Simple Passwords for Windows Users

You can create simple passwords with either ConsoleOne or iManager.

- "Using ConsoleOne" on page 33
- "Using iManager" on page 33

Using ConsoleOne

1. At the Administrator Workstation, log in as a user with the Supervisor right.

   Make sure that the Administrator Workstation meets the prerequisites described in Section 3.2, "Administrator Workstation Prerequisites," on page 18.
2. Run consoleone.exe (located in the `\public\mgmt\consoleone\1.2\bin` directory).
3. Right-click the User object, then click *Properties*.
4. Click the *Login Methods* tab and select *Simple Password*.
5. Create a simple password for the selected user by filling in the following fields:
   - **Set Simple Password:** Specify a unique password for the user.
   - **Confirm Simple Password:** Specify the same password for confirmation.

   NOTE: If the simple password is different from the NetWare password, users specify the simple password when accessing the network with Native protocols and they specify the NetWare password when logging in with Novell Client software.
6. Click *OK*.
7. Repeat Step 3 through Step 6 in order to create a simple password for each user who requires network access using Novell Native File Access software.
8. (Optional) If you want users to be able to change their own simple passwords after they log in the first time, check the *Force Password Change* check box.

Using iManager

You can also use iManager to create simple passwords for individual users.

1. In a Web browser, specify the following in the address (URL) field:

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

   For example:

   `http://192.168.0.1/nps/iManager.html`
2. At the login prompt, specify the server administrator username and password.

3 In the left frame, click *Users*, then click either *Modify Users* if you are creating a simple password for an existing user or *Create Users* if you are creating a new user object and want to create a simple password for that new user object.

4 (Conditional) If you are creating a simple password for an existing user

4a Specify the username, or browse to and select the user that you want to create the simple password for.

4b Click the *Restrictions* tab and then click the *Set Password* link.

4c Click the *Set Simple Password* check box and specify the simple password you want to assign to the user.

Keeping the eDirectory password the same as the simple password is the easiest way to manage passwords.

5 (Conditional) If you are creating a simple password for a new user object

5a Specify the name and other requested information for the new user.

5b Click the *Set Simple Password* check box and specify the simple password you want to assign to the user.

NOTE: If the simple password is different from the NetWare password, users specify the simple password when accessing the network with Native protocols, and they specify the NetWare password when logging in with Novell Client software.

Now that you have created simple passwords for User objects in NetWare, those users can use Native protocols and familiar access methods (such as Network Neighborhood or My Network Places) to access and manipulate files on the server. When prompted to authenticate, users specify their NetWare username (without context) and their corresponding simple password

5.1.3 Enabling Users to Change Their Simple Passwords with iManager

You can use ConsoleOne to assign the necessary rights so that users can change simple passwords with iManager.

1 At the Administrator workstation, log in as a user with the Supervisor right.

Make sure that the Administrator workstation meets the prerequisites described in Section 3.2, “Administrator Workstation Prerequisites,” on page 18.

2 Run consoleone.exe (located in the `\public\mgmt\consoleone\1.2\bin` directory).

3 Right-click the User object, then click *Trustees of This Object*.

4 Select the User object and click *Assigned Rights* > *Add Property*.

5 Select the *SAS:Login Configuration* property from the list and click *OK*.

6 Click *Add Property*, select *SAS:Login Configuration Key* and click *OK*.

7 Enable Compare, Read, and Write rights for both of the properties you just added to the User object.

8 Click *OK* > *OK*.

5.1.4 Understanding Synchronization of NetWare Passwords and Simple Passwords

Native File Access for Windows (CIFS) software allows users to change their own passwords from a client workstation. Of course, this applies only when Local authentication is being used because the Domain authentication method does not use simple passwords. When users change their simple passwords, their NetWare passwords will be affected differently, as described in the following scenarios:

- If both the NetWare password and the simple password are already the same when the user changes the simple password, the NetWare password is synchronized and both passwords remain the same.
- If the NetWare password and the simple password are *not* the same when the user changes the simple password, the NetWare password is not synchronized with the new simple password. The two passwords remain different.
- Whenever a user changes the NetWare password, the simple password is not synchronized with the new NetWare password. The user must separately change the simple password for the two passwords to match.

NOTE: With the Universal password feature enabled in NetWare 6.5, there is no need to create separate simple passwords. The Universal password automatically keeps passwords synchronized.

5.1.5 Specifying Contexts in the Context Search File

An eDirectory search context is created automatically during the NetWare installation for Windows users who require access to the network. These contexts are saved in the context search file. When Windows users specify a username, the Native File Access component running on the server searches through each context in the list until it finds the correct User object.

NOTE: In Domain mode, if User objects with the same name exist in different contexts, each user object attempts authentication in order until one succeeds with the corresponding password.

You can add or remove contexts by editing the context search file.

1. Using any text editor, edit the `cifsctxs.cfg` file stored in the sys:\etc directory of the server.
2. On separate lines, specify the full contexts to search.

   For example if you had users with full eDirectory distinguished names such as Robert.sales.acme, Maria.graphics.marketing.acme, Sophia.graphics.marketing, and Ivan.marketing.acme, then you would specify the following contexts to the cifsctxs.cfg file:

   ```
   sales.acme
   graphics.marketing.acme
   marketing.acme
   ```
3. Save the file in the sys:\etc directory.
4. At the server console, specify `CIFSSTOP` to unload the current context search file.
5. Specify `CIFSSTRT` to load the new context search file and apply the changes.

When Windows users log in, they specify only a username and the simple password. The system finds the User object in the context specified in the `cifsctxs.cfg` file.

5.1.6 Managing Network Access with ConsoleOne

ConsoleOne helps you manage Novell Native File Access for each computer platform. You can create users and groups, assign and restrict rights to directories, and view the rights of specific users.

To provide rights to network access, do the following:

1. From the Administrator workstation, log in to the NetWare server running Novell Native File Access Protocols software.

   You must use a Windows workstation that meets the prerequisites as described in Section 3.2, "Administrator Workstation Prerequisites," on page 18.
2. Run consoleone.exe, located in `\public\mgmt\consoleone\1.2\bin\`.
3. Set up and manage rights as described in the *ConsoleOne 1.3.x User Guide*.

5.1.7 Providing Network Access to Domain Users

You can provide access to users from an existing NT domain by importing them into eDirectory.

1. Configure the Novell Native File Access Protocols software for Domain authentication.

   Importing users from an NT domain is not supported in Local Mode. In Local Mode, the main NetWare® Remote Manager page is displayed rather than the NFAP Import Users page.
2. Run NetWare Remote Manager.

   The NetWare Remote Manager is launched by specifying the IP address of the server into the URL field of an Internet browser.

   See *NW 6.5 SP8: Novell Remote Manager Administration Guide* in the NetWare 6.5 documentation.
3. In the left frame, click *Manage eDirectory > NFAP Import Users*.
4. Browse to the eDirectory Context that you will import the users into.

   Any time you reach a valid context for importing users, a Start button will appear.
5. Click *Start* to import users.

   The context that you select will be automatically written to the `cifsctxs.cfg` file, which contains all the contexts of all users.

   The status of the import is given on the interval that you select.
6. When the import is complete, click *Done* to clear the screen.

5.1.8 Enabling and Disabling CIFS

Administrators can enable or disable CIFS on NetWare servers by using iManager. CIFS is enabled by default when NetWare 6.5 is installed.

1. In a Web browser, specify the following in the address (URL) field:

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

   For example:

   `http://192.168.0.1/nps/iManager.html`
2. At the login prompt, specify the server administrator username and password.
3. In the left frame, click *File Protocols*, then click *CIFS*.

4 Type the NetWare server name where you want to enable or disable CIFS, or browse and select it.

5 Select or deselect the *Enable CIFS* check box to enable or disable CIFS.

6 Click *Apply* to save your changes.

5.1.9 Enabling and Disabling SMB Signing

SMB (or CIFS) signing is necessary to prevent "man-in-the-middle" attacks. It supports message authentication, which prevents active message attacks. SMB signing provides this authentication by placing a digital signature into each SMB. The digital signature is then verified by both the client and the server.

To use SMB signing, you must enable it on both the client and the server. If SMB signing is required on the server, clients cannot establish sessions with the server unless they have SMB signing enabled.

SMB signing is disabled by default. It can be enabled or disabled and set to mandatory or optional mode using either server console commands, or iManager.

If SMB signing is set to optional mode (the default mode after enabling it using console commands) it automatically detects whether or not individual clients have SMB signing enabled. If a client does not have SMB signing enabled, the server does not use SMB signing for client communication. If a client has SMB signing enabled, the server uses SMB signing for client communication.

If you set SMB signing to mandatory mode, all clients must have SMB signing enabled or they cannot connect to the server.

Using Console Commands

To enable SMB signing on a NetWare 6.5 SP4 or later server, specify the following command at the server console:

```
cifs signatures enable
```

If you have enabled SMB signing and want to disable it, specify the following command at the server console:

```
cifs signatures disable
```

To set SMB signing to mandatory mode after enabling it, specify the following command at the server console:

```
cifs signatures mandatory
```

SMB signing is set to optional mode by default after enabling it using console commands. If you have set SMB signing to mandatory and want to change it back to optional, specify the following command at the server console:

```
cifs signatures optional
```

Using iManager

1 In a Web browser, specify the following in the address (URL) field:

`http://`*`server_IP_address`*`/nps/iManager.html`

For example:

`http://192.168.0.1/nps/iManager.html`

2. At the login prompt, specify the server administrator username and password.
3. In the left frame, click *File Protocols,* then click *CIFS*.
4. Type the NetWare server name where you want to enable or disable SMB signing, or browse and select it.
5. Click the *Properties* button, then click the *Server* tab.
6. In the *SMB Signature* section of the page, select either *Mandatory* or *Optional* to enable SMB signing and to set it to either the optional or mandatory mode.

   After enabling SMB signing, you can select *Disabled* to disable it.
7. Click the *Apply* button to save your changes.

IMPORTANT: After enabling or disabling SMB signing, or changing the mode to optional or mandatory, clients must reconnect in order for changes to take effect. For example, if you have enabled SMB signing on the server, SMB signing will not be in effect for individual clients until each of those clients reconnect.

Mounting a CIFS Share

If you want to use the Linux mount command to create a mount point to a CIFS share from a Linux client, you must use the `mount -t cifs` command. Using the `mount -t smbfs` command does not work properly due to a problem in the smbfs client.

5.1.10 Changing CIFS Configuration

Administrators can customize the network environment for Windows workstations (CIFS) using iManager.

1. In a Web browser, specify the following in the address (URL) field:

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

   For example:

   `http://192.168.1.1/nps/iManager.html`
2. At the login prompt, specify the server administrator username and password.
3. In the left frame, click *File Protocols,* then click *CIFS*.
4. Type the NetWare server name where you want to change CIFS configuration, or browse and select it.
5. Ensure that the *Enable CIFS* check box is selected.
6. Create, edit, or delete CIFS shares as desired or click the Properties button to access additional configuration pages.

   See the descriptions below for details on the other configuration options.
7. Click *Apply* to save your settings.

- “CIFS Server Property Page Parameters” on page 39
- “CIFS Authentication Property Page Parameters” on page 39
- “Shares Parameters” on page 40

CIFS Server Property Page Parameters

In addition to the SMB signature options, the following parameter fields and options appear on the CIFS Properties page in iManager if you click the *Server* tab:

- ***CIFS Virtual Server Name:*** is the name of the server running Novell Native File Access Protocols. The length can be a maximum of 15 characters. This name is displayed in Network Neighborhood. This server name must be different from the NetWare server name. The default server name is the NetWare server name with an added dash (-) and a W. For example, a NetWare server named ACME1 would default to ACME1-W.

  NOTE: On NetWare CIFS, the first 14 characters of the different virtual server names cannot be the same.

  For example: CSI-SSIG-TBETA2, CSI-SSIG-TBETAn

- ***WINS IP Address:*** is the address of the WINS server to be used to locate the PDC, if the PDC and the server running Novell Native File Access Protocols are on different subnets.
- ***Comment*:** is the comment associated with the server name discussed above. This comment is displayed when viewing details.
- ***OpLocks* (Opportunistic Locking):** improves file access performance and is enabled by default for NetWare 6.5. You can disable or enable it by selecting or deselecting the check box.
- ***DFS* (Distributed File Services Support):** lets CIFS clients use the volume junction features of NSS. See "Installing DFS" in the *Novell Distributed File Services Administration Guide* for more information. You can enable or disable DFS support on this server for CIFS clients.

CIFS Authentication Property Page Parameters

The following options and parameter fields appear on the CIFS Properties page in iManager if you click the *Authentication* tab:

- ***Mode*:** indicates the method of authentication used by Novell Native File Access Protocols. You can select either *eDirectory (Local)* or *Third Party Domain* from the drop-down list:
  - ***Third Party Domain*:** Clients are members of a domain. A Windows domain controller performs user authentication.The username and password on the domain controller must match the username and password used to log in to the Windows workstation.
  - ***eDirectory Local*:** Clients are members of a workgroup. The server running Novell Native File Access Protocols performs the user authentication. The username and password on NetWare must match the username and password used to log in to the Windows workstation.
- ***Work Group/Domain Name:*** is the domain or workgroup that the server will belong to. *Workgroup* and *Domain* can be used interchangeably.
- ***Primary Domain Controller Name*:** is the name of the PDC server. This option should be used only when there is a valid reason for overriding WINS or DNS. This field can be changed only if *Domain Mode* is selected.
- ***Primary Domain Controller IP Address:*** is the PDC server's static IP address. This is needed if the PDC is on a different subnet. This option should be used only when there is a valid reason for overriding WINS or DNS. This field can be changed only if *Domain Mode* is selected.

IMPORTANT: The address of the PDC must be static; otherwise, if the PDC reboots and the address changes, the server running Novell Native File Access Protocols will not be able to contact the PDC.

Shares Parameters

The following fields appear if you click *New* or *Edit* on the CIFS Management page in iManager. Use the Shares page to add volumes or directories on the server to be specified as shared points and to be accessible via the Network Neighborhood.

NOTE: If no Shares are specified, then all mounted volumes are displayed.

- ***Share Name:*** is the name by which the sharepoint is displayed on Windows computers. For example, if you specify Company Photos as the sharename associated with `vol1\graphics`, then Windows workstations browsing the network see "Company Photos" instead of "`vol1\graphics`".
- ***Path*:** is the path to the server volume or directory which becomes the root of the sharepoint. Do not end the path with a backslash (\).
- ***Comment*:** is a description for the sharepoint that appears in Network Neighborhood or My Network Places.

5.1.11 Viewing Configuration Details

You can view details about how Novell Native File Access Protocols are configured by specifying the following commands at the server console.

`CIFS INFO` displays operational information.

`CIFS SHARE` displays all active sharepoints.

`CIFS SHARE sharename` displays information about a specific sharepoint.

5.2 Windows End User Tasks

When Novell Native File Access Protocols is properly configured, the Windows users on your network will be able to perform the following tasks:

- Section 5.2.1, “Accessing Files from a Windows Computer,” on page 40
- Section 5.2.2, “Mapping Drives from a Windows Computer,” on page 41

5.2.1 Accessing Files from a Windows Computer

From a Windows computer, you can access a file and folder each time it is required or you can map drives and create shortcuts that are retained after rebooting.

1. Specify your username (no context) and local password to log in to the computer.
2. Access the network by clicking the network icon.

   In Windows 2000, XP or Windows ME, click *My Network Places*. In Windows 95/98, click *Network Neighborhood*.

3 Browse to the workgroup or domain specified during the Novell Native File Access software installation.

4 Select the server running Novell Native File Access Protocols.

Although it is the same computer, the Novell Native File Access server name is *not* the same as the NetWare server name. For more information, ask your network administrator.

TIP: You can specify the server name or the server IP address in Find Computer to quickly access the server running Novell Native File Access software.

---

5 Browse to the desired folder or file.

IMPORTANT: Accessing files from a Windows computer requires NetBIOS over TCP/IP to be enabled on the Windows computer. If you have disabled NetBIOS over TCP/IP, you won't be able to access files and directories using CIFS.

5.2.2 Mapping Drives from a Windows Computer

1 Specify your username and local password for Microsoft Networking.

2 Click *Map Network Drive*.

There are several ways to access Map Network Drive. For example, you can use the Tools menu in Windows Explorer or you can right-click Network Neighborhood.

3 Browse to or specify the following path:

\\ *server_running_Novell_Native_File_Access_software*\ *sharepoint* | *volume* | *directory*\

4 Select the server running Novell Native File Access Protocols.

Although it is the same computer, the Novell Native File Access server name is *not* the same as the NetWare server name. For more information, contact your network administrator.

5 Complete the on-screen instructions for mapping the drive.

5.3 Troubleshooting Native File Access for Windows

This section contains the following troubleshooting issues:

- Section 5.3.1, "Workstations Unable to Access a Windows 2000 Primary Domain Controller," on page 42
- Section 5.3.2, "PDC and CIFS on Different Subnets," on page 42
- Section 5.3.3, "Password Changes," on page 42
- Section 5.3.4, "CIFS Server Not Visible in Network Neighborhood," on page 42
- Section 5.3.5, "Traditional Volume Access Not Supported," on page 42
- Section 5.3.6, "Virtual Server Restart Required after Stopping and Restarting CIFS," on page 43
- Section 5.3.7, "Trustee Rights Required to CIFS Virtual Server," on page 43

5.3.1 Workstations Unable to Access a Windows 2000 Primary Domain Controller

If the Primary Domain Controller (PDC) is a Windows 2000 server, Windows workstations might not be able to access the CIFS server.

To fix this using iManager:

1. In a Web browser, specify the following in the address (URL) field:

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

   For example:

   `http://192.168.1.1/nps/iManager.html`
2. At the login prompt, specify the server administrator username and password.
3. In the left frame, click *File Protocols* > *CIFS*.
4. Type the NetWare server name where CIFS is running, or browse and select one.
5. Click *Properties*, then click the *Authentication* tab.
6. Ensure that the Mode is set to *Third Party Domain* and that the Group Name is set correctly.
7. Specify the name and IP address for the Primary Domain Controller, then click *Apply*.
8. Specify `CIFSSTOP` and then `CIFSSTRT` at the server console.

5.3.2 PDC and CIFS on Different Subnets

If the PDC and CIFS servers are on different subnets, you must specify an IP address for the PDC on the CIFS Config property page for the Server object.

5.3.3 Password Changes

Trying to change a password from a Windows 9.*x* or NT4 client workstation might fail if the default network username and password in the client's cache are not a valid combination on the CIFS server where the password change was attempted.

To avoid this problem, validate the username and password combination in the client's cache on the CIFS server before attempting the password change. You can validate by attempting to access the file system on the CIFS server by browsing to Network Neighborhood.

5.3.4 CIFS Server Not Visible in Network Neighborhood

You might occasionally find that your CIFS server is not visible using Network Neighborhood. This can happen if you have a domain that contains only Windows 95/98 and no NT/2000/XP servers or clients. To correct this problem, specify the server name or IP address in Find Computer.

5.3.5 Traditional Volume Access Not Supported

Native File Access for Windows is supported only on NSS volumes. Traditional volumes are not available to Windows users.

5.3.6 Virtual Server Restart Required after Stopping and Restarting CIFS

If you have CIFS configured to run in ACTIVE/ACTIVE mode and you stop and then restart CIFS on a server, you must bring the virtual server resource offline and then online again to cause the CIFS ADD command to be executed from the load script. This is required for the cluster to be aware that CIFS has been restarted.

5.3.7 Trustee Rights Required to CIFS Virtual Server

If the CIFS virtual server (cluster-enabled volume) goes into a comatose state when starting, it could indicate that the CIFS ADD command fails to execute in the virtual server load script. This problem is common if servers running CIFS do not have trustee rights to the CIFS virtual server.

Ensure servers running CIFS have trustee rights to the CIFS Virtual Server object.

Setting Up Novell Native File Access Protocols in a NetWare 6.5 Cluster

6

NetWare® 6.5, Novell® Cluster Services™ software, and Novell Native File Access Protocols provide high availability, scalability, and security to your network while reducing administrative costs associated with managing client workstations.

This section describes how to set up a NetWare 6.5 clustered environment so that Macintosh and Windows computers can use Novell Native File Access Protocols to access files on the network.

NOTE: For information on setting up UNIX computers to use Novell Native File Access Protocols in a clustered NetWare 6.5 environment, see Chapter 7, "Working with UNIX Machines," on page 49.

- Section 6.1, "Prerequisites," on page 45
- Section 6.2, "Setting Up for Macintosh," on page 46
- Section 6.3, "Setting Up for Windows," on page 46
- Section 6.4, "What's Next," on page 47

6.1 Prerequisites

Before installing Novell Native File Access Protocols in a clustered environment, make sure that you have met the following prerequisites:

- ❑ Novell Cluster Services 1.8.4 installed on NetWare 6.5 servers

  For information on configuring Novell Cluster Services, see the *NW6.5 SP8: Novell Cluster Services 1.8.5 Administration Guide*.
- ❑ NetWare 6.5 configured as described in "Installing Novell Native File Access Protocols on a NetWare 6.5 Server" on page 17.
- ❑ Administrator workstation configured as described in Section 3.2, "Administrator Workstation Prerequisites," on page 18.
- ❑ Novell Native File Access Protocols installed on each server in the cluster that you want users to access.

  Follow the instructions in "Installing Novell Native File Access Protocols on a NetWare 6.5 Server" on page 17.

6.2 Setting Up for Macintosh

To set up the Macintosh portion of Novell Native File Access Protocols in an environment running Novell Cluster Services:

1. Ensure that `afptcp.nlm` is loaded on all servers in the cluster by specifying `MODULES` at the server system console and reviewing the list of loaded modules.

   Afptcp.nlm is loaded automatically on the server by the afpstrt.ncf file, which is automatically added to the autoexec.ncf file during the NetWare 6.5 installation.

2. Cluster enable the shared-disk pools or volumes by following the procedures described in "Enabling Sharing on a Device" in the *Novell Cluster Services Administration Guide*.

   When you create and cluster enable an NSS pool or volume by following the above-referenced procedures, a screen appears that lets you choose the advertising protocols. Ensure AFP is selected on this screen. This will cause an AFPBIND command to be added automatically to the cluster-enabled pool volume load script, which ensures that your cluster-enabled pools are highly available to Macintosh clients.

   AFPBIND allows AFP virtual server names to be advertised via SLP.

3. (Optional) Rename cluster-enabled volumes so Macintosh users will see the same volume name regardless of what server has the volume mounted.

   For instructions, see "Renaming Volumes" on page 23.

   Volumes are displayed as ServerName.VolumeName. If the server fails over, the user sees the next flivver server with the same volume name. For example, Server1.VOL1 becomes Server2.VOL1. Renaming each ServerName.VolumeName to a common name displays the common name regardless which server is providing the volume. For example, renaming Server1.VOL1 to Graphics, Server2.VOL1 to Graphics, and Server3.VOL1 to Graphics displays Graphics regardless which server is providing VOL1.

Macintosh clients should now be able to access files on the cluster by specifying the IP address or virtual server name of the cluster-enabled volume.

NOTE: Novell Native File Access Protocols does not support automatic reconnect for Macintosh computers. If the network connection between a Mac computer and one of the servers in the cluster fails, the user must reconnect using the same IP address for the cluster-enabled volume.

6.3 Setting Up for Windows

CIFS should be configured to work with Novell Cluster Services in ACTIVE/ACTIVE mode.

ACTIVE/ACTIVE mode is the recommended configuration because it provides faster recovery after a failure. ACTIVE/ACTIVE mode signifies that CIFS is running simultaneously on multiple servers in the cluster. When a server fails, the cluster volumes mounted on that server fail over to other servers in the cluster and users retain access to files and directories.

To configure CIFS for ACTIVE/ACTIVE mode with Novell Cluster Services:

1. Ensure the cifsstrt.ncf command is in the `Autoexec.ncf` file of each server in the cluster that will run CIFS.
2. Create and cluster enable pools by following the instructions in the "Creating Shared NSS Pools" section of the *NW6.5 SP8: Novell Cluster Services 1.8.5 Administration Guide*.

When you create and cluster-enable pools, ensure that the CIFS check box that appears in NetWare Remote Manager during the partition and pool creation process is checked, and specify the CIFS Server Name in the field provided. This can also be done using iManager or the NSSMU console utility. This will make the pool accessible and highly available to CIFS clients.

The CIFS server name is the server name CIFS clients see when they browse the network. A default server name is listed, but you can change the server name by editing the text in the field.

When you cluster enable a pool and make the pool accessible to CIFS clients, the CIFS ADD command along with the Fully Distinguished Name (FDN) of the virtual server (cluster-enabled pool) is automatically added to the pool load script and the CIFS DEL command is automatically added to the pool unload script. These commands are necessary to allow clients to connect to the cluster-enabled pool.

With CIFS configured to run in ACTIVE/ACTIVE mode, if you stop and then restart CIFS on a server, you must bring the virtual server resource offline and then online again to cause the CIFS ADD command to be executed from the load script.

Although ACTIVE/ACTIVE mode is the recommended configuration, CIFS can also be run in ACTIVE/PASSIVE mode. ACTIVE/PASSIVE mode signifies that CIFS software runs on only one node at a time in the cluster. When a server fails, CIFS starts on another specified node in the cluster, and the cluster volumes that were mounted on the failed server fail over to that other node. This makes ACTIVE/PASSIVE mode slower because, in addition to cluster volumes failing over, CIFS software has to load on other servers in the cluster before users can access files and directories.

To configure CIFS for ACTIVE/PASSIVE mode with Novell Cluster Services, follow the instruction above, except remove the CIFSSTRT.NCF command from the AUTOEXEC.NCF file of each server in the cluster and add it to the beginning of the load script of each cluster-enabled pool.

6.4 What's Next

With the NetWare 6.5 cluster configured with Novell Native File Access Protocols, Macintosh and Windows users can receive the benefits of a clustered environment—without needing additional client software.

For an explanation of how Macintosh users access network files and for more information on managing Macintosh workstations, see Chapter 4, “Working with Macintosh Computers,” on page 21.

For an explanation of how Windows users access network files and for more information on managing Windows workstations, see Chapter 5, “Working with Windows Computers,” on page 31.

Working with UNIX Machines 7

This section contains the following topics:

- Section 7.1, “Features of Native File Access for UNIX,” on page 49
- Section 7.2, “Overview of Native File Access for UNIX,” on page 51
- Section 7.3, “Prerequisites,” on page 51
- Section 7.4, “NFS Server,” on page 52
- Section 7.5, “Network Information Service,” on page 60
- Section 7.6, “User and Group Information,” on page 64
- Section 7.7, “ConsoleOne Administration,” on page 65
- Section 7.8, “Administration Utilities,” on page 66
- Section 7.9, “Upgrade Utility,” on page 67
- Section 7.10, “Refreshing the Cache to update UNIX Profile,” on page 68
- Section 7.11, “Configuring and Managing Native File Access for UNIX,” on page 68
- Section 7.12, “Configuring Server General Parameters,” on page 69
- Section 7.13, “Migrating NIS Maps,” on page 72
- Section 7.14, “Managing NFS Server,” on page 79
- Section 7.15, “Managing NIS Server,” on page 89
- Section 7.16, “Cluster-Enabling Native File Access for UNIX,” on page 113
- Section 7.17, “Interoperability,” on page 118
- Section 7.18, “Performance Tuning,” on page 119

7.1 Features of Native File Access for UNIX

- The NFS Server component has been completely redesigned for better performance. The new NLM™ program, xnfs.nlm, provides the NFS Server functionality.

  For details, refer to Section 7.18, “Performance Tuning,” on page 119.

- The NetWare and independent modes of file access are supported.

  For details, refer to “File Access Modes” on page 53.

- The cross protocol file locking feature ensures that a file is updated correctly before another user, application, or process can access it.

  For details, refer to “NFS Server File Lock Manager” on page 59.

- The NFS Server is completely MP enabled.

- The NFS exports entry format has been modified to make it more user friendly.

  For details, refer to “Export Options” on page 81 and the comments in the sys:/etc/exports file.

- You can now administer NFS Server, NIS, and UNIX User/Group Management using iManager from the Web.

For details, refer to "Managing NFS Server Using iManager" on page 84 and Section 7.15.1, "iManager-Based Management for NIS Server," on page 89.

- Native File Access for UNIX now supports both active/active and active/passive modes of cluster-enabling.

  For details, refer to "Active/Active Mode" on page 116.

- Only NSS volumes can be exported using Native File Access for UNIX. NFS Server does not support exporting NetWare Traditional file system.

- NFS Server

  Network File System (NFS) Server enables UNIX users to access a NetWare file system as if it is part of local file system on the UNIX workstation. Any client that supports the NFS protocol can access NetWare files using the NFS Server, if it is a trustee to one or more exported path.

  See Section 7.4, "NFS Server," on page 52.

