

Novell NetWare 6

www.novell.com

NOVELL NATIVE FILE ACCESS
PROTOCOLS INSTALLATION AND
ADMINISTRATION GUIDE



Novell[®]

Legal Notices

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

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

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

Copyright © 2001-2002 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.

U.S. Patent No. 5,157,663; 5,349,642; 5,455,932; 5,553,139; 5,553,143; 5,572,528; 5,594,863; 5,608,903; 5,633,931; 5,652,859; 5,671,414; 5,677,851; 5,692,129; 5,701,459; 5,717,912; 5,758,069; 5,758,344; 5,781,724; 5,781,724; 5,781,733; 5,784,560; 5,787,439; 5,818,936; 5,828,882; 5,832,274; 5,832,275; 5,832,483; 5,832,487; 5,850,565; 5,859,978; 5,870,561; 5,870,739; 5,873,079; 5,878,415; 5,878,434; 5,884,304; 5,893,116; 5,893,118; 5,903,650; 5,903,720; 5,905,860; 5,910,803; 5,913,025; 5,913,209; 5,915,253; 5,925,108; 5,933,503; 5,933,826; 5,946,002; 5,946,467; 5,950,198; 5,956,718; 5,956,745; 5,964,872; 5,974,474; 5,983,223; 5,983,234; 5,987,471; 5,991,771; 5,991,810; 6,002,398; 6,014,667; 6,015,132; 6,016,499; 6,029,247; 6,047,289; 6,052,724; 6,061,743; 6,065,017; 6,094,672; 6,098,090; 6,105,062; 6,105,132; 6,115,039; 6,119,122; 6,144,959; 6,151,688; 6,157,925; 6,167,393; 6,173,289; 6,192,365; 6,216,123; 6,219,652; 6,229,809. Patents Pending.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

Novell Native File Access Protocols Installation and Administration Guide

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

Novell Trademarks

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

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

eDirectory is a trademark of Novell, Inc.

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

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

NMAS is a trademark of Novell, Inc.

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

Novell Client is a trademark of Novell, Inc.

Novell Cluster Services is a trademark of Novell, Inc.

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

Third-Party Trademarks

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

Preface

This book 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 book is divided into the following chapters:

- ♦ **Chapter 1, “Overview,” on page 7** describes the benefits of Novell Native File Access Protocols software.
- ♦ **Chapter 2, “Installing Novell Native File Access Protocols on a NetWare 6 Server,” on page 9** describes how to install the software on a NetWare server.
- ♦ **Chapter 3, “Working with Macintosh Computers,” on page 17** describes how to set up and manage Macintosh workstations and how to access files on the network.
- ♦ **Chapter 4, “Working with Windows Computers,” on page 23** describes Windows authentication methods and passwords, how to set up and manage Windows workstations, and how to access files on the network.
- ♦ **Chapter 5, “Setting Up Novell Native File Access Protocols in a NetWare 6 Cluster,” on page 43** explains Novell Cluster Services™ and how to configure the Novell Native File Access Pack software for Macintosh and Windows computers in a clustered environment.
- ♦ **Chapter 6, “Working with UNIX Machines,” on page 49** describes how to set up and manage UNIX* workstations and how to access files on the network with Native File Access for UNIX.

Documentation Conventions

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

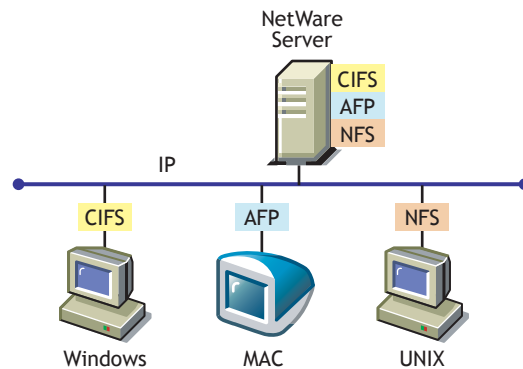
Also, a trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

1

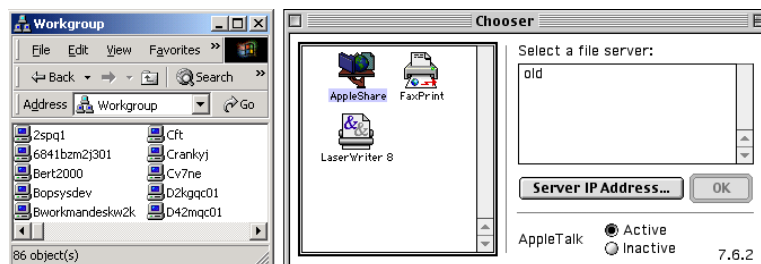
Overview

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. No client configuration. No problem.

Novell Native File Access Pack 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.



Network Neighborhood

Chooser

By consolidating user management through Novell Directory Services® (NDS®), Native File Access Protocols simplifies overall network administration. All users who need access to the network are represented in NDS through User objects, which enables you to easily and effectively assign trustee rights and access control 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).

Getting Started

Novell Native File Access Pack is easy to install. To get started, continue with [Chapter 2, “Installing Novell Native File Access Protocols on a NetWare 6 Server,”](#) on page 9.

2

Installing Novell Native File Access Protocols on a NetWare 6 Server

To install the Novell® Native File Access Protocols, you must complete the following tasks:

1. Prepare the NetWare® 6 server.
See “[NetWare Server Prerequisites](#)” on page 9.
2. Set up an Administrator Workstation.
See “[Administrator Workstation Prerequisites](#)” on page 10.
3. Ensure all of the client computers (Windows, Macintosh, and UNIX) that will use the Novell Native File Access Protocols software to access network resources are running a supported version of their respective operating systems.
See “[Client Computer Prerequisites](#)” on page 11.
4. Install the Native File Access Protocols software.
See “[Installing the Software](#)” on page 11.

NetWare Server Prerequisites

The NetWare 6 server must meet the following configuration requirements in order to run the Novell Native File Access Protocols software.

TIP: You can quickly check the server configuration with the NWCONFIG utility. At the server console, enter `NWCONFIG` and then select Product Options > View/Configure/Remove Installed Products.

- NetWare 6 server operating system.
- (For Macintosh/AFP only) Macintosh Name Space must be loaded on each traditional volume before installing Novell Native File Access Protocols.

To load Macintosh Name Space to a volume, enter the following commands at the server console:

```
LOAD MAC.NLM
```

```
ADD NAME SPACE MACINTOSH TO VOLUME volume_name.
```

- (For Macintosh/AFP only) AFP.NLM and APPLETLK.NLM must be unloaded from the server (if currently running).
 - (Conditional) If BorderManager® Enterprise Edition version 3.5 or later is running in the same eDirectory™ tree as the NetWare server where you are installing Novell Native Access software, you must create a Login Policy Object (LPO).
- 1 Log in to the server running BorderManager.

- 2** Run the NetWare Administrator utility (NWADMIN.EXE) located in the PUBLIC\WIN32\ directory.
- 3** From the Object menu, click Create > Login Policy > OK.
- 4** (Conditional) If the server running BorderManager does not have a local NDS[®] replica, complete the following:
 - 4a** From NetWare Administrator, select the Security container and the LPO.
 - 4b** Click Trustees of This Object > Add Trustee.
 - 4c** Select the Server object of the server running BorderManager.
 - 4d** Deselect all Object rights.
 - 4e** Click Selected Properties > SAS: Policy Credentials.
 - 4f** From Property Rights, click Read/Write > OK.

Administrator Workstation Prerequisites

You will install, configure, and manage Novell Native File Access services 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 installed
 - ◆ Windows NT/2000 running Novell Client for Windows NT/2000 version 4.80 or later installed

[Download Novell Client software \(http://download.novell.com\)](http://download.novell.com).

- Client NCI 1.5.7 (or later) for Windows (Strong Encryption) installed
[Download the NCI Encryption Module software \(http://download.novell.com\)](http://download.novell.com).

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

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

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, or Windows NT version 4
- 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 Free BSD

Installing the Software

You can install the Novell Native File Access Protocols software as part of the NetWare 6 installation, or later as a separate process.

Installing the Software during Server Installation

Novell Native File Access Protocols are part of the NetWare 6 server installation program. Instructions are located in the *NetWare 6 Overview and Installation Guide*.

If you did not install the Native File Access Protocols software during the NetWare 6 server installation, you can install it by following the procedures in the next section.

Installing the Software after Server Installation

Novell Native File Access Protocols can be installed after installing a NetWare 6 server using NetWare Deployment Manager or the Graphical Server Console screen. Each method provides an easy-to-follow installation program that guides you through the required steps.

Accessing and Starting the Installation Program from the NetWare Server Console

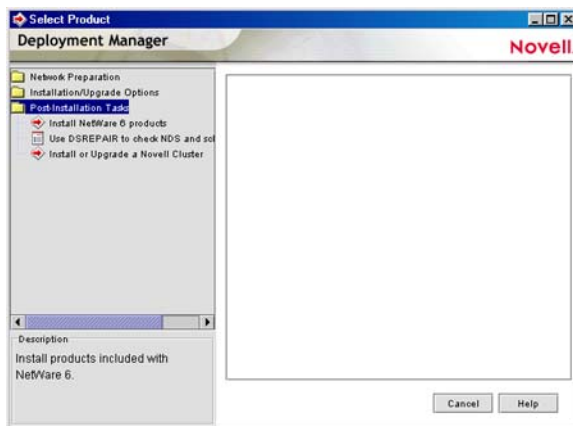
- 1** Obtain the *NetWare 6 Operating System* CD.
- 2** Ensure your NetWare 6 server meets the prerequisites described in “**NetWare Server Prerequisites**” on page 9.
- 3** Ensure your Administrator Workstation meets the prerequisites described in “**Administrator Workstation Prerequisites**” on page 10.
- 4** At the NetWare 6 server console, enter **STARTX** to launch the graphical server console.
- 5** Click Novell > Install.
- 6** At the Installed Products screen, click Add.
- 7** Enter the path to the *NetWare 6 Operating System* CD and select the PRODUCT.NI file.
The installation program begins.

Accessing and Starting the Installation Program from the NetWare Deployment Manager

- 1** Obtain the *NetWare 6 Operating System* CD.

- 2** Ensure your NetWare 6 server meets the prerequisites described in “[NetWare Server Prerequisites](#)” on page 9.
- 3** Ensure your Administrator Workstation meets the prerequisites described in “[Administrator Workstation Prerequisites](#)” on page 10.
- 4** At the Administrator Workstation, log in to the destination server that will run the Novell Native File Access Protocols software.
- 5** Insert the *NetWare 6 Operating System CD*.
- 6** Run NetWare Deployment Manager (NWDEPLOY.EXE) located on the root of the *NetWare 6 Operating System CD*.
- 7** Click Post-Installation Tasks > Install NetWare 6 Products.

TIP: If you are prompted to log in again while running NetWare Deployment Manager, you can enter the IP address of the server by clicking Details.



- 8** At the Product Selection screen, check the Novell Native File Access Protocols check box.
- 9** Click Next.

The installation program begins.

Installing the Software

- 1** At the Components screen, select the Native File Access components you want to install and then click Next.
 - ◆ If you choose to install the Native File Access for Macintosh (AFP*) component, the software will be installed transparently during the NetWare installation process. No further interaction is required for the Native File Access for Macintosh software installation. You can skip to [Step 8 on page 15](#).

For information on configuring Native File Access for Macintosh services and managing Mac users, see [Chapter 3, “Working with Macintosh Computers,” on page 17](#).
 - ◆ If you choose to install the Native File Access for Windows (CIFS) component, continue with [Step 2](#).

For information on configuring Native File Access for Windows services and managing Windows users, see [Chapter 4, “Working with Windows Computers,” on page 23](#).
 - ◆ For detailed information on installing and configuring the Native File Access for UNIX component, see [Chapter 6, “Working with UNIX Machines,” on page 49](#).

2 Click Next.

3 At the Server Properties screen, configure the following server settings and then click Next.

- ◆ **Server Name:** Enter a unique name for the NetWare server running CIFS that will appear in Network Neighborhood when users browse the network. The server name cannot be longer than 15 characters and must be different from the actual NetWare server name.

The default Server Name is the NetWare server name with an added underscore (_) and a W. For example, a NetWare server named SERVER1 defaults to SERVER1_W.

- ◆ **Server Comment (Optional):** Enter a comment for the server. The text in the Server Comment field displays when viewing details of the server from a Windows workstation.
- ◆ **Enable Unicode:** Specify whether to enable Unicode character support. When checked, this option enables Unicode characters that are used in double-byte languages.

To support Unicode, an additional file named UNINOMAP.TXT must be created and saved in the SYS:\ETC directory. When the UNICODE parameter is set to On, the UNINOMAP.TXT file is used to resolve Unicode-to-ASCII "no-map" problems.

To specify "no-map" cases in the UNINOMAP.TXT file, enter the first Unicode value to watch for and then the second value representing the ASCII replacement code. For example:

```
0178 98
```

```
20AC CC
```

Save the values in the UNINOMAP.TXT file. If an unmappable character is encountered, the system uses the ASCII substitution character specified in the file.

4 At the Authentication screen, select one of the following authentication methods and then click Next.

- ◆ **Local:** Select if your Windows users will authenticate using NDS.

With Local authentication, the NetWare server running Novell Native File Access Pack software performs the user authentication when clients are a member of a workgroup. With local authentication, the username and password on NetWare must match the username and password used to log in to the Windows workstation.

If you select Local as your authentication method, fill in the following fields:

- ◆ **Workgroup Name:** Enter the name of the domain or workgroup that the NetWare server will belong to. In this case, *workgroup* and *domain* are interchangeable terms.
- ◆ **WINS Address:** Enter the IP address of the WINS server to be used to locate the primary domain controller (PDC), if the PDC and server running Novell Native File Access Pack software are on different subnets.

Windows Internet Naming Service (WINS), part of the Microsoft Windows NT and 2000 Servers, manages the association of workstation names and locations with Internet Protocol (IP) addresses. WINS automatically creates and maintains a computer name and corresponding IP address mapping entry in a table. When a computer is moved to another geographic location, the subnet part of the IP address is likely to change. Using WINS, the new subnet information will be updated automatically in the WINS table.

- ◆ **Domain:** Select if your Windows users will authenticate using a Microsoft Networking Domain.

It is important to remember that a simple password is *not* required when using domain authentication. Because the password is kept on the Windows domain controller, it is not possible to use the Windows native Change Password feature to change the password. Instead, you must use the Windows domain management utilities. To work properly, the username and password on the domain controller must match the username and password used to log in to the Windows workstation.

If you select Domain as your authentication method, fill in the following fields:

- ◆ **PDC Is on the Same Subnet as This Server:** Select this option if the primary domain controller (PDC) is on the same subnet as the NetWare server.
 - ◆ **Specify PDC Using DNS or WINS:** Select this option to use DNS or WINS to specify the primary domain controller (PDC).
 - ◆ **PDC Name:** A PDC server name and static IP address are needed if the PDC is on a different subnet. This field should be used only when there is a valid reason for overriding WINS or DNS.
 - ◆ **PDC Address:** The address of the PDC must be static; otherwise, if the PDC reboots and the address changes, the server running Novell Native File Access Pack software will not be able to contact the PDC.
- 5** At the IP Addresses screen, specify the IP addresses on the server that you want to be attached to the CIFS protocol, or keep the default selection to Enable CIFS on All Addresses (recommended), and then click Next.
 - 6** At the Share Point Setup screen, specify additional NetWare volumes or folders that you want to appear as share points in Network Neighborhood, or keep the default selection to Share all Mounted Volumes, and then click Next.