- File Access Modes and Cross Protocol File Locking

  NFS Server is MP-enabled and supports the NetWare and independent modes of file access to maintain file and directory access security. It supports the cross-protocol file locking feature to ensure that a file is updated correctly before another user, application, or process can access it.

  See "File Access Modes" on page 53 and "NFS Server File Lock Manager" on page 59.

- Web-Based Administration for NFS Server

  iManager provides the web-based administration for NFS Server. Using this interface, you can start and stop NFS Server, update the umask value, export a new path, view and modify exported path properties, disable or delete an exported path.

  See "Managing NFS Server Using iManager" on page 84.

- Network Information Services

  NIS is a yellow pages service widely implemented in UNIX environments. NIS on NetWare acts as a central repository for NIS information by storing it as eDirectory objects that can be centrally maintained and administered.

  See Section 7.5, "Network Information Service," on page 60.

- UNIX User Management

  With the implementation of NIS over eDirectory, a single User/Group in the network contains both eDirectory and UNIX information. This brings up the user management to single point, namely eDirectory.

  See "UNIX User Management with eDirectory" on page 64.

- ConsoleOne® Administration for Network Information Services

  By using the ConsoleOne snap-in utility, you can administer and manage the NIS services.

  See Section 7.7, "ConsoleOne Administration," on page 65.

- iManager-Based Administration for Network Information Services

  iManager provides the Web-based administration for Network Information Services. Using this interface, you can migrate UNIX users and groups, set the Directory Access mode, and also modify NIS server settings.

  See Section 7.15.1, "iManager-Based Management for NIS Server," on page 89

- Cluster Services Support

To achieve high availability of services, Native File Access for UNIX can be run on Novell Cluster Services™.

See Section 7.16, “Cluster-Enabling Native File Access for UNIX,” on page 113.

- Upgrade Utility

  The upgrade utility helps retain the configurations of previous installations of NetWare NFS Services (versions 2. *x* and 3. *x*) during upgrade. Run the PERL upgrade script to upgrade the export file formats from previous versions of NetWare.

  See Section 7.9, “Upgrade Utility,” on page 67.

7.2 Overview of Native File Access for UNIX

Native File Access for UNIX provides an NFS Server that lets UNIX users access and store files on NetWare® servers. It is an implementation of the Network File System (NFS) protocol. The required software components are installed and run only on the NetWare servers; no additional software is required on the UNIX workstations. UNIX users attach to NetWare storage using NFS over the TCP/IP protocol.

The NSS file system is supported on NFS versions 2 and 3. NFS Server supports mount protocol versions 1, 2, and 3, NFS protocol versions 2 and 3, and Network Lock Manager protocols versions 1, 2, 3 and 4, and status monitor protocol over both UDP and TCP.

Native File Access for UNIX also provides complete Novell® eDirectory™ 8.7.3 enabled Network Information Services (NIS) which enables you to administer UNIX and NetWare users from a single point, namely eDirectory. NIS maintains its information in eDirectory and integrates the user information so that the eDirectory User object represents the NIS user.

Native File Access for UNIX has the following components and utilities:

- Section 7.4, “NFS Server,” on page 52.
- Section 7.5, “Network Information Service,” on page 60.
- Section 7.6, “User and Group Information,” on page 64.
- Section 7.7, “ConsoleOne Administration,” on page 65.
- Section 7.8, “Administration Utilities,” on page 66.
- Section 7.9, “Upgrade Utility,” on page 67.

7.3 Prerequisites

Before you start using Native File Access for UNIX, meet the following prerequisites for proper functionality.

- ❑ DNS is correctly configured.
- ❑ Novell eDirectory 8.0 or later is installed.

  This is required because NFS Server uses auxiliary classes. NFS Server does not load on a server in tree with NetWare 5.1 NDS 7 replica ring. For correct and complete functionality, the entire replica ring for all partitions specified in the NFS search_root, contexts must be on eDirectory 8.0 or later.

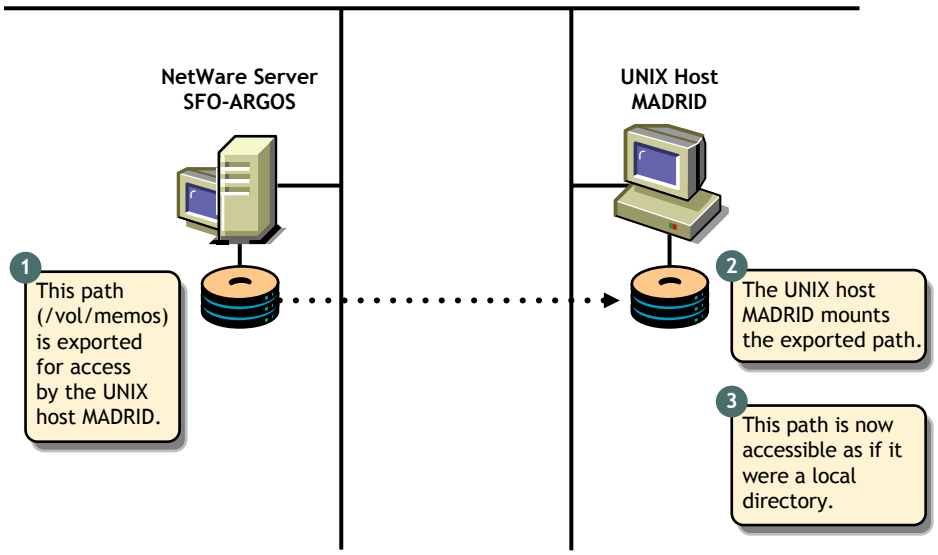
7.4 NFS Server

Network File System (NFS) Server enables UNIX users to access a NetWare file system as if it were a part of local file system on the UNIX workstation. Any client that supports the NFS protocol can access NetWare files using the NFS Server.

NOTE: Hard links and special files such as device files, named pipes, socket files are not supported in this release of NetWare NFS Server.

This section uses the UNIX operating system as the example when referring to the remote NFS client. The following figure shows an example of the NFS Server file sharing process.

Figure 7-1 *NFS Server Functionality*



NOTE: In this illustration, vol = NSS Volume on NetWare Server and memos = Directory inside vol, the NSS volume.

- Section 7.4.1, “Making NetWare File System Available to NFS Clients,” on page 52
- Section 7.4.2, “Accessing the NetWare File System from UNIX NFS Clients,” on page 53
- Section 7.4.3, “File Access Modes,” on page 53
- Section 7.4.4, “NFS Server File Lock Manager,” on page 59

7.4.1 Making NetWare File System Available to NFS Clients

Before UNIX users can access the NetWare file system, make it available to the UNIX workstations. This process is called *exporting* the file system. When exporting, you can define who should access the exported paths and how it is accessed by specifying the trusted systems and their level of access.

For example, you can restrict the access to specific UNIX hosts, and export the directory as Read-only.

7.4.2 Accessing the NetWare File System from UNIX NFS Clients

After exporting the NetWare file system from a NetWare server, mount the exported file system on the UNIX workstation for normal access. Mounting a NetWare file system from a UNIX workstation consists of the following:

- Creating a mount point

  A mount point is an empty directory that you create. This directory becomes the access point for the NetWare file system. When you select an existing directory as a mount point, the contents of the existing directory are not accessible until you unmount the remote file system.

- Mounting the NetWare directory

  Most UNIX systems use the `mount` command to mount a remote file system.

After these steps are complete, UNIX users can access the NetWare file system by accessing the local mount point. Different UNIX systems can use slightly varying options or user interfaces to mount a remote file system.

7.4.3 File Access Modes

The file access modes of Native File Access for UNIX enable you to maintain file and directory access security and help in mapping the trustee rights and attributes of NetWare to the UNIX file permissions.

Native File Access for UNIX provides the following file access modes:

- “Independent Mode” on page 53
- “NetWare Mode” on page 55
- “General Behavior Applicable to NetWare and Independent Modes” on page 59

In this section, the term *mapped user* refers to the eDirectory user with UNIX profile (UNIX UID / GID).

The term *unmapped user* refers to the eDirectory user without UNIX profile (UNIX UID / GID).

Independent Mode

This mode offers independent access control between NetWare rights and UNIX permissions without any interdependency between the two. No access mapping is required, and no mapping is done between UNIX file permissions and NetWare trustee rights or file attributes. The only mapping done is for the ownership of the file. The NetWare file owner becomes the UNIX file owner, and vice versa.

Independent mode is the default mode in which a path is exported.

Independent Mode Functionality

This mode functions as follows:

- NetWare trustees are not assigned.

- No mapping of RWX permissions to NetWare SRWCEMFA rights (Supervisor, Read, Write, Create, Erase, Modify, File scan, Access control) and vice versa is done.
- No NetWare attribute mapping is done.
- IRM is set to the default (SRWCEMFA).
- The NetWare OwnerID is mapped to the UNIX user on the NFS side.
- UNIX UID, GID, and UNIX permissions do not affect NetWare rights or attributes in any way.

The functions of this mode are outlined in the following table:

	Operation	NetWare Clients	NFS Clients
NetWare Side	Attributes - DI - RI - RO	- The DOS user cannot delete the file/directory. - The DOS user cannot rename the file. - The DOS user cannot write to the file.	The NFS user cannot delete file/ directory. The NFS user cannot rename the file. The NFS user can write to the file.
NFS Side	Creation	- OwnerID - The NetWare user is mapped to the NFS user creating the file. - IRM is the default SRWCEMFA. - No trustees are created for User/Group/Other. - No attributes are set according to UNIX permissions.	- UID/GID is set to whatever the file was created with. - File permission is set based on UNIX Umask.
	- chown - chgrp - chmod	- OwnerID does not change. - No change in the group trustee. - No change in attributes, IRM, or trustee rights.	- The UID is changed. - The GID is changed. - File mode is set based on permissions specified in the chmod command.

The following table outlines the mapped and unmapped user behavior of the file created from NetWare or UNIX.

	Mapped User Behavior	Unmapped User Behavior
File or directory is created from NetWare	◆ The NetWare FileOwner is set as the file creator. ◆ The UNIX UID is mapped to the NetWare FileOwner's UNIX UID. ◆ The UNIX GID is mapped to the NetWare FileOwner's primary group UNIX GID. ◆ File/directory permissions are set according to the umask specified. The default umask value is 022, which means: The file's permissions are rw-r--r-- The directory's permissions are rwxr-xr-x	The UNIX UID and GID are identified and set. If this fails, then the UID is set to 0 and the GID is set to1.
File or directory is created from UNIX	◆ The file's permissions are set according to the UNIX umask setting. ◆ The NetWare FileOwner is set to the mapped UNIX user.	The UNIX UID and primary GID of UNIX user is set as the UID/ GID of the file.

NetWare Mode

NetWare mode puts NetWare in control of UNIX permissions. Users who want greater control of file permissions on the NetWare side rather than NFS side must select the NetWare mode of access control.

The NetWare mode controls the rights of the files/directories when they are on the NetWare side and determines the user's rights to create or modify files on NetWare in a particular path.

This mode controls access to the exported NFS directory using NetWare access control methods such as NetWare rights and attributes. When using this mode, NFS permissions do not modify the settings of the NetWare rights and attributes.

To get the necessary UNIX permissions, make sure the user has necessary effective rights on the NetWare side.

World Object Behaviour

During the NetWare 6.5 install, the NFAUWorld group object is created by default and is located in the Server context. For NFS paths exported in NetWare mode, the effective rights of this object on the filesystem is used to compute and set the rwx permission for Others on UNIX side.

If the container where this object gets created has RWCEF NetWare rights to the file system, then by virtue of inheritance, NFAUWorld object also has those effective rights. This translates to rwx for Others on the UNIX side. This can be dangerous if not done intentionally because any user on UNIX side can wipe out the sub-directory structure.

If Others on the UNIX side are inheriting too many rights from containers above, use one of the following methods to restrict these:

- Remove file system rights from the containers above (parent container, grandparent, etc.) to prevent NFAUWorld from inheriting certain rights.
- Move the NFAUWorld object to another container which does not have those rights. However, when moving to another container, note that for NFS to find the NFAUWorld object, it has to be somewhere under a container listed as a SEARCH_ROOT context in sys:etc\nfs.cfg.
- Delete the NFAUWorld object, so Others will not get any permissions.

Export Option for NetWare Mode

The -nwmode option indicates if a particular path is exported in NetWare mode or not. If this is not specified, it is treated as an Independent mode export. If -nwmode is specified, the path is treated as being exported in NetWare mode.

For example:

```
/data -nwmode -rw -root
```

This exports the /data path in NetWare mode with read/write and root access.

NetWare Mode Functionality

This mode functions as follows:

- Trustees are not assigned and attributes are not mapped. [r-w-x] is not mapped to [SRWCEMFA].
- By default, IRM is set to SRWCEMFA.
- The default permissions for files created by UNIX users are based on the effective rights of the mapped NetWare user account.
- NetWare ownership of a file is determined by the mappings between eDirectory user object and its UNIX profile. The OwnerID (NetWare files) is mapped to the UNIX owner of the file.
- Files created from NetWare end by unmapped users have the UID set to 0.
- Touch command functionality is normal. In addition, it initiates a recomputation of permissions or owner change as required.
- Executing a chmod command reflects changes on the UNIX side only when the x (execute permission) for file is involved.

  The chmod commands allows setUID, setGID, and sticky bits to be set for a file or a directory and to be retained persistently between NetWare owner changes or permission recomputations.
- The chmod, chown, and chgrp commands have no effect on the NetWare rights and attributes of the file and they fail silently.

The functions of this mode are outlined in the following table:

	Operations	NetWare Clients	NFS Clients
NFS Side	Creation	◆ The Owner ID is mapped to the NetWare user. ◆ IRM is set to the default (srwcemfa). ◆ No trustees are created. ◆ No attributes are set based on FMode. ◆ GID is inherited from the parent directory	◆ The UID is set to Root. The UNIX user is mapped to Admin. ◆ The GID is set to whatever the file was created with. ◆ File mode is set.
	Modification ◆ chown ◆ chgrp ◆ chmod	◆ No owner ID or trustee change. ◆ No change in the group trustee. ◆ No attribute change. ◆ No trustee change. ◆ No IRM change.	◆ A UID change is not allowed. ◆ A GID change is not allowed. ◆ An FMode change is effective only for x.

Rights Mapping

The following table outlines the rights mapping for files, directories, and folders.

File / Directory	NetWare Right	Mapped UNIX Permission
File	Read	NFS Read (-r)
File	Write	NFS Write (-w)
Directory	Read and File Scan	NFS Read (-r) and Execute (-x)
Directory	Create and Erase set	NFS Write (-w)

TIP: You can set x, the NFS execute permission for a file, using the chmod command from the NFS client because there is no direct mapped attribute or effective right for an execute permission.

- The write permission is masked when the file/directory is read-only or the NetWare attribute is on.
- Read-only also sets the Rename Inhibit (RI) and the Delete Inhibit (DI) for the file and DI only for directory.
- Read-only files cannot be renamed or removed from NFS clients.
- Read-only folders cannot be deleted from NFS clients.

IMPORTANT: To ensure that Others in UNIX receive sufficient permissions see “World Object Behaviour” on page 55.

Refresh of Permissions

A refresh or recompute of the access permissions is done only in the following scenarios:

- When the UNIX or NetWare side detects a change of NetWare owner of a file or directory, the new owner's UnixUID is used and updated. The UnixGID and group permissions do not change.

  At times, the refresh of permissions because of the change in NetWare owner, trustees, or trustee permissions on the NFS Client might take some time as clients display the cached information. Updated information is available only when the client contacts the server for updated attributes and permissions.

- To enforce an immediate update of attributes, specify any one of the following commands, as required:

  ```
  touch *
  touch filename|directory_name
  touch.
  ```

  When you execute the touch command, the client receives the updated attributes from the NetWare NFS Server. This recomputes the permissions.

  In addition to the touch command, commands such as chown, chgrp, and chmod also initiate a recomputation of permissions even though the command itself might not be successful.

  For example, if the World Object has no permissions for a specific directory, you can give the Others Object r and x directory permissions by assigning Read and File Scan rights to the World Object.

The following table outlines the mapped and unmapped user behavior of the file created from NetWare or UNIX.

	Mapped User Behavior	Unmapped User Behavior
File or directory is created from NetWare	◆ When the file or directory created from the NetWare side is accessed for the first time from UNIX, the UNIX UID, UNIX GID, and permissions are determined and set. ◆ From the NetWare owner, the UnixUID and UnixGID of that user are picked up. This provides the NetWare group matching the UnixGID. ◆ Using the NetWare User, Group, and World objects, the r-w-x permissions for the User, Group, and Others are determined.	◆ When the file or directory created from the NetWare side is accessed for the first time from UNIX, the root-mapped user profile is set to the file/directory. ◆ The effective rights of the unmapped user along with World object determine the r-w-x permissions for User, Group, and Others.

	Mapped User Behavior	Unmapped User Behavior
File or directory is created from UNIX	◆ The UnixUID and UnixGID are used to find the matching mapped NetWare User and Group objects. ◆ Based on the effective rights of the mapped NetWare owner, mapped NetWare Group and World Group objects on the file or directory, the equivalent UNIX permissions are determined. ◆ Using this rights mapping, the read-write-execute (r-w-x) permissions for User, Group, and Others are determined.	◆ The effective rights and r-w-x permissions of User, Group and Others are based on the UnixUID and UnixGID of the root mapped User along with the World Group object.Therefore, the owner of the file/directory is set to root. ◆ The unmapped user gets permission to create files if World has rights to create a file/directory in that path. This removes the need to treat an unmapped user separately, and it is treated just as another user belonging to the Others category.

General Behavior Applicable to NetWare and Independent Modes

The following behavior is applicable to both NetWare and Independent modes:

- If the RI bit is set, rename fails.
- If the DI bit is set, remove fails.
- The execute (x) permission by itself is not enough for execution. The read (r) permission is also required.
- Symlinks have lrwxrwxrwx permissions. Operations such as chmod / setuid work on the linked file rather than on the symlink itself.

7.4.4 NFS Server File Lock Manager

When users share files, the system must provide a mechanism that prevents different users from making simultaneous changes to the same file. If there is not such a mechanism, two users can open one file at the same time. When this occurs, one user can overwrite the changes another user makes to the file, causing inconsistencies.

Both NetWare and UNIX systems control simultaneous file access using file locking. File locking ensures that a file is updated correctly before another user, application, or process can access it.

NetWare NFS Lock Manager file locking functions by setting advisory locks between NFS clients and is similar to the standard File Locking semantics on UNIX clients.

File locks are provided only when an application contacts the NetWare NFS lock manager. If an NFS user or process attempts to access a file through an application that does not contact the lock manager, no lock is issued. For example, if a UNIX user accesses a NetWare file using the vi editor, which does not contact the lock manager, no file lock is issued. If another UNIX user attempts to simultaneously access the same file, access is permitted and inconsistencies can occur.

However, this advisory nature of file locking is only between the NFS clients. The NetWare NFS Server synchronizes file locking by using both the NetWare and NFS lock managers. For cross-protocol file locking (simultaneous access using CIFS, or AFP), mandatory locking is enforced.

When a UNIX user accesses a NetWare file from an application that contacts the lock manager, the lock manager checks for existing file locks. If the NFS lock manager finds no existing locks on the file, it sets a lock on the file and file access is granted to the UNIX user. When a UNIX user attempts to access a file from an application that does not contact the lock manager, the request is sent directly to the NetWare server. If the NetWare lock manager finds no existing locks on the file, access is granted, but no lock is issued. Therefore, another UNIX user could access the file.

Byte-Range Locking

Two types of byte-range lock are used:

- **Exclusive Lock:** The locked byte range is read/write for the holder of the lock and deny-all for all others.

  A write lock on a byte range is acquired by an application that intends to write data into that byte range, and does not want other applications to be able to read or write to the byte range while it is accessing that byte range. A write lock on a given byte range is exclusive. It is grantable to only one requester at a time.

  A write lock denies other applications the ability to either read or write to the locked byte-range.

- **Shared Lock:** Also called an non-exclusive byte-range lock. The locked byte range is read-only for the holder of the lock and deny-write for all others.

  A read lock on a byte range is normally acquired by an application that intends to read data from the byte range, and does not want other applications to be able to write to the byte range while it is performing the read operation. A read lock on a given byte range is sharable, which means it is grantable to multiple requesters concurrently. However, it is incompatible with a concurrent write lock on the same byte range. A read lock denies other applications the ability to write to the locked byte range. In environments that implement advisory record locking rather than mandatory record locking, a read lock simply "advises" other applications that they should not write to the locked byte-range, even though they are technically able to do so.

7.5 Network Information Service

Network Information Service (NIS) software lets you administer both UNIX and NetWare from a single point, namely eDirectory.

NIS is a yellow pages service widely implemented in UNIX environments. NIS contains common information about users, groups, and hosts and other information that any client might require. This information could include a list of network hosts, protocol information, and even non-standard information that is likely to benefit from a centralized administration such as phone list.

NIS maintains its information in eDirectory and integrates the user/group information so that the eDirectory User/Group object also represents the NIS user/group. In the eDirectory enabled NIS, all NIS-related information is stored as eDirectory objects. The NetWare NIS can be set up to work in the various NIS configurations available.

NetWare Implementation of NIS: In the NetWare implementation of NIS, individual NIS Records, NIS Maps, NIS Domains, and NIS Servers are eDirectory objects with additional custom attributes defined to accommodate the NIS-specific information.

A typical UNIX system stores user account information in the /etc/passwd file and group information in the /etc/group file. The migration utility lets you migrate the user/group information to eDirectory. For more information on the migration utility, see Section 7.13, "Migrating NIS Maps," on page 72.

NetWare NIS is installed as part of the Native File Access for UNIX installation, and the NIS Server eDirectory object is created with the name NISSERV_ *ServerName* in the default (first) bindery context of the server or in the Server's eDirectory context.

This NISSERV_ *ServerName* is the main NIS Server eDirectory object. It maintains a list of all the NIS Domains it is serving. To view and edit the list:

1. Right-click the NISSERV_ *servername* object > Click *Properties*.
2. Click the Memberships tab to display the list of NIS Domains served by this NIS Server object.
3. Click the Others tab to view the IP address associated to *NISSERV_servername* object.

- Section 7.5.1, "NIS Information in eDirectory," on page 61
- Section 7.5.2, "Various NIS Configurations," on page 63
- Section 7.5.3, "UNIX User Management with eDirectory," on page 64

7.5.1 NIS Information in eDirectory

NIS Domain

The NIS services organizes nodes into administrative segments called *domains*. The NIS domain exists only in the local environment and usually covers a single network. A NIS domain is a hierarchical structure, so it is stored as a container in eDirectory. NIS does not impose any strict rules on domain naming; however, each domain must have a unique name.

An administrative NIS domain could be a company or a division of a company. Many administrators who use DNS prefer relating the NIS domain name to their DNS domain name, but this is not necessary.

NIS Maps

NIS stores all the common information pertaining to a domain as a set of NIS maps. Users can access the information in these NIS maps. In the eDirectory-enabled NIS, these maps are stored as containers under the NIS domain container. The migration utility lets you create the NIS maps under a specified domain.

The NIS Server supports both standard and custom maps.

Standard NIS Maps: Standard maps are created from the standard NIS text files.

The following standard maps are supported. They are classified according to the type of records that they contain.

- **Ethers Map:** A source of information about the Ethernet addresses (48-bit) of hosts on the Internet. The Ether objects (ieee802Device) store information about the Ethernet address and hostname.
- **Bootparams Map:** A source of information for various boot parameters. The Boot objects store information about the boot parameters of the various devices that are running. To migrate the Bootparams text filename from the ConsoleOne, name the text file to *bootp*.
- **Hosts Map:** Contains one entry for each IP address of each host. If a host has more than one IP address, it has an entry for each IP address. The Hosts objects store the IP address and hostname as distinguished values of CN, and aliases and nicknames are stored as other values of CN attributes.
- **Netgroup Map:** A source of information about Net Group parameters. It provides the abstraction of net groups.
- **Networks Map:** Contains a single object for each network. The Network objects store network names as distinguished values of CN, and aliases and nicknames are stored as other values of CN attributes.
- **Protocols Map:** Contains one object for each protocol. The Protocols objects store protocol names as distinguished values of CN, and aliases and nicknames are stored as other values of CN attributes.
- **RPC Map:** Contains one object for each Remote Procedure Call (RPC) program name. The RPC objects store RPC program names as distinguished values of CN, and aliases and nicknames are stored as other values of CN attributes.
- **Services Map:** Contains an object for each service. The Services objects store service names, ports, and protocols as distinguished values of CN, and aliases and nicknames are stored as other values of CN attributes.
- **Passwd Map:** Maintains the details of the users such as UID, Username, and home directory.
- **Group Map:** Maintains the details of the groups present such as GID, Group name, and Group members.
- **Ypservers Map:** Maintains a list of NIS slave servers which can serve the NIS domain.

Custom NIS Maps: You can use NIS to store any common configuration information that is valuable to NIS clients. Maps you create in addition to the standard NIS maps are called *custom maps*. For example, you can create an NIS map that provides an employee phone list.

You can create custom maps by creating a text file that contains the relevant configuration information. After creating the text file, you convert it into an NIS map through migration.

To create a phone list map, begin by creating a text file containing each employee's name and phone number.

An NIS map text file must conform to the following rules:

- Each data line begins a new entry key.
- The backslash character (\) at the end of a line appends the next line to the current line.

- The pound sign (#) at the beginning of a line tells the converter to ignore the line.
- Blanks separate the key and the value. Therefore, you must use underscores (_) to replace all other blanks within the key, such as the space between an employee's first and last names. Blanks are acceptable within the key values such as the phone list.

The following is an example of the phone list text file:

```
# This is the text file for the phone list map.

Janice_SmithMS 881-1456

Bob_RodriguezMS 235-6777

Eric_Mueller MS 769-8909
```

7.5.2 Various NIS Configurations

NIS can be configured in the following ways:

- "NIS Master Server" on page 63
- "NIS Slave Server" on page 63
- "NIS Client" on page 63

NIS Master Server

The master server is the true single owner of map data. It is responsible for all map maintenance and distribution to slave servers. After an NIS map is built on the master, the new map file is distributed to all slave servers for that domain, through the client-server relationship. You must, therefore, make all the modifications only on the master. The master maintains a list of slave servers within its domain in the form of a map named Ypservers.

NIS Slave Server

You can set up read-only copies of the NIS database on secondary servers. The secondary servers are referred to as *slaves*. When the server is set up as an NIS slave, it contacts the master NIS server and requests a complete copy of the NIS maps on that server.

After the slave server is set up, you do not need to manage the update process manually. The slave servers periodically query the master and request an update when the slave detects a more recent time stamp on the master. You can get an immediate update of the slave servers through ConsoleOne. A slave server can be added to the Ypservers map in the master.

We recommend that you set up at least one slave server for each NIS domain. The slave server can then function as a standby if the master server goes down, although it might not be necessary in all networks. Slave servers can be used for load distribution in the network. A master NIS server for one domain can function as a slave NIS server for another domain.

NIS Client

The NIS client enables users to query NIS map information from NIS servers.

For more information on setting up and managing NIS, see Section 7.15, "Managing NIS Server," on page 89.

7.5.3 UNIX User Management with eDirectory

With the implementation of NIS over eDirectory, a single user or group in the network contains both eDirectory and UNIX information. This brings the user management to single point, namely eDirectory.

For this purpose, the eDirectory schema has been extended and the relevant user information is placed in the eDirectory Library. The User object now stores UNIX information such as UID, GID, password, home directory, and shell in eDirectory.

By default, UNIX users or groups are looked for within the containers specified by the search_root parameter in the nfs.cfg configuration file. The search is recursive within the containers specified by this parameter. If the parameter does not contain any value, then the search is done under the default (first) bindery or servers context.

When a set of users or groups are migrated to eDirectory from a UNIX server, corresponding User/Group objects are created or updated in eDirectory. During migration, if the UNIX user or group does not exist, a new eDirectory User or Group object is created with default NetWare rights. If the User or Group object exists, the user or group's UNIX-related information is updated by default during the migration.

7.6 User and Group Information

Both NetWare and UNIX use the same User and Group objects to get the required information.

When a user or group makes a request to access one of the services, by default it searches for the User object on eDirectory. The services can be configured to look for users and groups from a remote NIS database.

- Section 7.6.1, "UNIX Users and Groups," on page 64
- Section 7.6.2, "UNIX Usernames, Group Names, and ID Numbers," on page 65
- Section 7.6.3, "User Home Directories," on page 65
- Section 7.6.4, "User Preferred Shells," on page 65
- Section 7.6.5, "Handling UNIX User Passwords," on page 65

7.6.1 UNIX Users and Groups

The user information includes the following:

- Username
- UNIX User Identification Number (UID)
- Home directory
- Preferred shell
- UNIX Group Identification Number (GID)
- Comments

The Group Information includes the following:

- Group name

- Group Identification Number (GID)
- Users present in this group

A typical UNIX system stores user account information in the /etc/passwd file and stores group information in the /etc/group file. You can migrate this data directly into eDirectory using the migration utility.

7.6.2 UNIX Usernames, Group Names, and ID Numbers

Each user uses a username to log in to the system. The UID identifies file and directory ownership information. The user's UID can be a number between 0 and 65,535, with the numbers 0 through 99 usually reserved. (0 is usually assigned to the Superuser.)

NFS group names have identification numbers. The range of numbers is between 0 and 65,535, with the numbers 0 through 99 reserved. The GID identifies the user as a member of the primary group identified by that GID.

7.6.3 User Home Directories

The home directory is the absolute pathname of the user's home directory on UNIX machines.

7.6.4 User Preferred Shells

The shell information identifies the path of the shell program that runs when the UNIX user logs in to the system. You can set the login account to run any program when a user logs in to the system, but the program typically creates an operating system working environment.

7.6.5 Handling UNIX User Passwords

The current implementation does not migrate the existing UNIX password field in the password map.

For information about UNIX user management, see Section 7.13, "Migrating NIS Maps," on page 72.

7.7 ConsoleOne Administration

You can use ConsoleOne to perform the following tasks:

- Configure the server's global parameters
- Configure and manage NIS services
- Configure error reporting
- Configure user and group UNIX information

For more information, see "ConsoleOne Configuration" on page 68.

7.8 Administration Utilities

The following administration utilities are provided with Native File Access for UNIX:

- Section 7.8.1, “SCHINST,” on page 66
- Section 7.8.2, “NISINST,” on page 66
- Section 7.8.3, “Manually Executing Administrative Utilities,” on page 67

7.8.1 SCHINST

The SCHINST utility runs automatically during the installation of Native File Access for UNIX.

This utility does the following:

- Extends the UAM schema necessary for storing the UNIX information of objects.
- Creates the NFAUUser object, and then adds the UNIX Profile of the root user as UID=0, GID=1, Home Directory=/
- Updates the NIS_ADMIN_OBJECT_CONTEXT parameter in nfs.cfg, the configuration file, with the context where the object is created or present.

All log messages that schinst generates are written to the sys:\etc\schinst.log file. You can view all information regarding schema extension in sys:\system\dsmisc.log.

The syntax is:

```
schinst -n -w
```

The SCHINST utility takes the administrator’s FDN and password as input for extending the schema.

7.8.2 NISINST

The NISINST utility runs automatically when Native File Access for UNIX is installed. It creates an eDirectory object with the name NISSERV_ *Servername* by default, or the name specified with the -s option.

The NIS Server uses this object to store the list of domain names served by the NIS Server. The NIS Server validates every request against the list of domains specified in this object. It serves the request only when the domain in the request is present in the list.

Run the NISINST utility manually, if the nisserver object is deleted.The syntax is:

```
nisinst [-s name] [-x context] [-i ip_address]
```

Parameter	Description
-s *name*	The name of the nisserver object. The parameter is optional.
-x *context*	The context where the object should be created in eDirectory. The parameter is optional.

Parameter	Description
-i *ipaddress*	The IP address to be attached to the NISServ Object. This option is useful in a cluster environment and for servers with multiple NIC cards. The parameter is optional.

7.8.3 Manually Executing Administrative Utilities

You need to manually run the administration utilities in any of the following situations:

- If you reinstall the directory services in the server.
- If you join the server to an existing tree.
- If the NFAUUser object is deleted

To manually run the administrative utilities:

1. Execute nfsstop.
2. Run SCHINST. The syntax is:

   ```
   schinst -n -w
   ```

   SCHINST takes the administrator's FDN and password as input for extending the schema.
3. Run `nisinst`
4. Execute `nfsstart`.

7.9 Upgrade Utility

The upgrade utility, nfauupg.nlm, is automatically invoked to upgrade the default configuration of NetWare NFS Services 2. *x* or 3.0 when you select Native File Access for UNIX while upgrading the operating system from NetWare 4. *x* or NetWare 5. *x* to NetWare 6. When invoked during installation, the upgrade utility retains the existing configuration in the new configuration files, nfs.cfg, nis.cfg, which are located in sys:\etc.

During installation, if the N4S schema is detected, then the UAM schema is extended automatically to support features such as multiple domain support, RFC2307 compliance for NIS, and starting and stopping NIS services from ConsoleOne.

- Section 7.9.1, "Upgrading Export Files from NetWare 5.1 / NetWare 6," on page 67

7.9.1 Upgrading Export Files from NetWare 5.1 / NetWare 6

At system console specify the following command:

```
perl sys:etc\NFS\NfsExportsUpgrade.pl
```

When you execute this Perl script, the export file format existing in NetWare 5.1 and NetWare 6 is converted to the NetWare 6.5 exports file format. The existing export paths from nfsexprt and nfsthost files are appended to `sys:etc/exports` file.

The files exported in Independent mode in the previous version are retained in the independent mode. However, the files exported in any other mode such as NFS-NetWare mode, NetWare-NFS mode are converted as NetWare mode.

If the export files from NetWare 5.1 and NetWare 6 are not available, then this command exits without doing anything.

7.10 Refreshing the Cache to update UNIX Profile

The ndsilib cache is refreshed after the timeout interval of two hours.To refresh the ndsilib cache instantly use the command line option `ndsilib cache refresh`.

7.11 Configuring and Managing Native File Access for UNIX

This section explains how to configure and manage Native File Access for UNIX Services. It includes information on the following:

- Section 7.11.1, “Configuration Methods,” on page 68

7.11.1 Configuration Methods

Configure Network Information Services either using ConsoleOne, or by setting the file-based configuration parameters of the various components.

ConsoleOne Configuration

Make sure that ConsoleOne 1.3.4 is installed on the server during the NetWare 6.5 install.

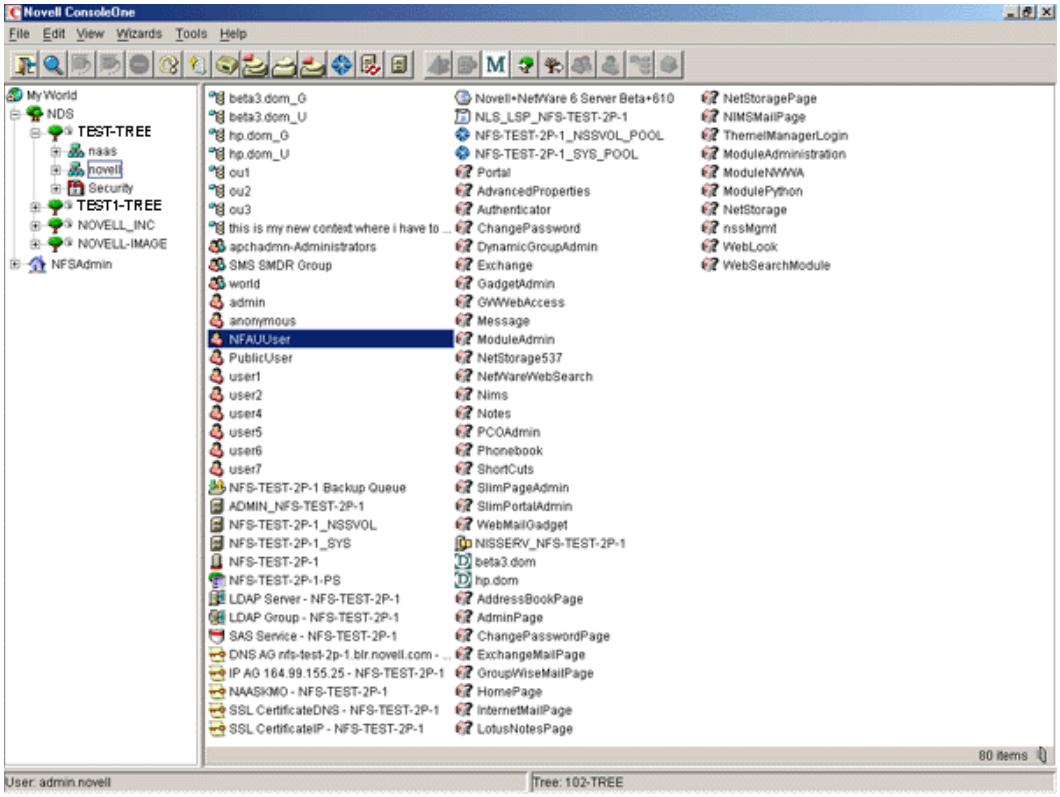
IMPORTANT: Before starting ConsoleOne, ensure that you run NFSSTART on the server that you want to administer.

To start ConsoleOne from the client:

1. Start ConsoleOne from the server where Native File Access for UNIX is installed.
2. Click *NFSAdmin*, then click the login toolbar icon.
3. Specify the tree name, context name, authorized username, and authorized password.
4. Click *OK*.
5. Specify the *hostname* or *IP address*, then click *OK*.

   IMPORTANT: To log in successfully, make sure that your file server name and hostname are the same and that you have logged in to the tree of the server you want to administer. Administering NetWare NFS Services 3.0 on NetWare 5.1 from ConsoleOne on NetWare 6 is not supported.

Figure 7-2 *Native File Access for UNIX Objects*



WARNING: After the Native File Access for UNIX installation, the objects NFAUWorld group object NFAUUser and NISSERV_Servername are created in the tree. Do not delete these objects.

File-Based Configuration

The configuration (.cfg) files are used to configure the services. All configuration files have the following format:

```
PARAMETER_NAME = VALUE
```

Within the .cfg files, a pound sign (#) indicates a comment.

In addition to these configuration files, there are specific files for exported volumes for the NFS Server and for the migration utility. All the configuration files are usually located in the sys:\etc directory. To configure the modules, change the required parameter value in the corresponding configuration file and restart the module.

7.12 Configuring Server General Parameters

The server general parameters required by Native File Access for UNIX are located in the nfs.cfg file. These parameters are common to NFS and NIS. When modifying this file, make sure to stop the services using `nfsstop` and restart using `nfsstart`.

- Section 7.12.1, “File-Based Configuration of Server General Parameters,” on page 70
- Section 7.12.2, “ConsoleOne Configuration of Server General Parameters,” on page 70

7.12.1 File-Based Configuration of Server General Parameters

The following table lists the configuration parameters in `nfs.cfg`.

Parameter	Default Value	Description
NDS_ACCESS	1	Lets you set the default access to eDirectory or NIS. To set the default access to eDirectory and retrieve all information from eDirectory, set this parameter to 1. (This is the default value.) Set this parameter to 0 to retrieve information from NIS server.
NIS_CLIENT_ACCESS	1	Lets you enable or disable NIS client. By default, NIS client access is enabled. To disable NIS client access, set this parameter to 0.
NIS_DOMAIN		Sets the NIS domain for NIS client access. No default can be provided.
NIS_SERVER		Provides the NIS server servicing the domain. If a specific server is needed for the domain, this parameter must be set. Otherwise, the NIS server is discovered using the broadcast. No default can be provided.
SEARCH_ROOT		Contains a list of fully distinguished names of containers separated by commas. These containers indicate where the search for users and groups should start. The NDSILIB module uses this parameter. The value can be either 25 containers or a string whose length should not exceed 2000 bytes, whichever is less. If you do not set any search containers, search starts from the default (first) bindery and then in the server's default context.

7.12.2 ConsoleOne Configuration of Server General Parameters

This section explains the following tasks:

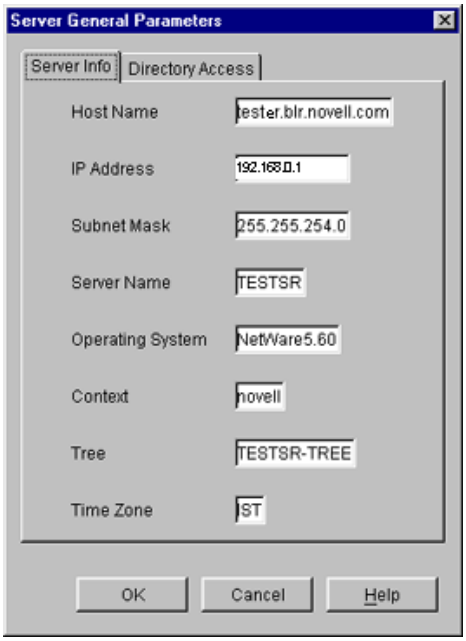
- “Viewing the Server General Parameters” on page 70
- “Configuring the Server General Parameters” on page 71

Viewing the Server General Parameters

1. In the ConsoleOne main menu, right-click *NFSAdmin*, select *Login to NFSAdmin*, then specify the IP address of the Server you want to administer.
2. Right-click the server object you want to configure, then select *NFSAdmin Properties*.

   The following dialog box appears:

Figure 7-3 *Server General Parameters Dialog Box*



These are the general parameters. The fields are read-only.

***Host Name*:** The name of the NetWare server.

***IP Address*:** The primary IP address of the NetWare server.

***Subnet Mask*:** The subnet mask that, when added to the IP address, provides the IP network number.

***Server Name*:** The name of the NetWare server.

***Operating System*:** The version of the operating system being used by the host.

***Context*:** The context or logical position of the server within the eDirectory tree.

***Tree*:** The current eDirectory tree.

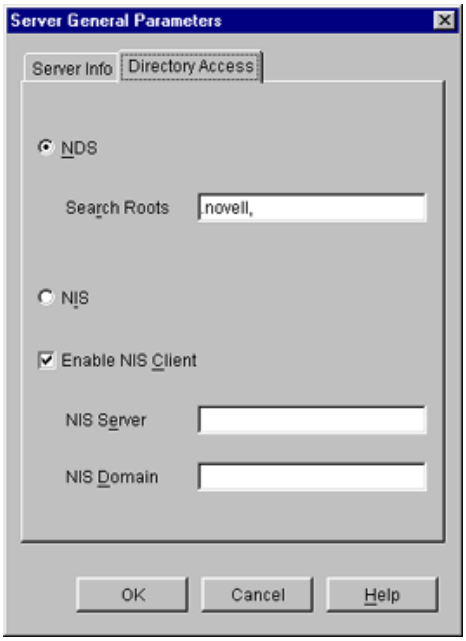
***Time Zone*:** The world time zone reference for your area. The time zone is used for time stamps and to set time synchronization. The time zone reference is set during the NetWare installation.

Configuring the Server General Parameters

1. In the ConsoleOne main menu, right-click *NFSAdmin*, select *Login to NFSAdmin*, then specify the IP address of Server to be administered.
2. Right-click the server object you want to configure, click *NFSAdmin Properties* > the *Directory Access* tab.

   The following dialog box appears:

Figure 7-4 *Server General Parameters - Directory Access Dialog Box*



This dialog box contains the parameters that can be configured to set the directory access of NetWare NFS Server.

3 Modify the following Directory Access parameters as necessary:

***NDS*:** Sets the access to eDirectory.

***Search Root*:** Lists the Fully Distinguished Name of containers from where the search should start for users and groups only. The names are separated by commas. Make sure that the parameter has valid values whenever the eDirectory structure changes.

***NIS*:** Enables remote NIS.

***Enable NIS Client*:** Specifies whether the NIS Client is enabled or not.

***NIS Server*:** Specifies the remote NIS server name.

***NIS Domain*:** Specifies the domain served by that remote NIS.

4 Click *OK*.

NOTE: Administering NetWare 5 NFS Services on NetWare 5 from ConsoleOne on NetWare 6 is not supported.

7.13 Migrating NIS Maps

If you already have a UNIX NIS Server (text-based) and you want the new NetWare NIS Server to serve the same data served by the old NIS server, copy all those text files into the specified location, then run the migration utility to create eDirectory entries for a specified domain.

The migration utility creates the Domain object in the default context as well as two other containers in the same context with the names *domainname*_U and *domainname*_G.

During migration, the utility searches for existing eDirectory users and groups under the containers specified by search_root, the configuration parameter (specified in `nfs.cfg`) and then, based on the migration option specified, modifies the UNIX information of those objects. If the objects are not found, the users are migrated to *domainname*_U and the groups are migrated to *domainname*_G. The rest of the data is migrated under the Map objects created under the Domain object.

IMPORTANT: The User and Group objects aren't created under the passwd and group Map object. They spread across the eDirectory tree and *DomainName*_U, *DomainName*_G depending upon the SEARCH_ROOT configuration parameter.

You can migrate maps using any one of the following three options:

- **UPDATE:** (Default) Updates all existing objects' information with the new information. If no objects exist, it creates new ones.
- **REPLACE:** Deletes all existing objects and creates new ones. For passwd and group maps, the old objects are not deleted. The UNIX profile of the objects does not change.
- **MERGE:** Retains all existing objects' information and logs them as conflicting records in the makenis.log file. If no objects exist, it creates new ones. The migrated users do not have UNIX passwords. To set the UNIX password, you need to log in as that NIS user from the NIS client run the YPPASSWD utility.

For more information on UNIX user management, see "UNIX User Management with eDirectory" on page 64.

- Section 7.13.1, "File-Based Migration," on page 73
- Section 7.13.2, "ConsoleOne Migration," on page 74
- Section 7.13.3, "Managing Users and Groups," on page 77

7.13.1 File-Based Migration

By default, migration uses the makefile sys:etc/nis/nismake, which contains the location of the text file for every map.

The syntax of the migration utility is:

```
makenis [-r resultfilename -[r]d domainname [-n context] [-f nismakefilename]
{[mapname -[l|b]p line or byte object in mapname]...}
```

NOTE: Use all options only in the specified order.

- To create a domain and migrate data or to use the existing domain object, use the following format:

  ```
  makenis -d domainname
  ```

  The *domainname parameter* is mandatory.
- To capture the results of the migration, use the following format:

  ```
  makenis -r resultfilename -d domainname
  ```
- To remove the existing domain data and then migrate, use the following format:

  ```
  makenis -rd domainname
  ```

- To specify the context where you want to create your Domain object and data, specify it as the *contextname*:

  ```
  makenis -d domainname -x contextname
  ```

  Edit the context parameter by prefixing each of the dots (.) in the Relative Distinguished Names with a backslash (\) to distinguish them from eDirectory names.

- To specify an NIS makefile other than the default sys:etc/nis/nismake, use the following format:

  ```
  makenis -d domainname -f makefilepath
  ```

  To specify the text files that you want to migrate, modify the NIS makefile. The NIS makefile is in the following format:

  ```
  map name    full path    parameters (if any)
  ```

  The comment character is the pound sign (#).

  If you do not specify anything, all the files in the makefile are migrated.

  For each map, specify the SECURE parameter so that only requests coming from secure ports are able to access the data. You can specify the migration options: UPDATE, REPLACE, or MERGE.

  For the Password map, you can specify two additional parameters: -u *uid* (which stops users with a UID less than a particular value from migrating to eDirectory) and AUTOGEN (which generates a UID from the program itself).

  You must specify the text file in the full path in DOS name format.

- To migrate specific maps, use the following format:

  ```
  makenis -d domainname mapname1, mapname2
  ```

- To migrate a map from a particular offset in a specified map text file, use the following format:

  ```
  makenis -d domainname mapname -lp lineoffset
  ```

  or

  ```
  makenis -d domainname mapname, -bp byteoffset
  ```

  Line offset is used to start migration from a particular line from the map text file. If the migration fails while migrating large maps, instead of migrating it again from the beginning, you can specify the byteoffset to start from the offset specified in the migration log file. For more details on this offset, refer to the description of the FILEMARK_LOG_FREQ configuration parameter in nis.cfg.

  Makenis adds users to the Members attribute, gives the user the rights equivalent to that of the group, and updates its Group Membership attribute.

7.13.2 ConsoleOne Migration

1. In the left pane of ConsoleOne, click The Network.
2. Select the server's tree where you want to manage the domains and maps.
3. Click the toolbar M icon.

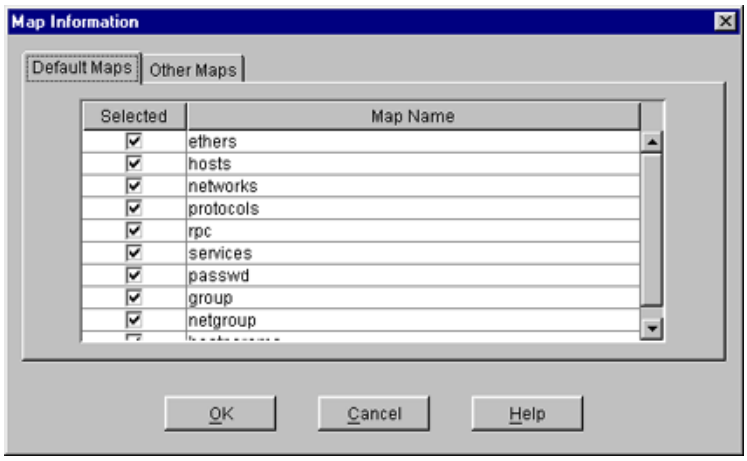
   The following dialog box appears:

Figure 7-5 *Migration Dialog Box*

4. Specify the *NetWare Host Name/IP Address*, *Domain Name*, and *Domain Context* to migrate a domain.
5. Select the *Set the Specified Host As Master Server* option to set the NIS Server as master for this specified domain.
6. In the Master Server Info section, select *Clear Existing Maps*, if you want to clear the existing maps.
7. Select the type of the migration you want to perform: *Replace*, *Update*, or *Merge*.
8. Specify the *Master Server Name/IP Address* in the Slave Server Info section to set the NIS Server as Slave Server.
9. Click *Migrate* to migrate the domain for default maps.

   The available default maps are ethers, hosts, networks, protocols, RPC, services, passwd, group, netgroup, and bootparams. By default, these files should be present in `sys:\etc\nis`.
10. Click *Advanced* to go to the Map Information dialog box to migrate the domain for specific maps.

Figure 7-6 *Map Information Dialog Box*

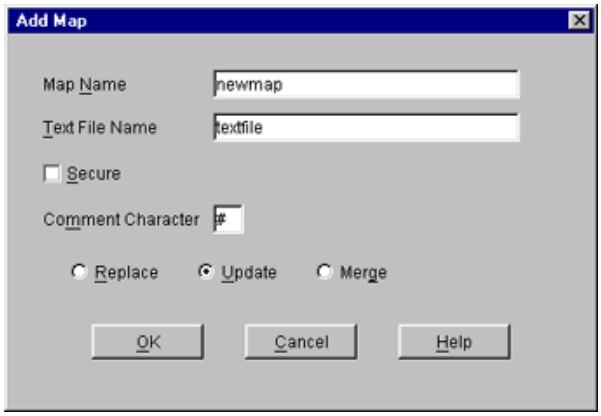


10a Click either *Default Maps* or *Other Maps*.

10b Select the desired maps from the list, deselect the maps you do not want to migrate, and click *OK*.

11 To modify an existing map or add a new map, click *Add* to go to the Add Map dialog box.

Figure 7-7 *Add Map Dialog Box*



11a Specify the *Map Name* and the *Text File name*.

11b (Conditional) Select *Secure* if you want to enable secure access to the map.

11c In the *Comment Character* box, specify the comment character present in the specified text file, then click *OK*.

The default comment character is the pound sign (#).

12 Click *Migrate*.

NOTE: When performing special map migration through ConsoleOne, you are required to give the complete path of the file. For example, `sys:etc\nis\phlist`.

7.13.3 Managing Users and Groups

You can add and modify the information of a User or Group object that already exists in eDirectory.

- "Modifying User Information" on page 77
- "Modifying Group Information" on page 78
- "Adding a New User or Group" on page 79
- "Managing Migration Utility Log Files" on page 79

Modifying User Information

1. In the left pane of the ConsoleOne main menu, click the eDirectory tree where the object resides.

   If you do not find the tree, click Novell Directory Services, select the tree and log in to it.

2. Double-click the container named *domainname*_U, where the User objects reside.

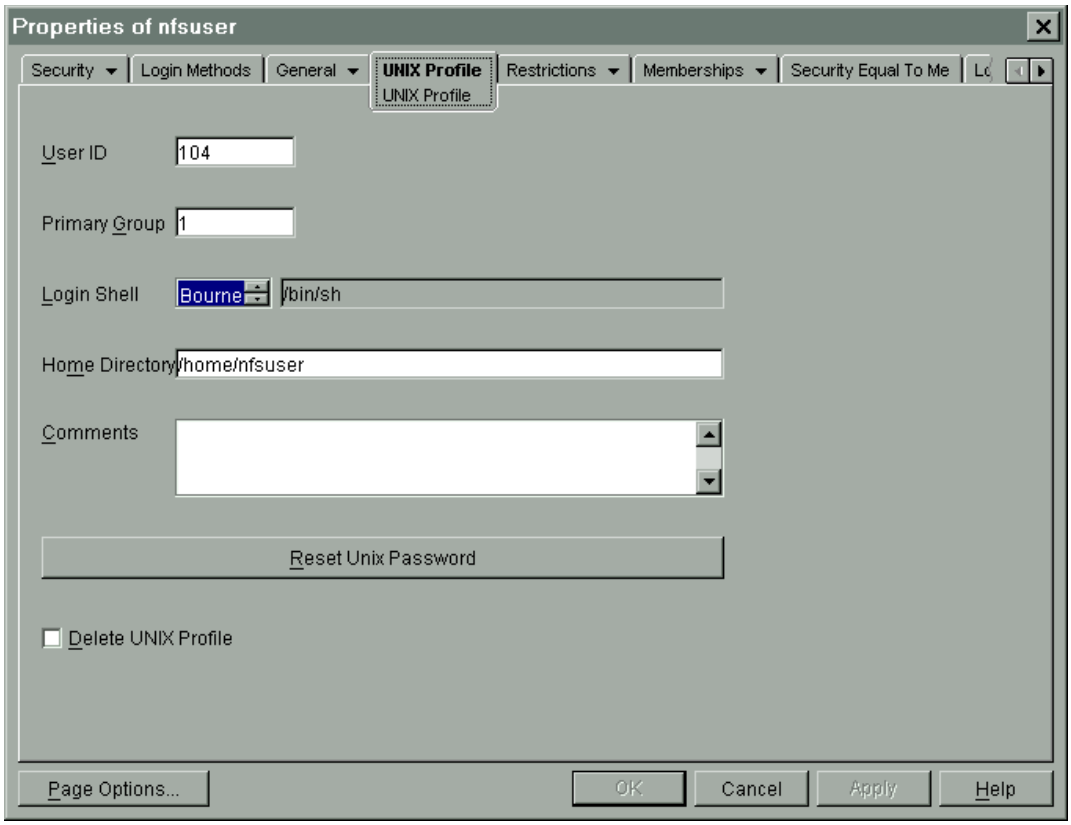
   The User objects under this particular container are displayed.

3. Right-click the User object whose properties you want to change, then click Properties.

   The following property page appears, displaying the various tabs that should be specified to add and modify the user information in eDirectory.

   All the tabs except the UNIX Profile tabs are standard forms.

Figure 7-8 *UNIX Profile Tab of User Properties Property Page*



4 Click UNIX Profile to modify the UNIX user profile, and specify the information in the following fields:

***User ID*:** The users' UNIX UID.

***Primary Group*:** The group ID (GID) of the group this user belongs to. To specify the GID of the user, click Browse and select the appropriate group.

***Login Shell*:** The preferred login shell of the user.

***Home Directory*:** The home directory the user wants to be placed in while logging in to the system.

***Comments*:** Any other comments that the user might want to specify.

***Reset UNIX Password*:** Use to reset the user's UNIX password.

5 Click *Apply*, then click *OK*.

Modifying Group Information

1 In the left pane of the ConsoleOne main menu, click the eDirectory tree where the object resides.

If you do not find the tree, click Novell Directory Services, then select the tree and log in to it.

2 Double-click the *domainname*_G container where the Group objects reside.

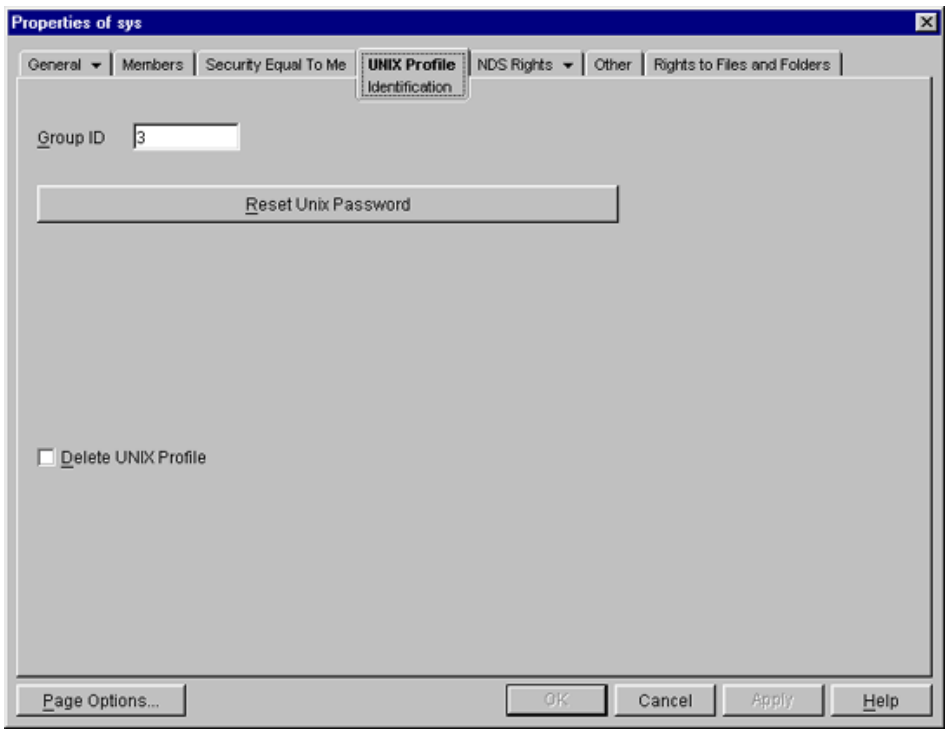
The groups under this particular container are displayed.