Any volume or directory on the server can be specified as a shared point and made accessible via the Network Neighborhood. If no share points are specified, then all mounted volumes are displayed in Network Neighborhood.

If you want to specify a share point, click New, fill in the following fields, and click Submit.

- ◆ **Directory:** Enter the path to the server volume or directory which will be the root of the sharepoint. Beginning at the volume name, the full path must be specified and it must end with a backslash (\). For example:

```
VOL1 : GRAPHICS \
```

- ◆ **Share Name:** Enter the name by which the sharepoint will be displayed to Windows computers. For example, if you enter "Lots of Pics" as the share name associated with VOL1\GRAPHICS, then Windows workstations browsing the network will see "Lots of Pics" instead of "VOL1\GRAPHICS."
- ◆ **Connections:** Enter the number of connections that will be allowed to access the sharepoint. Or, check Unlimited to allow an unlimited number of connections.
- ◆ **Comment:** Enter a description for the sharepoint that appears in Network Neighborhood.

- 7** At the Context Setup screen, specify the NDS contexts for your Windows (CIFS) users who need access to this NetWare server and then click Add.

NDS contexts added here are saved in a list in the CIFS context search file (SYS:\ETC\CIFSCTXS.CFG). When the Windows user enters a username, the Novell Native File Access Pack software searches through each context in the list until it finds the correct User object.

For example, if you had users with full NDS distinguished names such as Robert.sales.acme, Maria.graphics.marketing.acme, Sophia.graphics.marketing, and Ivan.marketing.acme, then you would enter the following contexts:

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

NOTE: 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.

The CIFSCTXS.CFG context search file can be edited manually after installation. For more information, see [“Specifying Contexts in the Context Search File” on page 28](#).

- 8** Check the Summary screen and then click Finish.

The installation program copies the required files to your server.

- 9** Restart the server by entering the following command at the server console:

```
RESTART SERVER
```

Starting and Stopping AFP and CIFS Protocols Service

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, enter **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, enter **AFPSTOP** to unload the Macintosh (AFP) protocols on the server.

Windows (CIFS) Protocols

- 1 At the server console, enter **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, enter **CIFSSTOP** to unload the Windows (CIFS) protocols on the server.

What's Next?

After installing the Native File Access Pack software, you must create simple passwords for Macintosh, Windows, and UNIX users before they can access files on the server using their native protocols.

To set up and manage Macintosh users, see [Chapter 3, "Working with Macintosh Computers,"](#) on [page 17](#).

To set up and manage Windows users, see [Chapter 4, "Working with Windows Computers,"](#) on [page 23](#).

To set up and manage UNIX users, see [Chapter 6, "Working with UNIX Machines,"](#) on [page 49](#).

3

Working with Macintosh Computers

This chapter contains the following information:

- ♦ [Administrator Tasks for Native File Access for Macintosh Services \(page 17\)](#)
- ♦ [Macintosh End User Tasks \(page 19\)](#)

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:

- ♦ [Creating Simple Passwords for Several Macintosh Users \(page 17\)](#).
- ♦ [Editing the Context Search File \(page 17\)](#).
- ♦ [Creating a Guest User Account \(page 18\)](#).
- ♦ [Renaming Volumes \(page 18\)](#).

Creating Simple Passwords for Several Macintosh Users

You can create simple passwords for users one at a time using ConsoleOne[®]. But 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 NDS[®] username and NDS password. Once the NDS password is verified, a simple password is automatically created and stored in NDS. The simple password is the same as the NDS 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.

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 enters 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 NDS context and username are longer than 31 characters, you must use a search list to provide access.

TIP: Macintosh users do not need to enter 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, enter the contexts to search.

For example, if you had users with full NDS distinguished names such as Robert.sales.acme, Maria.graphics.marketing.acme, Sophia.graphics.marketing, and Ivan.marketing.acme, then you would enter 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 enter only a username and the simple password. The system finds the User object in the context specified in the CTXS.CFG file.

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 the Guest object and then clicking Rights to Files and Folders.
- 3** Remove the ability for the user to change the password by clicking Restrictions and then unchecking Allow User to Change Password.
- 4** Enable the Guest account by adding the full NDS context of the Guest object to the context search file as described in [“Editing the Context Search File” on page 17](#).
- 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.

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, enter 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.

Once 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.

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:

- ♦ [Accessing Network Files \(page 19\)](#).
- ♦ [Logging In to the Network as Guest \(page 20\)](#).
- ♦ [Changing Passwords from a Macintosh Computer \(page 20\)](#).
- ♦ [Assigning Rights and Sharing Files from a Macintosh Computer \(page 20\)](#).

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** Enter the IP address or DNS name of the NetWare[®] server, and then click Connect.
- 3** Enter 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.

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 18, 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** Enter the IP address or DNS name of the NetWare server, and then click Connect.
- 3** Click Guest Login > Connect.

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

Changing Passwords from a Macintosh Computer

Macintosh users can change their passwords. When they change their simple password, their NDS 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** Enter the IP address or DNS name of the NetWare server, and then click Connect.
- 3** Enter the username.
- 4** Click Change Password.
- 5** Enter the old password and the new password, and then click OK.

Assigning Rights and Sharing Files from a Macintosh Computer

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

TIP: For more information on how to use ConsoleOne to set up and manage rights, see the [ConsoleOne User Guide](http://www.novell.com/documentation/lg/consol13/index.html) (<http://www.novell.com/documentation/lg/consol13/index.html>) or view the ConsoleOne Online Help.

NetWare Rights versus Macintosh Rights

Using Chooser 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 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.

NetWare uses both inherited *and* explicit rights to determine the actual rights that a user has. NetWare 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.

NetWare 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 NetWare folder, only the User/Group assignments are visible if there is an explicit assignment on the folder. If the NetWare 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 NetWare 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 NetWare utilities such as ConsoleOne.

When specifying Owners, Users, and Groups, there is no way to select from current groups. You must enter the correct NetWare name and context (fully distinguished NDS 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 NetWare environment, users can change access rights if they have been granted the Access Control right for the folder. In NetWare, an owner means the one who created the file. A NetWare owner has no rights by virtue of ownership. In the NetWare 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 NetWare owner is not the current user. If the current user does not have rights to change access and is also the NetWare 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 NetWare, 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 through other NetWare 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 NetWare allows multiple users and groups to be assigned file access rights. If both users and groups have access to a NetWare 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 enters 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 NetWare 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

Working with Windows Computers

This chapter contains the following information:

- ♦ [Administrator Tasks for Native File Access for Windows Services \(page 23\)](#)
- ♦ [Windows End User Tasks \(page 34\)](#)

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:

- ♦ [Creating Simple Passwords for Windows Users \(page 23\)](#)
- ♦ [Enabling Users to Change Their Simple Passwords with NetWare Remote Manager \(page 27\)](#)
- ♦ [Understanding Synchronization of NetWare Passwords and Simple Passwords \(page 27\)](#)
- ♦ [Specifying Contexts in the Context Search File \(page 28\)](#)
- ♦ [Managing Network Access with ConsoleOne \(page 28\)](#)
- ♦ [Providing Network Access to Domain Users \(page 29\)](#)
- ♦ [Customizing the Network Environment for CIFS \(page 29\)](#)
- ♦ [Viewing Configuration Details \(page 34\)](#)

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 ConsoleOne[®]. For more information, see the *ConsoleOne Users Guide* (<http://www.novell.com/documentation/lg/consol12d/index.html>).

In addition, 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.

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

NOTE: For information about selecting an authentication method during the installation, see [Step 4 of “Installing the Software” on page 11](#).

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 was selected during installation. 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/NDS® 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 Controller. 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 enter 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. 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 entering 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 which are not installed with Novell Client software. 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.

Two Methods for Creating Simple Passwords for Windows Users

You can create simple passwords either with ConsoleOne or NetWare Remote Manager.

Using ConsoleOne

The ConsoleOne management utility lets you create simple passwords for users one at a time by completing the following steps.

- 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 [“Administrator Workstation Prerequisites” on page 10](#).

- 2** Run CONSOLEONE.EXE (located in the \PUBLIC\MGMT\CONSOLEONE\1.2\BIN directory).
 - 3** Right-click the User object and 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:** Enter a unique password for the user.
 - ◆ **Confirm Simple Password:** Enter the same password for confirmation.
- NOTE:** If the simple password is different from the NetWare password, users enter the simple password when accessing the network with native protocols and they enter 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 that 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 NetWare Remote Manager

You can also use NetWare Remote Manager (previously known as NetWare Management Portal) to create simple passwords either for an individual user or for multiple users at once.

Accessing NetWare Remote Manager

- 1** In the Address field of your Web browser, enter the IP address of the server where you installed Novell Native File Access Protocols.

If the NetWare Enterprise Web Server is installed on your server, you will have to add the port number 8008 at the end of the IP address. For example, if your Portal server's IP address were 137.65.123.11, you would enter `http://137.65.123.11:8008` in the Address field of your browser.

- 2** At the login prompt, enter the server administrator username and password.
- 3** In the left frame, click Manage eDirectory > NFAP Security.

The NFAP security page appears.

TIP: For more information about using NetWare Remote Manager, see the [NetWare Remote Manager Administration Guide](http://www.novell.com/documentation/lg/nw6p) in the NetWare 6 documentation (<http://www.novell.com/documentation/lg/nw6p>).

Creating Simple Passwords for Multiple Users

1 In the NFAP Multi-User Simple Password Set Utility section, select a method for designating which users on your network will receive simple passwords. There are two methods for selecting users:

- ◆ To select all User objects in that particular context, enter a full context in the NDS Context field.
- ◆ To select all User objects in the NDS tree, check the Traverse Context Tree for User Objects check box.

NOTE: Searching the entire NDS tree might take several minutes.

2 (Optional) If you want an automatic message to be sent to the selected users notifying them of their simple password, check the Send Password to User check box.

IMPORTANT: To use the Send Password to User feature, you must first use the Access Mail Notification Control Page to set up NetWare Remote Manager to perform e-mail notification.

The Access Notification Control Page is available by clicking the configuration icon on the top of the screen.

3 Specify a common simple password for all users by checking the User Supplied Password check box and entering a password in the field provided.

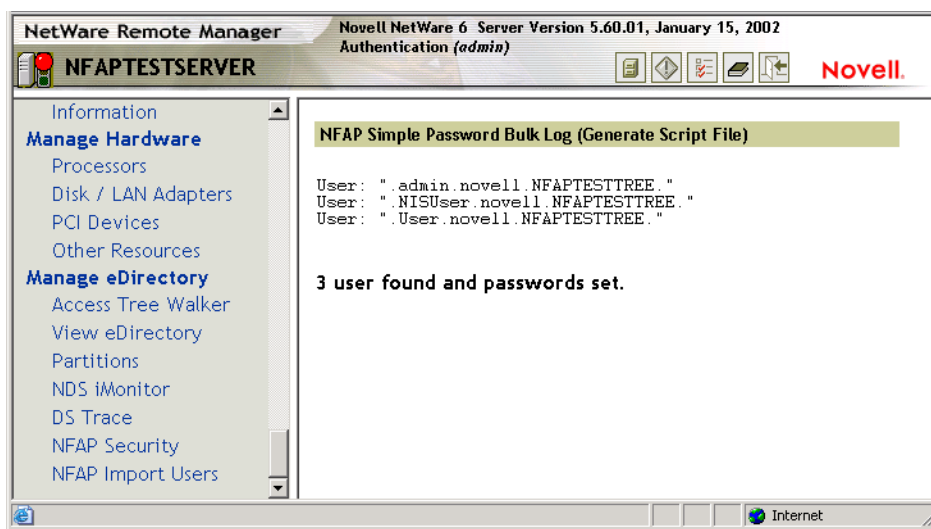
4 Check the Generate Script File check box and enter a filename for the script file.

The generated script file contains a list of users and will be processed by the utility to create the simple passwords for those users. You can choose any name for the script file.

5 (Optional) You can verify the contents of a generated script file before actually processing the script file. We recommend that you test the script file until it contains the appropriate list of users.

5a Make sure the Process Script File check box is unchecked and then click Start.

The contents of the script file displays in the right frame.



IMPORTANT: No file will be generated and you will get an error in the browser if you do not fill in a filename for the script file.

5b If the list is what you want, go to the next step and process the script file. If the list is not correct, click the Back button on your browser, change the NDS context settings, and click Start again. Repeat this process until the script file contains the appropriate information.

6 When you are ready to process the script file, check the Process Script File check box and enter the name of the script file.

The names in the Generate Script File and Process Script File fields must match exactly.

7 Click Start to process the script file.

The utility creates simple passwords for all of the users listed in the script file.

Creating a Simple Password for a Single User

1 In the NFAP Single-User Simple Password Set Utility section, enter the username (including the full context) in the Username and Context field.

2 Enter the text to be used for the user's simple password in the New Password field.

3 Click Set.

IMPORTANT: Remember to notify the user of the password.

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 enter their NetWare username (without context) and their corresponding simple password.

Enabling Users to Change Their Simple Passwords with NetWare Remote Manager

You can use ConsoleOne to assign the necessary rights so that users can change simple passwords with the NetWare Remote Manager tool.

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 [“Administrator Workstation Prerequisites” on page 10](#).

2 Run CONSOLEONE.EXE (located in the \PUBLIC\MGMT\CONSOLEONE\1.2\BIN directory).

3 Right-click the User object and 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.

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 since 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: Password synchronization is simpler for Macintosh users. 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.

Specifying Contexts in the Context Search File

During the installation, you specified the NDS contexts for Windows users who require access to the network. These contexts are saved in the context search file. When Windows users enter 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 running Novell Native File Access Protocols.
- 2** On separate lines, enter the full contexts to search.

For example if you had users with full NDS distinguished names such as Robert.sales.acme, Maria.graphics.marketing.acme, Sophia.graphics.marketing, and Ivan.marketing.acme, then you would enter 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, enter **CIFSSTOP** to unload the current context search file.
- 5** Enter **CIFSSTRT** to load the new context search file and apply the changes.

When Windows users log in, they enter only a username and the simple password. The system finds the User object in the context specified in the CIFSCTXS.CFG file.

IMPORTANT: Remember that users must have a simple password before they can access the network.

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 “Administrator Workstation Prerequisites” on page 10.

- 2 Run CONSOLEONE.EXE located in \PUBLIC\MGMT\CONSOLEONE\1.2\BIN\.
- 3 Set up and manage rights as described in the *ConsoleOne Users Guide* (<http://www.novell.com/documentation/lg/consol12d/index.html>).

Providing Network Access to Domain Users

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

- 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 entering the IP address of the server into the URL field of an Internet browser.

See the *NetWare Remote Manager Administration Guide* in the NetWare 6 documentation (<http://www.novell.com/documentation/lg/nw6p>).

- 3 In the left frame, click Manage eDirectory > NFAP Import Users.

- 4 Browse to the NDS 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.TXT file, which contains all the contexts of all users.

Status of the import is given on the interval that you select.

- 6 When the import is complete, click Done to clear the screen.