3 Right-click the Group object whose properties you want to change, then click Properties.

The following property page appears, displaying the various forms which should be specified to add and modify the group information in eDirectory.

All the forms except the UNIX Profile form are standard forms.

Figure 7-9 *UNIX Profile Tab of Group Properties Property Page*



4 Click the *UNIX Profile* tab and specify the following information to modify the UNIX group profile:

***Group ID*:** The group's UNIX GID.

5 Click *Apply*, then click *OK*.

Adding a New User or Group

To add a new user:

1 In the left pane of the ConsoleOne main menu, click the context where you want to add the new user.

2 Select *File* > *New*, then click *User*.

3 Provide the user information.

To add a new group:

1 In the left pane of the ConsoleOne main menu, click the context where you want to add the new group.

2 Select *File* > *New*, then click *Group*.

3 Specify the group information.

To make this newly added user or group an NIS User and NIS Group record, add the nisUserGroupDomain attribute to the object. This attribute holds a list of the domains to which that record belongs.

IMPORTANT: When you update a UNIX profile from ConsoleOne, execute NFSSTOP and NFSSTART, for NFS Server to get the modified UNIX information.

Managing Migration Utility Log Files

When you execute the makenis migration utility, the makenis.log log file is created by default in `sys:\etc\nis`. This file records messages that provide following information:

- The containers added, such as domainname container, domainname_U (for users), and domainname_G (for groups).
- The maps added and attached to the container.
- Parsing statistics for each map. For example, the number of records read, migrated, conflicts, and invalid records.
- Conflicting record details.

7.14 Managing NFS Server

This section discusses the following topics:

- Section 7.14.1, “Starting and Stopping NFS Server,” on page 80
- Section 7.14.2, “NFS Server Load Time Options,” on page 80
- Section 7.14.3, “NFS Server Console Commands,” on page 80
- Section 7.14.4, “Export Options,” on page 81

- Section 7.14.5, “Managing NFS Server Using iManager,” on page 84
- Section 7.14.6, “Administering NFS Server,” on page 85
- Section 7.14.7, “Managing the Exported Paths,” on page 86
- Section 7.14.8, “Exporting a New Path,” on page 87
- Section 7.14.9, “Editing Exported Path Properties,” on page 89

7.14.1 Starting and Stopping NFS Server

To start NFS Server: At the system console, specify

```
load xnfs
```

To stop NFS Server: At the system console, specify

```
unload xnfs
```

7.14.2 NFS Server Load Time Options

Load Time Option	Description
-Umask *octalvalue*	Umask refers to the file mode creation mask for default UNIX permissions. The default value = 022. Specify octal digits in the value range 000 to 777. Manually add -umask to the nfsstart.ncf for permanent changes.
-nodnscheck	Allows the IP addresses whose DNS name is not resolved in the export list. By default, it checks for the DNS resolution for the IP addresses. Manually add -nodnscheck to the nfsstart.ncf for permanent changes. This option weakens the security when identifying trusted hosts by their hosts names. When using this load time option, make sure that: Either **only** IP addresses / IP ranges are used to identify trusted hosts Or Use this option during testing phases when secure systems and data are not involved, and ease of testing is required. For example, not all test system names and addresses are resolvable in DNS, hosts files.

7.14.3 NFS Server Console Commands

The following table lists the NFS Server console parameters and their description.

Command	Description
?	Lists xnfs load time options
SHARE	Lists all shared paths
SHARE refresh	Refreshes the share list from exports file
SHARE /path ExportOptions	Shares a path dynamically
UNSHARE /path	Unshares a path shared using SHARE
MOUNT {stats}	Displays MOUNT protocol statistics
NFS {info|stats}	Displays NFS protocol info or statistics
LOCKD {info|stats}	Displays LOCK protocol info or statistics
TRACE {on|off|clr}	Turns on, turns off, or clears the NFS Trace screen
nodnscheck	Allows the IP addresses of those whose DNS name is not resolved, in the export list. By default, does will not allow as it was.Manually add -nodnscheck to the nfsstart.ncf for permanent changes. This option weakens the security when identifying trusted hosts by their hosts names. Therefore, when using this load time option, make sure that either **only** IP addresses / IP ranges should be used to identify trusted hosts or during testing phases when secure systems and data are not involved, and ease of testing is required. Because not all test system names and addresses are resolvable in DNS, hosts files.

7.14.4 Export Options

The NFS Server uses the exports file located in `sys:\etc`. The export file lets you export a path and specify export options and trusted hosts for the exported path.

You can upgrade the export files existing in NetWare 5.1 and NetWare 6 by executing the upgrade utility, as specified in “Upgrading Export Files from NetWare 5.1 / NetWare 6” on page 67.

The syntax for exporting a pathname is

```
/volumename[/dir1[/dir2...]] [/[-anon][-deny][-nwmode][-ro|-rw][-root]
```


- “Pathname Export Guidelines” on page 81
- “Updating the Exports List” on page 82
- “Export Option Examples” on page 83
- “Export Options Usage Guidelines” on page 84

Pathname Export Guidelines

- Always prefix the pathname with a slash (/). For example, `/nssvol`.
- The pathname can have up to 256 characters. It cannot be blank.

- Do not use an exclamation mark (!) in the pathname because it indicates a disabled path, and will not be exported.
- When exporting a path, the volume name is not case sensitive. However, any directory names in the path should exactly match the directory names that exist in the NFS (UNIX) name space.

  To view the name as it displays in the NFS (UNIX) name space, use NWAdmin, browse to the volume and to the folder, then select Details. You can view the name of the folder as it exists in every name space in the details.

  Alternately, on the Server Console, specify the following to get the UNIX namespace information:

  ```
  xnfs getinfo /volumename[/dir1[/dir2...]]
  ```
- When you do not specify any option, the export is not a valid one and the path will not be exported. It is mandatory to provide options.
- Use iManager or other Language (i18N) enabled editors to export paths in languages other than English.
- For more information on using the export options, see "Export Option Examples" on page 83, and "Export Options Usage Guidelines" on page 84.

Updating the Exports List

To update the exports list after manually modifying the exports file, execute the following command on the server console:

```
xnfs share refresh
```

Alternately, unload and reload xnfs.nlm.

The following table explains the various export options:

IMPORTANT: In the table, the term *host* refers to the IP address or the DNS name of the server.

Export Option	Description
-anon	Exports the pathname with rights for anonymous user access to the file system, based on Others' permissions. **WARNING:** Do not use this option when root access is given to all the clients.
-anon= host[:host]...	Exports the pathname with rights for anonymous user access **only** for the listed clients.
-deny	Denies the host all permissions so that the host cannot even mount. The host is added to the exports file with -deny token. When this is specified, all other access is disabled.

Export Option	Description
-nwmode	Indicates if a particular path is exported in NetWare mode or not. If -nwmode is specified, the path is treated as being exported in NetWare mode. If it is not specified, it is treated as an Independent mode export.
-ro = host[:host]	Exports the pathname with read-only rights **only** to the listed clients. The listed clients do not have root access.
-root	Exports the pathname with root access rights to all the clients.
-root = host[:host]...	Exports the pathname with root access rights **only** to the listed clients. No other clients have root access unless you specify the corresponding -ro or -rw options.
-rw	Exports the pathname with the read-write rights to all the clients.
-rw = host[:host]...	Exports the pathname with read-write rights **only** to the listed clients.The listed clients do not have root access.

Export Option Examples

Here are a few examples of using the export options:

In the example, nssvol is the NSS volume name and dir1, dir2, dir3 and dir4 are directories under nssvol that are exported using NFS Server with varying export options.

- To export the pathname with read-only rights without root and anonymous access (default):

  ```
  /nssvol/dir1 -ro
  ```

- To export the pathname with read-write and root access to all clients:

  ```
  /nssvol/dir2 -rw -root
  ```

- To export the pathname with read-only and root access to all clients:

  ```
  /nssvol/dir1 -ro -root
  ```

- To export the pathname with read-only to host1 and read-write and root access to host2:

  ```
  /nssvol/dir2 -ro=host1 -rw=host2 -root=host2
  ```

- To export the pathname with read-write access to all clients and enable anonymous access only for host6 and host7:

  ```
  /nssvol/dir3 -rw -anon=host6:host7
  ```

- To export the pathname with read-write and root access to host1 and host3, only read-write access to host2, read-only root access to host4, and anonymous access for all clients:

  ```
  /nssvol/dir4 -rw=host1:host2:host3 -ro=host4 -root=host1:host3:host4 -anon
  ```

Export Options Usage Guidelines

- Prefix all options with a hyphen (-). Do not put a space between the hyphen (-) and the first letter of the options.

  For example: `- ro` is incorrect, but `-ro` is correct.
- Do not use double quotes (" ") to separate the options.
- Use the colon (:) to separate multiple hosts when specifying the same option for the hosts.

  For example, to give read-only access to host1 and host2, use the following format:

  ```
  /nssvol -ro=host1:host2
  ```

  The following is incorrect:

  ```
  /nssvol -ro=host1 -ro-host2
  ```
- Do not specify the same option globally as well as for a client.

  For example, the following syntax is incorrect:

  ```
  /nssvol -ro -ro=host1
  ```
- When you specify the -ro, -rw, -root or -anon options for individual clients, these options override the global permissions for that client.

  For example, in

  ```
  /nssvol -ro -rw=host1
  ```

  host1 has read-write access even though other clients continue to have the global permission of read-only, and in

  ```
  /nssvol -rw -ro=host1
  ```

  host1 has read-only access even though other clients continue to have the global permissions of read-write.
- When you repeat the same entries with multiple options, then the later option overrides the previous option.

  For example, in

  ```
  /nssvol -ro=host1 -rw=host1
  ```

  host1 has read-write access.
- When you export a parent directory, the client can also mount the subdirectories. However, both the parent directory and subdirectory cannot be exported at the same time. When a subdirectory is already exported, you cannot export the parent directory and vice-versa.

  For example, when the exports file has the following two entries

  ```
  /nssvol/dir1 -rw=host1 -root=host4:host5
  ```

  ```
  /nssvol -rw -root
  ```

  then you cannot export /nssvol (the parent directory) because /nssvol/dir1, (the subdirectory) is already exported.

For more information on NFS Server, see Section 7.4, “NFS Server,” on page 52.

7.14.5 Managing NFS Server Using iManager

You can perform the following administrative tasks using the iManager:

- “Starting and Stopping NFS Server” on page 80

- "Managing the Exported Paths" on page 86
- Section 7.15.1, "iManager-Based Management for NIS Server," on page 89
- "Exporting a New Path" on page 87
- "Editing Exported Path Properties" on page 89

Meet the following requirements for NFS Server Administration gadget to be installed in iManager.

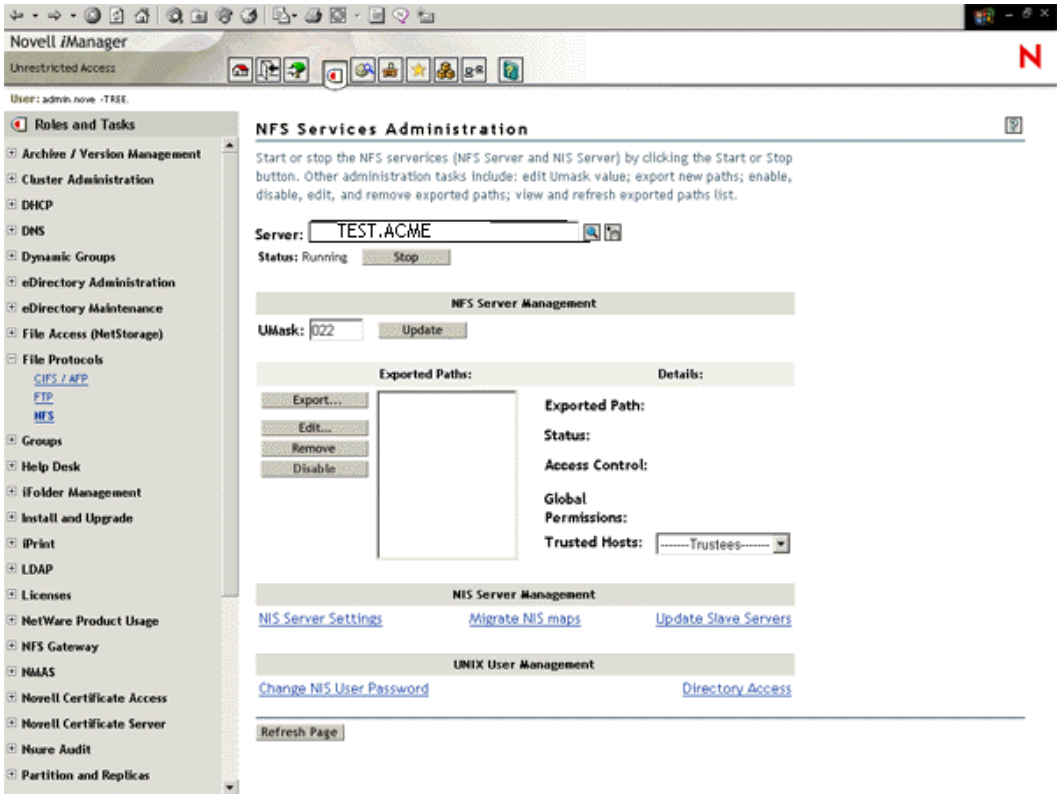
- ❑ The Apache Web Server is selected during NetWare 6.5 install.
- ❑ iManager 2.5 is selected during the NetWare 6.5 install.

  For more information about installing iManager 2.5, refer to the Installing Novell iManager section in the *Novell iManager 2.5 Installation Guide* (http://www.novell.com/documentation/imanager25/index.html?page=/documentation/imanager25/imanager_install_25/data/hk42s9ot.html#bktitle).

7.14.6 Administering NFS Server

1 In iManager, click `File Protocols > NFS Server` to view the NFS Services Administration page.

Figure 7-10 *NFS Services Administration Page*



2 Click the Object selector to select the server on which you have to administer the NFS Server.

3 ***Starting / Stopping NFS Services*:** Click Stop or Start as required.

  The Stop button displays when the NFS Server is running. The Start button displays when the NFS Server is not running.

4 ***NFS Server Management*:** Specify the umask value and click Update. Specify octal digits in the value range 000 to 777.

The default value = 022. Umask refers to the file mode creation mask for default UNIX permissions.

5 ***Exported Paths*:** Displays all valid enabled and disabled exported paths in the exports file located at `sys:\etc`.

Command-line shared entries, prefixed with (Shared) are also displayed. These entries are typically exported cluster enabled paths in Active/Active cluster configuration and correspond to the command line share entries present in the load script of cluster resources.These entries cannot be modified. If you stop and start NFS Server either from user interface or the Server console, then the shared entries are not available. Share them afresh using the command line.

elect an exported path in the Exported Paths list to perform operations such as exporting a new path, editing, enabling or disabling, removing, and refreshing the exported paths.

6 ***NIS Server Management*:** Click *NIS Server Settings*, *Migrate NIS Maps* or *Update Slave Servers* as required.

For more details, see Section 7.15.1, “iManager-Based Management for NIS Server,” on page 89.

7 ***UNIX User Management*:** Click *Change NIS Password* or *Directory Access* as required.

For more details, see Section 7.15.1, “iManager-Based Management for NIS Server,” on page 89.

7.14.7 Managing the Exported Paths

1 In the Exported Paths list of the NFS Services Administration page, view the list of exported paths.

2 Select a path in the Exported Paths list to view path details such as the Exported path, Access Control Mode, Global Permissions, and Trusted hosts.

3 Select a path in the Exported Paths list to manage the exported paths.

Command-line shared entries, prefixed with (Shared) are also displayed. These entries are typically exported cluster-enabled paths in Active/Active cluster configuration and correspond to the command line share entries present in the load script of cluster resources. These entries cannot be modified. If you stop and restart NFS Server either from the user interface or the Server console, then the shared entries are not available. Share them afresh using the command line.

You can perform operations such as exporting a new path, viewing or modifying, enabling or disabling, refreshing, and removing the exported paths.

- “Exporting a New Path” on page 86
- “Editing Path Properties” on page 87
- “Removing a Path” on page 87

Exporting a New Path

Click Export to display the Export Options page, where you can export a new path. For details, refer to “Exporting a New Path” on page 87.

Editing Path Properties

Click *Edit* to display the *Export Options* page, where you can view or modify the properties of an exported path. For details, refer to “Editing Exported Path Properties” on page 89.

Removing a Path

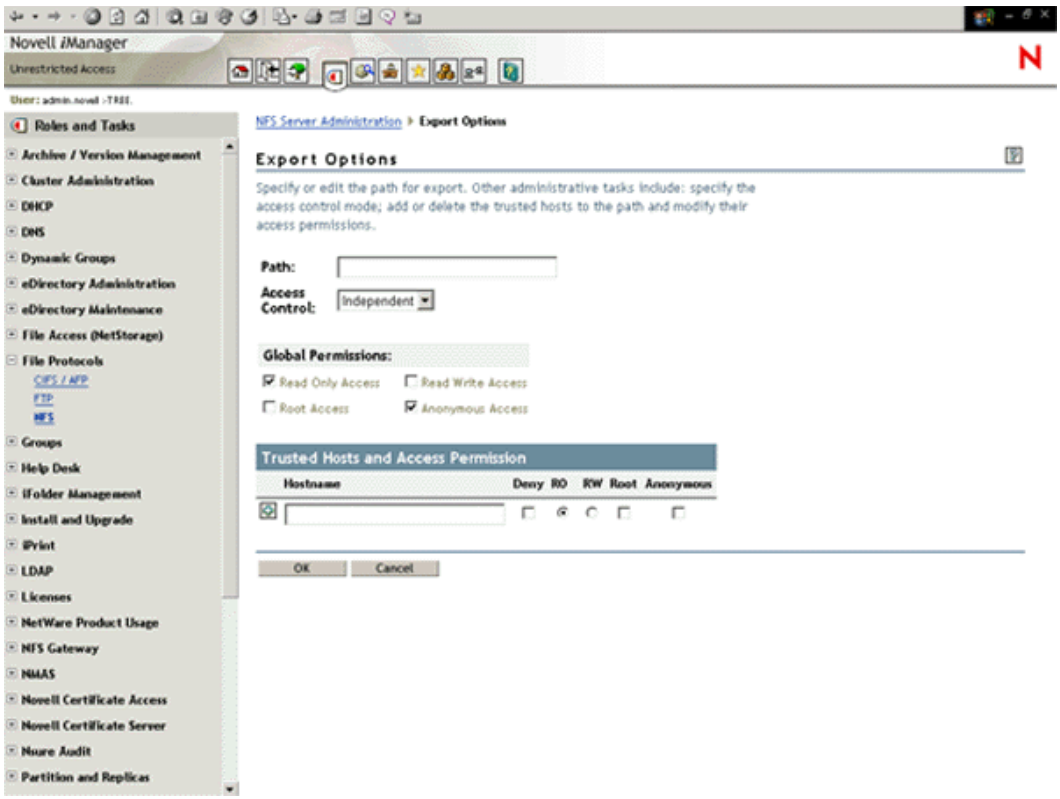
Click *Remove* to remove the exported path.

This removes the path from the `sys:/exports` file, and saves and refreshes the changes on the server side.

7.14.8 Exporting a New Path

1 In the *NFS Server Administration* page, click *Export* to display the *Export Options* page.

Figure 7-11 *Export Options Page*



2 In the Path field, specify the path in the format */volumename*[/dir1[/dir2...]].

3 In the Access Controls field, select the Independent or NetWare modes of access control mode from the drop-down list.

Default mode = Independent.

For more information on Independent and NetWare modes of access, see “File Access Modes” on page 53.

4 In the Global Permissions section, assign the required access permissions to the trusted host. The default permissions, Read Only access and Anonymous access, are selected by default.

When you add a trusted host for the exported path and give it RO/RW, Root, or Anonymous access in the Trusted Hosts table, then the corresponding global access check box is disabled (deselected). If there are no trusted hosts with this access, the global access permissions are restored.

- Select *Read/Write* to give read/write access to the trusted hosts. This access is denied by default.
- Select *Root* access to give root access to the trusted hosts. This access is denied by default.
- Deselect *Anonymous* access to deny anonymous access to the trusted host. This access is given by default.

5 In the Trusted Hosts and Access Permissions section, specify the hostname that you want to make a trusted host for the exported path.

The trusted hostname cannot have null or special characters. The trusted hostname can have up to 256 characters.

You can specify trusted hostnames in the following formats:

- Individual hosts based on complete or short DNS name or IP address.
  - The IP address. For example,

    aaa.bbb.ccc.ddd.
  - Complete or short DNS name. For example,

    xyz or xyz.us.acme.com
- A complete DNS domain, or a subnet based on network number.
  - DNS domain is distinguished from a complete DNS hostname by a prefixed dot (.). For example, to trust all the hosts in the us.acme.com DNS domain, specify

    .us.acme.com
  - The network or subnet component is prefixed by an at sign (@). For example, to trust all hosts in the 129.144.255 network, specify

    @129.144.255

    If the network prefixes are not byte-aligned, the syntax allows a mask length to be specified explicitly following a slash (/) delimiter. For example, to mask the 22 leftmost contiguous significant bits in the corresponding IP address (for example, for a subnet with net number 129.144.132 and net mask 255.255.252.0), specify

    @129.144.132/22

6 Click the Add symbol (+) to add the host to the trusted host list.

7 Select the *Deny*, *RO* (Read-Only), *RW* (Read-Write), *Root*, or *Anonymous* check boxes as required.

After this, you can add another host to the trustee list.

8 Click *OK* to save the modifications and return to the NFS Server Administration page, or click *Cancel* to cancel the modifications and return to the NFS Server Administration page.

This updates the `etc/exports` file on the server and refreshes the NFS Server. When you specify access permissions, the default permissions given in the All row are unchecked.

7.14.9 Editing Exported Path Properties

1. In the NFS Server Administration page, click Edit after selecting the path from the Exported Paths list.

   This displays the Exports Options page, where you can view and modify the properties of the exported path.
2. In the Path field, browse or edit to modify the pathname.
3. Update the access control mode. You can do this by selecting NetWare or Independent as required from the Access Control Mode drop-down list.
4. Update access permissions for the trusted hosts. For information on assigning access permissions, refer Step 4 on page 87.
5. Add the trusted hosts. For information on adding trusted hosts, refer Step 5 on page 88.
6. Click the Add symbol (+) beside the text box to add the host to the trusted host list.
7. Click the *Delete* symbol (X) beside the text box to delete the trusted host.
8. Click *OK* to save the modifications and return to the NFS Server Administration page, or click *Cancel* to cancel the modifications and return to the NFS Server Administration page.

7.15 Managing NIS Server

There is an NIS Server object in eDirectory called NISSERV_ *Servername*, which is created during installation. The migration utility adds the domain details to this object when a domain is migrated. NIS Server services the list of domains present in this object.

For every user moved, NIS Server updates the user's Group Membership attribute and gives rights equivalent to that of the Group.

For more information about NIS, see Section 7.5, "Network Information Service," on page 60.

This section includes the following:

- Section 7.15.1, "iManager-Based Management for NIS Server," on page 89
- Section 7.15.2, "File-Based Management for NIS Server," on page 95
- Section 7.15.3, "ConsoleOne Management for NIS Server," on page 98

7.15.1 iManager-Based Management for NIS Server

You can perform the following administrative tasks using iManager:

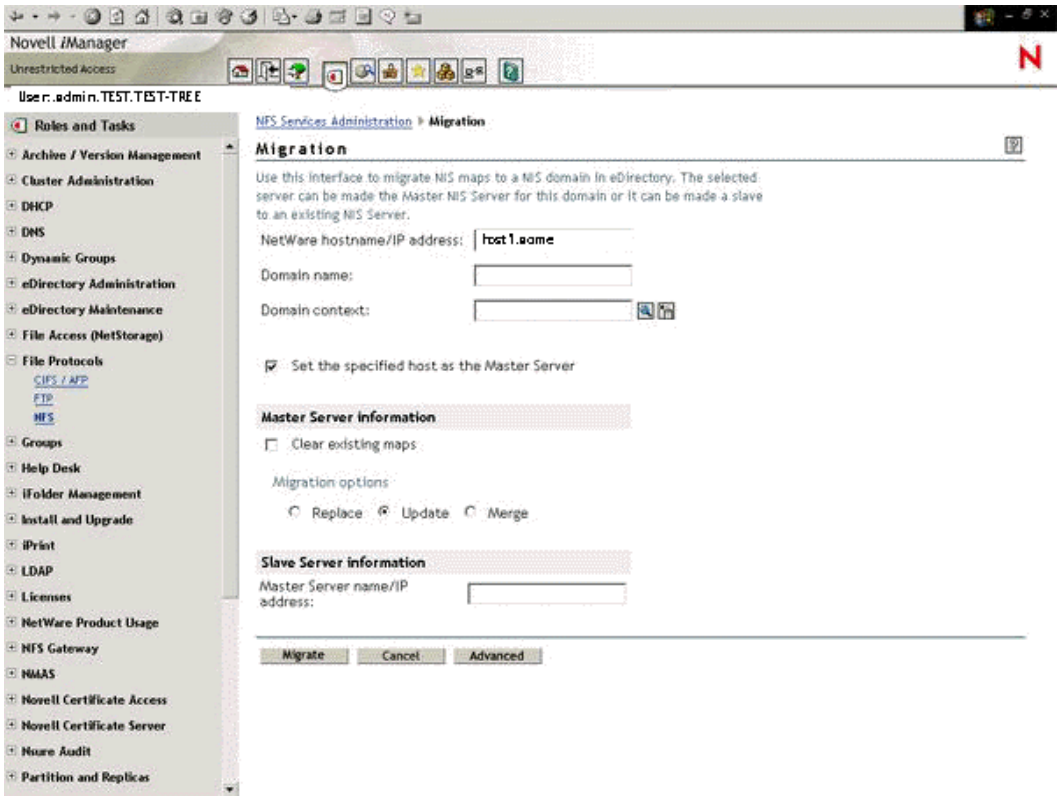
- "Migrating NIS Maps to eDirectory" on page 90
- "Directory Access" on page 91
- "Modifying NIS Server Settings" on page 92
- "Updating Slave Servers" on page 93
- "Changing NIS Passwords" on page 94

In iManager, click *File Protocols* > *NFS Server* to view the NFS Services Administration page. Use the object selector to select the server.

Migrating NIS Maps to eDirectory

1 On the NFS Services Administration page, click *Migrate NIS Maps* in the NIS Server Management section to display the Migration page.

Figure 7-12 *NIS Maps Migration Page*



This page lets you set the parameters to migrate the NIS maps to eDirectory.

2 Make the changes as required.

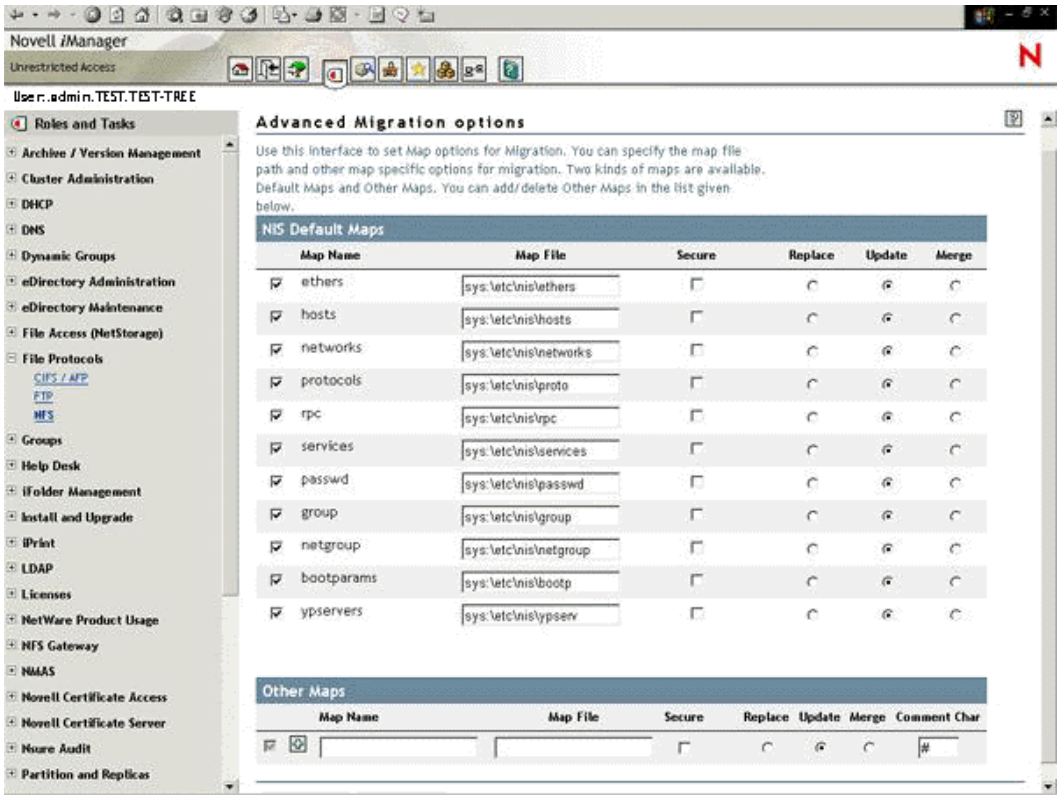
Refer to the online help for details on parameters.

3 Do one of the following:

- Click *Migrate* to migrate the domain for default maps. The default maps are ethers, hosts, networks, protocols, rpc, services, passwd, group, netgroup, bootparams, and ypservers.
- Click *Cancel* to cancel the modifications and return to the NFS Services Administration page.

4 (Optional) Click *Advanced* to display the Advanced Migration Option page where you can set map options for migration.

Figure 7-13 *Advanced Migration Options*



Use this page to add new or edit properties NIS default maps as well as other maps.

4a Make the changes as required.

Refer to the online help for details on parameters.

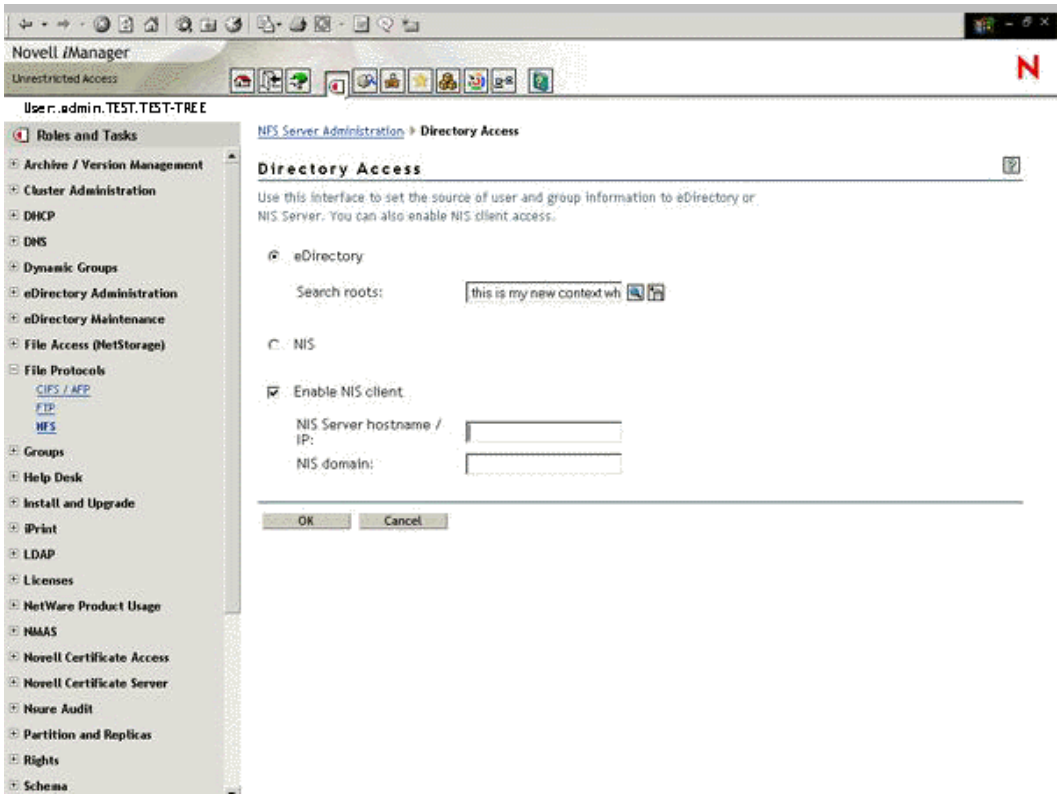
4b Do one of the following:

- Click *OK* to saves the changes made in this page for migration, then return to the Migration page.
- Click *Cancel* to discard the changes made in this page, then return to the Migration page.

Directory Access

1 On the NFS Services Administration page, click *Directory Access* to display the Directory Access page.

Figure 7-14 *Directory Access Page*



This page lets you set the source of user and group information to eDirectory or NIS Server. You can also enable NIS client access.

2 Make the changes as required.

Refer to the online help for details on parameters.

3 Do one of the following:

- Click *OK* to update the `sys:\etc\nis.cfg`.

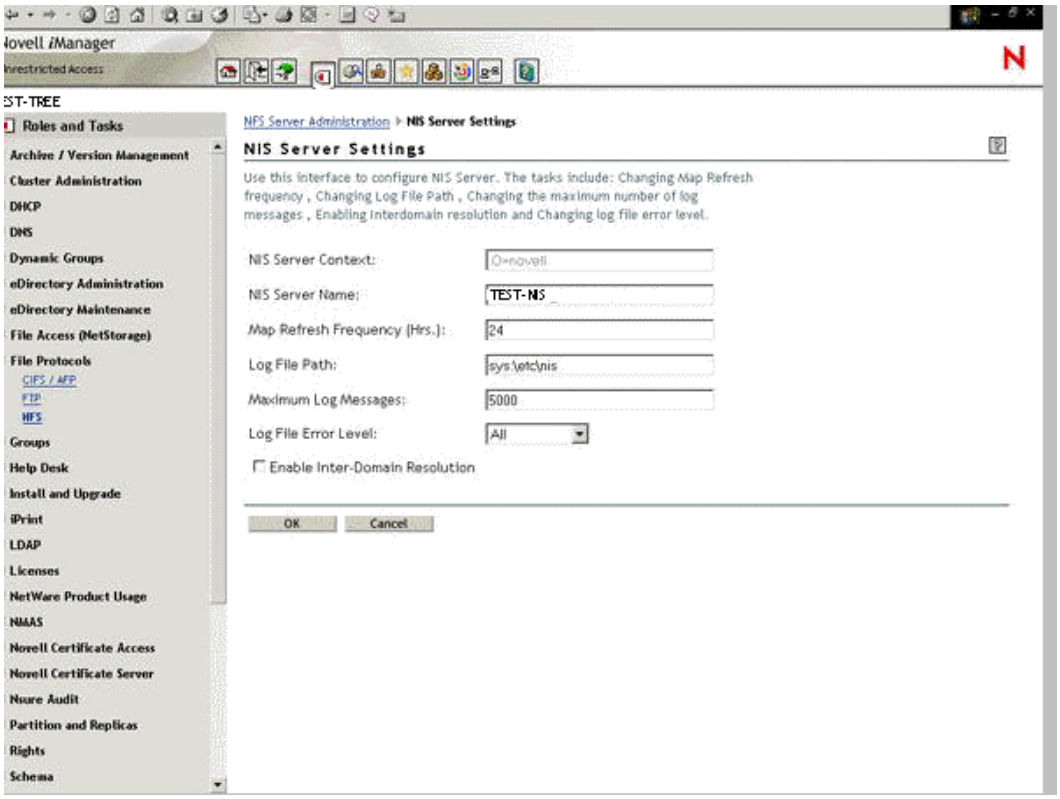
  If NISBIND is running on the server and NIS Domain and NIS Server Hostname/IP were specified, then ypset is executed on the server to change the NIS bindings to the specified domain and server. If the specified NIS server is running and serving the specified domain, NISBIND is bound to that server for the specified domain. For status of the ypset execution, see the server logger screen.

- Click `Cancel` to cancel the modifications you made and return to the NFS Services Administration page.

Modifying NIS Server Settings

1 On the NFS Services Administration page, click *NIS Server Setting*s to display the NIS Server Settings page.

Figure 7-15 *NIS Server Settings Page*



Use this page to modify the general configurable parameters of NIS Server, such as the map refresh frequency, log file path, maximum number of log messages, enabling Interdomain resolution, and changing the log file error level.

2 Make the changes as required.

Refer to the online help for information on parameters.

3 Click *OK* to update the `sys:\etc\nis.cfg`.

Or

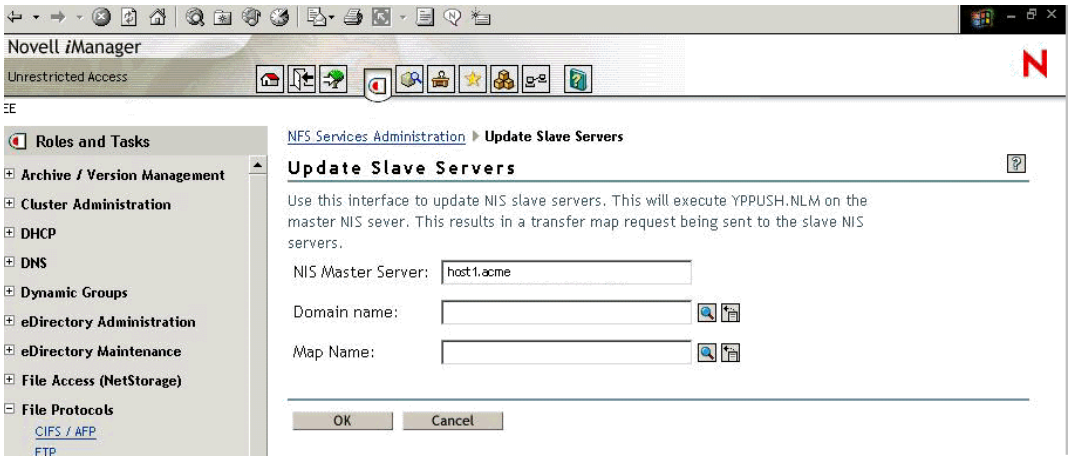
Click *Cancel* to cancel the modifications you made and return to the NFS Services Administration page.

4 For the changes to take effect, stop and start NFS Services on the NFS Services Administration page.

Updating Slave Servers

1 On the NFS Services Administration page, click *Update Slave Servers* to display the Update Slave Servers page.

Figure 7-16 *Update Slave Servers*



Use this page to update NIS Slave servers by executing the yppush utility on the Master NIS Server.

2 Make the changes as required. Refer to the online help for information on parameters.

3 Click *OK* to execute the yppush utility and then returns you to the NFS Services Administration screen.

The yppush utility copies a new version of the named Network Information Service (NIS) map from the master NIS server to the slave NIS servers. The yppush utility is normally run only on the master NIS server after the master databases are changed and the change has to be updated in the NIS slave servers immediately. The yppush utility first constructs a list of NIS slave server hosts by reading the NIS map ypservers within the same domain, then a transfer map request is sent to the slave NIS server on each host.

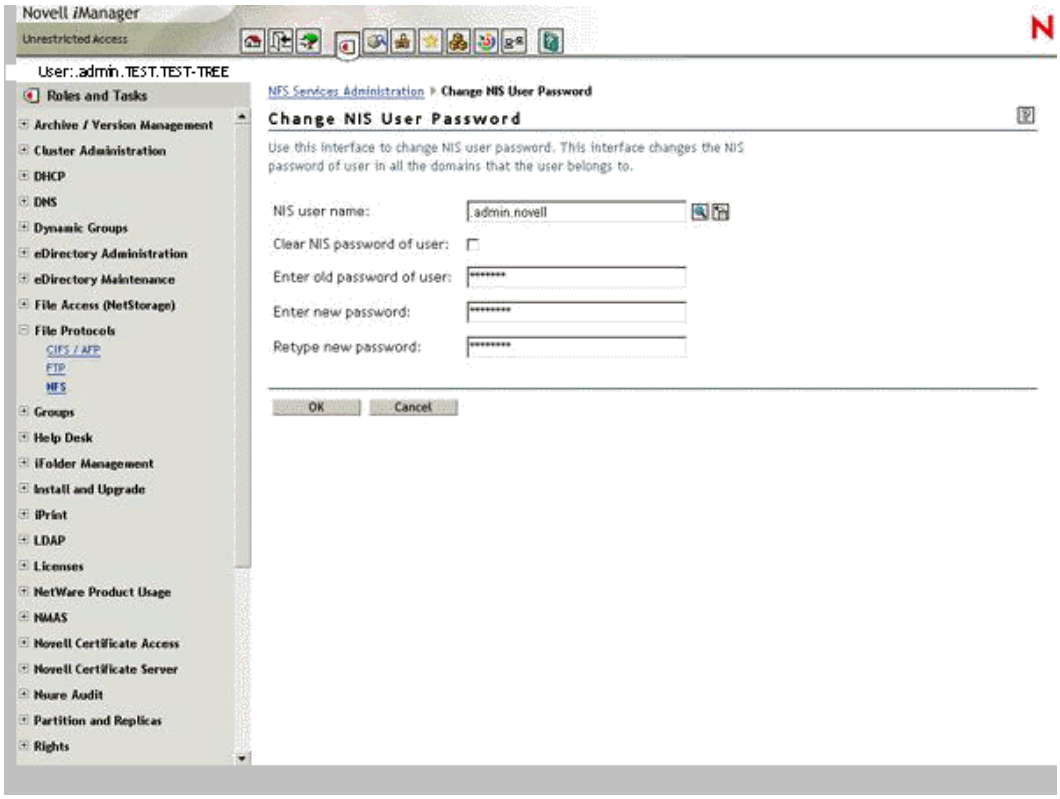
Or

Click *Cancel* to discard the modifications you made and return to the NFS Services Administration screen.

Changing NIS Passwords

1 On the NFS Services Administration page, click *Change NIS Password* to display the Change NIS User Password page.

Figure 7-17 *Change NIS User Password*



Use this page to change the password of a user in all the domains that the user belongs to.

2 Make the changes as required.

Refer to the online help for information on parameters.

3 Click *OK* to read the list of domains the user belongs to from eDirectory, change the user password all those domains, then return to the NFS Services Administration screen.

Or

Click *Cancel* to discard the modification you made, and then return to the NFS Services Administration screen.

7.15.2 File-Based Management for NIS Server

- "NIS Server Configuration Parameters" on page 95
- "Setting Up a NetWare Server As a NIS Master" on page 96
- "Setting Up a NetWare Server as NIS Slave Server" on page 97
- "Setting Up a NetWare Server As a NIS Client" on page 97
- "Setting Password of NIS User" on page 98

NIS Server Configuration Parameters

The configuration parameters required for NIS Services are available in the nis.cfg file. The following table lists the parameters in nis.cfg.

Parameter	Default Value	Description
NIS_SERVER_CONTEXT		The eDirectory context where the NIS server object is created. It holds all the domain FDNs, and the NIS server reads the domains from here.
NIS_SERVER_NAME		The name by which the NIS server is referenced. By default, the NISINST utility creates an object named NISSERV_ *ServerName*.
INTERDOMAIN_RESOLUTION	0	Specifies whether interdomain resolution is allowed or not. If allowed, DNS is contacted for hostname resolution even if NIS is not running. This is used for host maps only.
FILEMARK_LOG_FREQ	100	Puts the file in the log after parsing the specified number of records. This is used by the migration utility when the administrator wants to migrate maps that have large records. After transferring a number of records successfully, an index is maintained. If a transfer breaks, it can start from the index kept previously.
LOG_FILE_PATH	`sys:etc\nis`	The path in the NetWare server where you want to write the log file for migration.
MAX_LOG_MSG	5000	Upper limit of number of log messages that can be logged. The information is specific to each log file. By default the last 5000 messages are displayed. If the number of log messages is set to *n*, the last *n* messages are retained.
NIS_LOG_LEVEL	7	The log level indicates the types of messages to be logged. You can either select one of these or a combination of these. To get the combination, add two or more log levels. For example, to get Error and Information Messages, set the Log level to, 5= (1+4). By default, you get all the messages.
MAP_REFRESH_DEFAULT	24:00:00	Specifies the default time interval for refreshing the maps by synchronizing the maps in the slave server with the master.
NIS_ADMIN_OBJECT_ CONTEXT		The context where the NIS Admin object is created.

Setting Up a NetWare Server As a NIS Master

1 Copy the NIS-related text files required for the domain (they are available in /etc in UNIX) from the UNIX machine into `sys:\etc\nis`.

2 (Conditional) Set up another NIS server as a slave to this NIS server:

2a Create a text file called YPSERV in `sys:\etc\nis`. For every slave server, provide the hostname of the slave server in this file in the following format:

slaveserverhostname1 slaveserverhostname1

slaveserverhostname2 slaveserverhostname2

NOTE: The first field should not be IP Address.

2b Specify the YPSERVERS map entry in `sys:\etc\nis\nismake` with its path in the following format:

`YPSERVERS sys:\etc\nis\ypserv`

3 Migrate the domain. For migration information, see "File-Based Migration" on page 73.

4 Load nisserv.nlm.

The NetWare NIS Server is now set up as a master NIS Server.

5 (Conditional) If the map data in this NIS master is modified at any time, and the changes need to be immediately updated in the slave servers, then execute the following command:

`yppush -d domainname [-v] mapname`

NOTE: The changes on the NIS master are periodically updated on the slave servers.

Setting Up a NetWare Server as NIS Slave Server

1 While setting up the UNIX machine as the master, add the NetWare server name to the slave server list.

2 In the NetWare server, make sure that the parameter NIS_CLIENT_ACCESS=1 is in the `sys:\etc\nfs.cfg` file.

3 Set the domain to the one that is being served by the UNIX NIS server, using the following command:

`ypset domainname hostname`

4 Ensure that nisserv.nlm is loaded.

5 Run MKSLAVE to set up the NetWare machine as a slave, using the following parameters:

`mkslave -d domainname -m master [-x contextname]`

Setting Up a NetWare Server As a NIS Client

1 Run NFSSTOP.

2 In the NetWare server, make sure that the parameter NIS_CLIENT_ACCESS=1 is in the `sys:\etc\nfs.cfg` file

3 Run NFSSTART.

4 Set the default domain by specifying

`ypset domainname hostname/IP_address`

Setting Password of NIS User

From UNIX

1. Bind to a domain which contains the user.
2. Execute the yppasswd command and follow the on-screen instructions.

From NetWare Console

1. Execute the following command:

   `yppasswd` [*`username`*]

   Where *username* specifies the user's name. It can be the fully qualified username (for example,.username.domainname_U.novell) or the user's common name (for example, user1).
2. Follow the on-screen instructions to specify the old password and then the new password.

This command reads the list of domains the user belongs to from eDirectory and changes the user's password on all those domains.

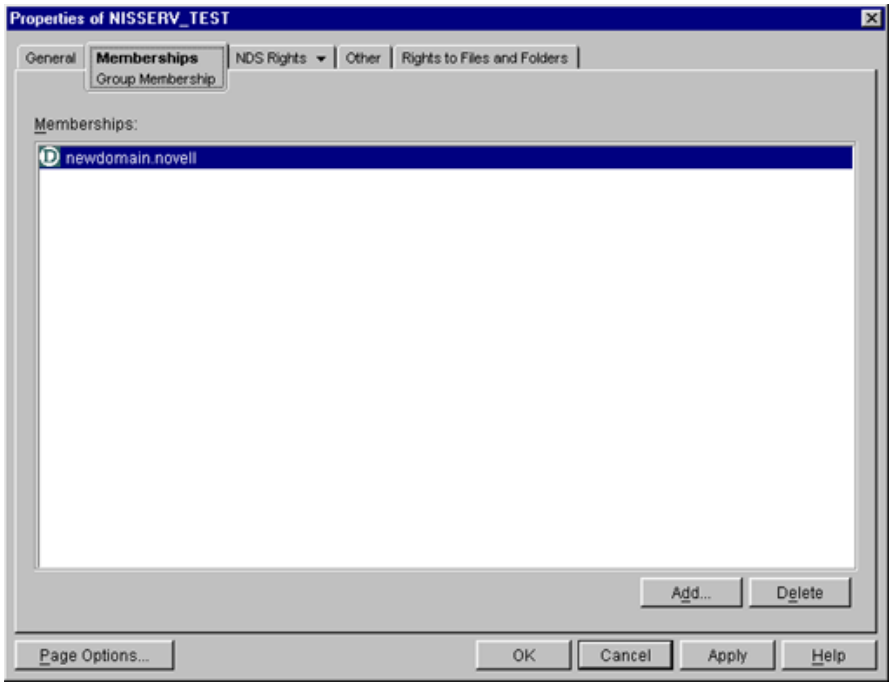
7.15.3 ConsoleOne Management for NIS Server

- "NIS Server Configuration Parameters" on page 98
- "Viewing Domains Served by NIS Server" on page 99
- "Setting Up a NetWare Server as a NIS Master" on page 100
- "Setting up a NetWare Server as a NIS Slave Server" on page 101
- "Configuring eDirectory Objects to Be Served by NIS Server" on page 101
- "Managing NIS Data in eDirectory" on page 102
- "Administering Maps" on page 104
- "Starting and Stopping NIS Server from ConsoleOne" on page 113

NIS Server Configuration Parameters

To configure the parameters required for NIS services, right-click *NISSERVER_ servername*, then click *Properties*. A dialog box similar to the following appears:

Figure 7-18 *NIS Parameters Dialog Box*



***Map Refresh Frequency*:** The frequency at which all the records of the map should be refreshed. Range = 1 to 2400 hours (100 days).

***Log File Path*:** The path to the NetWare server where you want to write the NIS log files.

***Maximum Log Messages*:** The maximum number of log messages that can be logged. The information is specific to each log file. By default, the last 5000 messages are displayed. If the number of log messages is set to *n*, the last *n* messages are retained.

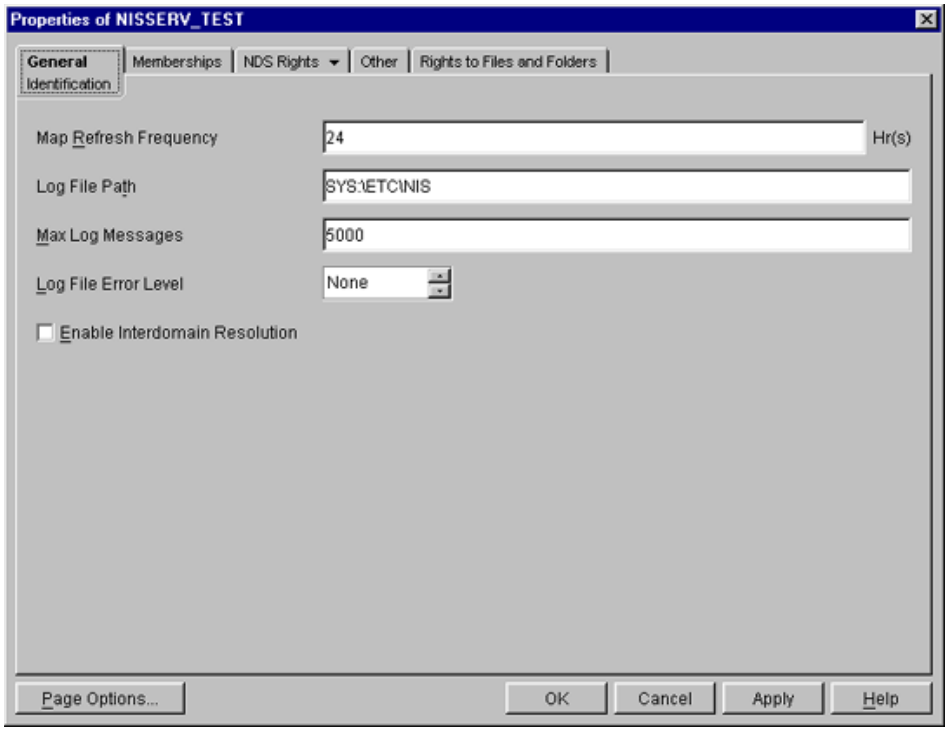
***Log File Error Level*:** The level of error messages written to the audit.log file. Select an error level from the drop-down list.

***Enable Interdomain Resolution*:** Check this box to allow interdomain resolution. DNS is then contacted for hostname resolution for NIS client calls on host maps only.

Viewing Domains Served by NIS Server

To view the domains served by the NIS Server, right-click *NISSERVE_ servername*, then click *Properties* > *Memberships*. A dialog box similar to the following appears.

Figure 7-19 *NIS Server Membership Dialog Box*



You can add or delete domains from this dialog box. For more details, see the online help.

Setting Up a NetWare Server as a NIS Master

1. Copy the NIS-related text files required for the domain from the UNIX machine (which are available in `/etc` in UNIX) to `sys:\etc\nis`.
2. (Conditional) Set up another NIS server as slave to this NIS server.

   2a Create a text file called YPSERV in sys:\etc\nis. For every slave server specify the hostname of the slave server in this file in the following format:

   ```
   slaveserverhostname1 slaveserverhostname1
   slaveserverhostname2 slaveserverhostname2
   ```

   NOTE: The first field should not be IP Address.

   2b Specify the YPSERVERS map entry in sys:\etc\nis\nismake with its path in the following format:

   ```
   YPSERVERS sys:\etc\nis\ypserv
   ```

3. Migrate the domain.

   For migration information, see “ConsoleOne Migration” on page 74.

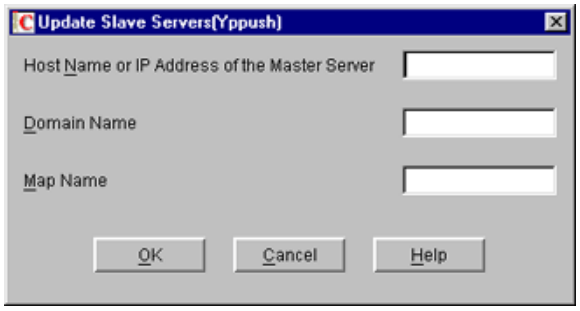
4. Start NISSERV.
5. (Conditional) Use the YPPUSH utility to update the slave NIS Server.

   The YPPUSH utility copies a new version of the named NIS map from the master NIS server to the slave NIS servers. The YPPUSH utility is normally run only on the master NIS server after the master databases are changed and the changes need to be updated in the NIS slave servers

immediately. The YPPUSH utility first constructs a list of NIS slave server hosts by reading the NIS map Ypservers within the same domain. Then a transfer map request is sent to the NIS server on each host.

Right-click *NISSERV_ servername*, then click *Update Slave Server*. A dialog box similar to the following appears:

Figure 7-20 *YPPUSH Dialog Box*



Specify the required details such as HostName or IP Address of the Master Server, Domain Name, and Map Name. For more details, see the online help.

NOTE: The changes done to the NIS master are periodically updated on the slave servers.

Setting up a NetWare Server as a NIS Slave Server

1. While setting up the UNIX machine as the master, add the NetWare server name to the slave server list.
2. In the left pane of ConsoleOne, click The Network.
3. Select the server tree where you want to manage the domains and maps.
4. Click the M icon on the toolbar to display the Migration dialog box.
5. Specify the *NetWare hostname/IP* address, slave *Domain Name*, and context where the Domain object is to be created, to migrate a domain.
6. Deslect *Set the Specified Host As Master Server* to set the NIS Server as slave for this specified domain.
7. Specify the master server's name /IP address in the save server information.
8. Click *Migrate* to migrate the domain.

Configuring eDirectory Objects to Be Served by NIS Server

NIS Server recognizes eDirectory users and groups as NIS users and groups only if they have a UNIX profile attached to them. To configure existing eDirectory User or Group objects to be served by NIS Server:

1. Select the eDirectory User or Group object, right-click *Properties*, then click *UNIX Profile*. Specify information in the required fields in this page.
2. In the *Other* tab, click *Add* > *nisUserGroupDomain Attribute*.
3. Browse and select the NIS Domain object that you want to attach these users and groups to.

This is a multivalued attribute and you can attach as many NIS domains to this as you want. These users and groups now belong to these NIS domains and are listed under all these domains.

4 Verify that the eDirectory context that these user and groups exist in is listed in the NIS Domain object by right-clicking Domain Object, then clicking *Properties* > *Memberships*.