Customizing the Network Environment for CIFS

Administrators can customize the network environment for Windows workstations (CIFS) by using one of the following methods:

- ♦ [Using ConsoleOne to Configure CIFS \(page 29\)](#)
- ♦ [Using the CIFS.CFG File to Configure CIFS \(page 31\)](#)

IMPORTANT: You can use ConsoleOne to configure CIFS only if you have installed the SP1 software on the server running Novell Native File Access Protocols. In fact, if SP1 software is installed on your server, the CIFS.CFG file will be disabled and contain a note to use ConsoleOne for configuration.

Using ConsoleOne to Configure CIFS

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

Make sure that the Administrator Workstation meets the prerequisites described in “Administrator Workstation Prerequisites” on page 10.

- 2** Run CONSOLEONE.EXE (located in \PUBLIC\MGMT\CONSOLEONE\1.2\BIN\).
- 3** Right-click the Server object and then click Properties.
- 4** Click the CIFS tab and select one of the three CIFS pages: Config, Attach, or Shares.
- 5** Enter the desired parameters in the fields provided.
See the page description sections below for details.
- 6** Click Apply to save your settings.

Config Page Parameters

The following parameter fields appear on the Config Page under the CIFS tab in ConsoleOne:

- ◆ *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.
- ◆ *Comment* is the comment associated with the server name discussed above. This comment is displayed when viewing details.
- ◆ *WINS 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.
- ◆ *Unicode* specifies whether Unicode character support is enabled. Unicode characters are used in double-byte languages.

IMPORTANT: To support Unicode, an additional file named UNINOMAP.TXT must be created and saved in the SYS:\ETC directory. When the -UNICODE value is set to On, the UNINOMAP.TXT file is used to resolve Unicode-to-ASCII "no-map" problems.

To specify "no-map" cases in the UNINOMAP.TXT file, enter the first Unicode value to watch for and then the second value representing the ASCII replacement code. For example:

```
0178 98
```

```
20AC CC
```

Save the values in the UNINOMAP.TXT file. If an unmappable character is encountered, the system uses the ASCII substitution character specified in the file.

- ◆ *OpLocks* is not functional in the NetWare 6 Support Pack 1 software release.
- ◆ *Authentication Mode* indicates the method of authentication used by Novell Native File Access Protocols. You can select either Domain or Local from the drop-down list:
 - ◆ 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.
 - ◆ 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.
- ◆ *Authentication Workgroup 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 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.

- ◆ *Primary Domain Controller 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.

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.

Attach Page Parameters

Use the Attach page to bind the CIFS protocol to the IP address specified.

- ◆ *IP Addresses* show a list of the addresses that are bound to the CIFS protocol. You can enter multiple addresses in the fields provided.

By default, CIFS is bound to all IP addresses on the server.

Shares Page Parameters

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.

- ◆ *Name* is the name that the sharepoint is known by to the Windows computers.
- ◆ *Path* is the path to the server volume or directory which becomes the root of the sharepoint. This path must end with a backslash (\).
- ◆ *Comment* is a description for the sharepoint that appears in Network Neighborhood or My Network Places.
- ◆ *Maximum Number of Connections* is the number of connections allowed to the sharepoint. A zero (0) indicates an unlimited number of connections.

Using the CIFS.CFG File to Configure CIFS

1 Log in to the server running the Novell Native File Access Protocols.

2 Change to the SYS:\ETC\ directory.

3 Edit CIFS.CFG using a text editor.

Enter the desired parameters following the rules for syntax (see the Configuration File Parameters section below for details).

4 Save the CIFS.CFG file to the same directory (SYS:\ETC).

5 Restart the server.

Configuration File Parameters

The following parameters can be set in the SYS:\ETC\CIFS.CFG file to customize the user experience for your environment.

TIP: Any parameter can be excluded by placing a # at the beginning of the command line. If the parameter is excluded, the default value is used.

-SERVERNAME

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.

Value: *'Server_Name'*

Default: None

-COMMENT

The comment associated with the server name listed above. This comment is displayed when viewing details.

Value: *'Comments'*

Default: None

-AUTHENT

The method of authentication used by Novell Native File Access Protocols.

- ◆ 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.
- ◆ 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.

Value: Domain | Local

Default: Local

-DOMAIN

The domain or workgroup that the server will belong to.

Value: *'Domain_Name'*

Default: Workgroup

-WORKGROUP

The domain or workgroup that the server will belong to. Workgroup and Domain can be used interchangeably.

Value: *'Workgroup_Name'*

Default: Workgroup

-PDC

The PDC server name and 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.

NOTE: 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.

Value: *'PDC_Name' Address*

Default: None

-WINS

Address of WINS server to be used to locate the PDC, if the PDC and server running Novell Native File Access Protocols are on different subnets.

Value: *IP_Address*

Default: None

-ATTACH

Bind the CIFS protocol to the IP address specified. For multiple addresses, repeat the command as needed.

Value: *IP_Address*

Default: Bound to all addresses.

-SHARE

Allow any volumes or directories on the server to be specified as shared points and to be accessible via the Network Neighborhood. If no -SHARE line is specified (or is commented out), then all mounted volumes are displayed.

- ◆ *Localpath* is the path to the server volume or directory which becomes the root of the sharepoint. This path must end with a backslash (\).
- ◆ *Sharename* is the name by which the sharepoint is known to the Windows computers.
- ◆ *Connection Limit* is the number of connections allowed to the sharepoint (0 is unlimited).
- ◆ *Comment* is a description for the sharepoint that appears in Network Neighborhood or My Network Places.

Value: '*Localpath*' '*Sharename*' *Connection Limit* '*Comment*'

Default: All mounted volumes are shared.

-UNICODE

When On (enabled), this command enables Unicode characters (used in double-byte languages).

Value: On | Off

Default: Off (disabled)

IMPORTANT: To support Unicode, an additional file named UNINOMAP.TXT must be created and saved in the SYS:\ETC directory. When the -UNICODE value is set to On, the UNINOMAP.TXT file is used to resolve Unicode-to-ASCII "no-map" problems.

To specify "no-map" cases in the UNINOMAP.TXT file, enter the first Unicode value to watch for and then the second value representing the ASCII replacement code. For example:

```
0178 98
```

```
20AC CC
```

Save the values in the UNINOMAP.TXT file. If an unmappable character is encountered, the system uses the ASCII substitution character specified in the file.

Sample CIFS.CFG Configuration File

```
#This name will display in Network Neighborhood with the #following comment.
-SERVERNAME 'NW6-NNFAP'
-COMMENT 'Server running Novell Native File Access Protocols'
#Novell Native File Access Protocols is configured to use Local
#authentication.
-AUTHENT LOCAL
#The workgroup name is ONENET.
-WORKGROUP 'ONENET'
#When this volume is mounted, the local path CIFSVOL:\ will appear as a
sharepoint named Graphics Volume with unlimited connections (0) and its
corresponding comment.
-SHARE 'CIFSVOL:\' 'Graphics Volume' 0 'Lots of image files'
```

CIFS.CFG Configuration File Shortcuts

You can enter the following commands at the server console to modify the configuration file.

CIFS SHARE ADD '*localpath*' '*sharename*' *connectionlimit* '*comment*'
adds a new sharepoint and also adds the command to the CIFS.CFG file.

CIFS SHARE REMOVE '*sharename*' removes the sharepoint and comments it out of the CIFS.CFG file.

Viewing Configuration Details

You can view details about how Novell Native File Access Protocols are configured by entering 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.

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:

- ◆ [Accessing Files from a Windows Computer \(page 35\)](#)
- ◆ [Mapping Drives from a Windows Computer \(page 35\)](#)
- ◆ [Changing Passwords from a Windows Computer \(page 35\)](#)

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** Enter 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 or Windows ME, click My Network Places > Computer Near Me. 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 enter 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.

Mapping Drives from a Windows Computer

- 1** Enter 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 enter 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.

Changing Passwords from a Windows Computer

Windows users can change and synchronize their local password and their simple password. When users change the local password, they also change and synchronize their simple password.

From a Windows 2000/NT Computer

- 1** Press Ctrl+Alt+Delete.
- 2** Click Change Password.
- 3** In the Domain field (or the Log On To field in Windows 2000), enter the name of the server running Novell Native File Access Protocols.

If your Windows computer is running Novell Client software, click Show All Resources and select the appropriate server.

- 4** Enter the username, old password, and new password as prompted.

The NetWare password and the simple password will be synchronized only if the old simple password matches the NetWare password. If they are different, the NetWare password will not be changed and access to the network will be denied. To change and synchronize the NetWare password, you must use the Administrator Workstation running Novell Client software.

From a Windows 95/98/ME Computer

- 1** Change the local password.

- 1a** Click Start > Control Panel > Passwords.

- 1b** Click Change Passwords > Change Windows Password.

- 1c** Enter the username, old password, and new password as prompted.

- 2** Change the simple password.

- 2a** Click Start > Run.

- 2b** Enter

```
NET PASSWORD
server_running_Novell_Native_File_Access_software
```

For example:

```
NET PASSWORD NetWare1
```

WARNING: The Windows NET PASSWORD utility sends unencrypted text (called *clear text*) over the network. If you are concerned about someone capturing your password over the network, you should manage passwords using ConsoleOne™ from the Administrator Workstation. For more information on why this issue exists, contact Microsoft Corporation.

- 2c** Enter the same username, old password, and new password when prompted.

The NetWare password and the simple password will be synchronized only if the old simple password matches the NetWare password. If they are different, the NetWare password will not be changed and access to the network will be denied. To change and synchronize the NetWare password, you must use the Administrator Workstation running Novell Client software.

For more information on simple passwords, see [“Creating Simple Passwords for Windows Users” on page 23](#). For information on synchronization between simple passwords and NetWare (NDS) passwords, see [“Understanding Synchronization of NetWare Passwords and Simple Passwords” on page 27](#).

For Computers Using Domain Authentication

If the computer is configured to use domain authentication, then the password checking is done by the domain controller. The password can be changed using the Windows administration tools for a domain controller. For more information, contact your network administrator.

5

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

NetWare® 6, Novell® Cluster Services™ software, and Novell Native File Access Protocols provides high availability, scalability, and security to your network while reducing administrative costs associated with managing client workstations.

This chapter describes how to set up a NetWare 6 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 environment, see [Chapter 6, “Working with UNIX Machines,” on page 49](#).

Prerequisites

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

- Novell Cluster Services 1.6 installed on NetWare 6 servers

For information on configuring Novell Cluster Services, see the [Novell Cluster Services Overview and Installation Guide](http://www.novell.com/documentation/lg/ncs6p/index.html) (<http://www.novell.com/documentation/lg/ncs6p/index.html>).

- NetWare 6 configured as described in [“NetWare Server Prerequisites” on page 9](#)
- Administrator workstation configured as described in [“Administrator Workstation Prerequisites” on page 10](#)
- Novell Native File Access Protocols installed on each server in the cluster that you want users to access.

Follow the instructions in [“Installing the Software” on page 11](#).

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 AFPTCP.NLM is loaded on all servers in the cluster by entering **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 Native File Access Protocols portion of the NetWare 6 installation.

- 2** Cluster enable the shared-disk pools or volumes by following the procedures described in "Create Shared Disk Partitions" in the [Novell Cluster Services Overview and Installation Guide](http://www.novell.com/documentation/lg/ncs6p/index.html) (<http://www.novell.com/documentation/lg/ncs6p/index.html>).

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 18](#).

Volumes are displayed as ServerName.VolumeName. If the server fails over, the user sees the next failover 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 server cluster by entering the IP address or 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.

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.

We recommend that you have NetWare 6 Support Pack 2 installed prior to configuring CIFS for ACTIVE/ACTIVE mode with Novell Cluster Services.

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 [Cluster Enable Pools and Volumes](#) section of the Novell Cluster Services Overview and Installation documentation.

When you create and cluster-enable pools, ensure the CIFS check box that appears in ConsoleOne during the pool creation process is checked, and enter the CIFS Server Name in the field provided. 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.

If you already have pools that are cluster enabled, go to [Step 3 on page 45](#).

3 (Conditional) To make pools that have already been cluster enabled (virtual servers) accessible to CIFS clients, you must manually add an NFAP auxiliary class attribute to the Virtual Server object and also manually add the CIFS ADD and CIFS DEL commands to the cluster volume load and unload scripts.

3a Using ConsoleOne[®], browse to and click the Cluster object of the cluster that contains the cluster-enabled pool you want to make available to CIFS clients.

3b In the right pane, right-click the cluster-enabled pool, then click Properties.

3c Click the Scripts tab and add the CIFS ADD and CIFS DEL commands along with the Fully Distinguished Name (FDN) of the virtual server to the load and unload scripts.

The FDN must include the eDirectory™ tree name and leading and ending dots.

For example, if the virtual server name is CLUSTER1_SALESPool_SERVER, the tree name is CAJU, and the context of the Virtual Server object is sales.novell, you would add

```
CIFS ADD .CN=CLUSTER1_SALESPool_SERVER.  
OU=SALES.O=NOVELL.T=CAJU.
```

just above the last line of the load script and

```
CIFS DEL .CN=CLUSTER1_SALESPool_SERVER.OU=SALES.  
O=NOVELL.T=CAJU.
```

just above the last line of the unload script.

The load and unload scripts should now appear similar to the following examples:

LOAD SCRIPT

```
nss /poolactivate=SALESPool  
mount TEST VOLID=253  
mount NDPS VOLID=254  
CLUSTER CVSBIND ADD CLUSTER1_SALESPool_SERVER 137.  
65.86.218
```

```

NUDP ADD CLUSTER1_SALESPOOL_SERVER 137.65.86.218

CIFS ADD .CN=CLUSTER1_SALESPOOL_SERVER.OU=SALES.
O=NOVELL.T=CAJU.

add secondary ipaddress 137.65.86.218

UNLOAD SCRIPT

del secondary ipaddress 137.65.86.218

CLUSTER CVSBIND DEL CLUSTER1_SALESPOOL_SERVER 137.
65.86.218

NUDP DEL CLUSTER1_SALESPOOL_SERVER 137.65.86.218

CIFS DEL .CN=CLUSTER1_SALESPOOL_SERVER.OU=SALES.
O=NOVELL.T=CAJU.

nss /pooldeactivate=SALESPOOL /override=question

```

3d Right-click the Virtual Server object in the left pane, then click Extensions of this Object.

3e Click the Add Extension button, select nfapCIFSConfigInfo, then click OK.

3f Enter the Extension name, then click OK.

The Extension name is the name you want to give the extension. You could name the extension nfapCIFSConfigInfo.

3g Right-click the Virtual Server object in the left pane, then click Properties.

3h Click the CIFS tab, then enter the CIFS server name.

The CIFS server name is the server name CIFS clients see when they browse the network.

3i Click the CIFS tab again, select the Shares option, then enter the CIFS share points.

See [“Installing the Software” on page 12](#) for more information on CIFS shares.

3j Click the CIFS tab again, select the Attach option, then add the IP address of the virtual server.

3k Bring the virtual server resource offline and then online again to have the changes take effect.

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.

What's Next

With the NetWare 6 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 3, “Working with Macintosh Computers,” on page 17](#).

For an explanation of how Windows users access network files and for more information on managing Windows workstations, see [Chapter 4, “Working with Windows Computers,” on page 23](#).

6

Working with UNIX Machines

Novell® Native File Access for UNIX* provides an NFS Server that lets UNIX workstations 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. They can mount the exported network storage and use it as their own file system.