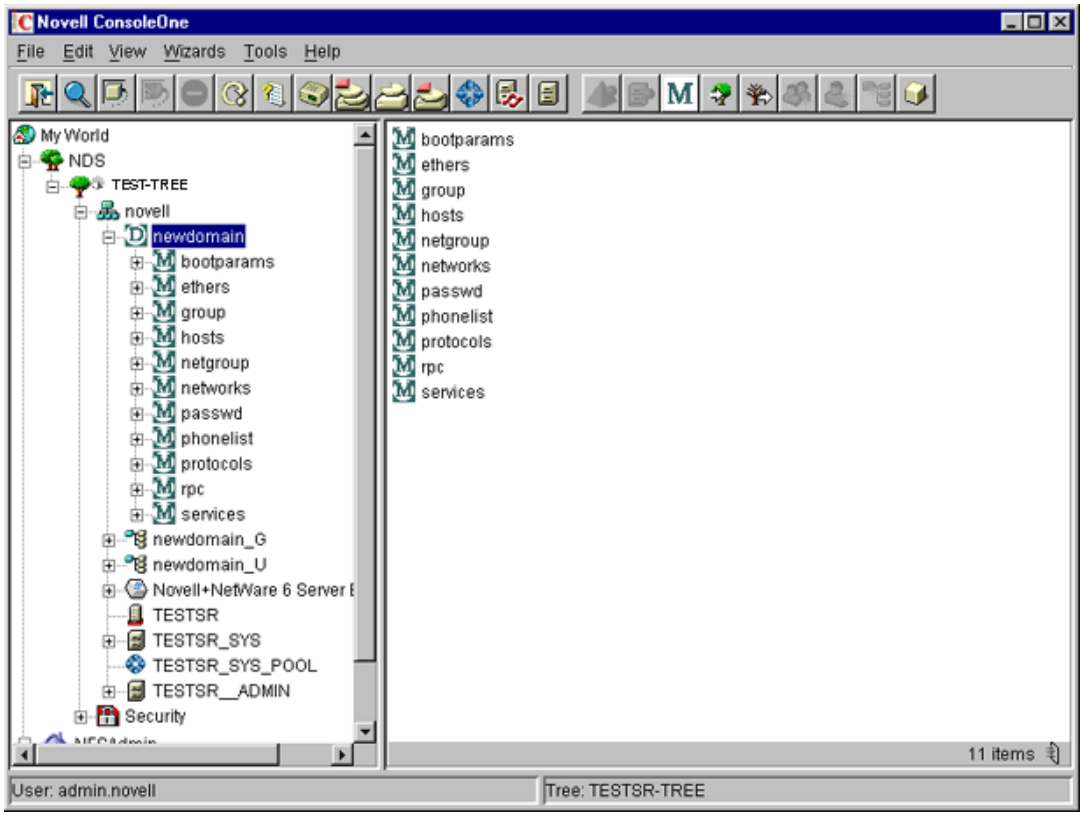
You can create new NIS maps and NIS map records under the NIS domain object as you create normal eDirectory objects.

NOTE: No objects are under the passwd and group Map objects in the domain. When managing NIS through ConsoleOne, eDirectory objects of type ipService and nisObject cannot be created.

Managing NIS Data in eDirectory

After migration, the NIS maps and records are available as objects under the migrated NIS domain object.

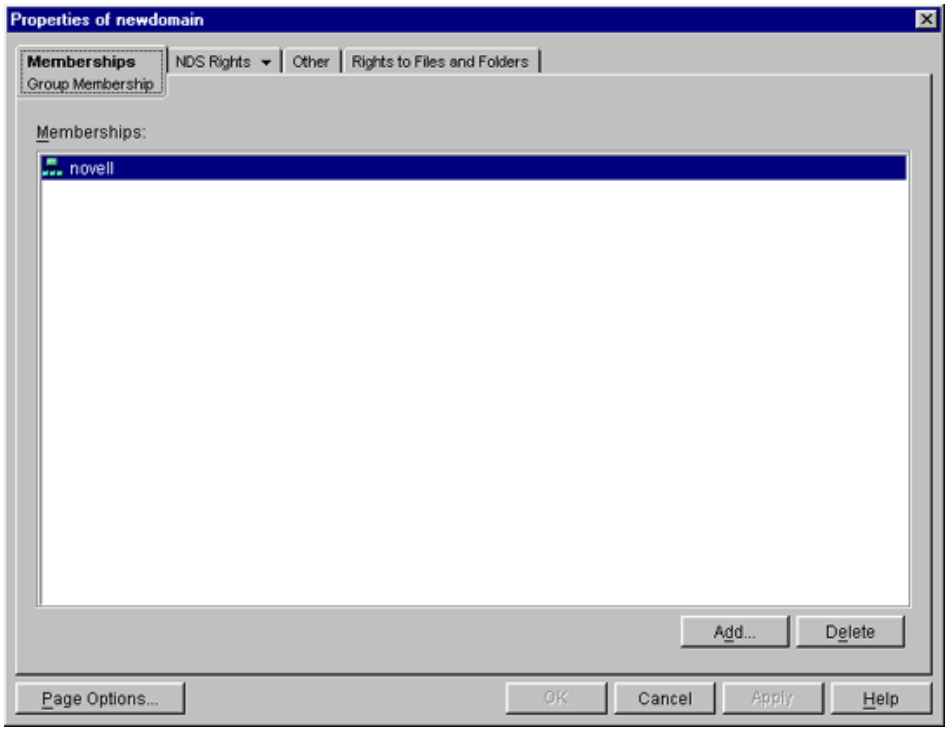
Figure 7-21 *Maps under the Migrated Domain*



When a client call is made to this domain, the NIS Server lists the data present under the corresponding Domain object. However, for user and group details, it looks for users and groups belonging to the domain under the contexts specified by an attribute of the Domain object.

To view the list of contexts where the users and groups are located, right-click the Domain object, then click *Properties* > *Membership*. A dialog box similar to the following appears.

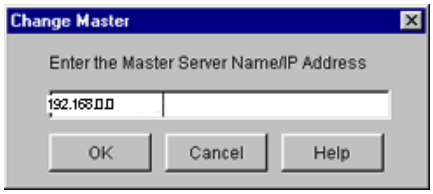
Figure 7-22 *Domain Properties Dialog Box*



If the NetWare NIS Server is a slave for a domain and the master NIS server for that domain is changed to some other server, to get the updates from the new master you need to change the NIS master server name for the Domain object in the NetWare NIS slave server.

Right-click the *Domain* object, then click *Change Master*. A dialog box similar to the following appears:

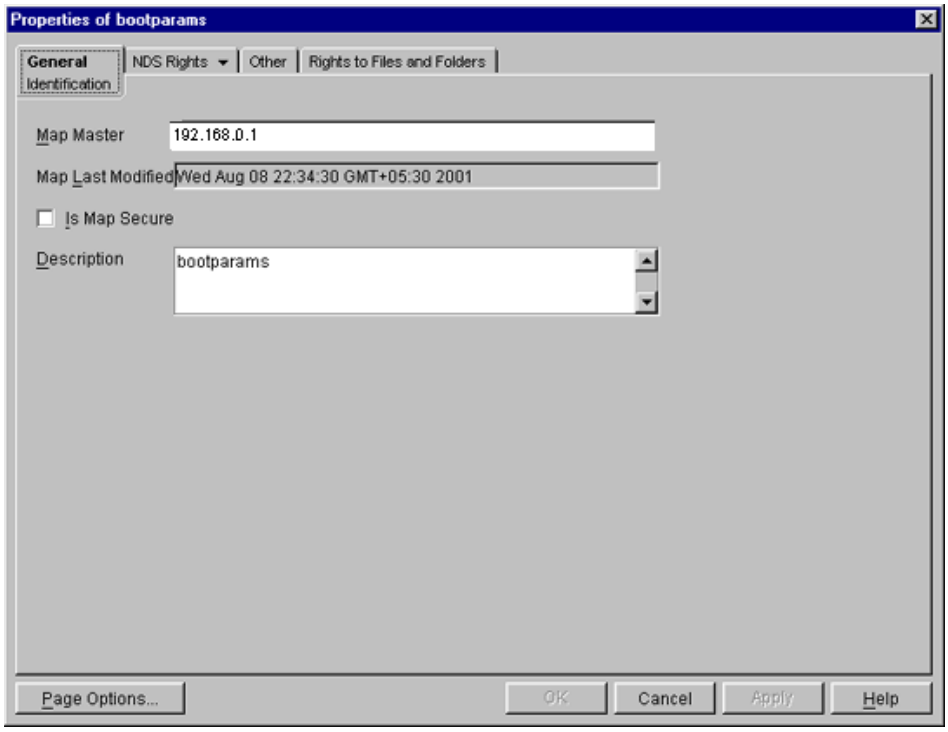
Figure 7-23 *Change Master Dialog Box*



Specify the IP address of the new NIS master server. The NIS slave server now contacts the new master server for updates on all the maps under this domain.

You can view the properties for each map. Right-click *Map Object* > click *Properties*. A property page similar to the following appears:

Figure 7-24 *General Map Properties Property Page*



***Map Master*:** The name of the master server serving this map.

***Map Last Modified*:** The last time the map was modified by adding or removing records.

***Is Map Secure*:** Sets the secure flag of the map when checked.

***Description*:** Any general comments that you want to record.

Click each map to perform operations on it and to see the records under the map.

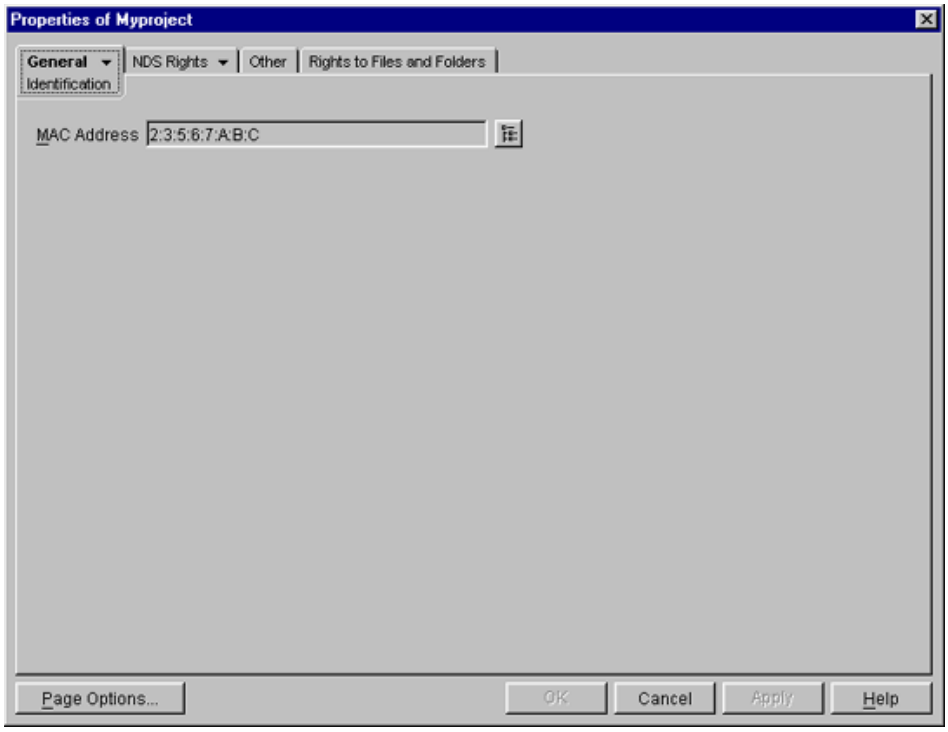
To add an object to a map, right-click the map in the left pane, click *New*, select the object, then specify the details of the object in the dialog box.

Although the dialog boxes for records on the same map are the same, they differ from map to map.

Administering Maps

The following figures show the main map property pages and are followed by procedures for using each page's basic fields. Using these pages, you can view or modify the map record's properties. The standard fields remain the same.

Figure 7-25 *Ethers Map Records Property Page*

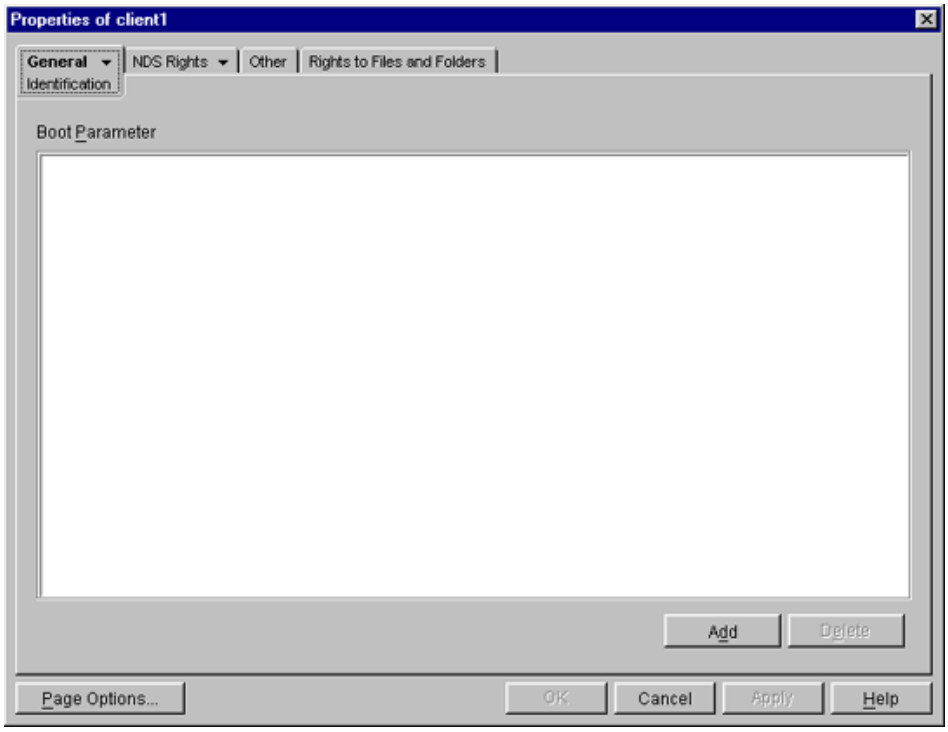


This property page shows the Ethernet address of the host.

The standard address form is *x*: *x*: *x*: *x*: *x*: *x*, where *x* is a hexadecimal number.

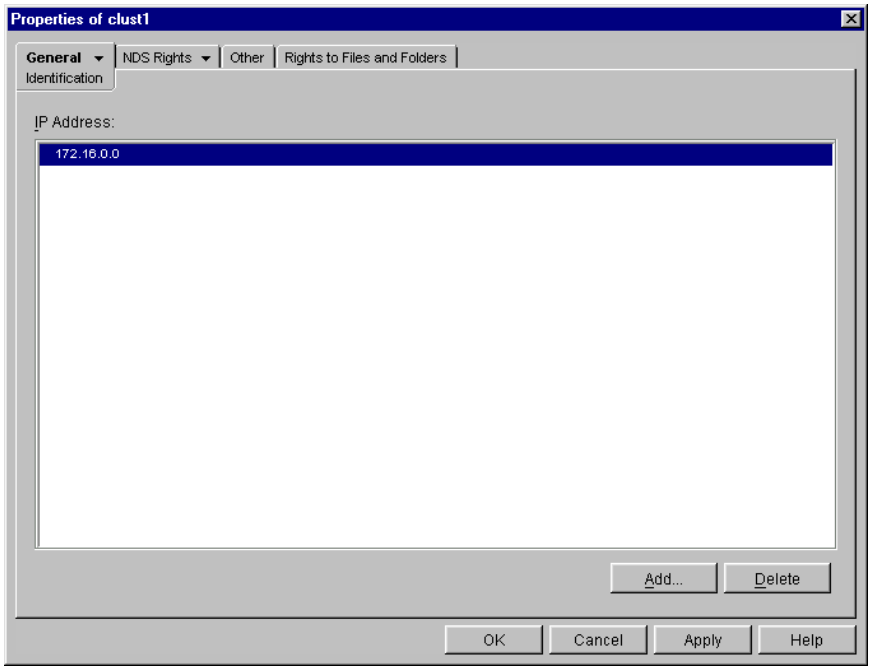
Click the icon to specify the Ethernet address of the host, click *Apply*, then click *OK*.

Figure 7-26 *Boot Map Records Property Page*



1. To add the device's boot parameter, click *Add*, specify the boot parameter of the device in the Boot Parameter field, click *Apply*, then click *OK*.
2. To delete the device's boot parameter, select the boot parameter of the device in the *Boot Parameter* field, click *Delete*, click *Apply*, then click *OK*.

Figure 7-27 *Host Map Records Property Page*

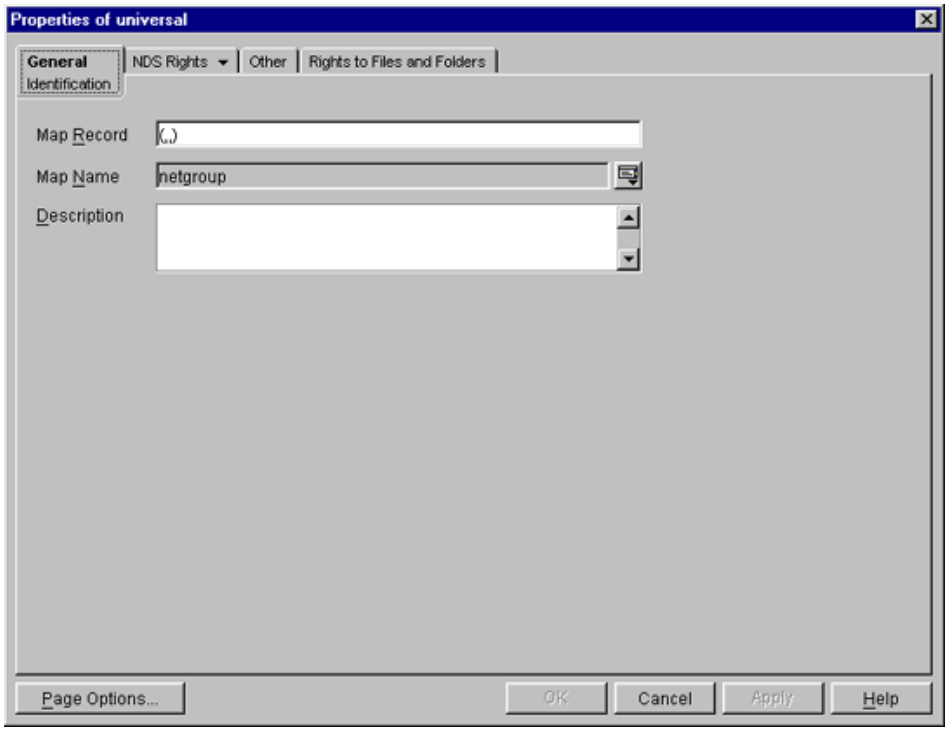


1. To add the host address, click *Add*, specify the IP address of the host, click *Apply*, then click *OK*.

   The network addresses are written in the conventional decimal dot notation.

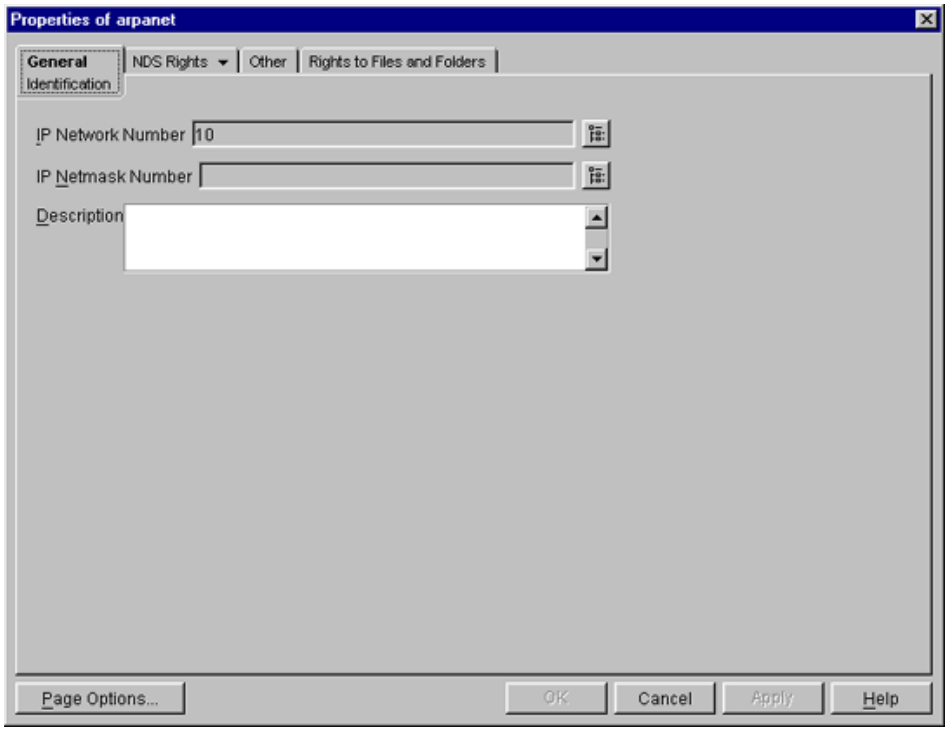
2. To delete the host address, select the host's IP address from the *IP Address* field, click *Delete*, click *Apply*, then click *OK*.

Figure 7-28 *Netgroup Map Records Property Page*



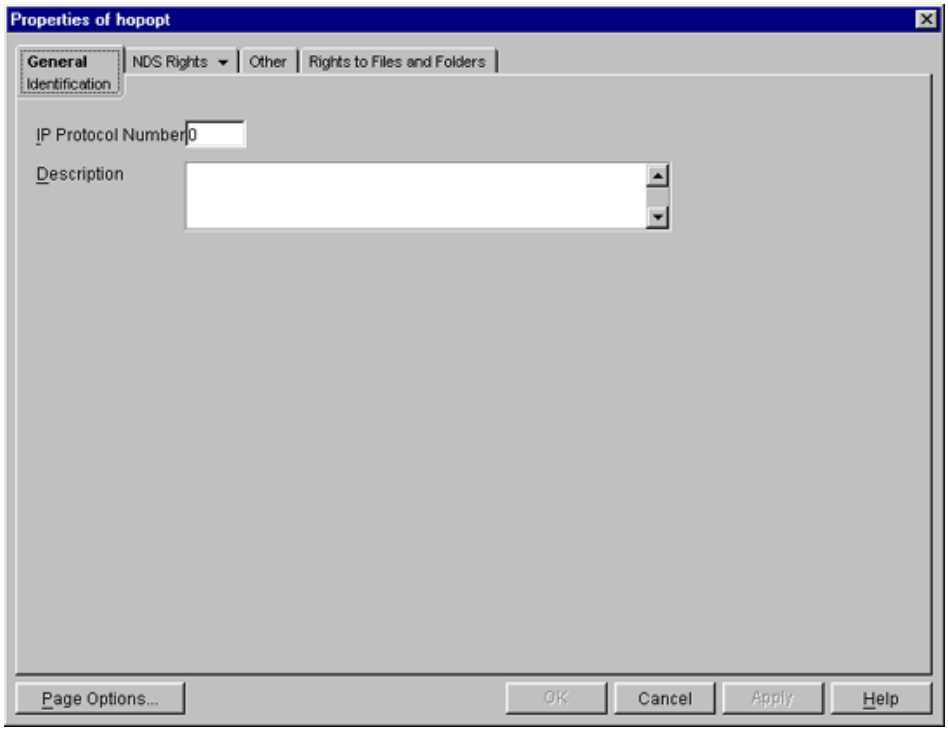
To add a netgroup address, specify the name of the *Map Record*, browse for the *Map Name*, specify the map *Description*, click *Apply*, then click *OK*.

Figure 7-29 *Network Map Records Property Page*



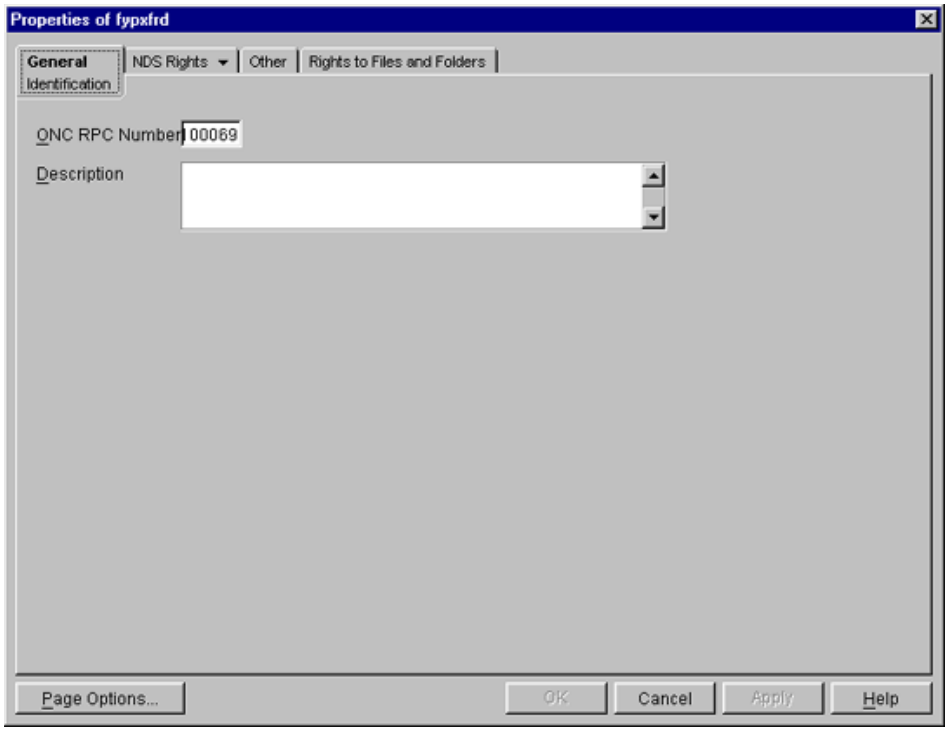
1. To specify the *IP Network Number*, click *Browse*, specify the network number, then click *OK*.
2. To specify the *IP Netmask Number*, click *Browse*, specify the netmask number, click *OK*, specify the description of the record, click *Apply*, then click *OK*.

Figure 7-30 *Protocols Map Records Property Page*



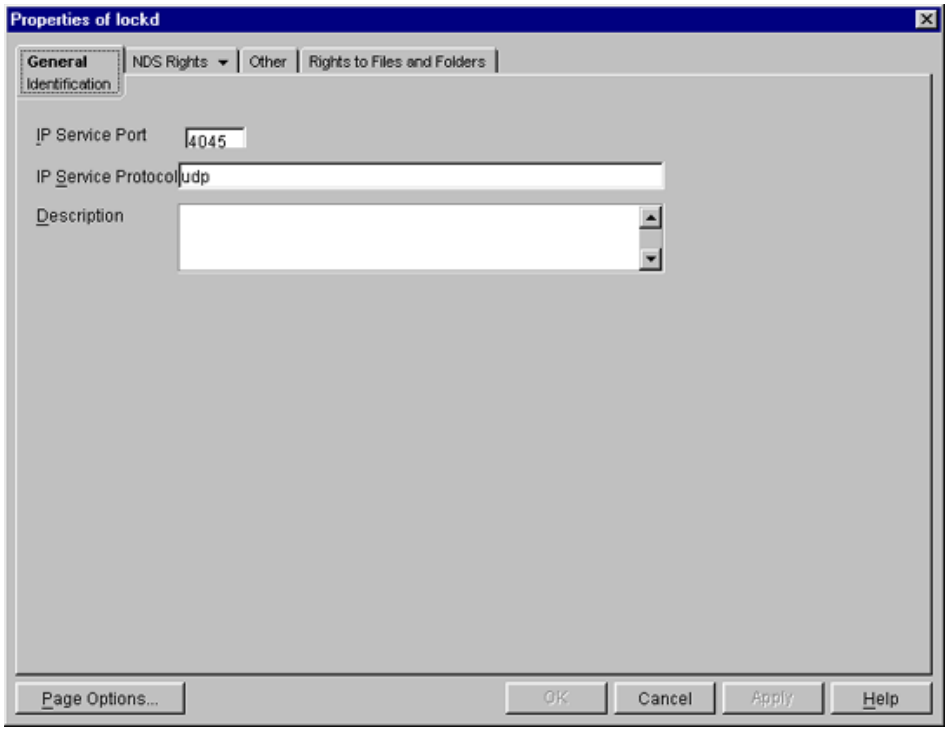
1. Specify the *IP Protocol Number* and a brief description of the record.
2. Click *Apply*, then click *OK*.