The traditional NetWare file system is supported only on NFS version 2. The NSS file system, however, is supported on NFS versions 2 and 3. NFS Server provides mount protocol versions 1, 2, and 3 over UDP. The NFS Server supports NFS protocol versions 2 and 3 on UDP and TCP.

Native File Access for UNIX also provides a complete Novell eDirectory™- enabled Network Information Services (NIS) with which UNIX and NetWare users can be administered from a single point, namely eDirectory. NIS maintains its information in eDirectory and integrates the user information so that the eDirectory User object also represents the NIS user.

Features of Novell Native File Access for UNIX

Novell Native File Access for UNIX includes the following features:

- ◆ NFS Server

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

See [“NFS Server” on page 50](#).

- ◆ 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 them as eDirectory objects that can be centrally maintained and administered.

See [“Network Information Service” on page 52](#).

- ◆ UNIX User Management

With the implementation of NIS over eDirectory, there exists only one user/group in the network which contains both eDirectory information and UNIX information. This brings up the user management to single point, namely eDirectory.

See [“UNIX User Management Using eDirectory” on page 54](#).

- ◆ ConsoleOne-Based Administration

By using ConsoleOne’s snap-in utility for Native File Access for UNIX, you can administer and manage the services.

See “[ConsoleOne-Based Administration](#)” on page 56.

- ◆ Cluster Services Support

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

See “[Novell Cluster Services Support](#)” on page 56.

- ◆ Upgrade Utility

The upgrade utility helps to retain the configurations of previous installations of NetWare NFS Services (versions 2.x and 3.x) during a NetWare 6 upgrade.

See “[Upgrade Utility](#)” on page 58.

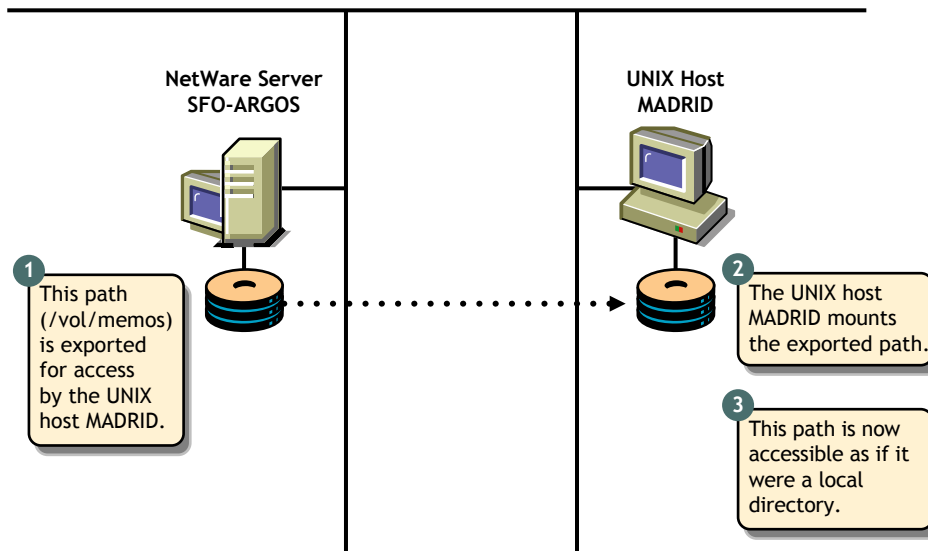
Overview of Native File Access for UNIX

NFS Server

Network File System (NFS) enables UNIX users to access a NetWare file system as if it were a local directory on the UNIX workstation. Any client that supports the NFS protocol can also access NetWare files using the 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 1 NFS Server Functionality



Making the NetWare File System Available to NFS Clients

Before UNIX users can access the NetWare file system, it must be made available to the UNIX workstations. This process is called *exporting* the file system. When exporting, you can define who should access the information and how it is accessed by specifying the trusted systems and export options. For example, you can restrict the access to specific UNIX workstations, export the directory as Read-only, etc.

Guidelines

- ◆ If the filename of the file created on the NFS Client in a traditional volume has more than 80 characters, the filename in long namespace gets truncated to 80 characters.
- ◆ If the NetWare server code page is 932, then the file creation from Japanese EUC NFS clients fails for certain characters

Accessing the NetWare File System from NFS Clients

After exporting the NetWare file system from a NetWare server, you must mount the exported file system on the UNIX workstation for normal access. This process is called *mounting* the file system. Mounting a NetWare file system from a UNIX workstation consists of the following:

- ◆ Creating a mount point

A mount point is an empty directory you create. This directory becomes the access point for the NetWare file system. If you choose an existing directory as a mount point, the contents of the existing directory become unavailable 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 different commands or user interfaces to mount a remote file system.

Accessing the NFS Server from the Web

The Web-NFS component of the NFS software enables direct Web access to data on NFS servers. It defines a new NFS URL that complements HTTP. The format is as follows:

NFS://Hostname or IP Address

Using this URL, browsers with Web-NFS support can access data from any server.

Web-NFS extends NFS to support operations over a WAN. With Web-NFS, clients can obtain file handles more easily without going through the portmapper or the mount protocols. This makes it firewall-friendly and enables NFS operations across WANs and the Internet. It also improves performance over a WAN by reducing the number of turnarounds.

For each NFS server, only one of the exported paths can be enabled for Web-NFS access.

NFS Server Access Control

NetWare and UNIX use different methods for controlling access to files. Although both have similar directory and file security, NetWare security is more elaborate. At a basic level, both systems assign access controls to similar user types.

The access control mode is known as Independent Mode wherein there are no rights/permissions mappings. NFS Client rights apply to NFS client access and NetWare rights apply to NetWare client access.

For information about NFS Server configuration and management, see [“NFS Server” on page 69](#).

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 like phone lists.

NIS maintains its information in eDirectory and also 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 also 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.

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 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, do the following:

- 1 Right-click `NISSERV_Servername` object.
- 2 Click Properties.
- 3 Click the Memberships Tab to display the list of NIS Domains served by this NIS Server object.
- 4 Click the Others Tab to view the IP Address of the NetWare server where NIS server is installed.

NIS Information on eDirectory

NIS Domain

The NIS system organizes nodes into administrative segments called *domains*. The NIS domain exists only in the local environment and usually covers a single network. An NIS domain is a hierarchical structure; hence 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 using DNS choose to relate their 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. A migration utility is available to 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 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. If the Bootparams text filename is to be migrated from the ConsoleOne, it should be named *bootp*.

Hosts Map—Contains one entry for each IP address of each host. If a host has more than one IP address, it will have one entry for each. 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, home directory etc.

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 also 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, you would 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_SpillerMS 235-6777  
  
Jim_Miller MS 769-8909
```

Various NIS Configurations

NIS can be configured in the following ways:

- ◆ [NIS Master Server](#)
- ◆ [NIS Slave Server](#)
- ◆ [NIS Client](#)

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. Once 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.

Once the slave server is set up, you don't 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 utility. 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 also be used for load distribution in the network. A master NIS server for one domain can also function as a slave NIS server for another domain.

NIS Client

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

For more information on setting up and managing NIS, see [“NIS Server” on page 77](#).

UNIX User Management Using eDirectory

With the implementation of NIS over eDirectory, there exists only one user/group in the network which contains both eDirectory information and UNIX information. This brings up 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 on eDirectory.

By default, UNIX users /groups are looked for within the containers specified by the parameter SEARCH_ROOT in the configuration file NFS.CFG. The search is recursive within the containers specified by this parameter. In case the parameter does not contain any value, then the search is done under the default bindery or servers context.

When a set of users/groups are migrated to eDirectory from a UNIX server, corresponding User/Group objects are created /updated in eDirectory. During migration, if the UNIX user or group is not present, 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.

User and Group Information

NetWare and UNIX both use the same User and Group objects to get the information they need.

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

Information about 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.

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 also 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.

User Home Directories

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

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.

Handling UNIX User Passwords

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

Before migrating the users and groups, remove the password field ("*", "x", or "!") from the corresponding text file and then migrate. After doing this, you can set the UNIX password from the UNIX machine. This is done by making the UNIX machine an NIS client to the NetWare machine, logging in as that NIS user and running an NIS client utility named YPPASWD to set the UNIX password.

For information about UNIX user management, see [“Migration of NIS Maps” on page 63](#).

ConsoleOne-Based Administration

You can use ConsoleOne to perform the following Native File Access for UNIX tasks:

- ◆ Configure the server's global parameters
- ◆ Start and stop services
- ◆ Configure and manage services
- ◆ Configure error reporting
- ◆ Monitor performance and adjust parameters affecting performance
- ◆ Configure user and group UNIX information

For more information, see [“ConsoleOne-Based Configuration” on page 58](#).

Novell Cluster Services Support

In a non-cluster environment, if the server running Native File Access for UNIX fails, then UNIX users will not be able to use this service until the NetWare server is up. To achieve high availability, you can run Native File Access for UNIX on Novell Cluster Services™.

The product is installed on all the required nodes in the cluster. Cluster enabling is achieved by storing the required configuration files on the shared disk in the cluster. Native File Access for UNIX then accesses these files through an always or highly available virtual IP address. NFS/NIS clients must, therefore, use the virtual IP Address for NFS mounts and issuing NIS client calls. In case the server where the services are currently running fails, the shared disk volume with configuration files automatically remounts along with the virtual IP on a designated node in the cluster.

Native File Access for UNIX supports only active-passive mode on the cluster. This means that only one node in the cluster will be running NFS Services.

Running Novell Native File Access for UNIX on Novell Cluster Services provides the following benefits:

- ◆ There is no need to replicate configuration information as the configuration files are stored on the shared disk.

- ◆ Services can be automatically restarted without user intervention in case of a node failure in a cluster.
- ◆ The services can be migrated and controlled between the various nodes in the cluster using ConsoleOne.
- ◆ Since the cluster volume is the same regardless of which server it is mounted on, no configuration information is lost or out of date.

For information on configuring Native File Access for UNIX on Novell Cluster Services see [“Setting Up Novell Native File Access for UNIX with Novell Cluster Services” on page 89.](#)

Administration Utilities

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

SCHINST

This utility is run automatically during the installation of Native File Access for UNIX. This utility extends the schema necessary for storing the UNIX information of objects. If the directory services are reinstalled or if the NISUserDef/NFAUUser object is deleted, run this utility manually. The syntax is as follows:

```
schinst [ -f filename ]
```

The **-f filename** is an optional parameter. It is the name of the file that contains the list of schema files that need to be extended. If a filename is not specified, the default file, SYS:\ETC\UNIXSCH, is used.

SCHINST takes the administrator's FDN and password as input for extending the schema.

SCHINST extends the UAM schema. It creates NFAUUser object and also adds the UNIX Profile of the root user as UID=0, GID=1, Home Directory=/home to this object. It updates the parameter NIS_ADMIN_OBJECT_CONTEXT in the configuration file NFS.CFG with the context where the object is present.

NOTE: You also have to run **nisinst** after this.

All log messages generated by SCHINST are written to the SYS:\ETC\SCHINST.LOG file. All information regarding schema extension can be found in SYS:\SYSTEM\DSMISC.LOG.

NISINST

This utility creates an eDirectory object with the name NISSERV_*Servername* by default or whatever name was specified with the **-s** option. NIS Server uses this object to store the domains served by the NIS Server. 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 above list. The syntax is as follows:

```
nisinst [-s name] [-x context] [ -i ip address ]
```

The parameter **-s** is optional. It specifies the name to be given to the nisserver object. The parameter **-x** is also optional. It specifies the context where the object should be created in eDirectory. The optional command line option **-i** is to specify 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.

Run the NISINST manually, if the nisserver object is deleted.

IMPORTANT: If directory services are removed, you need to comment the SEARCH_ROOT parameter in NFS.CFG and do the following:

```
nfsstop  
schinst  
nisinst  
nfsstart
```

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 choose 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 into the new configuration files, NFS.CFG, NIS.CFG, and NFSSERV.CFG located in SYS:\ETC. The existing configuration files NFSTHOST, and NFSEXPRT are retained.

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

Setting Up and Managing Novell Native File Access for UNIX

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

- ◆ [Configuration Methods \(page 58\)](#)
- ◆ [Configuring Server General Parameters \(page 59\)](#)
- ◆ [Migration of NIS Maps \(page 63\)](#)
- ◆ [NFS Server \(page 69\)](#)
- ◆ [NIS Server \(page 77\)](#)

Configuration Methods

Novell Native File Access for UNIX can be configured using ConsoleOne™ and also by setting the file-based configuration parameters of the various components.

ConsoleOne-Based Configuration

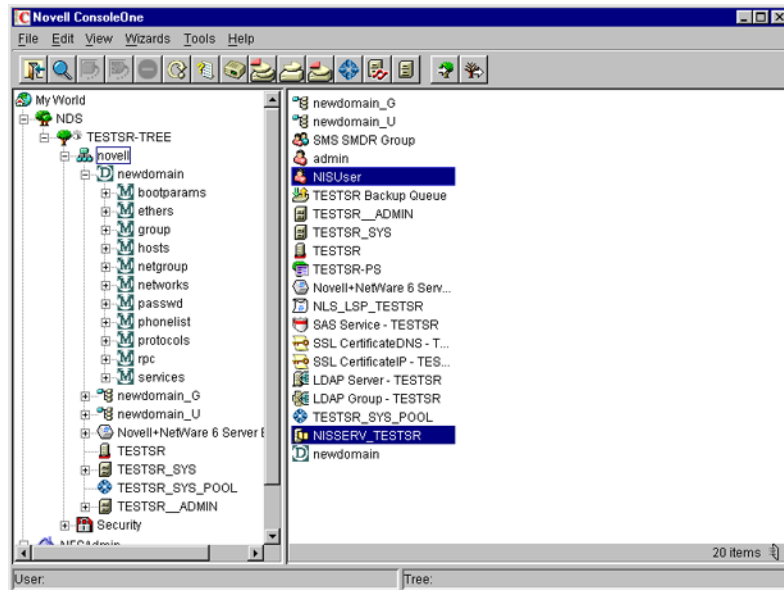
To start ConsoleOne from the client, complete the following steps.

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

- 1** Start ConsoleOne from the server where Native File Access for UNIX is installed.
- 2** Click NFSAdmin and then the login toolbar icon.
- 3** Enter the tree name, context name, authorized username, and authorized password.
- 4** Click OK.
- 5** Enter the hostname or IP address and 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. You will not be able to administer a NetWare NFS Services 3.0 on NetWare 5.1 from ConsoleOne on NetWare 6.

Figure 2 Novell Native File Access for UNIX Objects



WARNING: After the Novell Native File Access for UNIX installation, two objects are created in the tree: NFAUUser / NISUserDef and NISSERV_Servername. These objects should not be deleted.

File-Based Configuration

The configuration (.CFG) files are used to configure the services. All of these 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, you need to change the desired parameter value in the corresponding .CFG file and restart the module.

NOTE: In a cluster environment, the configuration files will be located in the ETC directory of the shared volume.

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 you stop the services using **nfsstop** and restart using **nfsstart**.

File-Based Configuration of Server General Parameters

The following table lists the configuration parameters in NFS.CFG.

Table 1 Novell Native File Access for UNIX General Parameters

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 will start from the bindery and then in the server's default context.

ConsoleOne-Based Configuration of Server General Parameters

This section explains the following tasks:

- ◆ [Viewing the Server General Parameters \(page 60\)](#)
- ◆ [Configuring the Server General Parameters \(page 61\)](#)

Viewing the Server General Parameters

- 1 In the ConsoleOne main menu, right-click the server you want to configure and then click Properties.

The following panel appears:

Figure 3 Server General Parameters Panel



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.

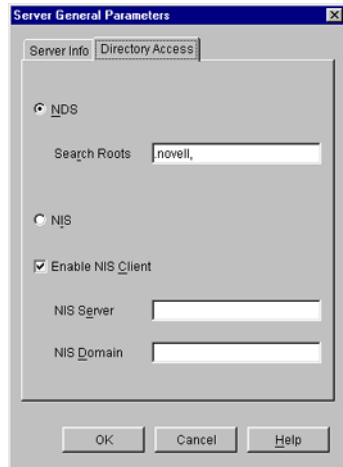
Time Zone—The world time zone reference for your area. The time zone is used for time stamps and to set time synchronization. The time zone reference is set during the NetWare installation.

Configuring the Server General Parameters

- 1 In the ConsoleOne main menu, right-click the server you want to configure and then click Properties > Directory Access.

The following panel appears:

Figure 4 Server General Parameters - Directory Access Panel



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

2 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.

3 Click OK.

4 Modify the following parameters as necessary:

SNMP Alert Level—The level of SNMP alerts reported to SNMP management stations. Select an alert level from the drop-down list. You can also turn off SNMP reporting from this list.

- ◆ None—Suppresses SNMP reporting.
- ◆ Critical—Warns you about urgent problems that require immediate action to prevent widespread failure.
- ◆ Major—Warns you about serious problems that require prompt action to prevent failure of the object and possibly some related objects.
- ◆ Minor—Provides information about problems that can be addressed as work schedules permit.
- ◆ Informational—Provides descriptive information that can be used for such things as trend analysis and planning.

Each level incorporates the information from the levels listed above it. For example, if you select Minor, you also receive messages about major and critical alerts.

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

Migration of NIS Maps

If you already have an UNIX NIS Server (text-based) and you want the new NetWare NIS Server to serve the same data served by the old NIS server, you can copy all those text files into the specified location and 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 the migration, the utility searches for existing eDirectory users and groups under the containers specified by the SEARCH_ROOT configuration parameter (specified in NFS.CFG) and, 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 will not be created under the passwd and group Map object. They will spread across the eDirectory tree and *DomainName_U*, *DomainName_G* depending upon the SEARCH_ROOT configuration parameter.

Maps can be migrated using 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.

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.

Before migrating the users and groups, remove the password field ("*", "x", or "!") from the corresponding text file and then migrate. After doing this, you can set the UNIX password. This is done by making the UNIX machine an NIS client to the NetWare machine, logging in as that NIS user, and running an NIS client utility named YPPASWD to set the UNIX password.

NOTE: The password for a migrated UNIX user (one who already has the password) cannot be set from an NIS client. A password can be set only for users who do not have a password.

For more information on UNIX user management, see [“UNIX User Management Using eDirectory” on page 54](#).

File-Based Migration

Migration, by default uses the makefile SYS:ETC/NIS/NISMAKE, which contains the location of the text file for every map. The general 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: All options should be used only in the specified order.

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