Figure 7-31 *RPC Map Records Property Page*



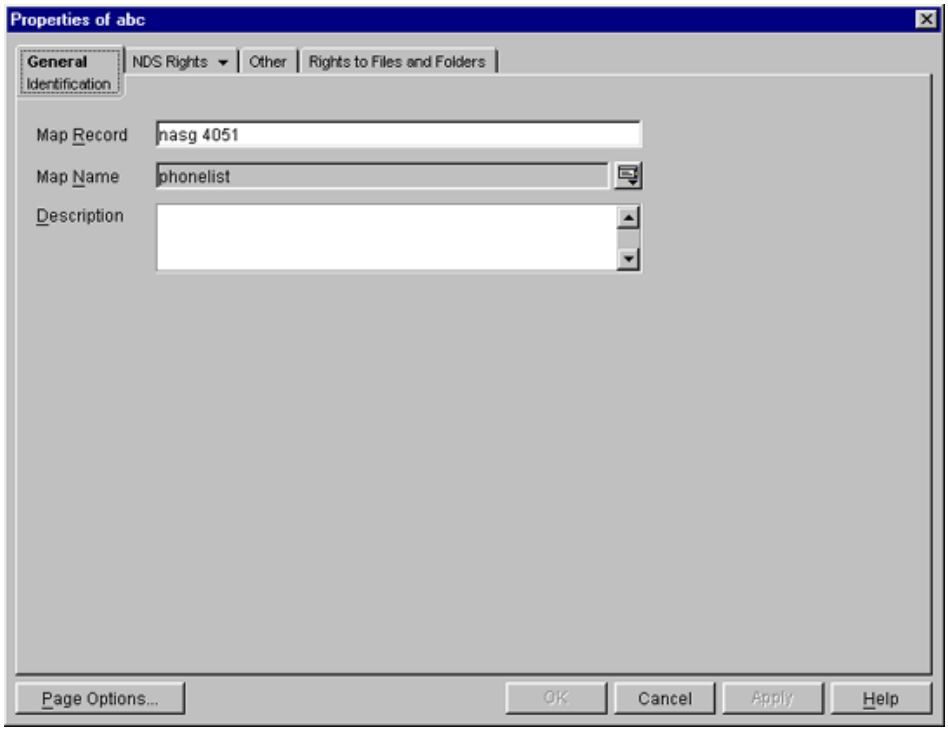
1. In the *ONC RPC Number* field, specify the RPC number of the program.
2. Specify a brief *Description* of the record.
3. Click *Apply*, then click *OK*.

Figure 7-32 *Services Map Records Property Page*



1. In the *IP Service Port* field, specify the port number that this service is available on.
2. In the *IP Service Protocol* field, specify the protocol used to access the specified service.
3. Specify a brief description of the record.
4. Click *Apply*, then click *OK*.

Figure 7-33 *General Map Records Properties*



1. In the *Map Record* field, specify the map record using the following format:

   `key record`
2. Specify the *Map Name* that the record belongs to.
3. Provide a brief *Description* of the record.
4. Click *Apply*, then click *OK*.

Starting and Stopping NIS Server from ConsoleOne

Right-click *NISSERV_ servername*, then click *Start/Stop* Services.

NOTE: You can start and stop the NIS Services by using the NIS Server menu. Make sure to refresh ConsoleOne after changing the status of NIS using the menu.

7.16 Cluster-Enabling Native File Access for UNIX

Cluster-enabling Native File Access for UNIX lets you have the advantage of using NFAU services even when the server on which it is installed fails.

In a cluster-enabled Native File Access for UNIX, if the node or server where the services are running fails, then the shared volume along with configuration files mounts along with the virtual IP address on the designated node in the cluster. After failover to another node, the NFAU service fails-over to this node and starts servicing the clients from this node. The failover that happens in the cluster is transparent to all clients.

You can select to configure Native File Access for UNIX to work with Novell Cluster Services in active/active, or in active/passive mode.

- Section 7.16.1, “Prerequisite,” on page 114
- Section 7.16.2, “Cluster-Enabling Native File Access for UNIX,” on page 114
- Section 7.16.3, “Upgrading Cluster-Enabled Native File Access for UNIX,” on page 117
- Section 7.16.4, “Component-Specific Configuration,” on page 118

7.16.1 Prerequisite

❑ Install and set up Novell Cluster Services.

For step-by-step information on setting up Novell Cluster Services, refer to the Installation and Setup chapter of the *OES 2 Novell Cluster Services 1.8.4 Administration Guide for NetWare* (http://www.novell.com/documentation/oes2/clus_admin_nw/data/h4hgu4hs.html#h4hgu4hs).

7.16.2 Cluster-Enabling Native File Access for UNIX

This section provides details for cluster-enabling Native File Access for UNIX in Active/Passive mode and Active/Active mode.

- “Active/Passive Mode” on page 114
- “Active/Active Mode” on page 116

Active/Passive Mode

In active/passive mode, the Native File Access for UNIX software runs on only one node at a time in the cluster. When a server fails, Native File Access for UNIX starts on another specified node in the cluster, and the cluster volumes that were mounted on the failed server fail over to that node.

This makes active/passive mode slower than active/active because, in addition to cluster volumes failing over, Native File Access for UNIX software must load on other servers in the cluster before users can access files and directories.

1. Stop NFS Services running on all the nodes that you are cluster-enabling.

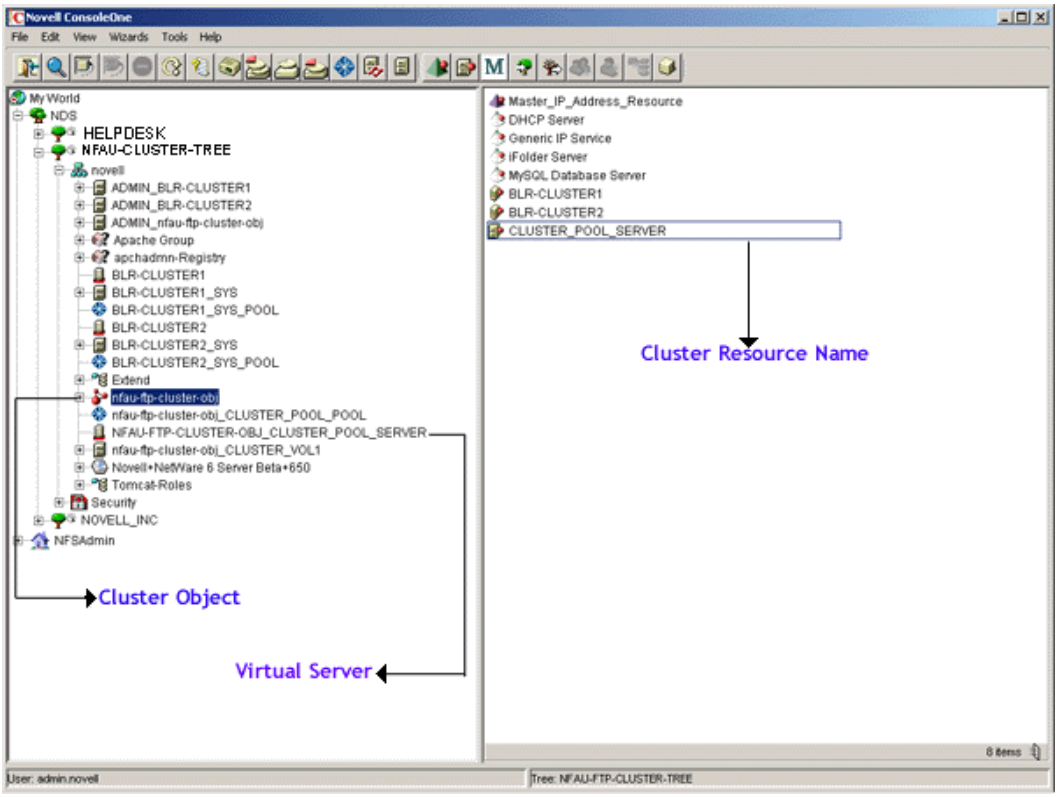
   To stop the NFS Services, execute the following on all nodes, one by one:

   ```
   nfsstop
   unload nfsadmin
   unload pkernel
   ```

2. Create the `sys:\nfsback` directory and back up the configuration file by copying the `nis.cfg` file from `sys:\etc` to `sys:\nfsback`.
3. On the node where the volumes of resources are mounted, execute the following command syntax:

   ```
   nisinst -s nisserv_resourcename -i ipaddress
   ```

Figure 7-34 *Cluster Objects*



Option	Description
-s nisserv_resourcename	View the cluster resource name by clicking the cluster object in ConsoleOne. Manually append nisserv to the resource name.
-i ipaddress	The IP address of the cluster resource object you created. To locate the IP address, right-click Cluster Resource > Properties > Cluster Resources > IP Address Tab.

This creates an eDirectory object with the name specified with the -s option.

4 Create the `\etc` directory on the shared volume. From the node where the volumes are mounted, copy the configuration files (`nfs.cfg` and `nis.cfg`) and exports file from `sys:\etc` to this `\etc` directory of the shared volume.

For example, if cluster_vol1 is the shared volume name, then copy the files to `cluster_vol1:\etc`.

NOTE: Remove all local exports (paths exported from the local disk) and export the shared path by adding the shared path to the exports file at `shared_vol_name:\etc`.

5 Create the `\system` directory on the shared volume and copy the `nfsstart.ncf` and `nfsstop.ncf` files from sys:system to `shared_vol_name:\system`.

6 Edit the NetWare configuration files (.ncf) files.

6a In the `shared_vol_name:\system\nfsstop.ncf`, uncomment unloading of `nfsadmin`, `pkernel`, and `rpcbstub`.

6b In autoexec.ncf, comment or remove `nfsstart` from every NFS server in the cluster. This lets Native File Access for UNIX be started by NetWare Cluster Services.

7 Modify the load script.

The load script specifies the commands to start the resource or service on a server, or to mount the volume on a server.

7a In ConsoleOne, select and right-click the *Cluster resource* object, then click *Properties* > *Scripts* > *Cluster Resource Load Script*.

7b Add the following at the end of the existing load script:

nfsclust *AAA.BBB.CCC.DDD shared_vol_name* resource_name

```
shared_vol_name:\system\nfsstart
```

For example,

```
nfsclust aaa.bbb.ccc.ddd cluster_vol1 CLUSTER_POOL_SERVER
cluster_vol1:\system\nfsstart
```

8 Modify the unload script.

Unload script specifies how the application or resource should terminate.

8a In ConsoleOne, select and right-click the *Cluster resource* object, then click *Properties* > *Scripts* > *Cluster Resource Unload Script*.

8b Add the following at the beginning of the unload script:

shared_vol_name:\system\nfsstop

unload nfsclust

For example,

```
cluster_vol1:\system\nfsstop
unload nfsclust
```

Native File Access for UNIX is now configured to run with Novell Cluster Services.

Active/Active Mode

Active/active mode is the recommended configuration because it provides faster recovery after a failure. Active/active mode signifies that Native File Access for UNIX is running simultaneously on multiple servers in the cluster. When a server fails, the cluster volumes mounted on that server fail over to other servers in the cluster and users retain access to files and directories.

1 If commented, uncomment the nfsstart.ncf command in the autoexec.ncf file of individual nodes/servers of the cluster that will run Native File Access for UNIX.

2 Modify the load script by adding the following syntax to at the end of every load script of the clustered volume or pool.

```
xnfs share /shared_vol_name[/dir1[/dir2...]] [export options]
```

The directories specified in the exported path are case sensitive. For details on export options, see “Export Options” on page 81.

The load script specifies the commands to start the resource or service on a server, or to mount the volume on a server.

The load script cannot exceed 700 characters and the command xnfs share can have up to 4096 characters in length, including the path length and trustee list.

To address a case where the command `xnfs share …` exceeds 700 characters or is significantly large complete the following:

2a Specify the command into a separate ncf file and store it on the same shared volume.

2b In the load script, in place of the command xnfs share …, invoke the ncf file you created in Step 2a.

For more information, see TID10057145: Cluster Warning- 10130: VIPStatus = 11 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10057145.htm).

3 Modify the unload script by adding the following syntax at the beginning of every unload script of clustered volume/pool.

`xnfs unshare /shared_vol_name[/dir1[/dir2...]]`

The unload script cannot exceed 700 characters and the command `xnfs unshare` can have up to 4096 characters in length, including the path length.

To address a case where the command `xnfs unshare …` exceeds 700 characters or is significantly large, then complete the following:

3a Specify the command into a separate ncf file and store it on the same shared volume.

3b In the load script, in place of the command xnfs share …, invoke the ncf file you created in Step 3a.

For more information, see TID10057145: Cluster Warning- 10130: VIPStatus = 11 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10057145.htm).

If you move a volume or pool, it is unshared on the current node and shared on the target node.

Umask Value Updates in Active/Active Mode

In active/active mode, the umask value is specific to each server. If the umask values are different on the participating nodes of the cluster, then after a failover the umask value of the target Server will be used for the shared_vol that fails over.

If the umask value is different from the default value of 022, then you need to ensure that the umask values is the same even after failover. Copy the nfsstart.ncf file with a umask value to all the nodes in the cluster.

7.16.3 Upgrading Cluster-Enabled Native File Access for UNIX

This section provides information for upgrading a cluster-enabled Native File Access for UNIX installation.

- “Active/Passive Cluster Mode” on page 117

Active/Passive Cluster Mode

1 After the upgrade from NetWare 6 Support Pack 3 / NetWare 5.1 Support Pack 6 is completed, stop NFS Services on all the nodes that you are cluster-enabling.

To stop the NFS Services, execute the following on all nodes, one by one:

```
nfsstop
unload nfsadmin
unload pkernel
```

2. Bring the resource offline.
3. Complete Step 6 on page 116.
4. Complete Step 7 on page 116.

7.16.4 Component-Specific Configuration

Configuring the components of Native File Access for UNIX for cluster-enabled setup is much the same as configuring components without cluster services.

- "NFS Server" on page 118
- "Network Information Service" on page 118

NFS Server

While configuring the NFS Server:

- Export only the volumes in the shared pool.
- When mounting exported shared volumes from an NFS client, use the virtual IP address of the cluster volume object.

Network Information Service

While configuring the NIS clients:

- Bind the NIS clients to the NIS server running on the cluster by using a virtual IP address.

7.17 Interoperability

The following table summarizes the various UNIX clients with which Native File Access for UNIX has been tested with.

UNIX Client	TCP V2 Support	TCP V3 Support	UDP V2 Support	UDP V3 Support
Solaris* 8.0 for Intel	Yes	Yes	Yes	Yes
Solaris 8.0 for SPARC*	Yes	Yes	Yes	Yes
Solaris 9.0 for SPARC	Yes	Yes	Yes	Yes
Linux Red Hat* 7.2 / 8.0	Yes	Yes	Yes	Yes
Linux SuSE	Yes	Yes	Yes	Yes
HP-UX* 11.0	No	No	Yes	Yes
FreeBSD 4.5, 4.7	Yes	Yes	Yes	Yes
IBM* AIX 4. *x* and 5.0	No	No	Yes	No
UnixWare* 7. *x*	No	No	Yes	No

7.18 Performance Tuning

The performance of Native File Access for UNIX can be enhanced if you tune NSS performance.

For details on fine tuning NSS performance, refer to Fine Tuning NSS Performance in the *Storage Services Administration Guide* (http://www.novell.com/documentation/lg/nw65/index.html?page=/documentation/lg/nw65/stor_nss_lx_nw/data/hn0r5fzo.html).

- Section 7.18.1, “Performance Testing,” on page 119

7.18.1 Performance Testing

NFS Server has been tested with 300 clients simultaneously performing basic file operations using a script over NFS Version 2 and 3 with combinations using both UDP and TCP as transport. Over TCP the number of connections was scaled up to 600 using two IP addresses on the server and establishing two NFS connections per client.

Performance of NFS over TCP has improved almost five times over previous NFS releases and is now almost equivalent to UDP performance. Operations that used to take up to 25 minutes on an average, are now complete within 5 minutes.

Primary Domain Controllers on NetWare

8

The Primary Domain Controller on NetWare® functionality provides the capability to make a Novell® CIFS server a Windows NT 4 style Primary Domain Controller (PDC) in a network running the Microsoft CIFS protocol. While acting as a PDC, a Novell CIFS server will replace and become the Primary Domain Controller in a CIFS network. There are three main advantages of this new feature:

- Instead of having to create separate Microsoft domain and eDirectory™ user accounts (as was previously the case), user accounts now need to be created only once in eDirectory.
- The other CIFS workstations and CIFS servers in the network will function as if they were part of an NT4 domain.
- All CIFS clients will authenticate to a Novell CIFS server using eDirectory.

Although much of Microsoft PDC functionality is available with the PDC on NetWare feature, some functionality is not. The following list provides information on functionality not included.

- Microsoft Active Directory functionality is not included.
- Replication between a PDC on a Novell CIFS server and a BDC on a Microsoft server is not supported.

  If you want to replicate between a PDC on a Novell CIFS server and a BDC, the BDC must also be on a Novell CIFS server.
- Trusted Domain relationships are not supported.

  Every eDirectory user will implicitly belong to the PDC domains in the eDirectory tree (provided the appropriate eDirectory ACLs are in place to give domain controllers access to the User objects). This eliminates the need for trusted domain relationships in an eDirectory environment.
- Administration of domains hosted on Novell CIFS servers using Microsoft administration utilities is not supported.
- Roaming profiles are not supported.
- Microsoft NTFS ACL mappings are not supported.

  Microsoft clients cannot assign a Microsoft NTFS-style ACL to a file stored on a Novell NSS volume. Managing rights to files and directories on NSS volumes is done using Novell management utilities.

8.1 Requirements

The following requirements must be met prior to creating a Microsoft domain on a Novell CIFS server:

- ❑ NetWare servers that you will create Microsoft domains on must be running NetWare 6.5 Support Pack 2 or later

- ❑ You must have an understanding of the Microsoft Windows networking model
- ❑ NetWare CIFS servers that are configured to be Primary Domain Controllers (PDC) should have at least a Read/Write eDirectory Replica. Backup Domain Controllers (BDC) require at least a Read Only eDirectory Replica. Domain members do not require an eDirectory Replica.

8.2 Installing PDC on NetWare Software

PDC on NetWare software is automatically copied to the appropriate directories on your NetWare server during the NetWare 6.5 SP2 installation. No additional installation is required.

8.3 Configuring PDCs on NetWare Servers

Configuring a PDC on a NetWare CIFS server consists of the following:

- Section 8.3.1, “Creating a PDC on a NetWare CIFS Server,” on page 122
- Section 8.3.2, “Adding Servers to the Domain,” on page 124
- Section 8.3.4, “Adding an Access Control List for the Domain,” on page 125

8.3.1 Creating a PDC on a NetWare CIFS Server

To make a NetWare 6.5 SP 2 server a PDC, you must create a PDC on the server. The server where you create the domain cannot already be a domain controller or a domain member in any other domain.

To create a PDC on a NetWare CIFS server:

1. At the server console of the NetWare CIFS server where you want to create the PDC, specify the following console command:

   ```
   CIFS DOMAIN CREATE
   ```

   After specifying the command, you will be prompted separately for the domain name, context, username, and password.
2. Specify the domain name of the new PDC you are creating.

   The size and allowed characters of this name are the same as a legal CIFS workgroup name.
3. Specify the context where the PDC object will be created in the eDirectory tree.

   This is the eDirectory distinguished name of the context location in the eDirectory tree where the new domain is to be created. The following examples provide context format samples that can be used when specifying the context.

   ```
   sales.boston.acme
   ```

   ```
   .ou=sales.ou=boston.o=acme.t=acmetree.
   ```
4. Specify the username of a user with sufficient rights to create objects in the context you specified in Step 3.

   You must specify the eDirectory context of the user you specify.
5. Specify the password for the user you specified in Step 4.

As an alternative to specifying the required information when prompted, you could specify the command and necessary parameters all at the same time. In this case, specify the following command at the server console:

`CIFS DOMAIN CREATE domainName context comment username password`

Replace the command parameter variables with the domain name, context, comment, username, and password. The parameters are described in Step 1through Step 5 above. If you want to specify a comment when creating the PDC, you must specify the command and parameters at the same time.

When you create a PDC on a NetWare CIFS server, that PDC also functions as a Domain Master Browser.

eDirectory Domain Objects

When you create a PDC on a CIFS NetWare server, a domain object is automatically created in the eDirectory context you specify during the creation process. The domain object is a container object and contains five Group objects that are also automatically created. The names and purposes of the domain Group objects are as follows:

IMPORTANT: Do not add additional non-domain objects to the domain container.

`Domain Admins`—This group is added to the local Administrators group of each Windows workstation that joins the domain. Those users that are domain administrators must be members of the Domain Admins group. The eDirectory user that creates the domain is automatically included as a member of the Domain Admins group. Other users can be added to this group by the domain administrator. Any user in this group will have local administrator rights on any workstation or server that joins the domain.

`Domain Controllers`—Every domain controller configured to participate in the domain will be added as a member of the Domain Controller group. An Access Control List (ACL) will be automatically created giving this group the rights to manage the domain object. This allows all domain controllers in the domain to access the domain object. An ACL will also be automatically added giving this group rights to manage the RID and CIFS login script attributes of any user, group, profile or container object in the subtree at the same level as the domain object or below it.

`Domain Groups`—This group is strictly for internal use by the domain code. Any eDirectory groups that have been used in the domain are automatically added as members of the Domain Groups group.

`Domain Guests`—This group can be added to the local workstation Guests group if desired. It is not automatically assigned members and is not added to any local groups like the Domain Admins and Domain Users groups.

`Domain Users`—This group is added to the local Users group of each Windows workstation that joins the domain. All users that log in to the domain are automatically added to this group. Every user in this group will have the same rights as the local Users group on any workstation or server that joins the domain.

When clients and non-Novell servers join the domain, a special Machine Account object is automatically created for them. These machine accounts are required in the Microsoft domain model, but are not necessary for Novell CIFS servers that participate in the domain. These Machine Account objects are contained by the domain object. They are eDirectory User objects where the name of the user is the NetBIOS name of the computer with a dollar sign ($) at the end of the name.

8.3.2 Adding Servers to the Domain

After creating a PDC on a NetWare CIFS server, you can add additional NetWare CIFS servers to the domain as either Backup Domain Controllers (BDC) or domain members.

To add a NetWare CIFS server to a domain as either a BDC or a domain member:

1. At the server console of the NetWare CIFS server that you want to add to the domain, specify the following console command:

   ```
   CIFS DOMAIN JOIN
   ```

   After specifying the command, you will be prompted separately for the domain name and the mode (BDC or domain member).
2. Specify the eDirectory distinguished name of the domain you want to join the server to.
3. Specify whether you want the server to be a BDC or a domain member by specifying either `controller` or `member` at the prompt.
4. Specify the username of a user with sufficient rights to create objects in the context you specified in Step 3.

   You must specify the eDirectory context of the user you specify.
5. Specify the password for the user you specified in Step 4.

As an alternative to specifying the required information when prompted, you could specify the command and necessary parameters all at the same time. In this case, specify the following command at the server console:

```
CIFS DOMAIN JOIN domainName mode username password
```

Replace the command parameter variables with the domain name and mode that are described in Step 1 through Step 3 above. You can optionally specify a username and password by specifying the command and parameters at the same time.

The username must include the context and name of a user with sufficient rights to create objects in the specified context. If you do not specify a username, the rights for the Server object are used to attempt the join.

You can also add Windows and Samba servers to the domain as domain members. The procedure for adding Windows and Samba servers to the domain is the same as adding them to a domain hosted on a Windows server.

You cannot add BDCs hosted on Windows servers to domains hosted on NetWare servers.

IMPORTANT: If the CIFS server where the PDC is located is on a different subnet than the servers, workstations, or filers that will access it, you must configure a WINS address. The WINS address is the address of the WINS server used to locate the PDC. For information on configuring WINS addresses, see “Changing CIFS Configuration” on page 38.

8.3.3 Adding a Network Attached Storage Filer to the Domain

The procedure for adding network attached storage filers to the domain is the same as adding them to a domain hosted on a Windows server. Consult your network attached storage filer documentation for more information.

8.3.4 Adding an Access Control List for the Domain

If you have User objects in your eDirectory tree that are above the context where the PDC object was created or are in a different branch of the tree than the PDC object, you must add an Access Control List (ACL) for the domain. The ACL grants the domain's Domain Controllers group the rights to manage User object RIDS and login scripts at the specified context and below it in the eDirectory tree.

To add an ACL for the domain:

1. At the server console of the NetWare CIFS server where the PDC is located, specify the following console command:

   ```
   CIFS DOMAIN ADDACL
   ```

   After specifying the command, you will be prompted separately for the ACL context.

2. Specify the context for the ACL.

   This is the eDirectory distinguished name of the context location in the eDirectory tree where the ACL for the domain is to be placed.

As an alternative to specifying the required information when prompted, you could specify the command and necessary parameters all at the same time. In this case, specify the following command at the server console:

```
CIFS DOMAIN ADDACL context domainName username password
```

Replace the context parameter with the context that is described in Step 2 above. You can optionally specify the domain name, username, and password by specifying the command and parameters at the same time.

The domain name is the eDirectory distinguished name of the PDC. The domain name is required if you specify a username and password. If you do not specify a domain name, the server's current domain is used.

The username must include the context and name of a user with sufficient rights to create objects in the specified context. If you do not specify a username, the rights for the Server object are used to attempt to create the ACL.

8.4 Managing PDCs on NetWare Servers

PDC on NetWare software includes functionality to help you effectively manage your domains on NetWare servers. This management functionality includes the following:

- Section 8.4.1, "Removing Servers from the Domain," on page 125
- Section 8.4.2, "Deleting Domains," on page 126
- Section 8.4.3, "Promoting BDCs to PDCs," on page 126
- Section 8.4.4, "Getting Domain Information," on page 127

8.4.1 Removing Servers from the Domain

You can remove both BDCs and domain member servers from the domain. You cannot remove PDCs from the domain without deleting the domain. To remove a server from the domain, specify the following console command at the server console of the server you want to remove:

```
CIFS DOMAIN LEAVE
```

You can optionally specify a domain name, username and password by specifying the command with the following parameters:

```
CIFS DOMAIN LEAVE domainName username password
```

The domain name is the eDirectory distinguished name of the domain that the server belongs to. The domain name is required if you specify a username and password. If you do not specify a domain name, the server's current domain is used.

The username must include the context and name of a user with sufficient rights to access the domain. If you do not specify a username, the rights for the server object are used to access the domain.

8.4.2 Deleting Domains

You can delete entire CIFS domains. The server used to delete a domain must be the only domain controller remaining in the domain and must be the PDC of that domain.

To delete a domain:

1. At the server console of the NetWare CIFS server where the PDC is located, specify the following console command.

   ```
   CIFS DOMAIN DELETE
   ```

   After specifying the command, you will be prompted separately for a username and password.
2. Specify the username and context of a user with sufficient rights to delete objects in the context where the domain object is located.
3. Specify the password for the user you specified in Step 2.

8.4.3 Promoting BDCs to PDCs

You can promote a BDC to become the new PDC of the domain. If the former PDC is up and running, it will automatically be demoted to become a BDC as soon as you promote the new PDC. If the former PDC is not up and running, it will be demoted to a BDC when it is brought up.

To promote a BDC to a PDC, specify the following console command at the server console of the BDC you want to promote:

```
CIFS DOMAIN SET PDC
```

You can optionally specify a domain name, username, and password by specifying the command with the following parameters.

```
CIFS DOMAIN SET PDC domainName username password
```

The domain name is the eDirectory distinguished name of the domain that the server belongs to. The domain name is required if you specify a username and password. If you do not specify a domain name, the server's current domain is used.

The username must include the context and name of a user with sufficient rights to access the domain. If you do not specify a username, the rights for the Server object are used to access the domain.

8.4.4 Getting Domain Information

You can get information on domain configuration and find out which servers are domain controllers. To get domain configuration information, specify the following console command at the server console of a server that is a member of the domain:

```
CIFS DOMAIN INFO
```

You can optionally specify a domain name, username and password by specifying the command with the following parameters.

```
CIFS DOMAIN INFO domainName username password
```

The domain name is the eDirectory distinguished name of the domain that the server belongs to. The domain name is required if you specify a username and password. If you do not specify a domain name, the server's current domain is used.

The username must include the context and name of a user with sufficient rights to access the domain. If you do not specify a username, the rights for the Server object are used to access the domain.

To find out which servers are domain controllers, specify the following console command at the server console of a server that is a member of the domain:

```
CIFS DOMAIN LISTDC
```

You can optionally specify a domain name, username and password by specifying the command with the following parameters:

```
CIFS DOMAIN LISTDC domainName username password
```

The domain name is the eDirectory distinguished name of the domain that the server belongs to. The domain name is required if you specify a username and password. If you do not specify a domain name, the server's current domain is used.

The username must include the context and name of a user with sufficient rights to access the domain. If you do not specify a username, the rights for the Server object are used to access the domain.

8.5 Creating Login Scripts for Domain Users

Novell CIFS servers acting as PDCs support Windows client login scripts. Login scripts can be created for containers, profiles, and users, just like they can for NetWare clients. The order the login scripts are executed in is the same order they are executed for NetWare clients: the immediate container script runs first, followed by the profile script, followed by the user script.

Login scripts are supported for the following client types:

- Windows NT/2000/XP
- Windows 9x/ME

To create a login script:

1. Start Internet Explorer 5 or later and specify the URL for iManager.

The URL is *http:// server_ip_address/nps/imanager.html*. Replace *server_ip_address* with the IP address or DNS name of a NetWare 6.5 server in the eDirectory tree that has iManager installed.

2. Specify your administrator username and password.
3. Click the *View Objects* icon on the menu bar.
4. Click the container, Profile, or User object that you want to create a login script for.
5. (Conditional) If the schema classes have not been extended for the object you selected, extend them now.
   - **5a** Click the object, then select *Object Extensions*.
   - **5b** Ensure the proper object name is specified, then click *OK*.
   - **5c** Click *Add*, scroll down and select *nfapLoginProperties*, then click *OK*.

     nfapLoginProperties is an Auxiliary class that contains attribute definitions for CIFS login scripts which are applied to User, Profile, and container objects.
   - **5d** Click *Close*, then click the object you selected in Step 4.
6. Click *Modify Object*, then click *Other*.
7. (Conditional) If the nfapLoginScript attribute appears in the Valued Attributes list, double click it.
8. (Conditional) If the nfapLoginScript attribute does not appear in the Valued Attributes list, scroll down in the Unvalued Attributes list and select it, then click the arrow to move it to the Valued Attributes list.
9. Add or edit the desired commands for the login script.

   The syntax of the login script is that of standard Microsoft batch files. Many of the commands used in NetWare login scripts will not work in Windows client login scripts.

System Messages

A

This section describes the following system messages of the various components of Native File Access for UNIX:

- Section A.1, “NFS Server,” on page 129
- Section A.2, “MakeNIS,” on page 130
- Section A.3, “NIS Installation,” on page 131
- Section A.4, “NIS Services,” on page 131
- Section A.5, “Yppasswd,” on page 132

A.1 NFS Server

Error: NFS Services initialization failed during eDirectory interface library (ndsilib.nlm). Error Code: *n*

Explanation: The ndsilib.nlm is not loaded.

Action: Execute `dsrepair`

OR

Manually execute `schinst -n -w` on system console.

OR

If the error continues even after executing schinst, then do the following:

1. Make a note of all the nodes that share the NFAUUser object in that context.
2. Delete the NFAUUser object.
3. Run `schinst -n -w` on all the nodes that you made note of in Step 1 on page 138.

Warning: < *IP Address aaa.bbb.ccc.ddd*> Failed to mount *pathname*. Either the path is not available or is not exported.

Action: Complete the following:

1. Make sure that the *pathname* exists and is exported.
2. Mount *pathname* afresh.

Warning: Could not resolve < *IP Address aaa.bbb.ccc.ddd*> to a name. Mount will fail. Add an entry in hosts file or DNS.

Action: Add an entry in hosts file or DNS.

Warning: Failed to resolve trustee <*IP Address aaa.bbb.ccc.ddd*> to a name. Add an entry in hosts file or DNS.

Action: Add an entry in hosts file or DNS.

Warning: Failed to resolve trustee < *name*> to an IP address. Add an entry in hosts file or DNS.

Action: Add an entry in hosts file or DNS.

Warning: The host < *hostname*> is not notified. Failure code: *n*

Possible Cause: Either the host is down / not reachable, or name resolution has failed.

Action: Make sure that the host is up and reachable.

A.2 MakeNIS

Setting the log file

Possible Cause: The directory specified when creating the log file might be incorrect.

Action: Check for the validity of the directory path you specified.

Required parameters are missing

Explanation: The domain name is mandatory.

Possible Cause: The user has not specified the required parameters.

Action: Specify all the mandatory parameters.

Domain name is missing

Possible Cause: The user has not specified the domain name.

Action: Specify the domain name.

No make data for map

Possible Cause: There is no data corresponding to the map in the makefile.

Action: Specify the record corresponding to the map.

File is older than corresponding map

Possible Cause: The text file used for making this map is older than the map that exists on eDirectory.

Action: Change the time stamp on the text file by saving it again.

Object with same domain name already exists

Possible Cause: An eDirectory error occurred while adding the specified object.

Action: Check whether the object already exists.

Unable to add users to group objects

Explanation: Users are already present.

Unable to get the host name or IP address of the machine

Possible Cause: The configuration files containing the host data are not correct.

Action: Check the configuration file.

A.3 NIS Installation

Opening configuration file

Possible Cause: Either the file is not present in the specified location or the input is illegal.

Action: Check for the existence of the specified file or the validity of the input.

Reading configuration file

Possible Cause: It is not the correct configuration file.

Action: Check the configuration file.

Getting default host names

Possible Cause: Unable to get the DNS name of the current host.

Action: Check whether entries in relevant configuration files are correct.

Updating the configuration file

Possible Cause: Either the configuration file is not present or it is corrupted.

Action: Check the configuration file.

A.4 NIS Services

Internal error with refresh watchdog

Possible Cause: The refresh thread of the NIS Server is failing.

Action: Unload nisserv.nlm and load it again.

RPC error

Possible Cause: There was an error on the RPC client call to NIS Server.

Action: Unload nisserv.nlm and load it again.

Internal error

Possible Cause: Failure to allocate memory for the domain list of the NIS Server.

Action: Unload nisserv.nlm and load it again.

Resource failure

Possible Cause: An NIS Server internal error occurred while allocating memory for its internal structure.

Action: Unload nisserv.nlm and load it again.

Unable to allocate space for domain index list

Possible Cause: Failure to allocate memory for the domain list of NIS Server.

Action: Unload nisserv.nlm and load it again.

Unable to respond to RPC request

Possible Cause: Failure in sending the RPC response back to the client because of the pkernal.nlm.

Action: Repeat the client call.

A.5 Yppasswd

Cannot communicate with NISBIND. NIS Client access is disabled. Set NIS_CLIENT_ACCESS = 1 in the nfs.cfg and restart NIS Services.

Action: In nfs.cfg, the configuration file, set NIS_CLIENT_ACCESS = 1 and restart NIS Services.

Default domain is not set. Run ypset <domainname> or specify the values of NIS_DOMAIN and NIS_SERVER parameters in the file sys:\\etc\\nfs.cfg and restart NIS services.

Action: Make sure that the NISBIND is bound to the NIS server for some domain. You can verify this by executing ypset (which displays default domain binding) and ypwhich (which displays the NIS Server binding).

Failed to get the record for user *x*. Verify if the user *x* exists in eDirectory. (The name should be a Fully Qualified Name, e.g. '.user.domain_U.novell' or the Common Name e.g. 'user')

Action: Make sure that the user specified exists, or specify an existing and valid username.

User *x* does not belong to any NIS domain.

Action: Make sure that the user specified belongs to at least one NIS domain.

RPC failure. Password daemon is not running.

Action: If the master is a NetWare server, then nisswdd.nlm (passwd daemon) should be running there. If it is a UNIX or Linux machine, then passwd daemon is (usually) rpc.yppasswdd. Check if it is loaded.

User record was not found on the remote server.

Action: Make sure that the user specified exists on the Master NIS server.

Password does not match the user password on master server.

Action: Specify the password that matches the user password on the master server.

NFAU Known Issues

B

This section has the following known issue of Native File Access for UNIX:

- Section B.1, “UNIX/NFS Issues,” on page 135

B.1 UNIX/NFS Issues

Disabling the Software

To disable NFS, complete the following steps on each server running NFS:

1. Run `nfsstop` at the server console.
2. Remove the NFSSTART line from the `autoexec.ncf` file.

Installing Native File Access for UNIX after the Migration

After completing a NetWare 5.1 to NetWare 6.5 migration using the Migration Wizard, complete the following steps to ensure that Native File Access for UNIX installs correctly:

1. Delete the NFAUUser object.
2. Run the `schinst` utility.

   Syntax:

   ```
   schinst -n -w
   ```

   Schinst takes the administrator’s FDN and password as input for extending the schema.
3. Run `nisinst`.
4. Execute `nfsstart`.

NFS Server

- Exporting traditional volumes is not supported.
- If the NetWare server code page is 932, then the file creation from Japanese EUC NFS clients fails for certain characters.
- At times, the `rm -rf` command fails over NFS version 3 over TCP while executing recursive deletion.
- Exported paths cannot contain spaces. However, filenames and directories containing spaces can be created and used under the exported path.

Using iManager for Administering NFS Server

- You cannot administer NFS using iManager if iManager is installed on a different tree.
- The NFS Server iManager snap-in does not work in the NetWare Remote Manager browser.
- On the Export options screen, the Browse button for Path is now removed.

Error 9600

NDSILIB might not autoload in certain instances. If this happens, it will return Error 9600. To fix this problem, run `NFSSTOP` at the server console and then execute the operation again.

If the issue is not resolved, log in to ConsoleOne or NWADMIN and do the following:

1. Make a note of all the nodes that share the NFAUUser object in that context.
2. Delete the NFAUUser object.
3. Run `schinst -n -w` on all the nodes that you made note of in Step 1.

Makenis Issues

Do not use makenis to delete users and groups. Use ConsoleOne instead.

Pkernel Messages

If the pkernel screen displays messages similar to the following after executing yppush, ignore them. They do not affect functionality.

```
Out of memory, cannot create UDP Client handle.
```

Removing Users or Groups from the NetWare NIS Slave Server

When the NetWare server is made a NIS slave server and users and groups are deleted from the NIS master server, do the following to remove the users and groups from the slave server:

1. In the ConsoleOne main menu, right-click the *User* or *Group* object.
2. Click *Properties* > *Other*.
3. Under *Attributes*, select *nisUserGroupDomain* and then select the specific domain.
4. Click *Delete*.

Native File Access for UNIX FAQs

C

This section has the following Native File Access for UINX FAQs:

- Section C.1, “General FAQs,” on page 137
- Section C.2, “NFS Server FAQs,” on page 140
- Section C.3, “NIS Services FAQs,” on page 144

C.1 General FAQs

This section has general FAQs for Native File Access for UNIX.

- Section C.1.1, “When upgrading to NetWare 6.5 from NetWare 5.1 / NetWare 6.0, I am receiving a file overwrite warning for nfsstart.ncf. What should I do?,” on page 137
- Section C.1.2, “NFS Server is not loading on a server in tree with NetWare 5.1 NDS 7 replica ring. How can I resolve this?,” on page 138
- Section C.1.3, “When I try to load NFS Services using Ndsilib.nlm, -669 error displays on the logger screen. How can I resolve this?,” on page 138
- Section C.1.4, “When the administrator changes the UNIX profile of the user, the updated profiles are not cached immediately. How can the profile be updated immediately?,” on page 138
- Section C.1.5, “What is the significance of the SEARCH_ROOT parameter in SYS:ETC\NFS.CFG file?,” on page 138
- Section C.1.6, “How do I manually set the UNIX profile of a user?,” on page 138
- Section C.1.7, “How do I set a User’s UNIX profile to the Root’s profile?,” on page 139
- Section C.1.8, “Could not authenticate ContextHandle. Load schinst and try again. Exiting...9601,” on page 139
- Section C.1.9, “When I execute nfsstart after reinstalling the directory services in the server or joining the server to an existing tree or deleting the NFAUUser object, messages such as "Error unloading, killed loaded module (ndsilib.nlm)", or "Unable to Login.: error -669 Could not authenticate ContextHandle. Load schinst and try again. Exiting...-669" display. What should I do?,” on page 139
- Section C.1.10, “While executing the SCHINST -n, what does the message “Error: Unable to login. Error Code: 35076” imply? This is displaying even when the Schema is fine and nfauuser object has been recreated.,” on page 140
- Section C.1.11, “During nfsstop, ndsilib.nlm does not get unloaded and it displays a message showing dependency on nwftpd.,” on page 140

C.1.1 When upgrading to NetWare 6.5 from NetWare 5.1 / NetWare 6.0, I am receiving a file overwrite warning for nfsstart.ncf. What should I do?

Select to overwrite the existing `nfsstart.ncf` file.

C.1.2 NFS Server is not loading on a server in tree with NetWare 5.1 NDS 7 replica ring. How can I resolve this?

For complete and correct functionality, ensure that the entire replica ring for any partition containing the NFS search_root contexts are on eDirectory 8.0 or later.

C.1.3 When I try to load NFS Services using Ndsilib.nlm, -669 error displays on the logger screen. How can I resolve this?

Manually execute `schinst -n -w` on system console.

Or

If the error continues even after executing schinst, then do the following:

1. Make a note of all the nodes that share the NFAUUser object in that context.
2. Delete the NFAUUser object.
3. Run `schinst -n -w` on all the nodes that you made note of in Step 1.

C.1.4 When the administrator changes the UNIX profile of the user, the updated profiles are not cached immediately. How can the profile be updated immediately?

The profile gets updated after two hours. To update the profile before this time in the system console, execute `ndsilib cache refresh`.

C.1.5 What is the significance of the SEARCH_ROOT parameter in SYS:ETC\NFS.CFG file?

This parameter is a list of contexts under which NFS* modules search for users that have their UNIX* profile populated.

There are some rules that need to be observed to add to this search list:

- The specified contexts should begin with a period (.)
- Contexts can be specified as .Ou1.Top or as .Ou=Ou1.O=Top
- Items in the list must be separated by commas (,) but no spaces.

C.1.6 How do I manually set the UNIX profile of a user?

After the product installation is complete and the schema has been extended to have UNIX attributes, appropriate ConsoleOne® snap-ins are now available to populate those attributes.

To populate the UNIX attributes, follow these steps:

1. In ConsoleOne, select an existing Group object or create a new Group object.
2. Right-click this *Group* object and then click *Properties*.
3. Go to the *UNIX Profile* tab and specify the desired *GID Value*.

4 Select/create a User object whose UNIX profile needs to be updated.

5 Right-click this *User* object and then click *Properties*.

6 Click the *UNIX Profile* tab and then specify the desired *UID Value*.

   For the Primary Group field, specify the GID specified in Step 3 and then click on Apply/OK.

Now there is a user whose UNIX profile is populated; but to make this visible to NFS modules, this User's context or one of its parents' context needs to appear in the SEARCH_ROOT parameter in SYS:ETC\NFS.CFG. For this change to get reflected (if a fresh context was added to the SEARCH_ROOT list), do an nfsstop and nfsstart again.

C.1.7 How do I set a User's UNIX profile to the Root's profile?

In Step 6 above, setting the UID Value to 0 in the User ID field attaches the root profile to that User object. Again, make sure that either this User's context or one of its parents' context is in the SEARCH_ROOT list.

C.1.8 Could not authenticate ContextHandle. Load schinst and try again. Exiting...9601

In the following procedure .NSC = Organization name in the eDirectory tree.

1 Ensure that in the NFS.CFG, the NIS_ADMIN_OBJECT_CONTEXT is set to .NSC or .O=NSC and that SEARCH_ROOT also has the same context in the same format and is preceded by a dot (.).

2 Execute `nfsstop` and run `SCHINST.NLM` (get the `SCHINST.LOG` and `NFS.CFG` after this).

If this does not work, then do the following:

1 Make a note of all the nodes that share the NFAUUser object in that context.

2 Delete the NFAUUser object.

3 Run `schinst -n -w` on all the nodes that you made note of in Step 1.

4 Capture the log and configuration files and see if it works.

C.1.9 When I execute nfsstart after reinstalling the directory services in the server or joining the server to an existing tree or deleting the NFAUUser object, messages such as "Error unloading, killed loaded module (ndsilib.nlm)", or "Unable to Login.: error -669 Could not authenticate ContextHandle. Load schinst and try again. Exiting...-669" display. What should I do?

You need to do the following:

1 Execute `nfsstop`.

2 Execute `schinst -n -w`

   2a (Conditional) When you reinstall the directory services in the server or join the server to an existing tree, run `nisinst`.

3 Execute `nfsstart`.

C.1.10 While executing the SCHINST -n, what does the message “Error*:* Unable to login. Error Code: 35076” imply? This is displaying even when the Schema is fine and nfauuser object has been recreated.

This implies that the server’s /etc/hosts file does not contain the simple host name (server name).

To resolve this, do the following:

1 Make sure that the server's `/etc/hosts` file contains the simple host name (server name).

   For example, if the format is

   ```
   192.168.2.3 server1.domain.com
   ```

   then change the entry to,

   ```
   192.168.2.3 server1.domain.com server1
   ```

2 Restart the server and schinst should work fine.

C.1.11 During nfsstop, ndsilib.nlm does not get unloaded and it displays a message showing dependency on nwftpd.

NetWare FTP Server (Nwftpd.nlm) has a dependency on ndsilib.nlm. So if nwftpd.nlm is running, unloading ndsilib.nlm through nfsstop.ncf will fail. To avoid this, please unload nwftpd.nlm first and then unload ndsilib.nlm

C.2 NFS Server FAQs

This section has NFS Server FAQs for Native File Access for UNIX.

- Section C.2.1, “Where can I view / modify the NFS attributes of a file apart from a UNIX client?,” on page 141
- Section C.2.2, “When using NetWare mode, why does the NetWare owner change for directories not reflect right away on UNIX client?,” on page 141
- Section C.2.3, “What can I do when the mount point of a previously exported path is active even after the path is removed from exports file?,” on page 142
- Section C.2.4, “What is the difference in the export options /pathname -ro -root and /pathname -ro -anon?,” on page 142
- Section C.2.5, “What is the result of specifying only -ro as the export option?,” on page 142
- Section C.2.6, “I’m trying to export a traditional volume using NFS Server, but it fails to mount on an NFS Client even though showmount shows the export. Why?,” on page 142

- Section C.2.7, “I am using IBM AIX 4.3 NFS client and am facing issues in simultaneous acquiring and releasing of locks over the same region of a file from two different processes. Can I avoid them?,” on page 142
- Section C.2.8, “While upgrading the iManager snap-ins from iManager configuration, the message "This package has an earlier version than the module that is currently installed. Installation has been cancelled." displays. How can I resolve this?,” on page 142
- Section C.2.9, “I unable to export a non-English path if I use Notepad on Windows to modify the exports file. How can I resolve this?,” on page 143
- Section C.2.10, “Does NFS Server support exports for directories with spaces in the name?,” on page 143
- Section C.2.11, “The non-root user is unable to create files in mounted directory that is exported as rw without root access. Can this be resolved?,” on page 143
- Section C.2.12, “File operations are failing when NDS_ACCESS is set to 0 in etc\nfs.cfg. Can this be resolved?,” on page 143
- Section C.2.13, “Is there a tool or a utility using which I can view the user and group attributes?,” on page 143
- Section C.2.14, “Why are the mount points inaccessible after upgrading from NetWare 6.5 (FCS, Support Pack 1, or 2) to OES NetWare?,” on page 143
- Section C.2.15, “Why do the file permissions change when it is updated from a mapped drive from Windows client?,” on page 144
- Section C.2.16, “How do i enable hard link support after applying OES NetWare SP2(NetWare 6.5 SP4),” on page 144
- Section C.2.17, “Issues with initializing XNFS after upgrading NetWare from SP7 to SP8,” on page 144

C.2.1 Where can I view / modify the NFS attributes of a file apart from a UNIX client?

If netstorage is installed, then in netstorage, beside where you view/modify NetWare attributes, there is a new tab to view/modify NFS Information.

C.2.2 When using NetWare mode, why does the NetWare owner change for directories not reflect right away on UNIX client?

This is because the UNIX client displays the cached results.

It does not issue an NFS call because the change in the NetWare owner metadata does not affect the modification timestamps. Therefore, the client assumes its cache to be valid and displays cached results.

When the client refreshes the cache it will display the updated information.

Alternately, execute a `touch` *`file/directory_name`* to force the updates.

C.2.3 What can I do when the mount point of a previously exported path is active even after the path is removed from exports file?

When you unshare or remove a path from exports list, unmount all the client mounts for that share.

C.2.4 What is the difference in the export options /pathname -ro -root and /pathname -ro -anon?

When you specify `/pathname -ro -root`, the path is exported as read-only with root access to all clients.

However, when you specify `/pathname -ro -anon`, the path is exported as read-only with anonymous access to all clients. If you do not specify the anon option, then on the client side root cannot do any operations on the mount point.Even executing a cd to the mount point is not allowed.

C.2.5 What is the result of specifying only -ro as the export option?

When you specify only `-ro` option for the pathname, it exports the path as read-only to all clients. Because by default, root-access and anonymous access are disabled, the root cannot perform any operations except mounting on the mount point.

C.2.6 I'm trying to export a traditional volume using NFS Server, but it fails to mount on an NFS Client even though showmount shows the export. Why?

The NFS Server on NetWare 6.5 does not support export of NetWare Traditional File system.

C.2.7 I am using IBM AIX 4.3 NFS client and am facing issues in simultaneous acquiring and releasing of locks over the same region of a file from two different processes. Can I avoid them?

To avoid the issues, use AIX 5.0 or later NFS clients.

C.2.8 While upgrading the iManager snap-ins from iManager configuration, the message "This package has an earlier version than the module that is currently installed. Installation has been cancelled." displays. How can I resolve this?

To resolve this and install the latest NFS iManager snap-ins after deleting the previous module.

To delete the module, go to iManager *menu* > *Configure* > *iManager configuration* > *Modules*.

C.2.9 I unable to export a non-English path if I use Notepad on Windows to modify the exports file. How can I resolve this?

Use iManager or language (i18n) enabled editors to export non-English paths.

C.2.10 Does NFS Server support exports for directories with spaces in the name?

NFS Server does not support export of directories with spaces in the name. Make sure that users do not export a directory containing spaces. If users try to export a directory with spaces in the name, the exports fails without any message displayed.

C.2.11 The non-root user is unable to create files in mounted directory that is exported as rw without root access. Can this be resolved?

When the default umask of 022 is applied to the mount point, the non-root user must be the owner in order to have permission to work at the mount point.

To grant the non-root user permissions to perform all the operations:

1. After exporting a volume with root access and all rights, mount it on UNIX and execute a `chmod nnn` command along with a combination of chown and chgrp to the user's UID/GID.
2. Umount the mount point.
3. Export the same volume again with rw permissions.
4. Mount it on UNIX.

C.2.12 File operations are failing when NDS_ACCESS is set to 0 in etc\nfs.cfg. Can this be resolved?

NFS Server does not support the remote NIS feature.

To resolve this, modify etc\nfs.cfg and set NDS_ACCESS= 1 and restart nfsservices.

C.2.13 Is there a tool or a utility using which I can view the user and group attributes?

You can use the Ldapsearch tools to write all types of queries to get the information from eDirectory, including users and groups data. For more information on the Ldapsearch tools, refer the Novell eDirectory 8.6 documentation:Using LDAP Tools on Linux or Solaris (http://www.novell.com/documentation/ndsedir86/index.html?page=/documentation/ndsedir86/taoenu/data/a6qjdjx.html).

C.2.14 Why are the mount points inaccessible after upgrading from NetWare 6.5 (FCS, Support Pack 1, or 2) to OES NetWare?

This is because the NFS filehandle format has changed. To resolve this, unmount and remount the paths on the NFS clients.

C.2.15 Why do the file permissions change when it is updated from a mapped drive from Windows client?

This is because certain Windows based applications such as Wordpad do not actually modify files. When you save your modifications, they delete the original and save the modified version as a new file. Therefore, the new file gets the ownership of the modifying NetWare- windows user, and default permissions.

C.2.16 How do i enable hard link support after applying OES NetWare SP2(NetWare 6.5 SP4)

OES SP2 has the implementation of NSS hardlinks. For details on enabling hard link support for NFS, see Technical Information Document (http://support.novell.com/cgi-bin/search/searchtid.cgi?10099471.htm)

C.2.17 Issues with initializing XNFS after upgrading NetWare from SP7 to SP8

After upgrading your NetWare server to SP8, XNFS initialization fails. You will get the following error message:

```
Error: NFS services initialization failed during eDirectory interface library
(ndsilib.nlm) initialization - Error Code : 9600. Unloading XNFS.NLM.
```

Use the following workaround to resolve this error:

Manually execute `schnist -n -w` from your system console. If the error remains unresolved after this step, use the following steps to resolve it:

1. Make a note of all the nodes that share the NFAUUser object in that context.
2. Delete the NFAUUser object.
3. Run `schinst -n -w` on all the nodes.

C.3 NIS Services FAQs

This section has NIS Services FAQs for Native File Access for UNIX.

- Section C.3.1, “Why does the Solaris NIS Clients to NetWare NIS Server have problems? How can it be resolved?,” on page 145
- Section C.3.2, “When is the NISSERV_ ServerName object created and what is its role in NIS functionality?,” on page 145
- Section C.3.3, “When I select the properties of the NISSERVER object, an error message displays. What should I do?,” on page 145
- Section C.3.4, “I am unable to migrate or create a domain using makenis? What do I need to do?,” on page 145
- Section C.3.5, “I am unable to change the password from a UNIX machine for a migrated user. What do I need to do?,” on page 146

- Section C.3.6, “What is the 0_ 2 user object that is automatically and randomly created when installing two servers in to the same NDS tree?,” on page 146
- Section C.3.7, “I am viewing a series of messages such as "Nullpointer passed to routine Kmutex" when running makenis? How can this be resolved?,” on page 146
- Section C.3.8, “What are the ways to view the list of domains served by the nisServer object?,” on page 146

C.3.1 Why does the Solaris NIS Clients to NetWare NIS Server have problems? How can it be resolved?

The Solaris NIS Clients to NetWare NIS Server has problems if the entry in the /etc/hosts file located in the Solaris client does not match the entry in etc/hosts file on NetWare or in DNS in a case-sensitive fashion.

To resolve this, modify the etc/hosts in the Solaris client to be in the same case as in etc/hosts on NetWare Server or in DNS.

C.3.2 When is the NISSERV_ *ServerName* object created and what is its role in NIS functionality?

The NISServ_ *Servername* object holds the list of domains served by the NetWare NIS Server. It is created by the NISINST.NLM executed during the installation. For correct functionality of NIS Server, set the following parameters properly:

- The NIS_SERVER_CONTEXT parameter in SYS:ETC\NIS.CFG, indicates the NDS context where the NIS Server object exists.
- The NIS_SERVER_NAME parameter in SYS:ETC\NIS.CFG indicates the NIS Server object used to hold the NIS Domains that are being served by the NetWare NIS Server.

C.3.3 When I select the properties of the NISSERVER object, an error message displays. What should I do?

1. The schema might not be fully extended. This occurs when the NetWare 6 server is attached to a NetWare 5.1 tree.
2. Verify `ETC\SCHINST.LOG` to view whether the schema is extended.
3. Nfsadmin might not be running.

   Make sure that NFSADMIN is running on the target Server.

C.3.4 I am unable to migrate or create a domain using makenis? What do I need to do?

Make sure that ndsilib is running.

Verify `ETC\NIS.CFG` to view whether the NisServer context and name are set properly.

C.3.5 I am unable to change the password from a UNIX machine for a migrated user. What do I need to do?

1. Ensure that the NetWare server is set as the default NIS server of the UNIX system.
2. Use the UNIX command yppasswd for setting the NIS user password. The `NISSWDD.NLM` must be loaded on the NetWare server.
3. Execute ypset to set the default domain. The default domain must be the same as the UNIX client domain.

C.3.6 What is the 0_ *2* user object that is automatically and randomly created when installing two servers in to the same NDS tree?

When an object is created on eDirectory replica 1 and before it replicates to all replica servers, another object with the same name is created from another replica, the name of one of the objects changes.

This ensures that the two objects have unique names. The name will be in the format *number_ n.*

For example, the object name could be 0_2 or 0_3 with the NFAUUser appended as a suffix.

On viewing such objects, delete them.

C.3.7 I am viewing a series of messages such as "Nullpointer passed to routine Kmutex" when running makenis? How can this be resolved?

You might be running makenis on a server with no DS replica and when the Master replica is down.

These messages are displayed erroneously.

C.3.8 What are the ways to view the list of domains served by the nisServer object?

You can view the list of domains served by the nisServer object in eDirectory in the following ways:

- In the ConsoleOne, see the membership attribute of the nisServer object.
- In the NRM, see the membership attribute of the nisServer object
- Through the `DSBROWSE.NLM`, see the membership attribute of the nisServer object.

Documentation Updates

D

This *Novell Native File Access Protocols Guide* has been updated with the following information:

- Section D.1, “November 9, 2009,” on page 147
- Section D.2, “June, 2009,” on page 147
- Section D.3, “December, 2008,” on page 147
- Section D.4, “October, 2006 (NetWare 6.5 Support Pack 6),” on page 147

D.1 November 9, 2009

This guide has been modified for publication on the NetWare 6.5 SP8 Documentation Web site.

D.2 June, 2009

- A typo was corrected in Chapter 7, “Working with UNIX Machines,” on page 49.

D.3 December, 2008

- Guide updated to the revised Novell documentation standards
- Updated for user change requests and links

D.4 October, 2006 (NetWare 6.5 Support Pack 6)

Location	Change
Windows and Macintosh chapters.	Changes to the iManager plug-in for CIFS/AFP have been incorporated into the document.