```
makenis -d domainname
```

The parameter *domainname* 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, enter 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 nothing is specified, all the files in the makefile are migrated.

For each map, you can specify the SECURE parameter so that only requests coming from secure ports are able to access the data. You can also 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 configuration parameter FILEMARK_LOG_FREQ 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.

ConsoleOne-Based Migration

- 1 In the left panel 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.

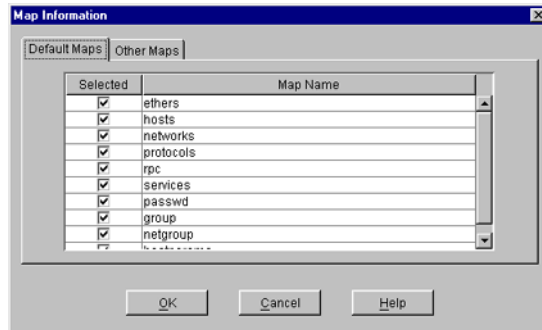
The following panel appears:

Figure 5 Migration Panel



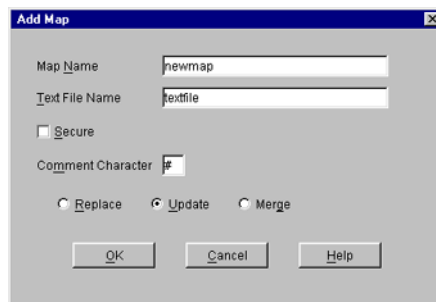
- 4** To migrate a domain, enter the NetWare Host Name/IP Address, Domain Name, and Domain Context.
- 5** To set the NIS Server as master for this specified domain, check Set the Specified Host As Master Server.
- 6** In the Master Server Info section, check Clear Existing Maps if you want to clear the maps already present.
- 7** Click the radio button for the type of the migration you want to perform: Replace, Update, or Merge.
- 8** To set the NIS Server as Slave Server, enter the Master Server Name/IP Address in the Slave Server Info section.
- 9** To migrate the domain for default maps, click Migrate.
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** To migrate the domain for specific maps, click Advanced to go to the Map Information panel.

Figure 6 Map Information Panel



- 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 panel.

Figure 7 Add Map Panel



- 11a** Enter the Map Name and the Text File name.
- 11b** If you want to enable secure access to the map, click Secure.
- 11c** In the Comment Character box, enter the comment character present in the specified text file and click OK.

The default comment character is #.

- 12** Click Migrate.

NOTE: When performing special map migration through ConsoleOne, the complete path of the file is required (for example, SYS:ETC\NIS\PHLIST).

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

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

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

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

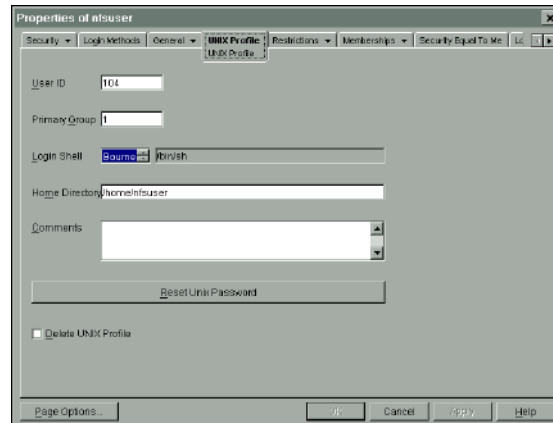
The User objects under this particular container appear.

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

The following panel 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 8 UNIX Profile Tab of User Properties Panel



- 4 To modify the UNIX user profile, click UNIX 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 enter 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 > OK.

Modifying Group Information

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

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

- 2 Double-click the container *domainname_G*, where the Group objects reside.

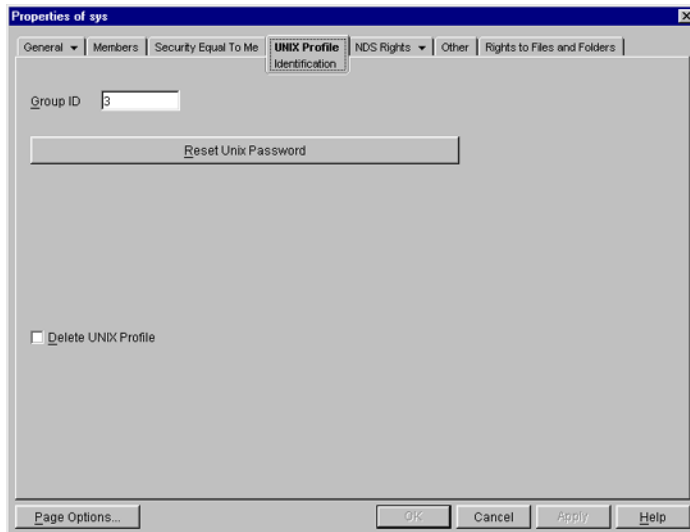
The groups under this particular container appear.

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

The following panel appears, showing 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 9 UNIX Profile Tab of Group Properties Panel



- 4 To modify the UNIX group profile, click the UNIX Profile tab and specify the information in the following field:

Group ID—The group's UNIX GID.

- 5 Click Apply > OK.

Adding a New User or Group

To add a new user, do the following:

- 1 In the left panel of the ConsoleOne main menu, click the context where you want to add the new user.
- 2 Select File > New, and then click User.
- 3 Enter the user information.

To add a new group, do the following:

- 1 In the left panel of the ConsoleOne main menu, click the context where you want to add the new group.
- 2 Select File > New, and then click Group.
- 3 Enter the group information.

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

IMPORTANT: When any update to a UNIX profile is done from ConsoleOne, execute `NFSSTOP` and `NFSSTART`, for NFS server to get the modified UNIX information.

Managing Migration Utility Log Files

When the migration utility, **makenis** is executed, the log file MAKENIS.LOG 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), 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, conflict and invalid records
- ◆ Conflicting record details are logged

IMPORTANT: Even in a clustered environment, MAKENIS.LOG is created in SYS:\ETC\NIS or in the path specified in the configuration parameter LOG_FILE_PATH.

NFS Server

The NFS Server uses the following files:

- ◆ NFSSERV.CFG which contains the configuration parameters
- ◆ NFSEXPRT which contains the exported path information
- ◆ NFSTHOST which contains the trusted hosts list for the exported path

For more information on NFS Server, see [“NFS Server” on page 50](#).

File-Based Management for NFS Server

NFS Server Configuration Parameters

The following table lists the parameters that can be set in NFSSERV.CFG:

Parameter	Default Value	Range	Description
REQ_Q_FULL_ALERT	90	20 - 99	Minimum percentage of request queue utilization which triggers an SNMP alert.
REQ_CACHE_FULL_ALERT	90	20 - 99	Minimum percentage of request cache utilization which triggers an SNMP alert.
OPEN_FILE_CACHE_FULL_ALERT	90	20 - 99	Minimum percentage of open file cache utilization which triggers an SNMP alert.
OPEN_FILE_CACHE_ENTRIES	512	32 - 1024	Number of open file cache entries.
CACHE_AGING_INTERVAL	60	0 - 2000	Duration (in seconds) the NFS server keeps a file's information in cache memory. The value 0 disables the open file cache.
REQ_CACHE_ENTRIES	256	64 - 512	Number of request cache entries.

Parameter	Default Value	Range	Description
CACHE_WRITE_THROUGH	NO	YES / NO	Indicates whether cached data should be written to disk immediately.
TYPE_OF_TRANSPORT	BOTH	TCP, UDP, or BOTH	Whether the NFS Server should support TCP, UDP, or BOTH.
NFS_VERSION	0	0/2/3 (0 = Both, 2 = only V2, and 3 = only V3)	Indicates which version of NFS protocol should be currently supported.
NFS_UMASK	022	000 - 777	File mode creation mask for default UNIX permissions.
NFS_V2_THREADS	5	1 -150	Number of NFS Server threads servicing the NFS 2 protocol.
NFS_V3_THREADS	5	1 - 150	Number of NFS Server threads servicing the NFS 3 protocol.
MOUNT_V2_THREADS	1	1 - 150	Number of threads servicing Mount V2 requests.
MOUNT_V3_THREADS	1	1 - 150	Number of threads servicing Mount V3 requests.
NFS_V2_TCP_SEND_Q_ENTRIES	30	1 - 150	Size of the TCP send queue for the NFS V2 protocol.
NFS_V3_TCP_SEND_Q_ENTRIES	30	1 -150	Size of the TCP send queue for the NFS V3 protocol.
NFS_V2_RECV_Q_ENTRIES	20	1 - 150	Size of the receive queue for the NFS V2 protocol.
NFS_V3_RECV_Q_ENTRIES	20	1 - 150	Size of the receive queue for the NFS V3 protocol.
LOG_DIR	SYS:\ETC		Directory where the NFS Server creates the log file.
LOG_FILE	NFSSERV		The name of the NFS server log file. A .LOG extension is automatically added to the file.
LOG_LEVEL	7	1 = Error Messages, 2 = Warning Messages, 4 = Information Messages	The log level indicates the types of messages to be logged. You can either choose 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 will get all the messages.

IMPORTANT: When trying to administer NFS Server through ConsoleOne while NFS configuration files are still open, inconsistent entries might be displayed in the configuration files or on ConsoleOne.

Exporting NetWare Volumes and Directories

The Export Path information file, NFSEXPRT, contains the list of the paths that are exported from the system. It also gives the specified properties for the exported path.

This file contains one exported path per line. The format of each line is as follows:

ExportedPath isReadOnly anonymousAccess mode webaccess

- ◆ **Exported Path**—The directory path to be exported. For example */nfsvol*.
- ◆ **isReadOnly**—Specifies whether to export the path in read-only mode or not. Values = 1 (read-only), 0.
- ◆ **anonymousAccess**—Specifies whether anonymous access to the exported path is allowed or not. Values = 1, 0.
- ◆ **mode**—Specifies the rights and permission mapping modes for the directory. Novell Native File Access for UNIX supports independent mode (value 512).
- ◆ **Web**—Specifies if Web access is allowed for this exported path. At any point in time, only one path can be enabled for Web access.

Example of an exported path:

```
/nfsvol 0 1 512 0
```

NFS Trusted Host File

The NFSTHOST file contains the list of all the trusted hosts that can access the exported directory. This is specified in conjunction with the NFSEXPRT file.

The format of every line is as follows:

Exported Path Host Name Access-Type Host/Hostgroup

- ◆ **Exported Path**—Gives the directory path to be exported. For example, */nfsvol*.
- ◆ **Host Name**—Gives access to the client host named by the user. To give access to all hosts, select (*).
- ◆ **Access Type (1, 2, 3)**—Specifies the type of access to be granted to a specific host. The values it can take are as follows:
 - ◆ Trusted 1
 - ◆ RootAccess 2
 - ◆ ReadWriteAccess 3
- ◆ **Host/Hostgroup (1, 0)**—This field shows whether the Host Name specified is a Host or a Hostgroup. This field should always be set to 1 (Host).

Example of an exported directory:

```
/nfsvol nfs-sun2 3 1
/nfsvol nfs-sun2 2 1
/nfsvol nfs-sun2 1 1
/nfsvol * 3 1
/nfsvol * 2 1
/nfsvol * 1 1
```

Removing an Exported Path

To remove an exported path, delete the corresponding directory entries from the files `NFSTHOST` and `NFSEXPRT`.

Getting the UNIX information from Remote NIS

For file system sharing by NFS server, the UNIX user and group information is obtained from eDirectory by default. This can be modified so that UNIX information is obtained from a remote NIS server. To set this, do the following:

- 1** Run `NFSSTOP`.
- 2** In the `NFS.CFG` file, set the parameters as follows:
 - ◆ `NDS_ACCESS=0`
 - ◆ `NIS_CLIENT_ACCESS=1`
 - ◆ `NIS_DOMAIN= nis domainname`
 - ◆ `NIS_SERVER= servername which is servicing the specified domain`
- 3** Run `NFSSTART`.
- 4** Load `NFSSERV`.

Starting and Stopping NFS Server

To start NFS Server enter at the system console, enter:

```
load nfsserv
```

To stop NFS Server enter at the system console, enter:

```
unload nfsserv
```

ConsoleOne-Based Management for NFS Server

This section describes how to manage the NFS Server from ConsoleOne.

NFS Server General Configuration Parameters

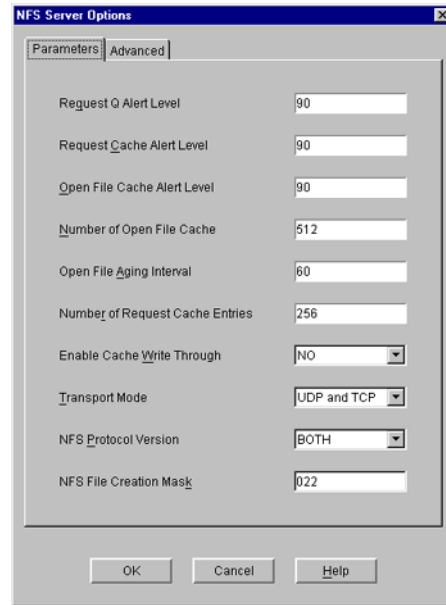
- 1** After logging in, click the server you want to administer from the list of servers under NFSAdmin in the ConsoleOne left panel.

The NFS Server toolbar icon and the NFS Server on the menu bar are displayed.

- 2** To administer NFS Server, click NFS Server on the menu bar and then click Options.

The following panel, which shows the NFS Server basic parameters and their default values, appears.

Figure 10 General Parameters in NFS Server Options Panel



3 Modify the following parameters as necessary:

Request Q Alert Level—After what percentage of request queue utilization an SNMP alert is sent. Default = 90. Range = 20 - 99.

Request Cache Alert Level—After what percentage of request cache utilization an SNMP alert is sent. Default = 90. Range = 20 - 99.

Open File Cache Alert Level—After what percentage of open file cache utilization an SNMP alert is sent. Default = 90. Range = 20 - 99.

Number of Open File Cache—Number of files the NFS server can have open simultaneously. Default = 512. Range = 32 - 1024.

Open File Aging Interval—How many seconds the NFS server keeps a file's information in cache memory. When a file is held in cache, NetWare users cannot access it. Larger values produce better performance, but they also make NetWare users wait longer to access files that are being manipulated by NFS. Default = 60. Range = 0 - 2000. Open File Caching is disabled at 0.

Number of Request Cache Entries—Number of requests that can be held in cache memory. Default = 256. Range = 64 - 512.

Enable Cache Write Through—Whether cached data should be written to disk immediately or not. By default, the data is not written immediately.

Transport Mode—Which transport mode NFS Server should support. The modes could be UDP, TCP, or Both. Default = Both.

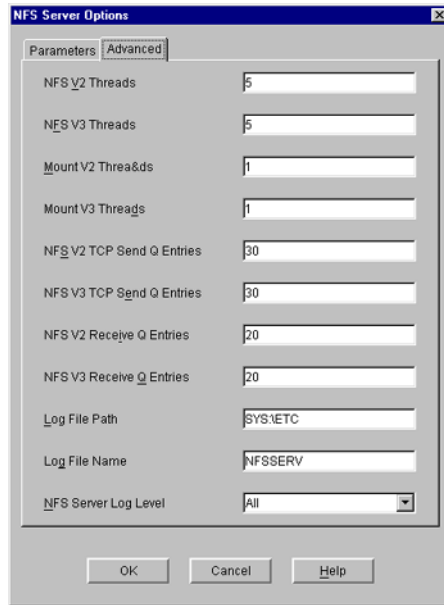
NFS Protocol Version—Version of the NFS protocol to be loaded. The values are 0/2/3.

NFS File Creation Mask—File mode creation mask in Independent Mode for default UNIX permissions of files and directories created from the NetWare side.

4 To specify the advanced parameters, click Advanced on the NFS Server Options panel.

The following panel, which shows the NFS Server advanced parameters and their default values, appears.

Figure 11 Advanced Parameters in the NFS Server Options Panel



5 Modify the following parameters as necessary:

NFS V2 Threads—Number of NFS Server threads servicing the NFS 2 protocol. Default = 5. Range = 1 - 150.

NFS V3 Threads—Number of NFS Server threads servicing the NFS 3 protocol. Default = 5. Range = 1 - 150.

Mount V2 Threads—Number of NFS Server threads servicing the Mount V2 Requests. Default = 1. Range = 1 - 150.

Mount V3 Threads—Number of NFS Server threads servicing the Mount V3 Requests. Default = 1. Range = 1 - 150.

NFS V2 TCP Send Q Entries—Size of the TCP send queue for the NFS 2 protocol. Default = 30. Range = 1 - 150.

NFS V3 TCP Send Q Entries—Size of the TCP send queue for the NFS 3 protocol. Default = 30. Range = 1 - 150.

NFS V2 Q Entries—Size of the receive queue for the NFS 2 protocol. Default = 20. Range = 1 - 150.

NFS V3 Receive Q Entries—Size of the receive queue for the NFS 3 protocol. Default = 20. Range = 1 - 150.

Log File Path—Directory that NFS Server creates the log file in. Default directory is SYS:\ETC.

Log File Name—Name of the NFS Server Log File. Default name is NFSSERV. A .LOG extension is automatically added.

NFS Server Log Level—Indicates the types of messages to be logged.

6 Click OK.

Exporting NetWare Volumes and Directories

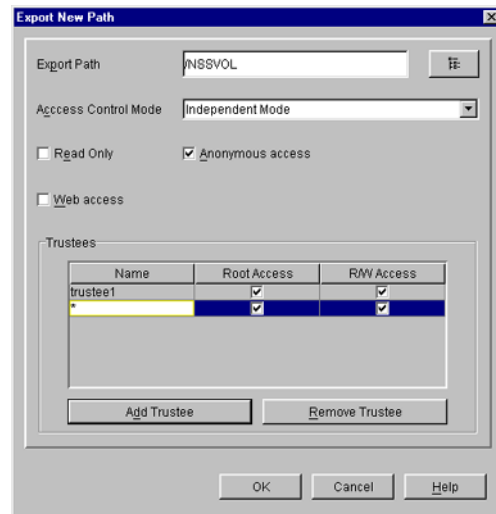
Exporting a directory enables NFS client users to view NetWare volumes and directories as part of the client file system.

You can export a NetWare path and manage it.

- 1 Make sure you have added the NFS name space, and then select Export New Path from the NFS Server drop-down list.

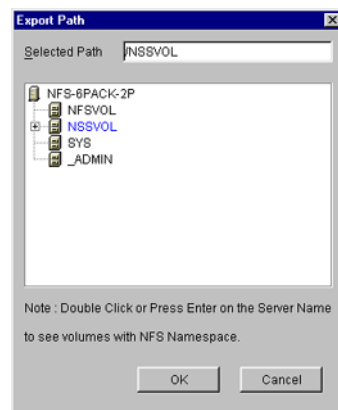
The Export New Path panel appears.

Figure 12 NFS Server Export New Path Panel



- 2 To export a new directory, click the Browse icon in the upper-right corner of the panel. The Export Path panel appears.

Figure 13 Browse Panel for exporting NetWare Volumes and Directories



- 3 Double-click the server name to see the volumes with NFS name space.
- 4 Select the volume or directory you want to export and click OK.
- 5 On the Export New Path panel, modify the following fields as necessary:

Export Path—Path of the directory to be exported.

Access Control Mode—The access control mode that applies to this directory: independent mode.

Read-Only—Indicates whether user access is limited to read-only. Selecting No (the default) provides all users with read/write access. Selecting Yes limits users to read-only access. If Yes is specified, even users on hosts identified as trusted are limited to read-only access. The same also applies to root users. To override this option, enter the name of that host in the Hosts with Read-Write Access field.

Anonymous Access—Indicates whether the users Nobody and Nogroup can access the exported path. Selecting Yes (the default) provides these users with access. Selecting No denies access.

Web Access—Enables WebNFS access for the selected directory when checked. At any point in time only one of the exported paths can be enabled for Web Access.

- 6 Click Add Trustee. Enter the hostname that you want to give exported directory/volume access to.

An asterisk (*) will give access to all the hosts.

You can also specify the type of access you want to give to the host.

- 7 Click the Trustee name on the Export New Path panel to set their access rights.

Hosts with Root Access—The host whose users with root privileges have Admin rights to the exported directory. Select this field to display a list of these hosts. If a host with access is not specified as having root access, root users on that host have the rights of the NFS user Nobody.

Hosts with Read-Write Access—The hosts with access whose users have read/write access to the exported path. Select this field to display a list of these hosts.

- 8 To remove a host from the Trustee list, select the trustee and click Remove Trustee.

Modifying the Exported Path

- 1 In the left panel of the ConsoleOne main menu, click the server that you want to administer.
The Export icon appears in the right panel.
- 2 Double-click Exports to see the currently exported path.
- 3 Right-click the exported path you want to modify and then click Properties.
You can now see the properties of the exported path and modify them.
- 4 Make the changes as required and then click OK.

Removing an Exported Path

- 1 In the left panel of the ConsoleOne main menu, click the server that you want to administer.
The Export icon appears in the right panel.
- 2 Double-click Exports to see the currently exported path.
- 3 Right-click the exported path you want to delete and then click Remove.

Getting the UNIX information from Remote NIS

For file system sharing by NFS server, the UNIX user and group information is obtained from eDirectory by default. This can be modified so that UNIX information is obtained from a remote NIS server. To set this, do the following:

- 1** Run NFSSTOP.
- 2** Set the parameters in the NFS.CFG file as follows by following Steps 1 to 5 in “[Configuring the Server General Parameters](#)” on page 61.
 - ◆ NDS_ACCESS=0
 - ◆ NIS_CLIENT_ACCESS=1
 - ◆ NIS_DOMAIN= *nis domainname*
 - ◆ NIS_SERVER= *servername which is servicing the specified domain*
- 3** Run NFSSTART.
- 4** Load NFSSERV.

Starting and Stopping NFS Server from ConsoleOne

- 1** Click NFSAdmin and log in to the server that you want to administer.
- 2** Click the S icon on the toolbar to start/stop the NFS Server. The background color of the S icon indicates the status of the NFS Server Software.

Refreshing the Exported Paths View

If the NFSEXPRT file is modified outside ConsoleOne, then to view the current contents of the file, do the following:

- 1** In the left panel of the ConsoleOne main menu, click the server that you want to administer. The Export icon appears in the right panel.
- 2** Right-click Exports and then click Refresh to view the currently exported paths.

Managing NFS Server Log Files

When NFS Server service is running it logs messages into a log file named NFSSERV.LOG created by default in SYS:\ETC. This file records messages that provide following information:

- ◆ When and where the services are started and stopped
- ◆ Clients where the exported volumes are mounted.

NIS Server

There is an NIS Server object in eDirectory called NISSERV_*Servername*. This object is created during installation. Migration utility adds the domain details to this object when a domain is migrated. NIS Server will service the list of domains present in this object.

Also, for every user moved, it updates the user's Group Membership attribute and gives rights equivalent to that of the Group.

For information about NIS, see “[Network Information Service](#)” on page 52.

File-Based Management for NIS Server

NIS Server Configuration Parameters

The configuration parameters required for NIS Services is available in the file NIS.CFG. The following table lists the parameters in NIS.CFG.

Table 2 NIS Parameters

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 will be referenced. By default the NISINST utility will create 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 which 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:ETCNIS	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 <i>n</i> , the last <i>n</i> messages are retained.
NIS_LOG_LEVEL	7	The log level indicates the types of messages to be logged. You can either choose 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 will 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.

Parameter	Default Value	Description
NIS_ADMIN_OBJECT_CONTEXT		The context where the NIS Admin object will be created.

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) into SYS:\ETC\NIS.
- 2** (Conditional) If you want to set up other NIS server as slave to this NIS server, do the following:
 - 2a** Create a text file called YPSERV in SYS:\ETC\NIS. For every slave server enter 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** Enter 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 63](#).
- 4** Load NISSERV.NLM. Now the NetWare NIS Server is setup as Master NIS Server.
- 5** (Conditional) If the map data in NIS master is modified anytime, and the changes done needs to be updated in the slave servers immediately then execute the following command:


```
yppush -d domainname [-v] mapname
```

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

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 in the file SYS:\ETC\NFS.CFG.
- 3** Set the domain to the one that is being served by the UNIX NIS server, using the following command:


```
ypset domainname hostname
```

To login or to set the password for a user from a UNIX NIS client, set the default domain in the NetWare server using ypset.
- 4** Make sure NISSERV.NLM is loaded.
- 5** Run MKSLAVE, to setup the NetWare machine as slave, with the following parameters:


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

Setting Up a NetWare Server as NIS Client

- 1** Run NFSSTOP.
- 2** In the NetWare server, make sure that the parameter NIS_CLIENT_ACCESS=1 in the file SYS:\ETC\NFS.CFG.

3 Run NFSSTART.

4 Set the default domain by entering

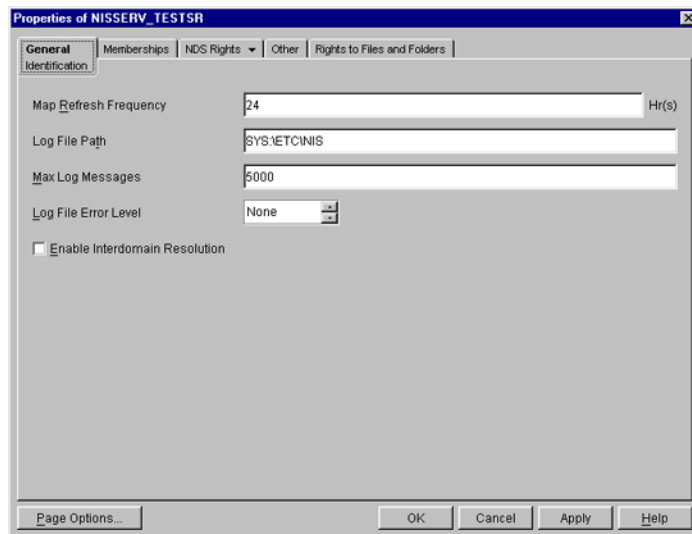
```
ypset domainname hostname/IP_address
```

ConsoleOne- Based Management for NIS Server

NIS Server Configuration Parameters

To configure the parameters required for nis services, right-click The Nisserv_ *servername* > Click Properties. A panel similar to the following appears:

Figure 14 Nis Server-general Parameters Panel



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 In 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.

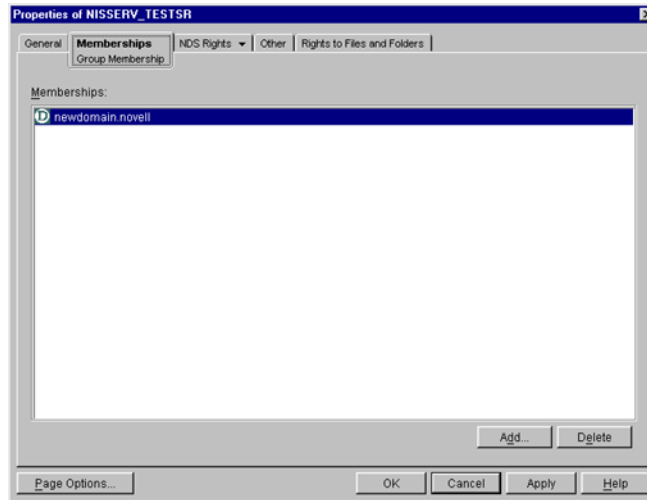
Log File Error Level—The Level Of Error Messages Written To The Audit.log File. Select An Error Level From The Drop-down List.

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 Nisserv_ *servername* > Click Properties > Memberships Tab. A Panel Similar To The Following Appears.

Figure 15 Nis Server: Membership Panel



You Can Add Or Delete Domains From This Panel. 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) into SYS:\ETC\NIS.
- 2** (Conditional) If you want to set up other NIS server as slave to this NIS server, do the following:
 - 2a** Create a text file called YPSERV in SYS:\ETC\NIS. For every slave server enter 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** Enter 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-Based Migration” on page 64.](#)
- 4** Start NISSERV.
- 5** (Conditional) You can 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* > click Update Slave Server . A panel similar to the following appears:

Figure 16 YPPUSH Dialog Box



Enter 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 on the NIS master are automatically updated on the slave servers periodically.

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 panel 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 panel.
- 5 To migrate a domain, enter the NetWare Host Name/IP Address, slave Domain Name, and context where the domain object is to be created.
- 6 To set the NIS Server as slave for this specified domain, uncheck Set the Specified Host As Master Server.
- 7 Enter the Master Server's Name /IP Address in the Slave server information.
- 8 To migrate the domain, click Migrate.

Configuring eDirectory Objects to be Served by NIS Server

NIS Server recognises eDirectory users/groups as NIS users/group only if they have a UNIX profile attached to them. To configure existing eDirectory user/group objects to be served by NIS Server, complete the following steps.

- 1 Choose the eDirectory User/Group object > right-click Properties > UNIX Profile. Enter the required fields in this page and move to the Other tab.
- 2 In the Other tab, choose Add > nisUserGroupDomain attribute.
- 3 Browse and select the NIS Domain Object to which you want to attach these Users and Groups.

This is a multi-valued 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 will be listed under all these domains.

- 4 Verify if the eDirectory Context under which these User and Groups exist is listed in the NIS Domain object. Right-click Domain Object > Properties > Memberships tab.

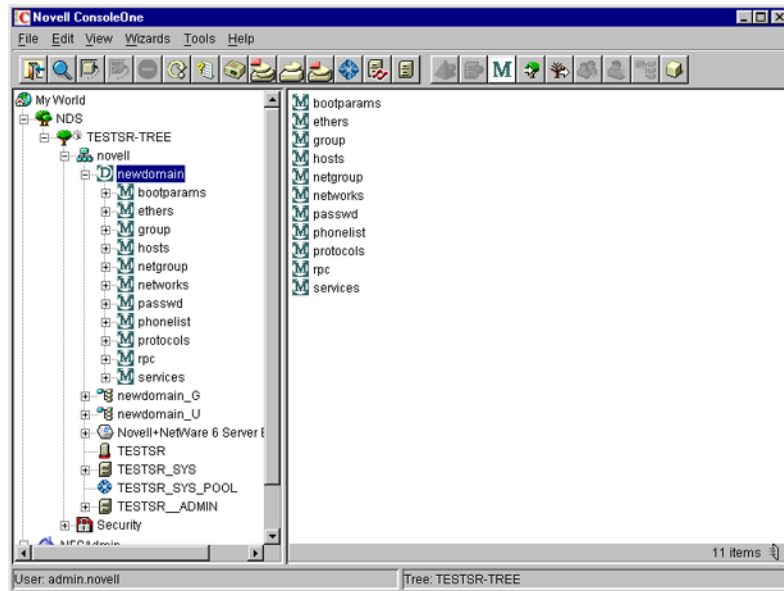
You can also create new NIS maps and NIS map records under NIS domain object as you create normal eDirectory objects.

NOTE: No objects will be there 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 on eDirectory

After migration the NIS maps and records will be available as objects under the migrated NIS domain object.

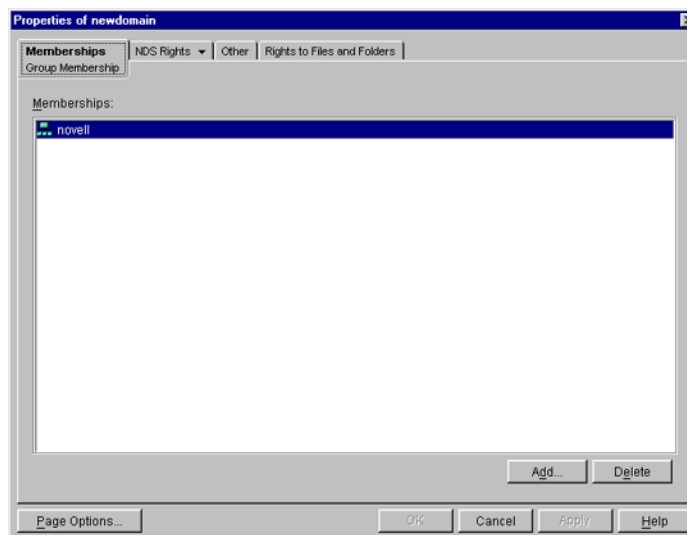
Figure 17 Maps under the Migrated Domain



When a client call is made to this domain, the NIS Server will list the data present under the corresponding domain object. However, for user/group details, it will look 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 will be located, right-click Domain object > click Properties > Membership Tab. A panel similar to the following appears.

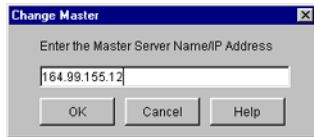
Figure 18 Domain Properties Panel



In case 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 present in the NetWare NIS slave server.

Right-click Domain object > click Change Master. A panel similar to the following appears:

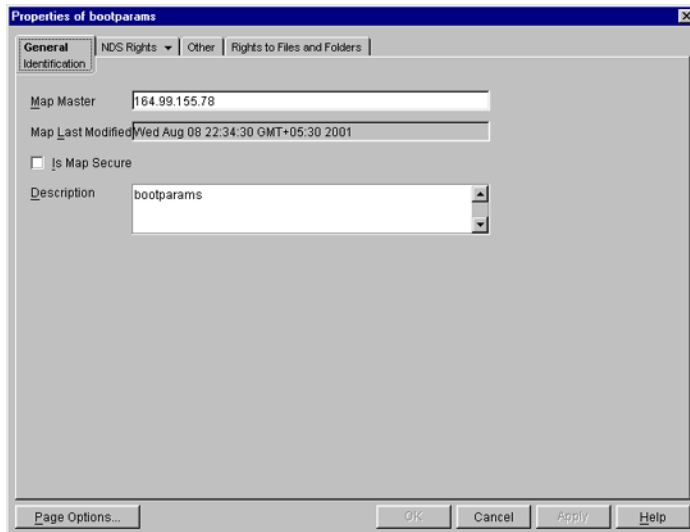
Figure 19 Change Master Dialog Box



Enter the IP address of the new NIS master server. The NIS slave server will now contact 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 panel similar to the following appears:

Figure 20 General Map Properties Panel



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 present under the map.

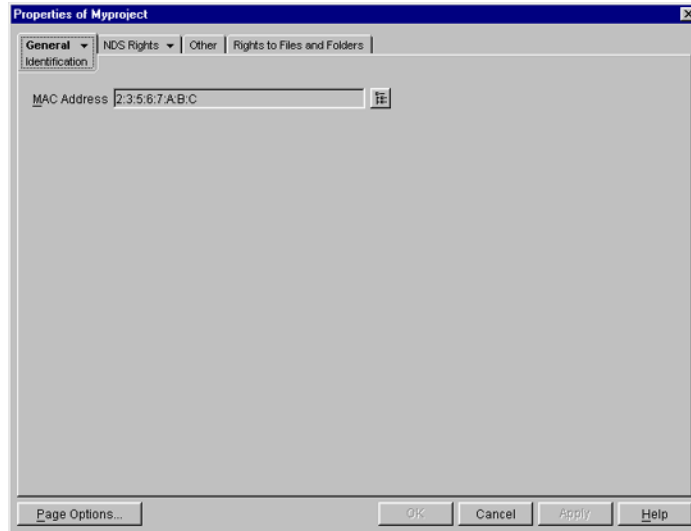
To add an object to a map, right-click the map in the left panel, click New, select the object and then specify the details of the object in the dialog box.

While the panels for records on the same map are the same, they differ from map to map.

Administering Maps

The following figures show the main map panels and are followed by procedures for using each panel's basic fields. Using these panels, you can view or modify the map record's properties. The standard fields remain the same.

Figure 21 Ethers Map Records Properties Panel

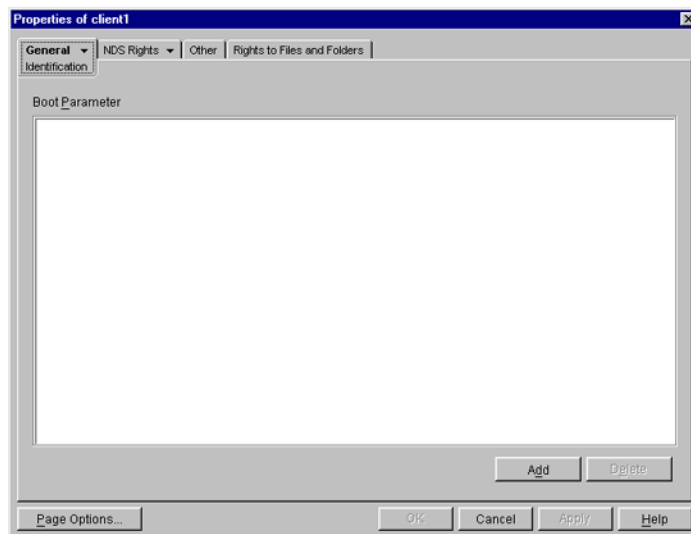


This panel shows the Ethernet address of the host.

The standard address form is $x:x:x:x:x:x$, where x is a hexadecimal number.

Click the icon to enter the Ethernet address of the host, and then click Apply > OK.

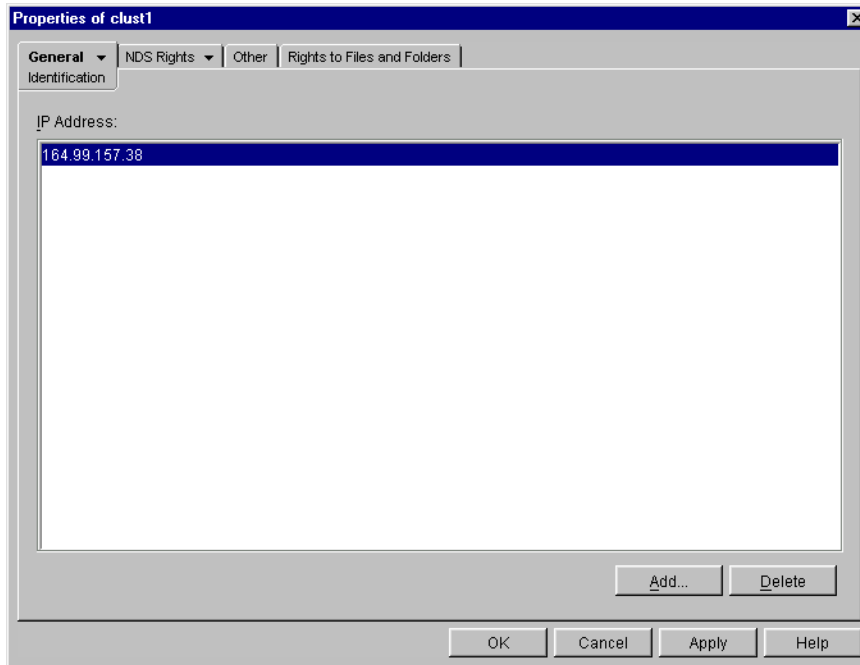
Figure 22 Boot Map Records Properties Panel



- 1 To add the device's boot parameter, click Add, enter the boot parameter of the device in the Boot Parameter field, and then click Apply > OK.

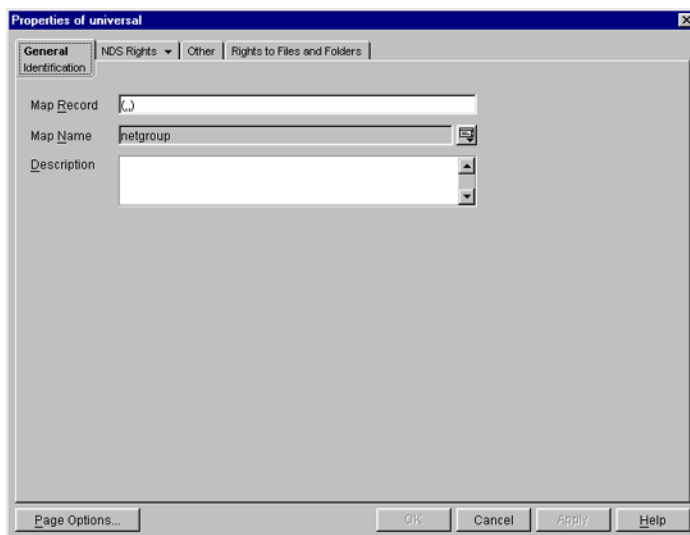
- 2 To delete the device's boot parameter, select the boot parameter of the device in the Boot Parameter field, and then click Delete > Apply > OK.

Figure 23 Host Map Records Properties Panel



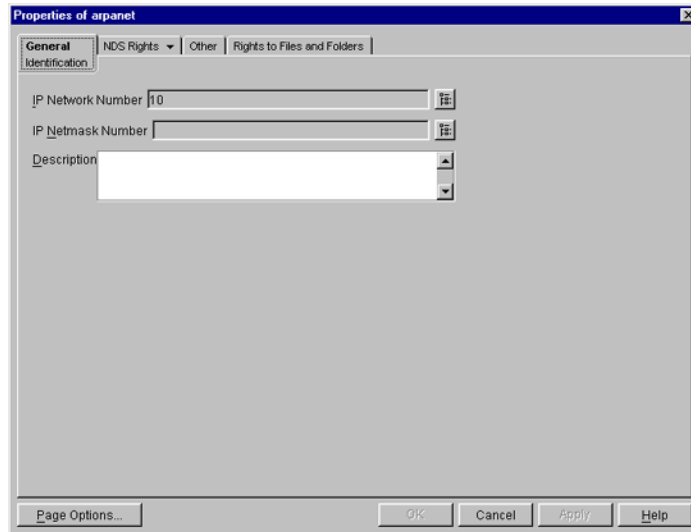
- 1 To add the host address, click Add, enter the IP address of the host, and then click Apply > OK. The network addresses are written in the conventional decimal dot notation.
- 2 To delete the host address, select the host's IP address from the IP Address field, and then click Delete > Apply > OK.

Figure 24 Netgroup Map Records Properties Panel



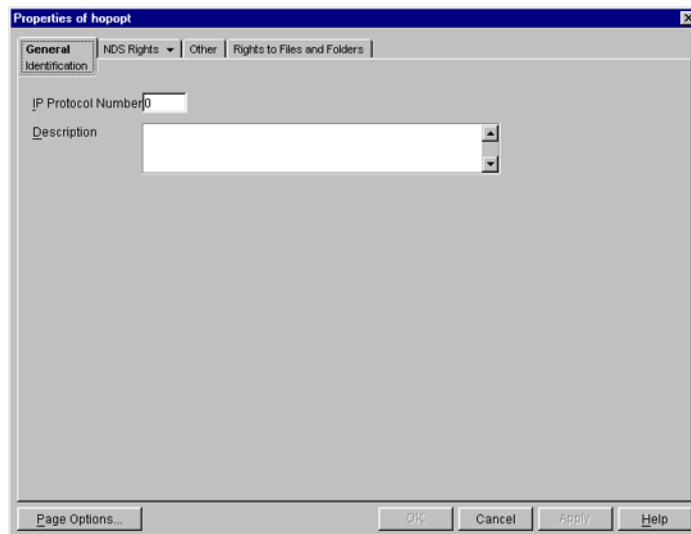
To add a netgroup address, enter the name of the Map Record, browse the icon for the Map Name, enter the description of the map, and then click Apply > OK.

Figure 25 Network Map Records Properties Panel



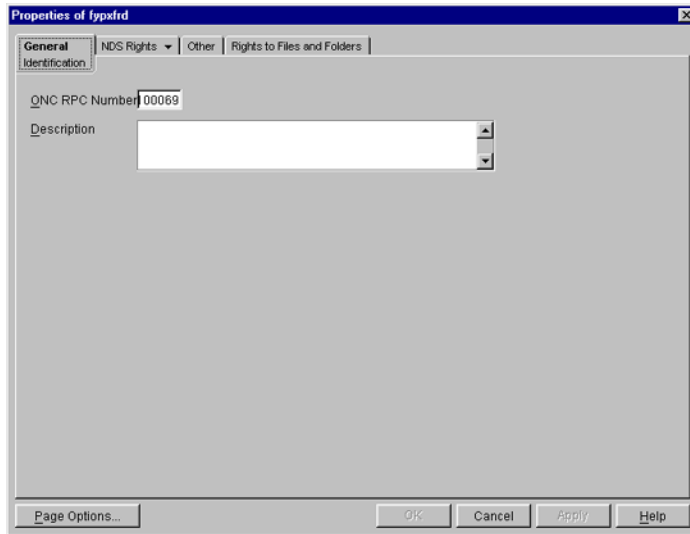
- 1** To enter the IP network number, click Browse, enter the network number, and click OK.
- 2** To enter the IP netmask number, click Browse, enter the netmask number, click OK, enter the description of the record, and then click Apply > OK.

Figure 26 Protocols Map Records Properties Panel



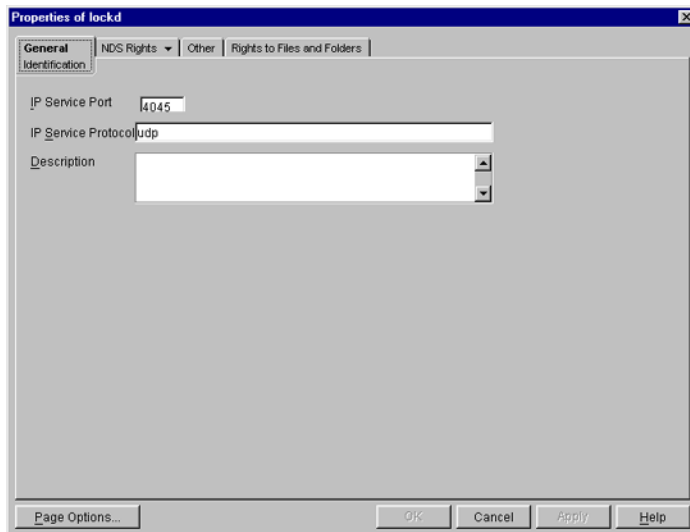
- 1** Enter the protocol number and a brief description of the record.
- 2** Click Apply > OK.

Figure 27 RPC Map Records Properties Panel



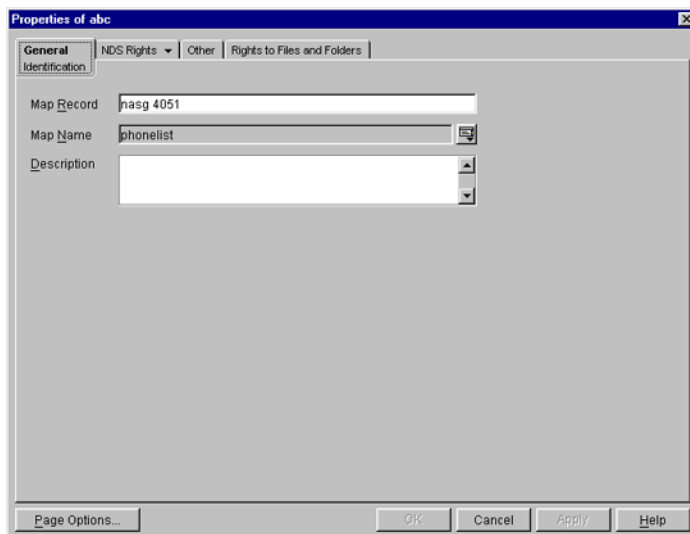
- 1** In the ONC RPC Number field, enter the RPC number of the program.
- 2** Enter a brief description of the record.
- 3** Click Apply > OK.

Figure 28 Services Map Records Properties Panel



- 1** In the IP Service Port field, enter the port number that this service is available on.
- 2** In the IP Service Protocol field, enter the protocol used to access the specified service.
- 3** Enter a brief description of the record.
- 4** Click Apply > OK.

Figure 29 General Map Records Properties



- 1 In the Map Record field, specify the map record using the following format:
key record
- 2 Enter the map name that the record belongs to.
- 3 Enter a brief description of the record.
- 4 Click Apply > OK.

Starting and Stopping NIS Server from ConsoleOne

Right-click NISSERV_*Servername* object > click Start/Stop Services.

NOTE: You can also start and stop the NIS Services by using the NIS Server menu. Make sure you refresh ConsoleOne after you change the status of NIS using the menu.

Setting Up Novell Native File Access for UNIX with Novell Cluster Services

To get the full benefit of using Novell Native File Access for UNIX with Novell Cluster Services™, the software must be installed and configured to work in a cluster environment.

This section describes the following:

- ♦ [Prerequisites \(page 89\)](#)
- ♦ [Configuring the Properties of Cluster Resource \(page 91\)](#)
- ♦ [Component-Specific Configuration \(page 93\)](#)
- ♦ [Starting and Stopping Native File Access for UNIX with Cluster Services \(page 94\)](#)

Prerequisites

Before installing Native File Access for UNIX with cluster support, create at least one shared pool and at least one volume in that pool.

- 1 Create the directory SYS:\NFSBACK.

- 2** Make a backup of the configuration files.
 - ◆ When cluster enabling for the first time, copy the configuration files NFS.CFG, NFSSERVER.CFG, NIS.CFG and NISSERV.CFG from SYS:\ETC to SYS:\NFSBACK.
 - ◆ When upgrading from a previously cluster enabled setup, copy the configuration files NFS.CFG, NFSSERVER.CFG, NIS.CFG and NISSERV.CFG from *Shared Vol Name* :ETC to SYS:\NFSBACK
- 3** Create a new sharable NSS partition.
- 4** In this partition, create a pool. Enter a name for the virtual server and the IP Address in the pop box displayed. Do not use nfsclust as this is a reserved word.

NOTE: ConsoleOne creates a virtual server as *clust-obj-name given_server* and also cluster volume resource object with *name given_server* in the cluster object.
- 5** Create a Cluster Pool and its object from ConsoleOne. To do this:
 - 5a** From the Tools menu > select Disk Management > NSS Pools.
 - 5b** Identify the tree / context / server. Click OK.
 - 5c** Click New to create a new pool. Give it a name. Click Next.
 - 5d** Select the storage device to be used. Adjust the used space as needed Click Next.
 - 5e** The pool attribute information appears. Make sure that the Cluster Enable on Creation box is checked. The Virtual Server name is built automatically.
 - 5f** Enter the IP address to be assigned to this virtual server (used for this shared pool).
 - 5g** Add any additional desired Advertising Protocols, then click Finish.
 - 5h** From the Media tab, select NSS Logical Volumes.
 - 5i** Click new and create at least one volume within the pool.

IMPORTANT: Instead of a pool object in the normal format <servername>_<poolname>_POOL, it will be named <clustername>_<poolname>_POOL. A virtual server object associated with the shared pool will be created, called <clustername>_<poolname>_SERVER. ConsoleOne also creates a Cluster Pool resource object called <poolname>_SERVER, inside the Cluster Container object.

For example, given a cluster named NFSC, shared pool named NFSP, and volume named VOL1, the objects seen would be:

Cluster container object: NFSC

Pool Object: NFSC_NFSP_POOL

Virtual Server Object: NFSC_NFSP_SERVER

Volume Object: NFSC_VOL1

Cluster pool resource object within cluster container: NFSP_SERVER

Setting Up

- 1** Install Native File Access For UNIX on all the nodes in the cluster.
- 2** On each node of the cluster, if the NFS Services are running, run **NFSSTOP**.Unload NFSADMIN and PKERNEL.Remove NFSSTARTfrom AUTOEXEC.NCF.
- 3** Delete all the NISSERV_<servername> objects in eDirectory.
- 4** To cluster enable and upgrade the configuration, use **SPINST**.

- ♦ **To cluster enable for the first time:** execute the following command on all nodes, one by one. Make sure to have the shared volume residing on the node at the time you run the command:

```
spinst -o 2 -v SHARE_VOL_NAME: -n RES_NAME -i RES_IP
```

Using the example names given in the prerequisites section, and assuming the address 10.2.3.4 is assigned to the shared pool, the command would be:

```
spinst -o 2 -v VOL1: -n NFSP_SERVER -i 10.2.3.4
```

- ♦ **To upgrade from a previously cluster enabled setup:** execute the following command on all nodes, one by one. Make sure to have the shared volume residing on the node at the time you run the command):

```
spinst -o 3 -v SHARE_VOL_NAME: -n RES_NAME -i RES_IP
```

In the command, you need to specify the shared volume name for -v, the resource name for -n and the resource IP address for -i.

Using the example names given in the prerequisites section, the command would be:

```
spinst -o 3 -v VOL1: -n NFSP_SERVER -i 10.2.3.4
```

- 5** Create an ETC directory on the shared volume. Copy the following files to shared_volume:\ETC\ :

```
sys:\etc\nis.cfg
```

```
sys:\etc\nfs.cfg
```

```
sys:\etc\nfsserv.cfg
```

```
sys:\system\nfsstart.ncf
```

```
sys:\system\nfsstop.ncf
```

Configuring the Properties of Cluster Resource

Load and Unload Script

Within the Cluster contain object (Console view), right-click the Cluster Pool resource object and then click Properties. Select the Scripts tab to find the Cluster Resource Load Script and Cluster Resource Unload Script. Following are the formats for these scripts.

Load Script

To the load script, add the following at the end of the existing script:

```
nfsclust AAA.BBB.CCC.DDD shared_vol_name shared_pool_name_SERVER
```

```
shared_vol_name:\ETC\NFSSTART
```

For the example names used in this document, the specific commands would be:

```
nfsclust 10.2.3.4 VOL1 NFSP_SERVER
```

```
VOL1:\ETC\NFSSTART
```

Unload Script

To the unload script, add the following at the beginning of the existing script:

```

shared_vol_name:\ETC\NFSSTOP
#(VOL1:\ETC\NFSSTOP, for our example)
unload nfsclust
unload nfsadmin
delay 2
unload pkernel

```

NOTE: A small delay might be needed before PKERNEL can unload, to allow dependant modules to finish unloading first. If the unload pkernel command fails, the pool may go comatose rather than migrate successfully. The delay command serves this purpose.

Setting the Start, Failover, and Failback Modes

The following table explains the different resource modes.

Mode	Setting	Description
Start	AUTO, MANUAL	AUTO allows Native File Access for UNIX to automatically start on a server when the cluster is first brought up.
		MANUAL lets you manually start Native File Access for UNIX on a server whenever you want. Default = AUTO
Failover	AUTO, MANUAL	AUTO allows Native File Access for UNIX to automatically start on the next server in the Assigned Nodes list in the event of a hardware or software failure.
		MANUAL lets you intervene after a failure occurs and before Native File Access for UNIX is moved to another node. Default = AUTO

Mode	Setting	Description
Failback	AUTO, MANUAL, DISABLE	<p>AUTO allows Native File Access for to UNIX automatically move back to its preferred node when the preferred node is brought back online.</p> <p>MANUAL prevents Native File Access for UNIX from moving back to its preferred node when that node is brought back online until you are ready to allow it to happen.</p> <p>DISABLE causes Native File Access for UNIX to continue running in an online state on the node it has failed to.</p> <p>Default = DISABLE</p>

To view or change the Start, Failover, and Failback modes, do the following:

- 1** In ConsoleOne, double-click the cluster object container.
- 2** Right-click the cluster resource object *shared vol name_SERVER* and select Properties.
- 3** Click the Policies tab on the property page.
- 4** View or change the Start, Failover, or Failback mode.

Component-Specific Configuration

The procedure to configure the components of Native File Access for UNIX is much the same as when you configure the components without cluster services. However, some points must be kept in mind while configuring the following components:

- ◆ [NFS Server \(page 93\)](#)
- ◆ [Network Information Service \(page 94\)](#)

For the location of the configuration files for Native File Access for UNIX with and without Cluster Services, see [“Location of Configuration Files” on page 94](#).

NFS Server

While configuring the NFS Server, note the following:

- ◆ Only the volumes in the pool can be exported.
- ◆ When mounting exported shared volumes from an NFS client, use the virtual IP address of the cluster volume object.

For more information on configuring the NFS Server, see [“ConsoleOne-Based Management for NFS Server” on page 72](#).

Network Information Service

While configuring the NIS clients, note the following:

- ◆ Bind the NIS clients to NIS server running on the cluster using a virtual IP address.

Location of Configuration Files

Most of the configuration files are now located in the shared volume's ETC directory. The following table lists the location with and without the cluster services.

Table 3 Location of Configuration Files

Filename	Without Cluster Services	With Cluster Services
NFS.CFG	SYS:\ETC	<i>shared_vol_name</i> :\ETC
NIS.CFG	SYS:\ETC	<i>shared_vol_name</i> :\ETC
NFSSERV.CFG	SYS:\ETC	<i>shared_vol_name</i> :\ETC
NFSEXPRT	SYS:\ETC	<i>shared_vol_name</i> :\ETC
NFSTHOST	SYS:\ETC	<i>shared_vol_name</i> :\ETC
Log file for NFSSERV (default is NFSSERV.LOG)	SYS:\ETC	<i>shared_vol_name</i> :\ETC
NISMAKE	SYS:\ETC\NIS	SYS:\ETC\NIS
NFSSTART.NCF	SYS:\SYSTEM	<i>shared_vol_name</i> :\ETC
NFSSTOP.NCF	SYS:\SYSTEM	<i>shared_vol_name</i> :\ETC

Starting and Stopping Native File Access for UNIX with Cluster Services

- 1** To start NFS Services, from Cluster ConsoleOne, click Cluster Object > View > Cluster State > Cluster Vol Object Online.
- 2** To stop NFS Services, from ConsoleOne, click Cluster Object > View > Cluster State > Cluster Vol Object Offline.

For additional information on setting up and configuring Novell Cluster Services, see the [Novell Cluster Services Overview and Installation Guide \(http://www.novell.com/documentation/lg/ncs6p/index.html\)](http://www.novell.com/documentation/lg/ncs6p/index.html).